19.0 SEVERE ACCIDENTS

19.0 Background

Since the U.S. Nuclear Regulatory Commission (NRC) issued Supplement 1 to the final safety evaluation report (FSER) in December 2005, the agency has issued requirements and guidance for addressing severe accidents in the following documents:

Regulatory Guide 1.200

Regulatory Guide (RG) 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," issued in February 2004, and revised in January 2007, describes one acceptable approach for determining whether the quality of the probabilistic risk assessment (PRA) (as a whole or in the parts used to support a particular application) provides sufficient confidence in the results such that the PRA can be used in regulatory decisionmaking for light-water reactors. This RG endorses, with certain restrictions, the American Society of Mechanical Engineers (ASME) "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications" (ASME RA-S-2002), including Addenda A and B, as well as the Nuclear Energy Institute (NEI) guidance entitled, "Probabilistic Risk Assessment Peer Review Process Guidance" (NEI 00-02).

10 CFR Part 52

The Commission initially issued Title 10, Part 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," of the *Code of Federal Regulations* (10 CFR Part 52), on April 18, 1989. This rule provides for issuing early site permits, standard design certifications, and combined licenses (COLs) with conditions for nuclear power reactors. It details the review procedures and licensing requirements for applications for these new licenses and certifications and is intended to achieve the early resolution of licensing issues, as well as to enhance the safety and reliability of nuclear power plants.

The NRC revised the rule on August 28, 2007. Specifically, 10 CFR 52.47, "Contents of Applications; Technical Information," now requires an application for design certification to describe the design-specific PRA and its results.

19.1 Probabilistic Risk Assessment

19.1.1 Introduction

Westinghouse Electric Company (Westinghouse or the applicant) requested an amendment to the AP1000 design certification rule (Appendix D, "Design Certification Rule for the AP1000 Design," to 10 CFR Part 52) and provided a revised design control document (DCD). Westinghouse had submitted a design-specific PRA of the AP1000 design as part of the AP1000 design documentation for the certified design. The applicant did not submit a revised PRA report with the amendment request; however, Westinghouse did describe, in a number of technical reports, the changes to the PRA that would result from the design modifications proposed in the amendment. The proposed changes to the DCD reflect these modifications.

The NRC's regulations at 10 CFR Part 52 no longer require submittal of the PRA report. Instead, applicants are to provide, in the DCD, a description of the PRA and a summary of its results. The design-specific PRA is available for the staff's review and still forms the basis for the site-specific, plant-specific PRAs that COL holders must prepare at application and upgrade and update before loading fuel.

Since certification of the AP1000 design, Westinghouse upgraded the PRA as part of a conversion from proprietary software to a widely used program called CAFTA. The PRA was also updated to reflect proposed design changes. As part of the AP1000 design certification amendment application, it reported all resulting changes to the insights, assumptions, and results of the analysis.

In addition to the revised DCD, the staff reviewed the following AP1000 COL standard technical reports:

- APP-GW-GL-011, "AP1000 Identification of Critical Human Actions and Risk Important Tasks" (WCAP-16555)
- APP-GW-GLN-016, "Generic Reactor Coolant Pump" (TR-34)
- APP-GW-GLN-022, Revision 1, "DAS Platform Technology and Remote Indication Change" (TR-97)
- APP-GW-GLR-016, "AP1000 Pressurizer Design" (TR-36)
- APP-GW-GLN-105, Revision 1, "Building and Structure Configuration, Layout and General Arrangement Design Updates" (TR-105)
- APP-GW-GLN-106, Revision 1, "Mechanical System and Component Design Update" (TR-106)
- APP-GW-GLR-021, "AP1000 As-built COL Information Items" (TR-6)
- APP-GW-GLR-065, "AP1000 Instrumentation & Control (I&C) Data Communication and Manual Control of Safety Systems and Components" (TR-88)
- APP-GW-GLR-070, "Development of Severe Accident Management Guidance" (TR-66)
- APP-GW-GLR-101, "AP1000 PRA Evaluation of External Events" (TR-101)
- APP-GW-GLR-102, "AP1000 PRA Update Report" (TR-102)
- APP-GW-GLR-130, "Editorial Format Changes Related to Combined License Applicant and Combined License Information Items" (TR-130)
- APP-GW-GLR-134, Revision 5, "AP1000 DCD Impacts to Support COLA Standardization" (TR-134)

- APP-PRA-GER-001, “AP1000 Design Change Proposal Review for PRA and Severe Accident Impact” (TR-135)

- APP-GW-GLN-147, Revision 1, “AP1000 CR and IRWST Screen Design” (TR-147)

This information is generic to the design and applies to all combined license applications (COLAs) that reference the AP1000 design certification.

19.1.1.1 Background and NRC Review Objectives

The general objectives of the NRC’s review of the most recent AP1000 DCD amendment include the following:

- identification of new risk-informed safety insights based on systematic evaluations of risk associated with the amended design

- confirmation that regulatory treatment of non-safety systems (RTNSS) remains appropriate

- confirmation that the design certification requirements, such as inspection, tests, analyses, and acceptance criteria (ITAACs), design reliability assurance program (D-RAP), and technical specifications, as well as COL and interface requirements, are amended as appropriate

- confirmation that the conclusions reached in the previous certification remain valid

During the construction stage, the COL applicant will ensure that detailed design documents are consistent with the certified design and that the key assumptions and risk insights from the PRA (documented in DCD Table 19.59-18) remain valid (D–RAP ITAAC). The COL applicant will ensure, through other ITAAC and preoperational programs, that the configuration of the plant, as built, is consistent with the detailed design. The Commission believes that updated PRA insights, if properly evaluated and used, could strengthen programs and activities in areas such as training, emergency operating procedures (EOPs) development, reliability assurance, maintenance, and evaluations performed pursuant to 10 CFR 50.59, “Changes, Tests and Experiments.” The design-specific PRA, developed as part of the design certification process, should be revised to account for site-specific information, as-built (plant-specific) information refinements in the level of design detail, technical specifications, plant-specific EOPs, and design changes. The COL holder is responsible for these updates. This is part of COL Information Item 19.59.10-2.

The NRC requires the COL applicant to develop a plant-specific PRA based on the design-specific PRA. At the time of application, the plant-specific PRA of internal events, at power and shutdown, must address, at the least, proposed deviations from the certified design. The plant-specific PRA of external events must evaluate external events applicable to the proposed site and confirm that they are bounded by the PRA. This is also part of COL Information Item 19.59.10-2. The staff expects that the COL applicant and holder will use the plant-specific PRA and revised failure rates (when available) to update, as appropriate, the quality assurance and reliability assurance programs (including the Maintenance Rule program).

19.1.1.2 Evaluation of Probabilistic Risk Assessment Quality and Closure of Open Issues

The NRC staff evaluated the information submitted by the applicant in accordance with NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants" (hereafter referred to as the SRP), Sections 19.0, "Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors," and 19.1, "Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities."

In APP-GW-GLR-102 (TR-102), the applicant described conversion of the PRA modeling software package from the Westinghouse proprietary program, WesSAGE, to the more widely used computer-aided fault tree analysis system (CAFTA). The applicant also updated the AP1000 PRA to include the most recent instrumentation and controls (I&C) design information. The applicant documented the basis for its determination that structures, systems, and components (SSCs) modeled in the PRA were not affected by other design changes in a manner that affected the PRA.

In its original review of the AP1000 PRA, the staff relied on the similarity between the AP600 and AP1000 certified designs to reduce the review effort. This similarity (e.g., in system design and overall plant layout) allowed the use of the AP600 PRA as the starting point in the development of the AP1000 PRA. Similarly, the PRA associated with the currently certified AP1000 design was the starting point for upgrading and updating the AP1000 PRA in support of the design certification amendment. In addition to reviewing the description of changes to the PRA, the staff reviewed the description of the new I&C design, specifically the plant control system (PLS) and protection and safety monitoring system (PMS).

The review of the quality and completeness of the AP1000 PRA included the issuance of several requests for additional information (RAIs) to the applicant (RAI-TR102-SPLA-01 through RAI-TR102-SPLA-08). The applicant responded to these RAIs in a letter from A. Sterdis to the NRC dated August 23, 2007 (DCP/NRC1981).

The staff used reported PRA results, as well as the results of sensitivity, uncertainty, and importance analyses, to focus its review. The staff also used applicable insights from previous PRA studies regarding key parameters and design features.

Following its review of the responses to the RAIs related to TR-102, the staff conducted an audit at the applicant's offices, focusing on three principal areas:

(1) assessment of the applicant's process to upgrade the PRA model, including the process by which Westinghouse assessed the design and operational changes for potential impact on the PRA

(2) review of the changes to the model since the applicant submitted the previous PRA report, especially those resulting from proposed changes to the certified design

(3) inspection of the model itself to confirm that the model accurately reflected modifications to the design and that the model is a suitable basis for PRAs required of COL applicants that reference the AP1000 design certification

In the process, the staff reviewed the qualifications of personnel involved in PRA-related activities and found them to be acceptable. The staff also examined the procedures the applicant used to review modifications for their potential impact on the PRA, to identify and correct problems in the model, to implement changes to the model, and to assess the results of analysis. During this review, the staff developed further requests for additional information based on SRP Chapter 19, discussed below.

The following sections document the staff's review of the AP1000 design certification amendment. The section numbering corresponds to that used in NUREG-1793, "Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design." In its evaluation, the staff categorized items that require additional attention by the applicant into one of the following categories:

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

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

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

Section 19.1.10 of this evaluation provides a summary of open items resulting from the review of Chapter 19.

19.1.2 Special Advanced Design Features

19.1.2.1 Special Advanced Design Features for Preventing Core Damage

Westinghouse has proposed changes to the certified AP1000 design that have the potential to affect the PRA. The following sections discuss these changes.

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

The AP1000 design incorporates several active systems that are capable of performing some of the same functions as those performed by the safety-related passive systems. The availability of such redundant systems minimizes the challenge to the safety-related passive systems by providing core cooling during normal plant shutdowns and a first line of defense during accidents.

The diverse actuation system (DAS) provides an alternate means for initiating automatic and manual reactor trip and actuation of selected engineered safety features that is diverse from the safety-related PMS. An additional DAS squib valve control cabinet, spatially separated from the DAS cabinet in the control room, provides additional confidence that operators can take manual actions to depressurize the reactor coolant system (RCS) and initiate key functions, such as in-containment refueling water storage tank (IRWST) injection, containment recirculation, and IRWST drain to containment. In DCD Table 19.59-18, the applicant clarified the degree of diversity between PMS and DAS. Section 7.7 of this report includes the staff evaluation of this modification. The staff requested additional information (RAI-SRP19.0-SPLA-06) on the potential of this modification to affect the timing of steps taken to mitigate an anticipated

transient without scram (ATWS) event (positively or negatively) and to reduce risk by providing a spatially diverse actuation station.

In a letter from R. Sisk to the NRC dated August 21, 2008 (DCP/NRC2233), the applicant responded that the addition of the remote DAS cabinet would not result in a significant change to the risk importance of any SSC or human action. The probability of using this remote cabinet is very low, as it would require several very unlikely events to occur. An example of such a situation would be the need to use manual controls coupled with the need to evacuate the control room coupled with a failure or unavailability of the remote PMS panels. It is very likely that a fire or event that would make the control room and the remote PMS panel unavailable for manual operation would also result in a successful automatic shutdown of the AP1000. In addition, human reliability analyses (HRAs) for the DAS use values that represent low probability of success, high-stress situations. This supports the conclusion that the modification would not result in a significant change to the risk importance of any SSC or human action. For that reason, the AP1000 PRA does not model separately the use of this remote panel.

The staff noted that the PRA models manual action as a single basic event irrespective of the location from which that action is taken. Furthermore, the proposed modification reduces uncertainty in the performance of the action. Because the need to use the remote DAS cabinet requires multiple, simultaneous, and highly unlikely events, the risk importance of SSCs or human actions will not be significantly altered by additional detail in the model. For these reasons, the staff concludes that the applicant's decision not to alter the modeling of this system is conservative and acceptable.

19.1.2.1.7 Redundant Long-Term Recirculation Systems

RCS recirculation is required for long-term core cooling during loss-of-coolant accidents (LOCAs) and whenever the feed-and-bleed method is used to cool the core during an accident. In the AP1000, recirculation can be achieved either by gravity (through the safety-related IRWST injection lines) or pumping (through the non-safety-related normal residual heat removal system (RNS)) with suction from the containment sump. Two redundant recirculation lines exist (one for each of the two redundant IRWST injection lines). Furthermore, each recirculation line has two paths that are redundant, with the exception of the recirculation screens. Though there are two separate screens, the applicant does not characterize them as redundant and explicitly models their common-cause failures (CCFs). Section 6.3 of this report documents the staff's evaluation of the screen design.

The staff asked the applicant to discuss the impact of changes to the design of the recirculation system on the results and insights of the shutdown risk assessment (RAI-SRP19.0-SPLA-04).

In a letter from R. Sisk to the NRC dated July 22, 2008 (DCP/NRC2211), the applicant stated that the structural integrity of the new recirculation screen configuration exceeds that of the screen-like material typically used in current pressurized-water reactor (PWR) sump screens, precluding the need for trash racks. Screen testing demonstrated that the new screens will not experience a significant head loss while operating within design-basis flow/debris conditions. A qualitative assessment concluded that the enhancement will reduce failure probability, while the increased flow area will improve accident response.

The staff finds it reasonable to expect that the proposed modification will improve performance of the recirculation screens as compared to the certified design. Although the large,

interconnected screens are not independent, the staff finds that the applicant adequately addressed CCF of the screens. For these reasons, the staff concludes that the applicant's decision not to alter the modeling of this system is conservative and acceptable.

19.1.2.1.9 Canned Reactor Coolant Pumps

The AP1000 design originally specified canned reactor coolant pumps (RCPs). In APP-GW-GLN-016, "AP1000 Licensing Design Change Document for Generic Reactor Coolant Pump" (TR-34), the applicant specified sealless RCPs, which may be a canned-motor or wet-winding pumps. For both canned-motor and wet-winding pumps, the motor and all rotating components are inside a pressure vessel. The pressure vessel consists of the pump casing, thermal barrier, stator shell, and stator cap, all of which are designed for full RCS pressure. Because the rotor and shaft connecting it to the impeller are contained within the pressure boundary, a seal is not required to restrict leakage out of the pump into containment. In addition, the heat exchanger that cools the RCP has been modified; it is now external to the pump. The applicant asserts that these changes do not alter the PRA model.

Section 5.4 of this report discusses the staff's evaluation of changes to the RCP design. The pump design is important because the use of sealless RCPs in the AP1000 design eliminates the RCP seal LOCA (an important contributor to risk for operating PWRs). In addition, water is used to lubricate and remove heat from pump bearings, eliminating the need for RCP lubricating oil systems and the attendant fire hazard. Because the proposed design alternative of a wet-winding rotor changes neither the failure modes of the RCP and its heat exchanger nor the estimated reliability of these components, the staff concludes that no change to the PRA model is required.

19.1.2.1.10 Improved Control Room Design and Digital Instrumentation and Control Systems

The AP1000 control room is an advanced design that is expected to provide information that is presented to the operator in a way that is more easily used than the displays in currently operating reactor designs. Similarly, control is expected to be easy and consistent, and nearly all actions can be performed from a single station. Section 7.1.4 of this report documents the staff's review of the AP1000 control room design.

The PRA took no credit for the impact of the advanced control room on normal operations and emergency response (e.g., initiating event frequency or HRA). Because the impact of an advanced control room is still the subject of research and control room design verification and validation cannot be performed until a control room is simulated, the staff concludes that this approach is conservative and acceptable for design certification.

During an audit of the applicant's PRA, the staff identified a discrepancy in the CCF probability of PMS component interface modules for the recirculation squib valve (V-118). The applicant immediately initiated corrective action. The staff requested correction of the discrepancy and an updated report of PRA results (RAI-SRP19.0-SPLA-07). Specifics requested included (1) the results of resolving and requantifying the baseline and RTNSS full-power PRA, the shutdown PRA, and the external events PRA, (2) new risk insights identified during requantification of the previously mentioned PRAs, and (3) the results of the revised importance analysis.

In a letter from R. Sisk to the NRC dated August 21, 2008 (DCP/NRC2233), the applicant reported that, in addition to correcting the discrepancy, analysts identified measures to improve

the realism of the PRA for I&C systems. Specifically, the analyses found the values selected for PMS and PLS component common-cause beta factors to be overly conservative. The applicant has revised the model to reflect component-specific common-cause beta factors for PMS and PLS system components modeled in the PRA.

In that letter, the applicant committed to revising APP-GW-GLR-102 (TR-102). The revision will reflect (1) the results of resolving and requantifying the baseline and RTNSS full-power PRA, the shutdown PRA, and the external events PRA, (2) any new risk insights identified during requantification of the previously mentioned PRAs, and (3) the results of the revised importance analyses. The applicant also reported that "requantification of the at-power PRA indicate that the core damage frequency (CDF) and large release frequency (LRF) values and top cutsets closely compare with these items documented in the DCD PRA…."

In a letter from R. Sisk to the NRC dated November 6, 2008 (DCP/NRC2284), the applicant reported some results of model correction and requantification. (The software used for this process automatically re-solves the model each time the model is requantified.) The letter reported only those results of the PRA that were point estimates of core damage frequency (CDF) and large release frequency (LRF) (total, at power, shutdown, and sensitivity to non-safety SSCs). The applicant reported no other changes in risk insights or importance analysis. The staff noted several changes that met the criteria of COL/DC-ISG-3, "PRA Information to Support Design Certification and Combined License Applications," during the onsite audit of the PRA. For example, the applicant had not reported a significant shutdown PRA sequence. In another case, design improvements had eliminated a risk-significant component. Because these and similar changes were not reported, the staff did not find this letter to be fully responsive. The staff identified the absence of corrected results in the DCD as Open Item OI-SRP19.0-SPLA-07.

19.1.2.1.11 Large Pressurizer and Low-Power Density

The AP1000 pressurizer is large in comparison to the pressurizer of currently operating plants. This reduces the frequency of reactor scrams by increasing transient operation margins. This feature also moderates the pressure rise during certain transient events, such as loss of main feedwater, thus reducing the likelihood of a challenge to the primary safety valves. A larger pressurizer volume, as compared to currently operating plants, also helps lower the peak pressure that can be reached after a postulated ATWS event.

The applicant found it necessary to alter the design of the pressurizer. APP-GW-GLR-016 (TR-36) details this change. Section 5.4.5 of this report documents the staff's evaluation of this design change. The applicant did not propose a change to the PRA because of this modification.

Because the applicant analyzed the proposed design changes to the pressurizer and found that they do not alter system-level thermal-hydraulic response or success criteria, the staff concludes that no change to the PRA model is necessary.

19.1.2.2 Special Advanced Design Features for Core Damage Consequence Mitigation

The following design features improve the ability of the containment to accommodate the challenges associated with severe core damage accidents. The AP1000 PRA and/or

supporting deterministic analyses model the impact of these features on severe accident mitigation and containment performance.

19.1.2.2.4 External Reactor Vessel Cooling

Refinements to the AP600 reactor vessel insulation system design were required to increase the heat transfer capability (critical heat flux (CHF)) from the reactor pressure vessel (RPV) to the surrounding water and to accommodate the higher decay heat level in the AP1000. APP-GW-GLR-060, "Reactor Vessel Insulation System—Verification of In-Vessel Retention Design Bases" (TR-24), addresses COL Information Item 5.3-5 by verifying that reactor vessel insulation is consistent with the design bases established for in-vessel retention of a damaged core. COL Information Item 5.3-4 requires a structural analysis of the AP1000 reactor vessel insulation and support structure. TR-24 reports relevant results of that analysis.

The effectiveness of external reactor vessel cooling in the AP1000 design depends, in part, on a reactor vessel insulation system that provides an engineered pathway for supplying water cooling to the vessel exterior and venting steam from the reactor cavity during severe accidents. It is designed to limit thermal losses during normal operations. Section 5.3 of this report documents this design, which is discussed in Section 19.1.8.24 and evaluated in Section 19.2.3.3.1.3.2.

The staff noted that some paints and coatings used to protect the reactor vessel during shipping could have detrimental effects on CHF performance (RAI-TR24-SPLA-06). In APP-GW-GLN-106, Revision 1 (TR-106), the applicant stated that the external surface of the reactor vessel is bare metal. AP1000 DCD Section 5.3.4.5 now reflects the fact that a temporary protective coating applied before shipment will protect carbon steel surfaces. In DCD Section 19.34.2.1, the applicant stated that the vessel will have no coatings on the outside surface of the reactor vessel. This ensures that wettability of the surface will not be inhibited and CHF performance will not be degraded; the staff finds this acceptable. The COL holder must remove these temporary coatings. The staff requested additional basis for confidence that this will be accomplished.

In a letter from R. Sisk dated April 14, 2009, the applicant clarified the nature of the protective covering, which is to be an industrial form of shrink wrap that will be removed in the receiving process. The staff agrees that no additional controls are required; the statement in DCD Section 19.34.2.1 is sufficient and RAI-TR24-SPLA-06 is resolved.

19.1.2.3 Residual Risk from Changes Not Explicitly Modeled

The applicant reviewed all design changes for their potential to affect risk. APP-PRA-GER-001 (TR-135) documented the process used for this review as well as the results of that process. The staff noted that, if a design change proposal (DCP) dealt with an SSC modeled in the PRA, the applicant evaluated its potential to affect the PRA results. However, the applicant did not necessarily evaluate other changes that may have an impact (e.g., changes to assumptions or PRA insights, as well as changes to model logic or changes that may alter probabilistic parameter estimates). For example, a new or revised operating procedure might alter, for some modes, the alignment of an SSC in a manner that is inconsistent with documented insights or assumptions. The equipment would then require realignment to prevent or mitigate the consequences of an event applicable to the mode in question. The staff identified the specific example of vacuum fill operation (RAI-SRP19.0-SPLA-05).

It may be appropriate to model a different basic event (and/or supporting SSCs) in the PRA model for that mode. Alternatively, additional constraints or conditions to control risk may be appropriate before initiating the proposed procedure. The staff expects an evaluation to be performed, even if it will usually result in a determination that no explicit model change or procedural constraint is necessary.

The staff asked the applicant to describe each DCP incorporated in the amended design and assess its potential impact on the PRA. For each DCP that may have an impact on the PRA or other risk studies (e.g., seismic and internal fire), the staff asked the applicant to evaluate and report its potential significance (RAI-SRP19.0-SPLA-05).

In a letter from R. Sisk to the NRC dated August 21, 2008 (DCP/NRC2233), the applicant provided the results of its evaluation of the vacuum fill operation. In addition, the applicant reported that it made a change in the process used for future DCPs. The staff reviewed each one for its impact on the PRA, with no initial screening for PRA-modeled SSCs. This effort included a documented review of the PRA assumptions and PRA insights affected, potential changes to model logic and probability data, the effect of operational changes on component modeling, and the impact on other risk studies (e.g., seismic and internal fire). The documentation of the review identifies and briefly describes every DCP and provides the rationale used to determine its impact on the plant risk and changes to the PRA or other risk studies (e.g., seismic and internal fire).

The staff concludes that the Westinghouse performed an appropriate evaluation of the risk implications of vacuum fill operations and that the design change process will provide adequate assurance that the risk implications of all changes after Revision 17 of the DCD will be assessed. In a letter from R. Sisk dated April 23, 2009, Westinghouse provided a schedule for re-evaluation (using the revised criteria) of all DCPs processed to date: changes reflected in Revision 17 of the DCD will be re-evaluated first and re-evaluation of all earlier changes documented prior to initial fuel loading. The results will be reflected in the plant-specific PRA as upgraded and updated prior to initial fuel load. The COL holder is responsible for these updates as part of COL Information Item 19.59.10-2. The staff finds that this provides adequate assurance that the risk implications of all changes will be appropriately assessed and, if necessary, analyzed. This is an acceptable method for controlling residual risk from changes that are not explicitly modeled.

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

Safety insights from the internal events Level 1 PRA include the following:

- dominant accident sequences contributing to CDF
- areas in which certain AP1000 design passive and defense-in-depth features were the most effective in reducing risk as compared to currently operating reactor designs
- major contributors to the estimated CDF from internal events, such as hardware failures, system unavailabilities, and human errors
- major contributors to maintaining the built-in plant safety (to ensure that risk does not increase unacceptably)

- major contributors to the uncertainty associated with the estimated CDF

- sensitivity of the estimated CDF from internal events to (1) potential biases in numerical values, (2) assumptions made, (3) lack of modeling details in certain areas, and (4) previously raised safety issues

Safety insights from the internal events Level 2 PRA include the following:

- core damage sequences and accident classes contributing to containment failure
- frequency and conditional probability of containment failure
- leading contributors to containment failure and risk

19.1.3.1 Level 1 Internal Events Probabilistic Risk Assessment

In APP-GW-GLR-102 (TR-102), the applicant described the results of the PRA that it had upgraded and updated to conform to the amended design.

The staff conducted an audit of the PRA model upgrade and update. The staff reviewed the qualification of the PRA staff, procedures used for conversion, and processes for updating the PRA. In addition, the staff examined the PRA model itself with emphasis on new fault trees developed for I&C systems. Chapter 7 of this report documents the staff's review of I&C system design changes. The staff also reviewed the electrical system model changes for consistency with APP-GW-GLN-079, Revision 1, "Electrical System Design Changes" (TR-79). Chapter 8 of this report documents the staff's review of electrical system design changes.

The staff found that the development of the I&C model was consistent with the amended I&C design, as described in APP-GW-GLN-004, "Instrumentation and Control Design Change" (TR-39); APP-GW-GLR-071, "AP1000 Protection and Safety Monitoring System Architecture Technical Report" (WCAP-16675-NP); APP-GW-GLR-018, "Failure Modes and Effects Analysis and Software Hazards Analysis for AP1000 Protection System"; and APP-GW-GLN-022, Revision 1 (TR-97). APP-GW-GLR-080, "Mark-up of AP1000 Design Control Document Chapter 7" (TR-80), documents the impact of these design changes on the DCD. Chapter 7 of this report documents the staff's review of the I&C design changes themselves. (Note that many of the design changes had no impact on the PRA and therefore no impact on the severe accident analysis, as documented in TR-102 and TR-135.)

In a letter from R. Sisk to the NRC dated November 6, 2008 (DCP/NRC2284), the applicant reported some results of the PRA model requantification. The applicant estimated the mean CDF for the AP1000 design from internal events during operation at power to be about 2.41×10^{-7} per year, unchanged from what the previous PRA reported. The applicant characterized this as equivalent, given appropriate treatment of uncertainties.

Although the applicant did not modify the initiating event frequencies in the model, the contribution of each initiating event to CDF changed slightly. The applicant reported that these changes were associated with the I&C model revision and updated electrical power dependencies. The applicant's assessment suggested that the changes were not of sufficient magnitude to alter the risk insights derived from the PRA results. For example, the top 10 cutsets were identical, and the CDF attributable to failure of the most risk-significant system (the PMS) changed (i.e., it became less risk significant) by only a small factor (less than 2).

Various LOCA categories of initiating events continue to dominate the CDF profile (about 85 percent), followed by reactor vessel rupture (about 4 percent) and transient events (about 4 percent). Contributions from steam generator tube rupture (SGTR) events are slightly higher (about 4 percent), while ATWS sequences and loss of offsite power/station blackout events contribute even less than before (less than 1 percent).

Based on these results and the audit that provided confidence in the model upgrade and update process, the staff finds that the amended Level 1 internal events PRA at power did not change significantly. The staff finds that a plant-specific PRA report that is identical to the PRA for the certified design continues to provide an acceptable basis for risk insights and assumptions related to internal events.

However, changes to the design have altered some of the insights derived from the PRA (e.g. improving the design by eliminating a risk-significant SSC). The staff requested the results of resolving and requantifying the baseline and RTNSS full-power PRA, shutdown PRA, and external events PRA, as well as the results of the revised importance analyses. In a letter from R. Sisk to the NRC dated August 21, 2008 (DCP/NRC2233), the applicant committed to resolving and requantifying the model after making some corrections. In a revised response dated November 6, 2008 (DCP/NRC 2284), the applicant altered this commitment, as discussed in Section 19.1.2.1.10, above, where it is identified as Open Item OI-SRP19.0-SPLA-07.

19.1.3.2.3.3 Human Actions

In APP-GW-GL-011 (WCAP-16555), the applicant reviewed human actions with respect to risk achievement worth (RAW) and risk reduction worth (RRW). In addition, Westinghouse reviewed human actions required for maintenance, test, inspection, and surveillance (MTIS) support. The applicant stated that, on a deterministic basis, no human actions were required to mitigate design-basis accidents (DBAs) or to prevent core damage following a DBA.

The applicant also identified 19 human actions as most significant from a probabilistic standpoint, though none of them came within an order of magnitude of the criteria previously accepted for a “critical” human action. The applicant added the following three human actions because an expert panel considered them to be significant:

(1) Failure to recognize the need for and failure to isolate the RNS system, given rupture of the RNS piping when the plant is at hot/cold conditions (RHN-MAN04). The applicant added this action because of the short time available for the operator to act and the conflicting goals (maintaining core cooling by the RNS versus isolating a leak or break in the RNS piping).

(2) Failure to recognize the need for and failure to actuate the hydrogen control system, given core damage following a LOCA (VLN-MAN01). The applicant added this action because its limiting RAW is relatively close to the criteria, and it is a function within the scope of RTNSS.

(3) Failure to close equipment hatch and personnel airlocks following core damage during a shutdown event. The applicant added this action because human action importance could not be calculated for shutdown, internal events, or LRF. The expert panel considered that, under these conditions, the largest risk of large release would come

from failure to close the containment. Closing the containment under these conditions involves closing the equipment hatch, personnel hatches, and temporary penetrations.

As noted by the staff, DCD Table 19.59-18 documents that "the ability to close containment hatches and penetrations during Modes 5 and 6 prior to steaming to containment is important." There is a commitment for procedures and training to ensure that this action will be taken when required.

The staff found that the results were consistent with the methodology prescribed for the certified design and that the applicant conservatively identified risk-important human actions. For these reasons, the staff finds the results to be consistent with the SRP and therefore acceptable.

19.1.3.3.3 Important Insights from Level 3 PRA and Supporting Sensitivity Analyses

The applicant deleted discussion of Level 3 PRA from Tier 2. The Level 3 PRA is now described only in the environmental assessment.

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

19.1.4.1 Level 1 Shutdown Internal Events Probabilistic Risk Assessment

The staff compared the results of the shutdown PRA, as seen in the current model, with the results reported in Revision 16 of the DCD (unchanged in Revision 17). Many of the results significantly differ from those reported in DCD Section 19.59.5.1, "Summary of Shutdown Level 1 Results." For example, Section 19.59.5.1 discusses the dominant sequences and key contributors to risk. The staff compared this documentation to the top 15 cutsets and the top 20 component basic events ranked by RAW from the CAFTA results. Loss of component cooling (supplied by the circulating water system (CWS)) or service water (supplied by the service water system) during drained conditions contributes at least 73 percent to the CDF, as seen in the CAFTA results, versus 64 percent as reported in the DCD. Loss of the RNS initiating event during drained conditions contributes at least 10 percent to the CDF as compared to 6 percent reported in the DCD. Inadvertent draining through valve V024 (IEV-LOCA24ND) contributes more to the CDF than the risk of RCS overdraining, as seen in the CAFTA results. However, the DCD does not report this event. Some of these changes appear to meet the importance criteria of COL/DC-ISG-3 and so they should be documented.

The staff asked the applicant to update DCD Table 19.59-15, "Summary of AP1000 Results," and to provide the following information:

(1) a list of cutsets for the AP1000 shutdown PRA that contribute to 95 percent of total shutdown CDF and any that contribute as much as 1 percent of total shutdown CDF

(2) a list of all SSCs in the shutdown PRA and their RAWs (if RAW greater than 2)

(3) a list of all human actions modeled in the shutdown PRA and their RAWs

(4) a list of all CCFs in the shutdown PRA and their RAWs (if RAW greater than 2) or confirmation that WCAP-16555 describes them all

In a letter from R. Sisk to the NRC dated August 21, 2008 (DCP/NRC2233), the applicant stated that the next revision of TR-102 will include the PRA model changes discussed in RAI-SRP19.0-SPLA-13. The staff will evaluate the statement in TR-102 that the internal events, evaluations, conclusions, and insights in AP1000 DCD Chapter 19 remain representative of the AP1000 design with the next revision of that report. In a subsequent letter from R. Sisk to the NRC dated November 6, 2008 (DCP/NRC2284), the applicant stated that it would revise TR-102 but proposed no changes to the DCD. The NRC staff identified this as the first part of Open Item OI-SRP19.0-SPLA-13.

19.1.4.2 Dominant Accident Sequences Leading to Core Damage

The staff asked the applicant to confirm that the list of major contributors to risk for each sequence that contributes more than 1 percent to the shutdown CDF remains consistent with the cutset results and to revise the DCD as necessary to describe all such sequences (RAI-SRP19.0-SPLA-13).

In a letter from R. Sisk to the NRC dated August 21, 2008 (DCP/NRC2233), the applicant stated that the next revision of TR-102 will include the PRA model changes discussed in this RAI. The staff will evaluate the statement in TR-102 that the internal events, evaluations, conclusions, and insights in the AP1000 DCD Chapter 19 remain representative of the AP1000 design with the next revision of that report. In a subsequent letter from R. Sisk to the NRC dated November 6, 2008 (DCP/NRC2284), the applicant stated that it would revise TR-102 but proposed no changes to the DCD. The NRC staff identified this as the second part of Open Item OI-SRP19.0-SPLA-13.

19.1.4.3 Risk-Important Design Features

The applicant now describes actuation of IRWST injection as the result of a fourth-stage automatic depressurization system (ADS) signal rather than a low hot-leg level signal. The staff asked the applicant to clarify the impact of this modification on the shutdown risk assessment (RAI-SRP19.0-SPLA-04).

The applicant responded that it had modified the logic description in the DCD to represent more clearly how the system is intended to function.

Appendix 19E to DCD Revision 15 described the logic in the AP1000 as follows:

- actuation of IRWST injection on low (empty) hot-leg level on a two-out-of-two basis (RCS hot-leg level channel basis)

- actuation of fourth-stage ADS valves on low (empty) hot-leg level on a two-out-of-two basis (RCS hot-leg level channel basis)

The DCD provides the following revised description:

- actuation of fourth-stage ADS valves on low (empty) hot-leg level on a two-out-of-two basis (RCS hot-leg level channel basis)

- actuation of fourth-stage ADS causes actuation of IRWST injection

This logic configuration forms the basis for the PRA model and shutdown risk assessment. The change in wording for the logic for actuation of IRWST injection has no impact on the results and insights of the shutdown risk assessment.

The staff agrees that the clarification did not alter the functional response of the system and confirmed that the change in description did not affect shutdown PRA insights.

COL Information Item 18.7-1 includes the following statement:

> Since inadvertent opening of RNS valve V024 results in a draindown of RCS inventory to the IRWST and requires gravity injection from the IRWST, the COL applicant will have administrative controls to ensure that inadvertent opening of this valve is unlikely. The control room design will take into account this error.

The staff requested information on the features of the control room design that will ensure that inadvertent opening of valve V024 is unlikely (RAI-19.0-SPLA-09).

In a letter from R. Sisk to the NRC dated August 21, 2008 (DCP/NRC2233), the applicant responded that, during shutdown, electrical power to valve V024 is blocked (breakers open and manually locked out) when RNS is in operation. This prevents inadvertent operation when the RCS would be depressurized. (ADS valves are open during shutdown conditions in accordance with Technical Specification 3.4.13.)

A permissive signal (valves V001A/B and V002A/B are fully closed and valve V023 is open) is required to permit manual opening of this valve V024. DCD Figure 7.2-1 shows a corresponding interlock to open the RNS hot-leg suction isolation valves, which is prevented if the IRWST cross-connects to the RNS (valves V023 and V024) are not fully closed.

The staff finds this to be an acceptable method of ensuring that inadvertent opening of valve V024 is unlikely and considers this portion of COL Information Item 18.7-1 to be closed.

19.1.4.3.2 Loss-of-Coolant Accidents during Safe Shutdown or Cold Shutdown or Both with the Reactor Coolant System Intact

Westinghouse modified the containment recirculation design to provide large, interconnected screens without separate trash racks or coarse and fine screens. Section 6.3 of this report documents the staff's assessment of this change. The staff asked the applicant to clarify the impact of this modification on the shutdown risk assessment (RAI-SRP19.0-SPLA-04).

The DCD reflects the use of large, interconnected recirculation screens for recirculation flow. The passive core cooling system (PXS) has two banks of interconnected screens that filter recirculation flow. The staff evaluated these screens using the guidance in RG 1.82, Revision 3, "Water Sources for Long-Term Recirculation Cooling Following a Loss-of-Coolant Accident," issued November 2003. The screens are constructed of perforated stainless steel plate that is used to form pockets. The structural integrity of this configuration is well in excess of the screen-like material that was typically used in PWR sump screens before actions were taken to close Generic Safety Issue (GSI)-191, "Experimental Studies of Loss-of-Coolant-Accident-Generated Debris Accumulation and Head Loss with Emphasis on the Effects of Calcium Silicate Insulation," issued May 2005, and respond to Generic Letter (GL) 2004-02, "Potential

Impact of Debris Blockage on Emergency Recirculation during Design Basis Accidents at Pressurized-Water Reactors," dated September 13, 2004. As is the case with current operating plants, the structural integrity of the API000 screens precludes the need for trash racks. APP-GW-GLN-147 (TR-147) also discusses the design of the AP1000 screens. Section 6.3 of this report documents the staff's evaluation of the screens.

The applicant judged the changes in the screen design to have no negative impact to the PRA; thus, it did not change the DCD PRA to reflect the screen changes. Instead, the applicant judged these changes to have a positive impact to the PRA resulting from a lower failure probability of the screens because of the enhanced design and increased flow area. The DCD PRA did not credit this change in failure probability; therefore, the applicant did not change the shutdown risk assessment as a result of the change in screen design.

The staff confirmed that the PRA appropriately modeled the CCF of the screens. For the design certification amendment, the modeling is conservative and therefore acceptable to the staff.

19.1.4.3.6 Loss of the Normal Residual Heat Removal System (due to Loss-of-Coolant Accidents) or Loss of the Normal Residual Heat Removal System or Its Support Systems during Reactor Coolant System Open Conditions

When the RCS is open, the importance of the RNS is higher than at other times because safety-related heat removal paths may not be available. An external event (high winds) can have an impact on alternating current power sources required for RNS function because those sources (and their fuel) are not protected by safety-related structures. In addition, if the RNS becomes unavailable, the containment must be closed before boiling begins in the RCS.

The staff asked the applicant to evaluate high winds while in MODE 5 and MODE 6 explicitly or to provide an acceptable basis for screening such events from consideration. The associated risks should be quantified and possibly controlled. The NRC staff identified this as Open Item OI-SRP 19.0-SPLA-18.

19.1.5 Safety Insights from the External Events Risk Analysis

Three sections of the AP1000 DCD address PRA of external events consistent with DCD Section 1.9.5.2.14:

(1) A risk-based seismic margin analysis (SMA), documented in DCD Section 19.55 and Appendix 19A, both titled "Seismic Margin Analysis," addresses seismic events. Sections 19.1.5.1 and 19A of this report document the staff's evaluation of the SMA.

(2) APP-GW-GL-022, "AP1000 Probabilistic Risk Assessment," Revision 8, Chapter 57, "Fire Risk Assessment," documents analysis of the risk associated with internal fires. (The analysis is not discussed in this supplement because it has not changed since initial certification of the AP1000 design.)

(3) DCD Section 19.58, "Winds, Floods, and Other External Events," addresses remaining external events. Sections 19.1.5.4 through 19.1.5.7 of this report document the staff's evaluation.

The objectives of the external events risk analysis provided in Section 19.58 of the AP1000 DCD are threefold:

(1) Determine screening criteria and identify potential external events that may affect the AP1000 risk on a site-specific basis.

(2) Provide generic risk analyses, based on bounding assumptions regarding site-specific parameters (e.g., frequency of each category of hurricanes) for relevant external events.

(3) Provide guidance to COL applicants regarding the verification of the applicability of these generic analyses to a specific site.

The AP1000 DCD addresses those external initiating events or external hazards whose causes are external to the plant, other than seismic events. Based on the modified individual plant examinations of external events (IPEEE) guidelines, DCD Section 19.58 discusses the following external events or external hazards:

- high winds (including tornadoes)
- external floods
- external fires
- transportation and nearby facility accidents

The scope of this analysis does not include sabotage, which is consistent with the SRP and therefore acceptable to the staff. The information provided in DCD Section 19.58 is based primarily on the following:

- NRC guidance for the preparation and submittal of IPEEE for operating nuclear power plants

- the AP1000 design certification PRA

- site-specific information related to external events for several proposed sites to build a nuclear plant referencing the AP1000 design

On June 28, 1991, the NRC issued Supplement 4 to GL 88-20, “Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities,” requesting that each licensee conduct an IPEEE. NUREG-1407, “Procedural and Submittal Guidance for the Individual Plant Examination of External Events for Severe Accident Vulnerabilities,” documents NRC guidelines for conducting IPEEE and on the structure and content of the IPEEE submittal. The staff examined these guidelines to verify their applicability to new reactor licensing and to investigate their completeness. The staff concludes that the IPEEE guidelines are applicable to the COL process after they are properly modified as follows:

- The IPEEE, performed by operating reactor licensees, takes into account plant-specific licensing information regarding external hazards that is not necessarily available to a COL applicant. For example, NUREG-1407 states, “[the] effects of external fires, other than loss of offsite power (LOSP), have been evaluated during the operating license (OL) review against sufficiently conservative criteria.” Thus, the assumptions made in NUREG-1407 (e.g., in deriving the list of external events to be included in the IPEEE

submittal) must be examined to determine whether a COL applicant must address events that were not included in the DCD.

- The baseline risks of the AP1000 design, as assessed in the design certification PRA, are lower than the corresponding risks of an average operating plant. At operating reactors, the combined CDF for external events may be of the same magnitude as CDF for internal events. For this reason, the criteria for screening out external events from the quantitative evaluation must be properly adjusted to maintain the conclusion reached in the design certification—that the AP1000 design represents a reduction in risk compared to existing plants.

Westinghouse gathered site-specific external events information from utilities interested in the AP1000 design and performed a generic analysis for each external event, based on the most limiting parameters from any site. In APP-GW-GLR-101 (TR-101), the applicant identified potential external events that may affect the AP1000 risk.

The staff finds that these external hazards are most likely a complete list of external events associated with candidate sites for an AP1000 plant as of the date of this SER. The staff evaluated the analysis of the AP1000 response to external events according to the SRP, which states that the applicant's analyses should be "comprehensive in scope and address all applicable...external events and all plant operating modes." The staff requested additional information in RAI-TR101-SPLA-01 through RAI-TR101-SPLA-08 to clarify the report. In a letter from A. Sterdis to the NRC dated October 19, 2007 (DCP/NRC2026), the applicant responded. The staff requested additional clarification on RAI-TR101-SPLA-03 (external fires) and RAI-TR101-SPLA-06 (external flooding), which was provided in a letter from A. Sterdis to the NRC dated February 8, 2008 (DCP/NRC2084).

The applicant added consideration of external fires to the external events PRA and provided additional information on flooding caused by storm surge.

The methods used by the applicant to analyze external hazards, as documented in TR-101 and described in the DCD, is consistent with RG 1.200. Therefore, the external events analysis is acceptable to the staff given the input parameters used. There are two exceptions. First, the analysis neither included an explicit discussion of the release of hazardous materials from nearby facilities (other than pipelines) nor identified this issue as a COL information item. The staff is concerned that some toxic materials are immediately dangerous to life and health at concentrations lower than the materials evaluated for pipelines, and some may not be readily detected. In RAI-SRP19.0-SPLA-17, the staff requested an assessment of risk from the release of toxic materials and a basis for a COL applicant to confirm that the assessment bounds the risk at the proposed site.

In a letter from R. Sisk dated March 9, 2009, the applicant addressed the release of hazardous materials from nearby facilities and provided justification for screening of toxic releases from further analysis. The applicant stated that no operator action was credited, obviating the need to evaluate specific toxic release events with respect to type and amount of material released. The result of the analysis was a conditional core damage probability of 6.26×10^{-8}. From this, a limiting event frequency was provided for COL applicants to use to confirm that the generic analysis is applicable to their proposed sites. The applicant identified several conservatisms in this analysis. In addition to the assumption that operators were immediately and completely unable to perform any

protective or mitigating actions, design features that assure control room habitability for 72 hours under nearly all circumstances were not credited.

In the same response, the applicant clarified the basis for using an initiating event frequency of 1×10^{-6} for the analysis of marine explosions, confirming that screening of the event was based on a negligible contribution to core damage frequency so long as the criteria of RG 1.91 are met.

The NRC staff agrees that there is considerable conservatism in the analysis of toxic gas release events that was described, and finds that it provides an acceptable basis for screening such events from further risk assessment. The limiting event frequency for toxic releases provided in the DCD provides an appropriate basis for COL applicants to confirm that this analysis bounds conditions where they propose to build a plant that references the AP1000 certified design. The staff considers the description of external events from transportation and nearby facility accidents to be complete and RAI-SRP19.0-SPLA-17 is resolved.

Second, the applicant did not address the case of high winds while in MODE 5 and MODE 6. This scenario should be screened from consideration or the associated risks quantified and possibly controlled. The staff requested that the applicant address this concern in RAI-SRP19.0-SPLA-18.

In a letter from R. Sisk dated March 26, 2009, the applicant addressed high wind events occurring in MODES 5 and 6. The applicant stated that emergency response requirements or emergency action levels will require that the RCS be taken out of mid-loop operation and prohibit entry when a potentially severe high wind event is anticipated. In addition, the response describes how core cooling is accomplished if diesel generators are not available.

The staff finds that the proposed measures are appropriate and sufficient to justify screening high wind events during MODES 5 and 6 from further analysis. The staff considers RAI-SRP19.0-SPLA-18 to be resolved.

The COL applicant must verify that the generic analysis for each external event bounds conditions at the proposed site.

DCD Section 2.2 requires a COL applicant to identify design changes in its safety analysis report if the occurrence of a safety hazard is $1x10^{-6}$ per year or greater. Accordingly, the COL applicant should assess the risk associated with any safety hazards that do not meet the criteria for being screened from further evaluation. In addition, the license holder must reevaluate the external event risk when a site-specific, plant-specific PRA is available.

The criteria for screening out external events from the quantitative evaluation are adjusted to maintain (for a plant referencing the AP1000 design) the conclusion reached in the design certification—that the AP1000 design represents a reduction in risk compared to existing plants. The AP1000 DCD uses the following criteria with respect to risk evaluation of external events or hazards:

- An event or hazard with frequency less than $1x10^{-7}$ per year is screened out from the evaluation.

- An event or hazard with frequency of $1x10^{-7}$ per year or higher is screened out from the evaluation if a qualitative or bounding analysis shows that the associated CDF is less than $1x10^{-8}$ per year.

- An event or hazard with frequency of $1x10^{-7}$ per year or higher is considered for further detailed analysis if it cannot be shown that the associated CDF is less than $1x10^{-8}$ per year.

Each COLA must confirm that the high winds, floods, and other external events analysis documented in the DCD are applicable to the site for which the COLA is submitted (i.e., the spectrum of events at the site is bounded by the events analyzed in the DCD). Chapter 19 of the final safety analysis report (FSAR) should document this applicability evaluation. Further evaluation will be required if any unbounded, site-specific susceptibilities are found.

The NRC requires, where applicable to the site, that the COL applicant perform a site-specific, PRA-based analysis of external flooding, hurricanes, or other external events pertinent to the site to reveal any site-specific vulnerabilities. It is sufficient for the COL applicant to provide the basis for a conclusion that, for the proposed site, a particular external event is no more frequent and no more severe than that same event as modeled for the certified design. The COL applicant must develop plant-specific and site-specific risk information before loading fuel. This is part of COL Information Item 19.59.10-2.

In addition, the PRA used to support the AP1000 design certification will be updated, as necessary, when site-specific and plant-specific (as-built) data become available. The staff will review differences between the as-built plant and the design used as the basis for the AP1000 PRA to determine whether the PRA results are significantly impacted. The staff will place special emphasis on areas of the design that either were not part of the certified design or were not detailed in the certification. This is part of COL Information Item 19.59.10-2.

The staff also asked the applicant to clarify how SSCs are designed to withstand the effects of flooding (RAI-SRP19.0-SPLA-02). In the same letter, the applicant responded that the AP1000 is protected against floods up to the 100-foot level. The 100-foot level corresponds to the plant ground level. From this point, the ground is graded so that water will naturally flow away from the structures. Additionally, all seismic Category I SSCs below grade (below ground level) are designed to withstand hydrostatic pressures, and they are protected against flooding by a water barrier consisting of waterstops and a waterproofing system.

The staff finds that the design of safety-related SSCs below the 100-foot level provides adequate protection from the effects of external flooding. Section 3.4 of this report discusses the staff's evaluation of internal flooding.

The COL applicant referencing the AP1000 certified design is responsible for (1) confirming in the COLA that the information provided in Section 19.58 of the DCD is applicable to the selected site and (2) addressing all site-specific action items discussed in Section 19.58 of the DCD.

The staff concluded that the methods used in the AP1000 PRA to evaluate external events provide the insights necessary to determine whether any design or procedural vulnerabilities exist for these external events. The staff finds that, for the events specified in the DCD, the

reported results are acceptable. However, the applicant must still address the case of high winds while in a shutdown mode. The NRC staff has identified this as Open Item OI-SRP19.0-SPLA-18. These methods provide insights needed for design certification requirements, such as ITAAC.

19.1.5.1 Probabilistic-Risk-Assessment-Based Seismic Margin Analysis

The seismic analysis and design of the AP1000 plant is based on the certified seismic design response spectra (CSDRS) shown in DCD Tier 1, Figures 1.0-1 and 1.0-2. The CSDRS are based on RG 1.60, "Design Response Spectra for Seismic Design of Nuclear Power Plants," with an enhanced spectral acceleration in the 25-hertz (Hz) region. Its dominant energy content is in the frequency range of 2 to 10 Hz.

AP1000 SSCs are designed to remain functional when subjected to 0.3g vibratory ground motion. Since certification, the applicant presented seismic analysis of the AP1000 nuclear island using a hard-rock high-frequency (HRHF) spectrum that envelops three particular sites in the Central and Eastern United States (CEUS) in APP-GW-GLR-115, "Effect of High-Frequency Seismic Content on SSCs" (TR-115). In addition to the results of these linear-elastic analyses, the applicant suggested that nonlinear features of the plant design would have the effect of filtering high-frequency vibration. This would limit high-frequency demands on SSCs. TR-115 also provides supplemental criteria for selection and testing of equipment whose function might be sensitive to high-frequency acceleration. Chapter 3.7 of this report discusses the staff's review of the seismic design.

Based on the acceptability of the seismic design and supplemental criteria for potentially susceptible equipment, the applicant stated that the conclusions of the PRA-based SMA are unchanged.

The AP1000 SMA estimated the high confidence, low probability of failures (HCLPF) capacity of the AP1000 plant in terms of a minimum peak ground acceleration value of 0.5 g, based on a Commission position. Specifically, in a staff requirements memorandum dated July 21, 1993, the Commission approved the following staff recommendation specified in Section II.N, "Site Specific Probabilistic Risk Assessments and Analysis of External Events" of SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," with a modification:

> PRA insights will be used to support a margins type assessment of seismic events. A PRA based seismic margins analysis will consider sequence level HCLPFs and fragilities for all sequences leading to core damage or containment failures up to approximately one and two thirds the ground motion acceleration of the design-basis safe shutdown earthquake (SSE).

The applicant established a review-level earthquake equal to 0.5 g for the SMA and used it to demonstrate a margin over the SSE of 0.3 g.

For new sites, the ground motion response spectra (GMRS) are obtained from site-specific probabilistic hazard-based ground motion. Many of the GMRS of the CEUS rock sites show higher amplitude at higher frequency than the CSDRS. For this reason, an HRHF spectrum has been developed that envelops three hard rock sites for which COLAs using the AP1000 as the vendor design are being prepared. DCD Figures 1.0-1 and 1.0-2 compare the HRHF at

foundation level against the AP1000 CSDRS for both the horizontal and vertical directions for 5-percent damping. The HRHF exceeds the CSDRS for a range of frequencies above about 15 Hz.

In APP-GW-GLR-115 (TR-115), the applicant evaluated representative SSCs that have been selected by screening as potentially sensitive to high-frequency input in locations where the GMRS demonstrated an exceedance (magnitude greater than the CSDRS) in the high-frequency region.

In APP-GW-GLN-144, "AP1000 Design Control Document High Frequency Seismic Tier 1 Changes" (TR-144), the applicant stated that additional equipment dynamic qualification effort beyond the seismic design bases for operating nuclear power plants to address high-frequency response effects is not warranted. However, the applicant noted that the effect of high-frequency input on potentially sensitive active components requires additional consideration.

Section 3.7 of this report discusses the staff evaluation of the seismic design. The staff requested the basis for the SMA of plants at hard rock sites, given that the SSE is now considered the HRHF GMRS (RAI-SRP19.0-SPLA-12).

In TR-144, the applicant concluded that, for structures, the HRHF loads will not govern the design. For the primary component supports and reactor coolant loop nozzles, seismic loads from the CSDRS enveloped those from the high-frequency input. Consequently, the staff considered these items to be acceptable seismic design for the HRHF input. For piping systems, the applicant concluded that the results of the HRHF seismic analysis are bounded by the stress results of the AP1000 CSDRS seismic analysis. For safety-related electrical equipment, the applicant concluded that the qualification methodology (analytical evaluations and testing procedures) currently employed generally leads to a more conservative design than that resulting from the HRHF spectra. Supplemental seismic testing of high-frequency-sensitive safety-related equipment or implementation of one of the other high-frequency screening techniques may be required to demonstrate acceptability under HRHF seismic demand conditions.

For structures, primary component supports, and reactor coolant loop nozzles, as well as piping systems, the applicant has demonstrated that, for the range of frequencies relevant to these SSCs, seismic loads are enveloped by CSDRS. This provides a sufficient basis for the staff to conclude that the seismic margins for these SSCs are acceptable.

However, for high-frequency-sensitive safety-related equipment, the staff cannot conclude that the applicant has demonstrated adequate seismic margin, given the higher amplitude of high-frequency components of the GMRS. Although safety-related equipment that exhibits natural frequencies within the HRHF exceedance range will be subject to supplemental high-frequency seismic evaluation to confirm an acceptable seismic design, the applicant must clarify the basis for confirming that seismic margin is adequate.

The previously certified design identified HCLPF at the sequence level using a minimum-maximum approach. The applicant should document confirmation that an acceptable seismic margin is maintained for HRHF sites using this method or an alternative that is adequately justified. The NRC staff identified this as Open Item OI-SRP19.0-SPLA-12.

19.1.5.4 High Winds Evaluation

High winds can affect plant structures in two ways: (1) structures can collapse or overturn from the excessive loading when wind forces exceed the load capacity of the structure and (2) lifting

and thrusting can cause materials to act as missiles against plant structures that house safety-related equipment. In addition, the applicant investigated the potential for debris generated by high winds clogging the drains to block the passive containment cooling system (PCS) air baffle.

The AP1000 structures protecting safety-related features are designed to withstand winds of up to 300 miles per hour (mph), as well as missiles generated by these winds (see design-basis wind speed discussed in Chapter 2 of the DCD). Also, the AP1000 operating basis wind speed is 145 mph, as discussed in Chapter 2 of the DCD. In general, there is some margin above the design and operating bases that the risk evaluation of high winds neither assesses nor credits. The applicant made the following assumptions in evaluating the risk from high winds:

- Safety-related structures, which house safety-related equipment, are not impacted by high winds of any kind (tornados and hurricanes, including extra-tropical cyclones) if the wind speed does not exceed 300 mph.

- Non-safety-related structures, which are designed and built according to uniform building code and house non-safety-related defense-in-depth or investment protection equipment, are not impacted by high winds of any kind (tornados and hurricanes, including extra-tropical cyclones) if the wind speed does not exceed 145 mph.

- High-wind events exceeding 300 mph are extremely rare events with a frequency of less than $1x10^{-7}$ per year; therefore, they are screened out from the risk analysis based on the screening criteria discussed in Section 19.1.5, above . The COL applicant referencing the AP1000 design must verify this assumption.

Westinghouse states in DCD Section 19.58.2.1 that no tornados or hurricanes are expected to reach 300 mph winds per the enhanced Fujita scale for tornados and the Saffir-Simpson scale for hurricanes. Though the staff does not assign an upper wind speed limit to these scales, the conclusion is consistent with the staff's position documented in RG 1.76, "Design-Basis Tornado and Tornado Missiles for Nuclear Power Plants," Revision 1 (RG 1.76). For the continental United States, the staff considers the highest tornado wind speed with a frequency of $1x10^{-7}$ to be 230 mph. AP1000 safety-related structures are designed to withstand winds of 300 mph. Clearly, the expected frequency of 300 mph tornadoes is significantly lower. For plants that are to be sited in the continental U.S., such events may be screened from further analysis.

Based on these assumptions, the applicant performed generic risk evaluations using initiating event frequencies that it described as "bounding." Six tornado event categories (defined in Table 19.58-1 of the DCD, which describes the enhanced Fujita scale for tornados) and five hurricane event categories (defined in Table 19.58-2 of the DCD, which describes the Saffir-Simpson scale for hurricanes) were evaluated. In addition, the applicant considered extra-tropical cyclones as a single category of high winds. Extra-tropical cyclones are normal storms and thunderstorms with winds expected to fall below the operating basis of 145 mph. The analysis assumed a bounding frequency of extra-tropical cyclones equal to $3x10^{-2}$ per year. COL applicants referencing the AP1000 design must verify that the frequency of each of the 12 high wind categories at the proposed site is bounded by the frequency assumed in Section 19.58 of the AP1000 DCD.

High winds cannot be screened out from the evaluation using the initiating event frequency criterion because the assumed frequency of high winds is greater than $1x10^{-7}$ per year.

However, bounding risk assessments have shown that the CDF associated with high winds is less than the criterion of $1x10^{-8}$ per year. Therefore, the applicant did not perform detailed risk assessments for high winds. Westinghouse did perform risk assessments for three cases—a baseline case and two sensitivity cases:

- The baseline case assumes two kinds of failures: (1) an unrecoverable LOSP event for all 12 high wind categories since the site switchyard is unprotected, and (2) failure of all non-safety-related structures for three categories of tornados (designated as EF3, EF4, and EF5 in Table 19.58-1 of the DCD) and three categories of hurricanes (designated as Category 3, 4, and 5 in Table 19.58-2 of the DCD) which exceed the operating basis of 145-mph winds that could impact non-safety-related structures. The applicant assumed that the failure of the non-safety-related structures leads to the failure of all non-safety-related systems credited in the AP1000 PRA with the exception of the manual DAS. The DAS manual actuation cables are located within the nuclear island and are therefore protected against high winds.

- The first sensitivity case assumes an unrecoverable LOSP event for all 12 high wind categories but no other failures. This sensitivity case removes the conservative assumption that all non-safety-related structures fail when the operating basis of 145 mph for high winds is exceeded, even though all structures are designed with some margin to withstand winds above the operating basis.

- The second sensitivity case assumes that all 12 high wind categories cause both an unrecoverable LOSP event and the failure of all non-safety-related structures. This sensitivity case is a very conservative upper case since it assumes that all non-safety-related structures fail even for categories of high winds that do not exceed the operating basis of 145 mph.

Table 19.58-3 of the AP1000 DCD summarizes the three risk assessment cases. The estimated CDF for the baseline case is about $5x10^{-9}$ per year, which is less than the criterion of $1x10^{-8}$ per year. Therefore, no detailed risk assessment of high winds is necessary. The CDF for the first and second sensitivity cases are about $2.3x10^{-9}$ and $1.4x10^{-8}$, respectively. The first sensitivity case indicates that the estimated risk is not significantly sensitive to assumptions about the impact on non-safety-related structures of high winds exceeding the operating basis. The second sensitivity case indicates that the screening criterion of CDF less than $1x10^{-8}$ per year is almost met even under very conservative assumptions about the failure of non-safety-related structures. The staff finds that the bounding risk assessments documented in Section 19.58 of the AP1000 DCD show that, under the stated assumptions for external events (which must be verified by the COL applicant), the risk from high winds (tornados and hurricanes) is so small that no detailed risk assessments for high winds are needed. The staff requested the addition of COL information items to enumerate the assumptions to be verified (RAI-SRP19.0-SPLA-03). In a letter from R. Sisk to the NRC dated August 21, 2008 (DCP/NRC2233), the applicant proposed to amend the DCD to state, “A site specific review of the generic PRA should be conducted to verify that the assumptions in the PRA bound the site specific conditions for the applicant’s site.” Because the COLA will include information by which the staff can assess this review, the staff finds the commitment to be sufficient.

In addition to structural failures, the applicant investigated qualitatively the potential for blockage or plugging of the PCS airflow path by debris generated by high winds. The applicant found that blockage or plugging of the PCS airflow path could occur by blockage of the screens, failure of

the louvers, or blockage of the chimney outlet. However, because of the presence of certain design features and operational requirements, these failure mechanisms are highly unlikely (i.e., their frequency is smaller than $1x10^{-7}$ per year). For this reason, the PRA does not model them.

- Screens and louvers cover 29 large vertical openings located all around the containment, each 9 feet high by 12 feet long, into an enclosed volume where the air inlet ducts are located. The screens are designed to prevent foreign objects or debris from entering the airflow path.

- Louvers are arranged within the air inlets to minimize the entrance of debris into the inlets. These louvers are fixed and therefore will not block the airflow path.

- The chimney outlet is designed to produce the necessary airflow in the event of an accident. The outlet contains two heavy grates to guard against missiles and is fully screened to prevent foreign objects from entering the containment annulus area. The presence of a positive airflow during normal operation prevents ice and snow from entering the chimney.

- There is a surveillance requirement (SR) to verify that the airflow path is unobstructed.

The staff requested that these insights related to high winds and containment cooling be added to the DCD (RAI-SRP19.0-SPLA-01, which also discussed external flooding, addressed in Sub-section 19.1.5.5). In a letter from R. Sisk to the NRC dated July 22, 2008 (DCP/NRC2211), the applicant proposed a revision to DCD Table 19.59-18, identifying these features and requirements among the PRA assumptions and insights. This is consistent with the SRP and is therefore acceptable to the staff.

In a letter from D. Lundgren to the NRC dated March 4, 2008 (DCP/NRC2095), the applicant responded to a request for information from the staff (RAI-TR142-SPCV-02 through RAI-TR142-SPCV-04). The applicant provided the results of an analysis demonstrating that most of the inlet area would have to be blocked before the PCS function is degraded. In addition, the applicant stated the following:

> There is a possibility that these [inlet] screens could become clogged with airborne debris. For this reason, there is access to the louvers and screens by an enclosed walkway between the wall containing the louvers and the shield building wall. Regular inspections of the louvers will be made and the screens will be kept free of debris. The frequency of inspections is expected to be once per month, and may change depending on the degree of blockage observed.

The staff finds that this commitment and the SR provide assurance that significant air blockages will not exist before high winds or ice storms. Because of the very large degree of blockage that would be required to challenge containment cooling, the staff considers the frequency of such an event to be negligible.

In DCD Revision 17, insights related to the protected location of DAS manual actuation cables and the assurance of adequate containment cooling air flow have been added to Table 19.59-18. The staff considers the portions of RAI-SRP19.0-SPLA-01 related to high winds to be resolved.

19.1.5.5 External Flooding Evaluation

The applicant assessed various scenarios with the potential to raise water levels and concluded that, even in combination, external flooding of safety-related SSCs (and certain risk-significant investment protection equipment) is prevented. For that reason, the effect of external flooding on risk-significant SSCs was not evaluated. Although storms, dam failure, and other external phenomena can cause flooding, the analysis assumed that the generic site was not subject to flooding by flash floods or failure of an upstream dam. COL applicants must show that this is also true for their proposed site. Otherwise, COL applicants must evaluate the other external events that can raise water levels at the site.

The risk evaluation of external floods is based on the following features from the design basis of the plant documented in Section 2 of the AP1000 DCD:

- The AP1000 is protected against floods up to the 100-foot level, which corresponds to the plant ground level. From this point, the ground is graded so that water naturally flows away from the plant structures.

- The plant is designed such that the 100-foot level is slightly above grade and the level of anticipated external flooding. Below grade is protected against flooding by a water barrier consisting of waterstops and a waterproofing system. Seismic Category I SSCs below grade are designed to withstand hydrostatic pressures.

- The seismic Category I SSCs below grade (below ground level) are protected against flooding by a water barrier consisting of waterstops and a waterproofing system.

The staff requested that these insights related to external flooding be added to the DCD (RAI-SRP19.0-SPLA-01, which also discussed high winds cooling, addressed in Sub-section 19.1.5.4).

In a letter from R. Sisk to the NRC dated July 22, 2008 (DCP/NRC2211), the applicant proposed a revision to DCD Table 19.59-18 identifying these features and requirements among the PRA assumptions and insights. This is consistent with the SRP and is therefore acceptable to the staff. In DCD Revision 17, insights related to external flooding have been added to Table 19.59-18. The staff considers the portions of RAI-SRP19.0-SPLA-01 related to external flooding to be resolved.

The risk evaluation of external floods is highly site specific. A detailed risk analysis of external floods requires information not only on potential sources of water but also on local configurations such as dikes, surface grading, locations of structures, and location of equipment within the structures. However, bounding assumptions about candidate sites are used to show that external floods can be screened from detailed risk evaluation. Assuming that the ground is graded away from the structures and there is no site susceptibility to dam failure or flash flooding, the remaining source of external flooding is storm surges capable of reaching the plant ground level. Hurricanes can produce the highest storm surges. The applicant performed a screening risk evaluation using as a reference the site most susceptible to external floods from hurricane surge water among potential candidate sites for an AP1000 plant. This site is located at an elevation of 45 feet above sea level and in an area where the highest storm surges due to hurricanes have occurred. All other proposed sites are located at higher elevations above sea level. Therefore, it would require a 45-foot hurricane storm surge to reach the plant ground

level. Any surge that stops below ground level at the plant has no impact on the plant due to flooding. Based on the Saffir-Simpson hurricane scale (Table 19.58-2 of the AP1000 DCD), only Category 5 hurricanes have the ability to generate storm surges in excess of 18 feet. Historically, the highest observed storm surges occurred during hurricane Katrina in 2005 and hurricane Camille in 1969. The maximum high water mark observation occurred during hurricane Katrina with a surge of 27.8 feet above normal tide levels at Pass Christian, on the immediate Gulf Coast just east of St. Louis Bay.

Based on the historical information, documented in Section 19.58.2.2 of the DCD, the applicant stated that a hurricane storm surge in excess of 28 feet can be classified as a rare event and a hurricane storm surge in excess of 45 feet as an extremely rare event and can be assigned a frequency of $1x10^{-7}$ per year or less. In addition, a risk assessment that was performed as a sensitivity study, which assumed loss of the switchyard and all non-safety-related SSCs, indicated that the CDF associated with external floods is insignificant when areas containing safety-related equipment are protected. Therefore, by recognizing the fact that the AP1000 design provides features (e.g., barriers) that provide protection against the propagation of flooding to areas where safety-related equipment is located, external floods that do not closely approach ground level at the plant are screened from detailed risk evaluation in accordance with the criteria discussed in Section 19.1.5.

On the basis of the discussion in DCD Section 19.58 and the large margin between the greatest storm surge observed and the water level required to affect plant safety, the staff finds that the frequency of external flooding caused by storm surge is negligibly small. The screening criteria are met and no further analysis is required. The staff expects a COL applicant to verify the applicability of the screening criteria to the proposed site.

COL applicants must confirm that all possible mechanisms of external flooding at the proposed site have been assessed, including credible combinations of those mechanisms. Otherwise, the COL applicant must screen out these external events by demonstrating that they occur with negligible frequency. COL Information Item 19.59.10-2 requires the COL applicant to re-evaluate the qualitative screening of external events.

Because this approach is consistent with RG 1.206, the staff considers this an acceptable way to address the risk of external flooding.

19.1.5.6 Transportation and Nearby Facilities Accident Evaluation

Section 19.58.2.3 of the AP1000 DCD discusses the risk from external events related to transportation accidents near the nuclear plant and to accidents at nearby industrial and military facilities. DCD Section 19.58 discusses the following types of accidents: (1) aviation, (2) marine, (3) pipeline, and (4) railroad and truck. The staff finds that these accidents form an acceptable set of transportation and nearby facility accidents based on the modified IPEEE guidelines discussed in Section 19.1.5, above. Each COL applicant should verify that these analyses bound all such hazards relevant to the proposed site.

19.1.5.6.1 Aviation Accidents

The risk evaluation for aviation accidents considers two cases: (1) small aircraft impact and (2) commercial aircraft impact. The applicant screened small aircraft impact accidents from

detailed risk evaluation by performing a bounding risk evaluation based on a limiting frequency of 1.2×10^{-6} impact events per year.

For small aircraft impact accidents, the applicant performed a bounding risk evaluation that assumed a limiting initiating event frequency of 1.2×10^{-6} per year, together with an LOSP and loss of non-safety systems. The likelihood that the impact of a small aircraft would challenge the safety systems (all located within the nuclear island) is considered negligible. Assuming that a small aircraft impact could cause an LOSP and loss of non-safety systems, the applicant showed that the associated CDF is less than 1×10^{-8} per year.

The applicant screened commercial-size aircraft impact accidents from detailed risk evaluation by assuming a limiting frequency of 1×10^{-7} impact events per year. Each COL applicant will demonstrate the assumed limiting event frequency for the selected site of 1.2×10^{-6} per year for small aircraft and 1×10^{-7} per year for commercial-size aircraft.

19.1.5.6.2 Marine Accidents

Sites close to large waterways with ship and/or barge traffic need to evaluate the risk associated with marine accidents. Marine accidents pose a hazard to a nuclear power plant due to (1) release of hazardous material towards the plant and (2) explosion with resulting damage to the plant.

The applicant evaluated the risk associated with the release of hazardous material towards the plant, following a marine accident, using a bounding analysis that assumed a limiting initiating event frequency of 1×10^{-6} per year, and showed that the associated CDF is less than 1×10^{-8} per year. Therefore, based on the screening criteria discussed in Section 19.1.5, the release of hazardous material in a marine accident requires no detailed risk evaluation. The applicant modeled the risk impact of a toxic release by assuming a reactor trip and guaranteed failure of all operator actions credited in the PRA (the toxic release is not expected to lead to any direct failure of safety equipment). This is a conservative analysis because the AP1000 has an additional level of defense against toxic airborne material. Specifically, with warning that a release has occurred, the operators can actuate passive control room habitability. This system isolates the control room from normal heating, ventilation, and air conditioning (HVAC) and actuates a separate system supplied from compressed air containers. The compressed air slightly pressurizes the control room above atmospheric pressure, preventing the entrance of toxic material for at least 72 hours. (This is adequate time for operators to deal with the event.)

The staff review finds that the bounding evaluation, documented in Section 19.58.2.3.2 of the AP1000 DCD, demonstrates that the risk associated with the release of hazardous materials in a marine accident is insignificant, assuming a limiting initiating event frequency of 1×10^{-6} per year. The COL applicant for the selected site will demonstrate the assumed frequency of 1×10^{-6} per year for release of hazardous materials that could pose a hazard to the plant by a marine accident.

The applicant screened out qualitatively the risk associated with an explosion following a marine accident with resulting damage to the plant from a detailed analysis based on the acceptance criteria of event frequency less than 1×10^{-7} per year and CDF less than 1×10^{-8} per year for the following reasons:

- Loss of service water events resulting from a marine explosion is not a nuclear safety concern for AP1000 since the design does not include a service water intake structure.

- RG 1.91, "Evaluations of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plants," provides the acceptance criterion of an overpressure event in excess of 1 pound per square inch (psi) at a frequency of less than $1x10^{-6}$ per year.

- Margin above the RG 1.91 acceptance criterion has been demonstrated. A study for the Waterford site, "Evaluation of External Hazards to Nuclear Power Plants in the United States: Other External Events," Supplement 2 (NUREG/CR-5042) indicated that the AP1000 safety-related buildings can withstand overpressures above the RG 1.91 acceptance criterion of 1 psi.

The staff review finds that the risk associated with an explosion following a marine accident is insignificant when the RG 1.91 acceptance criterion of an overpressure event in excess of 1 psi at a frequency of less than $1x10^{-6}$ per year is met. The COL applicant will demonstrate that the RG 1.91 criterion of an overpressure event in excess of 1 psi at a frequency of less than $1x10^{-6}$ per year is met for the selected site.

19.1.5.6.3 Pipeline Accidents

Sites close to pipelines need to evaluate the risk associated with pipeline accidents. Pipeline accidents pose a hazard to a nuclear power plant because of the potential for (1) a release of hazardous material towards the plant and (2) an explosion with resulting damage to the plant. The applicant evaluated the risk associated with the release of hazardous material towards the plant following a pipeline accident using a bounding analysis that assumed a limiting initiating event frequency of $1x10^{-6}$ per year. This analysis showed that the associated CDF is less than $1x10^{-8}$ per year. Therefore, based on the screening criteria discussed in Section 19.1.5, the release of hazardous material in a pipeline accident requires no detailed risk evaluation. The applicant modeled the risk impact of a toxic release by assuming a reactor trip and guaranteed failure of all operator actions credited in the PRA (the toxic release is not expected to lead to any direct failure of safety equipment). This is a conservative analysis because the AP1000 has an additional level of defense against toxic airborne material. Specifically, with a warning that a release has occurred, the operators can actuate passive control room habitability. This system isolates the control room from normal HVAC and actuates a separate system supplied from compressed air containers. The compressed air slightly pressurizes the control room above atmospheric pressure, preventing the entrance of toxic material for 72 hours. (This is adequate time for operators to deal with the event.)

The risk associated with an explosion following a pipeline accident with resulting damage to the plant was screened out qualitatively from a detailed analysis, based on the acceptance criteria of event frequency less than $1x10^{-7}$ per year. Section 19.58.2.3.3 of the AP1000 DCD documents an approach (pipeline accident model) that qualitatively illustrates potential scenarios from gas pipeline accidents. This approach briefly discusses the following considerations for evaluating the frequency of pipeline accidents: (1) gas pipe rupture frequency estimation, (2) gas cloud formation probability estimation, (3) gas cloud transportation and nondispersion probability estimation, and (4) onsite gas cloud ignition probability estimation.

The staff review finds that the risk associated with pipeline accidents is insignificant, assuming that the COL applicant will demonstrate that the frequency criterion of $1x10^{-7}$ per year is met for

the proposed site for pipeline accidents that could pose a hazard to the plant. The frequency of pipeline accidents will be evaluated by the COL applicant using the approach discussed in Section 19.58.2.3.3 of the DCD or another approach acceptable to the staff.

19.1.5.6.4 Railroad and Truck Accidents

Railroad and truck accidents could pose a hazard to an AP1000 plant, and COL applicants need to evaluate the risk associated with such accidents. As for marine and pipeline accidents, railroad and truck accidents could pose a hazard to a nuclear power plant because of the potential for (1) a release of hazardous material towards the plant and (2) an explosion with resulting damage to the plant. However, railroad and truck accidents are expected to be less likely to occur (e.g., because of the improved security barriers established at U.S. nuclear power plants) and cause less plant damage than aviation or marine accidents if they should happen. For these reasons, the risk impact from railroad and truck accidents is insignificant if the initiating event frequency criterion of $1x10^{-7}$ per year is met.

The staff review finds that the risk associated with railroad and truck accidents is insignificant, assuming that the COL applicant can demonstrate that the frequency criterion of $1x10^{-7}$ per year is met for the proposed site for railroad and truck accidents that could pose a hazard to the plant.

19.1.5.7 External Fires

External fires are those that occur outside the controlled site boundary. Potential effects on the plant could be LOSP, forced isolation of the plant ventilation, and control room evacuation. External fires are not expected to spread on site because of site clearing during the construction phase and control of combustibles during construction and operation. The staff requested that the applicant consider external fires more explicitly (RAI-TR101-SPLA-03).

In a letter from A. Sterdis to the NRC dated February 8, 2008 (DCP/NRC2084), the applicant agreed to address that based on site-specific information, the COL applicant should reevaluate the qualitative screening of external fires. Accordingly, based on the criteria discussed in Section 19.1.5, above, which were used to screen out external hazards in the PRA, a risk evaluation should be performed if the COL applicant cannot demonstrate that the frequency of external fires that could pose a hazard to the plant is less than $1x10^{-7}$ per year. If the COL applicant identifies any site-specific susceptibilities, the site-specific PRA performed to address COL Holder Item 19.59.10-2 should include external fires.

This is consistent with RG 1.200 and therefore acceptable to the staff.

19.1.5.8 Conclusions

Information documented in Section 19.58 of the AP1000 DCD addresses the second part of COL Information Item 19.59.10-2 which reads as follows:

> Based on site-specific information, the COL should also re-evaluate the qualitative screening of external events (PRA Section 58.1). If any site-specific susceptibilities are found, the PRA should be updated to include the applicable external event.

The information provided in Section 19.58 of the AP1000 DCD includes the following objectives:

- to show that screening criteria are met and to identify external events that may impact the AP1000 risk on a site-specific basis

- to provide generic risk analyses, based on bounding assumptions regarding site-specific parameters (e.g., frequency of each category of hurricanes) for some external events

- to provide guidance to COL applicants regarding the verification of the applicability of these "generic" analyses to a specific site

Based on modified IPEEE guidelines, DCD Section 19.58 discusses the following external events or external hazards:

- high winds (including tornadoes)
- external floods
- transportation and nearby facility accidents
- external fires

The staff review finds that these external hazards are most likely a complete list of events associated with candidate sites for an AP1000 plant. However, as stated in DCD Section 2.2.1, "Combined License Information for Identification of Site-specific Potential Hazards," the COL applicant must verify that this list adequately addresses external hazards at the proposed site. The COL applicant should use site-specific information to verify that the assumptions made in the analyses performed during the design certification stage are applicable. For example, screening on the basis of event frequency of external flooding due to tsunamis or upstream dam failures may not be possible at all sites.

The staff finds that the generic risk analyses and other information provided in Section 19.58 of the AP1000 DCD are acceptable, including the screening of events from inclusion in the PRA, given the documented assumptions.

However, these analyses are based on assumptions that are expected to envelop site-specific information at sites selected to build a nuclear plant referencing the AP1000 design. The COL applicant referencing the information provided in DCD Section 19.58 must (1) confirm in the COLA that the information provided in Section 19.58 of the DCD is applicable to the selected site and (2) ensure that the assumptions made in the generic risk evaluations documented in Section 19.58 of the DCD bound the site-specific conditions for the applicant's site. This is in agreement with the stipulation made in Section 19.58.3 of the AP1000 DCD, which states that the COL applicant should conduct a site-specific review of the generic PRA to verify that the assumptions in the PRA bound the site-specific conditions for the applicant's site (COL Information Item 19.59.10-2).

19.1.8.24 Reactor Pressure Vessel Thermal Insulation System

The AP1000 design includes a reflective reactor vessel insulation system (RVIS) that provides an engineered flow path to allow water ingress and venting of steam for external reactor vessel cooling (ERVC) in the event of a severe accident involving core relocation to the lower plenum. COL Action Item 19.2.3.3.1.3.2-1 calls for the COL applicants to complete the design for the RPV thermal insulation system. Section 39.10.2 of the AP1000 PRA specifies its functional

requirements. In addition to RCS depressurization and reactor cavity flooding, several other conditions are necessary: (1) the reactor vessel thermal insulation system design must be consistent with ULPU configuration V testing with prototypical insulation (ULPU-2000 is a boiling heat transfer test facility at the University of California at Santa Barbara used to investigate in-vessel retention of a damaged core), (2) the reactor vessel insulation system must maintain its integrity under the hydrodynamic loads associated with ERVC and not be 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.

Westinghouse has completed the design of the RVIS. In APP-GW-GLR-060 (TR-24), the applicant provided information to demonstrate that the reactor vessel insulation system is designed to provide adequate cooling to ensure in-vessel retention of a damaged and relocated core. On this basis, the applicant proposed to close COL Information Item 5.3-5. The staff's evaluation is in Section 19.2.3.3.1.3.2 of this supplement.

19.1.9 Conclusions and Findings

The staff has evaluated the AP1000 design PRA quality and its use in the design and certification processes. The NRC concludes that the quality and completeness of the AP1000 PRA are adequate for its intended purposes which are to support the design and certification processes and satisfy the requirements of 10 CFR 52.47. The approaches used by the applicant for both the core damage and containment analyses are logical and sufficient to achieve the desired goals of describing and quantifying potential core damage scenarios and containment performance during severe accidents. The conclusion the NRC previously reached after review of the AP1000 design remains valid for the amended design.

The use of PRA in the AP1000 design process improved the unique passive features of the design by providing a better understanding of plant response, including potential system interactions, during postulated accidents beyond the design basis. Such features contributed to the reduced CDF and conditional containment failure probability estimates of the AP1000 design when compared to those of operating PWRs. The applicant used the PRA results and insights to identify areas in which it is particularly important to implement the certification and operational requirements assumed during the design and certification processes (e.g., ITAAC, RTNSS requirements, D-RAP, COL action items, and technical specifications). On the basis of this review, the NRC believes that the amended AP1000 design meets the NRC's safety goals and represents an improvement in safety over operating PWRs in the United States.

19.1.10 Resolution of Safety Evaluation Report Open Items

Open Item OI-SRP19.0-SPLA-07: The applicant must implement corrective actions after the audit, resolving and requantifying the corrected model as well as revising TR-102 and making associated changes to the DCD consistent with COL/DC-ISG-3.

Open Item OI-SRP19.0-SPLA-12: The applicant must confirm that an acceptable seismic margin is maintained for HRHF sites.

Open Item OI-SRP19.0-SPLA-13: The applicant must provide an updated DCD description of events (human actions, common cause, and basic) and sequences contributing most to risk, both at power and while shutdown.

Open Item OI-SRP19.0-SPLA-14: The applicant must resolve the discrepancy in the containment inventory of radionuclides used for the survivability evaluation, determining whether the environmental assessment should include mechanical penetrations and hatches (e.g., gasket materials) and providing a COL holder item to finalize the list of equipment that must survive.

Open Item OI-SRP19F-SPLA-01: The staff will not review Appendix 19F, "Malevolent Aircraft Impact," to the AP1000 DCD until regulatory guidance has been issued on this topic. There is no RAI associated with this open item.

19.1.11 Combined License Information Items

19.1.11.1 As-Built Seismic Margin Assessment

COL Information Item 19.59.10-1 (NRC FSER COL Action Items 19A.2-1 and 19A.2-2) is associated with an as-built SSC HCLPF comparison to seismic margin evaluation. In APP-GW-GLR-021, the applicant noted that a COL applicant cannot complete the review and proposes instead to complete these actions before fuel loading.

Because the review requires that construction of SSCs be completed, the staff agrees that evaluation of as-built conditions cannot be provided with the COL application. The staff concludes that completion of the as-built SMA before fuel loading is timely and therefore acceptable. COL Information Item 19.59.10-1 is a COL holder item.

19.1.11.2 Site-Specific, Plant-Specific Probabilistic Risk Assessment

COL Information Item 19.59.10-2 is associated with evaluating an as-built plant versus design in AP1000 PRA and site-specific PRA external events. In APP-GW-GLR-021 (TR-6), the applicant noted that a COL applicant cannot complete an as-built review and proposes that the COL applicant referencing the AP1000 certified design will, instead, review differences between the as-built plant and the design used as the basis for the AP1000 PRA and Table 19.59-18. The applicant proposed that, if a screening analysis shows that the effect of the differences could result in a significant increase in CDF or LRF, the PRA would be updated to reflect these differences. In addition, the COL applicant should reevaluate the qualitative screening of external events (PRA Section 58.1). If any site-specific susceptibilities are found, the PRA should be updated to include the applicable external event.

The staff agrees that the design-specific PRA is a sufficient and acceptable basis for drawing safety conclusions for a license and should be described in the FSAR (with appropriate discussion of departures from the certified design). The FSAR should also identify key assumptions and insights from this PRA. The staff finds that a qualitative screening of external events, specific to the proposed plant site, is an acceptable way to confirm that site-specific vulnerabilities do not require risk assessment.

However, the staff finds that each licensee's PRA should model significant plant-specific and site-specific differences from the design PRA, whether positive or negative, to be consistent with

COL/DC-ISG-3. This is necessary to adequately support operational-phase reliability assurance activities, when more realistic assessment of risk is needed to avoid masking activities of risk significance. The NRC staff identified this as COL Information Item SRP19.1-01.

19.2 Severe Accident Performance

19.2.2 Deterministic Assessment of Severe Accident Prevention

19.2.2.1.2 Mid-Loop Operation

During refueling or maintenance activities, the RCS is sometimes reduced to a "mid-loop" level. The applicant summarized the specific AP1000 design features that address mid-loop operations in DCD Tier 2, Section 5.4.7.2.1, "Design Features Addressing Shutdown and Mid-Loop Operations." In addition, DCD Tier 2, Table 16.3-2, "Investment Protection Short-Term Availability Controls," ensures that the RNS is available during mid-loop operation.

Section 19.3, "Shutdown Evaluation," of this report documents the staff's evaluation of shutdown risk. Because RTNSS has not been amended, it is not discussed in this supplement. DCD Tier 2, Table 16.3-2, documents the availability controls provided for the RNS during normal and reduced inventory. The staff concludes that the AP1000 design conforms to the mid-loop operation guidance specified in SECY-93-087 and is therefore acceptable.

19.2.3.3.1.3.2 Reactor Pressure Vessel Thermal Insulation System

Section 5.3.5 describes the design of the RPV thermal insulation system. Section 19.1.2.2.4 discusses considerations related to risk assessment. This section addresses the staff's evaluation of conformance of the final design of the reactor vessel insulation system (RCIS) to the ULPU Configuration V testing, its integrity under the hydrodynamic loads associated with ERVC, absence of susceptibility to clogging, and absence of coatings that could interfere with wetting phenomena that contribute to effective heat removal.

The staff noted an apparent stepwise change in the cross-section of the annulus formed between the RVIS and the reactor vessel, formed by the neutron shield (RAI-TR24-SPLA-01). Other information was requested with respect to dimensions that could be important to the adequacy of the flow path (RAI-TR24-SPLA-04) and specific design documents (RAI-TR24-SPLA-05). In a letter from A. Sterdis to the NRC dated August 21, 2007 (ML072350140), the applicant provided additional details about the modeling of the flow path and flow areas. This allowed the staff to confirm that the design was consistent with the ULPU Configuration V testing.

The applicant changed the design of the RVIS inlet closure devices from floating balls to hinged, buoyant doors. The staff requested additional information to confirm that this was consistent with the ULPU Configuration V testing (RAI-TR24-SPLA-02, first part). Additional details on the configuration of the doors and the forces acting on them were also sought (RAI-TR24-SPLA-07). In the same letter (ML072350140), the applicant provided additional details about these active components of the system and the effect on flow areas and flow resistance. Because the new design retains the characteristic of actuation by buoyant forces, the cross-sectional area is maintained, and flow resistance is reduced, the staff considers this change to be an acceptable way to conform to the ULPU Configuration V testing.

Similarly, the applicant changed the design of steam vent ducts that provide a flow path for the steam/water within the reactor vessel insulation annular space to flow back to the containment flood-up region (RAI-TR24-SPLA-02, second part). In the same letter (ML072350140), the applicant explained that the previous design had multiple miter bends instead of a sudden contraction in the area of the flow path. The modification reduces flow resistance and allows higher mass flow. Because the results of the testing conservatively bound the expected performance of the RVIS, the staff considers this change to be an acceptable way to conform to the ULPU Configuration V testing.

The staff noted that the RVIS doors and the reactor coolant drain tank room ventilation damper, though described by the applicant as "passive," are considered by the staff to be active components. The staff requested information on periodic verification of the performance of moving parts (RAI-TR24-SPLA-03), as well as a discussion of ALARA considerations for testing and maintenance (RAI-TR24-SPLA-08). In the same letter (ML072350140), the applicant confirmed that RVIS is in the design reliability program (D-RAP). Proper fit and freedom of motion of the doors is confirmed during hot functional testing. Visual inspection and testing for freedom of rotation is to be performed during refueling outages at ten-year intervals, coordinated with other inspections in the same area. Individual doors and frames are designed for removal as a unit, so replacement, if required, would take little time. Because the applicant has applied a level of control and testing consistent with Commission policy on regulatory treatment of non-safety systems (RTNSS) and ALARA, the staff considers this to be acceptable.

Because the design of the RVIS is consistent with the ULPU Configuration V testing, the staff's evaluation of hydrodynamic loads and previous findings with respect to the potential for clogging of the flow path are unchanged.

The staff requested resolution of earlier test results (ULPU Configuration III and BETA tests) dealing with the wettability of the reactor pressure vessel surface if it were coated (RAI-TR24-SPLA-06). The applicant revised the DCD to reflect a commitment to ensure that the reactor vessel exterior is bare metal.

On the basis of the additional description, the staff was able to confirm that the new design is consistent with the ULPU Configuration V testing and is therefore acceptable. The staff concludes that COL Action Item 19.2.3.3.1.3.2-1 is closed for COL applicants referencing the AP1000 DCD.

19.2.3.3.7 Equipment Survivability

Electrical and mechanical equipment must survive to prevent and mitigate the consequences of severe accidents. The applicant addressed equipment survivability in Appendix 19D, "Equipment Survivability Assessment," to DCD Tier 2, which contains general requirements and equipment classification. Appendix D to the AP1000 PRA supporting document presents the analysis performed to determine the severe accident environmental conditions.

In APP-GW-GLR-069, "Equipment Survivability Assessment" (TR-68), the applicant submitted revised analysis in support of the design certification amendment. In reviewing TR-68, the staff noted that the severe accident environmental conditions were revised.

In APP-GW-VP-025, "AP1000 Equipment Survivability Assessment," an attachment to TR-68, the applicant stated that it had revised the fraction of the core inventory released to the

containment atmosphere from the original PRA Appendix D and that the values are consistent with the accident source term information presented in NUREG-1465, “Accident Source Terms for Light-Water Nuclear Power Plants—Final Report.”

However, the following analytical assumptions documented in APP-GW-VP-025 are unchanged from those in the original PRA and do not appear to be consistent with NUREG-1465:

- Power level (including 2-percent power uncertainty): 3,468 megawatt thermal
- Fraction of total core inventory released to the containment atmosphere:

· Noble Gases (xenon, krypton)	1.0
· Halogens (iodine, bromine)	0.75
· Alkali Metals (cesium, rubidium)	0.75
· Tellurium Group (tellurium, antimony, selenium)	0.305
· Barium, Strontium	0.12
· Noble Metals (ruthenium, rhodium, palladium, molybdenum, technetium, cobalt)	0.005
· Lanthanides (lanthanum, zirconium, neodymium, europium, niobium, promethium, praseodymium, samarium, yttrium, curium, americium)	0.0052
· Cerium Group (cerium, plutonium, neptunium)	0.0055

The staff requested clarification (RAI-SRP19.0-SPLA-14), but remains unable to confirm the basis for the results documented in TR-68 or to trace the assessment from the in-containment source term to the dose at which the equipment was evaluated. The NRC staff identified this as the first part of Open Item OI-SRP19.0-SPLA-14.

The radiation exposure inside the containment for a severe accident is conservatively estimated by considering the dose in the middle of the AP1000 containment with no credit for the shielding provided by internal structures. MAAP4 containment modeling is used to establish the thermal-hydraulic conditions for consideration of equipment survivability for the different containment regions.

During the development of the severe accident management guidance (SAMG) for AP1000, additional requirements were defined for accident management in Time Frame 2 (in-vessel severe accident phase) and Time Frame 3 (ex-vessel severe accident phase). For example, previously unidentified methods of injecting water into containment were added (e.g., providing makeup to overflow the IRWST by the RNS system). The use of containment spray was identified as a severe accident strategy (e.g., injecting water into containment and containment heat removal). Another method of depressurizing the RCS in Time Frame 2 was identified (i.e., reactor vessel head venting).

In addition, finalizing certain system designs resulted in the need to update lists of associated equipment and instrumentation. For example, the applicant eliminated low-pressure steam generator feed systems (i.e., service water and condensate water) from consideration.

Lastly, the applicant changed the equipment and instrumentation identification to conform to updated naming conventions for AP1000. The new list of equipment and instrumentation reflects the amended AP1000 design.

The applicant has not completed the identification of equipment and instrumentation for prevention of core damage (e.g., Time Frame 0 and Time Frame 1) because the EOPs are still in development. Upon finalization of the EOPs, the applicant can identify and assess the survivability of the equipment and instrumentation used in those procedures. This should be identified as a COL holder item. The NRC staff identified this as the second part of Open Item OI-SRP19.0-SPLA-14.

In general, the applicant claims that the AP1000 provides reasonable assurance that equipment, both electrical and mechanical, designed for mitigating the consequences of severe accidents will perform its functions as intended.

The applicant did not completely identify the SSCs required for containment isolation. Westinghouse has not determined whether the equipment survivability assessment needs to include mechanical penetrations and hatches (e.g., gasket materials) to ensure containment integrity. The NRC staff identified this as the third part of Open Item OI-SRP19.0-SPLA-14.

19.2.5 Accident Management

Accident management 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. Severe accident management is the process of extending the EOPs well beyond the plant design basis into severe fuel damage regimes and making full use of existing plant equipment, operator skills, and creativity to terminate severe accidents and limit offsite releases.

The NRC has taken an active role in ensuring that utilities adopt acceptable accident management practices. In January 1989, the staff issued SECY-89-012, “Staff Plans for Accident Management Regulatory and Research Programs,” which discusses essential elements of a utility accident management plan and offers an approach for accident management implementation. Subsequently, the NRC worked with the industry to define the scope and attributes of a utility accident management plan and to develop guidelines for plant-specific implementation. Section 5 of NEI 91-04, Revision 1, “Severe Accident Closure Guidelines,” which lays out the elements of the industry’s severe accident management closure actions that have been accepted by the staff, resulted from these efforts. This program involves the development of (1) a structured method by which utilities may systematically evaluate and enhance their abilities to deal with potential severe accidents, (2) vendor-specific accident management guidelines for use by individual utilities in establishing plant-specific accident management procedures and guidance, and (3) guidance and material to support utility activities related to training in severe accidents. Using the guidance developed through this

program, each operating plant has implemented a plant-specific accident management plan as part of an industry initiative.

Based on its reviews of these efforts, severe accident evaluations in individual plant examinations, and industry PRAs, the staff concluded that improvements to utility accident management capabilities could further reduce the risk associated with severe accidents. Although new reactor designs are to have enhanced capabilities for the prevention and mitigation of severe accidents, accident management remains an important element of defense in depth for these designs. However, the staff expects the increased attention on accident prevention and mitigation in these designs to alter the scope and focus of accident management relative to that for operating reactors. For example, the staff expects increased attention on accident prevention and the development of error-tolerant designs to decrease the need for operator intervention, while increasing the time available for such action if necessary. This permits a greater reliance on support from outside sources. For longer times after an accident (several hours to several days), the need for human intervention and accident management will continue.

For both operating and advanced reactors, the overall responsibility for accident management, including development, implementation, and maintenance of the accident management plan, lies with the nuclear utility, because the utility bears ultimate responsibility for the safety of the plant and for establishing and maintaining an emergency response organization capable of effectively responding to potential accident situations. However, the vendors have played key roles in providing essential SAMG and strategies for implementation. This guidance has served as the basis for severe accident management procedures and for training utility personnel in carrying out the procedures. Computational aids for technical support have been developed, information needed to respond to a spectrum of severe accidents has been provided, decisionmaking responsibilities have been delineated, and utility self-evaluation methodologies have been developed.

A COL applicant referencing the AP1000 design must develop and implement SAMG using the suggested framework provided in WCAP-13914, “Framework for AP600 Severe Accident Management Guidance,” Revision 3. This WCAP outlines a plan based on the Westinghouse Owners Group (WOG) SAMG for currently operating plants. Its scope is to address significant core damage accidents that might be possible in the AP600 and to provide the framework for developing guidance on how to cope with these accidents after the emergency response guidelines are no longer applicable. APP-GW-GLR-070 (TR-66) extends this framework to the AP1000 design.

In the AP1000 FSER, the staff states that it expects the COL applicant to follow the recommendations provided in WCAP-13914 in developing its plant-specific accident management guidance (COL Action Item 19.2.5-1). Westinghouse has taken steps to facilitate this process by producing TR-66, the AP1000 framework document, and the AP1000 severe accident management guidelines.

Westinghouse prepared and submitted TR-66 to close COL License Information Item 19.59.10-4 with respect to development of the SAMG. The information item states the following:

> The combined license applicant referencing the AP1000 certified design will develop and implement severe accident management guidance using the

suggested framework provided in WCAP-13914, “Framework for AP600 Severe Accident Management Guidance.”

APP-GW-GL-027, “Framework for AP1000 Severe Accident Management Guidance Development,” documents the framework for the AP1000. Based on this framework, Westinghouse has also developed severe accident management guidelines for the AP1000 (APP-GW-GJR-400, “AP1000 Severe Accident Management Guidelines,” Revision A), which COL holders will implement at each site using the AP1000 design. TR-66 is a road map for COL holders using these guidelines.

The staff requested clarification of the schedule for development and implementation of SAMG (RAI-SRP19.0-SPLA-15). In a letter from R. Sisk to the NRC dated August 21, 2008 (DCP/NRC2233), the applicant provided the requested information.

The starting point for the technical basis for the AP1000 is Electric Power Research Institute (EPRI) TR-101869, “Severe Accident Management Technical Basis Document” (Volumes 1 and 2). This document details the severe accident phenomenological understanding as it was in the early 1990s, when it formed the basis for the WOG guidelines. For the most part, this understanding is still current, although a number of important technical issues have been resolved and a few new ones identified since then. For example, direct containment heating in large-volume PWRs is no longer considered to be a major threat, but induced SGTRs in high-pressure scenarios have become a major concern. The AP1000 SAMG consists of three volumes:

(1) An executive volume describes the methodology and criteria for the development of the AP1000 SAMG. It includes all of the material in the framework document, an overview of the AP1000 SAMG, a writer’s guide for writing the SAMG and background documents, and a number of other important items related to the decisionmaking process, interfaces between the AP1000 EOPs and the SAMG, and interfaces between the SAMG and the site emergency plan.

(2) A guideline volume contains the SAMG guidelines to be used by the control room staff and the engineering support staff in the technical support center (TSC) in responding to a severe accident.

(3) A background volume details the technical basis for the guidance found in the guidelines volume.

Section 5.1 of NEI 91-04 states that accident management consists of those actions taken during the course of an accident by the plant’s emergency response organization (ERO), particularly the plant operations, technical support, and plant management staff, to achieve the following:

- prevent the accident from progressing to core damage
- terminate core damage progression once it begins
- maintain the capability of the containment as long as possible
- minimize onsite and offsite releases and their effects

The latter three actions constitute a subset of accident management referred to as severe accident management, or more specifically, severe accident mitigation.

NEI 91-04 also states that the goal of severe accident management is to enhance the capabilities of the ERO to mitigate severe accidents and prevent or minimize any offsite releases. The objective is to establish core cooling and to manage any current or immediate threats to the fission product barriers. Accomplishing this ERO should make full use of existing plant capabilities, including standard and nonstandard uses of plant systems and equipment.

The NRC staff agrees that NEI 91-04 properly defines the scope of severe accident management and believes that the framework for SAMG should be consistent with this scope.

The AP1000 SAMG consists of three parts: control room SAMG, TSC SAMG, and TSC challenge response guidance. The control room SAMG consists of two separate guidelines. The control room staff uses the first of these guidelines until the TSC is functional and its staff is ready to use the TSC SAMG. The staff uses the second guideline after the TSC is functional; this guideline provides the staff with a structured set of activities when the TSC is evaluating the plant conditions and potential responses.

The TSC staff will execute the TSC SAMG, using the diagnostic flow chart (DFC) and the severe challenge status tree to select the appropriate strategies to respond to variations in the key parameters. These strategies are contained in the seven severe accident guidelines:

(1) inject into containment
(2) depressurize the RCS
(3) inject into the steam generators
(4) inject into the RCS
(5) reduce fission product releases
(6) control containment conditions
(7) reduce containment hydrogen

The guidelines specify a method for a systematic, logical evaluation of the possible strategies and a process of deciding which actions to implement.

Another guideline, SAEG-1, monitors long-term activities after a particular strategy is implemented. Such activities depend on a number of factors, including the equipment put into service to implement the strategies, equipment already in service before implementing the SAMG that relates to the control of a DFC parameter, limitations on equipment usage identified in the guidelines that evaluate the possible strategies, equipment no longer in service if implementation of a strategy is discontinued, and changes in plant conditions following implementation of severe accident management strategies.

A final guideline, SAEG-2 for SAMG termination, comes into play when the plant has been put into a safe, stable state. At this time, selected parameters in the DFC are below their setpoint values and are stable or decreasing, and no new SAM strategies will be required. However, generic SAMG exit guidance has been developed.

Four computational aids have been developed to assist the TSC staff in diagnosing and formulating appropriate strategies:

(1) RCS injection to recover the core
(2) injection rate for long-term heat removal

(3) hydrogen flammability in containment
(4) containment water level and volume

The NRC staff reviewed TR-66, the AP1000 framework document (APP-GW-GL-027), and the executive volume of the AP1000 SAMG. The staff confirmed that the AP1000 SAMG reflects current understanding of severe accident progression. The staff examined the remaining two volumes to ensure that they are an appropriate extension of the EPRI guidance, consistent with the SAMG developed by the WOG for operating reactors, and address all necessary high-level actions. The DCD appropriately references these documents.

In the course of its review, the staff asked the applicant to explain how it will provide guidance to resolve potentially conflicting considerations when introducing water to a dry reactor vessel after core relocation (full or partial) to the bottom head. Concerns over hydrogen generation suggest maximizing the flow rate, while concerns about a degraded reactor vessel (overheating and wall thinning at or near the surface of the pool of relocated core material) suggest that flow should be controlled (RAI-SRP19.0-SPLA-16).

In a letter from R. Sisk to the NRC dated August 21, 2008 (DCP/NRC2233), the applicant stated that it will update the AP1000 SAMG guideline for "inject into the RCS" to address the recommended rate of injection into the RCS for situations in which the injection capability is recovered after significant core damage has occurred. The applicant will add a new item in the evaluation of the potential negative impacts of injecting into the RCS to note that high injection flow rates will minimize the potential for significant hydrogen generation while lower, controlled flow rates will minimize the potential for failure of the reactor vessel. The evaluation will explain that hydrogen generation caused by low flow rates will only be a concern if a significant amount of hydrogen is already in the containment indicating a failure of the hydrogen igniters or the recombiners, or both. On the other hand, the concern about reactor vessel integrity due to high injection flow rates will only exist when a prolonged period has elapsed since the onset of high core temperatures and the reactor vessel will be externally cooled by submergence in water. Attachment B to that the guideline and the associated background document will also provide a full discussion of the conditions under which each of the concerns is applicable. The NRC staff identified this as Confirmatory Item CI-SRP19.0-SPLA-16.

On the basis of this review, the staff concludes that SAMG for the AP1000 is consistent with NEI 91-04 and is a logical extension of the WOG SAMG. The discussions of the high-level actions, supported by the background documents provided, establish a sound technical basis for AP1000 COL applicants to develop their severe accident management procedures and training.

For this reason, the staff considers AP1000 COL Information Item 19.59.10-4 to be closed for COL applicants referencing the AP1000 DCD.

19.3 Shutdown Evaluation

19.3.7 Outage Planning and Control

The staff asked the applicant to clarify whether the development of freeze seal guidelines is the responsibility of the COL applicant, is included in the procedure development described in APP-GW-GLR-040, "Plant Operations, Surveillance, and Maintenance Procedures," Revision 1 (TR-70), or is controlled in some other way (RAI-SRP19.0-SPLA-10).

The applicant modified DCD Section 13.5 to include the following statement: "If freeze seals are to be used, plant-specific guidelines will be developed to reduce the potential for loss of RCS boundary and inventory when they are in use," and confirmed that COL Information Item 13.5-1 includes the guidelines for use of freeze seals. It is among the guidelines identified as "Phase 3" procedure activities.

The FSER described other COL action items related to shutdown procedures that the staff consolidated in COL Information Item 13.5-1. The staff asked the applicant how it would identify these action items to the COL applicant (RAI-SRP19.0-SPLA-11):

- FSER COL Action Item 19.1.8.1-4: The COL applicant will implement the maintenance guidelines as described in WCAP-14837, "AP600 Shutdown Evaluation Report".

- FSER COL Action Item 19.1.8.3-1: The COL applicant is responsible for developing procedures…to close containment hatches and penetrations following an accident during MODE 5 and MODE 6 before steam is released into the containment.

- FSER COL Action Item 19.1.8.16-1: The COL applicant will have policies that maximize the availability of normal residual heat removal (valve V-023) and procedures to open this valve during cold shutdown and refueling operations when the RCS is open and the passive residual heat removal system cannot be used for core cooling.

- FSER COL Action Item 19.1.8.16-2: The COL applicant will develop administrative controls to ensure that inadvertent opening of RNS valve V-024 is unlikely since inadvertent opening results in a draindown of the RCS inventory to the IRWST and requires gravity injection from the IRWST.

- FSER COL Action Item 19.1.8.16-4: The COL applicant will maintain procedures to respond to low hot-leg level alarms.

- FSER COL Action Item 19.3.7-1: The COL applicant will develop an outage planning and control program and will appropriately address the factors that improve low-power and shutdown operations consistent with DCD Tier 2, Chapter 19E, "Shutdown Evaluation," and NUMARC 91-06, "Guidelines for Industry Actions To Assess Shutdown Management."

- FSER COL Action Item 19.1.8.7-1: The COL applicant will implement procedures and policies to have the non-safety-related wide-range pressurizer level indication during cold shutdown.

Each of these action items has a corresponding entry in DCD Table 19.58-18. COL holders referencing the AP1000 design must verify that the insights and assumptions documented in this table are satisfied. The staff finds this to be an acceptable method for ensuring that appropriate administrative controls will be applied.

In TR-70, the applicant suggested that the procedures in Phase 3 need not be developed until after a COL is issued.

The staff agrees that these guidelines do not need to be completed at the time of application and finds that the program described in TR-70 is an acceptable method for providing assurance that appropriate guidance will be developed in a timely manner.

19.3.10 Flood Protection

The FSER states the following:

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

The staff expects the COL applicant to take compensatory measures to maintain adequate detection capability during maintenance activities. The staff identified two COL information items that address fire detection and suppression but not flooding. The staff asked the applicant to clarify how it will address concerns about flooding detection, barrier integrity, and control (RAI-SRP19.0-SPLA-08).

The applicant's response focused on aspects of the AP1000 design that obviate the need to compensate for a maintenance-related breach of flooding barriers. Specifically, the design does not include any watertight doors; flood barriers are permanent fixtures that are neither opened nor altered by normal activities, including maintenance. Moreover, the CDF contribution from internal flooding is extremely low.

The staff agrees with the applicant's assessment of internal flooding risk. As stated in the FSER, the results of the AP1000 study for internal flooding show that the AP1000 design is adequate because internal floods during shutdown do not represent a significant risk contribution.

19.5 Conclusion

The staff evaluated the information submitted by the applicant in accordance with SRP Sections 19.0 and 19.1. In addition to its review of the documents identified above, the staff conducted an audit in the applicant's Monroeville, Pennsylvania offices, described in an audit report which is accessible through the Agencywide Document Access and Management System (ADAMS), Accession No. ML083230705.

The applicant has updated the AP1000 PRA to include the most recent I&C design information. Additionally, to facilitate future updates, the applicant converted the PRA software package from the Westinghouse proprietary WesSAGE software package to the CAFTA software package. The applicant also documented the basis for its determination that other design changes did not affect the SSCs modeled in the PRA in a manner that affected the PRA.

In addition to reviewing the description of changes to the PRA, the staff reviewed the description of the new I&C design, specifically the PLS and PMS. The staff reviewed the methods and procedures for conversion of the PRA model from WesSAGE to CAFTA in the applicant's offices. The staff also reviewed the process by which the applicant incorporated the design changes in the PRA.

The staff noted that the applicant has a formal procedure for the review of design packages to ensure that it identifies and addresses any impact on the PRA. Design change packages are evaluated for the potential to alter the PRA model or to affect PRA assumptions or insights.

With the resolution of the open items described in Section 19.1.10 of this report, the staff concludes that the results and insights of the upgraded and updated design-specific PRA for the AP1000 are an acceptable basis for the risk-informed review of the amended AP1000 DCD and for the development of plant-specific PRAs to support COLAs. The staff also finds that the AP1000 PRA demonstrates that the AP1000 design will support the Commission's goals for improved safety of new reactors.

19.6 References

1. APP-GW-GL-011, "AP1000 Identification of Critical Human Actions and Risk Important Tasks" (WCAP-16555).
2. APP-GW-GLN-016, "Generic Reactor Coolant Pump" (TR-34).
3. APP-GW-GLN-022, Rev. 1, "DAS Platform Technology and Remote Indication Change" (TR-97).
4. APP-GW-GLN-105, Rev. 1, "Building and Structure Configuration, Layout and General Arrangement Design Updates" (TR-105).
5. APP-GW-GLN-106, Rev. 1, "Mechanical System and Component Design Update" (TR-106).
6. APP-GW-GLN-147, Rev. 1, "AP1000 CR and IRWST Screen Design" (TR-147), February 2008.
7. APP-GW-GLR-016, "AP1000 Pressurizer Design" (TR-36).
8. APP-GW-GLR-021, "AP1000 As-built COL Information Items" (TR-6).
9. APP-GW-GLR-065, "AP1000 Instrumentation & Control (I&C) Data Communication and Manual Control of Safety Systems and Components" (TR-88).
10. APP-GW-GLR-070, "Development of Severe Accident Management Guidance," (TR-66).
11. APP-GW-GLR-101, "AP1000 PRA Evaluation of External Events" (TR-101).
12. APP-GW-GLR-102, "AP1000 PRA Update Report" (TR-102).
13. APP-GW-GLR-130, "Editorial Format Changes Related to "Combined License Applicant" and Combined License Information Items" (TR-130).
14. APP-GW-GLR-134, Rev. 5, "AP1000 DCD Impacts to Support COLA Standardization" (TR-134).
15. APP-PRA-GER-001, "AP1000 Design Change Proposal Review for PRA and Severe Accident Impact" (TR-135).
16. APP-GW-GLR-021, "AP1000 As-built COL Information Items" (TR-6).
17. APP-GW-GLR-065, "AP1000 Instrumentation & Control (I&C) Data Communication and Manual Control of Safety Systems and Components" (TR-88).
18. Letter from A. Sterdis to the U.S. NRC dated May 26, 2007, re Westinghouse Application to Amend the AP1000 Design Certification Rule (DCP/NRC1912).
19. APP-GW-GL-700, Rev. 16, "AP1000 Design Control Document," May 2007.

20. Memorandum from M. Patterson to L. Mrowca re NRC Audit of the AP1000 PRA in Support of Design Certification Amendment (ADAMS Accession No. ML083230705).
21. APP-GW-GL-022, Rev. 8, “AP1000 Probabilistic Risk Assessment,” July 30, 2004.
22. SECY-89-012, “Staff Plans for Accident Management Regulatory and Research Programs,” January 18, 1989.
23. APP-GW-GLN-106, Rev. 1, “Mechanical System and Component Design Update” (TR-106).
24. APP-GW-GLR-060, “Reactor Vessel Insulation System—Verification of In-Vessel Retention Design Bases” (TR-24).
25. Letter from R. Sisk to the U.S. NRC dated July 22, 2008, re AP1000 Response to Requests for Additional Information (DCP/NRC2211) (ADAMS Accession No. ML082060194).
26. Letter from R. Sisk to the U.S. NRC dated August 21, 2008, re AP1000 Response to Requests for Additional Information (DCP/NRC2233) (ADAMS Accession No. ML082390117).
27. Letter from R. Sisk to the U.S. NRC dated September 5, 2008, re AP1000 Response to Requests for Additional Information (DCP/NRC2247) (ADAMS Accession No. ML082520821).
28. Letter from R. Sisk to the U.S. NRC dated November 6, 2008, re AP1000 Response to Requests for Additional Information (DCP/NRC2284) (ADAMS Accession No. ML083150689).
29. Letter from A. Sterdis to the U.S. NRC dated August 21, 2007, re AP1000 Response to Requests for Additional Information (DCP/NRC1977) (ADAMS Accession No. ML072350140).
30. Letter from A. Sterdis to the U.S. NRC dated August 23, 2007, re AP1000 Response to Requests for Additional Information (DCP/NRC1981) (ADAMS Accession No. ML072390023).
31. Letter from A. Sterdis to the U.S. NRC dated October 19, 2007, re AP1000 Responses to Requests for Additional Information (DCP/NRC2026) (ADAMS Accession No. ML072960049).
32. Letter from A. Sterdis to the U.S. NRC dated February 8, 2008, re AP1000 Responses to Requests for Additional Information (DCP/NRC2084) (ADAMS Accession No. ML080430077).