19.59 PRA RESULTS AND INSIGHTS

19.59.1 Introduction

This chapter summarizes the use of the AP600 PRA in the design process, PRA results and insights, plant features important to reducing risk, and PRA input to the design certification process.

AP600 is expected to achieve a higher standard of severe accident safety performance than currently operating plants, because both prevention and mitigation of severe accidents have been addressed during the design stage, taking advantage of PRA insights, PRA success criteria analysis, severe accident research, and severe accident analysis. Since PRA considerations have been integrated into the AP600 design process from the beginning, many of the traditional PRA insights relating to currently operating plants are not at issue for the AP600. The Level 1, Level 2, and Level 3 results show that addressing PRA issues in the design process leads to a low level of risk. The PRA results indicate that the AP600 design meets the higher expectations and goals for new generation passive pressurized water reactors (PWRs).

The core damage frequency (CDF) and large release frequency (LRF) for at-power internal events are extremely low, and meet the NRC safety goals with substantial margin. These frequencies are at least two orders of magnitude less than a typical pressurized water reactor plant currently in operation. This reduction in risk is due to many plant design features, with the dominant reduction coming from highly reliable and redundant passive safety-related systems that impact both at-power and shutdown risks. These passive systems are much less dependent on operator action and support systems than plant systems in currently operating plants.

The Level 3 analysis for at-power and shutdown events shows the potential offsite dose from a severe accident is very small and well within the established goals. The risk measured by the potential offsite dose does not increase significantly after the first 24 hours after a severe accident is assumed to cause a release to the environment.

Conservative, bounding fire and flood assessments show the core damage risk from these events is small compared to the core damage risk from at-power and shutdown events.

A synopsis of the insights gained from the PRA about the AP600 design includes:

- The AP600 design benefits from the high level of redundancy and diversity of the passive safety-related systems. The passive systems have been shown to be highly reliable, their designs are simple so that a limited number of components are required to function.

- AP600 is less dependent on nonsafety-related systems than current plants or advanced light water reactor evolutionary plants. When no credit is taken for nonsafety-related

systems following an accident, AP600 still meets the NRC safety goal, whereas current plants may not.

- The nonsafety-related support systems (ac power, component cooling water, service water, air) have a limited role in the plant risk profile because the passive safety-related systems do not require cooling water or ac power.

- AP600 is less dependent on human actions than current plants or advanced light water reactor evolutionary plants. Even when no credit is taken for operator actions, the AP600 meets the NRC safety goal, whereas current plants may not.

- The core damage and large release frequencies are low despite the conservative assumptions made in specifying success criteria for the passive systems. The success criteria have been developed in a more systematic, rigorous manner than typical PRA success criteria. The baseline success criteria are bounding cases for a large number of PRA success sequences. The baseline success sequences, in most cases, have been defined with:

  - worst (i.e., the most limiting) break size and location for a given initiating event
  - worst automatic depressurization system (ADS) assumption in the success criterion
  - worst number of core makeup tanks (CMT) and accumulators
  - worst containment conditions for in-containment refueling water storage tank (IRWST) gravity injection.

  Many less-limiting sequences are therefore represented by a baseline success criteria.

- Single system or component failures are not overly important due to the redundancy and diversity of safety-related systems in the design. For example, the following lines of defense are available for reactor coolant system (RCS) makeup:

  - chemical and volume control system
  - core makeup tanks
  - partial automatic depressurization system in combination with normal residual heat removal
  - full automatic depressurization system with accumulators and in-containment refueling water storage tank
  - full automatic depressurization system with core makeup tanks and in-containment refueling water storage tank

- Typical current PRA dominant initiating events are significantly less important for the AP600. For example, the reactor coolant pump (RCP) seal loss-of-coolant accident (LOCA) event has been eliminated as a core damage initiator since AP600 uses canned motor reactor coolant pumps which do not have seals. Another example is the loss of offsite power (LOOP) event. The station blackout and loss of offsite power event is a minor contributor to AP600 since the passive safety-related systems do not require the support of ac power.

- Passive safety-related systems are available in all shutdown modes. Planned maintenance of passive features is only performed during shutdown modes when that feature is not risk important. In addition, planned maintenance of nonsafety-related defense-in-depth features used during shutdown is performed at power.

- The AP600 passive containment cooling design is highly robust. Air cooling alone can prevent containment failure, although the design has other lines of defense for containment cooling such as fan coolers and passive containment cooling water.

- The potential for containment isolation and containment bypass is lessened by having fewer penetrations to allow fission product release. In addition, all normally open and risk important penetrations are fail-closed, thus eliminating the dependence on instrumentation and control (I&C) and batteries.

- The reactor vessel lower head has no vessel penetrations, thus eliminating penetration failure as a potential vessel failure mode. Preventing the relocation of molten core debris to the containment eliminates the occurrence of several severe accident phenomena, such as ex-vessel fuel-coolant interactions and core-concrete interaction, which may threaten the containment integrity. Therefore, AP600, through the prevention of core debris relocation to the containment, significantly reduces the likelihood of containment failure.

- The potential for the spreading of fires and floods to safety-related equipment is significantly reduced by the AP600 layout.

19.59.2 Use of PRA in the Design Process

The AP600 design has evolved over a period of years. PRA techniques have been used since the beginning in an iterative process to optimize the AP600 with respect to public safety. Each of these iterations has included:

- Development of a PRA model
- Use of the model to identify weaknesses
- Quantification of PRA benefits of alternate designs and operational strategies
- Adoption of selected design and operational improvements.

The scope and detail of the PRA model has increased from the early studies as the plant design has matured. This iterative design process has resulted in a number of design and

operational improvements. The use of PRA in the AP600 is presented in this section as five distinct stages including: conceptual design analysis (stages 1 and 2), PRA analysis as part of the design certification application (stage 3), and revisions of the PRA in support of further refinement of the design and modeling assumptions (stages 4 and 5).

19.59.2.1 Stage 1 - Use of PRA During the Early Design Stage

The initial AP600 design incorporated features that were intended to address leading causes of core damage and severe release, as identified from existing PRA studies, including the APWR (SP-90) and Sizewell. These features included passive safety-related core damage prevention and mitigation systems, active nonsafety-related systems, and other plant features. Passive safety-related core damage prevention systems are capable of mitigating PRA events, require no support systems other than instrumentation and control, and use equipment that fails in the safe position (i.e., the position that actuates or blocks the equipment, whichever is more safe) for the most common events. Passive system mitigative features included a reduced number of containment penetrations compared to currently operating plants, the penetrations that are open at power are fail-safe, improvement of the interfacing systems loss-of-coolant accident event, and hydrogen igniters in the containment. Other plant features factored into the initial design include a physical separation of electrical and instrumentation and control trains, reduction in the number of flooding sources, and a diverse actuation system (DAS) that provides diverse mitigation of anticipated transients without scram (ATWS) events, as well as diverse control functions.

Prior to 1989, several probabilistic scoping studies were performed on the AP600 conceptual design, which concentrated on quantifying the core damage frequency and large release frequency for internal initiating events during power operation. The early studies included detailed models of the passive safety-related fluid systems. They did not include detailed models of other systems such as instrumentation and control. The use of scoping studies was an iterative process at this stage of the design's evolution. Several feedback loops were included within the evaluation process: results and insights of a scoping study would identify areas of weakness, then alternative system designs and/or operational strategies were evaluated to optimize plant safety.

The outcome of the scoping study provided insights into the AP600 conceptual design, which led to many design and operational enhancements. Examples of design enhancements include:

- Originally the depressurization system consisted of three stages, each stage contained two lines with two normally closed motor-operated valves. An alternate design was then analyzed which included a fourth depressurization stage off the hot leg with valve types diverse from the first three stages.

- Diverse automatic actuation for certain safety-related functions was introduced. In addition, separate and diverse manual actuation for certain safety-related functions was provided. Specifically, the diverse actuation system was provided to automatically actuate passive residual heat removal (PRHR), core makeup tank, passive containment cooling system (PCS), reactor protection function, automatic depressurization, and

containment isolation. In addition, the diverse actuation system provides alarms and information to the main control room for manual actuation of these systems.

- The normal residual heat removal system (RNS) is a separate system from the spent fuel pool cooling system. The normal residual heat removal system, with piping routed outside of the containment, was designed with at least three isolation valves at each containment penetration to reduce the probability of interfacing systems loss-of-coolant accident events that result in containment bypass.

- Protection system logic modifications are adopted to preclude steam generator overfilling during a steam generator tube rupture (SGTR) event. This reduces the need for full reactor depressurization and, therefore, reduces the frequency of core damage for steam generator tube rupture events with the containment bypassed.

- The number of onsite power supplies was increased to two nonsafety-related diesel generators.

In addition to plant design changes, some changes to the success criteria were made. In the early stages of the PRA, the success criteria were primarily based on engineering judgement or preliminary design basis analyses. However, during the iterative process of this stage of the PRA, success criteria refinement was examined and computer simulations were run to investigate the plant response to various events. An example is the success criteria originally did not credit the accumulators for mitigation of a small loss-of-coolant accident event. Further examination of the response of the accumulators to small and medium loss-of-coolant accidents indicated that, if the core makeup tanks fail, the accumulators will inject and the core will be cooled provided the operators manually initiate the automatic depressurization system. Thus, the small and medium loss-of-coolant accident success criteria were enhanced.

Operational changes were also evaluated at this stage of the PRA.

19.59.2.2 Stage 2 - Preliminary PRA

Beginning in 1989, a preliminary PRA was conducted in support of the Westinghouse AP600 application for design certification. The preliminary PRA was performed on the AP600 design that existed at the time of completion of the scoping studies along with design changes made as a result of the final scoping study. The scope of the PRA was also expanded to evaluate both at-power and shutdown conditions as well as external events. Because the AP600 design was evolving throughout this period, the success criteria were primarily based on engineering judgement derived from preliminary design basis safety analyses. The system and component dependency analysis and the data used in the preliminary PRA were deliberately conservative. The results of the preliminary PRA identified important areas of the AP600 design where the design effort would focus. Examples of specific system design changes made during this stage of the PRA include:

- The in-containment refueling water storage tank system initially consisted of one line containing a normally closed motor-operated valve and two series check valves. To

improve the reliability of the injection phase of the system, a second parallel path of two check valves in series was added to the existing line. Additionally, the motor-operated valve was changed to be normally open, thus the system does not require the opening of a motor-operated valve, which would require an open signal, to initiate injection.

- To improve the reliability of the sump recirculation function, redundant and diverse recirculation valves were incorporated into the design. The AP600 conceptual design consisted of two parallel check valves from the sump. Diversity was modeled into the design by changing one of the check valves to a motor-operated valve; redundancy was incorporated by making each line contain two valves in series.

- Alarms are provided in the main control room to inform the operator of mispositioned isolation valves of the passive core cooling system (PXS) that have remote manual control capability. This reduces the probability of valve mispositioning.

In the first stage of the PRA, the success criteria were primarily based on engineering judgement. For this stage of the PRA, the success criteria were refined. Examples of more refined success criteria include:

- The more significant success criteria change related to the depressurization system. The original success criterion for a small loss-of-coolant accident was one-half of all the automatic depressurization system stages were required. Taking credit for a design change that increased the size of the fourth-stage valves and performing best-estimate loss-of-coolant accident calculations allowed the use of a success criteria that tolerated multiple failures.

- Analysis shows that the containment cooling system only requires air cooling to prevent containment failure.

Operational changes were also made as part of this stage of the PRA. The normal residual heat removal system and automatic depressurization system provide some examples of operational changes.

- Initiation of the normal residual heat removal system initially required the operators to first decide if it was appropriate to actuate normal residual heat removal system following depressurization. To start the normal residual heat removal system, it was necessary for the operators to locally open three valves. To reduce the operator's burden as to when it was appropriate to actuate normal residual heat removal, an operation change was made so that the operator initiates the system whenever automatic depressurization system is actuated, with the exception of cases when radiation could leak out of containment. Additionally, the system can now be manually actuated from the main control room instead of using local manual actuation.

- As an outcome of the scoping PRA stage, the automatic depressurization system stage 1, 2, and 3 valve configuration was changed from two normally closed valves to

one valve open and one valve closed in each line to improve reliability. Further evaluation of this configuration showed that the potential for spurious actuation of the automatic depressurization system had increased. Thus, during the preliminary PRA stage, the automatic depressurization system valve configuration was changed to two closed valves with quarterly testing.

19.59.2.3 Stage 3 - AP600 PRA Submittal to NRC (1992)

The third stage culminated with the submittal of the AP600 PRA report, along with the *AP600 Standard Safety Analysis Report* (SSAR), to the NRC on June 26, 1992. This stage included a complete Level 3 PRA. The PRA factored in design changes made as a result of the preliminary PRA findings. The success criteria assumptions were verified. Some of the conservative data and dependency factors were adjusted to be more realistic during this stage. The outcome of the PRA program, which was characterized by frequent interactions between PRA analysts and design engineers, is an AP600 design that exceeds the NRC safety goals.

Because of the extensive interactions during previous design/PRA studies, few plant changes resulted from this study. Two design changes that did result include:

- The core makeup tank can now be actuated on a low steam generator level plus high hot leg temperature indication. This was done to indirectly reduce the importance of operator actions to initiate passive feed and bleed.

- The scope of the diverse actuation system was expanded to include control rod insertion. The system was also expanded to include an actuation signal for opening of the in-containment refueling water storage tank motor-operated valves during mid-loop operations. This was done to provide automatic operation to reduce the dependence on operators to open the valves in the event of an accident during mid-loop operation.

19.59.2.4 Stage 4 - PRA Report Revision 1 (1994)

Stage 4 was the first revision to the AP600 PRA report. The revision, submitted in July 1994, included the following major changes: introduction of phenomenology into the Level 2 containment event tree and performance of the risk-based seismic margins analysis. In addition to Revision 1 of the PRA, this stage also included the focused PRA sensitivity study and initiating event evaluation as part of the regulatory treatment of nonsafety-related systems (RTNSS) topic.

In September 1993, the focused PRA sensitivity study and initiating event evaluation were submitted to the NRC via WCAP-13856, "AP600 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process", (Reference 19.59-1). The focused PRA sensitivity study evaluated the core damage and large release frequencies for AP600 without taking mitigation credit for nonsafety-related systems. The results of the study show that even with no credit taken for nonsafety-related systems, AP600 meets the regulatory goals.

The Level 2 PRA was revised to introduce the analysis and incorporation of important phenomena onto the containment event tree. Six phenomena were analyzed:

- In-vessel retention of molten core debris
- Thermally induced failures of the reactor coolant system pressure boundary
- In-vessel steam explosion
- Ex-vessel steam explosion
- Ex-vessel debris coolability
- Hydrogen combustion analysis.

A containment event tree displays the characteristics of the severe accident progression that impact the fission-product source term to the environment. The containment event tree from the Stage 3 PRA that was submitted to the NRC in 1992 was enhanced to include the phenomena that were analyzed.

A risk-based seismic margins analysis was also performed as part of Revision 1 of the AP600 PRA.

There were no appreciable changes in the plant design as a result of this stage of the PRA.

19.59.2.5 Stage 5 - PRA Report Revisions 2 - 13 (1995-1998)

This stage includes the updates leading to various report revisions submitted to the NRC during 1995 through 1998. The changes made to the PRA report resulted from plant changes and NRC questions. Most plant changes incorporated into the PRA report were made for other reasons than the PRA analysis and results. The design changes resulted in small changes to the core damage and large release frequencies. The primary emphasis of this stage of the PRA was to assess and incorporate, as appropriate, plant changes, and refine the success criteria calculations and the system and event tree modeling. Some of the changes to the PRA are summarized below.

- Further refinement of the PRA success criteria calculations resulted in making the automatic depressurization system success criteria more conservative.

- The automatic depressurization system stage 4 valves were changed from air-operated to explosive-operated (squib) valves. This design change was not PRA-motivated; however, a PRA sensitivity study was performed to provide input into the decision to change the fourth-stage valves to squib valves.

- Service water blowdown procedures and sources of makeup water were evaluated as a function of service water heat loads during various plant conditions to ensure that the assumed success criteria will be met. The heat loads were also evaluated to assess the required number of cooling tower fans that must operate to ensure adequate cooling. In addition, the initial evaluation indicated a potential vulnerability to bypass flow occurring upon loss of a dc power supply causing an air-operated valve to open. Consequently, the power supplies to the equipment were reevaluated.

- Initial PRA modeling of the need to open the main generator breaker in the fault trees for the 4160 vac buses following a plant trip highlighted the importance of certain functions initially assumed to be performed by the plant control system. It was determined that the plant control system would not be fast enough to perform this action and that a reverse power relay would control opening this breaker.

- Squib valves were added to the in-containment refueling water storage tank injection and recirculation lines. This design change improved the environment for the check valves in the in-containment refueling water storage tank injection and recirculation lines.

- The automatic actuation of the squib valves in the in-containment refueling water storage tank injection lines is from the core makeup tank level instrumentation. This increased the importance of the core makeup tank level instrumentation and the instrument and control system that performs the actuation.

- The automatic actuation of the squib valves in the recirculation lines is from the in-containment refueling water storage tank level instrumentation. This increased the importance of the in-containment refueling water storage tank level instrumentation and the instrument and control system that performs the actuation.

- The passive residual heat removal system was changed from two heat exchangers to one heat exchanger. This had a very small effect on the reliability of the passive residual heat removal system.

- The PXS valve/accumulator room exits on the maitenance floor were relocated to mitigate overtemperature of the containment wall and electrical penetrations from postulated diffusion flames.

- The reactor vessel reflective insulation design was modified to promote the in-vessel retention of core debris by providing an engineered pathway for water cooling of the reactor vessel external surface.

19.59.3 Core Damage Frequency from Internal Initiating Events at Power

Internal initiating events are transient and accident initiators that are caused by plant system, component, or operator failures. External initiating events, which include internal fire and flooding events, and events at shutdown are discussed in other subsections.

The AP600 mean plant core damage frequency for internal initiating events at power is extremely low. Twenty-six separate initiating event categories were defined to accurately represent the AP600. Of these event categories, 11 are loss-of-coolant accidents (LOCAs), 12 are transients, and 3 are anticipated transients without scram precursors (initiating events that result in an anticipated transient without scram sequence as a result of failure to trip the reactor). Initiating event categories unique to the AP600 have been defined and evaluated,

including safety injection line breaks, core makeup tank line breaks, and passive residual heat removal heat exchanger (HX) tube ruptures.

The contribution of initiating events to the total plant core damage frequency is summarized in Table 19.59-1. Figure 19.59-1 illustrates the relative contributions to core damage frequency from the various at-power initiating events. Table 19.59-2 shows the conditional core damage probability of the initiating events. The conditional core damage probability listed in Table 19.59-2 is the ratio of the core damage frequency contribution for an initiating event divided by the initiating event frequency.

Eight initiating events, including six loss-of-coolant accidents, one anticipated transient without scram precursor, and steam generator tube rupture, make up approximately 90 percent of the total at-power plant core damage frequency. The remaining initiating events contribute a total of approximately 8 percent to the core damage frequency from internal events. The dominant initiating events are:

- Large loss-of-coolant accident
- Safety (direct vessel) injection (SI) line break
- Intermediate loss-of-coolant accident
- Reactor vessel rupture
- Anticipated transient without scram precursor with loss of main feedwater
- Medium loss-of-coolant accident
- Steam generator tube rupture
- Small loss-of-coolant accident

The first three events account for a majority of the total core damage frequency. Reactor vessel rupture and anticipated transient without scram with loss of main feedwater events contribute a smaller percentage to the core damage frequency.

The results show a very low core damage frequency dominated by rare events (i.e., intermediate, medium, and large loss-of-coolant accidents, and anticipated transients with failure of reactor trip). This indicates that the AP600 design is robust with respect to its ability to withstand challenges from more frequent events (e.g., transients) and that adequate protection against the more severe events is provided through the defense-in-depth features.

For the PRA, the various loss-of-coolant accident categories have been defined based on which plant features are required to mitigate the events. As a result, the PRA and Chapter 15 loss-of-coolant accident size definitions are not identical. The following listing shows how the PRA and Chapter 15 break sizes are related and identifies the PRA size criteria.

- Chapter 15 break size definitions are large or small.

- PRA break sizes are defined as follows:

  - Large breaks -- Reactor vessel rupture is included in this category. The automatic depressurization system is not required for in-containment refueling water storage

tank injection for large breaks. For large breaks that are slightly larger than a medium break, there is a potential effect of containment isolation upon in-containment refueling water storage tank injection. The success criteria include automatic depressurization system in these cases.

- Medium breaks -- Core makeup tank line breaks and safety (direct vessel) injection line breaks are included in this category. Automatic depressurization system actuation is not required for normal residual heat removal system (RNS) operation for medium breaks, but is required for in-containment refueling water storage tank injection.

- Intermediate breaks -- Operation of automatic depressurization system stages 1, 2, or 3 (or, alternatively, passive residual heat removal) is not required to satisfy the automatic depressurization system stage 4 automatic actuation pressure interlock, but is required to depressurize the reactor coolant system to the normal residual heat removal system operating pressure.

- Small breaks -- Steam generator tube rupture and passive residual heat removal heat exchanger tube rupture break sizes fall within this range, but are evaluated as separate events based on differing initial plant response. Small breaks are larger than those for which the chemical and volume control system (CVS) can maintain reactor coolant system water level, but not large enough to allow automatic actuation of automatic depressurization system stage 4 without operation of either automatic depressurization system stages 1, 2, or 3 or passive residual heat removal.

- Coolant losses smaller than those resulting from small breaks are defined as reactor coolant system leaks. Operation of one chemical and volume control system makeup pump can maintain reactor coolant system water inventory for reactor coolant system leaks.

19.59.3.1 Dominant Core Damage Sequences

Over 400 potential core damage event sequences for internal initiating events at power are modeled in the AP600 PRA. These core damage sequences are the combinations of initiating event occurrences and subsequent successes and failures of plant systems and operator actions that result in core damage. Some of these sequences are composite sequences; that is, they consist of similar event sequences that are combined and analyzed together (such as consequential steam generator tube rupture resulting from various initiators). Therefore, a larger number of sequences are actually represented by the model.

The 19 dominant sequences are given in Table 19.59-3.

The dominant accident sequences that contribute over 90 percent of the core damage frequency from internal initiating events at power are discussed in this section. These sequences are listed in Table 19.59-3.

Sequence 1: Safety (Direct Vessel) Injection Line Break (SI-LB-02)

Description of Sequence

The initiating event is a break that occurs in one of the two safety (direct vessel) injection lines, resulting in a loss of reactor coolant. All capability for reactor coolant system injection from the core makeup tank and in-containment refueling water storage tank through this broken line is postulated to be lost due to excessive spillage through the break, but core makeup tank injection through the intact line is successful. Full reactor coolant system depressurization; that is, depressurization to the pressure at which gravity injection can occur, is successful through the operation of the automatically or manually actuated automatic depressurization system. However, in-containment refueling water storage tank injection through the intact line fails, and normal residual heat removal injection is assumed to be unavailable as a result of the break location.

Core damage is postulated due to reactor coolant loss through the break and the open automatic depressurization system valves, with subsequent lack of capability to maintain reactor coolant system inventory due to failure of injection through the intact in-containment refueling water storage tank line. Core damage will be delayed, since core makeup tank injection is successful; accumulator injection is expected due to success of full automatic depressurization system depressurization, but its status is not evaluated in this sequence, since core damage would not be prevented without gravity injection.

Some important modeling assumptions include the following:

- It is assumed that the break is large enough to cause one injection path to fail due to excessive spillage of the injected water. If a smaller break were to occur, the loss through the break, and also the spillage of the injected water through the break would be less than the total loss of the injection path.

- The size of the break can range from small to medium loss-of-coolant accidents. For this analysis, a medium loss-of-coolant accident is conservatively postulated.

- No credit is given for operation of normal residual heat removal following successful depressurization of the reactor coolant system because it is assumed the system would not effectively provide injection flow through the intact direct vessel injection line due to the normal residual heat removal system piping configuration.

Risk-Important Failures

The dominant cutsets for this sequence show that the risk-important failure is dominated by plugging of the in-containment refueling water storage tank discharge line strainer in the intact line. This is followed by common cause and random failure of squib valves or both check valves on the intact in-containment refueling water storage tank discharge line.

Sequence 2: Intermediate Loss-of-Coolant Accident (NLOCA-03)

Description of Sequence

This is an intermediate loss-of-coolant accident initiating event. After the break occurs, a core makeup tank injection signal is generated, either one or both core makeup tanks actuate, the reactor coolant pumps trip, and the core makeup tanks inject when required. Full reactor coolant system depressurization (i.e., depressurization to the point at which in-containment refueling water storage tank injection can occur) using the automatic depressurization system valves is successful, but the normal residual heat removal system fails to inject. In-containment refueling water storage tank injection is successful through at least one of the two injection lines. However, sump recirculation fails after the in-containment refueling water storage tank is depleted.

Core damage is postulated due to the failure to make up reactor coolant system inventory from both long-term sources (normal residual heat removal system and sump recirculation) after the core makeup tank has injected.

Risk-Important Failures

The dominant contributor to this sequence is common cause failure of four squib valves in recirculation lines to open. This is followed by: (1) common cause failure of in-containment refueling water storage tank level transmitters, and (2) operator failure to manually actuate sump recirculation, after automatic actuation fails.

Sequence 3: Large Loss-of-Coolant Accident (LLOCA-06)

Description of Sequence

This sequence is a large loss-of-coolant accident initiating event with a break size in the upper end of the break spectrum, followed by successful injection by one or more accumulators, but failure of in-containment refueling water storage tank injection from both lines, including the automatic actuation failures due to failure to actuate core makeup tanks. Core damage is postulated due to in-containment refueling water storage tank injection failure, after which it is assumed that the loss of reactor coolant system inventory cannot be made up in time to prevent core damage. After the accumulators are fully injected, the reactor coolant system water level will keep dropping due to boiloff and losses through the break.

An important modeling assumption is that no credit is taken for operator actions to actuate core makeup tank or in-containment refueling water storage tank injection because of the short time in which these actions would have to be accomplished.

Risk-Important Failures

The dominant failures for this sequence are the following:

- Common cause hardware failure of the protection and safety monitoring system engineered safety feature input logic groups, which fails core makeup tank, and thus in-containment refueling water storage tank, actuation
- Common cause failure of core makeup tank level sensors, which prevents in-containment refueling water storage tank actuation
- Common cause failures of core makeup tank air-operated valves and check valves
- Common cause failures of in-containment refueling water storage tank injection squib and check valves, or strainer plugging in the in-containment refueling water storage tank

Sequence 4: Large Loss-of-Coolant Accident (LLOCA-03)

Description of Sequence

This sequence is a large loss-of-coolant accident initiating event with a break size in the lower end of the break spectrum, followed by successful injection by one or more accumulators and successful containment isolation. In-containment refueling water storage tank injection from both lines fails, including the automatic actuation failures due to failure to actuate core makeup tanks. Core damage is postulated due to in-containment refueling water storage tank injection failure, after which it is assumed that the loss of reactor coolant system inventory cannot be made up in time to prevent core damage. After the accumulators are fully injected, the reactor coolant system water level will keep dropping due to boiloff and losses through the break.

Risk-Important Failures

The dominant failures for this sequence are the following:

- Common cause hardware failure of the protection and safety monitoring system engineered safety feature input logic groups, which fails core makeup tank, and thus in-containment refueling water storage tank, actuation
- Common cause failure of core makeup tank level sensors, which prevents in-containment refueling water storage tank actuation
- Common cause failures of core makeup tank air-operated valves and check valves
- Common cause failures of in-containment refueling water storage tank injection squib and check valves, or strainer plugging in the in-containment refueling water storage tank

Sequence 5: Reactor Vessel Rupture (RV-RP-02)

Description of Sequence

A reactor vessel rupture event occurs. This event is defined as a vessel break of a size and location such that the core cannot be kept covered with water. Core damage is postulated as a direct result of the initiating event.

A modeling assumption for this sequence is that the safety systems cannot keep the core covered after the event occurs.

Risk-Important Failures

The initiating event frequency is the only risk-important failure. There are no operator actions modeled. The only cutset for this event (Table 19.59-8) is the occurrence of the initiating event.

Sequence 6: Large Loss-of-Coolant Accident (LLOCA-11)

Description of Sequence

A large loss-of-coolant accident initiating event occurs. Both accumulators fail to inject. Core damage is postulated due to core uncovery as a result of failure of accumulator injection; core damage occurs before in-containment refueling water storage tank injection can reflood the core. No credit is taken for core makeup tank injection.

An important modeling assumption is that no credit is taken for core makeup tank injection. Core makeup tank injection is expected, but compared to the flow from the accumulators, the core makeup tank flow is too slow to have an appreciable effect and prevent core damage for this event. Core damage is assumed to occur solely on the failure of accumulators. This is conservative, since it is expected that core makeup tank injection would be effective for breaks at the smaller end of the size range defined for large loss-of-coolant accidents in the PRA.

Risk-Important Failures

Common cause failure of the accumulator check valves to open is the dominant failure mode. This is followed by various combinations of random failure of two check valves to open.

Sequence 7: Anticipated Transient Without Scram Precursor (Loss of Normal Feedwater with Failure of Reactor Trip) (ATWS-28)

Description of Sequence

This sequence encompasses all combinations of failures on the anticipated transient without scram/loss of main feedwater precursor event tree that do not lead directly to success or to core damage, and for which further evaluation of plant response is modeled in the event tree. There are several scenarios encompassed by this sequence:

- Failure of reactor trip as a result of failure of the protection and safety monitoring system trip signal, success of the diverse actuation system trip signal, but failure of the control rod motor-generator set breakers to open

- Successful protection and safety monitoring system trip signal generation, failure of the reactor trip breakers to open, and failure of the diverse actuation system reactor trip signal

- Successful protection and safety monitoring system trip signal generation, failure of the reactor trip breakers to open, successful diverse actuation system trip signal generation, but failure of the control rod motor-generator sets to trip. In each scenario, both automatic and manual actuations are modeled for the protection and safety monitoring system and diverse actuation system

Following failure to trip the reactor, heat removal by either startup feedwater or passive residual heat removal is successful. The operators fail to actuate the rod control system (via the plant control system (PLS)) so that the control rods fail to step into the core. This leads to a heatup and pressurization of the reactor coolant system. Reactor coolant system pressure relief fails as a result of either failure of one or both of the pressurizer safety valves to open, or as a result of the occurrence of the event early in the fuel cycle, during which the core reactivity feedback is not adequate to prevent reactor coolant system heatup in excess of the safety valve relief capacity.

Core damage is postulated due to an assumed high pressure and due to lack of analysis. It is likely that a break would occur in the primary side due to the high pressure. This break would eventually relieve the high reactor coolant system pressure, allowing operation of the various mitigation systems.

Some important modeling assumptions include the following:

- There is a period of time at the beginning of each cycle during which core reactivity feedback is not sufficient to prevent overpressurization of the reactor coolant system given a loss-of-normal-feedwater anticipated transient without scram. However, if the operators can initiate the stepping in of the control rods within a short time interval after the event occurs, sufficient negative reactivity will be inserted to eliminate the

concern that the capacity of the safety valves is exceeded due to insufficient reactivity feedback.

- If reactor coolant system pressure approaches or exceeds 3200 psi, core damage is assumed; no credit for loss-of-coolant accident mitigating systems is assumed.

- The time available for operator actions to trip the reactor is short for the loss-of-normal-feedwater anticipated transient without scram.

Risk-Important Failures

The dominant cutsets for this sequence indicate that the following failures are risk-important in this sequence:

- Failure of reactor coolant system depressurization
- Failure to deenergize the control rod motor-generator sets
- Common cause failure of protection and safety monitoring system hardware
- Common cause failure of reactor trip breakers to open

Three operator actions are important to success for this sequence. These are:

- Operator actuation of reactor trip via the protection and safety monitoring system

- Operator actuation of reactor trip (motor-generator set trip) by the diverse actuation system

- Operator actuation of control rod insertion via the plant control system

Sequence 8: Medium Loss-of-Coolant Accident (MLOCA-03)

Description of Sequence

A medium loss-of-coolant initiating event occurs. One or more core makeup tanks inject into the reactor coolant system, but the normal residual heat removal system fails. Reactor coolant system depressurization via the automatic depressurization system stage 4 valve operation and in-containment refueling water storage tank injection are successful. Sump recirculation fails. Core damage is postulated due to the inability to provide long-term reactor coolant system inventory makeup and core cooling following the failures of normal residual heat removal system and sump recirculation

Some important modeling assumptions for this sequence include:

- Credit is taken for manual actuation of the normal residual heat removal system in injection mode, followed by gravity recirculation, for successful termination of the event. However, sump recirculation fails in this sequence.

- According to the definition of medium loss-of-coolant accident, operation of the automatic depressurization system is not required in order to reach normal residual heat removal system operating pressure. However, automatic depressurization system operation is required to allow in-containment refueling water storage tank injection following normal residual heat removal system failure.

Risk-Important Failures

Table 19.59-11 lists the dominant cutsets for this sequence. The dominant risk-important failure is the common cause failure to open of squib valves on the recirculation lines. This is followed by common cause failure of in-containment refueling water storage tank level transmitters and operator action to open sump recirculation valves.

Sequence 9: Anticipated Transient Without Scram Precursor (Loss of Normal Feedwater with Failure of Reactor Trip) (ATWS-13)

Description of Sequence

This sequence encompasses all combinations of failures on the anticipated transient without scram/loss of main feedwater precursor event tree that do not lead directly to success or to core damage, and for which further evaluation of plant response is modeled in the event tree. There are several scenarios encompassed by this sequence:

- Failure of reactor trip as a result of failure of the protection and safety monitoring system trip signal, with success of the diverse actuation system trip signal, but failure of the control rod motor-generator set breakers to open.

- Successful protection and safety monitoring system trip signal generation, failure of the reactor trip breakers to open, and failure of the diverse actuation system reactor trip signal.

- Successful protection and safety monitoring system trip signal generation, failure of the reactor trip breakers to open, successful diverse actuation system trip signal generation, but failure of the control rod motor-generator sets to trip. In each scenario, both automatic and manual actuations are modeled for protection and safety monitoring system and diverse actuation system.

Following failure to trip the reactor, heat removal by either startup feedwater or passive residual heat removal is successful. The operators successfully actuate the rod control system (via plant control system) so that the control rods step into the core. However, manual boration by the chemical and volume control system (CVS) and core makeup tank injection fail. Thus, reactor coolant system inventory losses are not made up, and the long-term criticality control by boration is not established.

Some important modeling assumptions for this sequence include:

- Successful automatic depressurization system actuation, coupled with normal residual heat removal system or in-containment refueling water storage tank injection, may be able to successfully terminate the accident. However, core damage is conservatively assigned.

- The time available for operator action to trip the reactor is short for the loss of normal feedwater anticipated transient without scram.

Risk-Important Failures

In addition to the failures leading to the failure of the reactor trip, the common cause failures of various sensors in reactor coolant system are dominant contributors to this sequence.

Two operator actions are important to success for this sequence. These are:

- Operator actuation of reactor trip via the protection and safety monitoring system

- Operator actuation of reactor trip (motor-generator set trip) by the diverse actuation system

Sequence 10: Intermediate Loss-of-Coolant Accident (NLOCA-04)

Description of Sequence

This is an intermediate loss-of-coolant accident initiating event. After the break occurs, a core makeup tank injection signal is generated, either one or both core makeup tanks actuate, the reactor coolant pumps trip, and the core makeup tanks inject when required. Full reactor coolant system depressurization (i.e., depressurization to the point at which in-containment refueling water storage tank injection can occur) using the automatic depressurization system valves is successful, but both the normal residual heat removal system and the in-containment refueling water storage tank fail to inject.

Core damage is postulated due to the failure to make up reactor coolant system inventory from both long-term sources (normal residual heat removal system and in-containment refueling water storage tank) after the core makeup tank has injected

Risk-Important Failures

The dominant cutsets for this sequence are provided in Table 19.59-13. The dominant failure is common cause failure of the check valves or squib valves in both in-containment refueling water storage tank injection lines to open. The following are much lower contributors: (1) normal residual heat removal system isolation motor-operated valves (MOVs) 011, 022, or 023 fail to open due to hardware failure, (2) normal residual heat removal system check

valves 15A and 15B fail to open by common cause, and (3) common cause plugging of strainers in the in-containment refueling water storage tank.

Sequence 11: Safety (Direct Vessel) Injection Line Break (SI-LB-03)

Description of Sequence

The initiating event is a break that occurs in one of the two safety (direct vessel) injection lines, resulting in a loss of reactor coolant. All capability for reactor coolant system injection from the core makeup tank and in-containment refueling water storage tank through this broken line is postulated to be lost due to excessive spillage through the break, but core makeup tank injection through the intact line is successful. Full reactor coolant system depressurization (that is, depressurization to the pressure at which gravity injection can occur) fails.

Core damage is postulated due to the inability to inject in-containment refueling water storage tank water into the core after the core makeup tank inventory is depleted, because, without automatic depressurization system operation, the reactor coolant system pressure remains above the pressure at which in-containment refueling water storage tank injection can occur.

Some important modeling assumptions for this seqeunce include:

- It is assumed that the break is large enough to cause one injection path to fail due to excessive spillage of the injected water. If a smaller break were to occur, the loss through the break, and also the spillage of the injected water through the break would be less than a total loss of the injection path.

- The size of the break can range from small to medium loss-of-coolant accident. For this analysis, medium loss-of-coolant accident is postulated.

- It has been conservatively assumed that the break occurs in the line to which the normal residual heat removal system is connected. Thus, no credit is given for operation of normal residual heat removal following successful depressurization of the reactor coolant system.

Risk-Important Failures

The dominant failure is the common cause failure of the automatic depressurization system squib valves to open after an actuation signal is received.

Sequence 12: Small Loss-of-Coolant Accident (SLOCA-03)

Description of Sequence

A small loss-of-coolant initiating event occurs. One or more core makeup tanks inject into the reactor coolant system, and passive residual heat removal and the automatic depressurization system are successful. Normal residual heat removal fails and reactor coolant system inventory makeup by in-containment refueling water storage tank gravity injection is successful. Sump recirculation fails. Core damage is postulated due to the inability to provide long-term reactor coolant system inventory makeup and core cooling following failures of the normal residual heat removal system and sump recirculation.

An important modeling assumption is that credit is taken for manual actuation of the normal residual heat removal system in injection mode, followed by gravity recirculation, for successful termination of the event. However, sump recirculation fails in this sequence.

Risk-Important Failures

The dominant risk-important failure is the common cause failure to open of squib valves on recirculation lines. This is followed by common cause failure of in-containment refueling water storage tank level transmitters and operator action to open sump recirculation valves.

Sequence 13: Core Makeup Tank Line Break Accident (CMTLB-03)

Description of Sequence

A core makeup tank line break initiating event occurs. The intact core makeup tank injects into the reactor coolant system, but the normal residual heat removal system fails. Reactor coolant system depressurization, via automatic depressurization system stage 4 valve operation, and in-containment refueling water storage tank injection are successful. Sump recirculation fails. Core damage is postulated due to the inability to provide long-term reactor coolant system inventory makeup and core cooling following failures of the normal residual heat removal system and sump recirculation.

Some important modeling assumptions for this sequence include:

- Credit is taken for manual actuation of the normal residual heat removal system in injection mode (although the system hardware causes a failure). However, sump recirculation fails in this sequence.

- According to the definition of core makeup tank line break (medium loss-of-coolant accident size), operation of the automatic depressurization system is not required to reach normal residual heat removal system operating pressure. However, automatic depressurization system operation is required to allow in-containment refueling water storage tank injection following normal residual heat removal system failure.

Risk-Important Failures

The dominant risk-important failure is the common cause failure to open of squib valves on recirculation lines. This is followed by common cause failure of in-containment refueling water storage tank level transmitters and operator action to open sump recirculation valves.

Sequence 14: Steam Generator Tube Rupture Accident (SGTR-07)

Description of Sequence

A steam generator tube rupture initiating event occurs. Due to failures in nonsafety systems, such as startup feedwater or chemical and volume control systems, or failure to identify and isolate the faulted steam generator, the event continues as a challenge to passive core cooling systems, similar to that of a small loss-of-coolant accident event. One or more core makeup tanks inject into the reactor coolant system, and passive residual heat removal is successful. The automatic depressurization system fails and the pressurized reactor coolant system loses inventory through the break into the secondary side. The reactor coolant system inventory loss cannot be made up after the core makeup tanks inject, although the decay heat is being removed by the passive residual heat removal heat exchanger. Core damage is postulated due to the inability to provide long-term reactor coolant system inventory makeup.

The success criteria for this sequence are very conservative. This sequence may not be a core damage sequence since the decay heat is being removed by the passive residual heat removal and reactor coolant system inventory loss is made up by the core makeup tanks for a considerable time period. The loss of reactor coolant is expected to be stopped when passive residual heat removal cooling lowers the reactor coolant system pressure, thus terminating the loss-of-coolant accident and the need for automatic depressurization system and gravity injection.

Risk-Important Failures

The dominant risk-important failure is the common cause failure of protection and safety monitoring system engineered safety feature output logic software and manual diverse actuation system actuation. This is followed by various protection and safety monitoring system actuation common cause failures.

Credit is taken for the proceduralized operator action to manually actuate safety-related core cooling systems by using the diverse actuation system, if protection and safety monitoring system actuation fails.

Sequence 15: Steam Generator Tube Rupture Accident (SGTR-23)

Description of Sequence

A steam generator tube rupture initiating event occurs. Due to failures in nonsafety systems, such as startup feedwater or chemical and volume control systems, or failure to identify and isolate the faulted steam generator, the event continues as a challenge to passive core cooling systems, similar to that of a small loss-of-coolant accident event. One or more core makeup tanks are actuated to inject into the reactor coolant system, and passive residual heat removal is successful. However, reactor coolant pumps fail to trip and this is assumed to prevent core makeup tanks from injecting. The automatic depressurization system fails and the pressurized reactor coolant system loses inventory through the break into the secondary side. The reactor coolant system inventory loss cannot be made up, although the decay heat is being removed by the passive residual heat removal heat exchanger. Core damage is postulated due to the inability to provide long-term reactor coolant system inventory makeup.

The success criteria for this sequence are very conservative. This sequence may not be a core damage sequence since the decay heat is being removed by the passive residual heat removal heat exchanger and the reactor coolant pumps would be tripped eventually to allow core makeup tank injection. Then, this sequence would behave like the previously discussed steam generator tube rupture (SGTR-07) sequence.

Risk-Important Failures

The dominant risk-important failure is the common cause failure of reactor coolant pump breakers to open and operator to manually actuate the automatic depressurization system via the protection and safety monitoring system or diverse actuation system.

Credit is taken for the proceduralized operator action to manually actuate safety-related core cooling systems by using the diverse actuation system, if protection and safety monitoring system actuation fails.

Sequence 16: Large Loss-of-Coolant Accident (LLOCA-02)

Description of Sequence

This sequence is a large loss-of-coolant accident initiating event with a break size in the upper end of the break spectrum, followed by successful injection by one or more accumulators, and successful in-containment refueling water storage tank injection. However, sump recirculation fails. Core damage is postulated due to sump recirculation failure. After the in-containment refueling water storage tank is fully injected, the reactor coolant system water level will keep dropping due to boiloff and losses through the break.

Risk-Important Failures

The dominant failures for this sequence are: (1) common cause hardware failure of recirculation squib valves to open, (2) plugging of sump screens, and (3) common cause failure of in-containment refueling water storage tank level sensors and operator action to actuate sump recirculation.

Sequence 17: Large Loss-of-Coolant Accident (LLOCA-05)

Description of Sequence

This sequence is a large loss-of-coolant accident initiating event with a break size in the lower end of the break spectrum. The containment isolation is successful and is followed by successful injection by one or more accumulators, and successful in-containment refueling water storage tank injection. However, sump recirculation fails. Core damage is postulated due to sump recirculation failure. After the in-containment refueling water storage tank is fully injected, the reactor coolant system water level will keep dropping due to boiloff and losses through the break.

Risk-Important Failures

The dominant failures for this sequence are: (1) common cause hardware failure of recirculation squib valves to open, (2) plugging of sump screens, and (3) common cause failure of in-containment refueling water storage tank level sensors and operator action to actuate sump recirculation.

Sequence 18: Consequential Steam Generator Tube Rupture Accident (SGTRC-03)

Description of Sequence

A consequential steam generator tube rupture initiating event occurs. The starting point of this event may be a transient or a secondary line break (or a stuck-open secondary-side valve). One or more core makeup tanks inject into the reactor coolant system, and passive residual heat removal and the automatic depressurization system are successful. Normal residual heat removal fails and reactor coolant system inventory makeup by in-containment refueling water storage tank gravity injection is successful. Sump recirculation fails. Core damage is postulated due to the inability to provide long-term reactor coolant system inventory makeup and core cooling following failures of the normal residual heat removal system and sump recirculation.

It is important to note that this sequence may not be a core damage sequence since the decay heat is being removed by passive residual heat removal and reactor coolant system inventory loss is made up. The loss of reactor coolant is expected to be stopped, thus terminating the

loss-of-coolant accident and the need for sump recirculation, due to low reactor coolant system pressure terminating the break flow.

Risk-Important Failures

The dominant risk-important failure is the common cause failure to open of squib valves on recirculation lines. This is followed by common cause failure of in-containment refueling water storage tank level transmitters and operator action to open sump recirculation valves.

Sequence 19: Intermediate Loss-of-Coolant Accident (NLOCA-16)

Description of Sequence

An intermediate loss-of-coolant accident initiating event occurs. After the break occurs, a core makeup tank injection signal is generated, but one or more reactor coolant pumps fails to trip; this failure is assumed to prevent effective core makeup tank injection. Both full reactor coolant system depressurization (i.e., depressurization via the automatic depressurization system valves to the pressure at which in-containment refueling water storage tank injection can occur) and partial depressurization (i.e., depressurization via the automatic depressurization system to the pressure at which normal residual heat removal injection can occur) fail.

Core damage is postulated due to the inability to provide reactor coolant system injection. Failure of the reactor coolant pump trip prevents core makeup tank injection, and failure of the automatic depressurization system prevents injection from both normal residual heat removal and the in-containment refueling water storage tank in time to prevent core damage.

Some important modeling assumptions for this sequence include:

- Core makeup tank injection is assumed to fail as a result of failure of reactor coolant pump trip.

- In this sequence, no credit is taken for automatic depressurization system actuation, as a result of the failure of core makeup tank injection.

Risk-Important Failures

Risk-important component failures are related to failure of reactor coolant pumps to trip; specifically, (1) common cause failure to open the reactor coolant pump breakers, and (2) common cause failure of core makeup tank air-operated valves or check valves to open

Selected operator actions are important in this sequence because failure of core makeup tank injection prevents automatic actuation of the automatic depressurization system on low core makeup tank level. Failure of the protection and safety monitoring system-related operator action results in failure of both full and partial depressurization. Further, a failure probability

corresponding to a high dependency is assigned to the diverse actuation system-related operator action because it follows the similar protection and safety monitoring system-related action in the sequence.

19.59.3.2 Component Importances for At-Power Core Damage Frequency

This section intentionally blank.

19.59.3.3 System Importances for At-Power Core Damage

This section intentionally blank.

19.59.3.4 System Failure Probabilities for At-Power Core Damage

This section intentionally blank.

19.59.3.5 Common Cause Failure Importances for At-Power Core Damage

This section intentionally blank.

19.59.3.6 Human Error Importances for At-Power Core Damage

This section intentionally blank.

19.59.3.7 Accident Class Importances

This section intentionally blank.

19.59.3.8 Sensitivity and Importance Analyses Summary for At-Power Core Damage Frequency

Numerous importance and sensitivity analyses were performed on the core damage model for internal initiating events at power.

The analyses were chosen to address the following issues:

- Importances of individual basic events and their effect on plant core damage frequency
- Importances of safety-related and nonsafety-related systems in maintaining a low plant core damage frequency
- Effect of human reliabilities as a group on plant core damage frequency
- Other specific issues such as passive system check valve reliability, diesel generator mission time, and quantification cutoff probability

Component importance analyses were performed of all basic events appearing in the cutsets for the baseline core damage quantification. The importance measures are risk decrease and risk increase. Risk decrease (also called risk reduction worth) is the factor by which the core damage frequency would decrease if the failure probability for a given basic event is set to 0.0; it is a useful measure of the benefit that might be obtained as a result of improved component maintenance or testing, better procedures, or operator training. Risk increase (also called risk achievement worth) is the factor by which the core damage frequency would increase if the failure probability for a given basic event is set to 1.0; it is a useful measure of which components or actions would most adversely affect the core damage frequency if actual operating practices resulted in higher failure probabilities than assumed in the PRA.

The risk decrease results show that only one single component failure, the in-containment refueling water storage tank discharge line strainer plugging, contributes more than 10 percent to the core damage frequency.

The contribution to the core damage frequency from unscheduled maintenance is small; there is no scheduled maintenance for safety-related components at power.

These results indicate that there are no components for which an improvement in design, test or maintenance (i.e., a change resulting in a significant reduction of the component failure rate) would have a significant impact on the core damage frequency.

The risk increase results indicate there are only two components for which guaranteed failure results in a core damage frequency contribution increase of at least 10 times. Other single-component failures have significantly lower risk increase values, corresponding to a factor of six or lower increase in core damage frequency given an assumption of total unreliability for these components.

These results indicate that the AP600 design includes sufficient redundancy and diversity of protection so that single component-related failures do not have a large impact on the core damage frequency results.

The sensitivity analyses results indicate that:

- If no credit is taken for operator actions, the plant core damage frequency is small and is comparable with core damage frequencies for existing plants where credit is taken for operator actions.

- The most important systems for core damage prevention are the protection and safety monitoring system and Class 1E dc power. The risk-important systems are safety-related systems. The safety-related systems are all of high or medium importance. The nonsafety-related systems are only marginally important to the plant core damage frequency.

- The common cause risk decrease importance results show that common cause failures of hardware associated with the protection and safety monitoring system, common cause

failures of in-containment refueling water storage tank gravity injection components, common cause failures of tank level transmitters for the in-containment refueling water storage tank and CMTs, the CMT air-operated valves, and common cause automatic depressurization system squib valve failures are of potential significance in maintaining the current level of low plant core damage frequency.

- The risk increase importances for common cause failures of the following sets of components show that these are also of potential significance to the current low level of core damage frequency from internal events: common cause failure of software in the protection and safety monitoring system and plant control system, logic board failures of the protection and safety monitoring system; failures of transmitters used in the protection and safety monitoring system; failures of reactor trip breakers; plugging of containment sump recirculation screens; failures of in-containment refueling water storage tank gravity injection line check valves and squib valves; plugging of strainers in the in-containment refueling water storage tank; failures of fourth-stage automatic depressurization system squib valves and failures of output cards for the protection and safety monitoring system.

- There are no operator actions that would provide a significant risk decrease if they were made to be more reliable. There are only eight operator actions that would increase the core damage frequency by more than the base case if they were assumed to fail. The most important of these is the failure to diagnose a steam generator tube rupture event.

- A sensitivity was performed with no credit for operator actions. The resulting core damage frequency remains low, on the order of core damage frequency for current plants with credit for operators. Combined with the results of other studies, this means that, in general, operator actions are important in maintaining a very low plant core damage frequency for internal events at power but are not essential to establishing the acceptability of plant risk. This finding demonstrates a significantly lower dependence on human actions than exists for current plants. The AP600 meets the core damage frequency safety goal without human action.

- If the reliability of all check valves is assumed to be a factor of 10 worse, the total plant core damage frequency would only increase slightly. This shows that the passive safety-related systems that depend on check valve opening will perform acceptably, even if pessimistic check valve reliabilities are assumed.

- The plant core damage frequency is not affected by the diesel generator mission time duration. This is due to the AP600 design's passive features, which do not require ac power for operation.

- The common cause failure basic events, particularly those associated with safety-related systems, are important individually, and also as a group for plant core damage frequency. This is expected for a plant with highly redundant safety-related systems, for which individual component random failure contributions are of reduced significance.

19.59.3.9 Summary of Important Level 1 At-Power Results

The results of the PRA show that the following AP600 design features provide the ability to respond to internal initiating events and contribute to a very low core damage frequency.

- The manual feed and bleed operation in current pressurized water reactors is replaced by the automatic depressurization system and core makeup tank/in-containment refueling water storage tank injection. This increases the success probability for bleed and feed and helps reduce core damage contribution from transients with failure of decay heat removal.

- The switchover-to-recirculation operation in current pressurized water reactors is replaced with automatic recirculation of sump water into the reactor coolant system loops by natural circulation.

- The diverse actuation system provides diverse backup for automatic or manual actuation of safety-related systems, increasing the system reliability for the passive residual heat removal, core makeup tank, and automatic depressurization systems.

- The AP600 plant design is based on a defense-in-depth concept whereby there are several means (both active and passive) of providing reactor coolant system makeup following a loss-of-coolant accident, at both high and low pressures (i.e., chemical and volume control system pumps, core makeup tanks, accumulators, in-containment refueling water storage tank gravity injection, and normal residual heat removal system). Similarly, there are diverse means of core cooling, including the passive residual heat removal and normal residual heat removal systems.

- The ability to depressurize and establish feed and bleed heat removal via the automatic depressurization system and core makeup tanks without operator action provides an additional reliable means of core cooling and inventory control.

- The diversity and redundancy in the design of the automatic depressurization system provides a highly reliable system for depressurizing to allow injection and core cooling by the various sources of water.

- The design of the reactor coolant pumps eliminates the dependence on component cooling water and accompanying reactor coolant pump seal loss-of-coolant accident core damage contribution, which is typically significant for current plants.

- The design of the safety-related heat removal systems eliminates the dependence on service water and ac power during accidents; such dependencies can be significant contributors to core damage for current plants.

Core Damage Contribution from Important Initiating Events

Loss-of-Coolant Events. The at-power core damage results are dominated by various loss-of-coolant events, with the largest contribution from a safety (direct vessel) injection line break. The safety (direct vessel) injection line break is a special initiator, in that its occurrence partially defeats features incorporated into the plant to respond to losses of primary coolant. Even though the safety injection line break core damage frequency dominates the results, its value is very small, with little credit for nonsafety-related systems.

Anticipated Transients Without Scram. Anticipated transients without scram sequences contribute a small percentage of the at-power core damage frequency, in part due to modeling simplifications whereby, in the absence of specific modeling and success criteria, it has been assumed that core damage will occur given certain combinations of failures. With additional analysis and modeling detail, it is expected that the anticipated transient without scram core damage frequency would be shown to be lower.

Transients. The contribution of transients to core damage frequency is small. This is the result of the defense-in-depth features of the AP600 design, whereby core cooling following transients is available from main feedwater, startup feedwater, and passive residual heat removal, as well as from feed and bleed, using diverse and redundant sources of makeup (core makeup tanks, accumulators, in-containment refueling water storage tank, normal residual heat removal system), and of depressurization (four stages of automatic depressurization system).

Loss of Offsite Power. The loss of offsite power core damage frequency contribution at power is insignificant. AP600 passive systems require only dc power provided by the long-term batteries for actuation to provide cooling. In addition, the passive residual heat removal heat exchanger is backed up by bleed and feed cooling using the automatic depressurization system and core makeup tanks or in-containment refueling water storage tank gravity injection, which also require only dc power provided by long-term batteries. With onsite power available, startup feedwater provides an additional means of decay heat removal.

Steam Generator Tube Rupture. The steam generator tube rupture event provides a small contribution to the at-power core damage frequency. Compared to operating pressurized water reactors it is a very low contribution. Among the reasons for the small steam generator tube rupture core damage contribution are the following:

- The first line of defense is the startup feedwater system and chemical and volume control system
- A reliable safety-related passive residual heat removal system coupled with the core makeup tank subsystem, which provide automatic protection
- A third line of defense using automatic depressurization system and in-containment refueling water storage tank for accident mitigation should the above-mentioned systems fail.

Further, the automatic depressurization system provides a more reliable alternate decay heat removal path through feed and bleed than the high-pressure manual feed and bleed cooling of current operating plants.

Finally, the large capacity of the in-containment refueling water storage tank increases the long-term recovery probability for unisolable steam generator leaks that bypass containment, by preventing depletion of borated water and core damage.

Dependence on Operator Action

The results of the PRA show that the AP600 is significantly less dependent on operator action to reduce plant risk to acceptable levels than are current plants. This was shown through the sensitivity analyses and the operator action contributions from both the risk decrease and risk increase measures. Almost all operator actions credited in this PRA are performed in the control room; there are very few local actions outside the control room. Further, the human actions modeled in the AP600 PRA are generally simpler than those for current plants. Thus, the tasks for AP600 operators are easier and less likely to fail. If it were assumed that the operators never perform any actions credited in the PRA, the internal events core damage frequency would still be lower than the result obtained for many current pressurized water reactors including operator actions.

Dominant System/Component Failure Contributors

Contribution to Core Damage Frequency. Component-related contributors to core damage frequency from internal events at power are dominated by common cause failures. There are no single components for which an improvement in design, test, or maintenance (resulting in perfect component performance) would have a large impact on the core damage frequency results.

Dependence on Component Reliability. Most of the component failures with relatively high risk increase worth are common cause failures. This is an indication of the high degree of built-in redundancy and diversity of AP600 safety-related systems, particularly in view of the low baseline core damage frequency. The results demonstrate a well-balanced design, for which diversity eliminates any strong dependence on active valves or on any specific type of valve.

Sensitivity to Numerical Values and Modeling Assumptions. The core damage results are not strongly sensitive to increases in the failure probabilities of basic events. Check valves are relatively important; if the check valve failure probability is increased by a factor of 10, the core damage frequency increases by a factor of 3. This increase is not large, and shows that the core damage goal of 1E-05 is comfortably met. Finally, the modeling assumptions in system and accident sequence success criteria are bounding (e.g., conservative) whenever a range of conditions are represented by a single selected condition or success criterion. Since the modeling assumptions already represent an upper bound type estimate, there are no significant contributions to core damage due to conditions outside the assumed ranges that are unaccounted for. As an example, the automatic depressurization system success criteria for

loss-of-coolant accident events are selected to cover the worst conditions (e.g., break size, break location) of the range.

Test and Maintenance Unavailability Safety-related systems do not have scheduled test or maintenance during power operation. This eliminates the unavailability due to test or scheduled maintenance of safety-related system components at power.

System Reliability and Defense-in-Depth. The results show that the safety-related systems have demonstrated high reliabilities, due to the nature of the system designs (passive systems, with no test or maintenance requirements during power operation). Moreover, multiple means of success exist for transients and credible loss-of-coolant accident events. This means that a failure of a safety-related system will not lead to core damage, because other diverse systems back up the first one. This defense-in-depth philosophy contributes to the low core damage frequency.

19.59.4 Large Release Frequency for Internal Initiating Events at Power

The results of the Level 2 (containment response) and Level 3 (plant risk) analyses for the internal initiating events at power demonstrate that the AP600 containment design is robust in its ability to prevent releases following a severe accident and that the risk to the public due to severe accidents for AP600 is very low. The large release frequency (containment failure frequency) of the AP600 can be divided into two types of failures: 1) initially failed containment, in which the integrity of the containment is either failed due to the initiating event or never achieved from the beginning of the accident; and 2) containment failure induced by high-energy severe accident phenomena. The total of these failures is the overall large release frequency, which is very small and well within the established goals.

The Level 3 analysis shows that the resulting risk to the population is small and well within the established goals.

19.59.4.1 Dominant Large Release Frequency Sequences

The large release frequency is dominated by release categories BP (bypass) and CFE (early containment failure). These two categories make up approximately 98 percent of the plant large release frequency, followed by a very small contribution from the containment isolation failure release category. Contributions of the late containment failure (CFL) and intermediate containment failure (CFI) release categories to large release frequency are negligible.

The early containment failures are caused by an early hydrogen detonation event (hydrogen is produced by an early core uncovery and a failure of the hydrogen igniters, which allows a hydrogen detonation event to occur), or a failure of the reactor coolant system that allows core debris to exit the vessel. The hydrogen detonation and core ex-vessel phenomena are both assumed in the analysis to cause containment failure.

The dominant accident class in the large release frequency represents sequences in which the reactor coolant system is depressurized either due to the nature of the initiating event (such

as large loss-of-coolant accident), or through successful actuation of the automatic depressurization system. Early core damage is caused by a failure of in-containment refueling water storage tank injection.

The dominant large release frequency sequences are described below.

Sequence 1: Accident Class 3BE With Cavity Flooding Failure

Description of Sequence

This containment event tree (CET) sequence is initiated by the core damage sequences that follow large LOCAs or other events with full RCS depressurization. This accident class is labeled as 3BE.

This large release frequency sequence contains core damage sequences where the RCS is fully depressurized by the nature of the initiating event (e.g. large LOCA) or by the successful operation of ADS stage four. Core damage is caused by the failure of RCS inventory makeup by IRWST injection or RNS injection.

By definition, the RCS is depressurized at the time of core damage. The sequence develops with successful containment isolation and failure of the manually actuated cavity (sump) flooding. This is assumed to lead to reactor vessel failure. Containment failure is assumed within the time of core relocation. This sequence is binned into the release category CFE, early containment failure.

Some important modeling assumptions include the following:

- It is assumed that failure of cavity flooding leads to vessel failure; which in turn is assumed to fail the containment, before a significant fission-product deposition can occur, reducing the capacity for fission-product attenuation.

- If IRWST injection is failed due to common cause failure of squib valves in the IRWST injection lines, credit is taken for diverse squib valves in the sump flooding lines.

- Credit is taken for manual actuation of sump flooding by the operator, when the IRWST injection (or RNS injection, wherever applicable) fails.

The manually actuated sump flooding function has two redundant paths from the IRWST to the sump, each containing a motor-operated valve and a squib valve.

Risk-Important Failures

The dominant cutsets for this CET sequence show that the risk-important failures are failure of IRWST injection (and RNS injection, whenever applicable), coupled with the following failure modes of sump flooding:

- Common cause failure of strainers in IRWST
- Actuation software/hardware failures
- Common cause and random failure of both motor-operated valves
- Operator fails to open IRWST valves to flood reactor cavity.

The success of this CET sequence depends on the success of the operator action of actuating the sump flooding function by opening valves.

Sequence 2: Accident Class 6 With High-Pressure Core Damage

Description of Sequence

This CET sequence is initiated by the core damage sequences that follow SGTR, including consequential SGTR, and interfacing systems LOCA events where a direct path bypassing the containment exists due to the nature of the initiating event. This accident class is labeled as 6.

Accident class 6 contains event sequences where RCS may be fully depressurized, or at high pressure. The core damage is caused by the failure of RCS inventory makeup by IRWST injection or RNS injection.

Following a postulated core damage in accident class 6, the first CET question asked is the success of manual depressurization of the RCS by ADS actuation. The ADS depressurizes those sequences where the RCS is at high pressure at the time of core damage. Core damage frequency sequences in accident class 6 with successful ADS operation are treated like accident class 3BL.

If the manual ADS depressurization fails for high RCS pressure core damage sequences, it is classified as a containment bypass (BP release category) sequence for fission-product release.

An important modeling assumption is that those steam generator tube rupture sequences in which the ADS is successful behave like accident class 3BL. For these sequences, the path through the secondary side is not significant for fission-product release to the atmosphere, since the pressure inside the RCS is low, and water in the faulted steam generator acts as a barrier against large release.

Risk-Important Failures

The dominant cutsets for this CET sequence show that the risk-important failures are failure of PMS ESF output logic software and manual DAS actuation, common cause failure of

output drivers, and common cause failure of RCP trip breakers and operator actions to actuate ADS.

The success of this sequence depends on the success of the operator action to actuate the ADS.

Sequence 3: Accident Class 3A With High-Pressure Core Damage

Description of Sequence

This CET sequence is initiated by the core damage sequences that follow ATWS events. This accident class is labeled as 3A.

This large release frequency sequence contains core damage sequences where the RCS is not depressurized after an ATWS event.

Following the postulated core damage in accident class 3A, the first CET question asked is whether RCS pressure is controlled by the success of PRHR, RCP trip, and CMT injection. Also, steam generator tube integrity is questioned. If any one of these fails, the sequence is classified as high-RCS-pressure core damage leading to a failure of the RCS pressure boundary. This failure is assumed to be at the steam generator tubes, the most probable failure location. Failures in this sequence are classified as a containment bypass (BP release category) sequence for fission-product release.

Some important modeling assumptions include the following:

- Credit is taken for various operator actions to avoid or terminate an ATWS event.
- If the ATWS continues, success of PRHR and CMT/RCP trip is sufficient to keep the RCS pressure low.

Risk-Important Failures

The dominant cutsets for this CET sequence show that the risk-important failures are failure of transmitters and operator actions.

Sequence 4: Accident Class 1A With High-Pressure Core Damage

Description of Sequence

This CET sequence is initiated by the core damage sequences that follow transients or small LOCA events. This accident class is labeled as 1A.

This large release frequency sequence contains core damage sequences where the RCS is not depressurized after a transient or a small LOCA event.

Following the postulated core damage in accident class 1A, where partial and full ADS failed leading to core damage, the first CET question asked is whether the RCS pressure is controlled by the success of manual ADS actuation. If manual ADS actuation fails, the sequence is classified as high RCS pressure core damage leading to an assumed steam generator tube rupture and containment bypass. Failures in this sequence are classified in the BP release category.

An important modeling assumption is that credit is taken for manual ADS actuation after core damage.

Risk-Important Failures

The dominant cutsets for this CET sequence show that the risk-important failures are common cause failures of PMS and PLS software coupled with failures of DAS automatic and manual actuation.

Sequence 5: Accident Class 1AP With High-Pressure Core Damage

Description of Sequence

This CET sequence is initiated by the core damage sequences in which the RCS is not fully depressurized. This accident class is labeled as 1AP.

The large release frequency sequence contains core damage sequences where the RCS is not fully depressurized, but the PRHR is operating or the event is an intermediate LOCA.

Following the postulated core damage in accident class 1AP, where partial and full ADS failed leading to core damage, the first CET question asked is whether the RCS pressure is controlled by the success of manual ADS actuation. If manual ADS actuation fails, the sequence is classified as high-RCS-pressure core damage leading to an assumed steam generator tube rupture and containment bypass. Failures in this sequence are classified in the BP release category.

An important modeling assumption is that credit is taken for manual ADS actuation after core damage.

Risk-Important Failures

The dominant cutsets for this CET sequence show that the risk-important failures are hardware and software failures of PMS actuation, and failure of operator to actuate DAS.

Sequence 6: Accident Class 3C With High-Pressure Core Damage

Description of Sequence

This CET sequence is initiated by the core damage sequences in which a LOCA beyond the capacity of the safety-related systems occurs. This event is also termed "Vessel Failure." By the nature of the event, the RCS is depressurized. This accident class is labeled as 3C.

During this LOCA event, the core may or may not remain in the vessel, depending upon the break location. Based on analysis, approximately 90 percent of such events would result in the vessel retaining the core (e.g., the break occurs above the core). Only 10 percent of the events would result in a vessel failure resulting in the core being out of the vessel. In that case, the containment is assumed to fail without further analysis, and the sequence is classified as an early containment failure (CFE) for fission-product release.

An important modeling assumption is that credit is taken for the break occurring most of the time above the pressure vessel beltline.

Sequence 7: Accident Class 3D With High-Pressure Core Damage

Description of Sequence

This CET sequence is initiated by the core damage sequences in which RCS is partially depressurized. This accident class is labeled as 3D.

This large release frequency sequence contains event sequences where the RCS is partially depressurized, but IRWST injection fails.

In this CET sequence, the containment isolation is successful but cavity flooding fails. This is assumed to fail the reactor vessel without further analysis. The containment is also assumed to fail. This sequence is classified as an early containment failure (CFE) sequence for fission-product release.

Some important modeling assumptions include the following:

- Credit is taken for manual cavity flooding actuation after core damage when this operator action is possible (i.e., the control systems are operable).

- Common cause failures that would fail injection leading to core damage are also modeled for the manual cavity flooding after the core damage. Manual cavity flooding is not credited for sequences where the common cause failures exist.

Risk-Important Failures

The dominant cutsets for this CET sequence show that the risk-important failures include failures of PMS and manual DAS actuation, common cause failure of ADS fourth-stage squib valves, common cause failure of cavity flooding motor-operated valves, and to a lesser degree operator failure to actuate cavity flooding.

19.59.4.2 Sensitivity Analyses for Containment Response

Sensitivity analyses were performed in the large release frequency analysis.

The analyses show that the operator action to flood the reactor cavity is important as are the valves and other components required to accomplish this task. Other operator actions modeled in the Level 2 analyses are not as important.

Core damage events that result in a failure to flood the reactor cavity are relatively important. The failure to flood the reactor cavity is assumed to result in failure of the reactor vessel. Vessel failure is assumed to fail the containment. The ability to flood the reactor cavity helps to retain reactor coolant system integrity and prevent ex-vessel events, which are assumed to fail the containment.

Common cause failures dominate the basic events important to the large release frequency. These include the common cause failure of: pressure and tank level transmitters, instrumentation and control system, the check valves in the recirculation lines, and plugging of the in-containment refueling water storage tank strainers. Failure of the operator action to flood the reactor cavity is also important to the large release frequency.

19.59.4.3 Comparison of Initiating Event Importances for Core Damage Frequency and Large Release Frequency

A comparison of the initiating event contributions to large release frequency and core damage frequency shows the importance of the steam generator tube rupture, anticipated transient without scram, and transient initiating event categories increased in the large release frequency compared to their contributions to the core damage frequency. On the other hand, safety (direct vessel) injection line breaks and intermediate loss-of-coolant accidents contribute less to the large release frequency than they do to the core damage frequency. Large loss-of-coolant accident is the dominant contributor to large release frequency, as well as to core damage frequency.

The containment effectiveness reflects the ability of the containment to mitigate the effects of a serious accident. The containment effectiveness for loss-of-coolant accidents is very high. A loss-of-coolant accident is a rare event with serious potential consequences. In fact, the core damage frequency is dominated by loss-of-coolant accident sequences. In the unlikely event that a loss-of-coolant accident results in core damage, the containment is designed to prevent a large release.

For transients, the containment effectiveness is low. The core damage frequency from transients is small. But, if a transient does result in core damage, it is most likely as a result of a common cause failure of the instrument and control systems. This is also a rare event. Conservatively, no recovery action is modeled in the PRA for such failures. These recovery actions, such as finding alternative ways to actuate the automatic depressurization system, would certainly be undertaken by the operators. Also, if a transient does result in core damage, it sometimes results in a high-pressure event. These events are assumed, without further analysis, to lead to a failure of the reactor coolant system pressure boundary, which is assumed to fail the containment (again without further analysis). These are conservative assumptions in the PRA models for transients.

19.59.4.4 Summary of Important Level 2 At-Power Results

The results of the PRA show that the following AP600 design features provide the ability to respond to various severe accidents and contribute to a very small release frequency and a small release of radioactive material to the environment.

- The capability to flood the reactor cavity prevents the failure of the reactor vessel given a severe accident without water in the cavity. The vessel and its insulation are designed so that the water in the cavity is able to cool the vessel and prevent it from failing (in-vessel retention - IVR). By maintaining the vessel integrity, the core debris in the vessel eliminates the potential of a large release due to ex-vessel phenomena and its potential to fail the containment.

- The capability to depressurize the reactor coolant system in a high-pressure transient mitigates the consequences of a high-pressure severe accident. Such accidents have a large potential to fail the reactor coolant system pressure boundary vessel, piping, or steam generator tubes, and such a failure is assumed without further analysis if the reactor coolant system remains at high pressure. A high-pressure failure of the reactor coolant system pressure boundary is assumed to fail or bypass the containment. Thus, the capability to depressurize the reactor coolant system reduces the large release frequency due to high-pressure severe accidents.

- The insulation of the reactor vessel allows water in the reactor cavity to cool the vessel and helps to maintain the reactor coolant system integrity. This keeps the core debris in the vessel after a severe accident.

- The annular spaces in the containment design help to reduce the release of radioactive materials to the environment by enhancing the deposition of the materials before they exit the containment.

The Level 2 results highlight some insights in the AP600 design.

- The dominant sequence that leads to a large release is a low-pressure core damage sequence that leads to an early containment failure. The core damage is due to a failure of the in-containment refueling water storage tank injection to the vessel. The

containment failure is due to a failure to flood the reactor cavity, which is assumed to cause the vessel to fail. The vessel failure is assumed to lead to a containment failure. The failure of the in-containment refueling water storage tank injection is often due to an assumed common cause failure of the instrumentation and control systems or a common cause failure of the in-containment refueling water storage tank strainers. These same failures lead to the failure of the ability to flood the cavity. No recovery actions by the operators are modeled, although they are expected to occur. Also, these failures are based upon very conservative models such as the instrument and control system models.

- Bypass sequences are the next most important contributor to the large release frequency. These include induced steam generator tube ruptures and unrecovered steam generator tube ruptures. Common cause automatic actuation failures of the automatic depressurization system are the most dominant in these sequences, followed by a failure of the operator action to manually actuate the system. These failures are assumed to lead to a failure of the steam generator tubes. The steam generator tube failures bypass the containment.

- Direct ignition of a hydrogen detonation event is not credible in the AP600 containment. The progression of a hydrogen deflagration to a detonation event is postulated, and it is assumed to fail the containment without further analysis. The presence of hydrogen igniters is important to the mitigation of hydrogen detonation events (and the assumed containment failure), but they are not dominant. Similarly, the operator action to actuate the hydrogen igniters is important, but it is not dominant. The reliability of the igniters is not required to be high to maintain a low large release frequency.

- A containment failure caused by a diffusion flame is not credible.

- A reduced reliability in the ability to isolate the containment does not significantly change the large release frequency.

- There are no operator actions that could be significantly improved that would result in a significant reduction in the large release frequency.

- A reduced reliability in the passive containment cooling system does not significantly change the large release frequency.

- Common cause failures dominate the basic event importances. This shows that single independent failures do not have a large impact on the large release frequency for AP600 and reflects the redundancy and diversity of protection against large releases.

- The potential for a release of radioactive materials to the environment is very small. This is largely due to the very small core damage frequency and very small release frequency. The containment design provides enhanced deposition of core materials that

could be released in a severe accident, and the passive containment cooling system minimizes the energy available to expel such materials from the containment.

- The nonsafety-related containment spray system is not credited in the PRA. Failure of the containment spray does not prevent the plant from achieving the safety goals.

The results of the at-power analyses show the AP600 design includes redundancy and diversity not found in current plants. The safety-related passive systems do not require ac power or operator actions to actuate, and the plant design is robust in the prevention and mitigation of the consequences of an accident. The AP600 core damage frequency and large release frequency are much lower than has been seen in current generation plants, despite the many conservatisms built into the PRA models. The assumed dose to the environment given a severe accident and a large release is well within the goals set for that analysis.

19.59.5 Core Damage and Severe Release Frequency from Events at Shutdown

19.59.5.1 Summary of Shutdown Level 1 Results

The low-power and shutdown assessment calculated an extremely low core damage frequency. The top nine accident sequences contribute 90 percent of the Level 1 shutdown core damage frequency. The three dominant accident sequences involve failure of normal residual heat removal due to a loss of component cooling or service water system initiating event during a drained condition. These three sequences contribute approximately 70 percent to the shutdown core damage frequency. The next three dominant accident sequences involve failure of the normal residual heat removal system during a drained condition. These sequences contribute approximately 10 percent to the shutdown core damage frequency.

The descriptions of the dominant sequences are provided in the following paragraphs.

Loss of Component Cooling or Service Water System Initiating Event during Drained Condition

The first three sequences are a loss of decay heat removal initiated by failure of the normal residual heat removal system as a result of failure of the component cooling water or service water system during mid-loop/vessel flange operation. Core damage occurs if automatic and manual actuation of the in-containment refueling water storage tank injection valves and manual actuation of the normal residual heat removal system pump suction valve fails, or if ADS stage 4 valves fail, or if containment sump recirculation fails.

The major contributors to core damage frequency due to loss of component cooling water system/service water system during drained condition are:

- Hardware failures of both service water pumps or common cause failure of the output logic I/Os from the plant control system

- Common cause failure of the in-containment refueling water storage tank injection valves and normal residual heat removal system pump suction valve
- Common cause failure of the ADS stage 4 squib valves
- Common cause failure of the sump recirculation squib valves
- Common cause failure of the strainers in the in-containment refueling water storage tank
- Common cause failure of the containment sump strainers

Loss of Normal Residual Heat Removal System Initiating Event during Drained Condition

The three dominant sequences are a loss of decay heat removal initiated by failure of the normal residual heat removal system during drained conditions. The loss of decay heat removal occurs following failure of the normal residual heat removal system due to normal residual heat removal system hardware faults during mid-loop/vessel-flange operation. Core damage occurs if automatic and manual actuation of the in-containment refueling water storage tank injection valves and manual actuation of the normal residual heat removal system pump suction motor-operated valve fail, or if ADS stage 4 valves fail, or if containment sump recirculation fails.

The major contributors to core damage frequency due to loss of the normal residual heat removal system during drained condition are:

- Common cause failure of the normal residual heat removal system pumps to run
- Common cause failure of the in-containment refueling water storage tank injection valves and normal residual heat removal system pump suction valves
- Common cause failure of the ADS stage 4 squib valves
- Common cause failure of the sump recirculation squib valves
- Common cause failure of the strainers in the in-containment refueling water storage tank
- Common cause failure of containment sump strainers

Loss-of-Coolant Accident Initiating Event due to Inadvertent Opening of RNS-V024 during Safe/Cold Shutdown Conditions

This sequence is a loss-of-coolant accident initiated by inadvertent opening of RNS-V024 during safe/cold shutdown conditions when the reactor coolant system is filled and pressurized. Following the initiating event, the core makeup tanks are actuated, and the

automatic depressurization system actuates. Core damage occurs if the in-containment refueling water storage tank injection valves do not open.

The major contributors to core damage frequency due to a loss-of-coolant accident through RNS-V024 during safe/cold shutdown conditions are:

- Inadvertent opening of RNS-V024 due to operator error (an initiating event frequency contributor)
- Common cause failure of the in-containment refueling water storage tank injection valves
- Common cause failure of the strainers in the in-containment refueling water storage tank

Loss of Offsite Power Initiating Event during Drained Condition (with failure of grid recovery within 1 hour)

This sequence is initiated by loss of offsite power during mid-loop/vessel-flange operation. In this sequence, the normal residual heat removal system fails to restart automatically following the initiating event, and the grid is not recovered within 1 hour. Core damage occurs if automatic and manual actuation of the in-containment refueling water storage tank injection valves and manual actuation of the normal residual heat removal system pump suction valve fail.

The major contributors to core damage frequency given loss of offsite power (without grid recovery) during drained condition are:

- Software common cause failure of protection and safety monitoring system/plant control system instrumentation and control logic cards
- Failure of a normal residual heat removal system pump to restart or run
- Failure of a diesel generator to start and run
- Failure of main circuit breaker to open
- Failure to recover ac power within 1 hour
- Common cause failure of the in-containment refueling water storage tank injection valves and normal residual heat removal system pump suction valve
- Common cause failure of the strainers in the in-containment refueling water storage tank

Reactor Coolant System Overdraining Event during Drainage to Mid-Loop

This sequence is initiated by reactor coolant system overdraining during drainage to mid-loop conditions. Following the initiating event, manual isolation of the normal residual heat removal system fails. Core damage occurs if manual actuation of the in-containment refueling water storage tank injection valves and manual actuation of the normal residual heat removal system pump suction motor-operated valve fail.

The major contributors to core damage frequency due to reactor coolant system overdraining initiated during drainage to mid-loop are:

- Common cause failure of the chemical and volume control system air-operated valves to close automatically upon receipt of low hot leg level signals and failure of the operator to stop draining (initiating event frequency contributors)
- Operator fails to isolate the normal residual heat removal system
- Operator fails to open the in-containment refueling water storage tank injection valves
- Operator fails to open the normal residual heat removal system pump suction valve
- Common cause failure of the in-containment refueling water storage tank injection valves and normal residual heat removal system pump suction valve

Conclusions

The conclusions drawn from the shutdown Level 1 study are as follows:

- The overall shutdown core damage frequency is very small.
- Initiating events during reactor coolant system drained conditions contribute approximately 90 percent of the total shutdown core damage frequency; loss of decay heat removal capability (during drained condition) due to failure of the component cooling water system or service water system are the initiating events with the greatest contribution.
- Common cause failures of in-containment refueling water storage tank components are the dominant contributors to the total shutdown core damage frequency.
- The function of the automatic depressurization system stage 4 squib valves is important to preclude the effects of surge line flooding.
- Following an extended loss of RNS during safe/cold shutdown with the RCS intact and PRHR unavailable, it is important to establish and maintain venting capability with ADS stage 4 for gravity injection and containment recirculation.

- Human errors are not overly important to shutdown core damage frequency. There is no particular dominant contributor. Sensitivity results show that the shutdown core damage frequency would remain very low even with little credit for operator actions.

- Individual component failures are not significant contributors to shutdown core damage frequency, and there is no particular dominant contributor. This confirms the at-power conclusion that single independent component failures do not have a large impact on core damage frequency for AP600 and reflects the redundancy and diversity of protection at shutdown as well.

- The in-containment refueling water storage tank provides a significant benefit during shutdown because it serves as a passive backup to the normal residual heat removal system.

19.59.5.2 Large Release Frequency for Shutdown and Low-Power Events

The baseline PRA shutdown large release frequency is very low. The large release frequency is dominated by reactor vessel failure due to the failure to flood the reactor cavity. Containment bypass due to steam generator tube rupture, both as an initiating event and induced by high RCS pressure and temperature, is the second dominant contributor to the large release frequency. The third dominant contributor to the large release frequency is containment isolation failure. All other containment failure modes contribute negligibly to the large release frequency.

19.59.5.3 Shutdown Results Summary

The results of the low-power and shutdown assessment show that the AP600 design includes redundancy and diversity at shutdown not found in current plants; in particular, the in-containment refueling water storage tank provides a unique safety backup to the normal residual heat removal system. Maintenance at shutdown has less impact on the defense-in-depth features for AP600 than for current plants; in accordance with plant technical specifications, safety-related system planned maintenance is performed only during those shutdown modes when the protection provided by the safety-related system is not required. Further, maintenance of nonsafety systems, such as the normal residual heat removal system, component cooling water system, and service water system, is performed at power to avoid adversely affecting shutdown risk. These contribute to the extremely low shutdown core damage and large release frequency.

19.59.6 Insights from Internal Flooding, Internal Fire, and Seismic Margin Analyses

19.59.6.1 Insights from Internal Flooding Assessment

A scoping internal flooding analysis was performed.

The AP600 design philosophy of minimizing the number of potential flooding sources in safety-related areas, along with the physical separation of redundant safety-related components

and systems from each other and from nonsafety-related components, minimizes the consequences of internal flooding. The core damage frequencies from flooding events at power and during shutdown operations are not appreciable contributors to the overall AP600 core damage frequency.

The internal flooding analysis conservatively assumes that flooding of nonsafety-related equipment results in system failure of the affected system. This results in a higher flooding-induced core damage frequency at shutdown than at power, because of the use of the nonsafety-related normal residual heat removal system as the primary means of decay heat removal at shutdown.

The dominant at-power internal flooding core damage initiators result in loss of feedwater to both steam generators. The dominant shutdown internal flooding initiators result in loss of decay heat removal during RCS drained conditions.

19.59.6.2 Insights from Internal Fire Assessment

A scoping internal fire analysis was performed. The internal fire-induced core damage frequency is based on a bounding assumption that event mitigation is only available using safety-related systems; thus, no credit is taken for nonsafety-related systems or functions.

The results from the fire analysis, performed for the spectrum of expected at-power and shutdown modes of operation, confirm that the design characteristics of the AP600 provide an effective barrier against fire hazards. This is true even within the pessimistic assumptions used throughout the study. An example of the conservative approach that typified much of the analysis was the subsumption of moderate damage categories into those that are more severe.

Conservatisms employed in the AP600 internal fire analysis include the following:

- In order to minimize potential uncertainty in the results arising from the lack of as-built equipment location and cable routing information, a bounding approach to quantification was taken. Specifically, the nonsafety-related systems (e.g., main feedwater, startup feedwater, normal residual heat removal, diverse actuation system) are not credited. In reality, fires in only a few AP600 fire areas would be capable of disabling all the nonsafety-related systems.

- A fire originating from any ignition source in an area is assumed to disable all equipment located in the fire area. The historical evidence indicates that most fires are localized fires with limited severity.

- An assumed total at-power fire initiating event frequency well in excess of current plant experience and of that anticipated for AP600, was assumed.

- Manual fire suppression is not credited to limit the extent of damage in an area nor to prevent fire propagation to an adjoining area. Historical evidence indicates that the

majority of suppressed fires were manually suppressed with little or no additional damage.

- A conservative assumption was made that a single hot short could result in spurious automatic depressurization system actuation. However, the plant is designed such that a single hot short will not cause spurious ADS actuation.

- The estimation of containment fire frequency, not normally included in fire risk assessments, was done by taking a conservative approach.

The results of the AP600 internal fire study show that the plant's system and layout designs promote a low fire-induced core damage frequency compared with existing plants. Also, the results indicate that, when nonsafety-related systems are not credited and containment is treated as a special case, the fire-induced core damage frequency profile is a relatively flat one (i.e., no fire area is significantly more important than others).

The estimated core damage frequency from main control room fires at power is insignificant. This low contribution is a result of the following:

- The ignition frequency is low because of the use of low-voltage 48v 10 mA dc cables in the AP600 control room. These low-voltage cables do not produce enough energy to heat the cables, thus ignition is not probable.

- Redundancy in control room operations is available within the control room itself; that is, if control room evacuation is not required, there is at least one other means available within the control room to shut down and control the plant.

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

- The AP600 design provides for the availability of diverse and redundant systems for plant shutdown. Therefore, loss of control of one division of power or for a whole system is not risk-significant. In addition, the passive systems are designed to operate without the need for operator interaction. Therefore, operator actions that might be disrupted by the fire scenario are backup actions, and are not significant for AP600.

The primary reasons for the AP600's low overall fire-induced core damage frequency, even on a bounding basis, include the following:

- The AP600 fire protection design provides, to the extent possible, separation of the alternate safety-related shutdown components and cabling using 3-hour-rated fire barriers.

- Since the passive safety-related systems do not require cooling water or ac power, they are less susceptible to being unavailable due to a fire than currently operating plants'

active safe shutdown equipment. As a result, the impact of fires on the shutdown capability is significantly reduced compared to current plants.

The results of this analysis show that the AP600 design is sufficiently robust that internal fires during either power operation or shutdown do not represent a significant contribution to core damage frequency.

19.59.6.3 Insights from Seismic Margin Analysis

The AP600 seismic margin analysis demonstrates that for systems, structures, and components required for safe shutdown following a seismic event, the high confidence of low probability of failure (HCLPF) magnitudes are equal to or greater than the review level earthquake, which is approximately one and two-thirds the ground motion acceleration of the Design Basis safe shutdown earthquake (SSE).

The following assumptions were made in performing the seismic margin analysis:

- A seismic initiating event hierarchy tree forms the basis for the seismic initiating event categories by considering the order of impact for the various events. The order in terms of severity is as follows:

  1. Seismically induced gross structural collapse
  2. Seismically induced LOCA in excess of ECCS capacity
  3. Seismically induced large LOCA
  4. Seismically induced small LOCA
  5. Seismically induced ATWS
  6. Seismically induced loss of offsite power

- Seismically induced gross structural collapse of Nuclear Island buildings is assumed to lead directly to core damage and large fission product release.

- A LOCA in excess of the emergency core cooling system (ECCS) capacity represents vessel failure. The event is assumed to lead directly to core damage and large fission product release, because it is assumed the containment building fails when the vessel fails.

- Since the AP600 nonsafety-related components are not Seismic Category I, no credit is taken for the mitigation functions of the nonsafety-related components and systems.

- It is assumed that the seismic event results in loss of offsite power. In addition, no credit is taken for the onsite diesel generators to provide ac power.

- It is conservatively modeled that no credit is taken for operator actions.

- It was assumed that if one component fails due to the seismic event, than all components of that same type for that system fail as well.

- If the containment air path remains functional, passive containment air cooling is sufficient to remove post-accident containment heat.

The dominant contributor to the plant HCLPF is a seismically induced LOCA beyond ECCS capacity sequence. The sequence HCLPF is determined by seismic failure of the fuel in the reactor vessel. The second dominant contributor is a seismically induced ATWS event occurs.

The seismic margin analysis demonstrates the plant to be robust against seismic event sequences that contain station blackout coupled with other seismic or random failures.

19.59.7 Plant Dose Risk From Release of Fission-Products

The dose risks are quantified by multiplying the fission product release category frequency vector by the release category mean dose vectors. The goal is that a 24-hour, whole-body, site boundary dose greater than 25 rem has a frequency of less than 1E-06 per year. The AP600 large release frequency is less than the goal of 1E-06 per year. The AP600 meets the large offsite release goal with substantial margin.

19.59.8 Overall Plant Risk Results

- The total plant core damage and large release frequency analysis results show the following:

- The total mean core damage frequency is extremely low and meets the NRC safety goal with substantial margin.

- The total plant severe release frequency is approximately an order of magnitude smaller than that of the core damage frequency; that places such a release frequency in the range of incredible events.

- The plant core damage frequency is dominated by at-power events.

- A bounding analysis of the core damage due to internal fire and internal flooding events shows that these two categories of internal events are much lower for AP600 than are calculated for currently operating plants.

- The severe release frequency is almost equal for at-power and shutdown events.

- The results show that the design goals of low core damage frequency and low severe release frequency have been met. The AP600 frequencies are lower than the NRC goals set for new plant designs. These results show the effectiveness of passive systems in mitigating severe accidents and reflect the reduced dependence of AP600 on nonsafety-related systems and human actions.

The plant dose risk results indicate the following:

- Early containment failures account for a majority of the dose risk, for at-power events. This is mainly due to failure of cavity flooding following core damage. Reactor vessel failure is assumed without further analysis for these sequences, resulting in an assumed failure of the containment.

- There is less than a 10 percent increase in the dose risk following the first 24 hours after core damage. This demonstrates that the containment continues to provide protection beyond the first 24 hours after the accident.

19.59.9 Plant Features Important to Reducing Risk

Westinghouse used PRA results extensively in the AP600 design process to identify areas for design improvement and areas for further risk reduction. These results were also compared with existing commercial nuclear power plants to identify additional area of risk reduction. Examples of the more significant AP600 plant features and operator actions that reduce risk are discussed in this section. Examples are provided in the area of reactor design, system design, plant structures and layout, and containment design.

AP600 has more lines of defense as compared to current operating plants, which provide more success paths following an initiating event and provide redundancy and diversity to fight common cause-related concerns. Examples of extensive AP600 lines of defense follow:

- For criticality control:

  - control rod insertion via reactor trip breaker opening
  - control rod insertion via motor-generator set de-energization
  - ride out via turbine trip

- For core heat removal:

  - main feedwater
  - startup feedwater
  - passive residual heat removal
  - automatic depressurization system and feed-and-bleed via normal residual heat removal injection
  - automatic depressurization system and passive feed-and-bleed via in-containment refueling water storage tank injection

- For reactor coolant system makeup:

  - chemical and volume control system
  - core makeup tanks
  - automatic depressurization system and normal residual heat removal

- automatic depressurization system, accumulators, and in-containment refueling water storage tank injection
- automatic depressurization system, core makeup tanks, and in-containment refueling water storage tank injection

• For containment cooling:

- fan coolers
- normal residual heat removal
- passive containment cooling system with passive water drain
- passive containment cooling system with alternate water supply
- passive containment cooling system without water (air only)
- fire water

19.59.9.1 Reactor Design

The AP600 reactor coolant system has many features that reduce the plant risk profile. The pressurizer is larger than those used in comparable current operating plants, resulting in a longer drainage time during small loss-of-coolant accident events. The larger pressurizer increases transient operation margins, resulting in a more reliable plant with fewer reactor trips and avoiding challenges to the plant and operator during transients. The larger pressurizer also eliminates the need for fast-acting PORVs, which are a possible source of reactor coolant system leaks.

The AP600 core is larger than comparable operating plants, resulting in a lower power density. If, during a potential severe accident, the core were partially uncovered for a short period of time, the likelihood of fuel damage is reduced.

The AP600 steam generators have large secondary-side water inventories, allowing significant time (greater than 1 hour) to recover steam generator feedwater or other means of core heat removal. The AP600 steam generators also employ improved materials and design features that significantly reduce the probability of forced outages or tube rupture.

The AP600 has canned reactor coolant pumps, thus avoiding seal loss-of-coolant accident issues and simplifying the chemical and volume control system. The reactor coolant system has fewer welds, which reduces the potential for loss-of-coolant accident events.

19.59.9.2 Systems Design

System design aspects that are intended to reduce plant risk are discussed in terms of safety-related and nonsafety-related systems.

19.59.9.2.1 Safety-Related Systems

AP600 uses passive safety-related systems to mitigate design basis accidents and reduce public risk. The passive safety-related systems rely on natural forces such as density differences,

gravity, and stored energy to provide water for core and containment cooling. These passive systems do not include active equipment such as pumps. One-time valve alignment of safety-related valves actuates the passive safety-related systems using valve operators such as:

- DC motor-operators with power provided by Class 1E batteries
- Air-operators that reposition to the safeguards position on a loss of the nonsafety-related compressed air that keeps the safety-related equipment in standby
- Squib valves
- Check valves

The passive systems are designed to function with no operator actions for 72 hours following a design basis accident. These systems include the passive containment cooling system and the passive residual heat removal system.

Diversity among the passive systems further reduces the overall plant risk. An example of operational diversity is the option to use passive residual heat removal versus feed-and-bleed functions, and an example of equipment diversity is the use of different valve operators (motor, air, squib) to address common cause failures.

The passive residual heat removal heat exchanger protects the plant against transients that upset the normal steam generator feedwater and steam systems. The passive residual heat removal subsystem of the passive core cooling system contains no pumps and significantly fewer valves than conventional plant auxiliary feedwater systems, thus increasing the reliability of the system.

There is sufficient water in the in-containment refueling water storage tank to allow the passive residual heat removal to provide core cooling for at least 72 hours. This is true whether the containment is isolated or not. If the containment is isolated, passive residual heat removal can operate for much longer. If the passive containment cooling system and the water return system gutters are operable, passive residual heat removal can potentially operate indefinitely to provide core cooling.

For reactor coolant system water inventory makeup during loss-of-coolant accident events, the passive core cooling system uses three passive sources of water to maintain core cooling through safety injection: the core makeup tanks, accumulators, and in-containment refueling water storage tank. These sources are directly connected to two nozzles on the reactor vessel so that no injection flow can be spilled for larger pipe break events.

The automatic depressurization system is incorporated into the design for depressurization of the reactor coolant system. The automatic depressurization system has 10 paths with diverse valves to combat common cause failures and is designed for automatic or manual actuation by the protection and safety monitoring system or manual actuation by the diverse actuation system. The automatic depressurization system can be used in a partial depressurization mode

to provide long-term reactor coolant system cooling with normal residual heat removal system injection, or it can be used in full depressurization mode for passive in-containment refueling water storage tank injection for long-term reactor coolant system cooling. In either case, switchover from injection to recirculation is automatic without manual actions.

The safety-related Class 1E dc and UPS system has a large battery capacity to support passive safety functions for 72 hours. This system has four 24-hour batteries, two 72-hour batteries, and a spare battery. The spare battery improves testability.

The passive containment cooling system provides the safety-related ultimate heat sink for the plant. Heat is removed from the containment vessel following an accident by a continuous natural circulation flow of air, without any system actuations. By using the passive containment cooling system following a severe accident, the containment stays well below the predicted failure pressure. The steaming and condensing action of the passive containment cooling system enhances activity removal.

AP600 containment isolation is significantly improved over that of conventional PWRs due to a large reduction in the number of penetrations; the number of normally open penetrations is reduced, and there are no penetrations required to support post-accident mitigation features. Containment isolation is improved due to the chemical and volume control system being a closed system, the safety-related passive safety injection components are located inside the containment, and the number and size of HVAC penetrations are reduced.

Vessel failure potential upon core damage is reduced (in-vessel retention of the damaged core) by providing in-containment refueling water storage tank water into the reactor cavity. The vessel insulation enables this water to cool the vessel.

For events at shutdown, AP600 has passive safety-related systems for shutdown conditions as a backup to the normal residual heat removal system. This reduces the risk at shutdown through redundancy and diversity.

Features are incorporated into the AP600 passive system design to allow for accident management. These features include refilling the in-containment refueling water storage tank, the reactor cavity and the passive containment cooling system water tank, should such actions become necessary.

19.59.9.2.2 Nonsafety-Related Systems

AP600 has nonsafety-related systems capable of mitigating accidents. These systems use redundant components, which are powered by offsite and onsite power supplies. AP600 has certain design features in the nonsafety-related systems to reduce plant risk. The main feedwater system can automatically adjust flow to reduce the number of transients and provide a continuous decay heat removal function even after the reactor trips in most transients. During transient events, the startup feedwater system can act as a backup to the main feedwater system if the latter is unavailable due to the nature of the initiating event or fails during the transient. During loss of ac power events, startup feedwater pumps are powered by the diesel generators and can be used to remove decay heat since main feedwater is not

available. The main feedwater and startup feedwater pumps are motor-driven, rather than steam-driven, for better reliability. Main feedwater controls are digital for better reliability; thus, the main feedwater and startup feedwater system design results in less transients and provides additional nonsafety-related means for decay heat removal for transients. This makes the plant response to transients very robust due to the existence of two nonsafety-related systems in addition to the passive safety-related means of removing decay heat.

The nonsafety-related normal residual heat removal system plays a role in decay heat removal in response to power and shutdown events. The normal residual heat removal system and is designed to withstand the reactor coolant system pressure to eliminate interfacing systems loss-of-coolant accident concerns that lead to containment bypass. The normal residual heat removal system provides reliable shutdown cooling, incorporating lessons learned from shutdown events. During mid-loop operations, operational procedures require the normal residual heat removal system pumps to be operable for risk reduction.

Component cooling water and service water systems have a limited role in the plant risk profile because the passive safety-related systems do not require cooling, and the canned-motor reactor coolant pumps do not require seal cooling from the component cooling water.

The nonsafety-related ac power system (onsite and offsite) also has a limited role in the plant risk profile since the plant safety-related systems do not depend on ac power. This causes the loss of offsite power event to be less important for the AP600 than in current operating plants. The plant has full load rejection capability to minimize the number of reactor trips although this is not modeled in the PRA and no credit is taken for it. The onsite ac power has two nonsafety-related diesel generators. The diesel generator life is improved and the run failure rate is reduced by avoiding fast starts.

The compressed and instrument air system has low risk importance since the safety-related air-operated valves are fail safe if the air system fails. This causes the loss of air event to be less important than in current plant PRAs.

19.59.9.3 Instrumentation and Control Design

Three instrumentation and control systems are modeled in the AP600 PRA: protection and safety monitoring system, plant control system, and diverse actuation system. Both the protection and safety monitoring system and plant control system are microprocessor-based; they can perform more functions with less components and provide better control capability that analog systems. Four divisions of redundancy are provided for the protection and safety monitoring system. Auto testing for the protection and safety monitoring system, and diagnostic self-testing for the protection and safety monitoring system and the plant control system, provide higher reliability in these systems. Both the protection and safety monitoring system and the plant control system use fiber optic cables (with fire separation) and multiplexers. Unlike current plants, there is no cable spreading room, thus eliminating a potential fire area with common cause failure of multiple functions. Additional fault tolerance is built into the plant control system so that one failure does not prevent the operation of important functions.

Improvements in the plant control system and the protection and safety monitoring system are coupled with an improved control room and man-machine interfaces; these include improvements in the form and contents of the information provided to control room operators for decision making to limit commission errors (for example, an overview panel for conveying crucial information to the operators, alarm priority, computerized procedures, longer operator action times, integration of NSSS/BOP presentation). In addition, the remote shutdown control is designed to have more functions, similar to the control room, to be performed at the remote shutdown control location, as opposed to operators sending out personnel to local valves.

The diverse actuation system provides a diverse automatic and manual backup function to the protection and safety monitoring system and reduces risk from anticipated transients without scram events. The diverse actuation system also compensates for potential common cause failures in the protection and safety monitoring system.

19.59.9.4 Plant Layout

Plant layout is designed to minimize the consequences of fire and flooding by maximizing the separation of electrical and mechanical equipment areas in the non-radiologically controlled area of the auxiliary building. This separation is designed to minimize the potential for propagation of leaks from the piping areas and the mechanical equipment areas to the Class 1E electrical and Class 1E instrumentation and control equipment rooms. The potential flooding sources and volumes in areas of the plant that contain safety-related electrical and instrumentation and control equipment are limited to minimize the consequences of internal flooding.

AP600 is designed to provide better separation between divisions of safety-related equipment. Unlike current plants, there is no safety-related cable spreading room. Safety-related cables, divisions B and D are routed separately from divisions A and C.

19.59.9.5 Plant Structures

AP600 has design features in the plant structures that reduce risk, especially for events such as fires, flooding, and seismic events. A fire or flood event in the turbine building does not affect safety-related systems.

The number of buildings and the building volume housing safety-related equipment is reduced compared to a current plant. All safety-related equipment is located on the nuclear island, which has a common basemat. This common basemat reduces the effects of a sesimic event on equipment functionality.

19.59.9.6 Containment Design

The containment pressure boundary is the final barrier to the release of fission products to the environment. The AP600 containment has provisions which help to maintain containment integrity in the event of a severe accident.

The AP600 provides significant protection to the public and the environment against the release of radiation by reducing the likelihood of the occurrence of severe accidents. The at-power core damage frequency is less than the NRC large release frequency goal of 1.0E-6 per reactor-year.

The at-power large release frequency is dominated by early containment failure and containment bypass events. For many of these events, the containment failure is conservatively assumed without further analysis. The probability of severe-accident-induced containment failures is approximately 7 percent of the core damage frequency. This distribution of the containment failure frequency demonstrates the robustness of the containment structure.

19.59.9.6.1 Containment Isolation and Leakage

Failure of the containment isolation system prior to a severe accident will lead to a direct release pathway from the containment volume to the environment. AP600 has approximately 55 percent fewer piping penetrations and a lower percentage of normally open penetrations compared to current generation plants. Normally open penetrations are closed by automatic valves, and diverse actuation is provided for valves on penetrations with significant leakage potential. Remotely operated isolation valves have control room indication to inform the operator of the current valve position.

Leakage of closed containment isolation valves in excess of technical specifications may also result in larger releases to the environment. Valves which historically have the greatest leakage problems have been eliminated, or their number significantly reduced in the AP600. Large purge valves have been replaced by smaller more reliable valves, and check valves have only been used in mild service where wear and service conditions would not be a challenge to successful operation.

Equipment and personnel hatches have the capability of being tested individually.

Therefore, AP600 provides significant protection against the failure of containment isolation.

19.59.9.6.2 Containment Bypass

Historically, containment bypass, an accident in which the fission products are released directly to the environment from the reactor coolant system, is the leading contributor to risk in a nuclear power plant. Typically the containment bypass accident class consists of two types of accident sequences: interfacing systems loss-of-coolant-accidents and unisolated, unrecovered steam generator tube ruptures.

An interfacing systems loss-of-coolant-accident is the failure of valves which separate the high pressure reactor coolant system from a lower pressure interfacing system which extends outside the containment pressure boundary. The failure of the valve causes the reactor coolant system to pressurize the interfacing system beyond its ultimate capacity and can result in a loss-of-coolant accident outside the containment. This provides a pathway for the direct release of fission products to the environment. In AP600, systems connected to the reactor

coolant system are designed with higher design pressures which reduces the likelihood of a pipe rupture in the event of the failure of the interfacing valves. This results in a very low interfacing systems loss-of-coolant-accident contribution to core damage.

Steam generator tube ruptures release coolant from the reactor coolant system to the secondary system and from there, potentially to the environment through the steam generator safety valves. An unisolated steam generator tube rupture can be mitigated by reducing the reactor coolant system pressure.

AP600 has multiple and diverse automatically actuated systems to reduce the reactor coolant system pressure and mitigate the steam generator tube rupture. The passive residual heat removal subsystem effectively reduces the reactor coolant system pressure to prevent the safety valve from opening. If the passive residual heat removal does not stop the loss of coolant, the automatic depressurization system will actuate and depressurize the system. No operator actions are required to mitigate the accident. Therefore, the likelihood of large release consequential to steam generator tube rupture has been reduced in AP600.

19.59.9.6.3 Passive Containment Cooling

The passive containment cooling system provides protection to the containment pressure boundary by removing energy from the containment. Heat is transferred to the environment through the steel pressure boundary. The heat transfer on the outside of the steel shell is enhanced by an annular flow path which creates a convective air flow across the shell and by the evaporation of water that is directed onto the top of the containment in the event of an accident. The evaporative heat transfer prevents the containment from pressurizing above the design conditions during most severe accidents.

In some postulated multiple-failure accident scenarios, the passive containment cooling system water flow may be failed. The heat removal is then limited to convection heat transfer to the air flow and radiation heat transfer to the annulus baffle. With no water film on the containment shell to provide evaporative cooling, the containment pressurizes above the design pressure to remove decay heat, but reaches a long-term equilibrium below the ultimate pressure of the containment.

Therefore, the passive containment cooling system provides decay heat removal from the containment in both wet and dry heat transfer conditions without reaching pressures which threaten the containment integrity. Long-term overpressure is not considered to be a credible containment failure mode for AP600 except in the event that the air flow in the annular spaces is blocked.

19.59.9.6.4 High Pressure Core Melt Scenarios

The automatic depressurization system and the passive residual heat removal heat exchanger provide reliable and diverse reactor coolant system depressurization which significantly reduces the likelihood of high pressure core damage. High pressure core damage sequences have the potential to fail steam generator tubes and create a containment bypass release, or to cause severe accident phenomena at the time of reactor vessel failure which may threaten

the containment pressure boundary. Reducing the reactor coolant system pressure during a severe accident significantly lowers the likelihood of phenomena which may induce large fission product releases early in the accident sequence.

19.59.9.6.5 In-Vessel Retention of Molten Core Debris

The AP600 reactor coolant system, reactor vessel and containment configuration have features which enhance the ability to maintain molten core debris in the reactor vessel. As it melts, debris relocates to the lower head of the reactor vessel where it heats and stresses the reactor vessel wall. The AP600 automatic depressurization system provides reliable pressure reduction in the reactor coolant system to reduce the stresses on the vessel wall. The reactor vessel lower head has no vessel penetrations, thus eliminating penetration failure as a potential reactor vessel failure mode. The containment configuration directs water to the reactor cavity and allows the in-containment refueling water storage tank water to be drained into the cavity to submerge the reactor vessel, cooling the external surface of the lower head. Cooling the reactor vessel prevents the failure of the reactor vessel wall. The reactor vessel reflective insulation has been designed with provisions to allow water inside the insulation panel to cool the reactor vessel surface, and with vents to allow steam to exit the insulation.

Preventing the relocation of molten core debris to the containment eliminates the occurrence of several severe accident phenomena, such as ex-vessel fuel-coolant interactions and core-concrete interaction, which may threaten the containment integrity.

19.59.9.6.6 Combustible Gases Generation and Burning

In severe accident sequences, high temperature metal oxidation, particularly zirconium, results in the rapid generation of hydrogen and possibly carbon monoxide. The first combustible gas release occurs in the accident sequence during core uncovery when steam oxidizes the zircaloy cladding and generates hydrogen. A second release may occur if the reactor vessel fails and ex-vessel debris degrades the concrete basemat. Steam and carbon dioxide are liberated from the concrete and are reduced to hydrogen and carbon monoxide as they pass through the molten metal in the debris.

AP600 employs a nonsafety-related hydrogen igniter system for control of combustible gases following a beyond design basis accident. The igniters are powered from ac busses or from either of the nonsafety-related diesel generators. Multiple glow plugs are located in each compartment. The igniters burn the gases at the lower flammability limit. At this low concentration, the containment pressure increase from the burning is small and the likelihood of detonation is negligible. The igniters are spaced such that the distance between them should not allow the burn to transition from deflagration to detonation.

During a severe accident, hydrogen that could be released from the reactor coolant system into the containment through the spargers in the in-containment refueling water storage tank or into the maintenance floor has the potential to produce a diffusion flame. A diffusion flame is produced when a combustible gas plume which is too rich to burn enters an oxygen rich atmosphere and is ignited by a glow plug or a random ignition source. The plume is ignited into a standing flame which lasts as long as there is a fuel source. Via convection and

radiation, the flame can heat the containment wall to high temperatures, increasing the likelihood of creep rupture failure of the containment pressure boundary. However, the time required to creep the containment wall to failure is estimated to be significantly larger than the duration of the hydrogen release. Therefore, the potential for containment failure from the formation of a diffusion flame at the in-containment refueling water storage tank vents is considered to be low.

There is little threat to the containment integrity from severe accident hydrogen releases, and hydrogen combustion events. The igniter system maintains the hydrogen concentration at the lower flammability limit.

19.59.9.6.7 Intermediate and Long-Term Containment Failure

The passive containment cooling system reduces the potential for decay heat pressurization of the containment. However, containment failure can also occur as a result of combustion. Due to the in-vessel retention of core debris, the potential for ex-vessel combustible gas generation from core-concrete interaction is low. The frequency of containment failures due to hydrogen combustion events is low given the reliability of the hydrogen igniters.

19.59.9.6.8 Fission-Product Removal

AP600 relies on the passive, natural removal of aerosol fission products from the containment atmosphere, primarily from gravitational settling, diffusiophoresis and thermophoresis. The AP600 containment has a low design leak rate to increase the time available for deposition. Natural removal is enhanced by the passive containment cooling system which provides a large, cold surface area for condensation of steam which increases the diffusiophoretic and thermophoretic removal processes. The site boundary dose is less than the established goals.

19.59.10 PRA Input to the Design Certification Process

The AP600 PRA was used in the design certification process to identify important safety insights and assumptions to support certification requirements such as the reliability assurance program (RAP).

19.59.10.1 PRA Input to Reliability Assurance Program

The AP600 reliability assurance program (RAP) identifies those systems, structures, and components (SSC) that should be given priority in maintaining their reliability through surveillance, maintenance, and quality control actions during plant operation. The PRA importance and sensitivity analyses identify those systems and components that are important in plant risk in terms of either risk increase (e.g., what happens to plant risk if a system or component, or a train is unavailable), or in terms of risk decrease (e.g., what happens to plant risk if a component or a train is perfectly reliable/available). This ranking of components and systems in such a way provides an input for the reliability assurance program. For more information on the AP600 reliability assurance program, refer to Section 17.4.

19.59.10.2 PRA Input to Tier 1 Information

Section 14.3 summarizes the design material contained in AP600 that has been incorporated into the Tier 1 Information from the probabilistic risk assessment.

19.59.10.3 PRA Input to MMI / Human Factors / Emergency Response Guidelines

The PRA models including modeling of operator actions in response to severe accident sequences follow the ERGs. The most risk important of these actions are manual actuation of systems in the highly unlikely event of automatic actuation failure. These operator actions and the main human reliability analysis (HRA) model assumptions are reviewed by human factors engineers for insights that they may provide to the man-machine interface (MMI) and human factors areas. For more information on the AP600 MMI, refer to Chapter 18.

In addition, the human reliability analysis models and operator actions modeled in the PRA were reviewed by the engineers writing the ERGs for consistency between the PRA models and the actual ERGs.

The PRA results and sensitivity studies show that the AP600 design has no critical operator actions and very few risk important actions. A critical operator action is defined as that action, when assumed to fail, would result in a plant core damage frequency of greater than 1.0E-04 per year; there are no such operator actions in the AP600 PRA.

19.59.10.4 Summary of PRA Based Insights

The use of the PRA in the design process is discussed in subsection 19.59.2. A summary of the overall PRA results is provided in subsections 19.59.3 through 19.59.8. A discussion of the AP600 plant features important to reducing risk is provided in subsection 19.59.9. PRA-based insights are developed from this information and are summarized in Table 19.59-29.

19.59.10.5 Combined License Information

The Combined License applicant referencing the AP600 certified design will review differences between the as-built plant and the design used as the basis for the AP600 seismic margins analysis. Differences will be evaluated to determine if there is significant adverse effect on the seismic margins analysis results. Spacial interactions are addressed by COL information item 3.7-3. Details of the process will be developed by the Combined License applicant.

The Combined License applicant referencing the AP600 certified design should compare the as-built SSC HCLPFs to those assumed in the AP600 seismic margin evaluation. Deviations from the HCLPF values or assumptions in the seismic margin evaluation should be evaluated to determine if vulnerabilities have been introduced.

The Combined License applicant referencing the AP600 certified design will review differences between the as-built plant and the design used as the basis for the AP600 PRA and Table 19.59-29. If the effects of the differences are shown, by a screening analysis, to

potentially result in a significant increase in core damage freqency or large release frequency, the PRA will be updated to reflect these differences.

The Combined License applicant referencing the AP600 certified design will review differences between the as-built plant and the design used as the basis for the AP600 internal fire and internal flood analysis. Differences will be evaluated to determine if there is significant adverse effect on the internal fire and internal flood analysis results.

The Combined License applicant referencing the AP600 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", (Reference 19.59-2).

The Combined License applicant referencing the AP600 certified design will perform a thermal lag assessment of the as-built equipment required to mitigate severe accidents (hydrogen igniters and containment penetrations) to provide additional assurance that this equipment can perform its severe accident functions during environmental conditions resulting from hydrogen burns associated with severe accidents. This assessment is only required for equipment used for severe accident mitigation that has not been tested at severe accident conditions. The Combined License applicant will assess the ability of the as-built equipment to perform during severe accident hydrogen burns, utilizing the Environment Enveloping method or the Test Based Thermal Analysis method discussed in EPRI NP-4354 (Reference 19.59-3).

19.59.11 References

19.59-1 "AP600 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process", WCAP-13856, Revision 1, January 1998.

19.59-2 "Framework for AP600 Severe Accident Management Guidance", WCAP-13914, Revision 3, January, 1998.

19.59-3 "Large Scale Hydrogen Burn Equipment Experiments", EPRI-NP-4354, December 1985.

Table 19.59-1
CONTRIBUTION OF INITIATING EVENTS TO CORE DAMAGE

This table intentionally blank.

Table 19.59-2
CONDITIONAL CORE DAMAGE PROBABILITY OF INITIATING EVENTS

This table intentionally blank.

Table 19.59-3
INTERNAL INITIATING EVENTS AT POWER DOMINANT CORE DAMAGE SEQUENCES

This table intentionally blank.

Table 19.59-4
SEQUENCE 1 - SAFETY INJECTION LINE BREAK DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-5
SEQUENCE 2 - INTERMEDIATE LOCA DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-6
SEQUENCE 3 - LARGE LOCA DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-7
SEQUENCE 4 - LARGE LOCA DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-8
SEQUENCE 5 - REACTOR VESSEL RUPTURE CUTSET

This table intentionally blank.

Table 19.59-9
SEQUENCE 6 - LARGE LOCA DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-10
SEQUENCE 7 - ATWS DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-11
SEQUENCE 8 - MEDIUM LOCA DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-12
SEQUENCE 9 - ATWS DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-13
SEQUENCE 10 - INTERMEDIATE LOCA DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-14
SEQUENCE 11 - SAFETY INJECTION LINE BREAK DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-15
SEQUENCE 12 - SMALL LOCA DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-16
SEQUENCE 13 - CORE MAKEUP TANK LINE BREAK DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-17
SEQUENCE 14 - STEAM GENERATOR TUBE RUPTURE DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-18
SEQUENCE 15 - STEAM GENERATOR TUBE RUPTURE DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-19
SEQUENCE 16 - LARGE LOCA DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-20
SEQUENCE 17 - LARGE LOCA DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-21
SEQUENCE 18 - CONSEQUENTIAL SGTR DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-22
SEQUENCE 19 - INTERMEDIATE LOCA DOMINANT CUTSETS

This table intentionally blank.

Table 19.59-23
TYPICAL SYSTEM FAILURE PROBABILITIES, SHOWING HIGHER RELIABILITIES FOR SAFETY SYSTEMS

This table intentionally blank.

Table 19.59-24
DOMINANT CET SEQUENCES

This table intentionally blank.

Table 19.59-25
COMPARISON OF INITIATING EVENT CONTRIBUTION TO CORE DAMAGE AND LARGE RELEASE FREQUENCIES

This table intentionally blank.

Table 19.59-26
SUMMARY OF AP600 PRA RESULTS

This table intentionally blank.

Table 19.59-27
COMPARISON OF AP600 PRA RESULTS TO RISK GOALS

This table intentionally blank.

Table 19.59-28
SITE BOUNDARY DOSE RISK AT 24 HOURS

This table intentionally blank.

Table 19.59-29 (Sheet 1 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
1.	The passive core cooling system (PXS) is composed of the following: - Accumulator subsystem - Core makeup tank (CMT) subsystem - In-containment refueling water storage tank (IRWST) subsystem - Passive residual heat removal (PRHR) subsystem. The automatic depressurization system (ADS), which is part of the reactor coolant system (RCS), also supports passive core cooling functions.	
1a.	The accumulators provide a safety-related means of safety injection of borated water to the RCS. The following are some important aspects of the accumulator subsystem as represented in the PRA:	6.3.2
	- There are two accumulators, each with an injection line to the reactor vessel/direct vessel injection (DVI) nozzle. Each injection line has two check valves in series.	Tier 1 Information
	- The reliability of the accumulator subsystem is important. The accumulator subsystem is included in the RAP.	17.4
	- Diversity between the accumulator check valves and the CMT check valves minimizes the potential for common cause failures.	6.3.2

Table 19.59-29 (Sheet 2 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
1b.	ADS provides a safety-related means of depressurizing the RCS.	Tier 1 Information
	The following are some important aspects of ADS as represented in the PRA:	
	ADS has four stages. Each stage is arranged into two separate groups of valves and lines. - Stages 1, 2, and 3 discharge from the top of the pressurizer to the IRWST - Stage 4 discharges from the hot leg to the RCS loop compartment.	Tier 1 Information
	Each stage 1, 2, and 3 line contains two motor-operated valves (MOVs).	Tier 1 Information
	Each stage 4 line contains an MOV valve and a squib valve.	Tier 1 Information
	The valve arrangement and positioning for each stage is designed to reduce spurious actuation of ADS. - Stage 1, 2, and 3 MOVs are normally closed and have separate controls. - Each stage 4 squib valve has redundant, series controllers. - Stage 4 is blocked from opening at high RCS pressures.	6.3.2
	The ADS valves are automatically and manually actuated via the protection and safety monitoring system (PMS), and manually actuated via the diverse actuation system (DAS).	Tier 1 Information
	The ADS valves are powered from Class 1E dc power.	Tier 1 Information
	The ADS valve positions are indicated and alarmed in the control room.	6.3.7
	Stage 1, 2, and 3 valves are stroke-tested every cold shutdown. Stage 4 squib valve actuators are tested every 2 years for 20% of the valves.	3.9.6
	Because of the potential for counter-current flow limitation in the surgeline, it is essential to establish and maintain venting capability with ADS Stage 4 for gravity injection and containment recirculation following an extended loss of RNS when the RCS is open during shutdown operations.	6.3.3.4.3
	ADS 4th stage squib valves receive a signal to open during shutdown conditions using PMS low hot leg level logic.	6.3
	The reliability of the ADS is important. The ADS is included in the RAP.	17.4

Table 19.59-29 (Sheet 3 of 26)

AP600 PRA-BASED INSIGHTS

INSIGHT	DISPOSITION
1.b (cont.) ADS is required by the Technical Specifications to be available in Modes 1 through 6 without the cavity flooded.	16.1
Stages 1, 2, and 3, connected to the top of the pressurizer, provide a vent path to preclude pressurization of the RCS during shutdown conditions if decay heat removal is lost.	16.1
Depressurization of the RCS through ADS minimizes the potential for high-pressure melt ejection events. - Procedures will be provided for use of the ADS for depressurization of the RCS after core uncovery.	Emergency Response Guidelines
The ADS mitigates high pressure core damage events which can produce challenges to containment integrity due to the following severe accident phenomena: - High pressure melt ejection - Direct containment heating - Induced steam generator tube rupture - Induced RCS piping rupture and rapid hydrogen release to containment	19.36
1c. The CMTs provide safety-related means of high-pressure safety injection of borated water to the RCS.	6.3.1
The following are some important aspects of CMT subsystem as represented in the PRA:	
There are two CMTs, each with an injection line to the reactor vessel/DVI nozzle. - Each CMT has a normally open pressure balance line from an RCS cold leg. - Each injection line is isolated with a parallel set of air-operated valves (AOVs). - These AOVs open on loss of Class 1E dc power, loss of air, or loss of the signal from the PMS. - The injection line for each CMT also has two normally open check valves in series.	6.3.2

Table 19.59-29 (Sheet 4 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
1c. (cont.)		
	The CMT AOVs are automatically and manually actuated from PMS and DAS.	Tier 1 Information
	CMT level instrumentation provides an actuation signal to initiate automatic ADS and provides the actuation signal for the IRWST squib valves to open.	6.3.1 & 7.3.1
	The CMT AOV positions are indicated and alarmed in the control room.	6.3.7
	CMT AOVs are stroke-tested quarterly.	3.9.6
	The CMTs are risk-important for power conditions because the level indicators in the CMTs provide an open signal to ADS and to the IRWST squib valves as the CMTs empty. - The CMT subsystem is included in the RAP.	17.4
	CMT is required by the Technical Specifications to be available in Modes 1 through 6 with RCS pressure boundary intact.	16.1
1d.	IRWST subsystem provides a safety-related means of performing the following functions: - Low-pressure safety injection following ADS actuation - Long-term core cooling via containment recirculation - Reactor vessel cooling through the flooding of the reactor cavity by draining the IRWST into the containment.	6.3
	The following are some important aspects of the IRWST subsystem as represented in the PRA:	
	IRWST subsystem has the following flowpaths: - Two (redundant) injection lines from IRWST to reactor vessel/DVI nozzle. Each line is isolated with a parallel set of valves; each set with a check valve in series with a squib valve. - Two (redundant) recirculation lines from the containment to the reactor vessel/DVI injection line. Each recirculation line has two paths: one path contains a squib valve and a MOV, the other path contains a squib valve and a check valve. - The two MOV/squib valve lines also provide the capability to flood the reactor cavity.	Tier 1 Information
	There are screens for each IRWST injection line and recirculation line.	Tier 1 Information

Table 19.59-29 (Sheet 5 of 26)

AP600 PRA-BASED INSIGHTS

INSIGHT	DISPOSITION
1d. (cont.)	
Squib valves provide the pressure boundary and prevent the check valves from normally seeing a high delta-P.	6.3.3
Squib valves and MOVs are powered by Class 1E dc power.	Tier 1 Information
The squib valves and MOVs for injection and recirculation are automatically and manually actuated via PMS, and manually actuated via DAS.	Tier 1 Information
The squib valves and MOVs for reactor cavity flooding are manually actuated via PMS and DAS from the control room.	Tier 1 Information
Diversity of the squib valves in the injection lines and recirculation lines minimizes the potential for common cause failure between injection and recirculation/reactor cavity flooding.	6.3.2
Automatic IRWST injection at shutdown conditions is provided using PMS low hot leg level logic.	7.3.1
The positions of the squib valves and MOVs are indicated and alarmed in the control room.	6.3.7
IRWST injection and recirculation check valves are exercised at each refueling. IRWST injection and recirculation squib valve actuators are tested every 2 years for 20% of the valves (This does not require valve actuation) . IRWST recirculation MOVs are stroke-tested quarterly.	3.9.6
The reliability of the IRWST subsystem is important. The IRWST subsystem is included in the RAP	17.4
IRWST injection and recirculation are required by Technical Specifications to be available in Modes 1 through 6 without the cavity flooded.	16.1
The operator action to flood the reactor cavity is determined in Emergency Response Guideline FR-C.1, which instructs the operator to flood the reactor cavity if injection to the RCS cannot be recovered or containment radiation reaches a level that indicates fission-product releases as determined by a core damage assessment guideline.	Emergency Response Guidelines
PXS recirculation valves are automatically actuated by a low IRWST level signal or manually from the control room, if automatic actuation fails.	6.3

Table 19.59-29 (Sheet 6 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
1e.	Passive residual heat removal (PRHR) provides a safety-related means of performing the following functions: - Removes core decay heat during accidents - Allows automatic termination of RCS leak during a steam generator tube rupture (SGTR) without ADS - Allows plant to ride out an ATWS event without rod insertion.	6.3.1 & 6.3.3
	The following are some important aspects of the PRHR subsystem as represented in the PRA:	
	PRHR is actuated by opening redundant parallel air-operated valves. These air-operated valves open on loss of Class 1E power, loss of air, or loss of the signal from PMS.	6.3.2
	The PRHR air-operated valves are automatically actuated and manually actuated from the control room by either PMS or DAS.	Tier 1 Information
	Diversity of the PRHR air-operated valves from the CMT air-operated valves minimizes the probability for common cause failure of both PRHR and CMT air-operated valves.	6.3.2
	Long-term cooling of PRHR will result in steaming to the containment. The steam will normally condense on the containment shell and return to the IRWST. If the steam condensation does not return to the IRWST, the IRWST volume is sufficient for at least 72 hours of PRHR operation. Connections are provided to IRWST from the spent fuel system (SFS) and chemical and volume control system (CVS) to extend PRHR operation. A safety-related makeup connection is also provided from outside the containment through the normal residual heat removal system (RNS) to the IRWST.	6.3.1 & system drawings
	Capability exists and guidance is provided for the control room operator to identify a leak in the PRHR HX of 500 gpd. This limit is based on the assumption that a single crack leaking this amount would not lead to a PRHR HX tube rupture under the stress conditions involving the pressure and temperature gradients expected during design basis accidents, which the PRHR HX is designed to mitigate.	6.3.3 & 16.1
	The positions of the inlet and outlet PRHR valves are indicated and alarmed in the control room.	6.3.7
	PRHR air-operated valves are stroke-tested quarterly. The PRHR HX is tested to detect system performance degradation evert 10 years.	3.9.6
	PRHR is required by the Technical Specifications to be available from Modes 1 through 6 with RCS pressure boundary intact.	16.1

Table 19.59-29 (Sheet 7 of 26)

AP600 PRA-BASED INSIGHTS

INSIGHT	DISPOSITION
1e. (cont.) The PRHR HX, in conjunction with the PCS, can provide core cooling for an indefinite period of time. After the IRWST water reaches its saturation temperature, the process of steaming to the containment initiates. Condensation occurs on the steel containment vessel, and the condensate is collected in a safety-related gutter arrangement, which returns the condensate to the IRWST. The gutter normally drains to the containment sump, but when the PRHR HX actuates, safety-related isolation valves in the gutter drain line shut and the gutter overflow returns directly to the IRWST. The following design features provide proper re-alignment for the gutter system valves to direct water to the IRWST: - IRWST gutter and its isolation valves are safety-related - Valves that redirect the flow are designed to fail closed on loss of compressed air, loss of Class 1E dc power, or loss of the PMS signal - Isolation valves are actuated automatically by PMS and DAS.	6.3.2.1.1
The PRHR subsystem provides a safety-related means of removing decay heat following loss of RNS cooling during safe/cold shutdown with the RCS intact.	16.1
2. The protection and safety monitoring system (PMS) provides a safety-related means of performing the following functions: - Initiates automatic and manual reactor trip - Automatic and manual actuation of engineered safety features (ESF).	Tier 1 Information
PMS monitors the safety-related functions during and following an accident as discussed in Regulatory Guide 1.97	7.1.1
PMS has four divisions of reactor trip and ESF actuation. PMS automatically produces a safety-related reactor trip or ESF initiation upon an attempt to bypass more than two channels of a function that uses 2-out-of-4 logic.	Tier 1 Information
PMS has redundant divisions of safety-related post-accident parameter display.	7.1.2.6 & Figure 7.1-8
Each PMS division is powered from its respective Class 1E dc division.	Tier 1 Information
PMS provides selected fixed controls in the control room.	Tier 1 Information

Table 19.59-29 (Sheet 8 of 26)

AP600 PRA-BASED INSIGHTS

INSIGHT	DISPOSITION
2. (cont.) Reliability of the PMS is provided by the following: - The reactor trip functions are divided into two functionally diverse subsystems. - The ESF functions are processed by two microprocessor-based subsystems that are functionally identical in both hardware and software.	7.1.2.2.1 7.1.2.2.6 & 7.1.2.3.1
Four sensors normally monitor variables used for an ESF actuation. These sensors may monitor the same variable for a reactor trip function.	7.3.1
Continuous automatic PMS system monitoring and failure detection/alarm is provided.	7.1.2
PMS equipment is designed to accommodate a loss of the normal heating, ventilation, and air conditioning (HVAC). PMS equipment is protected by the passive heat sinks upon failure or degradation of the active HVAC.	7.1.4.1.6
The reliability of the PMS is important. The PMS is included in the RAP.	17.4
The PMS software is designed, tested, and maintained to be reliable under a controlled verification and validation program written in accordance with IEEE 7-4.3.2 (1993) that has been endorsed by Regulatory Guide 1.152. Elements that contribute to a reliable software design include: - A formalized development, modification, and acceptance process in accordance with an approved software QA plan (paraphrased from IEEE standard, section 5.3, "Quality") - A verification and validation program prepared to confirm the design implemented will function as required (IEEE standard, section 5.3.4, "Verification and Validation") - Equipment qualification testing performed to demonstrate that the system will function as required in the environment it is intended to be installed in (IEEE standard, section 5.4, "Equipment Qualification") - Design for system integrity (performing its intended safety function) when subjected to all conditions, external or internal, that have significant potential for defeating the safety function (abnormal conditions and events) (IEEE standard, section 5.5, "System Integrity") - Software configuration management process (IEEE standard, section 5.3.5, "Software Configuration Management").	App 1A (Compliance with Reg. Guide 1.152)

Table 19.59-29 (Sheet 9 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
3.	The diverse actuation system (DAS) provides a nonsafety-related means of performing the following functions: - Initiates automatic and manual reactor trip - Automatic and manual actuation of selected engineered safety features.	Tier 1 Information
	Diversity is assumed in the PRA that eliminates the potential for common cause failures between PMS and DAS. - The DAS automatic actuation signals are generated in a functionally diverse manner from the PMS signals. Diversity between DAS and PMS is achieved by the use of different architecture, different hardware implementations, and different software.	Tier 1 Information
	DAS provides control room displays and fixed position controls to allow the operators to take manual actions.	7.7.1
	DAS actuates using 2-out-of-2 logic. Actuation signals are output to the loads in the form of normally de-energized, energize-to-actuate signals. The normally de-energized output state, along with the dual 2-out-of-2 redundancy, reduces the probability of inadvertent actuation.	7.7.1.11
	The actuation devices of DAS and PMS are capable of independent operation that is not affected by the operation of the other. The DAS is designed to actuate components only in a manner that initiates the safety function.	7.7.1.11
	The DAS reactor trip function is to trip the control rods by deenergizing the motor-generator set.	7.7.1.11
	In the PRA it is assumed the following eliminates the potential for common cause failures between automatic and manual DAS functions. - DAS manual initiation functions are implemented in a manner that bypasses the signal processing equipment of the DAS automatic logic.	Tier 1 Information
	The DAS, including the M-G set field breakers, is included in the RAP	17.4
4.	The plant control system (PLS) provides a nonsafety-related means of controlling nonsafety-related equipment. - Automatic and manual control of nonsafety-related functions, including "defense-in-depth" systems. - Provides control room indication for monitoring overall plant and nonsafety-related system performance.	7.1.3 & 7.1.1
	PLS has appropriate redundancy to minimize plant transients.	7.7.1.12
	PLS provides capability for both automatic control and manual control.	7.1.3

Table 19.59-29 (Sheet 10 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
4. (cont.)	Redundant signal selectors provide PLS with the ability to obtain inputs from the integrated protection cabinets in the PMS. The signal selector function maintains the independence of the PLS and PMS. The signal selectors select those protection system signals that represent the actual status of the plant and reject erroneous signals.	7.1.3.2
	PLS control functions are distributed across multiple distributed controllers so that single failures within a controller do not degrade the performance of control functions performed by other controllers.	7.1.3.1
5.	The onsite power system consists of the main ac power system and the dc power system. The main ac power system is a non-Class 1E system. The dc power system consists of two independent systems: the Class 1E dc system and the non-Class 1E dc system.	Tier 1 Information
5a.	The onsite main ac power system is a non-Class 1E system comprised of a normal and standby power system.	8.3.1.1
	The main ac power system distributes power to the reactor, turbine, and balance of plant auxiliary electrical loads for startup, normal operation, and normal/emergency shutdown.	8.3.1.1.3
	The arrangement of the buses permits feeding functionally redundant pumps or groups of loads from separate buses and enhances the plant operational reliability.	8.3.1.1.1
	During power generation mode, the turbine generator normally supplies electric power to the plant auxiliary loads through the unit auxiliary transformers. During plant startup, shutdown, and maintenance, the main ac power is provided from the high-voltage switchyard. The onsite standby power system powered by the two onsite standby diesel generators supplies power to selected loads in the event of loss of normal and preferred ac power supplies.	8.3.1.1.1
	Two onsite standby diesel generator units, each furnished with its own support subsystems, provide power to the selected plant nonsafety-related ac loads.	8.3.1.1.2.1
	On loss of power to a 4160 V diesel-backed bus, the associated diesel generator automatically starts and produces ac power. The normal source circuit breaker and bus load circuit breakers are opened, and the generator is connected to the bus. Each generator has an automatic load sequencer to enable controlled loading on the associated buses.	Tier 1 Information

Table 19.59-29 (Sheet 11 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
5b.	The Class 1E dc and uninterruptible power supply (UPS) system (IDS) provides reliable power for the safety-related equipment required for the plant instrumentation, control, monitoring, and other vital functions needed for shutdown of the plant.	8.3.2.1
	There are four independent, Class 1E 125 Vdc divisions. Divisions A and D each consists of one battery bank, one switchboard, and one battery charger. Divisions B and C are each composed of two battery banks, two switchboards, and two battery chargers. The first battery bank in the four divisions is designated as the 24-hour battery bank. The second battery bank in Divisions B and C is designated as the 72-hour battery bank.	Tier 1 Information
	The 24-hour battery banks provide power to the loads required for the first 24 hours following an event of loss of all ac power sources concurrent with a design basis accident. The 72-hour battery banks provide power to those loads requiring power for 72 hours following the same event.	Tier 1 Information
	Battery chargers are connected to dc switchboard buses. The input ac power for the Class 1E dc battery chargers is supplied from non-Class 1E 480 Vac diesel-generator-backed motor control centers.	8.3.2.1.1.1
	The 24-hour and the 72-hour battery banks are housed in ventilated rooms apart from chargers and distribution equipment.	8.3.2.1.3
	Each of the four divisions of dc systems are electrically isolated and physically separated to prevent an event from causing the loss of more than one division.	8.3.2.1.3
	The Class 1E batteries are included in the RAP.	17.4
5c.	The non-Class 1E dc and UPS system (EDS) consists of the electric power supply and distribution equipment that provide dc and uninterruptible ac power to nonsafety-related loads.	Tier 1 Information
	The non-Class 1E dc and UPS system consists of two subsystems representing two separate power supply trains.	8.3.2.1.2
	EDS load groups 1, 2, and 3 provide 125 Vdc power to the associated inverter units that supply the ac power to the non-Class 1E uninterruptible power supply ac system.	Tier 1 Information
	The onsite standby diesel-generator-backed 480 Vac distribution system provides the normal ac power to the battery chargers	Tier 1 Information
	The batteries are sized to supply the system loads for a period of at least two hours after loss of all ac power sources	8.3.2.1.2

Table 19.59-29 (Sheet 12 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
6.	The normal residual heat removal system (RNS) provides a safety-related means of performing the following functions: - Containment isolation for the RNS lines that penetrate the containment - Isolation of the reactor coolant system at the RNS suction and discharge lines - Long-term, post-accident makeup of containment inventory.	Tier 1 Information
	RNS provides a nonsafety-related means of core cooling through: - RCS recirculation at shutdown conditions - Low pressure pumped injection from the IRWST and long-term pumped recirculation from the containment.	5.4.7
	The RNS has redundant pumps and heat exchangers. The pumps are powered by non-Class 1E power with backup connections from the diesel generators.	5.4.7 & 8.3
	RNS is manually aligned from the control room to perform its core cooling functions. The performance of the RNS is indicated in the control room.	5.4.7
	The RNS containment isolation and pressure boundary valves are safety-related. The motor-operated valves are powered by Class 1E dc power.	Tier 1 Information
	The RNS containment isolation MOVs are automatically and manually actuated via PMS.	7.3.1
	Interfacing system loss-of-coolant accident (LOCA) between the RNS and the RCS is prevented by: - Each RNS line is isolated by at least three valves. - The RNS equipment outside containment is capable of withstanding the operating pressure of the RCS. - The RCS isolation valves are interlocked to prevent their opening at RCS pressures above its design pressure.	5.4.7.2.2
	CCS provides cooling to the RNS heat exchanger.	Tier 1 Information
	Planned maintenance affecting the RNS cooling function and its support systems CCS and SWS should be performed in modes 1, 2, and 3, when the RNS is not normally operating.	16.3

Table 19.59-29 (Sheet 13 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
7.	The component cooling water system (CCS) is a nonsafety-related system that removes heat from various components and transfers the heat to the service water system.	Tier 1 Information
	The CCS has redundant pumps and heat exchangers.	Tier 1 Information
	During normal operation, one CCS pump is operating. The standby pump is aligned to automatically start in case of a failure of the operating CCS pump.	9.2.2.4.2
	The CCS pumps are automatically loaded on the standby diesel generator in the event of a loss of normal ac power. The CCS, therefore, continues to provide cooling of required components if normal ac power is lost.	9.2.2.4.5.4
8.	The service water system (SWS) is a nonsafety-related system that transfers heat from the component cooling water heat exchangers to the atmosphere.	Tier 1 Information
	The SWS has redundant pumps, strainers, and cooling tower cells.	9.2.1.2.1
	During normal operation, one SWS train of equipment is operating. The standby train is aligned to automatically start in case of a failure of the operating SWS pump.	9.2.1.2.3.3
	The SWS pumps and cooling tower fans are automatically loaded onto their associated diesel bus in the event of a loss of normal ac power. Both pumps and cooling tower fans automatically start after power from the diesel generator is available.	9.2.1.2.3.6
9.	The chemical and volume control system (CVS) provides a safety-related means to terminate inadvertent RCS boron dilution.	Tier 1 Information
	The CVS provides a nonsafety-related means to perform the following functions: - Makeup water to the RCS during normal plant operation - Boration following a failure of reactor trip - Coolant to the pressurizer auxiliary spray line.	Tier 1 Information
	Two makeup pumps are provided. Each pump provides capability for normal makeup.	9.3.6.3.1
	Two safety-related air-operated valves provide isolation of normal CVS letdown during shutdown operation on low hot leg level.	9.3.6

Table 19.59-29 (Sheet 14 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
10.	The operation of RNS and its support systems (CCS, SWS, main ac power and onsite power) is RTNSS-important for shutdown decay heat removal during reduced RCS inventory operations. - These systems are included in the RAP. Short-term availability controls for the RNS during at-power conditions reduce PRA uncertainties.	16.3 17.4 16.3
11.	The information used by the COL regarding critical human actions (if any) and risk-important tasks from the PRA, as presented in Chapter 18 of the SSAR on human factors engineering, is important in developing and implementing procedures, training, and other human reliability related programs.	18
12.	Sufficient instrumentation and control is provided at the remote shutdown workstation to bring the plant to safe shutdown conditions in case the control room must be evacuated. There are no differences between the main control room and remote shutdown workstation controls and monitoring that would be expected to affect safety system redundancy and reliability.	7.4.3 7.4.3.1.1
13.	Separation or protection of the equipment and cabling among the divisions of safety-related equipment and separation of safety-related from nonsafety-related equipment minimizes the probability that a fire or flood would affect more than one safety-related system or train, except in some areas inside containment where equipment will be capable of achieving safe shutdown prior to damage. Although the containment is a single fire area, adequate design features exist for separation (structural or space), suppression, lack of combustibles, or operator action to ensure the plant can achieve safe shutdown. To prevent flooding in a radiologically controlled area (RCA) in the Auxiliary Building from propagating to non-radiologically controlled areas, the non-RCAs are separated from the RCAs by 2 and 3-foot walls and floor slabs. In addition, electrical penetrations between RCAs and non-RCAs in the Auxiliary Building are located above the maximum flood level.	3.4.1.1.2, 9.5.1.2.1.1 & 9A 9A 3.4.1.2.2.2

Table 19.59-29 (Sheet 15 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
14.	The following minimizes the probability for fire and flood propagation from one area to another and helps limit risk from internal fires and floods:	
	- Fire barriers are sealed, to the extent possible (i.e., doors)	9.5.1.2.1.1
	- Structural barriers which function as flood barriers are watertight below the maximum flood level.	3.4.1.1.2
	- Establishing administrative controls to maintain the performance of the fire protection system is the responsibility of the COL applicant.	Table 9.5.1-1, Item 29
15.	Fire detection and suppression capability is provided in the design. Flooding control features and sump level indication are provided in the design.	3.4.1, 9.5.1.2.1.2, & 9.5.1.8
	Establishing administrative controls to maintain the performance of the fire protection system is the responsibility of the COL applicant.	Table 9.5.1-1, Item 29
16.	AP600 main control room fire ignition frequency is limited as a result of the use of low-voltage, low-current equipment and fiber optic cables.	7.1.2 & 7.1.3
	There is no cable spreading room in the AP600 design.	Table 9.5.1-1
17.	Redundancy in control room operations is provided within the control room itself for fires in which control room evacuation is not required.	9.5.1.2.1.1
18.	The remote shutdown workstation provides redundancy of control and monitoring for safe shutdown functions in the event that main control room evacuation is required.	7.3 & 9.5
	The remote shutdown workstation is in a fire and flood area separate from the main control room.	7.1.2, 7.4.3.1.1. & 9A.3.1.2.5
19.	Although a main control room fire may defeat manual actuation of equipment from the main control room, it will not affect the automatic functioning of safe shutdown equipment via PMS or manual operation from the remote shutdown workstation. This is because the ESF and protection logic cabinets, in which the automatic functions are housed, are located in fire areas separate from the main control room.	7.1.2.7 & 9A.3

Table 19.59-29 (Sheet 16 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
20.	The main control room has its own ventilation system, and is pressurized. This prevents smoke, hot gases, or fire suppressants originating in areas outside the control room from entering the control room via the ventilation system.	9.4.1
	There are separate ventilation systems for safety-related equipment divisions (A & C and B & D). This prevents smoke, hot gases, or fire suppressants originating from one fire area to another to the extent that they could adversely affect safe shutdown capabilities	9.4.1 9.5.1.1.1
	The ventilation system for the remote shutdown workstation is independent of the ventilation system for the main control room.	9.4.1
21.	AP600 does not rely on ac power sources for safe shutdown capability since the safety-related passive systems do not require ac power sources for operation. Individual fires resulting in loss of offsite power or affecting onsite standby diesel generator operability do not affect safe shutdown capability.	8.1.4.2
22.	Containment isolation functions are not compromised by internal fire or flood. Redundant containment isolation valves in a given line are located in separate fire and flood areas or zones and, if powered, are served by different control and electrical division.	6.2.3
	One isolation component in a given line is located inside containment, while the other is located outside containment, and the containment wall is a fire/flood barrier.	6.2.3 & 9.5
23.	The AP600 design minimizes potential flooding sources in safety-related equipment areas, to the extent possible. The design also minimizes the number of penetrations through enclosure or barrier walls below the probable maximum flood level. Walls, floors, and penetrations are designed to withstand the maximum anticipated hydrodynamic loads.	3.4.1
24.	The Combined License applicant referencing the AP600 certified design will review differences between the as-built plant and the design used as the basis for the AP600 seismic margins analysis.	19.59.10.6
25.	The depressurization of the reactor coolant system below 150 psi facilitates in-vessel retention of molten core debris.	19.36

Table 19.59-29 (Sheet 17 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
26.	The reflective reactor vessel insulation provides an engineered flow path to allow the ingression of water and venting of steam for externally cooling the vessel in the event of a severe accident involving core relocation to the lower plenum. The reflective insulation panels and support members can withstand pressure differential loading due to the IVR boiling phenomena. Water inlets and steam vents are provided at the entrance and exit of the insulation boundary. The reactor vessel insulation is included in the RAP. No coatings are applied to the outside surface of the reactor vessel which will inhibit the wettability of the surface.	19.39, 5.3.5 & Tier 1 Information 17.4
27.	The reactor cavity design provides a reasonable balance between the regulatory requirements for sufficient ex-vessel debris spreading area and the need to quickly submerge the reactor vessel for the in-vessel retention of core debris.	19.39 & Appendix 19B
28.	The design can withstand a best-estimate ex-vessel steam explosion without failing the containment integrity.	Appendix 19B
29.	The containment design incorporates defense-in-depth for mitigating direct containment heating by providing no significant direct flow path for the transport of particulate molten debris from the reactor cavity to the upper containment regions.	Appendix 19B
30.	The hydrogen control system is comprised of passive autocatalytic recombiners (PARs) and hydrogen igniters to limit the concentration of hydrogen in the containment during accidents and beyond design basis accidents, respectively. Operability of the hydrogen igniters is addressed by short-term availability controls during modes 1, 2, 5 (with RCS pressure boundary open), and 6 (with upper internals in place and cavity levels less than full). The operator action to activate the igniters is the first step in ERG FR.C-1 to ensure that the igniter activation occurs prior to rapid cladding oxidation.	Tier 1 Information 16.3 Emergency Response Guidelines

Table 19.59-29 (Sheet 18 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
31.	Mitigation of the effects of a diffusion flame on the containment shell are addressed by the following containment layout features: - Vents from compartments where hydrogen releases can be postulated are not adjacent to the containment wall and penetrations or are hatched and locked closed. - IRWST vents near the containment wall are turned to direct releases away from the containment shell.	1.2, General Arrangement Drawings
32.	The containment structure can withstand the pressurization from a LOCA and the global combustion of hydrogen released in-vessel (10 CFR 50.34(f)).	19.41
33.	The steam generator should not be depressurized to cool down the RCS if water is not available to the secondary side. This action protects the tubes from large pressure differential and minimizes the potential for creep rupture. The COL will develop and implement severe accident management guidance using the suggested framework provided in WCAP-13914.	19.59.10
34.	Depressurizing the RCS and maintaining a water level covering the SG tubes on the secondary side can mitigate fission product releases from a steam generator tube rupture accident. The COL will develop and implement severe accident management guidance using the suggested framework provided in WCAP-13914.	19.59.10
35.	Loss of ac power does not contribute significantly to the core damage frequency. - Nonsafety-related containment spray does not need to be ac independent.	19.59
36.	AP600 has a nonsafety-related containment spray system. Containment spray is not credited in the PRA. Failure of the nonsafety-related containment spray does not prevent the plant achieving the safety goals. The COL will develop and implement severe accident management guidance for operation of the nonsafety-related containment spray system using the suggested framework provided in WCAP-13914.	6.5.2 19.59 19.59.10
37.	Passive containment can withstand severe accidents without PCS water cooling the containment shell. Air cooling alone is sufficient to maintain containment pressure below failure pressure. Flooding of the PCS annulus due to failure of the annulus drains is a PRA-postulated mechanism for the failure of PCS cooling.	19.40

Table 19.59-29 (Sheet 19 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
38.	Operation of ADS stage 4 provides a vent path for the severe accident hydrogen to the steam generator compartments, bypassing the IRWST, and mitigating the conditions required to produce a diffusion flame near the containment wall. The openings from the PXS valve/accumulator rooms and CVS compartment that can vent hydrogen to the maintenance floor are either located away from the containment wall and electrical penetration junction boxes or are covered by a secure hatch. This mitigates the effect of postulated diffusion flames.	19.41
39.	Containment isolation valves controlled by DAS are important in limiting offsite releases following core melt accidents. The containment isolation valves are included in the RAP. Operability of DAS for selected containment isolation actuations is addressed by short-term availability controls.	17.4 16.3
40.	Reflooding the reactor pressure vessel through the break can have a significant effect on a severe accident by quenching core debris, achieving a controlled stable state, and producing hydrogen.	19.38 & 19.41
41.	The type of concrete used in the basemat is not important. The reactor cavity design incorporates features that extend the time to basemat melt-through in the event of RPV failure. The cavity design includes: - A minimum floor area of 48 m^2 available for spreading of the molten core debris - A minimum thickness of concrete above the embedded containment liner of 0.85 m - There is no piping buried in the concrete beneath the reactor cavity; sump drain lines are not enclosed in either of the reactor cavity floor or reactor cavity sump concrete. Thus, there is no direct pathway from the reactor cavity to outside the containment in the event of core-concrete interactions. - The openings between the reactor cavity and cavity sump are small diameter openings in which core debris in the cavity will solidify. Thus, there is no direct pathway for core debris to enter the sump, except in the case where it might spill over the sump curbing.	Appendix 19B Appendix 19B
42.	No safety-related equipment is located outside the Nuclear Island.	3.4.1

Table 19.59-29 (Sheet 20 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
43.	Capability exists to vent the containment via the RNS suction lines to the spent fuel pool, with the RCS depressurized and open to the containment atmosphere via either the ADS or the vessel failure.	Appendix 19D
	The COL will develop and implement severe accident management guidance for venting containment using the suggested framework provided in WCAP-13914.	19.59.10
44.	A list of risk-important systems, structures, and components (SSCs) has been provided in the D-RAP.	17.4
	The risk-significant SSCs are included in the RAP.	17.4
45.	The Combined License applicant referencing the AP600 certified design will review differences between the as-built plant and the design used as the basis for the AP600 PRA and Table 19.59-29. If the effects of the differences are shown, by a screening analysis, to potentially result in a significant increase in core damage freqency or large release frequency, the PRA will be updated to reflect these differences.	19.59.10
46.	There are no watertight doors used for flood protection in the AP600 design.	3.4.1.1.2
	Plugging of the drain headers is minimized by designing them large enough to accommodate more than the design flow and by making the flow path as straight as possible.	9.3.5.1.2
47.	The maintenance guidelines as described in the Shutdown Evaluation Report (WCAP-14837) should be considered when developing the plant specific operations prodecures.	13.5.1
48.	Transient combustibles should be controlled	Table 9.5.1-1, Items 77 - 83
49.	There are two compartments inside containment (PXS-A and PXS-B) containing safe shutdown equipment other than containment isolation valves that are floodable (i.e., below the maximum flood height). Each of these two compartments contains redundant and essentially identical equipment (one accumulator with associated isolation valves as well as isolation valves for one CMT, one IRWST injection line, and one containment recirculation line). These two compartments are physically separated to ensure that a flood in one compartment does not propagate to the other. Drain lines from the PXS-A and PXS-B compartments to the reactor vessel cavity and steam generator compartment are protected from backflow by redundant backflow preventers.	3.4.1.2.2.1

Table 19.59-29 (Sheet 21 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
50.	There are four automatically actuated containment isolation valves inside containment subject to flooding. These four normally closed containment isolation valves would not fail open as a result of the compartment flooding. Also, there is a redundant, normally closed, containment isolation valve located outside containment in series with each of these valves.	3.4.1.2.2.1
51.	The passive containment cooling system (PCS) cooling water not evaporated from the vessel wall flows down to the bottom of the containment annulus. Two 100-percent drain openings, located in the side wall of the Shield Building, are always open with provisions provided to prevent entry of small animals into the drains.	19.40
52.	The major rooms housing divisional cabling and equipment (the battery rooms, dc equipment rooms, I&C rooms, and penetration rooms) are separated by 3-hour fire rated walls. Separate ventilation subsystems are provided. In order for a fire to propagate from one divisional room to another, it must move past a 3-hour barrier (e.g., a door) into a common corridor and enter the room through another 3-hour barrier (e.g., another door).	9A.3
53.	An access bay in the turbine building is provided to protect the north end of the Auxiliary Building, from potential debris produced by postulated seismic damage of the adjacent Turbine Building.	19.55.5
54.	There are no normally open connections to sources of "unlimited" quantity of water in the electrical and I&C portions of the Auxiliary Building such that it could affect safe shutdown capabilities.	Figure 9.5.1-1
55.	To prevent flooding in a radiologically controlled area (RCA) in the Auxiliary Building from propagating to non-RCAs, the non-RCAs are separated from the RCAs by 2- and 3-foot walls and floor slabs. In addition, electrical penetrations between RCAs and non-RCAs in the Auxiliary Building are located above the maximum flood level.	3.4.1.2.2.2
56.	The two 72-hour rated Class 1E division B and C batteries are located above the maximum flood height in the Auxiliary Building considering the possible flooding sources .	9A

Table 19.59-29 (Sheet 22 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
57.	Flood water propagated from the Turbine Building to the Auxiliary Building valve/piping penetration room at grade level is directed to drains. The presence of watertight walls and floor of the valve/penetration room prevents flooding from propagating beyond this area.	3.4.1.2.2.2
58.	The mechanical equipment and electrical equipment in the Auxiliary Building are separated to prevent propagation of leaks from the piping and mechanical equipment areas to the Class 1E equipment and Class 1E I&C equipment rooms.	3.4.1.2.2.2
59.	Connections to sources of "large" quantity of water are located in the Turbine Building. They are the service water system, which interfaces with the component cooling water system; and the circulating water system, which interfaces with the Turbine Building closed cooling system and the condenser. Features that minimize the flood propagation to other buildings are: - Flow from any postulated ruptures above grade level (elevation 100') in the Turbine Building flows down to grade level via floor grating and stairwells. This grating in the floors also prevents any significant propagation of water to the Auxiliary Building via flow under the doors. - A relief panel in the Turbine Building west wall at grade level directs the water outside the building to the yard and limits the maximum flood level in the Turbine Building to less than 6 inches. Flooding propagation to areas of the adjacent Auxiliary Building, via flow under doors or backflow through the drains, is possible but is bounded by a postulated break in those areas.	3.4.1.2.2.3
60.	Flood water in the Annex Building grade level is directed by the sloped floor to drains and to the yard area through the door of the Annex Building. Flow from postulated ruptures above grade level in the Annex Building is directed by floor drains to the Annex Building sump, which discharges to the Turbine Building drain tank. Alternate paths include flow to the Turbine Building via flow under access doors and down to grade level via stairwells and elevator shaft. The floors of the Annex Building are sloped away from the access doors to the Auxiliary Building in the vicinity of the access doors to prevent migration of flood water to the non-RCAs of the Nuclear Island where all safety-related equipment, except for some containment isolation valves, is located.	3.4.1.2.2.3

Table 19.59-29 (Sheet 23 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
61.	There are no connections to sources of "unlimited" quantity of water, except for fire protection, in the Annex Building.	Figure 9.5.1-1
62.	To prevent overdraining, the RCS hot and cold legs are vertically offset, which permits draining of the steam generators for nozzle dam insertion with a hot leg level much higher than traditional designs.	5.4.6
	To lower the RCS hot leg level at which a vortex occurs in the RNS suction line, a step nozzle connection between the RCS hot leg and the RNS suction line is used.	5.4.7 & Figure 5.1-5
	Should vortexing occur, air entrainment into the RNS pump suction is limited.	5.4.7
	There are two safety-related RCS hot leg level channels, one located in each hot leg. These level instruments are independent and do not share instrument lines. These level indicators are provided primarily to monitor RCS level during midloop operations. One level tap is at the bottom of the hot leg, and the other tap is on the top of the hot leg close to the steam generator.	Figure 5.1-5
	Wide range pressurizer level indication (cold calibrated) is provided that can measure RCS level to the bottom of the hot legs. This nonsafety-related pressurizer level indication can be used as an alternative way of monitoring level and can be used to identify inconsistencies in the safety-related hot leg level instrumentation.	Figure 5.1-5
	The RNS pump suction line is sloped continuously upward from the pump to the reactor coolant system hot leg with no local high points. This design eliminates potential problems in refilling the pump suction line if an RNS pump is stopped when cavitating due to excessive air entrainment. This self-venting suction line allows the RNS pumps to be immediately restarted once an adequate level in the hot leg is re-established.	5.4.7
	It is important to maximize the availability of the nonsafety-related wide range pressurizer level indication during RCS draining operations during cold shutdown. The Combined License applicant is responsible for developing procedures and training that encompass this item.	13.5
63.	Solid-state switching devices and electro-mechanical relays resistant to relay chatter will be used in the AP600 safety-related I&C system.	19.55
64.	The annulus drains will have the same or higher HCLPF value as the Shield Building so that the drain system will not fail at lower acceleration levels causing water blocking of the PCS air baffle.	19.59.10

Table 19.59-29 (Sheet 24 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
65.	The ability to close containment hatches and penetrations during Modes 5 & 6 prior to steaming to containment is important. The COL is responsible for developing procedures and training that encompass this item.	13.5 & 16.1
66.	Spurious actuation of squib valves is prevented by the use of a squib valve controller circuit which requires multiple hot shorts for actuation, physical separation of potential hot short locations (e.g., routing of ADS cables and low voltage cable trays, and, in the case of PMS, the use of redundant series controllers located in separate cabinets), and provisions for operator action to remove power from the fire zone.	9A.2.7
67.	For long-term recirculation operation, the RNS pumps can take suction from one of the two sump recirculation lines. Unrestricted flow through both parallel paths is required for success of the sump recirculation function when both RNS pumps are running. If one of the two parallel paths fails to open, operator action is required to manually throttle the RNS discharge MOV (V011) to prevent pump cavitation.	Emergency Response Guidelines
	The containment isolation valves in the RNS piping automatically close via PMS with a high radiation signal. The actuation setpoint was established consistent with a DBA non-mechanistic source term associated with a large LOCA. The containment radiation level for other accidents is expected to be below the point that would cause the RNS MOVs to automatically close.	7.3.1
	With the RNS pumps aligned either to the IRWST or the containment sump, the pumps' net positive suction head is adequate to prevent pump cavitation and failure even when the IRWST or sump inventory is saturated.	5.4.7
	Emergency response guidelines are provided for aligning the RNS from the control room for RCS injection and recirculation.	Emergency Response Guidelines
	The following are additional AP600 features which contribute to the low likelihood of interfacing system LOCAs between the RNS and the RCS: - A relief valve located in the common RNS discharge line outside containment provides protection against excess pressure. - Two remotely operated MOVs connecting the suction and discharge headers to the IRWST are interlocked with the isolation valves connecting the RNS pumps to the hot leg. This prevents inadvertent opening of these two MOVs when the RNS is aligned for shutdown cooling and potential diversion and draining of reactor coolant system. - Power to the four isolation MOVs connecting the RNS pumps to the RCS hot leg is administratively blocked at their motor control centers during normal power operation.	5.4.7

Table 19.59-29 (Sheet 25 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
67. (cont.)	Per the Shutdown Evaluation Report (WCAP-14837), operability of the RNS is tested, via connections to the IRWST, before its alignment to the RCS hot leg for shutdown cooling.	Shutdown Evaluation Report
	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 is responsible for developing administrative controls to ensure that inadvertent opening of this valve is unlikely.	13.5
	The reliability of the IRWST suction isolation valve (V023) to open on demand is important. The IRWST suction isolation valve is included in the RAP.	17.4
68.	The startup feedwater system pumps provide feedwater to the steam generator. This capability provides an alternate core cooling mechanism to the PRHR heat exchangers for non-LOCA or steam generator tube ruptures. The startup feedwater pumps are included in the RAP.	17.4
69.	Capability is provided for on-line testing and calibration of the DAS channels, including sensors.	7.7.1.11
	Short-term availability controls of the DAS during at-power conditions reduce PRA uncertainties.	16.3
70.	One CVS pump is configured to operate on demand while the other CVS pump is in standby. The operation of these pumps will alternate periodically.	19.15
	The safety-related PMS boron dilution signal automatically re-aligns CVS pump suction to the boric acid tank. This signal also closes the two safety-related CVS demineralized water supply valves. This signal actuates on reactor trip signal (interlock P-4), source range flux doubling signal, or low input voltage to the Class 1E dc power system battery chargers.	7.3
71.	The COL applicant will maintain procedures to respond to low hot leg level alarms.	Emergency Response Guidelines
72.	A COL applicant cleanliness program controls foreign debris from being introduced into the IRWST tank and into the containment sump during maintenance and inspection operations.	6.3.2.2.7.2, 6.3.2.2.7.3, & 6.3.8.1
73.	For floor drains, from the reactor cavity to PXS-A and PXS-b rooms, appropriate precautions such as check valves, back flow preventors, and siphon breaks are assumed to prevent back flow from a flooded space to a nonflooded space.	3.4.1.2.2

Table 19.59-29 (Sheet 26 of 26)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
74.	Plant ventilation systems include features to prevent smoke originating from one fire area to another to the extent that they could adversely affect safe shutdown capabilities	9.4.2.2
75.	An alternative gravity injection path is provided through RNS V-023 during cold shutdown and refueling conditions with the RCS open.	Emergency Response Guidelines
	The COL applicant is responsible for developing administrative controls to maximize the likelihood that RNS valve V-023 will be able to open if needed during Mode 5 when the RCS is open, and PRHR cannot be used for core cooling.	13.5
76.	The IRWST suction isolation valve (V023) and the RCS pressure boundary isolation valves (V001A/B, V002A/B) are environmentally qualified to perform their safety functions.	Tier 1 Information
77.	Following an extended loss of RNS during safe/cold shutdown with the RCS intact and PRHR unavailable, it is essential to establish and maintain venting capability with ADS Stage 4 for gravity injection and containment recirculation.	19.59.5

FIGURES 59-1 THROUGH 59-4
NOT INCLUDED IN THE DCD