

May 12, 2003

MEMORANDUM TO: James Lyons, Director
New Reactor Licensing Project Office
Office of Nuclear Reactor Regulation

FROM: Michael Tschiltz, Chief/~~RA~~ M. Rubin for
Probabilistic Safety Assessment Branch
Division of Systems Safety and Analysis
Office of Nuclear Reactor Regulation

SUBJECT: SPSB INPUT TO AP1000 DSER - CHAPTERS 19.2, 19.4 and 20.

Attached is a part of the SPSB input to the Draft Safety Evaluation Report. It contains chapters 19.2, 19.4, and SPSB input to Chapter 20. Please, note that the section 19.2.6 (Containment Ultimate Capability) is missing. Draft Section 19.2.6 is being developed by Division of Engineering (Goutam Bagchi) and will be sent to you separately.

Attachment: As stated

CONTACTS: R. Palla, SPSB/DSSA, 415-1095
A. Drozd, SPSB/DSSA, 415-1308

May 12, 2003

MEMORANDUM TO: James Lyons, Director
New Reactor Licensing Project Office
Office of Nuclear Reactor Regulation

FROM: Michael Tschiltz, Chief/~~RA~~ M. Rubin for
Probabilistic Safety Assessment Branch
Division of Systems Safety and Analysis
Office of Nuclear Reactor Regulation

SUBJECT: SPSB INPUT TO AP1000 DSER - CHAPTERS 19.2, 19.4 and 20.

Attached is a part of the SPSB input to the Draft Safety Evaluation Report. It contains chapters 19.2, 19.4, and SPSB input to Chapter 20. Please, note that the section 19.2.6 (Containment Ultimate Capability) is missing. Draft Section 19.2.6 is being developed by Division of Engineering (Goutam Bagchi) and will be sent to you separately.

Attachment: As stated

Distribution: SPSB: r/f

Accession#ML031320760

G:\spsb\drozd\Ap1MEMO-DSER-19-2.wpd

NRR-106

OFFICE	SPSB	SPSB	SPSB/DSSA	SPSB/DSSA
NAME	ADrozd	RPalla	MRubin	MTschiltz/ RA MRubin for
DATE	05/12/03	05/12/03	05/12/03	05/12/03

OFFICIAL RECORD COPY

19.2 Severe Accident Performance

19.2.1 Introduction

The purpose of Section 19.2 is to evaluate the approach proposed by Westinghouse for resolving severe accident issues for the AP1000 design and determine whether the criteria in SECY-93-087, SECY-96-128, SECY-97-044 and the corresponding SRMs dated July 21, 1993, January 15, 1997, June 30, 1997, respectively, have been met.

To provide adequate protection of the public health and safety, current NRC regulations require conservatism in design, construction, testing, operation, and maintenance of nuclear power plants. A defense-in-depth approach has been mandated in order to prevent accidents from happening and, if accidents should occur, to mitigate their consequences. Siting in less populated areas is emphasized. Furthermore, the NRC, State, and local governments mandate emergency response capabilities to provide additional defense-in-depth protection to the surrounding population.

The reactor and containment systems design are a vital link in the defense-in-depth philosophy. Current reactors and containments are designed to withstand a LOCA and to comply with the siting criteria of 10 CFR Part 100 and general design criteria of Appendix A to 10 CFR Part 50. The large-break LOCA and other accidents analyzed in accordance with the NRC's SRP are documented in Chapters 6 and 15 of the AP1000 DCD Tier 2.

The high-level of confidence in the defense-in-depth approach results, in part, from stringent requirements for meeting the single failure criterion, redundancy, diversity, quality assurance, and utilization of conservative models. The staff concludes that existing requirements ensure a safe containment design.

The NRC also has requirements to address conditions beyond the traditional design-basis spectrum, such as anticipated transients without scram (10 CFR 50.62), station blackout (10 CFR 50.63), and combustible gas control (10 CFR 50.44); however, a definitive set of regulatory requirements for addressing specific severe accident phenomena does not exist. However, an assessment of the severe accident response of a proposed design provides useful insights regarding its response to accidents of extremely low likelihood that are beyond the plant design basis. Existing regulations that require conservative analyses and inclusion of features for design-basis events provide margin for severe accident challenges. This design-basis margin coupled with regulatory guidance to address severe accidents in the form of policy positions ensures a robust design that satisfies the Commission's policy statement on severe accidents.

19.2.2 Deterministic Assessment of Severe Accident Prevention

19.2.2.1 Severe Accident Preventive Features

The design of the AP1000 copes with plant transients and LOCAs without any adverse impact on the environment. However, the potential does exist, albeit remote, for a LOCA or seemingly ordinary plant transient coupled with numerous plant failures to progress to a severe accident with the potential for substantial offsite releases. Such potential is used through the use of probabilistic risk assessment methods.

Accident initiators separate 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, loss of offsite power, and loss of feedwater. In addition to these transients, there is an entire spectrum of LOCAs that are accident initiators. LOCAs fall into three categories: small, medium, and large, dependent on the size of the line break.

Following the accident initiator, normal and emergency plant systems respond to control reactivity, reactor pressure, reactor water level, steam generator water level, and containment parameters within the design-bases spectrum. Of most importance is to ensure inventory control and sufficient heat removal from the core to prevent overheating and subsequent fuel damage. Failure to provide heat removal or inventory control results in core uncover, fuel overheating, and the potential for oxidation and melting of the reactor core.

In response to accident initiators identified through operating reactor experience and performance of probabilistic risk assessments, the NRC developed criteria for advanced light water reactors (ALWRs) to prevent the occurrence of such initiators from leading to a severe accident. In SECY-93-087 the staff specifies these criteria and include design provisions for the following: anticipated transients without scram, mid-loop operation, station blackout, fires, and intersystem loss-of-coolant accidents.

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 reactor coolant pumps, tripping of the turbine generator set, isolation of the main condenser, and loss of all offsite power. Depending on the transient and its severity, the plant may recover and continue normal operation, or the plant may require an automatic shutdown (scram) via the RPS. The RPS is designed to safely shut down the reactor to prevent core damage.

These transients, when coupled with a failure of the RPS, may lead to conditions beyond what some plants were originally designed to meet. In these cases, the reactor must be manually scrammed in order to avoid reactor fuel damage or coolant system damage. Subsequent failure of the manual scram system and inadequate core cooling would lead to core damage.

Transients with the greatest potential for significant damage to the reactor core and containment are those that lead to an increase in reactor pressure and temperature, a loss of feedwater, or a failure of the RPS to scram the reactor. During an ATWS event, reactor power, pressure, and temperature must be controlled or the potential exists for a severe accident.

In SECY-93-087, the staff indicated that it was evaluating the passive designs to ensure compliance with Commission regulations and guidance regarding ATWS. Regulations to address ATWS were promulgated in 10 CFR 50.62. The Commission issued further guidance in its SRM of June 26, 1990, which stated that diverse scram systems should be provided. However, the Commission also directed that the staff should accept an applicant's alternative to the diverse scram system, if the applicant can demonstrate that the consequences of an ATWS are acceptable.

As described in Section 7.7.1.11 of the AP1000 DCD Tier 2 has a diverse actuation system (DAS). The staff's evaluation of the DAS to meet the requirements of 10 CFR 50.62 is contained in Sections 7.7.2 and 15.2.7 of this report. On the basis of the staff's evaluation of the DAS to meet the requirements 10 CFR 50.62, the staff concludes that the AP1000 design conforms to the ATWS criteria specified in SECY-93-087.

19.2.2.1.2 Mid-Loop Operation

During refueling or maintenance activities, the reactor coolant system is sometimes reduced to a "mid-loop" level. During this period, the potential exists for loss of decay heat removal capability as a result of air entrainment of the RHR pumps. In SECY-93-087, the staff indicates that all passive plants must have a reliable means of maintaining decay heat removal capability during all phases of shutdown activities, including refueling and maintenance. Westinghouse summarizes the specific AP1000 design features that address mid-loop operations in Section 5.4.7.2.1 of the DCD Tier 2. Availability controls for the normal heat removal system (RNS) during mid-loop operations have been provided in Table 16.3-2, "Investment Protection Short-Term Availability Controls," of the DCD Tier 2. On the basis of the staff's evaluation in Section 19.3, "Shutdown Evaluation," and Chapter 22, "Regulatory Treatment of Non-safety Systems," of this report and the additional availability controls provided for the RNS during normal and reduced inventory in Table 16.3-2 of the DCD Tier 2, the staff concludes that the AP1000 design conforms to the mid-loop operation criteria specified in SECY-93-087.

19.2.2.1.3 Station Blackout

An SBO involves the complete loss of alternating current (ac) electric power to the essential and nonessential switchgear buses in a nuclear power plant (i.e., a LOOP concurrent with turbine trip and unavailability of the onsite emergency ac power system).

In accordance with SECY-90-016, the evolutionary designs provided a large-capacity, alternate ac power source with the capability to power one complete set of normal safe-shutdown loads. However, the AP1000 does not rely on active systems for safe shutdown following an event. The AP1000 design has redundant non-safety-related onsite ac power sources (diesel generators) to provide electrical power for the non-safety-related active systems that provide defense-in-depth. In SECY-93-087, which expanded on the guidance given in SECY-90-016, the staff indicated that it believed that the diesel generators might require some regulatory treatment.

The staff outlined the process for resolving the regulatory treatment of non-safety systems 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 8.6.2.4 of this report. Additional availability controls have been provided for the electrical power systems in Table 16.3-2, "Investment Protection Short-Term Availability Controls," of the DCD Tier 2. On the basis of the staff's evaluation in Section 8.6.2.1, "Station Blackout," of this report and the additional availability controls provided in Table 16.3-2 of the DCD Tier 2, the staff concludes that the AP1000 design conforms to the station blackout criteria specified in SECY-93-087, and is therefore, acceptable.

19.2.2.1.4 Fire Protection

The Commission concluded that fire protection issues that have been raised through operating experience and the External Events Program must be resolved for passive LWRs. In SECY-93-087, the staff recommended that the Commission approve the position that the passive plants be reviewed against the enhanced fire protection criteria specified for evolutionary designs in SECY-90-016. The Commission, in an SRM dated June 26, 1990, subsequently approved this position. In an SRM dated July 21, 1993, the Commission approved the staff's position for passive plants and asked to be kept informed of the staff's resolution of the issue related to common-mode failures through common ventilation systems. A description of the AP1000's fire protection system is in Section 9.5.1 of the DCD Tier 2 and the fire protection analysis is contained in Appendix 9A of the DCD Tier 2. The staff's acceptance of the AP1000 fire protection systems relative to the criteria in SECY-93-087 is discussed in Section 9.5.1 of this report.

19.2.2.1.5 Intersystem Loss-of-Coolant Accident

Intersystem LOCAs (ISLOCAs) are defined as a class of LOCAs in which a breach occurs in the interface of the RCS pressure boundary with a system of lower design pressure. The breach may occur in portions of piping located outside of the primary containment, causing a direct and potentially unisolable discharge from the RCS to the environment. An ISLOCA is of concern because of potential direct releases to the environment, loss of core cooling, and loss of core makeup. An ISLOCA occurs when high pressure is introduced to a low-pressure system as the result of valve(s) failure or an inadvertent valve actuation. In either case, the overpressurization can cause the low-pressure system or components to fail.

In SECY-93-087, the staff recommended that the Commission approve the position that the passive plants be reviewed for compliance with the ISLOCA criteria approved in the Commission's SRM of June 26, 1990, relating to SECY-90-016. In an SRM dated July 21, 1993, the Commission approved the staff's position for passive plants.

In SECY-90-016, the staff recommended that designs reduce the possibility of a LOCA outside containment by designing (to the extent practicable) all systems and subsystems connected to the RCS to an ultimate rupture strength (URS) at least equal to the full RCS pressure. The "extent practicable" phrase is a realization that all systems must eventually interface with atmospheric pressure and that for certain large tanks and heat exchangers, it would be difficult or prohibitively expensive to design such systems to a URS equal to full RCS pressure. The staff further recommended that systems that have not been designed to withstand full RCS pressure should include the following attributes: (a) the capability for leak testing of the pressure isolation valves, (b) valve position indication that is available in the control room when isolation valve operators are de-energized, and (c) high-pressure alarms to warn control room operators when rising reactor coolant pressure approaches the design pressure of attached low-pressure systems and both isolation valves are not closed.

The staff evaluated the issue of ISLOCA for AP600, relative to the criteria of SECY-93-087, as part of its resolution of Generic Safety Issue 105 in Section 20.3 of NUREG 1512. The staff concluded that the AP600 design conforms to the ISLOCA criteria specified in SECY-93-087. Since these criteria remain valid, and the staff's review of the relevant AP1000 piping revealed

the AP1000 piping is identical to that of AP600, therefore the acceptance of ISLOCA for AP600 can be extended to AP1000.

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 m³ (2,060,000 ft³). 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 passive containment cooling system (PCCS) is a safety-related system that removes heat directly from the containment vessel and transmits it to the environment. The PCCS uses the steel containment vessel as a heat transfer surface. The surrounding concrete shield building is used, along with a baffle, to direct air from the top-located air inlets down to a lower elevation of the containment and back up along the containment vessel. A 2,858 m³ (755,000 gallon) water storage tank is supported by the shield building to allow gravity drain of the water exterior to, and on the top of the steel containment vessel. Indications of inadequate containment cooling, such as high containment pressure or temperature, automatically initiate the PCCS water flow. These signals open valves to initiate the flow of water onto the top of the containment vessel. The air and the evaporated water exhaust through an opening in the roof of the shield building.

19.2.3.2 Severe Accident Progression

A description of the processes, both physical and chemical, that may occur during the progression of a severe accident, and how these phenomena affect containment performance, follows in this section. Due to the complex processes involved there will be potential variability in the postulated core melt progression scenarios. Assessments reported previously in NUREG/CR-5132, NUREG/CR-5597, and NUREG/CR-5564 provide generic insights that are also applicable to the AP1000 design. The following is a summary of the accident progression information applicable to the AP1000 response to postulated severe accident scenarios.

Severe accident progression can be divided into in-vessel and ex-vessel phases. The in-vessel phase generally begins with insufficient decay heat removal and can lead to melt-through of the reactor vessel. The ex-vessel phase involves the release of the core debris from the reactor vessel into the containment, which results in phenomena such as core-concrete interaction, fuel-coolant interaction, and direct containment heating.

19.2.3.2.1 In-Vessel Melt Progression

In severe accidents that proceed to vessel failure and release of molten core material into the containment, the in-vessel melt progression establishes the initial conditions for assessing the

thermal and mechanical loads that may ultimately threaten the integrity of the containment. In-vessel melt progression encompasses the phenomena and processes involved in a severe core damage accident starting with core uncover and initial heatup, and continuing until either of the following occurs: (a) stabilization and cooling of the degraded core within the reactor vessel, or (b) breach of the reactor vessel occurs and molten core material is released into the containment. The phenomena and processes in the AP1000 that can occur during in-vessel melt progression include:

- core heatup resulting from loss of adequate cooling
- metal-water reaction and cladding oxidation
- eutectic interactions between core materials
- melting and relocating cladding, structural materials, and fuel
- formation of blockages near the bottom of the core as a result of the solidification of relocating molten materials (wet core scenario)
- drainage of molten materials to the vessel lower head region (dry core scenario)
- formation of melt pool, natural circulation heat transfer, crust formation, and crust failure (wet core scenario), and
- reactor vessel breach from a local failure or global creep-rupture.

Removal of decay heat produced by the core must take place in order to achieve adequate core cooling and prevent initiation of a severe accident. In the event that all of the safety-related and non-safety-related systems fail to remove the decay heat, the core will heat up to the point at which damage to the fuel and fuel cladding may occur. Transfer of decay heat is through the radiative, conductive, and convective heat transfer to the steam, other core materials, and non-fuel materials within the reactor. The insufficient cooling supply results in coolant boiloff and a decreasing level within the reactor vessel as the decay heat generation exceeds the heat removal rate. The coolant level within the core further decreases so that the fuel rods above the coolant level cool only by rising steam. The fuel rods begin to overheat and cladding oxidation in the presence of steam begins at high temperatures. Generation of hydrogen and additional heat occurs as the cladding oxidizes in the presence of steam. A zirconium alloy called Zircaloy makes up the fuel cladding for AP1000. The initial Zircaloy oxidation involves oxygen diffusion through a ZrO_2 surface layer. As the fuel rods continue to heat up from decay heat and the exothermic zirconium oxidation reaction occurs, the expectation is that materials within the reactor with low melting points will melt first and may form eutectics. Eutectics are mixtures of materials with a melting point lower than that of any other combination of the same components.

Zircaloy, with a melting point of 1,757 °C (3,194 °F), begins to melt during a severe accident, breaking down the protective ZrO_2 layer, which exposes unoxidized Zircaloy. Following this, local melting of the fuel rods may cause changes in the core geometry resulting in differing steam flow paths. This can lead, on the one hand, to an increase in the oxidation process as access to the unoxidized Zircaloy becomes available; on the other hand, the melt formation or

changes in the steam flow path could reduce the Zircaloy surface available for oxidation and thereby decrease the overall reaction process. In some accident scenarios in which residual amounts of water remain in the bottom of the core and lower plenum, substantial steaming and oxidation can take place.

In addition to oxidation, the potential exists for the Zircaloy to interact with the UO_2 fuel, forming low-melting-point eutectics. Formation of eutectics may decrease the effective surface area for oxidation and the overall oxidation rate. The melting point of Zircaloy depends on its state and lattice structure. Zircaloy has three melting points: 1,877 °C (3,410 °F) (beta-Zr), 1,977 °C (3,590 °F) (alpha-Zr(O)), and 2,677 °C (4,850 °F) (ZrO_2). When partially oxidized Zircaloy is in contact with UO_2 , an alpha-Zr(O)/ UO_2 -based eutectic will form with a liquefaction temperature of approximately 1,897 °C (3,446 °F). Therefore, in the presence of good fuel/cladding contact, fuel liquefaction and melt relocation will commence around this temperature. This has the potential to affect the oxidation behavior of Zircaloy-based melt.

Various severe fuel damage (SFD) test programs sponsored by the NRC indicate that the oxidation of the Zircaloy is largely controlled by the availability of a steam supply and that high rates of hydrogen generation can continue after melt formation and relocation. Some of these experiments indicate that the majority of the hydrogen generation occurred after onset of Zircaloy melting and fuel dissolution. In steam-rich experiments, oxidation took place over most of the fuel bundle length and most of the hydrogen generation occurred early. For steam-starved experiments, oxidation was limited to local regions of the fuel bundle, and the majority of the hydrogen generation occurs after the onset of Zr/ UO_2 liquefaction and relocation.

Hydrogen production and accumulation during a severe accident may represent challenges to the containment in numerous ways, including deflagration, detonation, and pressurization, as hydrogen gas is non-condensable. The AP1000 containment has 64 hydrogen igniters to consume hydrogen as it is produced during a severe accident, thereby introducing the potential for hydrogen detonation events that would challenge containment integrity.

The SFD tests indicated the potential for incoherent melt-relocation as a result of non-coherent temperatures within the test bundles. This is because of the different core materials present with a wide range of melting points and eutectic temperatures. Formation of eutectics would result in a nonuniform melting and relocation process. Further differences in the melt-relocation process can be attributed to asymmetric bundle heating that can increase upon Zircaloy oxidation. This process begins when one area of the fuel bundle is initially at a temperature higher than the other areas. The higher temperature Zircaloy will consume the available steam through oxidation at a quicker rate. The oxidation reaction increases the hotter areas to even higher temperatures, which further increases the oxidation rate and the local temperatures. This autocatalytic nature of Zircaloy oxidation appears to contribute to asymmetric bundle heatup and the potential for incoherent melt relocation behavior.

As the temperature of the core increases, vaporization and release of some fission products occur. Steam and/or hydrogen then carry these fission products throughout the primary system where they are subject to deposition on the surfaces of internal components. The deposition mechanisms include condensation on the heat sinks (diffusiophoresis), gravitational settling, and thermophoresis. The fission products that are not deposited remain airborne and are released to the containment, where the dominant removal mechanisms are gravitational settling and diffusiophoresis.

The core melt progression, including relocation and fission product release, becomes increasingly difficult to predict as it continues to degrade. The core melt could relocate into the lower reactor vessel plenum. If water is present in the lower plenum, the potential exists for in-vessel steam explosions, where molten core rapidly fragments and transfers its energy, causing rapid steam generation and shock waves. Once in the lower plenum, the potential exists to halt the core melt progression through external vessel cooling. The AP1000 is designed to flood up the reactor cavity with water from the IRWST, thereby providing cooling of the core debris through the reactor vessel.

The in-vessel core melt progression, including core degradation, relocation, and failure of the reactor vessel, contains considerable uncertainty. This uncertainty includes the following:

- the potential for in-vessel steam explosion (see Section 19.2.3.3.5.1 of this report)
- the interaction between core debris and internal vessel structures
- the potential for external vessel cooling of core debris (see Section 19.2.3.3.1 of this report)
- the time and mode of vessel failure
- the composition of the core debris released at vessel failure
- the amount of in-vessel hydrogen generation
- the in-vessel fission-product release and transport, and
- retention of fission products and other core materials in the RCS.

19.2.3.2.2 Ex-Vessel Melt Progression

The following conditions affect ex-vessel severe accident progression:

- the mode and timing of the reactor vessel failure
- the primary system pressure at reactor vessel failure
- the composition, amount, and character of the molten core debris expelled
- the type of concrete used in containment construction, and
- the availability of water to the reactor cavity

The initial response of the containment from ex-vessel severe accident progression is largely a function of the pressure of the RCS at reactor vessel failure and the existence of water within the reactor cavity. If not prevented by design features, early containment failure mechanisms and bypass usually dominate risk consequences. Early containment failure mechanisms result from energetic severe accident phenomena, such as high pressure melt ejection with direct containment heating and ex-vessel steam explosions. The long-term containment pressure and temperature response from ex-vessel severe accident progression is largely a function of an interaction between molten core and concrete, known as core-concrete interaction (CCI), and the availability of mechanisms to remove heat from the containment.

At high RCS pressures, ejection of the molten core debris from the reactor vessel could occur in jet form, causing fragmentation into small particles. The potential exists for the core debris ejected from the vessel to be swept out of the reactor cavity and into the upper containment. Finely fragmented and dispersed core debris could heat the containment atmosphere and lead to large pressure spikes. In addition, chemical reactions of the core debris particulate with oxygen and steam could add to the pressurization loads. Hydrogen, pre-existing in the containment or produced during direct containment heating, could ignite adding to the loads on the containment. This phenomena is known as high pressure melt ejection with direct containment heating.

Reactor vessel failure at high or low pressure coincident with water present within the reactor cavity may lead to interactions between fuel and coolant with the potential for rapid steam generation or steam explosions. Rapid steam generation involves the pressurization of containment compartments from nonexplosive steam generation beyond the capability of the containment to relieve the pressure so that the containment fails because of local overpressurization. Steam explosions involve the rapid mixing of finely fragmented core debris with surrounding water resulting in rapid vaporization and acceleration of surrounding water creating substantial pressure and impact loads.

The eventual contact of molten core debris with concrete in the reactor cavity will lead to core-concrete interaction (CCI.) Such interaction will lead to a decomposition of concrete and can challenge the containment by various mechanisms, including: (a) pressurization as a result of the production of steam and noncondensable gases to the point of containment rupture, (b) the transport of high-temperature gases and aerosols into the containment leading to high-temperature failure of the containment seals and penetrations, (c) containment liner melt-through, (d) reactor support structures melt-through leading to the relocation of the reactor vessel and tearing of containment penetrations, and (e) the production of combustible gases such as hydrogen and carbon monoxide. CCI is affected by many factors, including the availability of water to the reactor cavity, the containment geometry, the composition and amount of core debris, the core debris superheat, and the type of concrete involved.

19.2.3.3 Severe Accident Mitigative Features

19.2.3.3.1 External Reactor Vessel Cooling (ERVC)

The AP1000 design incorporates ERVC as a strategy for retaining molten core debris in-vessel in severe accidents. The objective of ERVC is to remove sufficient heat from the vessel exterior surface that the thermal and structural loads on the vessel (from the core debris which has relocated to the lower head) do not lead to failure of the vessel. By maintaining RPV integrity, the potential for large releases due to ex-vessel severe accident phenomena (i.e., ex-vessel FCIs and CCI) is eliminated. A residual challenge to containment from hydrogen combustion remains, but it diminishes with successful ERVC since combustible gas production would be limited to in-vessel hydrogen generation. ERVC will remove some decay heat through the RPV in design basis LOCAs (which result in a flooded reactor cavity as a direct consequence of the sequence), but in the absence of loss of core cooling and core debris relocation, this heat removal is insignificant and is not credited in design-basis accidents. This section provides the results of the staff's review of the ERVC strategy for the AP1000.

Background

The AP1000 design includes several features that enhance ERVC relative to operating plants, specifically: (1) safety-grade systems to provide RCS depressurization and reactor cavity flooding, (2) a "clean" lower head that is unobstructed by in-core instrument lines or other penetrations, and (3) a RPV thermal insulation system which limits thermal losses during normal operations, but provides an engineered pathway for supplying water cooling to the vessel and venting steam from the reactor cavity during severe accidents. The AP1000 design further enhances the ability to flood the reactor cavity by a containment and reactor cavity arrangement which permits the RCS inventory (breakflow) to drain to the cavity, in addition to the manually-actuated cavity flooding system.

ERVC is credited with preventing RPV failure in the AP1000 PRA on the basis of a DOE-sponsored analysis by the University of California, Santa Barbara (UCSB) using the Risk Oriented Accident Analysis Methodology (ROAAM). The UCSB analysis of ERVC, documented in DOE/ID-10460, "In-Vessel Coolability and Retention of a Core Melt", July 1995 (Peer Re-Review Version) and October 1996 (Final), concluded that thermally-induced failure of an AP600-like reactor vessel is "physically unreasonable" provided the RCS is depressurized and the RPV is submerged in water to a depth of at least the top of the debris pool. Based on AP1000-specific testing and analyses (and resulting modifications to the AP1000 insulation design), this work was extended to the AP1000 design, and, similar to the AP600 PRA, sequences with successful RCS depressurization and reactor cavity flooding are assigned zero probability of vessel breach, and sequences with either inadequate RCS depressurization or reactor cavity flooding are assumed to fail the reactor vessel and containment in the AP1000 PRA.

Staff review of ERVC centered on 3 major areas including: (1) the likelihood of achieving RCS depressurization and reactor cavity flooding in the AP1000 design, both of which are required for successful ERVC, (2) the likelihood of maintaining RPV integrity given successful RCS depressurization and reactor cavity flooding, and (3) system-related considerations and design requirements for the cavity flooding system and the RPV thermal insulation system. The results of the review are provided below.

19.2.3.3.1.1 Likelihood of Achieving Requisite Conditions for ERVC in AP1000

Both RCS depressurization and reactor cavity flooding are required for successful ERVC. Important considerations include the manner in which these conditions are defined in the PRA success criteria, the potential for the RCS to be depressurized automatically or by manual backup of ADS, and the potential for the reactor cavity to be flooded passively by gravity draining or by manual actuation of the cavity flooding system.

The AP1000 PRA defines the success criteria for ERVC as: (1) depressurization of the RCS to below 150 psi before RCS pressure boundary challenge, and (2) flooding of the reactor cavity to a level above the reactor vessel nozzle gallery (98-ft elevation) prior to the time at which core debris would relocate to the lower head, vaporize the water in the lower head, and reheat to the point of melting additional structures. Each of these criteria is discussed below.

RCS Depressurization

RCS depressurization can occur as a result of the initiating event (e.g., a large LOCA), or operation of the safety-grade ADS. In the event that automatic actuation of the ADS does not occur, manual actuation is addressed in Emergency Response Guidelines and credited in the PRA. In the Level 1 PRA, the majority of Level 1 sequences (about 90 percent) involve events with at least partially successful RCS depressurization and relatively low RCS pressure (<150 psig) at the time of core uncover. For high pressure core melt sequences, the potential to depressurize the RCS in the time period between the onset of core damage and challenge of the RCS pressure boundary is further evaluated in the Level 2 event trees. After credit for late depressurization, an even larger fraction of the core melt sequences (about 95 percent) are estimated to involve a depressurized RCS before the time of substantial core damage.

The RCS pressure associated with successful ERVC in the PRA (i.e., 150 psig or less) is greater than the RCS pressure assumed in the baseline analysis in the UCSB study for AP600 (the UCSB study assumed a fully depressurized RCS). However, a supplemental structural analysis is provided in Appendix G of the UCSB report which illustrates that there is margin in the load carrying capacity of a thinned RPV (with 5 cm wall thickness) at an elevated pressure of 400 psig. The supplemental analysis considers the effect of vessel creep under high temperature and elevated pressure, and concludes that there is margin in the load carrying capacity of the vessel shell.

The pressure challenge to RPV lower head integrity for AP1000 is greater than in AP600 due to the higher decay heat level and core mass in AP1000. The higher decay heat level results in greater heat flux through the RPV lower head relative to AP600 and further thinning of the RPV wall in the region of maximum heat flux. The larger core mass results in an increased dead-load that must be carried by the thinned RPV wall. In Section 39.4 of the PRA, Westinghouse provided an assessment of the RPV wall thickness available to carry the internal loading in the portion of the vessel conducting heat at the peak critical heat flux, where maximum thinning occurs. The analysis indicates that the portion of the vessel wall available to carry the load (at a wall temperature less than the yield strength temperature of 900K) is approximately 0.8 cm thick. Given the mass of the AP1000 core and RPV internals, and the offsetting buoyancy forces on the vessel associated with a fully-flooded reactor cavity, this wall thickness is 36 times the minimum thickness required to carry the dead load.

Although significant, this margin can be eroded by residual pressure or pressure pulses within the RCS, such as might occur during late-phase core relocation or reflood of the molten core debris pool. For example, an internal pressure of 1 psid within the RPV would be roughly equivalent to the dead load on the lower head (i.e., the weight of the core debris less the buoyancy force), and a pressure of 35 psid would be sufficient to eliminate the estimated margin to failure in the thinned wall. In response to RAI 720.45, Westinghouse provided additional analyses of the RCS pressures during representative severe accident sequences, and the maximum RCS pressurization that would occur during reflood of a molten debris bed. This information indicates that the RCS is essentially fully depressurized in relevant severe accident sequences due to the lack steam generation and the available discharge area through the open ADS valves, and that the maximum RCS pressurization during reflood would be limited to about 22 psid, given the available discharge area through open ADS valves or In-containment Refueling Water System Tank (IRWST) spargers. Based on this assessment, vessel reflood is not predicted to fail the weakened vessel due to pressurization by steam.

The staff notes that the assessment of RCS pressurization during reflood is based on steaming rates from the flat plate critical heat flux and an assumption that molten fuel and coolant do not interact energetically. These assumptions are considered reasonable given the high surface temperatures of the molten debris pool and the large density differences between water and molten core debris, both of which would tend to produce film boiling. Although the potential for energetic interactions cannot be ruled out, the likelihood of such interactions will be minimized in AP1000 by COL Action Item 19.2.5-1 regarding the severe accident management program. As part of COL Action Item 19.2.5-1, the COL applicant will develop and implement severe accident management guidance on reflooding a damaged core retained in-vessel.

The staff concludes that for sequences that are considered depressurized in the PRA (and are also successfully flooded as described below), RPV structural integrity will be maintained. Thus, the success criteria for RCS pressure as applied in the AP1000 PRA is acceptable.

Reactor Cavity Flooding

On the basis of an assessment of the timing of core debris relocation and associated uncertainties, Westinghouse rationalized that the RPV lower head would not be thermally challenged until core debris would relocate to the lower head, vaporize the water in the lower head, and reheat to the point of melting additional structures. Based on a review of accident progression analyses for AP1000, Westinghouse estimated that debris bed dryout and reheat would not occur until 70 minutes after the core exit temperature first exceeds 1200F. Successful IRWST injection is necessary to meet this criterion because Core Make-up Tank (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 107 ft, which completely covers the RPV hot leg and cold legs. This final level is consistent with the containment water level simulated in tests performed by the University of California in the ULPU facility, which form the basis for the exterior heat transfer coefficients employed in the ERVC analysis for AP1000.

An assessment of reactor cavity flooding rates presented in Chapter 39 of the PRA indicates that with both cavity flood (recirculation) lines open, the 98-ft elevation is reached within about 30 minutes of opening the valves, and with one line open the same elevation is reached within about 50 or 65 minutes of opening the valves, depending on whether the less restrictive or the more restrictive of the two flooding lines is used. Thus, in the most limiting scenario the operator has about 5 minutes to open the cavity flood valves after high core exit temperatures signal the need for cavity flooding within emergency response guideline. The operator instructions to flood the cavity have been moved from the end of ERG AFR.C-1 (in AP600) to the entry of the procedure (in AP1000) to achieve the water depths and flooding times required for successful ERVC in AP1000. This procedure is entered when core exit temperatures exceed 1200F.

In the quantification of human error probabilities, the PRA assigns a probability of 0.003 to failure to recognize the need to flood the reactor cavity and open the valves in 1 of 2 lines to flood the cavity within a 20 minute time window. This probability is reasonable for AP1000 if either both flooding lines function (in which case 40 minutes would be available for operator action) or only the less restrictive of the two flooding lines functions (in which case 20 minutes is available for operator action). The assumed human error probability is optimistic for the most limiting situation in which only the more restrictive flooding line (5 minutes for operator action) is

available. However, a sensitivity study performed by Westinghouse shows that increasing this probability by a factor of 10 (for all flood line combinations) would increase the containment failure frequency by only about 30 percent (from 1.9E-8/y to 2.6E-8/y).

The effectiveness of reactor cavity flooding was confirmed by Westinghouse through MAAP calculations for selected sequences for each accident class in the PRA. These calculations, documented in Chapter 34 of the PRA, indicate that the cavity would be passively flooded before or at the time of onset of oxidation in many sequences (although not to a level sufficient to provide long-term cooling), and approximately 70 minutes or more typically exists to manually flood the cavity.

The staff performed limited calculations using the MELCOR code to confirm the general nature of core melt progression in the AP1000. Although these calculations revealed some significant differences in predicted behavior, the code comparisons confirm the order and approximate timing of major events in the accident progression, and the overall thermal hydraulic behavior during the accidents analyzed. Of particular note is the MELCOR calculation for the frequency-dominant sequence that would require manual actions to flood the reactor cavity (the 3BE sequence). The MELCOR calculation indicates that there would be approximately 75 minutes between the onset of rapid core oxidation and the first relocation of core debris into the lower head. The time between core exit temperatures exceeding 1200F and debris bed dryout will be substantially greater. These results confirm that there is margin implicit in the Westinghouse success criterion for cavity flooding. In view of this confirmation, the staff concludes that the Westinghouse characterization of melt progression and the time available for manual actions, which forms the basis for assessing the likelihood of successful operator action in the PRA, is reasonable and acceptable.

In the baseline PRA, adequate reactor cavity flooding is achieved in about 98 percent of the sequences. About half of the core damage events require operator actuation of the cavity flooding system to ensure successful cavity flooding, but the remaining half would adequately flood as a direct consequence of the accident progression, even without manual actions. The availability of the power sources, availability of the valves, ability of the operator to diagnose the situation, and success of the operator are all considered in the fault tree used to quantify the failure probability of cavity flooding. Since the system fault trees are linked to the CET, the availability of power sources is treated consistently for all sequences in the CET.

In summary, the staff concludes that the success criteria for RCS depressurization and reactor cavity flooding is appropriate, and that the safety-related systems for RPV depressurization and reactor cavity flooding provide high confidence that the requisite conditions for ERVC, i.e., a depressurized RCS and timely flooding of the reactor cavity, will be achieved in most core melt sequences. In those events where either condition is not met, the sequence is conservatively assumed to lead to containment failure in the AP1000 PRA. The staff therefore considers the PRA models and assumptions for estimating the likelihood of achieving the requisite conditions for ERVC, and the consequences of not achieving these conditions, to be acceptable.

19.2.3.3.1.2 Likelihood of Successful ERVC

The UCSB study for AP600 evaluated two debris configurations or debris/vessel contact modes that were considered to bound the thermal loads from all other debris configurations that can reasonably be expected to occur in the time period between the initial relocation event and the

final steady state where essentially the entire core debris is contained in the lower head. One configuration was dominated by transient forced convection and jet impingement effects, and the other was dominated by natural convection in the final steady state. Analyses described in the UCSB report showed that vessel failure would not occur as a result of jet impingement. This was consistent with the staff's independent assessment of this threat. Thus, thermal loads to the vessel for the final steady state configuration were considered bounding and were analyzed in detail. Key aspects of the steady state configuration, termed the "Final Bounding State" or FIBS in the UCSB report, are: (1) fully-developed natural circulation of a homogeneous oxidic molten pool in the lower head of the RPV with an overlying metallic layer, (2) debris pool masses corresponding to relocation of essentially all of the core and most of the steel structures, (3) a depressurized RCS, and (4) heat transfer coefficients on the outside of the reactor vessel corresponding to a fully-flooded reactor cavity.

The technical treatment in the UCSB study for AP600 includes the following: (1) experimental data and correlations from tests conducted specifically to address ERVC for the AP600 design, including work carried out by UCSB to investigate boiling and critical heat flux in inverted, curved geometries (the ULPU experiments) and heat transfer from volumetrically heated pools and non-heated layers on top (the mini-ACOPO and MELAD experiments, respectively), (2) a detailed computer model to sample limited input parameters over specified uncertainty ranges, and to produce probability distributions of thermal loads and margins to departure from nucleate boiling at each angular position on the lower head, and (3) detailed structural evaluations that indicate that departure from nucleate boiling, i.e., heat flux in excess of critical heat flux (CHF), is a necessary and sufficient criterion for reactor vessel failure. The UCSB study concluded that thermally-induced failure of an AP600-like reactor vessel is "physically unreasonable" provided the RCS is depressurized and the vessel is submerged in water to a depth at least to the top of the debris pool. Additional conditions on the applicability of the UCSB conclusions are that the as-built reactor vessel thermal insulation system and RPV exterior coatings are in accordance with the system design and surface coatings evaluated in the prototypical testing carried out in the ULPU Configuration III tests, and that the insulation maintains its integrity under thermal-hydraulic loads associated with ERVC. RPV pressure loads associated with late reflood of the reactor vessel were not addressed as part of the UCSB analysis of ERVC.

The UCSB report was peer-reviewed by 17 internationally recognized experts in the fields of severe accidents, heat transfer, and structural mechanics. Numerous technical issues related to ERVC were identified and addressed as part of the peer review. The impact of these issues on the study conclusions was addressed as part of the peer review comment resolution process by performing sensitivity studies and additional evaluations to address the impact of these issues on the margins to failure. The results of the further assessments indicated that even when these issues are taken into consideration, the margins to failure are significant, and failure of the lower head is "physically unreasonable."

To assist in the NRC's evaluation of ERVC for AP600, parallel review efforts were undertaken by the NRC Office of Research (RES) and the Idaho National Engineering and Environmental Laboratory (INEEL). The review included: (1) an in-depth review of the UCSB study and the model used to assess ERVC effectiveness, (2) an in-depth review of the peer review comments and their resolution to identify areas where technical concerns were not addressed, and (3) independent analyses to investigate the impact of residual concerns and parameter uncertainties on the margins to failure and conclusions presented in the UCSB report. The latter activity included performing steady-state analyses of the thermal loads associated with

alternate debris bed configurations, including stratified intermediate states and inverted metallic and oxidic layers.

The review concluded that the UCSB study provides a comprehensive treatment of the concept of retaining the degraded core in-vessel through external cooling of the vessel wall, but identified the following as areas of concern:

- The potential to form a "stratified intermediate state" before final relocation of melt to the lower head. A stratified intermediate state, if formed, would result in a thinner metallic layer on top of the oxidic melt pool than the "final bounding state" evaluated in the UCSB study, and proportionally higher heat fluxes to the vessel wall.
- The potential for an inversion of the metallic and oxidic layers. An inversion of the layers, i.e., the metallic layer settling below the oxidic layer, would result in a different partitioning of the heat fluxes, and increased thermal loads on the bottom part of the vessel where heat removal capability (CHF) is at a minimum.
- The possibility of chemical interactions between the melt and the RPV wall. Such interactions could lead to thinning of the vessel wall and reduced margins to failure.

For the "final bounding state" configuration defined in the UCSB study, INEEL found that heat fluxes from the vessel remained below CHF even when peer reviewer concerns and additional parameter uncertainties were explicitly addressed in the integral solution. Reactor vessel integrity would therefore be expected to be maintained in the long term, provided the "final bounding state" can be achieved without prior vessel failure. However, INEEL also found that the "final bounding state" defined in the UCSB report does not necessarily bound all possible heat loads to the vessel. Steady-state calculations performed for several postulated alternate debris bed configurations indicate that heat fluxes can be higher than for the final bounding state and greater than CHF. Three configurations were: (1) a stratified intermediate state similar to the configuration analyzed in the UCSB study but with a thinner overlying metallic layer (Configuration A), (2) an intermediate state in which a limited amount of relocated metallic melt is trapped or sandwiched between two oxidic pools (Configuration B), and (3) a configuration in which a metallic/oxidic layer inversion occurs, resulting in a more dense heat generating metallic layer (consisting of uranium dissolved in zirconium) settling to the bottom of the vessel where CHF is at a minimum (Configuration C).

The staff concluded for AP600 that reactor vessel integrity is likely to be maintained if the requisite conditions for ERVC are met, but in view of the potential for certain hypothetical debris configurations to produce heat fluxes exceeding CHF, that RPV failure could not be ruled out for all possible core melt scenarios.

The applicability of these conclusions to AP1000 was assessed. The AP1000 decay heat level is higher than for AP600, and the RPV lower head dimensions are equivalent. Thus, the heat flux from the RPV would be greater, and the margins to RPV failure (with respect to CHF) potentially less for AP1000. To offset the potential reduction in the margin to CHF, Westinghouse has increased the CHF value by: (1) refining the RPV insulation system so as to streamline the flow between the RPV and the insulation, as discussed in Section 19.2.3.3.1.3, and (2) increasing the reactor cavity flood level associated with successful cavity flooding (as discussed in Section 19.2.3.3.1.1) to ensure that sufficient water/steam flows past the RPV are

achieved, consistent with the conditions simulated in ULPU Configuration IV and V testing. These changes have been shown to achieve up to a 30 percent increase in CHF based on the results of ULPU Configuration IV testing.

Westinghouse calculations provided in Chapter 39 of the PRA indicate that with the AP1000 insulation modifications (as represented in ULPU Configuration IV testing) and with the reactor cavity adequately flooded, significant margin to RPV failure remains for the AP1000. Westinghouse has indicated that test results from ULPU Configuration V (with proto-typical AP1000 insulation) show a further improvement in coolability performance relative to Configuration IV. Thus, the margins to RPV failure may be even greater in the as-built AP1000 design.

In support of the staff's review for AP1000, confirmatory analyses were performed by ERI using a mathematical model for lower head thermal behavior under severe accident conditions (ERI/NRC 03-202, April 2003). This model is based on a conceptual representation of a stratified molten pool consisting of a dense metallic bottom layer of Zr-U-SS, a middle ceramic layer of $\text{UO}_2\text{-ZrO}_2\text{-M}_x\text{O}_y$, and a top metallic layer of Fe-Zr. Input to the model is in the form of point estimate values and probability density functions. Output from the model is provided in terms of probability distributions for the heat flux on the exterior surface of the RPV at different locations on the lower head. The following two debris configurations were evaluated:

- Configuration I - a molten ceramic (oxide) pool with an overlying molten metallic layer
- Configuration II - a molten ceramic pool sandwiched between a bottom heavy metallic layer and an overlying metallic layer

These configurations are considered to be bounding in terms of their impact on the lower head integrity for AP1000. The first configuration is similar to Configuration A in the INEEL study for AP600. The second configuration is a combination of Configurations A and C in the INEEL study.

For Configuration I, one of the most important aspects is the potential for the formation of a top metallic layer thin enough to cause a significant focusing of heat on the RPV wall. For a low ceramic pool mass, the lower core support plate would not be submerged, and the amount of steel in the metallic layer would be limited, resulting in a thin metallic layer and increased heat fluxes to the RPV wall in the metallic layer region. For higher ceramic pool masses, the core support plate would be submerged, resulting in a thick metallic layer and reduced heat fluxes to the RPV wall. The quantities of core debris relocated into the lower plenum were treated in the model using a probability density function. Results for Configuration I show a zero probability of exceeding CHF within the molten oxide region. However, the probability of exceeding CHF is about 0.15 within the metallic layer region. This probability was found to vary from 0.04 to 0.3 in sensitivity analyses examining the impact of heat transfer correlations, material properties, and the mass of debris in the lower plenum.

For Configuration II, parametric calculations were performed using point estimate mean values of the masses from Configuration I. The mass fraction of uranium in the bottom layer was fixed at 0.4 and provides a bottom layer (Zr-U-SS) density greater than that of the oxide layer, consistent with this configuration. The results of these calculations indicate that the heat fluxes

from the vessel remain below CHF at all locations. Thus, the vessel would not be expected to fail if partitioning of the heavy metals from the ceramic pool were to occur.

Westinghouse does not consider a thin metallic layer in Configuration I to be applicable to the AP1000 because: (1) their analyses indicate that the lower plenum debris pool will contact the lower support plate and create a thick metal layer, and (2) in the transient stages before the debris contacts the lower support plate the debris will be either water cooled or quenched rather than a fully developed naturally circulating pool. For Configuration II, Westinghouse provided an analysis which produced results similar to the staff analysis, i.e., the heat fluxes from the vessel remain below CHF at all locations (response to RAI 720.48, Revision 1).

Since the review of the AP600 design, additional experiments relevant to in-vessel retention of molten core debris have been performed as part of programs sponsored by the Organization for Economic Cooperation and Development (OECD), in particular, the RASPLAV and MASCA programs. The RASPLAV project confirmed previous evaluations of the natural convection behavior of an oxidic corium pool that were based on simulant material. In addition, RASPLAV tests revealed that prototypic sub-oxidized corium which also contained some amount of carbon can stratify into a uranium-rich layer on the bottom and a zirconium-rich layer on the top. Other structural material in the reactor, such as boron, could also have the same influence on a sub-oxidized molten pool. The MASCA program (both small scale and confirmatory large scale) has largely confirmed the prediction that iron containing sub-oxidized corium can stratify (partition) into metallic and oxidic phases (D. A. Powers, "Chemical Phenomena and Fission Product Behavior During Core Debris/Concrete Interactions," Proceedings of CSNI Specialists' Meeting on Core Debris Concrete Interactions, published by Electric Power Research Institute, February 1987.) More importantly, the metallic phase may be denser than the oxidic phase and relocate to the lower part of the lower head.

Despite an increased understanding of core melt progression and lower head behavior since AP600, significant uncertainties remain. Uncertainties in the likelihood of forming various debris bed configurations are largely the result of the inherent limitations in the modeling of core melt progression/relocation and lower head debris bed behavior, and the difficulty in accurately simulating proto-typical reactor conditions in experiments. Additional experiments and detailed, transient modeling of lower head debris bed and molten pool behavior would be needed to determine and assess viable lower plenum debris configurations. The calculations would need to be dependent on realistic, validated models for debris quenching, debris bed reheating and remelting, and mixing and stratification of the newly formed molten pool. Such calculations are considered to be beyond current severe accident analysis capabilities, and results of any such calculations would be highly speculative and be subject to considerable uncertainties.

For purposes of design certification, the staff has accepted the Westinghouse characterization of ERVC in the AP1000 PRA on the basis of the margin to vessel failure for the "final bounding state" configuration defined in the UCSB study, in conjunction with results of probabilistic and deterministic analyses of the impact of vessel failure on containment integrity. The deterministic analyses for core concrete interactions and ex-vessel FCI, described in Sections 19.2.3.3.3 and 19.2.3.3.5.2 of this report, indicate that RPV failure and subsequent melt relocation is not expected to result in early containment failure. The probabilistic assessment discussed in Section 19.1.3.2.3 of this report illustrates that if credit for successful ERVC is reduced or eliminated, containment failure frequency would increase proportionally since all RPV breaches are assumed to lead to early containment failure in the baseline PRA.

Under the most limiting assumption of no credit for ERVC, the containment failure frequency would approach the core melt frequency given the pessimistic characterization of containment response to an RPV breach in the PRA. Even then, however, the containment failure frequency would remain below the general plant performance guideline of 1E-06/y for a large release of radioactive material (as proposed in the Safety Goal Policy Statement) because of the low estimated core damage frequency. The staff therefore concludes that the design of the AP1000 for ERVC is acceptable. The Westinghouse position that RPV failure is physically-unreasonable does not appear justified in light of the uncertainties in the late-phase melt progression and the melt configuration in the lower head. Nevertheless, this assumption is inconsequential from the overall risk perspective as discussed in Section 19.1.3.2.3, and is considered acceptable by the staff.

19.2.3.3.1.3 System Considerations

Reactor Cavity Flooding System

The reactor cavity flooding system is comprised of two 20.3-cm (8-in.) diameter lines drawing from the IRWST gravity injection line (which connects to the IRWST sump) and discharging into the recirculation sumps at Elevation-90' of containment. The water flows out of the recirculation sumps and eventually fills the floodable region of containment to the Elevation-107'. One motor-operated valve and one explosive valve is installed in each line. All valves are Class 1E and are powered by Class 1E dc power. The line sizing for the system is based on the design function of the lines which is to provide suction for the RNS pumps in the recirculation mode.

The containment recirculation squib valves and isolation MOVs, and the containment recirculation screens are included as risk significant SSCs within D-RAP. In-service inspection and testing programs provide surveillance and maintenance requirements on the related piping and valves. The operator action to flood the reactor cavity is specified in the first step of ERG AFR.C-1, which would be entered when core exit temperatures exceed 1200F. The core exit thermocouples are used to monitor the need for cavity flooding within the inadequate core cooling (ICC) portion of the EOPs, and are also Class 1E and powered by Class 1E dc power. The staff therefore concludes that treatment of the reactor cavity flooding system in the SSAR and ITAAC is acceptable.

Reactor Pressure Vessel Thermal Insulation System

In addition to RCS depressurization and reactor cavity flooding, several conditions must also be met in order to support ERVC, specifically: (1) the reactor vessel thermal insulation system is constructed in accordance with the final design description developed through ULPU Configuration V testing with proto-typical insulation, (2) the reactor vessel insulation system maintains its integrity under the hydrodynamic loads associated with ERVC, and is not subject to clogging of the coolant flow path by debris, and (3) RPV exterior coatings do not preclude the wetting phenomena identified as the cooling mechanism in the ULPU testing. Each of these areas is discussed below.

The RPV thermal insulation system is designed to limit thermal losses during normal operations, but also to provide an engineered pathway for supplying water cooling to the vessel and venting steam during severe accidents. The general features of the insulation system are described in SSAR Section 5.3.5, and Chapter 39 of the PRA. Water enters the insulation

system through water inlets located below the RPV lower head. From there, it flows upward and outward along the spherical lower head of the RPV where significant boiling and steam production occurs. The escaping liquid/steam mixture flows into the annular gap between the cylindrical portion of the RPV and the curved insulation panels to the top of the reactor vessel cylindrical section. It then passes through one of four steam flow paths/ducts, which are embedded in the concrete biological shield, into the vessel nozzle gallery at Elevation 98'. The coolant returns to the RCDT room via a grated opening between the vertical access tunnel and the RCDT room (approximately 100 ft² area), and enters the reactor cavity compartment through a passively-actuated damper installed in the doorway between the reactor cavity compartment and the RCDT room.

Key attributes of the reactor vessel insulation system include the following:

- the water inlets at the bottom of the insulation and the bouyant covers over the outlets of the 4 embedded water/steam flow paths in the shield wall, both of which change position during flood-up of the reactor cavity
- specific RPV/insulation clearances and water/steam flow areas on which experimental facility scaling for ULPU Configuration V was based
- insulation panel and support members designed to withstand the hydrostatic and hydrodynamic loads associated with ERVC

The water inlet at the bottom of the insulation is sized so that the pressure drop through the inlet is negligible during the circulation of water associated with the in-vessel retention phenomena, and would have a minimum total flow area of 6 ft². Each of the four steam ducts in the biological shield wall have a flow area of 3 ft² which would provide a flow area greater than or equal to the minimum flow area in the structures forming the circulation loop. On the basis of results from the ULPU Configuration V tests (with proto-typical insulation), Westinghouse estimates that the upper limit flow rate past the RPV would be approximately 57 kL/min (15,000 gpm). This information was provided informally, and will need to be documented as part of the Open Item regarding documentation of ULPU Configuration V testing discussed below. 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 floodup to permit water to flow from the RCDT room into the reactor cavity compartment. The damper opening has a minimum flow area of 0.74 m² (8 ft²), and is constructed of light-weight material to minimize the force necessary to open the door.

The AP1000 RPV insulation system is purchased equipment and not within the Westinghouse scope. The COL applicant will be responsible for completing the design of the reactor vessel insulation system. This will include the detailed design of the water inlets and outlets, RPV/insulation clearances and water/steam flow areas, and the structural analysis of the reactor vessel insulation panels and support members. General design requirements for the AP1000 insulation are provided in Section 39.10 of the PRA. Information needed to complete the final design, such as the hydrostatic and dynamic load information, will be obtained from the UPLU Configuration V test data as described below. For AP600, Westinghouse specified a set of functional requirements for the RPV insulation system on the basis of the ULPU Configuration III experiments, and performed a structural analysis that showed that the

insulation design was able to meet each of the functional requirements. Thus, a design that meets the functional requirements is feasible.

Tests performed in ULPU Configuration IV focused on improvements to coolability performance (CHF) that could be achieved by streamlining the flow path between the RPV and insulation, thereby enhancing convection. The tests evaluated CHF for a curved baffle located at various positions/spacings from the vessel, and showed that a significant enhancement in CHF is possible relative to the Configuration III experiments for AP600 (see Quantification of Limits to Coolability in ULPU-2000 Configuration IV, CRSS-02.05.3, May 2002). As such, these tests provide a basis for further optimizing the insulation design.

The AP1000 insulation design was refined based on insights from the Configuration IV tests, and a proto-typical insulation design for AP1000 was evaluated as part of the ULPU Configuration V test program. Westinghouse has indicated that the Configuration V test results show a further improvement in coolability performance relative to Configuration IV, and also include information on transient pressure loads needed by the COL-applicant to establish the pressure loads for the structural analysis of the final insulation design. Westinghouse has not provided documentation of: the RPV insulation design evaluated in Configuration V, the results of the Configuration V testing, or the functional requirements for the AP1000 RPV insulation system. Such information is needed in order for the staff to conclude on the margins to lower head failure for AP1000, and the viability of Westinghouse's proposal that the COL-applicant complete the RPV insulation design. This is a DSER Open Item.

The RCS blowdown during a LOCA may tend to carry debris created by the accident toward the reactor cavity. In response to a staff request, Westinghouse performed an evaluation of the potential for such debris to block the ERVC flow path. On the basis of the estimate of 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 1 ft/s. Such an approach velocity would prevent significant transport of large debris. The opening between the vertical access tunnel and the RCDT room is covered by a metal grating that will prevent any large pieces of debris from entering the RCDT room. In addition, the damper between the RCDT room and the reactor cavity compartment, as well as the entrance into the RPV insulation is elevated. Because the water level at the time of debris relocation is several meters above the bottom of the insulation, floating or submerged debris cannot be ingested into the insulation flowpath. Finally, a functional requirement will be included in the RPV insulation design to assure that the minimum flow area through each water inlet, as well as around the recirculating flow loop is met. The staff considers the potential for debris blockage of the ERVC flow path to be adequately addressed by the functional requirements of the insulation design and the related system ITAAC, and therefore the resolution of debris blockage is acceptable.

The ULPU testing included tests using prototypical RPV steel with paint applied according to Westinghouse paint application specifications. This paint is intended to protect the vessel carbon steel surface during shipment and storage, and is not expected to be removed. In the ULPU tests, the paint surface was judged to actually increase the wettability of the vessel external surface and increase the critical heat flux. Therefore it is important that Westinghouse paint application specifications for the RPV exterior be met.

Contingent upon resolution of the Open Item regarding documentation of ULPU Configuration V testing, the COL applicant will be responsible for completing the design of the reactor vessel

insulation system. This is COL Action Item 19.2.3-1. The RPV insulation system and the damper between the reactor cavity and the RCDT room are included as risk-significant SSCs in the reliability assurance program, and important criteria associated with the design are incorporated into the ITAAC.

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

These positions are codified in 10 CFR 50.34(f)(2)(ix). In its SRM, dated July 21, 1993, the Commission approved the staff's position. The staff's evaluation of the Hydrogen Igniter Subsystem to meet the requirements of 10 CFR 50.34(f)(2)(ix) and the criteria in SECY-93-087 is contained in Section 6.2.5 of this report.

9.2.3.3.3 Core Debris Coolability

Core concrete interactions (CCI) is a severe accident phenomenon that involves the melting and decomposition of concrete in contact with core debris. This phenomenon would occur following reactor vessel breach, if the molten core debris discharged from the RPV is not quenched and cooled. CCI can challenge the containment by various mechanisms including: (1) pressurization from non-condensable gas and steam production, (2) destruction of structural support members, and (3) melt-through of the containment liner and basemat.

In SECY-93-087, the staff recommended that the Commission approve the position that both the evolutionary and passive LWR designs meet the following criteria:

- provide reactor cavity floor space to enhance debris spreading
- provide a means to flood the reactor cavity to assist in the cooling process
- protect the containment liner and other structural members with concrete, if necessary
- ensure that the best-estimate environmental conditions (pressure and temperature) resulting from CCI do not exceed ASME Code Service Level C limits for steel containments, or factored load category for concrete containments, for approximately 24 hours

In addition, the designs should ensure that the containment capability has margin to accommodate uncertainties in the environmental conditions from CCI. In its July 21, 1993, SRM, the Commission approved the staff's position.

The AP1000 design relies primarily on safety grade RCS depressurization and reactor cavity flooding capabilities to prevent RPV breach and CCI, but also incorporates plant features consistent with the criteria in SECY-93-087 and the EPRI URD criterion regarding debris coolability. In the unlikely event of RPV failure, these features would reduce the potential for containment failure from CCI. The AP1000 design features include the following items:

- a cavity floor area and sump curb that provides for debris spreading without debris ingress 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 cavity flooding system is discussed in Section 19.2.3.3.1 of this report. The reactor cavity floor area and response of the concrete basemat is discussed below.

The reactor cavity is comprised of two interconnected compartments – an octagonal shaped room below the RPV, and an adjacent room containing the normal containment sump and the RCDT. The total floor area is 48 m² (517 ft²), divided approximately equally between the two compartments. A 5 foot wide tunnel, and a 3 foot wide ventilation duct connects the two volumes. The tunnel connecting the two regions of the cavity is protected by a door that serves as an HVAC barrier during normal operation. The door and ventilation ductwork are expected to be displaced by the pressurization associated with RPV breach before the arrival of core debris, thereby permitting core debris to spread within the two compartments.

The reactor cavity sump is located along the back side of the wall dividing the two compartments, and is surrounded by an 61-cm (24-in.) high, 30.5-cm (12-in.) thick concrete curb. The location of the sump (out of the line-of-sight of the RPV) and the concrete curb provide protection against entry of core debris into the sump, as discussed later. The sump is covered with a stainless steel plate that supports the reactor cavity drain pumps. A number of sleeved ½-inch drain holes pass through the curbing at floor level to permit water to drain into the sump, but these passages are sufficiently small that molten core material would quench and solidify in the passages before entering the sump.

The embedded steel containment liner beneath the reactor cavity region is ellipsoidal in shape. The minimum distance from the reactor cavity floor to the embedded steel liner (0.85 m (2.8 ft)) occurs at the end of the RCDT room furthest from the reactor vessel. The distance from the floor of the cavity sump to the steel liner is only slightly less (0.52 m (2.7 ft)) because of the ellipsoidal shape of the liner and the more central location of the sump. In the calculations discussed below, the thickness of concrete above the liner is taken to be the minimum distance of 0.85 m (2.8 ft).

The ratio of reactor cavity floor area to rated thermal power for the AP1000 design is 0.014 m²/MW_{th}. This is less than the EPRI URD design criterion of 0.02 m²/MW_{th} for debris coolability, which represents the EPRI estimate of what is required to adequately cool core debris. (The EPRI criterion corresponds to a debris depth of about 10-inches, which is less than the debris depth in AP1000.) The staff notes that the floor area provided in the AP1000

design, in conjunction with the reactor cavity flooding system, will promote debris coolability (via debris spreading, quenching by pre-existing water in then cavity, and long-term heat removal by the overlying water pool) but will not necessarily ensure it. Accordingly, the staff has relied on deterministic calculations described below, rather than the EPRI criterion, in judging the adequacy of the reactor cavity design for CCI.

As described in Section 19.2.3.3.1 of this report, external reactor vessel cooling (ERVC) features reduce the frequency of RPV breach in the baseline PRA to less than $1E-08/y$. The staff considers reliance on the ERVC strategy consistent with Commission guidance in the SRM pertaining to SECY-93-087. In particular, under the topic of core debris coolability, the Commission stated that the staff should not limit vendors to only one method for addressing containment responses to severe accident events, but permit other technically justified means for demonstrating adequate containment response. However, in view of the complexity of the technical issues impacting the reliability of the ERVC strategy, the staff, in SECY-96-128, recommended that the Commission approve the position that Westinghouse use a balanced approach, involving reliance on in-vessel retention of the core complemented with limited analytical evaluation of ex-vessel phenomena, to address the adequacy of the AP600 design for ex-vessel events. In its January 15, 1997, SRM, the Commission approved the staff's position. The deterministic calculations for CCI are of particular significance for AP1000 since, compared to other ALWRs, the AP1000 ex-vessel debris bed is deeper and the concrete basemat is thinner. In addition, the AP1000 design does not impose any restrictions on the type of concrete that can be used for the containment basemat and the reactor cavity walls.

Westinghouse performed deterministic calculations of CCI for a postulated vessel breach event. A MAAP4 analysis of CCI assuming a uniform debris bed within the AP1000 reactor cavity is provided in Appendix D of the PRA as part of the equipment survivability analysis. These calculations were performed for two different reactor cavity/basemat concrete compositions, i.e., limestone/common sand and basaltic concrete. For a basemat composed of limestone concrete (which maximizes non-condensable gas generation and minimizes concrete ablation) basemat penetration would occur after about 4 days following the onset of core damage. Containment pressure is not predicted to reach Westinghouse's Service Level C estimate (91 psig) until even later. For a basemat composed of basaltic concrete (which maximizes concrete ablation and minimizes non-condensable gas generation) the predicted time of basemat melt-through is reduced to about 2 days, with containment over-pressure failure expected some time later.

Westinghouse performed additional, detailed calculations in which the metallic and oxidic components of the in-vessel core debris were tracked separately during the release, spreading, and CCI phases, thereby allowing evaluation of concrete ablation in different regions of the reactor cavity. These calculations are documented in Appendix B to the PRA. Westinghouse assumed an initial in-vessel core debris pool configuration consistent with the "Final Bounding State" in the DOE assessment of external reactor vessel cooling (DOE/ID-10460), i.e., essentially the entire inventory of core materials and steel structures, with the metal layer overlying the oxide pool. Westinghouse assumed the release of the entire mass of core debris in a molten state. This represents a conservative upper limit in terms of the mass of debris that could participate in CCI.

The following two vessel failure scenarios were evaluated: (1) a "hinged failure" in which a localized opening occurs near the vessel beltline immediately followed by the vessel tearing

around nearly all its circumference, and the lower head hinging/swinging downward and coming to rest on the cavity floor, and (2) a "localized failure" in which a localized opening occurs near the vessel beltline (releasing molten core debris above the breach), and over time, moves downward releasing additional debris. For the localized failure mode, which involves a slow release and greater water depth than the hinged failure mode, Westinghouse used the THIRMAL code to assess the break-up and freezing of the melt as it falls through the water pool; these metal-water interactions were not considered for the hinged failure mode.

The MELTSPREAD code was used to analyze the spreading of the core debris over the various regions of the cavity floor for AP600. This permitted the metallic and oxidic components of the in-vessel core debris to be tracked separately during the release, spreading, and CCI phases. For both RPV failure modes, the analyses show a non-uniform distribution of the melt constituents, with the debris consisting primarily of oxides (and most of the decay heat) in the region directly under the reactor, and primarily of metals at the opposite end of the reactor cavity. The equilibrium depth of the debris in the two regions of the cavity is approximately equal in the "hinged failure" case since the debris remains molten during the spreading. However, the equilibrium debris depth in the "localized failure" case is greater under the reactor than in the RCDT room because of an accumulation of solidified debris below the reactor in this scenario.

The results of the MELTSPREAD analyses for AP600, in terms of the characterization of debris composition in the two regions of the cavity, were considered applicable to AP1000 (based on the similarities in the postulated in-vessel molten pool and RPV lower head failure scenarios), and were used as input to the MAAP4 code for analysis of CCI for AP1000. Two separate MAAP analyses were performed for each RPV failure mode – the first analysis to treat the debris under the reactor vessel, and the second to treat the core debris at the opposite end of the cavity, where the sump and RCDT is located. The MELTSPREAD results were also used to assess the likelihood and impact of debris entering the reactor cavity sump in the two vessel failure scenarios considered.

Westinghouse evaluated the effects of CCI assuming two different reactor cavity/basemat concrete compositions, i.e., limestone/common sand and basaltic concrete. For a basemat composed of limestone concrete (which maximizes non-condensable gas generation and minimizes concrete ablation) basemat penetration would occur at about 4 days following the onset of core damage. Containment pressure is not predicted to reach Westinghouse's Service Level C estimate (91 psig) until even later. For a basemat composed of basaltic concrete (which maximizes concrete ablation and minimizes non-condensable gas generation) the predicted time of basemat melt-through is reduced to about 3 days, with containment over-pressure failure expected some time later. For both RPV failure scenarios and both concrete types, the concrete basemat in the region under the reactor vessel is eroded more rapidly than the region of the RCDT, and is the limiting location for basemat failure.

Although basemat penetration is unlikely, the Westinghouse assessment indicates that the molten core debris will reach the embedded liner (i.e., ablate through 0.85 m (2.8 ft) of concrete) within 9 to 11 hours of RPV breach with basaltic concrete, and within 11 to 13 hours of RPV breach with limestone concrete. However, in all cases, the top of the molten core debris pool is well above the embedded liner when melt-through first occurs, thereby preventing an airborne release of fission products. The staff does not consider the interface between the concrete basemat and embedded containment liner to be a viable pathway for significant

airborne release of fission products to the environment in AP1000 in view of the minimal gaps, if any, between the concrete and the liner, and the considerable distance that fission products would need to travel along this pathway to reach the environment (a distance approximately equal to the radius of the containment). Accordingly, the staff's focus in assessing the capability of the AP1000 to cope with CCI is on the time of basemat penetration rather than the time of melt-through of the embedded liner.

The MELTSPREAD calculations for the "localized failure" case indicate a maximum core debris depth of 25 cm (10 in.) in the region of the sump at any time in the transient for AP600. The core debris mass and height is greater for AP1000 but the maximum debris height will remain below the AP1000 curb height of 24 inches. Thus, the reactor curb will prevent the entry of core debris into the sump for this scenario. Calculations for the "hinged failure" mode predict that a wave of molten core debris would be reflected off the back wall of the RCDT room and achieve a maximum height of about 63 cm (25 in) in the vicinity of the sump curb during passage of the wave for AP600. The maximum height will be greater for AP1000 and will exceed the 24 inch curb height temporarily, The equilibrium height of debris is about 18 inches 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. Westinghouse does not consider this situation to pose a threat to containment because the core debris entering the sump would consist primarily of the metallic component of the melt, similar to the rest of the RCDT compartment. MAAP calculations for AP1000 show that the concrete penetration on the RCDT side of the cavity (by debris composed primarily of metals) is minimal compared to the penetration on the reactor side of the cavity (by debris composed primarily of oxides). Since the distance to the liner in the sump (0.82 m (2.7 ft)) is not significantly different than the distance assumed in the CCI calculations (0.85 m (2.8 ft)), the concrete penetration on the reactor side of the cavity is still expected to be limiting.

The staff considers Westinghouse's rationale regarding the significance of CCI in the cavity sump to be consistent with our expectations for the postulated failure scenarios, and reasonable. In judging the adequacy of the sump protection, the staff has also considered the following:

- the low probability of reactor vessel breach in the AP1000 design, given that the requisite conditions for in-vessel retention (RCS depressurization and reactor cavity flooding) would be achieved in over 90 percent of core damage events, and the high confidence that vessel integrity would be maintained when these conditions are achieved
- the likelihood that considerably less core debris would be released than assumed by Westinghouse, particularly in events with earlier times to reactor vessel breach, such as the alternate debris bed configurations postulated in Section 19.2.3.3.1 of this report
- the AP1000 will have no piping embedded in the concrete floor that could represent a potential path out of containment

On these bases, the staff considers the sump protection in the AP1000 design to be acceptable.

The staff performed calculations using the MELCOR code to confirm the degree of basemat ablation for AP1000 (ERI/NRC 03-201). The calculations indicate a maximum ablation depth of about 1.3 m (4.3 ft) for both limestone and basaltic concrete 2.5 days after accident initiation, assuming a dry reactor cavity and uniform distribution of debris within the reactor cavity. The calculations were terminated at this time. The ablation rates predicted by MELCOR are considerably lower than predicted by MAAP, partially as a result of a later time of RPV failure in the MELCOR calculation (8 hours in MELCOR versus 2 hours in MAAP). While not directly comparable to the Westinghouse calculations, the MELCOR calculations support the Westinghouse finding that basemat penetration would not occur for several days.

The staff concludes that in the event that core debris is not retained in vessel, the AP1000 design provides adequate protection against early containment failure and large releases resulting from CCI. Specifically, the AP1000 incorporates features that adequately address all criteria called out in SECY-93-087 related to core debris coolability. Although several factors in the AP1000 design mentioned earlier could tend to increase the severity of basemat melt-through, best-estimate calculations performed by Westinghouse and confirmed by NRC-sponsored calculations indicate that in the event of unabated CCI, containment basemat penetration or containment pressurization above ASME Code Service Level C limits will not occur until well after 24 hours, regardless of concrete composition. On this basis, the staff finds the AP1000 design acceptable in terms of its protection against CCI.

19.2.3.3.4 High-Pressure Core Melt Ejection

High pressure core melt ejection (HPME) and subsequent direct containment heating (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.

Westinghouse has incorporated several features in the AP1000 design to prevent and mitigate the effects of DCH, specifically, the automatic depressurization system and reactor cavity design features.

In SECY-93-087, the staff recommended that the Commission approve the general criteria that the evolutionary and passive LWR designs provide a reliable depressurization system and cavity design features to decrease the amount of ejected core debris that reaches the upper containment. Examples of cavity design features that will decrease the amount of ejected core debris reaching the upper containment include ledges or walls that would deflect core debris and an indirect path from the reactor cavity to the upper containment. In its July 21, 1993, SRM, the Commission approved the staff's position.

One of the major features of the AP1000 design is the automatic depressurization system (ADS). The ADS is an automatically-actuated, safety-grade system consisting of 4 different valve stages that open sequentially to reduce RCS pressure sufficiently so that long-term cooling can be provided from the passive core cooling system. In the event that automatic actuation fails, the ADS is initiated by operator action from the main control room using the diverse actuation system. The ADS valves are designed to remain open for the duration of any ADS event, thereby preventing repressurization of the RCS. The performance of the ADS for

design-basis accident is discussed in SSAR Section 6.3 and Sections 5.1.3.7 and 6.3 of this report. The modeling of ADS in the PRA is described in Chapters 11 and 36 of the PRA.

The Level 1 PRA includes consideration of RCS depressurization (by automatic and manual actuation of ADS) early in an event to prevent core damage. For those sequences that proceed to core uncover at high RCS pressure, the potential to manually depressurize the RCS before the occurrence of thermally-induced SGTR or HPME is further evaluated in the Level 2 PRA. The survivability of the ADS valves and related instrumentation within the early phase of a severe accident during which late depressurization is viable is addressed in Appendix D of the PRA and Section 19.2.3.3.7 of this report. This assessment indicates that the design basis temperature will only be exceeded for a short time preceding late actuation of the valves. Because the ADS valves will be actuated before the time of rapid cladding oxidation and high RCS blowdown temperatures, the staff concludes that the ADS valves will be available to depressurize the RCS.

As discussed in Section 19.1.3.2.1 of this report, the majority of Level 1 sequences in the baseline PRA (about 90 percent) involve events with at least partially successful RCS depressurization, and relatively low RCS pressure (<150 psig) at the time of core uncover. With credit for late RCS depressurization, an even larger fraction of the core melt sequences (about 95 percent) are estimated to involve a depressurized RCS at the time of RCS pressure boundary challenge. Thus, only about 5 percent of the core damage events would potentially result in DCH. In the PRA, high pressure core melt sequences (with unsuccessful late depressurization) are assumed to result in failure of the SG tubes before reactor vessel failure. This obviates the need for additional thermal-hydraulic and probabilistic analyses of the following:

- the likelihood of RCS piping versus steam generator tube over-pressure failures in ATWS events
- the likelihood of containment failure from DCH pressure loads in high pressure core melt accidents
- the relative challenge and timing of creep-rupture failures in RCS piping, hot leg nozzles, pressurizer surge line, and steam generator tubes in high pressure core melt accidents

However, if such a failure does not occur and all high pressure core melt accidents result in RPV failure, the resulting frequency of HPME events would remain very small (about 1E-08/y).

The design of the reactor cavity is expected to decrease the amount of ejected core debris that reaches the upper containment. The pathways for debris transport from the AP1000 reactor cavity include the following:

- the annular openings between the coolant loops and the biological shield wall, that lead to the steam generator 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 steam generator compartments

Debris particles traveling along the first two paths would pass between the RPV and the cavity walls, around the boro-silicone neutron shield blocks, through the HVAC air flow slots in the RPV vessel supports, and into the nozzle gallery surrounding the upper portion of the vessel, before passing through either the annular openings between the coolant loops and the biological shield or the gap around the permanent cavity seal ring. Particles traveling along the third path would pass into the RCDT side of the reactor cavity, up into a ventilation shaft in the ceiling of the RCDT room, into a common tunnel between the two steam generator compartments, and into the steam generator compartments. In all cases, the particles would change direction and encounter obstacles before reaching the upper containment.

Westinghouse evaluated the containment pressure loads for a postulated RPV breach event in the AP600 design using the 2-cell equilibrium model developed by Pilch, et. al., under NRC-sponsorship for resolution of the DCH issue. The peak containment pressure for a postulated DCH event was estimated to be about 81 psig, which is below Westinghouse's estimated value for Service Level C for AP600 and is sufficiently small that the corresponding probability of containment failure is negligible (less than 0.1 percent). Although a similar calculation was not performed for AP1000, the probability of containment failure in AP600 is judged by the staff to be applicable to AP1000 based on similar reactor cavity designs in AP600 and AP1000, similar ratios of containment volume to core debris mass (0.61 m³/kg for AP1000 versus 0.66 m³/kg for AP600), and higher ultimate pressure capacity for AP1000 (e.g., the containment pressure corresponding to a 10⁻³ probability of failure is approximately 95 psig in AP1000 versus 80 psig in AP600.) The latter two factors would offset the effect of a higher core mass in AP1000.

The staff concludes that the AP1000 design provides adequate protection against early containment failure and large releases due to DCH. Specifically, the AP1000 incorporates a safety-grade depressurization system, and reactor cavity design features that are expected to decrease the amount of ejected core debris that leaves the reactor cavity in the event of a high pressure melt ejection event. These features adequately address all criteria called out in SECY-97-187 related to high pressure melt ejection. In the event of an RPV breach at high pressure, calculations performed by Westinghouse for AP600 and applicable to AP1000 indicate that the peak containment pressure will remain sufficiently small, and that the corresponding probability of containment failure is negligible. On these bases, the staff finds the AP1000 design acceptable in terms of its protection against DCH.

19.2.3.3.5 Fuel-Coolant Interactions

The containment function can be challenged by energetic fuel-coolant interactions (FCI), also known as "steam explosions." The term steam explosion refers to a phenomenon in which molten fuel rapidly fragments and transfers its energy to the coolant, resulting in rapid steam generation, high local pressures, and the propagation of the pressure wave in the water. Section J, "Containment Performance," of SECY-93-087 indicates that the staff will evaluate the impact of FCI on containment integrity by using the containment performance goal. The purpose of this section is to perform such an evaluation for steam explosions that may occur either inside (in-vessel) or outside (ex-vessel) the AP1000 reactor vessel.

19.2.3.3.5.1 In-Vessel Steam Explosions

In-vessel steam explosion is addressed in section 19.34.2.2.1 of the AP1000 DCD Tier 2, and in section 34.2.2.1 of the AP1000 PRA supporting document. Westinghouse claims that based on the in-vessel core relocation scenario for the AP1000, the conclusions from the in-vessel steam explosion analysis performed for the AP600 can be extended to the AP1000. The claim is based on the facts that the geometry of the AP1000 lower head is the same as AP600, and expected molten core mass flow rate, its superheat and composition to be “essentially the same” as AP600.

The AP600 in-vessel steam explosion analysis was performed using Risk Oriented Accident Analysis Methodology (ROAAM) in the report “In-vessel Coolability and Retention of a Core Melt,” DOE/ID-10460 (Reference 19.34-2 in AP1000 DCD Tier 2, and Reference 34-3 in AP1000 PRA.) The ROAAM analysis concludes that the lower head vessel failure from in-vessel steam explosion is “physically unreasonable with very large margin to failure.”

Because of its applicability, the following is a summary of staff’s evaluation and conclusions presented in Section 19.2.3.3.5.1 of AP600 Final Safety Evaluation Report, NUREG 1512.

The report “In-vessel Coolability and Retention of a Core Melt,” DOE/ID-10460 is henceforth denoted as IVR report. Other reports used in the AP600 analysis are “Lower Head Integrity Under In-Vessel Steam Explosion Loads,” DOE/ID-10541, henceforth denoted as the IVSE report, and its companion reports: “Propagation of Steam Explosions: ESPROSE.m Verification Studies,” DOE/ID-10503, and “Pre-mixing of Steam Explosions: PM-ALPHA Verification Studies,” DOE/ID-10504.

Briefly, the ROAAM approach involves decomposing the in-vessel steam explosion issue into a set of contributing physical processes, quantifying these processes through a combination of “causal relations” representing best estimate physics and probability distributions representing “intangible parameters” and finally, combining the quantification of individual processes into an integral assessment of the overall issue. The physical processes are as follows:

- melt relocation into the lower plenum
- initial melt-water interactions leading to coarse breakup of melt and forming a premixture
- triggering of premixture and energetic melt-water interactions
- consequent loading of the lower head and its response

The causal relations describing these physical processes, in their respective order, are:

- melt progression (analytical treatment founded on physics)
- premixing (PM-ALPHA code and associated models)
- explosion propagation (ESPROSE.m code and associated models)
- structural loads and response (ABAQUS code)

The intangible parameters, identified in the IVSE report, are as follows:

- the location and size of the failure
- melt characteristic length scale (initial size of melt particles)
- evolution of melt length scale (breakup rate)
- trigger strength and timing

Of these intangible parameters, some were treated in a deterministic manner (e.g., failure location, trigger strength), whereas probability distributions were assigned to others (i.e., failure size, initial melt particle size, melt breakup rate, and trigger timing).

The staff noted that the usual ROAM approach, i.e., consideration of splinter scenarios, assignment of probability distributions to intangibles, and convolution of causal relations with the probability distribution (illustrated in Figure 2.3 of the IVSE report) was not rigorously followed in this case. Three reasons were cited: (1) a unique melt relocation scenario, (2) bounding approach taken with regard to premixing and explosion calculations, and (3) non-intersecting load and fragility curves. Moreover, the IVSE report argued that the bounding approach obviated any parametric and sensitivity calculations.

Regarding melt relocation, the staff accepted Westinghouse conclusion that, given AP600 geometry (i.e. relatively flat radial power profile, high aspect ratio and relatively thick core plate), the melt release would occur following a sideways growth of the crust surrounding the melt pool, breach of the reflector and the core barrel, and melt flow out of the pool into the lower plenum water. As a consequence, the staff found the calculated hole in the baffle plate and the rates of molten core relocation to be acceptable. However, the staff also acknowledged that although the downward melt relocation is less likely (because of the potential for the coolability of the blockage in the lower core region), the high level of uncertainty associated with crust failure and the limited qualitative arguments provided by Westinghouse made the staff unable to completely eliminate the downward scenario from further consideration.

Regarding quantification of premixtures (i.e. initial condition for an energetic FCI), the staff found the Westinghouse method (i.e. PM-ALPHA code) to quantify pre-mixtures as applied to the AP600 acceptable. The staff had not conducted an independent verification of the PM-ALPHA code. However, the staff reviewed the submitted information and concluded that a reasonably large assessment data base supported Westinghouse's use of the PM-ALPHA code for this assessment. In particular, the staff agreed that Westinghouse sufficiently demonstrated that larger melt length scales would actually produce mixtures that were much more difficult to explode and, therefore, the choice of mixing length scale was conservative.

Regarding quantification of explosion loads, the staff found that the Westinghouse approach to triggering, both timing and location, to be conservative. The staff noted that the influence of trigger location to energetics, if discernible, is likely to be bounded by sensitivity analysis involving trigger timing. On the basis of the review of the information submitted by Westinghouse, the staff found the used methodology, as applied to AP600 and documented in DOE/ID-10503 report, and the analytical results to be acceptable.

Regarding structural failure criteria, the staff concluded that IVSE report, along with its companion reports, DOE/ID-10543 and DOE/ID-10504, are acceptable for addressing the in-vessel steam explosions, and for determining the magnitude of in-vessel steam explosions

for the sideways melt release scenario for the AP600. The staff noted that this conclusion cannot be extended to downward relocation scenario, which the staff considered to be less likely to occur. In addition, although the staff did not review and approve Westinghouse's structural analyses, the staff believes there is an adequate safety margin to support the conclusion that (for the sideways melt release scenario) in-vessel steam explosions of sufficient magnitude to challenge the structural integrity of the AP600 lower head are of sufficiently low probability to be discounted from further consideration.

Westinghouse did not submit AP1000-specific in-vessel steam explosion analysis, but provided arguments in support of the assertion that AP600 analyses are extendable to AP1000. The staff did not perform an independent analysis of in-vessel steam explosions for AP1000, nor did it perform one for AP600. For AP600, the staff reviewed extensive documentation of the in-vessel steam explosion analysis provided by Westinghouse which supporting the argument that the lower head failure from in-vessel steam explosions was of sufficiently low probability. The staff concluded that for the range of uncertainties associated with the late phase core melt progression considered in the analysis, the argument was acceptable. For AP1000, the staff performed a review of Westinghouse's approach to analysis of AP1000 in-vessel steam explosions which is based entirely on the similarity argument between AP1000 and AP600. Because of a high degree of similarity between AP600 and AP1000 geometries, the staff believes the range of uncertainties associated with the physical processes involved in the in-vessel steam explosions is same, or very similar for both configurations. Moreover, the staff recognizes the prevailing experts' opinion that the alpha-mode failure is not risk-significant (NUREG-1524), i.e., estimated probability of such a failure is below an accepted level of credibility.

Based on the above, the staff accepts the Westinghouse position that the conclusions from the AP600 in-vessel steam explosion analysis can be extended to AP1000. The staff, however, notes that an extension of the similarity argument to in-vessel retention may not be clearly evident. As such, the likelihood of lower head failure due to high heat fluxes resulting, for example, from the focusing effect is non-negligible (see Section 19.2.3.3.1 of this report.)

19.2.3.3.5.2 Ex-Vessel Steam Explosion

Ex-vessel steam explosion is addressed in section 19.34.2.2.2 of the AP1000 DCD Tier 2, and in section 34.2.2.2 of the AP1000 PRA supporting document. As stated, the first level of defense for ex-vessel explosions is the in-vessel retention of the molten core debris. However, in the event of the lower head failure and a dry reactor cavity (i.e. cavity not flooded) the PRA analysis assumes early containment failure. The issue of ex-vessel steam explosions appears only when the vessel fails with a flooded cavity. For this case Westinghouse claims that the conclusions from the ex-vessel steam explosion analysis performed for the AP600 can be extended to the AP1000. The claim is based on the following reasons: (i) the vessel failure modes are the same for both designs, (ii) the initial debris mass, superheat and composition are expected to be the same, and (iii) since AP1000 vessel lower head is closer to the cavity resulting in less debris mass participating in the interaction with water, it is conservative to use the AP600 analysis.

A structural response analysis of the reactor cavity during postulated AP600 ex-vessel steam explosions was performed in the Reference 19.34-5, Appendix B to DCD Tier 2. The following

is a summary of staff's evaluation and conclusions presented in Section 19.2.3.3.5.2 of AP600 Final Safety Evaluation Report, NUREG 1512.

The review was performed following the guidance given in Section J, "Containment Performance," of SECY-93-087. Therefore, within the context of containment performance goal, the staff evaluated the impact of steam explosions on the integrity of the containment. The staff found Westinghouse's treatment of ex-vessel steam explosions in the PRA to be conservative.

Following the guidance given in the SECY 93-087, Westinghouse evaluated the ex-vessel steam explosion loadings on the reactor cavity, reactor pressure vessel, and the containment liner using the TEXAS code. Two reactor vessel failure modes were considered: (1) localized creep rupture of the vessel leading to a small localized opening, and (2) global creep rupture leading to "unzipping" of the lower head (denoted as the "hinged" failure mode) at or near the transition between the hemispherical lower head and cylindrical vessel structure. The first of these modes produces a small (~3.8 kg/s), localized flow of melt out of the vessel sidewall into the cavity water pool through an equivalent 6.0 cm diameter opening, while the second produces a massive flow (15,100 kg/s) through a much larger opening (~100 cm diameter) caused by global creep rupture failure at the belt line (transition between the hemispherical and the cylindrical parts). The details of each of the assumed reactor vessel failure modes are provided in Reference B-6, DOE/ID-10523, "Analysis of Melt Spreading in an AP600-Like Cavity," of Appendix B to the AP1000 PRA. Both failures are considered at a fully depressurized RPV condition and, as such, the conclusions are valid only for that condition.

Westinghouse performed two baseline calculations – one each for the localized and hinged failure modes – and four sensitivity calculations for the localized failure mode only. Westinghouse also assessed the vertical uplift of the reactor pressure vessel resulting from the impulse loads calculated for the hinged failure mode. The conclusion was that in every case the structural integrity of the steel containment vessel would be maintained, even though in the case of hinged failure the structural integrity of the concrete cavity floor and wall would not be retained.

The staff reviewed the assumptions used in the AP600 analysis as well as the results. The staff found the selected hole sizes for both the localized failure and the hinged failure cases to be acceptable. Moreover, for the localized failure case, a reasonable variation in hole sizes is not expected to change the overall conclusion (as may be evident from the sensitivity analysis) that the containment integrity would not be challenged. The staff also verified Westinghouse's assumptions of melt temperature and superheat for the hinged failure case through an independent study, "Potential for AP600 In-Vessel Retention Through Ex-Vessel Flooding," (INEEL/EXT-97-00779).

In assessing the structural integrity of the containment due to ex-vessel steam explosions, Westinghouse used the loading associated with the hinged failure mode and found the containment capacity to have 20 percent margin. The staff performed an independent evaluation and found the Westinghouse analysis acceptable. The staff also performed an evaluation of the reactor vessel uplift due to explosion loading and found the uplift did not lead to containment failure.

The staff's acceptance of Westinghouse containment integrity analysis, performed for AP600, during postulated ex-vessel steam explosions were based on calculations performed by Energy Research, Incorporated (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 acceptable, relative to the containment performance goal.

The staff, through its contractor, ERI, performed an independent evaluation of the AP1000 ex-vessel steam explosions. The results are reported in "Analysis of in-vessel retention and ex-vessel fuel coolant interaction for AP1000", ERI/NRC 03-202. The approach used in this study consists of the specification of initial and boundary conditions; determination of the mode, the size and the location of lower head failure using detailed analyses; computer simulation of the FCI processes; and finally, an examination of the impact of the uncertainties in the initial and boundary conditions as well as the FCI model parameters on the fuel coolant interaction energetics through a series of sensitivity calculations.

The cavity design in AP600 and AP1000 are similar, but the AP1000 reactor vessel lower head is closer to the cavity floor. Based on the in-vessel retention analysis, discussed in Section 19.2.3.3.1 of this report, the base case for the ex-vessel steam explosion is assumed to involve a side failure of the vessel involving a metallic pour into the cavity water. For the AP1000 analysis, the entire reactor vessel lower head is modeled based on the insights from the AP600 study by ERI. The impulse loads on the reactor vessel are found to be similar to those on the cavity wall due to the proximity of the explosion zone to both the reactor vessel and the cavity wall. A number of sensitivity studies were also performed for AP1000. The results of the ex-vessel fuel coolant interaction analyses for AP1000 show that the impulse loads on the cavity wall remain below the calculated loads for AP600. In the AP600 analysis, the base case involved a mostly ceramic melt pour, while in the present AP1000 analysis the base case involves a metallic pour, which potentially might lead to a larger impulse load. However, the sensitivity calculations for the most severe case of a deeply flooded cavity in AP1000, clearly show that the previously reported AP600 impulse load predictions are bounding.

The staff acknowledges that the underlying physical phenomena associated with the fuel coolant interaction issue are not fully understood and significant uncertainties remain in some areas. With that understanding, the staff accepts the extension of the conclusions from the AP600 steam explosions analyses to AP1000, based on a high degree of similarity between the two designs.

19.2.3.3.6 Containment Bypass

Severe accident containment bypass for the AP1000 includes three issues: (1) interfacing system LOCAs (ISLOCA) outside containment, (2) steam generator tube rupture (SGTR) events leading to offsite releases through the steam generator relief valves, and (3) containment integrity failure during a severe accident scenario. The evaluation of design options to minimize containment bypass from SGTR events is addressed below. Containment

bypass from SGTR events is discussed in Section 5.4.2.2 of this report. ISLOCA is addressed in Section 19.2.2.1.5 of this report, and maintenance of containment integrity during severe accidents is addressed in Sections 19.2.3.3.7 and 19.2.6 of this report.

In SECY-93-087, the staff recommended that the Commission approve the position to require that the advanced plant designer consider design features to reduce or eliminate containment bypass leakage that could result from SG tube ruptures. The following design features were identified as able to mitigate the releases associated with a tube rupture:

- a highly reliable (closed loop) SG shell-side heat removal system that relies on natural circulation and stored water sources
- a system that returns some of the discharge from the SG relief valve back to the primary containment, and
- increased pressure capacity on the SG shell side with a corresponding increase in the safety valve setpoints

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

Westinghouse evaluated the following design options as part of their assessment of Severe Accident Mitigation Design Alternatives (SAMDA) for AP1000:

- a passive safety-related heat removal system to the secondary side of the steam generators. The system would provide closed loop cooling of the secondary side using natural circulation and stored water cooling, thus preventing a loss of primary heat sink in the event of a loss of startup feedwater and passive RHR heat exchanger. The system was estimated to cost \$1.3 million.
- redirecting the flow from all steam generator safety and relief valves to the IRWST (as well as a lower cost option of this design improvement, consisting of redirecting only the discharge from the first stage safety valve to the IRWST). The system would prevent or reduce fission product release from bypassing the containment in the event of a SGTR event. The system was estimated to cost \$0.6 million.
- increasing the design pressure of the steam generator secondary side and safety valve setpoint to the degree that a SGTR will not cause the secondary system safety valve to open. This design change would also prevent the release of fission products that bypass the containment via the SGTR. The system was estimated to cost \$8.2 million.

On the basis of the estimated CDF and risk from internal events in the AP1000 design, any potential design modifications for accident mitigation that cost more than about \$500 would not be cost effective, even if the modifications were to totally eliminate all offsite consequences. If the baseline core damage frequency is increased by a factor of 100 to account for external events and other accident sequences not included in the analysis, and the design modifications completely eliminate all offsite consequences, this value rises to about \$50,000. The above design changes involve a major redesign effort, pose serious design drawbacks and are prohibitively expensive. In view of the low residual risk for AP1000 and the significant costs associated with the aforementioned design changes, the staff concludes that the risk reduction

offered by the design changes is not significant, and that the design changes are impractical and would excessively impact on the plant.

In Section 19.1.3.1.2 of this report, the staff concludes that preventive and mitigative features in the AP1000 design result in a reduction in the estimated CDF for SGTR sequences to about $7E-09/y$. In Section 15.6.3 of this report the staff concludes that there is reasonable assurance that SGTR events pose no undue threat to the public health and safety. The staff further concludes that the three design alternatives identified in SECY-93-087 have been adequately assessed and that the criteria of SECY-93-087 have been met.

19.2.3.3.7 Equipment Survivability

The survivability of equipment, both electrical and mechanical, is needed to prevent and mitigate the consequences of severe accidents. Westinghouse addressed equipment survivability in Appendix 19D to the AP1000 DCD Tier 2 document which contains general requirements and equipment classification. The analysis performed to determine the severe accident environmental conditions is presented in Appendix D to the AP1000 PRA supporting document.

The requirements for equipment survivability are different from equipment qualification. The latter requires that the safety-related equipment, both electrical and mechanical, must perform its safety function during design bases events. Section 3.11 and Appendix 3D of the AP1000 DCD Tier 2 define the limiting environmental design conditions for all safety-related mechanical and electrical equipment. The level of assurance provided for the equipment operability during design bases events is called "environmental qualification" or "equipment qualification."

Beyond-design-basis events can be divided into two classes: in-vessel and ex-vessel severe accidents. During the in-vessel events the core is losing its coolability leading to at least a partial fuel melt. During the ex-vessel events a reactor vessel failure is assumed, leading to a relocation of molten corium (i.e. mixture of fuel and structural materials) to the containment. Such postulated severe accidents result in environmental conditions that are generally more limiting than those from design bases events. The NRC established a criterion to provide a reasonable level of confidence that the necessary equipment will perform its mitigative function in the severe accident environment for the time span for which it is needed. This criterion is referred to as "equipment survivability."

SECY-93-087 indicated that the staff would evaluate the ALWR vendor's identification of equipment needed to perform mitigative functions and the conditions under which the mitigative systems must operate. In SECY-93-087, the staff recommended that the Commission approve the staff's position that passive plant design features provided only for severe accidents mitigation need not be subject to the 10 CFR 50.49 environmental qualification requirements; 10 CFR Part 50, Appendix B quality assurance requirements; and 10 CFR Part 50, Appendix A redundancy/diversity requirements. The staff concluded that guidance such as that found in Appendices A and B of RG 1.155, "Station Blackout," is appropriate for equipment used to mitigate the consequences of severe accidents. In the SRM dated July 21, 1993, the Commission approved the staff's position.

The applicable criterion for equipment, both mechanical and electrical, required for recovery from in-vessel severe accidents is provided in 10 CFR 50.34(f).

- In Part 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 Part 50.34(f)(3)(v), the NRC states that systems necessary to ensure containment integrity shall be demonstrated to perform their function under conditions associated with an accident that releases hydrogen generated from 100 percent fuel-clad metal-water reaction.
- In Part 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 Part 50.34(f)(2)(xix), the NRC requires instrumentation adequate for monitoring plant conditions following an accident that includes core damage.

These regulations collectively indicate the need to perform a systematic evaluation of all equipment, both electrical and mechanical, and instrumentation to ensure its survivability for intervention into an in-vessel severe accident. The applicable criteria required to mitigate the consequences of ex-vessel severe accidents are discussed in the “Equipment Survivability” sections of SECY-90-016 and SECY-93-087.

In Appendix 19D to the DCD Tier 2 Westinghouse discusses the NRC requirements regarding equipment survivability, various phases of accidents progression (i.e. pre-core uncover, core heatup, in-vessel severe accident phase and ex-vessel severe accident phase), instrumentation needed for monitoring accident progression and equipment required to mitigate consequences of severe accidents. Westinghouse had not included information regarding severe accident conditions in the DCD Tier 2. Such information, however, was provided in the Appendix D to AP1000 PRA supporting document.

The following safety evaluation is based on information included in both Appendix 19D to the DCD Tier 2 and in the Appendix D to AP1000 PRA supporting document.

Westinghouse defined four phases of accidents progression:

- Time Frame 0: Pre-Core Uncovery,
- Time Frame 1: Core Heatup,
- Time Frame 2: In-Vessel Severe Accident Phase, and
- Time Frame 3: Ex-Vessel Accident Phase

Westinghouse claims that requirements to equipment to survive and function vary as accident progresses. During Time Frames 0 and 1 the equipment survivability is covered under the design basis equipment qualification program. During Time Frame 2 the equipment is designed to fulfill the recovery actions under the severe accident management strategies, while during Time Frame 3 the equipment and instrumentation is designed to monitor accident progression,

maintain containment integrity and mitigate fission product releases to the environment. The staff concurs with this characterization.

Specifically, sufficient instrumentation should exist to inform operators of the status of the reactor and the containment at all times as the in-vessel severe accident is intended to be recoverable from and lead to safe shutdown with containment integrity maintained. The emergency response guidelines (ERGs) direct specific manual operator actions determined by instrumentation readings and as such all instrumentation should exist where manual operator actions are specified within the ERGs.

The applicable criteria for equipment, both electrical and mechanical, required to mitigate the consequences of ex-vessel severe accidents is discussed in the "Equipment Survivability" section of SECY-93-087. Mitigative features should be designed to provide reasonable assurance that they will operate in the severe accident environment for which they are intended and over the time span for which they are needed. In cases where safety-related equipment (equipment provided for DBAs) is relied upon to cope with severe accident situations, there should be reasonable assurance that this equipment will survive accident conditions for the period that is needed to perform its intended function. Also, sufficient instrumentation needs to be identified to inform operators of the status of the containment at all times. Of particular interest is the status of the reactor vessel integrity.

Westinghouse analyzed various severe accident scenarios and identified the equipment needed to perform various functions during a severe accident and the environmental conditions under which the equipment must function. The results are summarized in tables 19D-1 through 19D-7 in Appendix 19D to the DCD Tier 2. The severe accidents environment conditions, i.e. pressure, temperature and radiation, in which the equipment is relied upon to function, is provided in Appendix D to the AP1000 PRA supporting document.

Of particular interest is the issue of hydrogen control, i.e. maintaining hydrogen concentration in containment below a globally flammable limit. This function is performed by hydrogen igniters. The emergency response guidelines (ERGs) require activating the igniters in Time Frame 1, even though a significant amount of hydrogen is not generated until the Time Frame 2. The staff's analyses performed by its contractor, ERI, using MELCOR computer program indicate that integrity of the AP1000 containment is not challenged by hydrogen burn during postulated severe accidents, as discussed in Section 19.2.6 of this report. That conclusion applies also to the case, presented by Westinghouse, of a global hydrogen burn (i.e., burn of amount of hydrogen generated by oxidation of 100 percent of the Zircaloy cladding in the active fuel zone.) A potential for hydrogen detonation is eliminated by design, i.e., limiting to hydrogen concentration in the AP1000 containment to a maximum of 10 percent. In addition, the AP1000 containment is equipped with passive autocatalytic recombiners (PARs), not credited for severe accident. Also, previous NRC-sponsored studies of the hydrogen issues (i.e. SECY-02-080 and SECY-00-0198) indicate that combustible gas generated from severe accidents is not risk significant for large, dry containments such as AP1000. Therefore, the staff accepts the AP1000 hydrogen control measures as adequate.

In general, Westinghouse claims that AP1000 provides reasonable assurance that equipment, both electrical and mechanical, designed for mitigating the consequences of severe accidents, will perform their functions as intended. Based on the review of information provided in Chapter

19 of the DCD Tier 2, and Appendix 19D of the AP1000 PRA supporting document, as well as staff's independent severe accident analyses, staff concurs.

19.2.3.3.7.1 Equipment and Instrumentation Necessary to Survive

Westinghouse considers the actions defined by the AP600 Emergency Response Guidelines, Revision 3, May 1997 (Ref. 19D-2), and WCAP-13914, "Framework for AP600 Severe Accident Management Guidance (SAMG)," Revision 1, November 1996 (Ref. 19D-1) to be directly applicable to AP1000 design. Staff performed an independent comparison between the two designs, including independent analyses of AP1000 response to various severe accident scenarios, and concurs with such an approach.

In WCAP-13914, Westinghouse defines a controlled, stable core state and a controlled, stable containment state. The core state can be summarized as having a process for transferring the energy being generated in the core to a long-term heat sink such as a flooded reactor cavity. The conditions associated with this state are considered indicative of a degraded in-vessel core damage accident. The containment state can be summarized as having a process for transferring the energy that is released to an intact containment to a long-term heat sink such as the PCCS. The conditions associated with this state are considered indicative of an ex-vessel severe accident.

Westinghouse determined that the necessary equipment and instrumentation along with the environmental conditions varied over the course of a severe accident. Therefore, Westinghouse identified four equipment survivability time frames. Time Frame 0 is defined as the period of time in the accident sequence after accident initiation and before core uncover. Time Frame 1 is defined as the period of time after core uncover and before the onset of significant core damage as evidenced by the rapid oxidation of the core. Time Frame 2 is the period of time in the severe accident after the accident progresses beyond the design basis of the plant and before the establishment of a controlled, stable core state (end of in-vessel relocation), or prior to reactor vessel failure. Time Frame 3 is defined as the period of time after the reactor vessel fails until the establishment of a controlled, stable containment state or the end of the sequence. The equipment and instrumentation needed for each time frame are summarized in Tables 19D.6-3 through 19D.6-5 of the AP1000 DCD Tier 2.

The equipment listed provides the operator with the ability to (1) inject into the RCS, steam generators and containment, (2) depressurize the RCS, steam generators and containment, (3) control hydrogen, (4) isolate containment, and (5) remove heat and fission products from the containment atmosphere. The list of equipment also includes the cavity flooding system and the containment penetrations. The instrumentation was chosen so that the operator could confirm and trend the results of actions taken and that adequate information would be available for those responsible for making accident management decisions.

The staff performed an independent assessment of the list of equipment and instrumentation provided in Tables 19D.6-3 through 19D.6-5 and compared them to the more extensive lists required by RG 1.97 and 10 CFR 50.34(f) to ensure that the equipment and instrumentation provided is sufficient. The staff concludes that the equipment and instrumentation needed to perform and monitor the mitigative functions necessary during a severe accident are adequate.

19.2.3.3.7.2 Severe Accident Environmental Conditions

The severe accident environmental conditions are discussed in Appendix D to the AP1000 PRA supporting document.

The radiation exposure inside the containment for a severe accident is estimated by considering the dose in the middle of the AP1000 containment with no credit for the shielding provided by internal structures. The instantaneous gamma and beta dose rates are provided in Figures D.1 and D.2, respectively. The source term is based on the emergency safeguards system core thermal power rating of 3,468 MWt, which includes 2% power uncertainty.

The radionuclide groups and elemental release fractions are consistent with the accident source term presented in NUREG-1465, "Accident Source Terms for Light-Water Nuclear Power Plants," February 1995. The timing of the release is founded on NUREG-1465 assumptions. Westinghouse assumes an initial release of activity from the gaps of a number of failed fuel rods at 10 minutes into the accident, which is based on an NRC approved leak-before-break approach. Over the next 30 minutes, from 10 to 40 minutes into the accident, 5 percent of the core inventory of the noble gases, iodine and cesium is assumed to be released to the containment. During the early in-vessel release phase, the fuel as well as other structural materials in the core reach sufficiently high temperatures that the reactor core geometry is no longer maintained and fuel and other materials melt and relocate to the bottom of the reactor vessel. The in-vessel phase is estimated to last 1.3 hours. The ex-vessel release phase begins when molten core debris exits the reactor pressure vessel and ends when the debris has cooled sufficiently that significant quantities of fission products are no longer being released. The ex-vessel phase is assumed to last 2 hours. The late in-vessel period continues for an additional 8 hours. Ultimately, the total fraction of radionuclides core inventory released to the containment includes 100 percent of noble gases, 75 percent of cesium and iodine, and 30.5 percent of tellurium. The staff finds the timing and duration for the early in-vessel, late in-vessel, ex-vessel and the late in-vessel release phases consistent with the NUREG-1465, and, therefore, acceptable.

Evaluation of containment thermal-hydraulic conditions following selected severe accidents was performed by Westinghouse using MAAP4.04 computer code. Five cases were analyzed:

- (i) IGN - DVI line break with vessel reflood, cavity flooding, and igniters,
- (ii) IVR - same as IGN but no vessel reflood,
- (iii) NOIGN - 4-inch DVI line break with vessel reflood, cavity flooding, and no igniters,
- (iv) CCI - large LOCA with igniters, no vessel or cavity reflood, and
- (v) GLOB - global burning of hydrogen from 100-percent cladding reaction.

The timing for each case is presented in Table D-6. The key elements relate to the equipment survivability time frames, as defined above.

The staff, through its contractor at Energy Research, Inc. (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 of the total Core Damage Frequency (CDF). Four scenarios were selected that constitute about 56% of the total AP1000 CDF. These are:

- (1) 3BE - DVI line break with PRHR unavailable (29 % of CDF),
- (2) 3BR - Hot Leg Large Break LOCA (18% of CDF),
- (3) 3D - Spurious ADS actuation (stage 1/2/3) (9% of CDF), and

(4) 1A - Transient initiated by loss of MFW (0.6% of CDF)

For equipment survivability the most important parameter is temperature. The two sets of analyses are not directly comparable since the risk dominant scenarios, selected by staff, are not the worst-case scenarios from the point of view of equipment survivability. Such an approach is acceptable because of inherent analytical uncertainties associated with current state of knowledge of the involved physical phenomena. Given that, and absent global hydrogen burning, the two analyses are similar and result in calculated environmental conditions that are comparable. 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 (476F).

Westinghouse'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 of hydrogen, and an instantaneous maximum containment temperature (Figure D-45 in Appendix D to AP1000 PRA) was about 1300 K (1880 F), while a "steady state" temperature was below 500K (440F). For comparison, the maximum amount of hydrogen produced in the NRC analyses (case 1A) was 621 kg, and maximum containment dome temperature was below 440 K (332 F).

Based on the confirmation provided in the AP1000 PRA supporting document and the independent analysis performed by the NRC's contractor (ERI) the staff concludes that the thermal hydraulic profiles predicted above by MAAP are acceptable approximations of the environmental conditions for which mitigative features and instrumentation, identified in this section, must survive.

19.2.3.3.7.3 Basis for Acceptability

In SECY-93-087, the staff recommended that the Commission approve the general criteria that the staff evaluate the ALWR vendor's review of the various severe accident scenarios analyzed and identify the equipment needed to perform its function during a severe accident and the environmental conditions under which the equipment must function. In its July 21, 1993 SRM, the Commission approved the staff's position.

The staff has performed this evaluation and concludes that the equipment and instrumentation identified by Westinghouse in Tables 19D-3 to 19D-5 of Appendix 19D to the AP1000 DCD Tier 2, and the applicable environments described in Appendix D to the AP1000 PRA supporting document meets the above guidance of SECY-93-087 and 10 CFR 50.34(f) as delineated in Section 19.2.3.3.7 of this report. Reasonable assurance that the equipment and instrumentation identified in this section will operate in the severe accident environment for which they are intended and over the time span for which they are needed is provided by the environmental qualification ITAAC and because of a COL Action Item. Specifically, the COL applicant referencing the AP1000 certified design will perform a thermal response assessment of the as-built equipment used to mitigate severe accidents to provide additional assurance that this equipment can perform its severe accident functions during environmental conditions resulting from hydrogen burns. This assessment is COL Action Item 19.2.3.3.7-1.

19.2.3.3.8 Containment Vent Penetration

Use of a containment vent to prevent containment over-pressure failure is a means of mitigating the consequences of a severe accident. In SECY-93-087, the staff indicated that the need for a containment vent for the passive plant designs would be evaluated on a design-specific basis, and that if acceptable analyses indicate that a vent would not be needed to meet the severe accident criteria, such as the Commission's containment performance goal discussed in Section 19.2.4 of this report, the staff would not propose to implement a vent requirement.

The staff relied on the evaluation of the containment performance goal in Section 19.2.4 of this report for determining the need for inclusion of a containment vent. As discussed therein, for the most likely severe accident challenges, containment pressure would remain below Service Level C as a result of successful retention of core debris in-vessel, and operation of PCS. Accordingly, containment venting will not be required for the more likely severe accident sequences since they do not result in over-pressure failure.

The staff identified two situations in which venting would eventually be required, specifically, events involving either failure of PCS or RPV failure followed by unmitigated CCI. However, these events are much less likely, and do not contribute appreciably to containment failure frequency, as discussed below.

In the event of PCS failure, containment pressure would eventually reach Service Level C, necessitating containment venting (see Section 19.1.3.2.2). In the baseline PRA, the frequency of core damage events involving failure of PCS water delivery is estimated to be about $3E-13/y$. With air cooling only, containment pressure is estimated to reach Service Level C at about 24 hours. In the AP600 PRA, PCS failure was dominated by blockage of the PCS annulus drain lines, which was estimated to have a probability of $1E-04$. This failure mechanism is not modeled in the AP1000 PRA, but at that same failure probability would have a corresponding containment failure frequency of about $2E-11/y$. Containment pressurization will initially be limited by PCS water delivered to the containment shell. However, following depletion of PCS water inventory (at approximately 72 hours) containment pressure will increase and eventually exceed Service Level C due to blockage of the air cooling path.

In the event of RPV failure followed by unmitigated CCI, containment pressure (due to non-condensable gas build-up) would reach Service Level C after about 3 days or later depending on the type of concrete used in the basemat (see Section 19.2.3.3.3). The frequency of core damage with RPV failure and relocation of core debris to the reactor cavity is $5E-09/y$ in the baseline PRA, on the basis of an assumption that RCS depressurization and reactor cavity flooding always result in successful retention of molten core debris in-vessel. As discussed in Section 19.2.3.3.1, the staff's review of ERVC supports this assumption for the core debris configuration considered in the related ROAAM analysis, but uncertainties in the likelihood of retaining a molten core in-vessel are large. Under the most limiting assumption of no credit for ERVC, the frequency of events that result in reactor vessel failure would approach the core melt frequency. However, the frequency of events that require containment venting would be somewhat less than this since the reactor cavity would be flooded in these sequences, potentially resulting in quenching of the core debris and termination of CCI.

The frequency of events that would necessitate containment venting is on the order of $1E-08/y$ founded on the PRA for internal events, and the time at which venting would be required would be 24 hours or later. This frequency could increase substantially if ERVC is not effective in preventing RPV failure. However, even with no credit for ERVC, the frequency of events

requiring venting would be on the order of $1\text{E-}07/\text{y}$ and well below the $1\text{E-}06/\text{y}$ general plant performance guideline for a large release of radioactive material. The staff concludes that the containment performance goals regarding large release frequency and CCFP are met without a containment vent, and therefore, a containment vent is not required for the AP1000 design.

Although containment venting capability is not required to meet the containment performance goals it may be beneficial to depressurize the containment in a controlled manner under certain conditions during a severe accident. Westinghouse considered the impact of venting the AP1000 through penetrations with effective sizes of 4, 6, 10, and 18 inches diameter. The results of the analysis show that over-pressure failure can be successfully mitigated using any of these vent sizes. Westinghouse did not specify the particular line(s) that could be used to vent the AP1000 containment. However, given the range in line sizes that would be effective for venting, and the relatively low pressure requirements associated with venting, a number of different penetrations might be used. The COL applicant, as part of COL Action Item 19.2.5-1 regarding accident management, will identify the specific penetration(s) for containment venting, and will develop and implement severe accident management guidance for venting containment using the framework provided in WCAP-13914, Revision 3.

19.2.3.3.9 Non-Safety-Related Containment Spray

Performance of numerous risk assessment studies over the past 20 years show that the risk to the public from severe accidents is usually dominated by accidents that result in early containment failure commensurate with a significant release of radioactive material. Many design features have been added to the AP1000 design to reduce this risk. Examples include allowing for depressurization of the reactor coolant system, controlling hydrogen generation, and cooling of molten core debris in-vessel. The large passively-cooled AP1000 containment provides significant benefit to cope with severe accident challenges because the failure modes of the containment heat removal system are independent of the scenarios that could lead to containment challenges and of the vulnerabilities associated with reliance on human actions. While the use of passive systems enhances the safety of the plant during early containment challenges, the ability to intervene and provide control over the course of a severe accident has significant benefit in terms of accident management. For existing plants an internal containment spray system and other features can accomplish this. However, the AP1000 relies solely on enhanced natural processes for aerosol fission product removal. The state-of-the-science for evaluating the effectiveness of natural removal processes in harsh environments has uncertainty levels that are greater than those for current operating plants that do not credit these processes.

The concept of passive safety systems is appealing because the design relies primarily on gravity. Passive safety system designs are also attractive because they minimize the need for support systems and reduce reliance on human actions. However, there are uncertainties regarding the performance of passive safety systems. Net driving forces are small compared to active systems. For example, the reliability and functionality of check valves can no longer be taken for granted in passive designs. While a sticking check valve in an active system can be easily overcome by the forces developed by a pump, there is less assurance that the low driving head developed by gravity injection in a passive design will similarly overcome a sticky check valve. In addition, the parallel flow paths existing in the AP1000, combined with the low driving heads, make calculation of flow distributions more uncertain. Although the staff is confident that, within the design basis, the testing program data and conservatism inherent in

design basis analyses bound these uncertainties, the uncertainties become much more significant when considering severe accidents.

In the unlikely event that a severe accident in the AP1000 occurs, the cause is likely to be some combination of events and passive system failures that had not been specifically evaluated or assessed. Assuming the failure of the passive core cooling system features, the containment becomes the primary mitigation system to protect public health and safety. As with other passive systems, there are large uncertainties associated with the passive nature of the containment system design. Heat transfer and fission product removal from the AP1000 containment atmosphere is dependent upon mass condensation onto cool surfaces, predominantly the walls inside containment. Given a severe accident, the long-term buildup and distribution of non-condensable gases within the containment and their effects (as a result of stratification and increasing concentration gradients within the inner containment boundary layer) cannot be assessed with existing analytical tools.

In view of the uncertainties associated with the reliance on passive systems in mitigating severe accidents Westinghouse included a containment spray function as part of the AP1000 fire protection system design. The spray system is described in Section 6.5.3 of DCD Tier 2. This design feature is not safety-related and is not credited in any accident analysis including the dose analysis provided in Section 15.6.5 of DCD Tier 2. Existence of the non-safety spray system introduces additional possibility for operator intervention as part of the design's accident management strategy.

The possibility of inadvertent actuations of the containment spray system is evaluated in Section 6.2.1.1.4, "External Pressure Analysis," of this report.

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

- (1) the capability for site personnel upon recognition of elevated radiation levels in the containment atmosphere to quickly and substantially remove aerosol fission products following activation,
- (2) mixing the containment atmosphere following a severe accident, especially the boundary layer inside the containment shell,
- (3) short term pressure reduction upon injection because of the heat capacity of the subcooled spray water.

19.2.4 Containment Performance Goal

The containment performance goal (CPG) is intended to ensure that the containment structure has a high 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 conditional containment failure probability (CCFP) be less than approximately 0.1 for the composite of all core damage sequences assessed in the PRA.

In SECY-93-087, the staff recommended that the Commission approve the following deterministic containment performance goal for the passive ALWRs:

The containment should maintain its role as a reliable, leak-tight barrier (for example, by ensuring that containment stresses do not exceed ASME Service Level C limits for metal containments or factored load category for concrete containments) for approximately 24 hours following the onset of core damage under the more likely severe accident challenges and, following this period, the containment should continue to provide a barrier against the uncontrolled release of fission products.

In discussions during the Commission meeting on this subject, the staff informed the Commission that it also intends to continue to apply the probabilistic containment performance goal of 0.1 CCFP in implementing the Commission's defense-in-depth regulatory philosophy and the Commission's policy on Safety Goals. (The 0.1 CCFP goal had been proposed by the staff for evolutionary designs in SECY-90-016, and approved by the Commission in its SRM of June 26, 1990.)

In the SRM dated July 21, 1993, the Commission approved the staff's position to use the deterministic CPG in the evaluation of the passive ALWRs as a complement to the CCFP approach, subject to the staff's review and recommendations resulting from public comments on the "Advance Notice of Proposed Rulemaking on Severe Accident Plant Performance Criteria for Future ALWRs." In SECY-93-226, "Public Comments on 57 FR 44513 - Proposed Rule on ALWR Severe Accident Performance", the staff provided the Commission with a summary of public comments received regarding the ANPR, and recommendations regarding policy issues raised in these comments. On the basis of a review of these comments and experience gained from the evaluation of the evolutionary reactor designs, the staff concluded that use of both a deterministic and probabilistic containment performance goal should be pursued for the passive reactor designs. Accordingly, the staff has considered both the deterministic and probabilistic CPGs in assessing the performance of the AP1000 containment.

Deterministic Containment Performance Goal

The staff used the deterministic containment performance criteria to confirm that an acceptable level of containment performance has been achieved. For purposes of this evaluation, containment failure was defined as events in which the containment fails to maintain its role as a reliable, leak-tight barrier for approximately 24 hours following the onset of core damage, or following this period, fails to continue to provide a barrier against uncontrolled release of fission products. Containment was assumed to fail if any of the following conditions occur (even if the conditions occur after 24 hours):

- internal pressure exceeds the value associated with ASME Code Service Level C Limits
- the containment is bypassed, such as in SGTR and ISLOCA events
- the containment fails to isolate
- containment seal materials fail as a result of over-temperature
- molten core debris melts through the concrete basement into the subsoil

Controlled venting of containment would not constitute containment failure provided venting occurs after approximately 24 hours following onset of core damage.

On the basis of the Level 2 PRA results, the more likely severe accident challenges are defined by sequences in which the RCS is fully depressurized, the reactor cavity is flooded, the reactor vessel is reflooded and intact, the containment is isolated, and the PCS and hydrogen igniter systems are operable. (Such sequences represent more than 90 percent of the core damage frequency). Each of these sequence characteristics is directly attributable to corresponding safety-grade features incorporated in the AP1000 design, and the very low contribution of station blackout sequences to core damage frequency. The peak containment pressure for these sequences would be on the order of 30 psig, and the long-term pressure would be on the order of 10 to 20 psig.

All relevant severe accident challenges were evaluated for these sequences, including hydrogen combustion, high pressure melt ejection, temperature-induced creep rupture of steam generator tubes, fuel-coolant interactions, and core-concrete interactions. These phenomena do not contribute to containment over-pressure or over-temperature failure because of operation of the safety systems incorporated in the AP1000 design. Specifically, operation of the hydrogen igniter system produces peak hydrogen burn pressures well below Service Level C, and eliminates the potential for deflagration-to-detonation transitions. RCS depressurization eliminates high pressure melt ejection and temperature-induced SGTR challenges, and terminates fission product releases to the environment in SGTR and ISLOCA events. Reactor cavity flooding, in conjunction with RCS depressurization, provides reasonable assurance that core debris will be retained within the reactor vessel, thereby preventing ex-vessel FCIs, core concrete interactions/basemat melt-through, and long-term over-pressurization of containment. The operation of PCS, in conjunction with reactor cavity flooding, maintains containment pressure below Service Level C and containment temperature below levels where over-temperature failure would be a concern. Finally, core damage events involving failure of containment isolation account for less than one percent of the total core damage frequency in the baseline PRA.

For the less likely events in which these safety-grade systems do not operate, the probability of containment failure from the associated severe accident phenomena is assessed in the Level 2 PRA and in separate deterministic calculations of each phenomena described elsewhere in Section 19.2 of this report, i.e., hydrogen combustion (Section 19.2.3.3.2), high pressure melt ejection (Section 19.2.3.3.4), ex-vessel FCI (Section 19.2.3.3.5.2), and core concrete interactions (Section 19.2.3.3.3). The results of these assessments indicate that the containment is generally capable of withstanding the challenges from these phenomena, with a small attendant probability of containment failure. The probability of containment failure is addressed below in the context of the probabilistic containment performance goal. The contribution of the various phenomena to the overall containment failure frequency is described further in Section 19.1.3.2.2 of this report.

On the basis of the availability of the severe accident mitigation design features in the majority of the core damage sequences, and the ability of the containment to accommodate the corresponding severe accident loads, the staff concludes that the AP1000 containment will maintain its role as a reliable, leak-tight barrier for the more likely severe accident challenges, in accordance with the deterministic containment performance goal.

Probabilistic Containment Performance Goal

The staff used the probabilistic containment performance criteria to confirm that an acceptable level of containment performance has been achieved, and to identify important contributors to containment failure. For purposes of calculating containment failure frequency, containment failure was defined as above, with the exception that containment over-pressure failure was on the basis of a plant-specific containment failure probability distribution (containment fragility curve) rather than the Service Level C Limit. Using this approach, the probability of containment failure reflects best-estimate structural capabilities and associated uncertainties rather than the more conservative assumption that containment failure occurs whenever Service Level C is exceeded. A general plant performance guideline of $1\text{E-}06/\text{y}$ for a large release of radioactive material (as proposed in the Safety Goal Policy Statement) and a conditional containment failure probability goal of 10 percent (as discussed above) were used as points of reference for the probabilistic assessment. As described in Section 19.1.3.2, essentially all of the containment failure frequency (99 percent) is the result of either containment bypass, containment isolation failure, or early containment failure. Thus, containment failure frequency and large early release frequency are equivalent in this application.

The containment failure frequency for internal events is $1.9\text{E-}08/\text{y}$ in the baseline PRA, which is nearly two orders of magnitude below the large release guideline. The corresponding CCFP is 8.1 percent, which is below the CCFP goal. In Section 19.1.3.2.4 the staff discusses the results of the probabilistic assessment and supporting sensitivity analyses. Through these analyses the staff concludes that for reasonable variations in Level 2 input assumptions and CET split fractions, increases in the containment failure frequency and CCFP are limited to a factor of about 3, and the containment failure frequency remains below $1\text{E-}07/\text{y}$. Also, modest changes in the containment failure probability distribution used in the analysis would not noticeably impact the containment failure frequency since the bulk of the containment failures in the existing analyses are driven by the frequency of events with failure of RCS depressurization or reactor cavity flooding, rather than the frequency at which containment pressure loads exceed the containment pressure capability.

The staff concludes that the AP1000 containment design satisfies the Commission's probabilistic containment performance goal. Specifically, the estimated containment failure frequency in the baseline PRA is well below the large release guideline of $1\text{E-}06/\text{y}$. The conditional containment failure probability is below the CCFP goal of 10 percent in the baseline PRA. Although the CCFP goal is exceeded in several sensitivity cases, these increases are modest, and the corresponding containment failure frequencies remain well below $1\text{E-}06/\text{y}$. In view of the approximate nature of the containment performance goal, the recognition that PRA results contain considerable uncertainties, and the fact that under more realistic modeling assumptions a large fraction of the containment failures reflected in the calculated CCFP in the baseline PRA would actually involve late basemat melt-throughs (or no containment failures) rather than early releases to the atmosphere, the staff concludes that the AP1000 design satisfies the Commission's goals for both large release frequency and CCFP.

19.2.5 Accident Management

Accident management (AM) encompasses those actions taken during the course of an accident by the plant operating and technical staff to (1) prevent core damage; (2) terminate the progress of core damage if it begins and retain the core within the reactor vessel; (3) maintain containment integrity as long as possible; and (4) minimize offsite releases. AM, in effect, extends the defense-in-depth principle to plant operating staff by extending the operating procedures well beyond the plant design-basis into severe fuel damage regimes, and by making full use of existing plant equipment and operator skills and creativity to terminate severe accidents and limit offsite releases.

On the basis of PRAs and severe accident analyses for the current generation of operating plants, the NRC staff concluded that the risk associated with severe accidents could be further reduced through improvements to utility accident management capabilities. Although future reactor designs such as the AP1000 will have enhanced capabilities for the prevention and mitigation of severe accidents, accident management will remain an important element of defense-in-depth for these designs. However, the increased attention on accident prevention and mitigation in these designs can be expected to alter the scope, focus, and overall importance of accident management relative to that for operating reactors. For example, increased attention on accident prevention and the development of error tolerant designs, can be expected to decrease the need for operator intervention, while increasing the time available for such action if necessary. This will tend to relieve the operators of the need for rapid decisions, and permit a greater reliance on support from outside sources. For longer times after an accident (several hours to several days), human intervention and accident management will continue to be needed.

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

For both operating and advanced reactors the overall responsibility for AM, including development, implementation, and maintenance of the accident management plan, lies with the nuclear utility, since the utility is ultimately responsible for the safety of the plant and for establishing and maintaining an emergency response organization capable of effectively responding to potential accident situations. However, the development and implementation of accident management in future reactors involves both the reactor designer and the plant owner/operator, particularly in view of the fact that many of the design details are still to be developed (such as balance of plant equipment and final piping layout). The plant designer is responsible for developing the technical bases for the plant-specific accident management program or plan, whereas the owner/operator is responsible for developing and implementing the complete accident management plan, including those areas beyond the purview of the plant designer, such as the content and techniques for severe training, and the delineation of decision making responsibilities at a plant specific level.

The COL applicant will develop and submit an accident management plan as part of the COL application. This was previously identified as COL Action Item 19.2.5-1. The plan will provide a commitment to perform a systematic evaluation of the plant's ability to deal with potential severe accidents, and to implement the necessary enhancements within the detailed plant design and organization, including severe accident management guidelines and training. General areas that will be addressed in the plan include the following five items: (1) accident management strategies and implementing procedures, (2) training in severe accidents, (3) guidance and computational tools for technical support, (4) instrumentation, and (5) decision making responsibilities.

All AP1000 PRA insights and COL action items that fall within the scope of accident management should be specifically addressed as part of the COL applicant's accident management plan, including:

- development of detailed guidance and procedures for the use of the severe accident features in the AP1000 design, including the ADS (manual actuation after core uncover), the hydrogen igniter system, the reactor cavity flood system, the containment spray system, and containment venting
- development of guidance and procedures on protection of fission product barriers, including:
 - filling the SGs, and avoiding SG depressurization if water is not available, in order to prevent a thermally-induced SGTR
 - depressurizing the RCS and maintaining a secondary side water level covering the SG tubes in order to mitigate fission product releases from a SGTR event
 - using the containment spray system and associated water sources for containment fission product scrubbing in events with intact or vented containments
 - using containment venting to control fission product releases
- development of guidance and procedures for actions that are expected to be taken in the longer-term (post-72 hours), including:
 - using the ancillary ac diesel generators to power the post-accident monitoring system, main control room lighting, and the PCS recirculation pumps
 - aligning and using the PCS recirculation pumps to refill the PCCWST from a mobile water source using power from the ancillary diesel generators
 - changeover of the main control room habitability system from air bottles to circulation using diesel-powered ancillary fans
 - water makeup to the spent fuel pool and containment
 - reflooding a damaged core which is retained in-vessel

- development of guidance and procedures for actions that may need to be taken in events during shutdown operations, such as actions to flood the reactor cavity
- evaluation of information needed to implement the accident management guidelines, and plant instrumentation that could be used to supply the needed information considering instrumentation availability and survivability under severe accident conditions

Westinghouse 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 severe accident management requirements, the anticipated structure for the decision making process, the goals that must be accomplished for severe accident management, a summary of possible strategies for AP1000 severe accident management, and potential adverse impacts of AM strategies. The COL applicant is expected to follow the recommendations provided in WCAP-13914, Revision 3 in developing their plant-specific AM guidance. This is COL Action Item 19.2.5-1.

The staff will review the accident management plan at the COL stage to assure that the evaluation process and commitments proposed by the COL applicant provide an acceptable means of systematically assessing, enhancing, and maintaining AM capabilities, consistent with staff expectations. The COL applicant would subsequently implement the plan and submit the results for staff review before plant operation. This plan should be developed on the basis of the final, as-built plant, the accident management-related information developed by the plant designer, and the accident management program guidance developed for the current generation of operating reactors. As previously discussed this is COL Action Item 19.2.5-1.

19.2.6 Ultimate Pressure Capacity of the Containment [Goutam]

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

In 10 CFR 50.34(f)(1)(i), the NRC requires an applicant to "perform a plant/site specific probabilistic risk assessment, the aim of which is to seek such improvements in the reliability of core and containment heat removal systems as are significant and practical and do not impact excessively on the plant." For AP600, Westinghouse provided an evaluation of potential design improvements (Severe Accident Mitigation Design Alternatives) in Appendix 1B of the SSAR. The details of this evaluation, which included a design description and estimated risk reduction and costs for each alternative, and estimated offsite exposure for each of the major release categories, formed the basis for the staff's review. A similar evaluation was not provided in Appendix 1B of the DCD or in the PRA for AP1000, but was submitted in response to RAI 720.60.

Based on a review of the RAI response, the staff determined that the Westinghouse evaluation did not address a number of items called out in the RAI and had several additional deficiencies, as summarized below:

- A. the cost benefit methodology appears to be based on an outdated guidance document (NUREG/CR-3568, 1983), rather than the current guidance for regulatory analysis contained in NUREG/BR-0184 (1997) and NUREG/BR-0058 (2000).
- B. replacement power costs were omitted. These averted onsite costs need to be included consistent with SECY-99-169.
- C. the CDF and population dose values used in the evaluation only reflect internal events. The contribution to CDF and population dose from shutdown and fire events should also be included.
- D. the RAI requested an explanation of how insights from the AP1000-specific PRA and supporting risk analyses for external and shutdown events, including importance analyses and cutset screening, were used to identify potential plant improvements. This was not addressed in the response.
- E. the RAI requested justification that the potential improvements identified through a systematic process (as suggested above) are included within the set of 15 SAMDAs identified in Appendix 1B of the AP1000 DCD. This was not addressed in the response.

In a revised RAI response dated March 31, 2003, Westinghouse provided an updated evaluation addressing these concerns. The staff has not completed of its evaluation of SAMDAs for AP1000. This is a AP1000 DSER Open Item.

=====

Issue II.B.8: Rulemaking Proceedings on Degraded Core Accidents Description

Item II.B.8 of NUREG-0933 discussed the need to establish policy, goals, and requirements to address accidents resulting in core damage greater than the existing design basis. The Commission expects that new designs 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 developed guidance and goals for designers to strive for in accommodating events that are beyond what was previously known as the design basis of the plant.

For advanced passive nuclear power plants, like the AP1000, the staff concluded that vendors should address severe accidents during the design stage to take full advantage of the insights gained from such input as probabilistic safety assessments, operating experience, severe accident research, and accident analysis by designing features to reduce the likelihood that severe accidents will occur and, in the unlikely occurrence of a severe accident, to mitigate the consequences of such an accident. Incorporating insights and design features during the design phase has been demonstrated to be much more cost effective than modifying existing plants.

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

- the "NRC Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants"

- the "NRC Policy Statement on Safety Goals for the Operations of Nuclear Power Plants"
- the "NRC Policy Statement on Nuclear Power Plant Standardization"
- 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 Regulatory Requirements", and the corresponding staff requirements memorandum (SRM) dated June 26, 1990
- SECY-93-087, "Policy, Technical And Licensing Issues Pertaining to Evolutionary and Advanced Light-water Reactor (ALWR) Designs", and the corresponding SRM dated July 21, 1993

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

The basis for resolution of severe accident issues for the AP1000 is 10 CFR Part 52 and SECY-93-087. 10 CFR Part 52 requires (a) compliance with the TMI requirements in 10 CFR 50.34(f), (b) resolution of unresolved safety issues and generic safety issues, and (c) completion of a design-specific probabilistic risk assessment. The staff evaluates these criteria in Sections 20.3, 20.1 and 20.2, and 19.1 of this report, respectively.

The Commission-approved positions on the issues discussed in SECY-93-087 form the basis for the staff's deterministic evaluation of severe accident performance for the AP1000. The staff evaluates the AP1000 relative to these criteria in Section 19.2 of this report. Issue II.B.8 is resolved for the AP1000 design on the basis of the staff's evaluation of the probabilistic and deterministic analyses in the AP1000 PRA, as documented in Chapter 19 of this report.

Insert to Table 20.7-2

GL-88-02, Integrated Safety Assessment Program II (ISAP II)	This issue is resolved for AP1000. Risk insights are already an integral part of the staff's AP1000 design review process as discussed in Chapter 19 of this report on severe accidents and PRA for the design. This generic letter is resolved for the AP1000 design.
--	--

.....

Insert to Table 20.7-2

GL-88-20, Individual Plant Examination for Severe-Accident Vulnerabilities	This issue is resolved for AP1000. Risk insights are already an integral part of the staff's AP1000 design review process as discussed in Chapter 19 of this report on severe accidents and PRA for the design. This generic letter is resolved for the AP1000 design.
--	--