# AP1000 DESIGN CERTIFICATION REVIEW

## Response to Request For Additional Information

**Design Control Document (DCD) Revision:**

The sections 19.59.9.2 through 19.59.9.5, 19.59.10 and 19.59.11 and the table 19.59-18 are added (see below).

### 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

AP1000 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 for decay heat removal functions, and an example of equipment diversity is the use of different valve operators (motor, air, squib) to avoid 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 are fewer potential equipment failures (pumps and valves) and less maintenance activities.

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 avoid 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. Switchover from injection to recirculation is automatic without manual actions.

The safety-related Class 1E dc and UPS system has a battery capacity sufficient to support passive safety-related systems for 72 hours. This system has four 24-hour batteries, two 72-hour batteries, and a spare battery. The presence of 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 an accident, the containment stays well below the predicted failure pressure. The steaming and condensing action of the passive containment cooling system enhances activity removal.

AP1000 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. 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 of heating, ventilation, and air conditioning (HVAC) penetrations is reduced (no maxi purge connection).

Vessel failure potential upon core damage is reduced (in-vessel retention of the damaged core) by providing a provision to dump 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, AP1000 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.
Post-72-hour connections are incorporated into the passive system design to allow for long-term accident management. These connections allow for the refill of the in-containment refueling water storage tank, or the reactor cavity, should such actions become necessary.

### 19.59.9.2.2 Nonsafety-Related Systems

AP1000 has nonsafety-related systems capable of mitigating accidents. These systems use redundant components, which are powered by offsite and onsite power supplies. AP1000 has certain design features in the nonsafety-related systems to reduce plant risk compared to current operating plants. 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 creates fewer 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 has additional isolation valves 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, operation procedures require both normal residual heat removal system pumps to be operable for risk reduction.

Component cooling water and service water systems have a very 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 very limited role in the plant risk profile since the plant safety-related systems do not depend on ac power. The loss of offsite power event is less important for the AP1000 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 AP1000 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. Four trains of redundancy are provided for the protection and safety monitoring system; 2-out-of-4 actuation logic in the protection and safety monitoring system reduces the potential for spurious trips due to testing and allows for better testing. Automatic 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) for data transmission. Unlike current plants, there is no cable spreading room, thus eliminating a potential fire hazard. 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. In addition, the remote shutdown workstation is designed to have functions similar to the control room.

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 common cause failures in the protection and safety monitoring system.

### 19.59.9.4 Plant Layout

The plant layout minimizes 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 IE instrumentation and control equipment rooms. The potential flooding sources and volumes in areas of the plant that contain safety-related electrical and I&C equipment are limited to minimize the consequences of internal flooding.

AP1000 is designed to provide better separation between divisions of safety-related equipment.

### 19.59.9.5 Containment Design

The containment pressure boundary is the final barrier to the release of fission products to the environment. The AP1000 containment has provisions that help to maintain containment integrity in the event of a severe accident.

### 19.59.9.5.1 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. AP1000 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. All isolation valves have control room indication to inform the operator of the current valve position.

Similarly to containment isolation failure, leakage of closed containment isolation valves in excess of technical specifications may result in larger releases to the environment. Valves that historically have the greatest leakage problems have been eliminated, or their number significantly reduced in the design. 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 to ensure a leak-tight seal. Hatch seals can easily be verified.

Therefore, AP1000 provides significant protection against the failure to isolate the containment and against failure of isolation valves to fully close.

### 19.59.9.5.2 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 steam generator tube ruptures.

An interfacing systems loss-of-coolant accident is the failure of valves that separate the high pressure reactor coolant system with 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. Reactor coolant is lost outside the containment, providing a pathway for the direct release of fission products to the environment. In AP1000, systems connected to the reactor coolant system are designed with higher design pressure, 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 to containment bypass.

Steam generator tube ruptures release coolant from the reactor coolant system to the secondary system. The AP1000 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 is actuated automatically on the S-signal and effectively reduces the reactor coolant system pressure to stop the break flow. If the passive residual heat removal does not stop the loss of coolant, the secondary relief valve can open to keep the secondary system pressure below the opening pressure of the steam generator safety valve. If the loss of reactor coolant continues, the RCS automatic depressurization system will actuate and depressurize the system. No operator actions are required to mitigate the accident, and the secondary system remains sealed against releases to the environment after the relief valve or its block valve are closed.

To create a containment bypass release pathway from a steam generator tube rupture, the accident scenario must include multiple system failures such that the steam generator tube rupture is not mitigated, and the secondary system pressure increases enough to open a safety valve. The safety valve must fail to reseat, thereby providing a containment bypass pathway for the loss of coolant and for the possible release of fission products to the environment.

Multiple, diverse systems act to mitigate steam generator tube rupture. Therefore, the likelihood of a steam generator tube rupture progressing to containment bypass has been significantly reduced in AP1000.

### 19.59.9.5.3 Passive Containment Cooling

The passive containment cooling system provides protection to the containment pressure boundary by removing the decay and chemical heat that slowly pressurize the containment. The 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 design basis accidents.

In some postulated multiple-failure accident scenarios, the water flow may fail. The heat removal is limited to convection heat transfer to the air flow and radiation 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. Containment failure within 24 hours is highly unlikely.

### 19.59.9.5.4 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 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 that may induce large fission product releases early in the accident sequence.

### 19.59.9.5.5 In-Vessel Retention of Molten Core Debris

The AP1000 reactor vessel and containment configuration have features which enhance the design's ability to maintain molten core debris in the reactor vessel. The AP1000 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 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 vessel to cool the external surface of the lower head. Cooling the vessel and reducing the stresses prevents the creep rupture failure of the vessel wall. The reactor vessel reflective insulation has been designed with provisions to allow water inside the insulation panel to cool the vessel surface, and with vents to allow steam to exit the insulation without failing the insulation support structures. The insulation is designed so that it promotes the cooling of the external surface of the vessel.

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. Through the prevention of core debris relocation to the containment, the AP1000 design significantly reduces the likelihood of containment failure.

### 19.59.9.5.6 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 the oxidation of the zircaloy cladding by passing steam generates hydrogen. A second release may occur if the 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. These gases are highly combustible and in high concentrations in the containment may lead to detonable mixtures.

AP1000 employs a nonsafety-related hydrogen igniter system for severe releases of combustible gases. The igniters are powered from ac busses, from either of the nonsafety-related diesel generators or from the non-Class 1E batteries. 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 will not allow the burn to transition from deflagration to detonation. The combustible gases are removed with no threat to the containment integrity.

There is little threat of the failure of the system power in the event that it is required to operate. The igniters are only needed in core damage accidents, and the AP1000 is designed to mitigate loss of power events without the sequence evolving into a severe accident. Loss of ac power is a small contributor to the core damage frequency.

The reliability of reactor coolant system depressurization reduces the threat to the containment from sudden releases of hydrogen from the reactor coolant system. Low pressure release of in-vessel hydrogen enhances the ability of the igniter system to maintain the containment atmosphere at the lower flammability limit.

During a severe accident, hydrogen that could be injected from the reactor coolant system into the containment through the spargers in the in-containment refueling water storage tank or into the core makeup tank room has the potential to produce a diffusion flame. A diffusion flame is produced when a combustible gas plume that 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. The AP1000 uses a defense-in-depth approach to release hydrogen in benign locations away from the containment shell and penetrations. 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 very 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.

### 19.59.9.5.7 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 high likelihood of in-vessel retention of core debris, the potential for ex-vessel combustible gas generation from core-concrete interaction is very low. The frequency of containment failures due to hydrogen combustion events is very low given the high reliability of the hydrogen igniters.

### 19.59.9.5.8 Fission-Product Removal

AP1000 relies on the passive, natural removal of aerosol fission products from the containment atmosphere, primarily from gravitational settling, diffusiophoresis and thermophoresis. Natural removal is enhanced by the passive containment cooling system, which provides a large, cold surface area for condensation of steam. This increases the diffusiophoretic and thermophoretic removal processes. Accident offsite doses at the site boundary that could exist in the first 24 hours after a severe accident are either less than 25 rem, or for those releases that are greater than 25 rem, have a frequency of much less than 1E-06. Minimal credit is taken for deposition of fission products in the auxiliary building. The site boundary dose and large release frequency are much less than the established goals.

### 19.59.10 PRA Input to the Design Certification Process

The AP1000 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 AP1000 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 AP1000 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 AP1000 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 human system interface (HSI) and human factors areas. For more information on the AP1000 HSI, 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 AP1000 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 AP1000 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 AP1000 plant features important to reducing risk is provided in subsection 19.59.9. PRAbased insights are developed from this information and are summarized in Table 19.59-18.

### 19.59.10.5 Combined License Information

The Combined License applicant referencing the AP1000 certified design will review differences between the as-built plant and the design used as the basis for the AP1000 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 AP1000 certified design should compare the as-built SSC HCLPFs to those assumed in the AP1000 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 AP1000 certified design will review differences between the as-built plant and the design used as the basis for the AP1000 PRA and Table 19.59-18. If the effects of the differences are shown, by a screening analysis, to potentially result in a significant increase in core damage frequency or large release frequency, the PRA will be updated to reflect these differences.

The Combined License applicant referencing the AP1000 certified design will review differences between the as-built plant and the design used as the basis for the AP1000 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 AP1000 certified design will develop and implement severe accident management guidance using the suggested framework provided in WCAP-13914, "Framework for AP600 Severe Accident Management Guidance", (Reference 19.59-1).

The Combined License applicant referencing the AP1000 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 19.59-2).

## 19.59.11 References

19.59-1 "Framework for AP600 Severe Accident Management Guidance", WCAP-13914, Revision 3, January, 1998.

19.59-2 "Large Scale Hydrogen Burn Equipment Experiments", EPRI-NP-4354, December 1985.

Table 19.59-29 (Sheet 1 of 26)

AP1000 PRA-BASED INSIGHTS

| INSIGHT | DISPOSITION |
|---|---|
| 1. The passive core cooling system (PXS) is composed of the following:<br>- Accumulator subsystem<br>- Core makeup tank (CMT) subsystem<br>- In-containment refueling water storage tank (IRWST) subsystem<br>- Passive residual heat removal (PRHR) subsystem.<br><br>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.<br><br>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 D-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)**

**AP1000 PRA-BASED INSIGHTS**

| INSIGHT | DISPOSITION |
|---|---|
| **1b. ADS provides a safety-related means of depressurizing the RCS.**<br>**The following are some important aspects of ADS as represented in the PRA:** | **Tier 1 Information** |
| **ADS has four stages. Each stage is arranged into two separate groups of valves and lines.**<br>**- Stages 1, 2, and 3 discharge from the top of the pressurizer to the IRWST**<br>**- 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.**<br>**- Stage 1, 2, and 3 MOVs are normally closed and have separate controls.**<br>**- Each stage 4 squib valve actuation requires signals from two separate PMS cabinets.**<br>**- Stage 4 is blocked from opening at high RCS pressures.** | **6.3.2 & 7.3** |
| **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 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.** | **6.3.3.4.3** |
| **The reliability of the ADS is important. The ADS is included in the D-RAP.** | **17.4** |

Table 19.59-29 (Sheet 3 of 26)

AP1000 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:<br>- High pressure melt ejection<br>- Direct containment heating<br>- Induced steam generator tube rupture<br>- 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.<br>- Each CMT has a normally open pressure balance line from an RCS cold leg.<br>- Each injection line is isolated with a parallel set of air-operated valves (AOVs).<br>- These AOVs open on loss of Class 1E dc power, loss of air, or loss of the signal from the PMS.<br>- 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)

AP1000 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<br>6.3.7 |
| The CMT AOV positions are indicated and alarmed in the control room. | 3.9.6 |
| CMT AOVs are stroke-tested quarterly. | |
| 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.<br>- The CMT subsystem is included in the D-RAP. | 17.4<br>16.1 |
| CMT is required by the Technical Specifications to be available in Modes 1 through 5 with RCS pressure boundary intact. | |
| 1d. IRWST subsystem provides a safety-related means of performing the following functions:<br>- Low-pressure safety injection following ADS actuation<br>- Long-term core cooling via containment recirculation<br>- 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:<br>- 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.<br>- 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.<br>- 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)<br>AP1000 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 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 |
| The injection squib valves and the recirculation squib valves in series with check valves are diverse from the other recirculation squib valves in order to minimize the potential for common cause failure between injection and recirculation / reactor cavity flooding. | 6.3.2 |
| Automatic IRWST injection at shutdown conditions is provided using PMS low hot leg level logic. | 6.3.3.4.3 & 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 D-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 AFR-C.1, which instructs the operator to flood the reactor cavity when the core-exit thermocouples reach 1200F. | 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)

AP1000 PRA-BASED INSIGHTS

| INSIGHT | DISPOSITION |
|---|---|
| **1e.** Passive residual heat removal (PRHR) provides a safety-related means of performing the following functions:<br>- Removes core decay heat during accidents<br>- Allows automatic termination of RCS leak during a steam generator tube rupture (SGTR) without ADS | 6.3.1 & 6.3.3 |
| - Allows plant to ride out an ATWS event without rod insertion. | PRA App. A4 |
| 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 by safety-related features.. 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 every 10 years. | 3.9.6 |
| PRHR is required by Technical Specifications to be available from Modes 1 through 5 with RCS pressure boundary intact. | 16.1 |

Table 19.59-29 (Sheet 7 of 26)

AP1000 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:<br>- IRWST gutter and its drain isolation valves are safety-related<br>- These isolation valves are designed to fail closed on loss of compressed air, loss of Class 1E dc power, or loss of the PMS signal | 6.3.2.1.1 & 6.3.7.6 |
| - These isolation valves are actuated automatically by PMS and DAS. | 7.3.1.2.7 |
| The PRHR subsystem provides a safety-related means of removing decay heat following loss of RNS cooling during shutdown conditions with the RCS intact. | 16.1 |
| 2. The protection and safety monitoring system (PMS) provides a safety-related means of performing the following functions:<br>- Initiates automatic and manual reactor trip<br>- Automatic and manual actuation of engineered safety features (ESF). | Tier 1 Information |
| PMS monitors the safety-related functions during and following an accident as required by Regulatory Guide 1.97 | 7.1.1 |
| PMS initiates an automatic reactor trip and an automatic actuation of ESF. PMS provides manual initaition of reactor trip. PMS 2-out-of-4 initiation logic reverts to a 2-out-of-3 coincidence logic if one of the 4 channels is bypassed. PMS does not allow simultaneous bypass of 2 redundant channels. | Tier 1 Information |
| PMS has redundant divisions of safety-related post-accident parameter display. | 7.5.2.2.1 & 7.5.4 |
| Each PMS division is powered from its respective Class 1E dc and UPS division. | Tier 1 Information |
| PMS provides fixed position controls in the control room. | Tier 1 Information |

Table 19.59-29 (Sheet 8 of 26)

AP1000 PRA-BASED INSIGHTS

| INSIGHT | DISPOSITION |
|---|---|
| 2. (cont.)<br>Reliability of the PMS is provided by the following:<br>- The reactor trip functions are divided into two subsystems.<br>- The ESF functions are processed by two microprocessor-based subsystems that are functionally identical in both hardware and software. | <br><br>7.1.2.1.1<br>7.1.2.2 |
| 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. | 3.11 & 6.4 |
| The reliability of the PMS is important. The PMS is included in the D-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:<br>- A formalized development, modification, and acceptance process in accordance with an approved software QA plan (paraphrased from IEEE standard, section 5.3, "Quality")<br>- A verification and validation program prepared to confirm the design implemented will function as required (IEEE standard, section 5.3.4, "Verification and Validation")<br>- 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")<br>- 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")<br>- 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)

AP1000 PRA-BASED INSIGHTS

| INSIGHT | DISPOSITION |
|---|---|
| 3. The diverse actuation system (DAS) provides a nonsafety-related means of performing the following functions:<br>- Initiates automatic and manual reactor trip<br>- 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.<br>- The DAS automatic actuation signals are generated in a 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.<br>- 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 D-RAP. | 17.4 |
| 4. The plant control system (PLS) provides a nonsafety-related means of controlling nonsafety-related equipment.<br>- Automatic and manual control of nonsafety-related functions, including "defense-in-depth" functions.<br>- Provides control room indication for monitoring overall plant and nonsafety-related system performance. | 7.1.3 & 7.7.1 |
| PLS has appropriate redundancy to minimize plant transients. | 7.1.3 & 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)

AP1000 PRA-BASED INSIGHTS

| INSIGHT | DISPOSITION |
|---|---|
| 4. (cont.)<br>Signal selector algorithmes provide the PLS with the ability to obtain inputs form the PMS. The signal selector algorithms 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, preferred, and standby power supplies. | 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. | 8.3.1.1.1 |
| 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 6900 V diesel-backed bus, the associated diesel generator automatically starts and produces ac power. The normal source circuit breaker and bus load circuit breakers are opened, and the generator is connected to the bus. Each generator has an automatic load sequencer to enable controlled loading on the associated buses. | Tier 1 Information |

Table 19.59-29 (Sheet 11 of 26)

AP1000 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 D-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)

AP1000 PRA-BASED INSIGHTS

| INSIGHT | DISPOSITION |
|---|---|
| 6. The normal residual heat removal system (RNS) provides a safety-related means of performing the following functions:<br>- Containment isolation for the RNS lines that penetrate the containment<br>- Isolation of the reactor coolant system at the RNS suction and discharge lines<br>- Pathway for long-term, post-accident makeup of containment inventory. | Tier 1 Information |
| RNS provides a nonsafety-related means of core cooling through:<br>- RCS recirculation cooling during shutdown conditions<br>- Low pressure pumped makeup flow from the SFS cask loading pit and long-term recirculation from the IRWST and the containment.<br>- Heat removal from IRWST during PRHR operation | 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. | 7.3.1.2.20 |
| Interfacing system loss-of-coolant accident (LOCA) between the RNS and the RCS is prevented by:<br>- Each RNS line is isolated by at least three valves.<br>- The RNS equipment outside containment is capable of withstanding the operating pressure of the RCS.<br>- 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)

AP1000 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 exchanger. | 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 and to preserve containment integrity by isolation of the CVS lines penetrating the containment. | Tier 1 Information |
| The CVS provides a nonsafety-related means to perform the following functions:<br>- Makeup water to the RCS during normal plant operation<br>- Boration following a failure of reactor trip<br>- Makeup water 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. | 9.3.6.7 |

Table 19.59-29 (Sheet 14 of 26)

AP1000 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. | 16.3 |
| - These systems are included in the D-RAP. | 17.4 |
| Short-term availability controls for the RNS during at-power conditions reduce PRA uncertainties. | 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 DCD 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. | 7.4.3 |
| 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. | 7.4.3.1.1 |
| 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. | 3.4.1.1.2, 9.5.1.1.1, 9.5.1.2.1.1 & 9A |
| 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. | 9A |
| 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. | 3.4.1.2.2.2 |

Table 19.59-29 (Sheet 15 of 26)

AP1000 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. AP1000 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 AP1000 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. | 7.4.3 & 9.5 |
| The remote shutdown workstation is in a fire and flood area separate from the main control room. | 3.4.1.2.2.2, 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 PMS 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)

AP1000 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<br>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. AP1000 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 divisions. | 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 & 9A |
| 23. The AP1000 design minimizes potential flooding sources in safety-related equipment areas, to the extent possible. The design also minimizes the number of penetrations through enclosure or barrier walls below the probable maximum flood level. Walls, floors, and penetrations are designed to withstand the maximum anticipated hydrodynamic loads. | 3.4.1 |
| 24. The Combined License applicant will confirm the AP1000 certified design will review differences between the as-built plant and the basis for the AP1000 seismic margin analysis. | 19.59.10.5 |
| 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)

AP1000 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.<br><br>The reflective insulation panels and support members can withstand pressure differential loading due to the IVR boiling phenomena.<br><br>Water inlets and steam vents are provided at the entrance and exit of the insulation boundary.<br><br>The reactor vessel insulation is included in the D-RAP. | 19.39, 5.3.5 & Tier 1 Information<br><br>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 particulated 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.<br><br>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 or cavity levels less than full).<br><br>The operator action to activate the igniters is the first step in ERG AFR.C-1 to ensure that the igniter activation occurs prior to rapid cladding oxidation. | Tier 1 Information<br><br>16.3<br><br>Emergency Response Guidelines |

Table 19.59-29 (Sheet 18 of 26)

AP1000 PRA-BASED INSIGHTS

| INSIGHT | DISPOSITION |
|---|---|
| 31. Mitigation of the effects of a diffusion flames on the containment shell are addressed by the following containment layout features: | 1.2, General Arrangement Drawings |
| - Vents from the PXS and CVS compartments (where hydrogen releases can be postulated) to the CMT room are located well away from the containment shell and containment penetrations. The access hatch to the PXS-B compartment is located near the containment wall and is normally closed to adress severe accident considerations. The access hatch to the PXS-B compartment is accessible from Room 11300 on elevation 107'-2"... | 3.4.1.2.2.1 & 19.41.7 |
| - IRWST vents are designed so that those located away from the containment wall open to vent hydrogen releases. In this situation IRWST vents located close to the containment wall would not open because flow of hydrogen through the other vents would not result in a IRWST pressure sufficient to open them. | 6.2.4.5.1 |
| 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.<br>- Nonsafety-related containment spray does not need to be ac independent. | 19.59 |
| 36. AP1000 has a nonsafety-related containment spray system. | 6.5.2 |
| Containment spray is not credited in the PRA. Failure of the nonsafety-related containment spray does not prevent the plant achieving the safety goals. | 19.59 |
| 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. | 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 with high probability.. | 19.40 |

Table 19.59-29 (Sheet 19 of 26)

AP1000 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. | 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 D-RAP. | 17.4 |
| Operability of DAS for selected containment isolation actuations is addressed by short-term availability controls. | 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. | Appendix 19B |
| The reactor cavity design incorporates features that extend the time to basemat melt-through in the event of RPV failure. The cavity design includes:<br>- A minimum floor area of 48 $m^2$ available for spreading of the molten core debris<br>- A minimum thickness of concrete above the embedded containment liner of 0.85 m<br>- 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.<br>- 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 |
| 42. No safety-related equipment is located outside the Nuclear Island. | 1.2 & 3.4.1 |

**Table 19.59-29 (Sheet 20 of 26)**

**AP1000 PRA-BASED INSIGHTS**

| INSIGHT | DISPOSITION |
|---|---|
| 43. Capability exists to vent the containment.<br><br>The COL will develop and implement severe accident management guidance for venting containment using the suggested framework provided in WCAP-13914. | Appendix 19D<br><br>19.59.10 |
| 44. A list of risk-important systems, structures, and components (SSCs) has been provided in the D-RAP.<br><br>The risk-significant SSCs are included in the D-RAP. | 17.4<br><br>17.4 |
| 45. The Combined License applicant referencing the AP1000 certified design will review differences between the as-built plant and the design used as the basis for the AP1000 PRA and Table 15.59-29. If the effects of the differences are shown, by a screening analysis, to potentially result in a significant increase in core damage frequency 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 AP1000 design.<br><br>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. | 3.4.1.1.2<br><br>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 procedures. | 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 that normally do not flood although they are below the maximum flood height. Each of these two compartments contains redundant and essentially identical equipment (one accumulator with associated isolation valves as well as isolation valves for one CMT, one IRWST injection line, and one containment recirculation line). A pipe break in one of these compartments can cause that room to flood. 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)

AP1000 PRA-BASED INSIGHTS

| INSIGHT | DISPOSITION |
|---|---|
| 50. There are seven automatically actuated containment isolation valves inside containment subject to flooding. These seven 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 screens 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 for A and C and for B and D division rooms. In order for a fire to propagate from one divisional room to another, it must move past a 3-hour barrier (e.g., a door) into a common corridor and enter the other room through another 3-hour barrier (e.g., another door). | 9.5.1 & 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 a postulated seismic damage of the adjacent Turbine Building. | 1.2 |
| 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 as 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 all possible flooding sources. | 3.4.1.2.2.2 |

Table 19.59-29 (Sheet 22 of 26)

AP1000 PRA-BASED INSIGHTS

| INSIGHT | DISPOSITION |
|---|---|
| 57. Flood water in the Turbine Building drains to the yard and does not affect the Auxiliary Building. The presence of watertight walls and floor of the Auxiliary Building 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:<br><br>- 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.<br>- 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.<br><br>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.<br><br>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 is located. | 3.4.1.2.2.3 |

Table 19.59-29 (Sheet 23 of 26)

AP1000 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. | 7.2.1 |
| 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. | 5.4.7.2.1 & Figure 5.1-5 |
| Should vortexing occur, air entrainment into the RNS pump suction is limited. | 5.4.7.2.1 |
| 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. | Tier 1 Information<br>Figure 5.1-5<br>19E 2.1.1 |
| 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. | Tier 1 Information<br>Figure 5.1-5<br>19E 2.1.1 |
| 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. | 5.4.7.2.1 |
| 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 AP1000 safety-related I&C system. | 19.55.2.3 |
| 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)

AP1000 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 in low voltage cable trays, and, in the case of PMS, the use of arm and fire signals from separate PMS cabinets), and provisions for operator action to remove power from the fire zone. | 9A.2.7.1 |
| 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 valve 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. | 6.2.3 & 7.3.1.2.20 |
| 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 AP1000 features which contribute to the low likelihood of interfacing system LOCAs between the RNS and the RCS:<br>- A relief valve located in the common RNS discharge line outside containment provides protection against excess pressure.<br>- 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.<br>- 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. | 5.4.7.2 |

**Table 19.59-29 (Sheet 25 of 26)**

**AP1000 PRA-BASED INSIGHTS**

| INSIGHT | DISPOSITION |
|---|---|
| 67. (cont.) Per the Shutdown Evaluation, operability of the RNS is tested, via connections to the IRWST, before its alignment to the RCS hot leg for shutdown cooling. | 19E |
| 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 D-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 D-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. | 9.3.6.3.1 & 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. | 7.3.1.2.14 |
| 71. The COL applicant will maintain procedures to respond to low hot leg level alarms. | Emergency Response Guidelines |

Table 19.59-29 (Sheet 26 of 26)

AP1000 PRA-BASED INSIGHTS

| INSIGHT | DISPOSITION |
|---|---|
| 72 The containment recirculation screens are configured such that the chance of clogging is minimized during operation following accidents at power and at shutdown. The configuration features that reduce the chance of clogging include:<br>- Redundant screens are provided and located in separate locations<br>- Bottom of screens are located well above the lowest containment level as well as the floors around them<br>- Top of screens are located well below the containment floodup level<br>- Screens have protective plates that are located close to the top of the screens and extend out in front and to the side of the screens<br>- Screens have conservative flow areas to account for plugging. Adequate PXS performance can be supported by one screen with at least 90% of its surface area completely blocked<br>- During recirculation operation, the velocities approaching the screens are very low which limits the transport of debris. | 6.3.2 |
| 73. A COL applicant cleanliness program controls foreign debris from being introduced into the IRWST tank and into the containment during maintenance and inspection operations. | 6.3.2.2.7.2, 6.3.2.2.7.3, & 6.3.8.1 |
| 74. For floor drains, from the reactor cavity PXS-A and PXS-B rooms, appropriate precautions such as check valves, back flow preventers, and siphon breaks are assumed to prevent back flow from a flooded space to a nonflooded space. | 3.4.1.2.2 |
| 75. 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 |
| 76. 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 |
| 77. 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 |
| 78. 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 | 19.59.5 |

| capability with ADS Stage 4 for gravity injection and containment recirculation. | |
|---|---|

## PRA Revision:

The sections 59.9.2.1, 59.9.3, 59.9.4, 59.9.5.3, 59.9.5.5, 59.9.5.6 are changed (see below).
The sections 59.10 and 59.11 are added (see below).
The table 59-29 is added (this Table is similar to DCD Table 19.59-18. See above).

### 59.9.2.1 Safety-Related Systems

AP1000 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 ~~(RHR)~~ 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 **for decay heat removal** functions, and an example of equipment diversity is the use of different valve operators (motor, air, squib) to avoid 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 are fewer potential equipment failures (pumps and valves) and less maintenance activities.

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 ~~severe accident~~ depressurization of the reactor coolant system. The automatic depressurization system has 10 paths with diverse valves to avoid 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. Switchover from injection to recirculation is automatic without manual actions.

The safety-related Class 1E dc and UPS system has a ~~large~~ battery capacity **sufficient** to support passive safety-related systems for 72 hours. This system has four 24-hour batteries, two 72-hour batteries, and a spare battery. The presence of 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 an ~~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.

AP1000 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. 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 of heating, ventilation, and air conditioning (HVAC) penetrations ~~are~~ is reduced (no maxi purge connection).

Vessel failure potential upon core damage is reduced (in-vessel retention of the damaged core) by providing a **provision to dump** 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, AP1000 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.

Post-72-hour connections are incorporated into the passive system design to allow for long-term accident management. These connections allow for the refill of the in-containment refueling water storage tank, or the reactor cavity, should such actions become necessary.

---

## 59.9.3 Instrumentation and Control Design

Three instrumentation and control systems are modeled in the AP1000 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. Four trains of redundancy are provided for the protection and safety monitoring system; 2-out-of-4 actuation logic in the protection and safety monitoring system reduces the potential for spurious trips due to testing and allows for better testing. Automatic 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~~for data transmission. Unlike current plants, there is no cable spreading room, thus eliminating a potential fire hazard. 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. In addition, the remote shutdown ~~control~~ workstation is designed to have functions similar to the control room.

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 common cause failures in the protection and safety monitoring system.

### 59.9.4 Plant Layout

The plant layout minimizes 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 IE instrumentation and control equipment rooms. The potential flooding sources and volumes in areas of the plant that contain safety-related electrical and I&C equipment are limited to minimize the consequences of internal flooding.

AP1000 is designed to provide better separation between divisions of safety-related equipment.

---

### 59.9.5.3 Passive Containment Cooling

The passive containment cooling system provides protection to the containment pressure boundary by removing the decay and chemical heat that slowly pressurize the containment. The 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 design basis accidents.

In some postulated multiple-failure accident scenarios, the water flow may fail. The heat removal is limited to convection heat transfer to the air flow and radiation 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. ~~The containment reaches a long-term equilibrium pressure that may fail the containment even with dry PCS shell~~. Containment failure within 24 hours is highly unlikely.

### 59.9.5.5 In-Vessel Retention of Molten Core Debris

The AP1000 reactor vessel and containment configuration have features which enhance the design's 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 causing it to creep to failure.~~ The AP1000 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 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 vessel to cool the external surface of the lower head. Cooling the vessel and reducing the stresses prevents the creep rupture failure of the vessel wall. The reactor vessel reflective insulation has been designed with provisions to allow water inside the insulation panel to cool the vessel surface, and with vents to allow steam to exit the insulation without failing the insulation support structures. The insulation is designed so that it promotes the cooling of the external surface of the vessel.

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. Through the prevention of core debris relocation to the containment, the AP1000 design significantly reduces the likelihood of containment failure.

### 59.9.5.6 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 the oxidation of the zircaloy cladding by passing steam generates hydrogen. A second release may occur if the 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. These gases are highly combustible and in high concentrations in the containment may lead to detonable mixtures.

AP1000 employs a nonsafety-related hydrogen igniter system for severe releases of combustible gases. The igniters are powered from ac busses, ~~or~~ from either of the nonsafety-related diesel generators **or from the non-Class 1E batteries**. 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 will not allow the burn to transition from deflagration to detonation. The combustible gases are removed with no threat to the containment integrity.

~~The hydrogen igniter system is typically powered from ac sources with battery backup capability.~~ There is little threat of the failure of the system power in the event that it is required to operate. The igniters are only needed in core damage accidents, and the AP1000 is designed to mitigate loss of power events without the sequence evolving into a severe accident. Loss of ac power ~~contributes 0.6 percent~~**is a small contributor** to the core damage frequency.

The reliability of reactor coolant system depressurization reduces the threat to the containment from sudden releases of hydrogen from the reactor coolant system. Low pressure release of in-vessel hydrogen enhances the ability of the igniter system to maintain the containment atmosphere at the lower flammability limit.

During a severe accident, hydrogen that could be injected from the reactor coolant system into the containment through the spargers in the in-containment refueling water storage tank or into the core makeup tank room has the potential to produce a diffusion flame. A diffusion flame is produced when a combustible gas plume that 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. The AP1000 uses a defense-in-depth approach to release hydrogen in benign locations away from the containment shell and penetrations.~~ Additionally, 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 very 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.

---

## 59.10 PRA Input to the Design Certification Process

**The AP1000 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).**

### 59.10.1 PRA Input to Reliability Assurance Program

**The AP1000 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 AP1000 reliability assurance program, refer to AP1000 DCD Section 17.4.**

### 59.10.2 PRA Input to Tier 1 Information

**AP1000 DCD Section 14.3 summarizes the design material contained in AP1000 that has been incorporated into the AP1000 DCD Tier 1 Information from the probabilistic risk assessment.**

### 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 human system interface (HSI) and human factors areas. For more information on the AP1000 HSI, refer to AP1000 DCD 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 AP1000 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 AP1000 PRA.

### 59.10.4 Summary of PRA Based Insights

The use of the PRA in the design process is discussed in subsection 59.2. A summary of the overall PRA results is provided in subsections 59.3 through 59.8. A discussion of the AP1000 plant features important to reducing risk is provided in subsection 59.9. PRAbased insights are developed from this information and are summarized in Table 59-18.

### 59.10.5 Combined License Information

The Combined License applicant referencing the AP1000 certified design will review differences between the as-built plant and the design used as the basis for the AP1000 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 AP1000 certified design should compare the as-built SSC HCLPFs to those assumed in the AP1000 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 AP1000 certified design will review differences between the as-built plant and the design used as the basis for the AP1000 PRA and Table 59-18. If the effects of the differences are shown, by a screening analysis, to potentially result in a significant increase in core damage frequency or large release frequency, the PRA will be updated to reflect these differences.

The Combined License applicant referencing the AP1000 certified design will review differences between the as-built plant and the design used as the basis for the AP1000 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 AP1000 certified design will develop and implement severe accident management guidance using the suggested framework provided in WCAP-13914, "Framework for AP600 Severe Accident Management Guidance", (Reference 59-1).

The Combined License applicant referencing the AP1000 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 59-2).

## 59.11 References

59-1 "Framework for AP600 Severe Accident Management Guidance", WCAP-13914, Revision 3, January, 1998.

59-2 "Large Scale Hydrogen Burn Equipment Experiments", EPRI-NP-4354, December 1985.

# AP1000 DESIGN CERTIFICATION REVIEW

## Response to Request For Additional Information

RAI Number: 720.040

***Question:***

Please provide representative examples of PRA use in the AP1000 design process to achieve each of the following objectives: (a) enhance the AP1000 design by adding or modifying design features or operational requirements; (b) quantify the effect of new design features and operational strategies on plant risk to confirm the risk reduction credit for such improvements; (c) select among alternative features, operational strategies or design options.

**Westinghouse Response:**

Some examples of PRA use in AP1000 design process are provided below.

**(a) Enhance the AP1000 design by adding or modifying design features or operational requirements**

Westinghouse has been using PRA as a design tool since the beginning of the AP600 project in the late 1980's. Each of the 7 major PRA quantifications performed on the AP600 has lead to improvements made to the design, operating instructions and T&H performance understanding of the plant. Since the AP1000 is closely based on the AP600 plant using the same configuration for the plant and its safety / nonsafety systems, its initial PRA performance was very good. In any case, there were some changes that were made to the design and operating procedures that were based on the PRA results.

1. Changed the normal position of the two Containment motor operated recirculation valves (in series with squib valves) from closed to open

The normal position of the two MOV lines in the two sump recirculation lines have been changed from NORMALLY CLOSED to NORMALLY OPEN to improve the reliability of opening these paths. These 2 paths support containment recirculation for core cooling and IRWST draining for IVR. This change reduced the CDF and LRF contribution from the failure modes to open the MOVs.

2. Changed IRWST drain procedure so it occurs earlier for IVR support

Credit is taken for operator action to drain the IRWST into the sump to preserve reactor vessel integrity following core melt. The procedure for this severe accident response has been modified so that the operator action associated with IRWST draining is moved to the beginning of the procedure to allow more time for operator success and also to fill the cavity as soon as possible. This improves the probability of success of the operator action.

3. Improved IVR heat transfer

In going from AP600 to AP1000, the heat loads during IVR are increased due to the larger core power level which reduced the margins in the heat removal capability through the reactor vessel head during IVR. To compensate for the increase in core power, the critical heat flux limit on the outside of the reactor vessel has been increased by changes made to the flow path between the outside of the reactor vessel and the reactor vessel insulation. Testing has confirmed the robustness of the IVR heat transfer.

4. Improved IRWST vents

The larger core in the AP1000 can generate more hydrogen in a severe accident. In the AP1000 hydrogen analysis for Level II, it was observed that the standing hydrogen diffusion flames at the IRWST vents resulted in a larger thermal loads to the containment steel shell, potentially leading to containment wall failure. The design of the vents were changed so that the IRWST vents located well away from the containment would open and the IRWST vents located next to the containment would not open during a severe to eliminate or minimize this potential concern.

5. Incorporated low boron core (ATWT)

In AP600, ATWS contribution to LRF was noticed to be high relative to other initiating events. A low boron core was incorporated into the design to reduce the potential contribution of ATWS to plant risk.

6. Added 3rd Passive Containment Cooling drain valve (MOV diverse to AOV)

Due to reduced containment surface area per MW of core power, natural air circulation without PCS water drain may not always be sufficient for long term (> 1 day) containment heat removal in AP1000. For AP600 it was always sufficient for an indefinite time. To reduce the uncertainty in whether air cooling is sufficient to provide adequate long-term containment heat removal, a third path was added to the PCS drain lines to increase PCS reliability. The isolation valve used in the third path is an MOV, which is diverse from the AOVs used in the other two lines. This provides considerable improvement in the PCS water drain reliability.

7. Two Accumulators required for large CL LOCA

For the AP1000 the accumulators have not been increased in size. As a result, the increase in core power has resulted in a increase in the peak clad temperature, such that the accumulator success criteria needed to be changed to 2 of 2. The fact that the Large LOCA frequency due to pipe breaks was recently reduced in a NRC-sponsored study is used to compensate for the change in accumulator success criteria. Significantly increasing the accumulator capacity to allow 1 of 2 success criteria would not significantly reduce the total CDF, since the Large LOCA risk is already reasonably low due to low initiating event frequency and the reliability of 2 of 2 accumulators. In addition, spurious ADS stage 4 actuation initiating event is separated out from Large LOCA (two were lumped into a single initiating event category in AP600) since it is a hot-leg LOCA which can still be mitigated by 1 of 2 accumulator success criteria.

8. Reducing CCF for Recirculation-Line Squib Valves

An examination of AP1000 plant CDF cutsets revealed that the CCF of 4/4 recirculation line squib valves is a dominant contributor to CDF and LRF. This failure mode can be reduced by re-aligning the diverse squib valves already used in the AP1000 (and AP600) IRWST injection paths (high pressure valves) and the containment recirc paths (low pressure valves). By making the recirculation squib valves two sets of two LP and HP squib valves, which are different and belong to different CCF groups. This design change reduces the CCF failure contribution of the recirculation squib valves. The increase in the group size of the HP squib valves from 4 to 6 (including the four from the IRWST injection lines) does not add an appreciable contribution to the plant CDF.

**(b) Quantify the effect of new design features and operational strategies on plant risk to confirm the risk reduction credit for such improvements**

The new design features and operational strategies are already incorporated into the current AP1000 PRA. Some of these are already discussed in part (a) above. We did not keep a record of plant CDF/LRF with or without these revisions. However, basic event and initiating event importance already reported in the AP1000 PRA provide insights about the importance of components and operator actions that are involved in these design changes and operational features.

**(c) Select among alternative features, operational strategies or design options**

There was no systematic study performed to select among alternative features, operational strategies, or design options. This is partially due to the fact that AP1000 is very similar to the AP600 design, which has been already studied in PRA sense over a period of 1990 – 1996. Based on the insights and experience obtained in AP600 PRA, AP1000 was deemed not to require a further systematic study to select among different design options.

**Design Control Document (DCD) Revision:**

None

**PRA Revision:**

None

# AP1000 DESIGN CERTIFICATION REVIEW

## Response to Request For Additional Information

RAI Number: 720.044

***Question:***

Reactor cavity flooding success criteria has been modified to account for higher water depth and earlier flooding times required for AP1000. Operator instructions to flood cavity have been moved from the end of AFR.C-1 in AP600 (before entering the Severe Accident Management Guidelines), to the entry to AFR.C-1 in AP1000. Please confirm that moving this action does not adversely impact other operator actions that might be critical to core damage prevention or mitigation, or conflict with other objectives of AFR.C. (AFR.C-1 is the functional restoration guideline within the Westinghouse AP1000 emergency response guidelines for response to inadequate core cooling.)

**Westinghouse Response:**

The AP1000 Emergency Response Guidelines are constructed as symptom-based guidelines, in the style of the ERG developed for Westinghouse operating plants. The ERG include Optimal Recovery Guidelines (ORG) that provide the guidance the operators would follow following a reactor trip or safeguards actuation signal. The operators follow the ORG and continue to monitor the plant safety status trees, to ensure that critical safety parameters are acceptable. The ORG provide guidance for the operator to progress through the verification of the proper actuation of the passive safety systems,

The ERG also contain Function Restoration Guidelines which the operator would transition to upon an indication of a loss of a critical safety function. AFR.C-1 is entered once the core exit thermocouples reach a temperature of 1200F which is an indication of impending core damage. This is a severe accident condition, and the operator has entered this guideline after failure to recover the plant with the appropriate ORG.

In the AP600 ERG AFR-C.1, the action to initiate reactor cavity flooding is step 17. Based on the rules of usage in the ERG, the operator would quickly progress through the steps of the ERG in a relatively short time. However, in recognition of the results of the phenomenological analyses presented in the AP1000 PRA, it was recommended to move this action to the beginning of AFR-C.1. It should be noted that Steps 1 through 16 are all part of the ORG that the operator would have been following prior to entry into AFR-C.1. Steps 1 through 16 include the operator actions that the operator would already have attempted (and presumably failed) using the ORG. These actions include passive safety injection, CVS and RNS makeup, primary side depressurization with either automatic depressurization or available RCS heat sinks such as the steam generators and the PRHR heat exchanger. Therefore moving Action 17 – Reactor Cavity Flooding to the beginning of AFR-C.1 is appropriate.

This action begins draining the IRWST to the reactor cavity to provide ex-vessel cooling. Following this step, the operator will continue to try to re-establish core cooling by more conventional means outlined in Steps 1 through 16. Considering that the entry into AFR.C-1 is predicated in core exit TC > 1200F, which is an indication of impending core damage, it is appropriate to initiate cavity flooding to provide for ex-vessel cooling, and thus prevent vessel rupture.

See the response to RAI 440.109 for a related discussion of the applicability of the AP600 ERG to the AP1000.

**Design Control Document (DCD) Revision:**

None

**PRA Revision:**

None

# AP1000 DESIGN CERTIFICATION REVIEW

## Response to Request For Additional Information

RAI Number: 720.046

***Question:***

The containment isolation fault tree success criteria tables (Tables 24-5a through-c and 24-8) do not include all of the isolation valves listed in Table 24-1 for the 12 penetrations analyzed (some of which are initially open). Please discuss why only a partial listing is provided.

**Westinghouse Response:**

Table 24-1 is the total listing of all containment isolation system penetrations. Table 24-2 determines which of these system penetrations are retained for further evaluation. The system penetrations listed in Table 24-2 are in the same order as the system penetrations listed in Table 24-1. Of the 37 penetrations, 12 are retained for further evaluation. Those 12 penetrations are for the main steam, main feedwater, startup feedwater, steam generator (SG) blowdown, containment air filter supply, containment air filter exhaust, instrument air in, and the normal containment sump. Direct correlation to Tables 24-5a through c and Table 24-8 may be made for these 12 penetrations except for main steam, main feedwater and startup feedwater systems. These three penetrations that are not accounted for are discussed below.

**Main Steam System Penetrations**

All containment isolation valves are accounted for with the exception of the Steam Generator System Safety Valves V030A and B, V031A and B, V032A and B, V033A and B, V034A and B, V035A and B and globe-air valves V036A and B. Valves V030 through V035 are located upstream of the MSIVs and outside of containment.

The globe-air valves are 2-inch outside diameter valves that are located upstream of the Main Steam Isolation Valves (MSIVs) and outside of containment. The valves are contained in a drain branch line from the main steam line and are used to drain condensate from the main steam system. Downstream of the V036 valves are 2-inch normally closed, fail closed and air operated V086 valves. When the Protection and Safety Monitoring System (PMS) sends a signal to the MSIV to close, similar signals go to valves V036 and V086.

**Assessment:** The Steam Generator System (SGS) Safety Valves are pressure operated relief valves and open at higher than relief valve set point line pressures and are not automatically operable. The risk factor issues for the safety valves are discussed in other node events of the Probabilistic Risk Assessment (PRA).

The penetration P23 (or P24, depending on the faulted loop) are not explicitly modeled in the fault tree CIA. The two air operated valves (AOVs) in one of these penetrations are in series; one is normally closed; both get the same PMS signal as the MSIV. Thus, the PMS signal failure is accounted for. The failure probability that one normally closed valve is open AND both AOVs fail upon receipt of a PMS signal is small compared to failure of the MSIV to close, which is already modeled. Thus, these valves do not contribute much to the fault tree CIA failure, compared to the valves already modeled.

**Main Feedwater System Penetrations**

The containment isolation valves for the Main Feedwater System (MFW) are V057A and B, V250A and B and V058A and B.

**Assessment:** In the PRA model, one SG train is chosen as faulted. Thus, only one set of isolation valves (V057B, V250B and V058B) and one SG (B) are included in the fault tree CIB (set of "B" valves). The models are as intended.

**Startup Feedwater System Penetrations**

The containment isolation valves for the Startup Feedwater System (SFW) are motor operated valves (MOVs) 067A and B, AOV255A and B, and check valves (CVs) 256A and B. These valves are outside of containment and exist in separate lines from the main feedwater system. AOV255A and B are normally closed, fail closed and air operated valves.

**Assessment:** Isolation of MFW path (through closure of valves AOV057, or AOV250 or CV058) is included in the fault tree CIB. Isolation of the SFW path (through valves MOV067, AOV255 or CV256) is not included. The failure probability that the normally closed AOV is open AND both valves fail upon receipt of a PMS signal AND the check valve fails is small compared to failure of the MFW penetration valves to close, which is already modeled. The failure probability of the fault tree CIB is calculated to be 4.85E-03 per year. The failure probability of MOV067 and AOV255 is relatively small and would not significantly affect the results.

**Design Control Document (DCD) Revision:**

None

**PRA Revision:**

None

# AP1000 DESIGN CERTIFICATION REVIEW

## Response to Request For Additional Information

RAI Number: 720.047

***Question:***

Please discuss the implications of the most recently completed experimental work related to in-vessel retention of molten core debris on the reliability of the in-vessel retention strategy for the AP1000 design, including the work performed as part of the RASPLAV project and any available results from the Organization for Economic Cooperation and Development (OECD)-sponsored MASCA program at the Russian Research Center, and the SIMECO and FOREVER programs in Sweden. Specifically address the implications of this work on the potential for debris bed stratification and chemical interactions between molten debris and the reactor vessel wall.

**Westinghouse Response:**

**RASPLAV program**

The first part of the RASPLAV program includes *prototypic-materials* experiments. However, it should be noted that RASPLAV experiments were run in conditions far from prototypic. Therefore, extreme care needs to be exercised in interpreting and extrapolating RASPLAV experimental results to reactor situations of interest.

With respect to IVR applications, the range of Raleigh number realized in the RASPLAV prototypic-materials experiments was too low, Ra ~ $10^{10}$. The data obtained in RASPLAV homogeneous-pool experiments are consistent with heat transfer data obtained in other experiments for the same range of Raleigh number. It confirms the applicability of heat transfer correlations to prototypic-materials melt pool. This outcome is expected.

Most controversially, two RASPLAV AW-200 corium tests show the debris stratify into a uranium-rich layer at the bottom and Zr-rich layer above it. Following this observation, it was found that such stratification phenomena are specific to suboxidized corium (less than 10% of Zr oxidized) or to corium with carbon content more than 0.3-0.4%. It was then confirmed by the RASPLAV program that corium compositions of practical interest do not fall in the so-called miscibility gap that was thought to be the reason for the corium stratification observed in the RASPLAV AW-200 tests.

Most importantly, it should be noted that a (side-wall) heating procedure used in the RASPLAV AW-200 experiments renders a given-composition mixture to start to thaw as soon as a solidus point temperature is approached. Upon heating, high-conductivity and low-melting point materials heat up and smelt first. In particular, the heating procedure caused a Zr-based $ZrO_X$ liquid to form within the $(UZr)O_{2-X}$ matrix that gives raise to the observed stratification. In a prototypic reactor situation, the heating is volumetric and the corium was discharged from the reactor core to the reactor lower head in liquid form as contrasted to corium briquettes used in experiments. Thus, the RASPLAV experiments may have *prototypic-chemical composition*, but actually ***fail*** to represent *prototypic material properties in a relevant context of reactor safety.* This artifact is amplified and resonated with non-prototypic heating procedures to generate much-confused results with respect to the IVR application to which the program was intended to contribute.

In other words, ***stratification of corium melts*** is brought about by non-prototypic conditions in the experiments, and therefore irrelevant to the assessment of IVR.

Complementary RASPLAV experiments were performed using non-eutectic salts as stimulant. Using a liquidus point as the pool boundary temperature, heat transfer data from the RASPLAV salt experiments are consistent with ACOPO data that formed the backbone of the AP-600 IVR analysis. More importantly, the RASPLAV salt tests demonstrate that convection in the melt pool is not affected by the pool crust formation. Such an approach was taken in the assessment of IVR for AP-600 and remains equally valid for AP-1000.

**MASCA program**

MASCA (Materials Scaling) program is a continuation of the RASPLAV.

From the MASCA program, experiments that are new, interesting and potentially significant for AP-1000 are MA-1, MA-2 and T-7 tests. In these tests, steel pellets were introduced into a corium pool. It was found that metallic U and Zr are extracted from corium in a reduction-oxidation reaction to form together with steel materials a dense metallic phase that sinks to the bottom.

We show (below) that highly-non-prototypical conditions realized in these tests may have been responsible for the observed result. Therefore, at this point discussion on implications of MASCA test results is premature.

The key argument in support of this view is that due to heating techniques and test section design and procedures used, the molten steel in the experiments is overheated and in direct contact with liquid corium (rather than separated by an 1-cm oxide crust layer as in a prototypic reactor scenario). These factors may have helped dissolution of steel into corium and facilitated U-Zr extraction reactions.

First of all, test T-7 employed a radiant heating method that transfers energy from an inductively-heated (to 3000°C) graphite block to corium materials located below. Therefore, no crust layer formed and existed at the corium pool when the steel pellets were introduced to the pool.

In MA-1 ands MA-2 tests, the volumetric heat generation rate is estimated to be above 160 $MW/m^3$ that is two orders of magnitude higher than reactor situations (1-2 $MW/m^3$). Accordingly, the upward surface heat flux in the MA-1 and MA-2 tests is at the level of 6 $MW/m^2$, versus 1 $MW/m^2$ in a prototypic IVR situation. Consequently, the pool is overheated and the crust surface temperature is elevated to 2200°C as measured by pyrometers in the experiments.

Introduction of steel pellets to this pool surface (crust) causes an immediate melting of steel, which spreads to a thin layer over the crust surface. Due to the steel low emissivity (0.4 compared to 0.9 of oxides), the upward heat flux suddenly decreases, increasing the pool temperature and cause the upper, already thin (1-2 mm), oxidic crust to melt. The resulting direct contact of molten steel and liquid corium then facilitated chemical reactions that led to formation of metal-rich dense phase. In addition, it is noted that inductive heat generation in the molten steel can be significant that contribute further to the heatup and thermal insulation effect that leads to the above-discussed crust remelting.

Experiments should be carried out under proper temperature and heat flux conditions representative of IVR. It is known that under such conditions an oxide crust is thick and stable, preventing any direct contact of molten steel and core melt. Also note that to correctly represent the reactor crust, the "corium materials" in experiments must be pre-melted and let solidified before a real run. This shall allow the crust to be sintered and impermeable, as contrasted to "crust" that formed from powder (200μm particles) in the experiments.

**METCOR program**

The main result of the METCOR tests (Phase I funded by ISTC) on molten corium-vessel steel interactions is that the corium oxidic crust serves as protective layer against steel corrosion. Lack of oxygen in gas environment would further diminish corrosion rate. This does not come as a surprise.

***No chemical reactions*** between the molten corium and reactor vessel wall need to be considered as to their effect on potential performance of IVR.

**FOREVER program**

The FOREVER program performed at Royal Institute of Technology (Sweden) aims to obtain data on the vessel creep and vessel failure behavior on a 1/5-scale facility using oxidic melts at temperature upto 1300°C. In general, the FOREVER experiments are irrelevant to the in-vessel retention, when the reactor vessel is externally flooded.

In addition to the vessel creep experiments, the FOREVER program was also designed to investigate efficiency of gap cooling by reactor water entering the gap open between an oxidic debris and the creeping vessel. In a recent test, FOREVER-5 (June 18, 2002) with water flooded on top of the heated oxide melt pool/debris no evidence of gap cooling was found. A post-test examination confirmed no gap formation between the oxide debris and the vessel.

**SIMECO program**

SIMECO is a 2D slice facility, using water, glyceron, eutectic and non-eutectic $NaNO_3$-$KNO_3$ as simulants. Due to limitations of experimental technique used in SIMECO, natural convection heat transfer experiments performed to date in this facility were limited to a pool Raleigh number around $10^{13}$. Several experiments were performed with miscible two-layer pools, and are irrelevant to in-vessel melt coolability scenarios. Other tests were performed with an immiscible two-layered pool with heat input provided to the lower layer.

Neither systematic data and correlations nor definitive evaluation of data quality and comparison to existing correlations were reported. In general, the SIMECO program has not produced any new and substantial findings that are relevant to the in-vessel retention assessment.

**Design Control Document (DCD) Revision:**

None

**PRA Revision:**

None

RAI Number: 720.049

***Question:***

Describe how the water/steam flow path and flow areas specified for the AP1000 in Chapter 5.3.5 of the AP1000 Design Control Document (DCD) were simulated in the ULPU-2000 experiments, including scaling effects.

**Westinghouse Response:**

The ULPU-2000 facility Configuration IV was modified to allow it to fully accommodate all important specifications that involve ex-vessel water/steam flow path of the AP-1000 reactor design in the IVR scenario. The main objective of the modifications was to ensure a correct modeling of flow regimes and pressure drops in the IVR two-phase natural circulation loop. The approach taken is to provide a **full height** and geometrical representation of flow paths **(inclination, cross section areas**) in the ULPU-2000 that allows natural-convection driving forces and pressure losses to be correctly (maybe somewhat conservatively) modeled (see Figure 720.049-1 of ULPU facility schematic). Also, to remove any substantial hydraulic resistance in the downward section of the natural circulation loop (loop compartment, reactor vessel cavity) the downward section in the ULPU-2000 facility was modified to have 6" diameter that then connects to the "slice" cavity.

The baffle in ULPU-2000 models a streamlined insulation that is shaped to closely follow the contour of the vessel lower head (see Figure 720.049-1). Different baffle positions are possible in ULPU-2000 to optimize the flowpath for a maximum critical heat flux. Three heater blocks (15 cm wide) represent the reactor vessel wall. At 90° angle, this 15 cm width corresponds to 1:84 of the AP-1000 vessel lower head circumference (d= 4m). Accordingly, cross-section areas of the riser and vent duct (that connect the riser to the nozzle gallery) are chosen to be 1:84 of the flow path area in the riser and vent duct of AP-1000. Furthermore, the vent duct is made to accommodate a flow area change from circumferential to 4 ducts and with an inclination that faithfully reflects the AP-1000 design (see Figure 720.049-2 of ULPU vent path design). Modifications were also made to faithfully represent the water inlet geometry (see Figure 720.049-3 of ULPU water inlet configuration).

Special considerations are given to heat flux profile to account for the difference between the reactor vessel hemisphere and the ULPU-2000 slice geometry. Description of the power profile methodology was given in the AP-600 IVR assessment. Specifically, in a test that measures CHF at angle $\gamma^*$ ($\gamma^* < 90°$), the heat flux is shaped for $\gamma < \gamma^*$ to ensure that two-phase flow conditions (enthalpy) at the test location ($\gamma^*$) represents that in a reactor situation at this location. Heat flux in the region above $\gamma^*$ ($90° > \gamma > \gamma^*$) is reduced to exclude possibility for burnout to occur in that region. As a result, the total driving force for the two-phase flow loop is reduced, compared to that of a reactor case, leading to conservative CHF values.

The ULPU-2000 facility provides an effectively full-scale (i.e., prototypical) simulation of boiling crisis on a RPV under IVR.

**Design Control Document (DCD) Revision:**

None

**PRA Revision:**

None

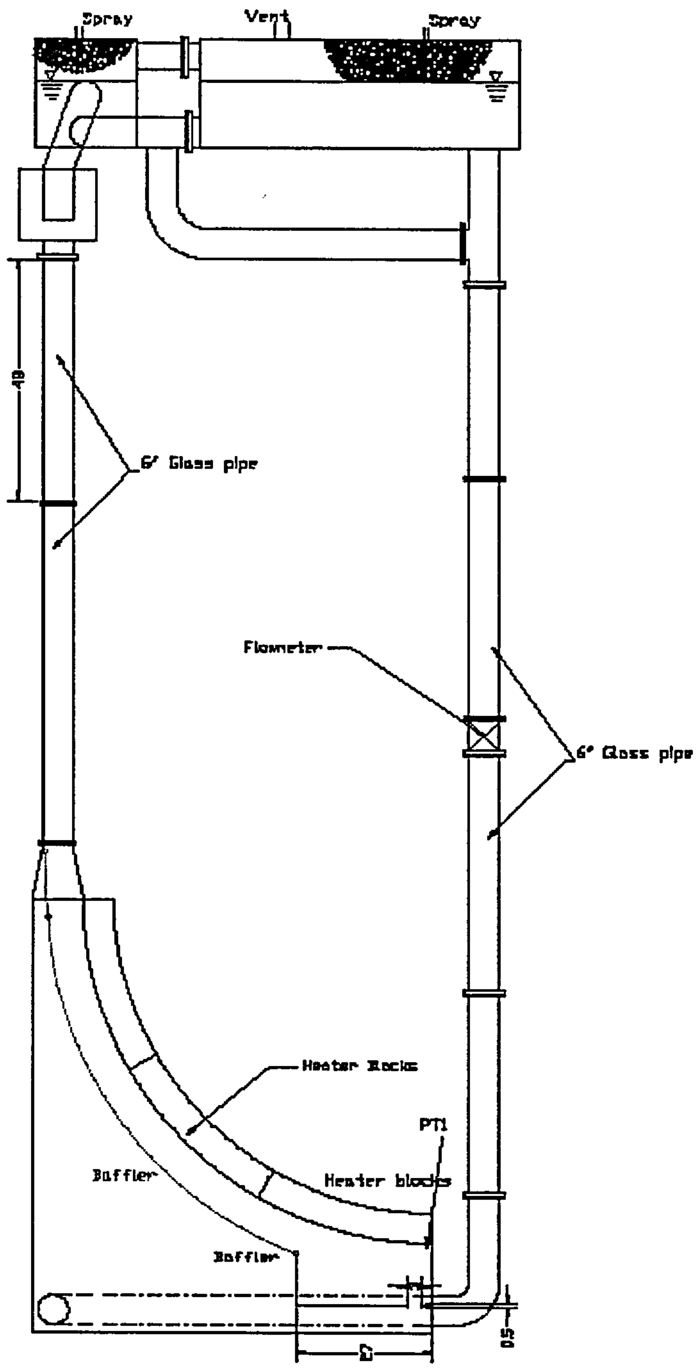


Figure 720.049-1
**ULPU facility schematic**

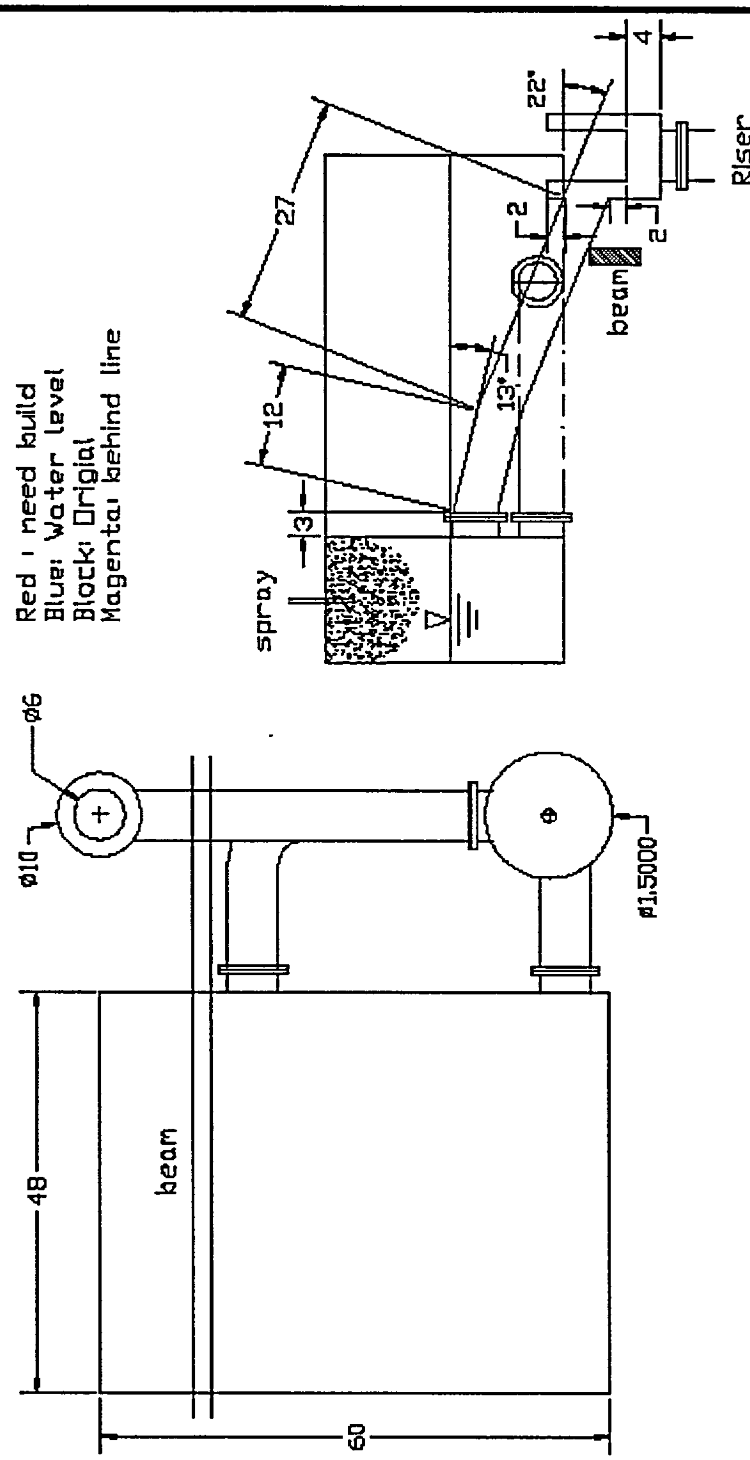


Figure 720.049-2
**ULPU vent path design**

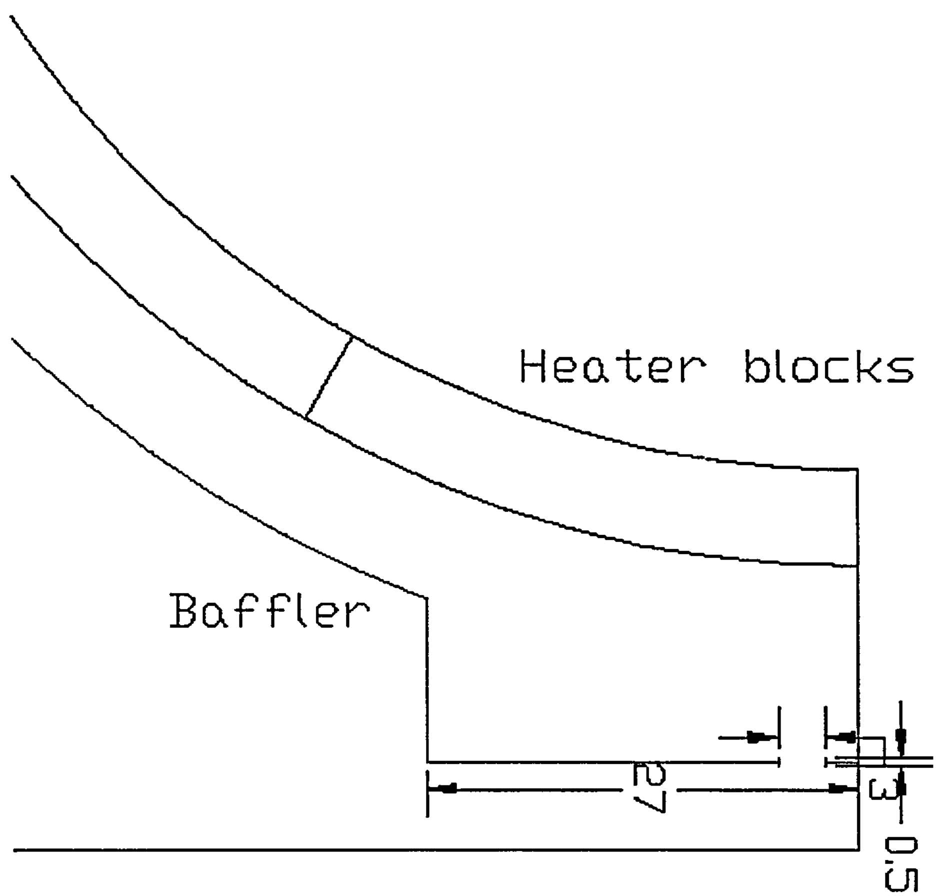


Figure 720.049-3
**ULPU water inlet configuration**

# AP1000 DESIGN CERTIFICATION REVIEW

## Response to Request For Additional Information

RAI Number: 720.055

***Question:***

An assessment of direct containment heating (DCH) was performed for AP600 using the methodology developed as part of the DCH issue resolution (i.e., NUREG/CR-6338 "Resolution of the Direct Containment Heating Issue for a Westinghouse Plants with Large Dry Containments or Subatmospheric Containments," February 1996). Rather than update this assessment for AP1000, Westinghouse (in Appendix B.3) provided a qualitative argument that the AP1000 design includes reactor cavity design features to decrease the amount of ejected core debris from reaching the upper compartment, as called out in SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Passive Advanced Light-Water Reactor Designs." This qualitative argument provides an insufficient technical basis for addressing the DCH, given the potential for a greater DCH pressure loading in AP1000 (due to the larger core mass), and the more recent and technically-defensible methodology that is now available. Please provide the results of a deterministic assessment based on the methodology developed as part of DCH issue resolution.

**Westinghouse Response:**

The AP1000 meets the requirements of SECY-93-087 with regards to High Pressure Core Melt Ejection. The following is taken from SECY-93-087:

"I. High Pressure Core Melt Ejection

In SECY-90-016, the staff recommended that the Commission approve the position that evolutionary ALWR designs should include a depressurization system and cavity design features to contain ejected core debris in order to reduce the potential for containment failure as a result of direct containment heating (DCH). The staff is concerned that this event might result from the ejection of molten core debris under high-pressure from the reactor vessel. Such an ejection might result in wide dispersal of core debris, rapid oxidation, and extremely rapid addition of energy to the containment atmosphere.

In its SRM of June 26, 1990, the Commission approved the staff's position. The Commission also directed that the cavity design, as a mitigating feature, should not unduly interfere with operations, including refueling, maintenance, or surveillance activities. Examples of cavity design features that will decrease the amount of ejected core debris that reaches the upper containment include (1) ledges or walls that would deflect core debris and (2) an indirect path from the lower reactor cavity to the upper containment. The staff will review the LWR design relative to the above criteria.

In it letter of May 5, 1992, EPRI indicated that the requirements document specifies an RCS depressurization system and cavity retention capability for both evolutionary and passive plants. EPRI further indicated that since the passive plant emergency core cooling system (ECCS) relies on RCS depressurization, redundancy and diversity have been specified for the depressurization system to ensure very high reliability.

In its letter of August 17, 1992, ACRS indicated that because direct containment heating is an extremely improbable event, two modes of coping with the possibility are not needed. ACRS stated that because of the possible safety benefits for other events, reliable depressurization is the preferred approach.

The staff agrees with the ACRS assertion that a reliable depressurization system is needed. However, the staff proposes to provide a design concept with a degree of consequence mitigation along with a certain amount of accident prevention. The depressurization system retains a degree of uncertainty. Such questions as the rate of depressurization, the timing for operator initiation of manual depressurization, and the cut-off pressure may never be totally resolved. As a result, the staff believes that a design can be developed to decrease the direct flight path to the upper containment at little or no added expense.

The plant designers have provided features to address this issue for evolutionary ALWR designs. The staff is in the process of evaluating their submittals to ensure acceptable implementation of the Commission's guidance on this issue. The staff's preliminary review of the passive ALWRs has also identified the importance of RCS depressurization to the safety shutdown of the plant during transients or accidents. RCS depressurization is crucial to the operation of the passive safety features that limit the likelihood of core damage, as well as to reducing the potential for containment failure by direct containment heating from the ejection of core debris at high pressure. Therefore, the staff has determined that the passive ALWR designs should include a highly reliable depressurization system.

<u>The staff recommends that the Commission approve the general criteria that the evolutionary and passive LWR designs</u>

- <u>Provide a reliable depressurization system: and.</u>
- <u>Provide cavity design feature to decrease the amount of ejected core debris that reaches the upper containment."</u>

The AP1000 clearly meets the requirements of SECY-93-087. The AP1000 automatic depressurization system fulfills the requirements for a reliable depressurization system (ADS). The ADS is an automatically-actuated, safety-related system consisting of 4 different valve stages that open sequentially to reduce RCS pressure sufficiently so that long-term cooling can be provided from the passive core cooling system. In the event that automatic actuation fails, the ADS is initiated by operator action from the main control room using the diverse actuation system. The ADS valves are designed to remain open for the duration of any ADS event, thereby preventing repressurization of the RCS. The performance of the ADS for design-basis accident is discussed in DCD Section 6.3 and Sections 5.1.3.7. The modeling of ADS in the PRA is described in Chapters 11 and 36 of the AP1000 PRA. The inclusion of an automatic depressurization system is sufficient to meet the requirements of SECY-93-087.

In addition, the AP1000 reactor cavity contains the same geometry and design features that were acceptable for AP600. As discussed in the AP1000 PRA Appendix B, the AP1000 reactor cavity is designed to decrease the amount of ejected core debris that can reach the upper containment. The paths from the reactor cavity to the upper containment volume in AP1000 include the following:

- the area around the reactor vessel flange
- the area where the coolant loops penetrate through the biological shield
- a ventilation shaft from the roof of the reactor coolant drain tank room that leads to the steam generator compartments.

These paths are convoluted, hence a portion of the corium will be de-entrained and removed from the atmosphere before reaching the upper containment region, thereby reducing the pressure rise associated with DCH.

The AP1000 design meets the requirements of SECY-93-087, and no additional analyses are required. Furthermore, the AP1000 Large Release Frequency (LRF) has been calculated assuming that high pressure core damage sequences lead to containment failure. The calculated AP1000 LRF is for internal events at-power is $1.95 \times 10^{-8}$ and this is quite acceptable.

**Design Control Document (DCD) Revision:**

None

**PRA Revision:**

None

# AP1000 DESIGN CERTIFICATION REVIEW

## Response to Request For Additional Information

RAI Number: 720.057

***Question:***

Sensitivity and importance analyses for large release frequency and sensitivity analyses for offsite dose risk were provided in Chapter 50 of the PRA for the AP600. Sensitivity analyses and top event importance analyses are provided in Chapter 43 for AP1000. However, component and operator action importance analyses, and sensitivity analyses for offsite dose risk have not been included. Please provide this additional information for AP1000.

**Westinghouse Response:**

AP1000 PRA offsite dose analysis contains two sensitivity analyses. To be responsive to this request, we provide five sensitivity analyses for the offsite dose calculations, including the two that are already provided in the submittal. These sensitivity analyses can be found in Attachment A.

At the time of the AP1000 PRA submittal, we provided LRF cutsets only for the top 6 sequences. These were not enough for calculation of component and operator action importances. To answer this question, we added the cutsets from the first 26 LRF sequences which make up more than 99% of the LRF. Then we calculated the component, operator action, and initiating event importances based on these cutsets. The results are given in Attachment B to this response.

**Design Control Document (DCD) Revision:**

None

**PRA Revision:**

None

**Attachment A to RAI 720.057 – AP1000 PRA**

## Sensitivity Analyses for AP1000 Offsite Dose Calculations

Chapter 49 of AP1000 PRA contains the "offsite Dose Risk Quantification". We will designate the site boundary whole body dose at 24 hours as the base case. A discussion of why the acute red bone marrow dose may be used to represent the acute whole-body dose, determined at the site boundary (0.5-mile radius), is already given in the AP1000 PRA. However, we chose the whole body dose since it is larger than that of the red bone marrow dose and makes the point that is being sought in this write-up.

### 1. The Base Case

The base case defined above is already calculated in the AP1000 PRA and is given in Table 49-8. It is also given in the attached Table 720.057-1. From this table, it is observed that the Large Release Frequency as defined by 25 REM or more whole body dose at the site boundary at 24 hours is 1.95E-08/year. This is below the acceptance level of 1.0E-06/year, with a comfortable margin; namely a factor of 50.

### 2. Sensitivity Case 1: DIRECT Release

The following sensitivity case is already presented in the AP1000 PRA submittal: "Additionally, one sensitivity evaluation (called DIRECT) is performed. The DIRECT release case is a modification of the IC release category in which no credit is assumed for aerosol nuclide deposition in the middle annulus. This case is conservative."

The results of this case are given in the attached Table 720.057-2. From this table, it is apparent that this case does not affect the results and insights of the offsite dose release.

### 3. Sensitivity Case 2: 72-Hour Dose

The site boundary whole body risk at 72 hours is already calculated in the AP1000 PRA and is given in Table 49-9. It is also given in the attached Table 720.057-3. From this table, it is observed that the Large Release Frequency as defined by 25 REM or more whole body dose at the site boundary at 24 hours stays at 1.95E-08/year. There is a modest increase in the mean value of the risk, 12%.

### 4. Sensitivity Case 3: Upper-Bound Release Frequencies at 24 Hours

This sensitivity analysis addresses the case where the release category frequency may be considerably higher than those used in the base case. For this case, a set of "upper-bound" release frequencies are defined, as shown below in Table 720.057-A. These frequencies are a factor of 5 to 100 times the base release category frequencies (lower the base frequency, higher the uncertainty factor). The resulting total release frequency is 1.32E-06/yr, which is a factor of 5.5 higher than the base case value.

The resulting LRF value (From Table 720.057-4) is 2.212E-07/yr, which is an order of magnitude higher than the base case, but is still well below the acceptance criteria of 1.0E-06/yr.

**Table 720.057-A. Upper Bound (UPB) Release Frequencies**
Site Boundary Whole Body Dose (Effective Dose Equivalent, EDE)

| | Mean | UPB/Mean | UPB |
|---|---|---|---|
| CFI | 1.89E-10 | 30 | 5.67E-09 |
| CFE | 7.47E-09 | 10 | 7.47E-08 |
| IC | 2.21E-07 | 5 | 1.11E-06 |
| BP | 1.05E-08 | 10 | 1.05E-07 |
| CI | 1.33E-09 | 20 | 2.66E-08 |
| CFL | 3.45E-13 | 100 | 3.45E-11 |
| **Totals =** | **2.40E-07** | **5.5** | **1.32E-06** |

### 5. Sensitivity Case 4: Upper-Bound Release Frequencies at 72 Hours

This case is similar to case 3, except the calculations are made at 72-hours, using the upper-bound release category frequencies. The results are given in Table 720.057-5. The LRF value is 2.12E-07/yr, which is the same as that at 24-hours. There is 9% increase in the risk.

### 6. Sensitivity Case 5: 10 Times the Release Frequency and 10 Times the Dose

In this sensitivity analysis, the release category frequencies are increased by a factor of 10, and the dose for each category is also increased by a factor of 10, for the 24-hour base case. The - results are given in Table 720.057-6. The total release frequency is 2.4E-06/yr. LRF is increased to 1.95E-07/yr, which is a factor of 10 higher than that of the base case. LRF is still well below the acceptance criteria of 1.0E-06/yr.

### Summary and Conclusions

Table 720.057-7 summarizes the results of the base case and the six sensitivity analyses. The results indicate that, even with generous conservatisms introduced in release category frequencies, and dose amounts, the plant LRF stays well below the acceptance criteria of 1.0E-06/yr.

| Table 720.057-1<br>Base Case | | Site Boundary Whole Body Dose (Effective Dose Equivalent, EDE)<br>24 Hours | | | | |
|---|---|---|---|---|---|---|
| **Release Category** | **Release Frequency (/ry)** | **Mean Dose (sieverts)** | **Dose (REM)** | **Risk (REM/ry)** | **Percent Contribution to Total Risk** | **LRF** |
| CFI | 1.89E-10 | 1.18E+01 | 1.18E+03 | 2.23E-07 | 0.33% | 1.89E-10 |
| CFE | 7.47E-09 | 7.38E+01 | 7.38E+03 | 5.51E-05 | 81.06% | 7.47E-09 |
| IC | 2.21E-07 | 8.16E-03 | 8.16E-01 | 1.80E-07 | 0.27% | |
| BP | 1.05E-08 | 2.78E+00 | 2.78E+02 | 2.92E-06 | 4.29% | 1.05E-08 |
| CI | 1.33E-09 | 7.19E+01 | 7.19E+03 | 9.56E-06 | 14.06% | 1.33E-09 |
| CFL | 3.45E-13 | 1.95E-02 | 1.95E+00 | 6.73E-13 | 0.00% | |
| Totals = | 2.40E-07 | | | **6.80E-05** | 100.00% | **1.95E-08** |

| Table 720.057-2<br>Sensitivity case 1 | | Site Boundary Whole Body Dose (Effective Dose Equivalent, EDE)<br>24 Hours; IC replaced by DIRECT | | | | |
|---|---|---|---|---|---|---|
| **Release Category** | **Release Frequency (/ry)** | **Mean Dose (sieverts)** | **Dose (REM)** | **Risk (REM/ry)** | **Percent Contribution to Total Risk** | **LRF** |
| CFI | 1.89E-10 | 1.18E+01 | 1.18E+03 | 2.23E-07 | 0.33% | 1.89E-10 |
| CFE | 7.47E-09 | 7.38E+01 | 7.38E+03 | 5.51E-05 | 80.65% | 7.47E-09 |
| IC | 2.21E-07 | 2.37E-02 | 2.37E+00 | 5.24E-07 | 0.77% | |
| BP | 1.05E-08 | 2.78E+00 | 2.78E+02 | 2.92E-06 | 4.27% | 1.05E-08 |
| CI | 1.33E-09 | 7.19E+01 | 7.19E+03 | 9.56E-06 | 13.99% | 1.33E-09 |
| CFL | 3.45E-13 | 1.95E-02 | 1.95E+00 | 6.73E-13 | 0.00% | |
| Totals = | 2.40E-07 | | | **6.84E-05** | 100.00% | **1.95E-08** |

| Table 720.057-3 Sensitivity case 2 | | Site Boundary Whole Body Dose (Effective Dose Equivalent, EDE) 72 hours | | | | |
|---|---|---|---|---|---|---|
| **Release Category** | **Release Frequency (/ry)** | **Mean Dose (sieverts)** | **Dose (REM)** | **Risk (REM/ry)** | **Percent Contribution to Total Risk** | **LRF** |
| CFI | 1.89E-10 | 1.25E+01 | 1.25E+03 | 2.36E-07 | 0.31% | 1.89E-10 |
| CFE | 7.47E-09 | 7.97E+01 | 7.97E+03 | 5.95E-05 | 77.86% | 7.47E-09 |
| IC | 2.21E-07 | 1.51E-01 | 1.51E+01 | 3.34E-06 | 4.36% | |
| BP | 1.05E-08 | 3.17E+00 | 3.17E+02 | 3.33E-06 | 4.35% | 1.05E-08 |
| CI | 1.33E-09 | 7.54E+01 | 7.54E+03 | 1.00E-05 | 13.11% | 1.33E-09 |
| CFL | 3.45E-13 | 5.38E-01 | 5.38E+01 | 1.86E-11 | 0.00% | 3.45E-13 |
| Totals = | 2.40E-07 | | | **7.65E-05** | 100.00% | **1.95E-08** |

| Table 720.057-4 Sensitivity case 3 | | Site Boundary Whole Body Dose (Effective Dose Equivalent, EDE) 24 Hours - upper-bound release frequencies | | | | |
|---|---|---|---|---|---|---|
| **Release Category** | **Release Frequency (/ry)** | **Mean Dose (sieverts)** | **Dose (REM)** | **Risk (REM/ry)** | **Percent Contribution to Total Risk** | **LRF** |
| CFI | 5.67E-09 | 1.18E+01 | 1.18E+03 | 6.69E-06 | 0.86% | 5.67E-09 |
| CFE | 7.47E-08 | 7.38E+01 | 7.38E+03 | 5.51E-04 | 70.74% | 7.47E-08 |
| IC | 1.11E-06 | 8.16E-03 | 8.16E-01 | 9.02E-07 | 0.12% | |
| BP | 1.05E-07 | 2.78E+00 | 2.78E+02 | 2.92E-05 | 3.75% | 1.05E-07 |
| CI | 2.66E-08 | 7.19E+01 | 7.19E+03 | 1.91E-04 | 24.54% | 2.66E-08 |
| CFL | 3.45E-11 | 1.95E-02 | 1.95E+00 | 6.73E-11 | 0.00% | |
| Totals = | 1.32E-06 | | | **7.79E-04** | 100.00% | **2.12E-07** |

| Table 720.057-5 Sensitivity case 4 | | Site Boundary Whole Body Dose (Effective Dose Equivalent, EDE) 72 Hours - upper-bound release frequencies | | | | |
|---|---|---|---|---|---|---|
| **Release Category** | **Release Frequency (/ry)** | **Mean Dose (sieverts)** | **Dose (REM)** | **Risk (REM/ry)** | **Percent Contribution to Total Risk** | **LRF** |
| CFI | 5.67E-09 | 1.25E+01 | 1.25E+03 | 7.09E-06 | 0.83% | 5.67E-09 |
| CFE | 7.47E-08 | 7.97E+01 | 7.97E+03 | 5.95E-04 | 69.80% | 7.47E-08 |
| IC | 1.11E-06 | 1.51E-01 | 1.51E+01 | 1.67E-05 | 1.96% | |
| BP | 1.05E-07 | 3.17E+00 | 3.17E+02 | 3.33E-05 | 3.90% | 1.05E-07 |
| CI | 2.66E-08 | 7.54E+01 | 7.54E+03 | 2.01E-04 | 23.51% | 2.66E-08 |
| CFL | 3.45E-11 | 5.38E-01 | 5.38E+01 | 1.86E-09 | 0.00% | 3.45E-11 |
| Totals = | 1.32E-06 | | | **8.53E-04** | 100.00% | **2.12E-07** |

| Table 720.057-6 Sensitivity case 5 | | Site Boundary Whole Body Dose (Effective Dose Equivalent, EDE) 24 Hrs - 10 times release frequency and 10 times mean dose | | | | |
|---|---|---|---|---|---|---|
| **Release Category** | **Release Frequency (/ry)** | **Mean Dose (sieverts)** | **Dose (REM)** | **Risk (REM/ry)** | **Percent Contribution to Total Risk** | **LRF** |
| CFI | 1.89E-09 | 1.18E+02 | 1.18E+04 | 2.23E-05 | 0.33% | 1.89E-09 |
| CFE | 7.47E-08 | 7.38E+02 | 7.38E+04 | 5.51E-03 | 81.06% | 7.47E-08 |
| IC | 2.21E-06 | 8.16E-02 | 8.16E+00 | 1.80E-05 | 0.27% | |
| BP | 1.05E-07 | 2.78E+01 | 2.78E+03 | 2.92E-04 | 4.29% | 1.05E-07 |
| CI | 1.33E-08 | 7.19E+02 | 7.19E+04 | 9.56E-04 | 14.06% | 1.33E-08 |
| CFL | 3.45E-12 | 1.95E-01 | 1.95E+01 | 6.73E-11 | 0.00% | |
| Totals = | 2.40E-06 | | | **6.80E-03** | 100.00% | **1.95E-07** |

Table 720.057-7

| Summary Table of Dose Sensitivity Cases<br>Site Boundary Whole Body Dose (Effective Dose Equivalent, EDE) | | | | |
|---|---|---|---|---|
| Description | | Release Freq. | LRF | Risk (REM/ry) |
| **Base Case** | 24 Hours | 2.40E-07 | 1.95E-08 | 6.80E-05 |
| **Sens 1** | 24 Hours; IC replaced by DIRECT | 2.40E-07 | 1.95E-08 | 6.84E-05 |
| **Sens 2** | 72 hours | 2.40E-07 | 1.95E-08 | 7.65E-05 |
| **Sens 3** | 24 Hours - upper-bound release frequencies | 1.32E-06 | 2.12E-07 | 7.79E-04 |
| **Sens 4** | 72 Hours - upper-bound release frequencies | 1.32E-06 | 2.12E-07 | 8.53E-04 |
| **Sens 5** | 24 Hrs - 10 times release frequency and 10 times mean dose | 2.40E-06 | 1.95E-07 | 6.80E-03 |

**Attachment B to RAI 720.057 – AP1000 PRA**

**Calculation of LRF Component, Operator Action and Initiating Event Importances for Internal Events At Power**

The objective of this section is to provide basic event, operator action, and component importances for AP1000 LRF for at power events, which were documented in Chapter 43 of the AP1000 PRA already submitted to the NRC. At the time of this submittal, the LRF cutsets for the top 6 dominant LRF sequences were provided in Table 43-6. These cutsets were not sufficient to make importance calculations. Thus no importance tables were provided at that time.

In order to make component/operator action/initiating event importance analyses, first the LRF cutsets from the top 26 LRF sequences are collected. these comprise more than 99.9% of the LRF for at power events. During this process, a few errors are identified and fixed. Based on these fixes, the LRF is calculated to be 1.92E-08/yr. The new value of the LRF compares favorably with that of 1.95E-08/yr which appears in Chapter 43.

The dominant sequences associated with the new LRF value are given in the attached Table 720.057-8. Using the 26 top sequences from this table, 27,881 LRF cutsets are collected for importance analyses, with a LRF value of 1.91E-08/year.

Based on these LRF cutsets, the following importance analyses are made and given in the Attached Table 720.057-9, 10 and 11:

Table 720.057-9: The contribution initiating event categories to LRF (initiating event importances) are calculated and are reported in this table.

Table 720.057-10: The risk increase measures of component and operator action basic events are reported in this table.

Table 720.057-11: The risk decrease measures of component and operator action basic events are reported in this table.

### Table 720.057-8 Dominant LRF Sequences

| CET SEQ | REL CAT | PDS | FREQ | % CONTRIBUTION | SEQUENCE DESCRIPTION |
|---|---|---|---|---|---|
| 23 | BP | 3A | 4.077E-09 | 21.28% | Containment Bypass |
| 23 | BP | 6 | 3.773E-09 | 19.69% | Containment Bypass |
| 21 | CFE | 2E | 2.667E-09 | 13.92% | Sump Flooding Fails |
| 21 | CFE | 3D | 2.046E-09 | 10.68% | Sump Flooding Fails |
| 23 | BP | 1A | 2.042E-09 | 10.66% | Containment Bypass |
| 10 | CFE | 3C | 9.973E-10 | 5.20% | Vessel Failure |
| 12 | CFE | 3D | 9.706E-10 | 5.07% | Core Reflooding Fails; Diffusion Flame |
| 21 | CFE | 6 | 6.456E-10 | 3.37% | Sump Flooding Fails |
| 23 | BP | 1P | 6.052E-10 | 3.16% | Containment Bypass |
| 22 | CI | 2L | 5.826E-10 | 3.04% | Containment Isolation Fails |
| 22 | CI | 3D | 3.622E-10 | 1.89% | Containment Isolation Fails |
| 22 | CI | 2E | 1.317E-10 | 0.69% | Containment Isolation Fails |
| 22 | CI | 2R | 7.669E-11 | 0.40% | Containment Isolation Fails |
| 22 | CI | 6 | 5.513E-11 | 0.29% | Containment Isolation Fails |
| 22 | CI | 3C | 2.658E-11 | 0.14% | Containment Isolation Fails |
| 6 | CFE | 2E | 2.514E-11 | 0.13% | Hydrogen Igniters Fail; Early DDT |
| 16 | CFE | 3D | 1.704E-11 | 0.09% | Core Reflooding Fails; Hydrogen Igniters Fail; Early DDT |
| 2 | CFE | 1P | 1.477E-11 | 0.08% | Diffusion Flame |
| 6 | CFE | 2R | 1.002E-11 | 0.05% | Hydrogen Igniters Fail; Early DDT |
| 4 | CFI | 2E | 9.605E-12 | 0.05% | Hydrogen Igniters Fails; Intermediate DDT |
| 22 | CI | 3A | 6.328E-12 | 0.03% | Containment Isolation Fails |
| 4 | CFI | 2R | 5.555E-12 | 0.03% | Hydrogen Igniters Fails; Intermediate DDT |
| 22 | CI | 1A | 4.602E-12 | 0.02% | Containment Isolation Fails |
| 16 | CFE | 2E | 4.373E-12 | 0.02% | Core Reflooding Fails; Hydrogen Igniters Fail; Early DDT |
| 6 | CFE | 3C | 1.954E-12 | 0.01% | Hydrogen Igniters Fail; Early DDT |
| 22 | CI | 1P | 1.324E-12 | 0.01% | Containment Isolation Fails |
| 4 | CFI | 3C | 1.083E-12 | 0.01% | Hydrogen Igniters Fails; Intermediate DDT |
| 16 | CFE | 2L | 1.826E-13 | 0.00% | Core Reflooding Fails; Hydrogen Igniters Fail; Early DDT |
| 14 | CFI | 3D | 1.705E-13 | 0.00% | Core Reflooding Fails; Hydrogen Igniters fails; Intermediate DDT |
| 4 | CFI | 1P | 1.151E-13 | 0.00% | Hydrogen Igniters Fails; Intermediate DDT |
| 9 | CFL | 2E | 9.802E-14 | 0.00% | Passive Containment Cooling Fails; Venting Fails; Containment Fails |

| CET SEQ | REL CAT | PDS | FREQ | % CONTRIBUTION | SEQUENCE DESCRIPTION |
|---|---|---|---|---|---|
| 19 | CFL | 3D | 8.602E-14 | 0.00% | Core Reflooding Fails; Passive Containment Cooling Fails; Venting Fails; Containment Fails |
| 9 | CFL | 2R | 5.200E-14 | 0.00% | Passive Containment Cooling Fails; Venting Fails; Containment Fails |
| 6 | CFE | 1P | 5.055E-14 | 0.00% | Hydrogen Igniters Fail; Early DDT |
| 14 | CFI | 2L | 4.725E-14 | 0.00% | Core Reflooding Fails; Hydrogen Igniters fails; Intermediate DDT |
| 14 | CFI | 2E | 4.290E-14 | 0.00% | Core Reflooding Fails; Hydrogen Igniters fails; Intermediate DDT |
| 16 | CFE | 6 | 3.947E-14 | 0.00% | Core Reflooding Fails; Hydrogen Igniters Fail; Early DDT |
| 19 | CFL | 2E | 3.571E-14 | 0.00% | Core Reflooding Fails; Passive Containment Cooling Fails; Venting Fails; Containment Fails |
| 9 | CFL | 3A | 2.419E-14 | 0.00% | Passive Containment Cooling Fails; Venting Fails; Containment Fails |
| 19 | CFL | 2L | 2.349E-14 | 0.00% | Core Reflooding Fails; Passive Containment Cooling Fails; Venting Fails; Containment Fails |
| 9 | CFL | 3C | 1.037E-14 | 0.00% | Passive Containment Cooling Fails; Venting Fails; Containment Fails |
| 14 | CFI | 6 | 1.021E-14 | 0.00% | Core Reflooding Fails; Hydrogen Igniters fails; Intermediate DDT |
| 9 | CFL | 1A | 9.712E-15 | 0.00% | Passive Containment Cooling Fails; Venting Fails; Containment Fails |
| 19 | CFL | 6 | 5.076E-15 | 0.00% | Core Reflooding Fails; Passive Containment Cooling Fails; Venting Fails; Containment Fails |
| | | | | | |
| | | **Sum** | **1.92E-08** | **100.00%** | |

**Table 720.057-9 Initiating Event Importances in LRF**

| SYSTEM UNAVAILABILITY (Q) = 1.91E-08 | | | | | |
|---|---|---|---|---|---|
| NUMBER OF BASIC EVENTS = 26 | | | | | |
| NUMBER OF CUTSETS = 27881 | | | | | |
| | **Initiating Event Category** | **% Contribution to LRF** | **Number of Cutsets** | **LRF Contribution** | **Initiating Event Frequency** |
| | | | | | |
| 1 | IEV-ATWS | 17.11% | 225 | 3.27E-09 | 4.81E-01 |
| 2 | IEV-SGTR | 15.87% | 2675 | 3.04E-09 | 3.88E-03 |
| 3 | IEV-SPADS | 13.14% | 1882 | 2.51E-09 | 5.40E-05 |
| 4 | IEV-SI-LB | 9.82% | 3234 | 1.88E-09 | 2.12E-04 |
| 5 | IEV-TRANS | 7.49% | 1628 | 1.43E-09 | 1.40E+00 |
| 6 | IEV-SLOCA | 5.94% | 3499 | 1.14E-09 | 5.00E-04 |
| 7 | IEV-RV-RP | 5.37% | 85 | 1.03E-09 | 1.00E-08 |
| 8 | IEV-MLOCA | 4.71% | 3432 | 9.02E-10 | 4.36E-04 |
| 9 | IEV-ATW-T | 3.72% | 8 | 7.12E-10 | 1.17E+00 |
| 10 | IEV-LCOND | 2.73% | 565 | 5.22E-10 | 1.12E-01 |
| 11 | IEV-LOSP | 2.46% | 539 | 4.70E-10 | 1.20E-01 |
| 12 | IEV-LMFW | 1.98% | 754 | 3.80E-10 | 3.35E-01 |
| 13 | IEV-LLOCA | 1.65% | 1016 | 3.16E-10 | 5.00E-06 |
| 14 | IEV-RCSLK | 1.53% | 3185 | 2.93E-10 | 6.20E-03 |
| 15 | IEV-SLB-V | 1.22% | 283 | 2.33E-10 | 2.39E-03 |
| 16 | IEV-LMFW1 | 1.11% | 445 | 2.12E-10 | 1.92E-01 |
| 17 | IEV-CMTLB | 1.03% | 1690 | 1.98E-10 | 9.31E-05 |
| 18 | IEV-LCCW | 0.72% | 369 | 1.37E-10 | 1.44E-01 |
| 19 | IEV-ATW-S | 0.53% | 49 | 1.01E-10 | 1.48E-02 |
| 20 | IEV-LCAS | 0.52% | 319 | 1.00E-10 | 3.48E-02 |
| 21 | IEV-POWEX | 0.50% | 1055 | 9.49E-11 | 4.50E-03 |
| 22 | IEV-PRSTR | 0.45% | 723 | 8.64E-11 | 1.34E-04 |
| 23 | IEV-SLB-U | 0.26% | 132 | 4.97E-11 | 3.72E-04 |
| 24 | IEV-LRCS | 0.08% | 67 | 1.58E-11 | 1.80E-02 |
| 25 | IEV-SLB-D | 0.05% | 14 | 9.07E-12 | 5.96E-04 |
| 26 | IEV-ISLOC | 0.00% | 8 | 4.74E-13 | 5.00E-11 |
| | | | | | |
| | Sum = | 100.00% | | 1.91E-08 | 2.38E+00 |
| | | | | | |

### Table 720.057-10. Component And Operator Action Basic Events Listed By RAW Value > 1.19 for LRF

| BASIC EVENT ID | Probability | RAW | Description |
|---|---|---|---|
| CCX-SFTW | 1.20E-06 | 8.90E+04 | CCF SOFTWARE - ALL CARDS |
| CCX-PMXMOD1-SW | 1.10E-05 | 1.00E+04 | CCF OF PMS ESF OUTPUT LOGIC SOFTWARE |
| CCX-EP-SAM | 8.62E-06 | 1.00E+04 | CCF OF EPO BOARDS IN PMS (POWER INTERFACE OUTPUT BOARD) |
| IWX-FL-GP | 1.20E-05 | 9.39E+03 | CCF OF STRAINERS IN IRWST TANK |
| ADX-EV-SA | 3.00E-05 | 1.10E+03 | CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE |
| ADX-EV-SA2 | 5.90E-05 | 1.05E+03 | CCF OF 2 SQUIB VALVES TO OPERATE |
| CCX-XMTR | 4.78E-04 | 4.45E+02 | CCF OF PRESSURE TRANSMITTERS |
| CCX-BY-PN | 4.70E-05 | 4.45E+02 | COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B |
| CCX-XMTR195 | 4.78E-04 | 4.30E+02 | COMMON CAUSE FAILURE OF PZR LEVEL SENSORS |
| ALL-IND-FAIL | 1.00E-06 | 2.94E+02 | GENERIC INDICATION FAILURE PROBABILITY |
| IWX-EV-SA | 2.60E-05 | 2.23E+02 | CCF OF 4 GRAVITY INJECTION & 2 RECIRCULATION SQUIB VALVES |
| CMX-VS-FA | 3.84E-05 | 2.22E+02 | CCF OF CMT LEVEL SWITCHES |
| IWX-CV-AO | 3.00E-05 | 2.17E+02 | CCF OF 4 GRAVITY INJECTION CVs |
| CCX-INPUT-LOGIC | 1.03E-04 | 1.96E+02 | CCF OF ESF INPUT LOGIC (HARDWARE) |
| ED3MOD07 | 3.05E-04 | 1.78E+02 | EDS3 EA 1 DISTR. PNL FAILURE OR T&M |
| CCX-IN-LOGIC-SW | 1.10E-05 | 1.73E+02 | CCF OF ESF INPUT LOGIC SOFTWARE |
| CCX-PMXMOD2-SW | 1.10E-05 | 1.73E+02 | CCF OF PMS ESF ACTUATION LOGIC SOFTWARE |
| REX-FL-GP | 1.20E-05 | 1.67E+02 | CCF PLUGGING OF BOTH RECIRC LINES DUE TO SUMP SCREENS |
| CCX-AV-LA | 6.20E-05 | 1.50E+02 | COMMON CAUSE FAILURE OF 4 AOVS TO OPEN |
| CMX-CV-GO | 5.10E-05 | 1.29E+02 | COMMON CAUSE FAILURE OF 4 CHECK VALVES TO OPEN |
| CCX-PMXMOD4-SW | 1.10E-05 | 1.23E+02 | CCF OF SOFTWARE - MUX LOGIC GROUPS (CCX-P##MOD4-SW) |
| IWA-PLUG | 2.40E-04 | 1.10E+02 | IWRST DISCHARGE LINE "A" STRAINER PLUGGED |
| IWX-EV1-SA | 5.80E-06 | 1.10E+02 | CCF OF 2 GRAVITY INJECTION SQUIB VALVES IN 1/1 LINES TO OPEN |
| IWX-CV1-AO | 5.40E-07 | 1.09E+02 | CCF OF GRAVITY INJECTION CVs IN 1/1 LINES TO OPEN |
| CMX-TK-AF | 1.20E-07 | 8.34E+01 | COMMON CAUSE FAILURE OF TANKS |
| RPX-CB-GO | 4.20E-04 | 7.91E+01 | CCF TO OPEN OF 4.16 KVAC CIRCUIT BREAKERS |
| PXX-AV-LA | 9.60E-05 | 6.72E+01 | FAILURE OF PRHR DUE TO COMMON CAUSE OF AOVs |
| PXX-AV-LA1 | 9.60E-05 | 6.72E+01 | FAILURE OF IRWST GUTTER DUE TO COMMON CAUSE OF AOVs |
| ADX-MV3-GO | 3.24E-04 | 6.30E+01 | CCF OF 4 COMBINATIONS OF 3 STAGES #2 AND #3 MOVS |
| IWX-XMTR | 4.78E-04 | 5.53E+01 | CCF OF IRWST LEVEL TRANSMITTERS |

| BASIC EVENT ID | Probability | RAW | Description |
|---|---|---|---|
| IWNTK001AF | 2.40E-06 | 3.68E+01 | FAILURE OF THE PRHR DUE TO IRWS TANK FAILURE |
| PCNHR001ML | 2.40E-06 | 3.68E+01 | PLUG/LEAK OF PRHR HEAT EXCHANGER |
| RCX-RB-FA | 8.10E-06 | 2.99E+01 | CCF OF REACTOR TRIP BREAKERS |
| CIX-AV-LA | 7.70E-04 | 2.90E+01 | COMMON CAUSE FAILURE OF ALL CI AOVS TO CLOSE |
| CCX-XMTR1 | 4.78E-04 | 2.89E+01 | CCF OF PRESSURE TRANSMITTERS FOLLOWING ACCIDENT (CCX-XMTR1) |
| CCX-TRNSM | 4.78E-04 | 2.48E+01 | CCF NON-SAFETY TRANSMITTERS INTERFACING SYSTEM PRESSURE |
| IDBBSDS1TM | 3.00E-04 | 2.33E+01 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| IDBBSDD1TM | 3.00E-04 | 2.33E+01 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| CMA-PLUG | 7.27E-04 | 2.18E+01 | FLOW TUNING ORIFICE PLUGS |
| CMX-AV-LA | 9.60E-05 | 2.17E+01 | COMMON CAUSE FAILURE (DELTA) FOR 2 AOVS TO OPEN |
| CMATK002AF | 2.40E-06 | 2.14E+01 | CMT TANK T002A RUPTURES |
| CMA-CV | 2.00E-06 | 2.13E+01 | CHECK VALVES V016A/017A FAIL TO OPEN |
| CMAOR001EB | 7.20E-07 | 2.09E+01 | FLOW TUNING ORIFICE RUPTURES |
| IDDBSDS1TM | 3.00E-04 | 1.59E+01 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| IDDBSDD1TM | 3.00E-04 | 1.59E+01 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| CCX-BC-SA | 8.40E-06 | 1.38E+01 | COMMON CAUSE FAILURE OF THE BATTERY CHARGERS |
| IDBFD013RQ | 1.20E-05 | 1.35E+01 | FUSE DISCONNECT SWITCH (FD13) SPURIOUSLY OPENS |
| IDDFD019RQ | 1.20E-05 | 1.24E+01 | FUSE DISCONNECT SWITCH (FD19) SPURIOUSLY OPENS |
| CCX-TT-UF | 1.17E-04 | 1.20E+01 | CCF OF TEMPERATURE TRANSMITTERS (CCX-TT-UF) |
| CIB-MAN00 | 1.84E-03 | 1.11E+01 | COGNITIVE OPERATOR ERROR |
| IDBBSDS1LF | 4.80E-06 | 1.10E+01 | BUS IDSB-DS-1 FAILS (ALL MODES) |
| IDBBSDD1LF | 4.80E-06 | 1.10E+01 | BUS IDSB-DD-1 FAILS (ALL MODES) |
| IDDBSDD1LF | 4.80E-06 | 1.02E+01 | BUS IDSD-DD-1 FAILS (ALL MODES) |
| IDDBSDS1LF | 4.80E-06 | 1.02E+01 | BUS IDSD-DS-1 FAILS (ALL MODES) |
| IWX-EV4-SA | 5.80E-05 | 1.00E+01 | CCF OF 2 OUT 2 LOW PRESSURE RECIRCULATION SQUIB VALVES |
| MDAS | 1.00E-02 | 9.39 | UNAVAILABILITY GOAL FOR MANUAL DIVERSE ACTUATION SYSTEM |
| CIC-MAN01 | 1.20E-03 | 9.27 | OPERATOR FAILS TO RECOGNIZE NEED AND FAILS TO ISOLATE CMT GIVEN CORE DAMAGE AFTER A LOCA |
| CCX-PMS-HARDWARE | 7.89E-05 | 9.26 | PMS REACTOR TRIP SYSTEM HARDWARE CCF |
| REC-MANDAS | 1.16E-02 | 8.81 | FAILURE OF MANUAL DAS ACT. |
| REN-MAN03 | 3.40E-03 | 8.37 | FAILURE TO OPEN RECIRC MOVs |
| IWX-MV-GO | 4.40E-03 | 8.35 | CCF OF RECIRC MOVs TO OPEN |

| BASIC EVENT ID | Probability | RAW | Description |
|---|---|---|---|
| ACX-CV-GO | 5.10E-05 | 8.32 | CCF OF 2 ACCUMULATOR CHECK VALVES |
| OTH-SGTR | 1.00E-02 | 8.24 | CONSEQUENTIAL SGTR OCCURS |
| ATW-MAN05 | 5.20E-03 | 8.12 | OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS |
| EC1BS001TM | 2.70E-03 | 7.51 | UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDUL MAINTENANCE |
| CCX-EP-SA | 8.62E-06 | 6.97 | CCF OF THE POWER INTERFACE OUTPUT BOARD (CCX-EP-SA) |
| EC1BS012TM | 2.70E-03 | 6.95 | BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE |
| CIB-MAN01 | 1.34E-03 | 6.86 | OPERATOR ERROR TO CLOSE VALVES ON RUPTURED SG |
| IDABSDS1TM | 3.00E-04 | 6.51 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| IDABSDD1TM | 3.00E-04 | 6.50 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| DAS | 1.00E-02 | 6.44 | UNAVAILABILITY GOAL FOR DAS |
| IDCBSDS1TM | 3.00E-04 | 6.00 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| IDCBSDD1TM | 3.00E-04 | 6.00 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| CCX-IV-XR | 2.40E-05 | 5.68 | COMMON CAUSE FAILURE OF THE INVERTER |
| LPM-MAN01 | 1.34E-03 | 5.22 | OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING SLOCA |
| ACX-TK-AF | 1.20E-07 | 5.13 | CCF FAILURE OF ACCUMULATOR TANKS |
| ADN-MAN01 | 3.02E-03 | 4.95 | OPERATOR FAILS TO FULFIL MANUAL ACTUATION OF ADS |
| SGBAV040LA | 1.09E-03 | 4.51 | AOV MSIV V040B FAILS TO CLOSE |
| ATW-MAN03 | 5.20E-02 | 4.21 | OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS |
| EC1MOD12 | 4.80E-05 | 4.19 | FIXED COMPONENT FAULTS |
| OTH-DF | 1.70E-02 | 4.03 | CONTAINMENT FAILURE DUE TO DIFFUSION FLAME |
| CCX-PMAMOD1 | 1.41E-04 | 3.53 | CCF OF OUTPUT LOGIC I/Os (CCX- P##MOD1) |
| IDAFD003RQ | 1.20E-05 | 3.52 | FUSE DISCONNECT SWITCH (FD3) SPURIOUSLY OPENS |
| CCX-PMA030 | 9.69E-05 | 3.42 | CCF OF THE LOGIC GROUP PROCESSING (CCX-###03) |
| REA-PLUG | 2.40E-04 | 3.41 | SUMP SCREEN A PLUGS AND PREVENTS FLOW |
| REN-MAN04 | 1.00E-02 | 3.25 | OPER. FAILS TO ACT. SUMP RECIRC GIVEN IRW LEVEL SIGNAL FAILURE |
| VLX-HI-SA | 3.20E-04 | 3.24 | CCF OF THE HYDROGEN IGNITERS |
| EDSMOD01 | 3.05E-04 | 3.24 | FAILURE OF THE 12 VAC DISTRBN PANEL |
| VLX-ANLYZ | 7.58E-05 | 3.16 | CCF OF HYDROGEN ANALYZER SENSORS |
| OTH-SLSOV1 | 2.10E-02 | 3.12 | ANY SECOND. SIDE RELIEF VALVE FAILS TO CLOSE (2 SV + PORV) |
| REB-PLUG | 2.40E-04 | 3.00 | SUMP SCREEN B PLUGS AND PREVENTS FLOW |
| IDABSDS1LF | 4.80E-06 | 2.97 | BUS IDSA-DS-1 FAILS (ALL MODES) |
| IDABSDD1LF | 4.80E-06 | 2.97 | BUS IDSA-DD-1 FAILS (ALL MODES) |

| BASIC EVENT ID | Probability | RAW | Description |
|---|---|---|---|
| CCX-VS-FA | 3.84E-05 | 2.88 | CCF OF CMT LEVEL SWITCHES (CMX -VS-FA) |
| IDCFD007RQ | 1.20E-05 | 2.81 | FUSE DISCONNECT SWITCH (FD7) SPURIOUSLY OPENS |
| ED1BSDS1TM | 3.00E-04 | 2.72 | BUS EDS1 DS 1 UNAVAILABLE DUE TO CORRECTIVE MAINTENANCE |
| ED1MOD11 | 3.17E-04 | 2.69 | FIXED COMPONENTS FAILURE |
| ED1MOD113 | 3.17E-04 | 2.69 | FIXED COMPONENTS FAILURE |
| CVN-MAN00 | 3.10E-03 | 2.57 | FAILURE TO ALIGN CVCS IN AUX. SPRAY MODE |
| OTH-SLSOV | 1.10E-02 | 2.52 | ANY SECOND. SIDE RELIEF VALVE FAILS TO RECLOSE (1 SV + PORV) |
| IDCBSDD1LF | 4.80E-06 | 2.31 | BUS IDSC-DD-1 FAILS (ALL MODES) |
| IDCBSDS1LF | 4.80E-06 | 2.31 | BUS IDSC-DS-1 FAILS (ALL MODES) |
| EC2BS002TM | 2.70E-03 | 2.30 | UNAVAILABILITY OF BUS ECS ES 2 DUE TO UNSCHEDUL MAINTENANCE |
| RN11MOD3 | 1.41E-02 | 2.29 | HARDWARE FAILURE OF ISOLATION MOV 011 |
| RN22MOD4 | 1.41E-02 | 2.29 | HARDWARE FAILS TO OPEN MOV V022 / CB FTC / RELAY FTC |
| RN23MOD5 | 1.41E-02 | 2.29 | HARDWARE FAILS TO OPEN MOV V023 / CB FTC / RELAY FTC |
| RN55MOD1 | 1.41E-02 | 2.29 | MECHANICAL FAILURE OF RNS MOV V055 |
| CLP-UNAVAILABLE | 1.00E-02 | 2.29 | CASK LOADING PIT UNAVAILABLE DUE TO FUEL UNLOADING OPERATIONS |
| CCX-PMDMOD1 | 1.41E-04 | 2.28 | CCF OF OUTPUT LOGIC I/Os (CCX- P##MOD1) |
| RNX-KV1-GO | 4.90E-03 | 2.28 | CCF OF STOP CHECK VALVES V015A/B TO OPEN |
| EC1BS122TM | 2.70E-03 | 2.28 | BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE |
| RHN-MAN01 | 2.90E-03 | 2.28 | OPERATOR FAILS TO ALIGN AND ACTUATE THE RNS |
| IDABSDK1TM | 3.00E-04 | 2.27 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| RNNCV013GO | 1.75E-03 | 2.26 | CHECK VALVE V013 FAILURE TO OPEN |
| RNX-PM-FS | 7.70E-04 | 2.23 | CCF OF PUMPS TO START |
| RNX-KV-GO | 6.10E-04 | 2.23 | CCF OF STOP CHECK VALVES V007A/B TO OPEN |
| CCX-PMD030 | 9.69E-05 | 2.20 | CCF OF THE LOGIC GROUP PROCESSING (CCX-###03) |
| EC2BS022TM | 2.70E-03 | 2.18 | BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE |
| IDBBSDK1TM | 3.00E-04 | 2.16 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| VLN-MAN01 | 3.32E-04 | 2.15 | OPERATOR FAILS TO RECOGNIZE NEED AND FAILS TO START HYDROGEN CONTROL SYSTEM |
| RNNCV056GO | 2.19E-04 | 2.14 | CHECK VALVE V056 FAILS TO OPEN |
| EC0MOD01 | 5.08E-03 | 2.11 | MAIN GEN. BKR ES 01 FAILS TO OPEN [# 12] |
| AD4MOD07 | 5.80E-04 | 2.07 | HARDWARE FAILURE OF ST. #4 LINE 1 |
| AD4MOD10 | 5.80E-04 | 2.07 | HARDWARE FAILURE OF ST. #4 LINE 4 |

| BASIC EVENT ID | Probability | RAW | Description |
|---|---|---|---|
| AD4MOD09 | 5.80E-04 | 2.07 | HARDWARE FAILURE OF ST. #4 LINE 3 |
| AD4MOD08 | 5.80E-04 | 2.07 | HARDWARE FAILURE OF ST. #4 LINE 2 |
| EC2BS221TM | 2.70E-03 | 2.07 | BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE |
| RNDEP023SA | 1.71E-04 | 2.05 | FAILURE OF THE POWER INTERFACE BOARD (###EP####SA) |
| RNBEP011SA | 1.71E-04 | 2.05 | FAILURE OF THE POWER INTERFACE BOARD (###EP####SA) |
| RNAEP022SA | 1.71E-04 | 2.05 | FAILURE OF THE POWER INTERFACE BOARD (###EP####SA) |
| ADX-MV-GO | 7.48E-04 | 2.05 | 3/4 STAGE 2 & 3 LINES FAIL DUE TO CCF OF MOVs TO OPEN |
| CCX-PL4MOD1 | 1.41E-04 | 2.05 | CCF OF OUTPUT LOGIC I/Os (CCX- P##MOD1) |
| CCX-PLMMOD4 | 4.98E-05 | 2.02 | CCF OF MUX LOGIC GROUPS (CCX-P ##MOD4) |
| CCX-PL403 | 9.69E-05 | 1.98 | CCF OF THE LOGIC GROUP PROCESSING (CCX-###03) |
| ACACV029GO | 1.75E-03 | 1.94 | CHECK VALVE 029A FAILS TO OPEN |
| ACACV028GO | 1.75E-03 | 1.94 | CHECK VALVE 028A FAILS TO OPEN |
| CCX-PMAMOD4 | 4.98E-05 | 1.94 | CCF OF MUX LOGIC GROUPS (CCX-P ##MOD4) |
| ACAOR001SP | 7.27E-04 | 1.93 | FLOW TUNING ORIFICE PLUGS |
| CCX-PMDMOD4 | 4.98E-05 | 1.89 | CCF OF MUX LOGIC GROUPS (CCX-P ##MOD4) |
| RNX-CV-GO | 5.10E-05 | 1.88 | CCF OF CHECK VALVES V017A/B TO OPEN |
| CCX-PLMMOD4-SW | 1.10E-05 | 1.82 | SOFTWARE CCF OF MUX LOGIC GROUPS (CCX-P##MOD4-SW) |
| CANCV015GC | 2.45E-02 | 1.81 | INSIDE CONTAIN. CV V015 FAILS TO CLOSE |
| CANTP011RI | 5.23E-03 | 1.78 | FAILURE OF AIR COMPRESSOR TRANSMITTER |
| CVMOD04 | 7.37E-04 | 1.78 | DISCHARGE LINE FAILURE |
| EC1MOD122 | 1.68E-05 | 1.75 | FIXED COMPONENT FAULTS |
| RNX-PM-ER | 1.60E-05 | 1.75 | CCF OF PUMPS TO RUN |
| IDAFD004RQ | 1.20E-05 | 1.75 | FUSE DISCONNECT SWITCH (FD4) SPURIOUSLY OPENS |
| IDBFD014RQ | 1.20E-05 | 1.75 | FUSE DISCONNECT SWITCH (FD14) SPURIOUSLY OPENS |
| CCX-PL4MOD1-SW | 1.10E-05 | 1.74 | SOFTWARE CCF OF OUTPUT LOGIC I /Os (CCX-P##MOD1) |
| EC1BS001LF | 4.80E-06 | 1.70 | MECHANICAL FAULT ON BUS ECS ES 1 |
| LPM-MAN02 | 3.30E-03 | 1.68 | OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA |
| CANAV014LA | 8.76E-03 | 1.67 | AOV V014 FAILS TO CLOSE |
| ACATK001AF | 2.40E-06 | 1.66 | ACCUMULATOR TANK A (T001A) RUPTURES |
| ED1BSDS1LF | 4.80E-06 | 1.66 | EDS1 DS 1 SWITCHGEAR FAILURE |
| IDABSDK1LF | 4.80E-06 | 1.66 | BUS IDSA-DK-1 FAILS (ALL MODES) |
| IDBBSDK1LF | 4.80E-06 | 1.66 | BUS IDSB-DK-1 FAILS (ALL MODES) |

# AP1000 DESIGN CERTIFICATION REVIEW

## Response to Request For Additional Information

| BASIC EVENT ID | Probability | RAW | Description |
|---|---|---|---|
| EC1BS121TM | 2.70E-03 | 1.65 | BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE |
| CCX-PL4EH0 | 4.03E-06 | 1.65 | CCF OF MUX TRANSMITTERS (CCX-# ##EH0) |
| CCX-PMAEH0 | 4.03E-06 | 1.65 | CCF OF MUX TRANSMITTERS (CCX-# ##EH0) |
| CCX-PMDEH0 | 4.03E-06 | 1.65 | CCF OF MUX TRANSMITTERS (CCX-# ##EH0) |
| CIAEP014SA | 1.71E-04 | 1.62 | FAILURE OF THE POWER INTERFACE BOARD (###EP####SA) |
| CVMOD01 | 2.21E-04 | 1.62 | CVS SUCTION FOM BORIC ACID TANK FAILURE |
| RPTMOD07 | 8.76E-04 | 1.59 | COMPONENTS FAILURE |
| RPTMOD05 | 8.76E-04 | 1.59 | COMPONENTS FAILURE |
| RPTMOD03 | 8.76E-04 | 1.59 | COMPONENTS FAILURE |
| RPTMOD01 | 8.76E-04 | 1.59 | COMPONENTS FAILURE |
| OTH-SDMAN | 7.70E-04 | 1.58 | OPERATOR FAILS TO PERFORM CNTRL REACTOR SHUTDOWN DURING ACCIDENT |
| IWACV124AO | 1.75E-03 | 1.54 | CHECK VALVE 124A FAILS TO OPEN |
| IRWMOD06 | 1.46E-03 | 1.54 | HARDWARE FAILURE OF VALVE 125A |
| ACAOR001EB | 7.20E-07 | 1.54 | FLOW TUNING ORIFICE RUPTURES |
| ACBCV028GO | 1.75E-03 | 1.54 | CHECK VALVE 028B FAILS TO OPEN |
| ACBCV029GO | 1.75E-03 | 1.54 | CHECK VALVE 029B FAILS TO OPEN |
| IWDRS125AFA | 8.76E-04 | 1.54 | RELAY FAILS TO OPERATE |
| ACBOR001SP | 7.27E-04 | 1.54 | FLOW TUNING ORIFICE PLUGS |
| OTH-CNB | 1.00E-03 | 1.52 | CONTAINMENT ISOL FAILURE DUE TO RV RUPTURE |
| OTH-SLSOV3 | 5.40E-03 | 1.52 | FAILURE TO RECLOSE OF SG PORV & 1 SG SV ON RUPTURED SG |
| IWACV122AO | 1.75E-03 | 1.52 | CHECK VALVE 122A FAILS TO OPEN |
| IRWMOD05 | 1.46E-03 | 1.52 | HARDWARE FAILURE OF VALVE 123A |
| IWBRS123AFA | 8.76E-04 | 1.52 | RELAY FAILS TO OPERATE |
| CCX-PL3MOD1 | 1.41E-04 | 1.51 | CCF OF OUTPUT LOGIC I/Os (CCX- P##MOD1) |
| RC1CB051GO | 4.20E-03 | 1.51 | PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN |
| RC1CB053GO | 4.20E-03 | 1.51 | PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN |
| RC1CB061GO | 4.20E-03 | 1.51 | PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN |
| RC1CB063GO | 4.20E-03 | 1.51 | PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN |
| CCX-PLSMOD6 | 2.53E-04 | 1.50 | CCF OF SUB-SYSTEMS IN SIGNAL SELECTOR CABINET |
| SWAMOD09T | 2.52E-04 | 1.49 | OPERATING BLOWER FAN HARDWARE FAILURE |
| OTH-PRSOV | 1.00E-02 | 1.47 | EITHER PRZR SV FAILS TO RECLOSE |
| OTH-MGSET | 1.75E-03 | 1.47 | CONTROL ROD MG SETS FAIL TO TRIP |

| BASIC EVENT ID | Probability | RAW | Description |
|---|---|---|---|
| CFE-OCCURS | 1.00E-01 | 1.47 | EARLY CONTAINMENT FAILURE OCCURS DUE TO VESSEL FAILURE |
| CCX-PL303 | 9.69E-05 | 1.40 | CCF OF THE LOGIC GROUP PROCESSING (CCX-###03) |
| ED3MOD01 | 5.04E-04 | 1.40 | FIXED COMPONENT FAILS: CKT BKR, INVERTER, OR STATIC XFER SW |
| ACBTK001AF | 2.40E-06 | 1.38 | ACCUMULATOR TANK B (T001B) RUPTURES |
| ED4MOD112 | 3.17E-04 | 1.33 | FIXED COMPONENTS FAILURE |
| ED4MOD11 | 3.17E-04 | 1.33 | FIXED COMPONENTS FAILURE |
| ACBOR001EB | 7.20E-07 | 1.33 | FLOW TUNING ORIFICE RUPTURES |
| ED4BSDS1TM | 3.00E-04 | 1.32 | BUS EDS4 DS 1 UNAVAILABLE DUE TO CORRECTIVE MAINTENANCE |
| RC1CB054GO | 4.20E-03 | 1.31 | PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN |
| RC1CB052GO | 4.20E-03 | 1.31 | PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN |
| OTH-SLSOV2 | 1.00E-02 | 1.31 | ANY SECOND. SIDE RELIEF VALVE FAILS TO CLOSE (1 SV) |
| FWX-MV2-GO | 5.50E-04 | 1.30 | CCF OF SFW MOVS V013A, AND V013B |
| OTH-SGTR1 | 6.70E-03 | 1.30 | SINGLE CONSEQUENTIAL SGTR |
| FWX-PM2-FS | 5.40E-04 | 1.30 | CCF OF BOTH STARTUP FEED PUMPS TO START |
| RC1CB064GO | 4.20E-03 | 1.30 | PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN |
| RC1CB062GO | 4.20E-03 | 1.30 | PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN |
| CONDVACUUM | 1.00E-03 | 1.30 | FAILURE OF MAIN COND. EVACUATION SYST. TO PROVIDE VACUUM |
| ZOX-PD-ES | 2.00E-03 | 1.27 | CCF TO START OF ENGINE-DRIVEN FUEL PUMPS |
| CCX-PL9MOD1 | 1.41E-04 | 1.27 | CCF OF OUTPUT LOGIC I/Os (CCX- P##MOD1) |
| CAX-CM-ER | 1.20E-04 | 1.26 | CCF OF COMPRESSORS TO RUN |
| CCX-PLMOD3 | 1.03E-04 | 1.26 | CCF OF INPUT LOGIC GROUPS (CCX -PL#MOD3, -INPUT-LOGIC) |
| CCX-PL903 | 9.69E-05 | 1.26 | CCF OF THE LOGIC GROUP PROCESSING (CCX-###03) |
| CCX-PL3MOD5 | 6.98E-05 | 1.26 | CCF OF MODULATING GROUPS - OUTPUT LOGIC I/Os (CCX-PL#MOD5) |
| CCX-PL2MOD5 | 6.98E-05 | 1.26 | CCF OF MODULATING GROUPS - OUTPUT LOGIC I/Os (CCX-PL#MOD5) |
| ECX-CB-GC | 7.30E-04 | 1.25 | COMMON CAUSE FAILURE 4KV BREAKER TO CLOSE |
| ECX-CB-GO | 4.20E-04 | 1.25 | COMMON CAUSE FAILURE 4KV BREAKERS TO OPEN |
| ZOX-DG-DR | 4.40E-04 | 1.25 | COMMON CAUSE FAILURE STANDBY DG TO RUN |
| WLOAV057LA | 8.76E-03 | 1.24 | AOV VALVE V057 FAILS TO CLOSE |
| WLOAV006LA | 8.76E-03 | 1.24 | OUTSIDE CONTAIN. AOV V006 VALVE FAILS TO CLOSE |
| WLIAV055LA | 8.76E-03 | 1.24 | AOV VALVE V055 FAILS TO CLOSE |
| WLIAV004LA | 8.76E-03 | 1.24 | INSIDE CONTAINM. AOV V004 FAILS TO CLOSE |
| LPM-REC01 | 5.00E-02 | 1.23 | OPERATOR FAILS TO ACTUATE ADS AFTER CORE DAMAGE |

| BASIC EVENT ID | Probability | RAW | Description |
|---|---|---|---|
| ADN-REC01 | 5.00E-02 | 1.23 | OPERATOR FAILS TO ACTUATE ADS AFTER CORE DAMAGE |
| DUMP-MAN01 | 1.32E-03 | 1.22 | FAILURE TO CONTROL DUMP VALVES FOLLOWING A SG TUBE RUP. |
| CCX-PMAMOD2 | 3.04E-04 | 1.22 | CCF OF ACTUATION LOGIC GROUPS (CCX-P##MOD2) |
| RPTMOD08 | 8.76E-04 | 1.21 | COMPONENTS FAILURE |
| RPTMOD06 | 8.76E-04 | 1.21 | COMPONENTS FAILURE |
| RPTMOD04 | 8.76E-04 | 1.21 | COMPONENTS FAILURE |
| RPTMOD02 | 8.76E-04 | 1.21 | COMPONENTS FAILURE |
| ED1MOD03 | 2.70E-03 | 1.21 | BATTERY DB1 UNAVAILABLE |
| FSMOD255A | 5.80E-04 | 1.20 | MECHANICAL FAILURE OF AOV V255A |
| CCX-PMBMOD1 | 1.41E-04 | 1.20 | CCF OF OUTPUT LOGIC I/Os (CCX- P##MOD1) |

## Table 720.057-11 Component And Operator Action Basic Events Listed By RRW For LRF

| BASIC EVENT ID | Probability | RRW | Fussel-Vesely | Description |
|---|---|---|---|---|
| | | | | |
| CCX-XMTR | 4.78E-04 | 1.270 | 2.12E-01 | CCF OF PRESSURE TRANSMITTERS |
| CCX-XMTR195 | 4.78E-04 | 1.258 | 2.05E-01 | COMMON CAUSE FAILURE OF PZR LEVEL SENSORS |
| ATW-MAN03 | 5.20E-02 | 1.214 | 1.76E-01 | OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS |
| ATW-MAN04C | 5.26E-01 | 1.207 | 1.72E-01 | COND. PROB. OF ATW-MAN04 (OPER. FAILS TO TRIP REACTOR) |
| IWX-FL-GP | 1.20E-05 | 1.127 | 1.13E-01 | CCF OF STRAINERS IN IRWST TANK |
| CCX-PMXMOD1-SW | 1.10E-05 | 1.124 | 1.10E-01 | CCF OF PMS ESF OUTPUT LOGIC SOFTWARE |
| CCX-SFTW | 1.20E-06 | 1.120 | 1.07E-01 | CCF SOFTWARE - ALL CARDS |
| REC-MANDAS | 1.16E-02 | 1.101 | 9.16E-02 | FAILURE OF MANUAL DAS ACT. |
| CCX-EP-SAM | 8.62E-06 | 1.094 | 8.62E-02 | CCF OF EPO BOARDS IN PMS (POWER INTERFACE OUTPUT BOARD) |
| MDAS | 1.00E-02 | 1.093 | 8.48E-02 | UNAVAILABILITY GOAL FOR MANUAL DIVERSE ACTUATION SYSTEM |
| OTH-SGTR | 1.00E-02 | 1.079 | 7.31E-02 | CONSEQUENTIAL SGTR OCCURS |
| ADX-EV-SA2 | 5.90E-05 | 1.066 | 6.20E-02 | CCF OF 2 SQUIB VALVES TO OPERATE |
| REC-MANDASC | 5.06E-01 | 1.062 | 5.84E-02 | COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) |
| DAS | 1.00E-02 | 1.058 | 5.50E-02 | UNAVAILABILITY GOAL FOR DAS |
| ED3MOD07 | 3.05E-04 | 1.057 | 5.41E-02 | EDS3 EA 1 DISTR. PNL FAILURE OR T&M |
| OTH-DF | 1.70E-02 | 1.055 | 5.23E-02 | CONTAINMENT FAILURE DUE TO DIFFUSION FLAME |
| CFE-OCCURS | 1.00E-01 | 1.055 | 5.23E-02 | EARLY CONTAINMENT FAILURE OCCURS DUE TO VESSEL FAILURE |
| OTH-SLSOV1 | 2.10E-02 | 1.048 | 4.54E-02 | ANY SECOND. SIDE RELIEF VALVE FAILS TO CLOSE (2 SV + PORV) |
| ATW-MAN05 | 5.20E-03 | 1.039 | 3.72E-02 | OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS |
| ATW-MAN06C | 5.00E-01 | 1.038 | 3.63E-02 | COND. PROB. OF ATW-MAN06 (OPER. FAILS TO TRIP REACTOR VIA DAS) |
| ADX-EV-SA | 3.00E-05 | 1.034 | 3.30E-02 | CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE |
| RPX-CB-GO | 4.20E-04 | 1.034 | 3.28E-02 | CCF TO OPEN OF 4.16 KVAC CIRCUIT BREAKERS |
| IWX-MV-GO | 4.40E-03 | 1.034 | 3.25E-02 | CCF OF RECIRC MOVs TO OPEN |
| IWA-PLUG | 2.40E-04 | 1.027 | 2.63E-02 | IWRST DISCHARGE LINE "A" STRAINER PLUGGED |
| IWX-XMTR | 4.78E-04 | 1.027 | 2.60E-02 | CCF OF IRWST LEVEL TRANSMITTERS |
| REN-MAN03 | 3.40E-03 | 1.026 | 2.52E-02 | FAILURE TO OPEN RECIRC MOVs |
| OTH-R05 | 7.00E-01 | 1.025 | 2.46E-02 | FAILURE TO RECOVER OFFSITE AC POWER IN 30 MINUTES |
| REN-MAN04 | 1.00E-02 | 1.023 | 2.27E-02 | OPER. FAILS TO ACT. SUMP RECIRC GIVEN IRW LEVEL SIGNAL FAILURE |
| CIX-AV-LA | 7.70E-04 | 1.022 | 2.15E-02 | COMMON CAUSE FAILURE OF ALL CI AOVS TO CLOSE |

| BASIC EVENT ID | Probability | RRW | Fussel-Vesely | Description |
|---|---|---|---|---|
| | | | | |
| CCX-BY-PN | 4.70E-05 | 1.021 | 2.09E-02 | COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B |
| CANCV015GC | 2.45E-02 | 1.021 | 2.04E-02 | INSIDE CONTAIN. CV V015 FAILS TO CLOSE |
| ADX-MV3-GO | 3.24E-04 | 1.021 | 2.01E-02 | CCF OF 4 COMBINATIONS OF 3 STAGES #2 AND #3 MOVS |
| CCX-INPUT-LOGIC | 1.03E-04 | 1.020 | 2.01E-02 | CCF OF ESF INPUT LOGIC (HARDWARE) |
| PDS6-MANADS | 1.00E-01 | 1.020 | 1.98E-02 | OPERATOR FAILS TO ACTUATE ADS AFTER CORE DAMAGE |
| CIB-MAN00 | 1.84E-03 | 1.019 | 1.85E-02 | COGNITIVE OPERATOR ERROR |
| RN11MOD3 | 1.41E-02 | 1.019 | 1.85E-02 | HARDWARE FAILURE OF ISOLATION MOV 011 |
| RN22MOD4 | 1.41E-02 | 1.019 | 1.85E-02 | HARDWARE FAILS TO OPEN MOV V022 / CB FTC / RELAY FTC |
| RN23MOD5 | 1.41E-02 | 1.019 | 1.85E-02 | HARDWARE FAILS TO OPEN MOV V023 / CB FTC / RELAY FTC |
| RN55MOD1 | 1.41E-02 | 1.019 | 1.85E-02 | MECHANICAL FAILURE OF RNS MOV V055 |
| EC1BS001TM | 2.70E-03 | 1.018 | 1.76E-02 | UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDUL MAINTENANCE |
| OTH-SLSOV | 1.10E-02 | 1.017 | 1.70E-02 | ANY SECOND. SIDE RELIEF VALVE FAILS TO RECLOSE (1 SV + PORV) |
| EC1BS012TM | 2.70E-03 | 1.016 | 1.61E-02 | BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE |
| CMA-PLUG | 7.27E-04 | 1.015 | 1.51E-02 | FLOW TUNING ORIFICE PLUGS |
| CCX-XMTR1 | 4.78E-04 | 1.014 | 1.33E-02 | CCF OF PRESSURE TRANSMITTERS FOLLOWING ACCIDENT (CCX-XMTR1) |
| CLP-UNAVAILABLE | 1.00E-02 | 1.013 | 1.30E-02 | CASK LOADING PIT UNAVAILABLE DUE TO FUEL UNLOADING OPERATIONS |
| LPM-REC01 | 5.00E-02 | 1.012 | 1.21E-02 | OPERATOR FAILS TO ACTUATE ADS AFTER CORE DAMAGE |
| ADN-REC01 | 5.00E-02 | 1.012 | 1.21E-02 | OPERATOR FAILS TO ACTUATE ADS AFTER CORE DAMAGE |
| ADN-MAN01 | 3.02E-03 | 1.012 | 1.20E-02 | OPERATOR FAILS TO FULFIL MANUAL ACTUATION OF ADS |
| ADN-MAN01C | 5.00E-01 | 1.012 | 1.18E-02 | COND. PROB. OF ADN-MAN01(OPER. FAILS TO ACT. ADS) |
| CCX-TRNSM | 4.78E-04 | 1.012 | 1.14E-02 | CCF NON-SAFETY TRANSMITTERS INTERFACING SYSTEM PRESSURE |
| CIC-MAN01 | 1.20E-03 | 1.010 | 9.94E-03 | OPERATOR FAILS TO RECOGNIZE NEED AND FAILS TO ISOLATE CMT GIVEN CORE DAMAGE AFTER A LOCA |
| CCX-AV-LA | 6.20E-05 | 1.009 | 9.21E-03 | COMMON CAUSE FAILURE OF 4 AOVS TO OPEN |
| LPM-MAN01C | 5.00E-01 | 1.009 | 8.64E-03 | OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING SLOCA |
| CMX-VS-FA | 3.84E-05 | 1.009 | 8.50E-03 | CCF OF CMT LEVEL SWITCHES |
| ADF-MAN01 | 5.00E-01 | 1.008 | 8.08E-03 | OPERATOR FAILS TO FULFIL MANUAL ACTUATION OF ADS |
| CIB-MAN01 | 1.34E-03 | 1.008 | 7.86E-03 | OPERATOR ERROR TO CLOSE VALVES ON RUPTURED SG |
| IDBBSDS1TM | 3.00E-04 | 1.007 | 6.68E-03 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| IDBBSDD1TM | 3.00E-04 | 1.007 | 6.68E-03 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| CMX-CV-GO | 5.10E-05 | 1.007 | 6.55E-03 | COMMON CAUSE FAILURE OF 4 CHECK VALVES TO OPEN |
| IWX-CV-AO | 3.00E-05 | 1.007 | 6.47E-03 | CCF OF 4 GRAVITY INJECTION CVs |

| BASIC EVENT ID | Probability | RRW | Fussel-Vesely | Description |
|---|---|---|---|---|
| PXX-AV-LA | 9.60E-05 | 1.006 | 6.36E-03 | FAILURE OF PRHR DUE TO COMMON CAUSE OF AOVs |
| PXX-AV-LA1 | 9.60E-05 | 1.006 | 6.36E-03 | FAILURE OF IRWST GUTTER DUE TO COMMON CAUSE OF AOVs |
| RNX-KV1-GO | 4.90E-03 | 1.006 | 6.32E-03 | CCF OF STOP CHECK VALVES V015A/B TO OPEN |
| CANAV014LA | 8.76E-03 | 1.006 | 5.92E-03 | AOV V014 FAILS TO CLOSE |
| IWX-EV-SA | 2.60E-05 | 1.006 | 5.76E-03 | CCF OF 4 GRAVITY INJECTION & 2 RECIRCULATION SQUIB VALVES |
| LPM-MAN01 | 1.34E-03 | 1.006 | 5.66E-03 | OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING SLOCA |
| EC0MOD01 | 5.08E-03 | 1.006 | 5.65E-03 | MAIN GEN. BKR ES 01 FAILS TO OPEN [# 12] |
| REC-MANDAS1 | 1.00E+00 | 1.005 | 5.37E-03 | COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) |
| CVN-MAN00 | 3.10E-03 | 1.005 | 4.88E-03 | FAILURE TO ALIGN CVCS IN AUX. SPRAY MODE |
| OTH-PRSOV | 1.00E-02 | 1.005 | 4.79E-03 | EITHER PRZR SV FAILS TO RECLOSE |
| IDDBSDS1TM | 3.00E-04 | 1.004 | 4.46E-03 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| IDDBSDD1TM | 3.00E-04 | 1.004 | 4.46E-03 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| CANTP011RI | 5.23E-03 | 1.004 | 4.10E-03 | FAILURE OF AIR COMPRESSOR TRANSMITTER |
| SGBAV040LA | 1.09E-03 | 1.004 | 3.83E-03 | AOV MSIV V040B FAILS TO CLOSE |
| RHN-MAN01 | 2.90E-03 | 1.004 | 3.71E-03 | OPERATOR FAILS TO ALIGN AND ACTUATE THE RNS |
| ZO1DG001TM | 4.60E-02 | 1.004 | 3.55E-03 | STANDBY DG UNAVAILABLE DUE TO TEST AND MAINTENANCE |
| EC2BS002TM | 2.70E-03 | 1.004 | 3.53E-03 | UNAVAILABILITY OF BUS ECS ES 2 DUE TO UNSCHEDUL MAINTENANCE |
| EC1BS122TM | 2.70E-03 | 1.003 | 3.46E-03 | BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE |
| RNBMOD10 | 5.07E-02 | 1.003 | 3.26E-03 | HARDWARE FAILURE OF VALVES ON DVI LINE B (V 015B & 017B) |
| RNAMOD09 | 5.07E-02 | 1.003 | 3.26E-03 | HARDWARE FAILURE OF VALVES ON DVI LINE A (V 015A & 017A) |
| EC2BS022TM | 2.70E-03 | 1.003 | 3.19E-03 | BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE |
| OTH-SLSOV2 | 1.00E-02 | 1.003 | 3.09E-03 | ANY SECOND. SIDE RELIEF VALVE FAILS TO CLOSE (1 SV) |
| EC2BS221TM | 2.70E-03 | 1.003 | 2.90E-03 | BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE |
| OTH-SLSOV3 | 5.40E-03 | 1.003 | 2.82E-03 | FAILURE TO RECLOSE OF SG PORV & 1 SG SV ON RUPTURED SG |
| LPM-MAN02 | 3.30E-03 | 1.002 | 2.25E-03 | OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA |
| RNNCV013GO | 1.75E-03 | 1.002 | 2.22E-03 | CHECK VALVE V013 FAILURE TO OPEN |
| RC1CB051GO | 4.20E-03 | 1.002 | 2.14E-03 | PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN |
| RC1CB053GO | 4.20E-03 | 1.002 | 2.14E-03 | PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN |
| RC1CB061GO | 4.20E-03 | 1.002 | 2.14E-03 | PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN |
| RC1CB063GO | 4.20E-03 | 1.002 | 2.14E-03 | PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN |
| REG-MAN00 | 2.04E-01 | 1.002 | 2.12E-03 | MANUALLY REGULATE FLOW TO SG "A" |
| WLOAV057LA | 8.76E-03 | 1.002 | 2.10E-03 | AOV VALVE V057 FAILS TO CLOSE |

| BASIC EVENT ID | Probability | RRW | Fussel-Vesely | Description |
|---|---|---|---|---|
| | | | | |
| WLOAV006LA | 8.76E-03 | 1.002 | 2.10E-03 | OUTSIDE CONTAIN. AOV V006 VALVE FAILS TO CLOSE |
| WLIAV055LA | 8.76E-03 | 1.002 | 2.10E-03 | AOV VALVE V055 FAILS TO CLOSE |
| WLIAV004LA | 8.76E-03 | 1.002 | 2.10E-03 | INSIDE CONTAINM. AOV V004 FAILS TO CLOSE |
| OTH-SGTR1 | 6.70E-03 | 1.002 | 2.02E-03 | SINGLE CONSEQUENTIAL SGTR |
| REX-FL-GP | 1.20E-05 | 1.002 | 1.99E-03 | CCF PLUGGING OF BOTH RECIRC LINES DUE TO SUMP SCREENS |
| CMX-AV-LA | 9.60E-05 | 1.002 | 1.99E-03 | COMMON CAUSE FAILURE (DELTA) FOR 2 AOVS TO OPEN |
| CCX-IN-LOGIC-SW | 1.10E-05 | 1.002 | 1.89E-03 | CCF OF ESF INPUT LOGIC SOFTWARE |
| CCX-PMXMOD2-SW | 1.10E-05 | 1.002 | 1.89E-03 | CCF OF PMS ESF ACTUATION LOGIC SOFTWARE |
| SWN-MAN03 | 4.00E-02 | 1.002 | 1.84E-03 | FAILURE OF OPERATOR TO REFILL BASIN |
| EC1BS121TM | 2.70E-03 | 1.002 | 1.77E-03 | BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE |
| PDS6-MANADS | 9.00E-01 | 1.002 | 1.70E-03 | OPERATOR FAILS TO ACTUATE ADS AFTER CORE DAMAGE |
| IDABSDS1TM | 3.00E-04 | 1.002 | 1.65E-03 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| RNAMOD06 | 3.40E-02 | 1.002 | 1.65E-03 | PUMP 01A FAILS & ST CK V007A &C B FTC & RE FTC & CB ECS131 SPO |
| IDABSDD1TM | 3.00E-04 | 1.002 | 1.65E-03 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| ACACV029GO | 1.75E-03 | 1.002 | 1.65E-03 | CHECK VALVE 029A FAILS TO OPEN |
| ACACV028GO | 1.75E-03 | 1.002 | 1.65E-03 | CHECK VALVE 028A FAILS TO OPEN |
| SUC-RFL | 7.33E-01 | 1.002 | 1.63E-03 | SUCCESSFUL REFLODING OF A DEGRADED CORE |
| RNBMOD07 | 3.40E-02 | 1.002 | 1.56E-03 | PUMP 01B FAILS & ST CK V007B & C B FTC & RE FTC & CB ECS231 SPO |
| IDCBSDS1TM | 3.00E-04 | 1.002 | 1.50E-03 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| IDCBSDD1TM | 3.00E-04 | 1.002 | 1.50E-03 | BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE |
| CVMOD07 | 2.71E-02 | 1.001 | 1.47E-03 | MECHANICAL FAILURE OF AOV V081 FAILS TO CLOSE |
| CVMOD05 | 2.88E-02 | 1.001 | 1.36E-03 | MECHANICAL FAILURE OF AOV V084 AND CV V085 TO OPEN |
| CCX-PMXMOD4-SW | 1.10E-05 | 1.001 | 1.35E-03 | CCF OF SOFTWARE - MUX LOGIC GROUPS (CCX-P##MOD4-SW) |
| ZO1MOD01 | 2.02E-02 | 1.001 | 1.33E-03 | D/G FAILS TO START & RUN OR BKR 102 FAILS TO CLOSE |
| RC1CB054GO | 4.20E-03 | 1.001 | 1.30E-03 | PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN |
| RC1CB052GO | 4.20E-03 | 1.001 | 1.30E-03 | PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN |
| CCX-TT-UF | 1.17E-04 | 1.001 | 1.29E-03 | CCF OF TEMPERATURE TRANSMITTERS (CCX-TT-UF) |
| RC1CB064GO | 4.20E-03 | 1.001 | 1.26E-03 | PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN |
| RC1CB062GO | 4.20E-03 | 1.001 | 1.26E-03 | PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN |
| OTH-DTE | 2.45E-01 | 1.001 | 1.19E-03 | EARLY HYDROGEN DETONATION OCCURS |
| ZO2DG002TM | 4.60E-02 | 1.001 | 1.18E-03 | STANDBY DG UNAVAILABLE DUE TO TEST AND MAINTENANCE |
| IWACV124AO | 1.75E-03 | 1.001 | 9.52E-04 | CHECK VALVE 124A FAILS TO OPEN |

| BASIC EVENT ID | Probability | RRW | Fussel-Vesely | Description |
|---|---|---|---|---|
| | | | | |
| ACBCV028GO | 1.75E-03 | 1.001 | 9.48E-04 | CHECK VALVE 028B FAILS TO OPEN |
| ACBCV029GO | 1.75E-03 | 1.001 | 9.48E-04 | CHECK VALVE 029B FAILS TO OPEN |
| RNX-PM-FS | 7.70E-04 | 1.001 | 9.48E-04 | CCF OF PUMPS TO START |
| IWACV122AO | 1.75E-03 | 1.001 | 9.09E-04 | CHECK VALVE 122A FAILS TO OPEN |
| OTH-DTE-3D | 1.15E-01 | 1.001 | 8.39E-04 | EARLY HYDROGEN DETONATION OCCURS - AFTER PDS 3D |
| OTH-MGSET | 1.75E-03 | 1.001 | 8.30E-04 | CONTROL ROD MG SETS FAIL TO TRIP |
| IRWMOD06 | 1.46E-03 | 1.001 | 7.94E-04 | HARDWARE FAILURE OF VALVE 125A |
| ADX-MV-GO | 7.48E-04 | 1.001 | 7.89E-04 | 3/4 STAGE 2 & 3 LINES FAIL DUE TO CCF OF MOVs TO OPEN |
| IRWMOD05 | 1.46E-03 | 1.001 | 7.58E-04 | HARDWARE FAILURE OF VALVE 123A |
| RNX-KV-GO | 6.10E-04 | 1.001 | 7.51E-04 | CCF OF STOP CHECK VALVES V007A/B TO OPEN |
| VWBMOD05 | 2.19E-02 | 1.001 | 7.48E-04 | CHILLER MS 03 SEGMENT HARDWARE FAILURE OR MAINTENANCE |
| VLX-HI-SA | 3.20E-04 | 1.001 | 7.17E-04 | CCF OF THE HYDROGEN IGNITERS |
| CDNTF01BRI | 5.23E-03 | 1.001 | 7.08E-04 | FLOW TRANSMITTER FAILURE (###TF###RI) |
| EDSMOD01 | 3.05E-04 | 1.001 | 6.83E-04 | FAILURE OF THE 12 VAC DISTRBN PANEL |
| ACAOR001SP | 7.27E-04 | 1.001 | 6.79E-04 | FLOW TUNING ORIFICE PLUGS |
| CCX-PMS-HARDWARE | 7.89E-05 | 1.001 | 6.52E-04 | PMS REACTOR TRIP SYSTEM HARDWARE CCF |
| IWX-EV1-SA | 5.80E-06 | 1.001 | 6.32E-04 | CCF OF 2 GRAVITY INJECTION SQUIB VALVES IN 1/1 LINES TO OPEN |
| AD4MOD08 | 5.80E-04 | 1.001 | 6.23E-04 | HARDWARE FAILURE OF ST. #4 LINE 2 |
| AD4MOD09 | 5.80E-04 | 1.001 | 6.23E-04 | HARDWARE FAILURE OF ST. #4 LINE 3 |
| AD4MOD10 | 5.80E-04 | 1.001 | 6.23E-04 | HARDWARE FAILURE OF ST. #4 LINE 4 |
| AD4MOD07 | 5.80E-04 | 1.001 | 6.23E-04 | HARDWARE FAILURE OF ST. #4 LINE 1 |
| VWBMOD04 | 1.83E-02 | 1.001 | 6.23E-04 | CHILLER PUMP MP 03 SEGMENT HARDWARE FAILURE OR MAINTENANCE |
| OTH-DTE-2R | 1.90E-01 | 1.001 | 6.16E-04 | EARLY HYDROGEN DETONATION OCCURS - AFTER PDS 2R |
| REA-PLUG | 2.40E-04 | 1.001 | 5.78E-04 | SUMP SCREEN A PLUGS AND PREVENTS FLOW |
| CVMOD04 | 7.37E-04 | 1.001 | 5.74E-04 | DISCHARGE LINE FAILURE |
| ED1MOD03 | 2.70E-03 | 1.001 | 5.58E-04 | BATTERY DB1 UNAVAILABLE |
| ZOX-PD-ES | 2.00E-03 | 1.001 | 5.37E-04 | CCF TO START OF ENGINE-DRIVEN FUEL PUMPS |
| ED1MOD11 | 3.17E-04 | 1.001 | 5.34E-04 | FIXED COMPONENTS FAILURE |
| ED1MOD113 | 3.17E-04 | 1.001 | 5.34E-04 | FIXED COMPONENTS FAILURE |
| IWX-EV4-SA | 5.80E-05 | 1.001 | 5.24E-04 | CCF OF 2 OUT 2 LOW PRESSURE RECIRCULATION SQUIB VALVES |
| OTH-CNB | 1.00E-03 | 1.001 | 5.23E-04 | CONTAINMENT ISOL FAILURE DUE TO RV RUPTURE |
| ED1BSDS1TM | 3.00E-04 | 1.001 | 5.15E-04 | BUS EDS1 DS 1 UNAVAILABLE DUE TO CORRECTIVE MAINTENANCE |

| BASIC EVENT ID | Probability | RRW | Fussel-Vesely | Description |
|---|---|---|---|---|
| | | | | |
| RPTMOD01 | 8.76E-04 | 1.001 | 5.14E-04 | COMPONENTS FAILURE |
| RPTMOD05 | 8.76E-04 | 1.001 | 5.14E-04 | COMPONENTS FAILURE |
| RPTMOD07 | 8.76E-04 | 1.001 | 5.14E-04 | COMPONENTS FAILURE |
| RPTMOD03 | 8.76E-04 | 1.001 | 5.14E-04 | COMPONENTS FAILURE |
| AD2MOD02 | 5.64E-02 | 1.001 | 5.00E-04 | HARDWARE FAILURE OF ST. #2 LINE 2 |
| AD3MOD04 | 5.64E-02 | 1.001 | 5.00E-04 | HARDWARE FAILURE OF ST. #3 LINE 2 |
| AD3MOD03 | 5.64E-02 | 1.001 | 5.00E-04 | HARDWARE FAILURE OF ST. #3 LINE 1 |
| AD2MOD01 | 5.64E-02 | 1.001 | 5.00E-04 | HARDWARE FAILURE OF ST. #2 LINE 1 |
| EC1BS013TM | 2.70E-03 | 1.000 | 4.92E-04 | BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE |

# AP1000 DESIGN CERTIFICATION REVIEW

## Response to Request For Additional Information

RAI Number: 720.070

***Question:***

An assessment of shutdown risk, considering fires, internal floods, and seismic events has not been submitted. Please provide a shutdown assessment of these initiators considering (a) containment may be open, (b) fire/flood barriers may be breached for maintenance, and (c) transient combustibles for a given fire areas may be increased to support maintenance.

**Westinghouse Response:**

Included in the AP1000 PRA is an evaluation of the risk from internal initiating events that can occur during shutdown modes. The results of the AP1000 assessment show that the core damage frequency (CDF) from internal events at shutdown is found to be approximately 1.23E-07/year, which is equivalent to the AP600 CDF calculated for internal initiating events for shutdown modes. The AP1000 design features important to reducing shutdown risk are the same as the equivalent design features provided for in the AP600, and these design features are discussed in DCD Chapter 19 Appendix E.

It is useful to review a summary of the overall AP600 and AP1000 plant risk evaluations to further assess this RAI. The attached table summarizes the various AP600 and AP1000 plant risk evaluations that have been performed. Reviewing these results shows that the overall risk profile for the AP600 and AP1000 is very low, and is at least two to three orders of magnitude below the NRC safety goal for nuclear power plants. The calculated CDF and LRF for both plants is very low, and their similarities can be attributed to the similarities in the plant designs, system performance, and low dependence on operator actions derived from the robustness of the passive safety systems.

The RAI requests additional shutdown risk evaluations be performed for the AP1000. In the AP600 PRA, additional shutdown risk evaluations were performed including evaluations of fire, internal flooding, and seismic events including the issues raised above in items a, b, c. The results of these assessments further demonstrated that the risk from shutdown fires, floods and seismic events for the AP600 passive plant are very low, and have a negligible contribution to overall plant risk. Based on the similarities of the plant designs as well as the similarities in the calculated CDF and LRF for both plants from at-power initiating events, as well as shutdown initiating events, Westinghouse does not believe that additional shutdown assessments should be required for the AP1000. Westinghouse believes that the insights gained from these additional shutdown risk evaluations performed for the AP600 can be applied to the AP1000 as well.

| Scope | AP600 | AP1000 |
|---|---|---|
| At-Power Internal Initiating Events | Quantification Performed<br>CDF = 1.7E-07<br><br>LRF = 1.8E-08<br>Containment Effectiveness = 89.5% | Quantification Performed<br>CDF = 2.4E-07<br><br>LRF = 2.0E-08<br>Containment Effectiveness = 91.8% |
| | | |
| Internal Fire Events (At-Power and Shutdown) | Conservative (via focused PRA) Quantification Performed<br><br>CDF = 6.5E-07 (internal)<br>CDF = 3.5E-07 (shutdown) | Quantification Performed<br><br>CDF = 5.61 E-08 (internal) |
| Internal Flooding Events (At-Power) | Quantification Performed<br>CDF = 2.2E-10 | Quantification Performed<br>CDF = 8.8E-10 |
| Shutdown Internal Events | Quantification Performed<br><br>CDF = 1.0E-07<br>LRF = 1.5 E-08 | Quantitative Evaluation Performed for CDF only<br><br>CDF = 1.2E-07 |

**Design Control Document (DCD) Revision:**

None

**PRA Revision:**

None

# AP1000 DESIGN CERTIFICATION REVIEW

## Response to Request For Additional Information

RAI Number: 720.080

***Question:***

Gamma and Beta Doses in Figures D-1 and D-2 of the AP1000 PRA are less than the corresponding figures for the AP600. Considering the power rating has gone up, one would expect these doses to increase not decrease. Why is this less?

**Westinghouse Response:**

Relative to the AP600, the increase in the power rating would tend to result in higher doses for the AP1000 with all other parameters of equal values. A compensating design feature of the AP1000 is the larger containment volume.

The primary difference, though, is attributable to the total core inventory released and the timing of these releases. Both the AP600 and AP1000 calculations are based on NUREG-1465. For the AP600, additional considerations were made as defined by SECY-94-300 (December 1995). For the AP1000, the guidance provided in Regulatory Guide 1.183 (July 2000) was utilized. Tables 1 and 2, illustrate the releases as a function of time for the AP600 and the AP1000, respectively.

**Table 1 – AP600**
**Core Inventory Fraction Released into Containment versus Time Period**

| | 0-10 Minutes | 10 Minutes | 10-40 Minutes | 40-118 Minutes | 118-238 Minutes | 238-718 Minutes | Total |
|---|---|---|---|---|---|---|---|
| Noble Gases | 0.00 | 0.03 | 0.02 | 0.95 | 0.00 | 0.00 | 1.00 |
| Halogens | 0.00 | 0.03 | 0.02 | 0.35 | 0.25 | 0.10 | 0.75 |
| Alkali Metals | 0.00 | 0.03 | 0.02 | 0.25 | 0.35 | 0.10 | 0.75 |
| Tellurium Metals | 0.00 | 0.00 | 0.00 | 0.05 | 0.25 | 0.005 | 0.305 |
| Ba, Sr | 0.00 | 0.00 | 0.00 | 0.02 | 0.10 | 0.00 | 0.12 |
| Noble Metals | 0.00 | 0.00 | 0.00 | 0.0025 | 0.0025 | 0.00 | 0.005 |
| Lanthanides | 0.00 | 0.00 | 0.00 | 0.0002 | 0.005 | 0.00 | 0.0052 |
| Cerium Group | 0.00 | 0.00 | 0.00 | 0.0005 | 0.005 | 0.00 | 0.0055 |

| Table 2 – AP1000 Core Inventory Fraction Released into Containment versus Time Period | | | | |
|---|---|---|---|---|
| | 0-10 Minutes | 10-40 Minutes | 40-118 Minutes | Total |
| Noble Gases | 0.00 | 0.05 | 0.95 | 1.0 |
| Halogens | 0.00 | 0.05 | 0.35 | 0.4 |
| Alkali Metals | 0.00 | 0.05 | 0.25 | 0.3 |
| Tellurium Metals | 0.00 | 0.00 | 0.05 | 0.05 |
| Ba, Sr | 0.00 | 0.00 | 0.02 | 0.02 |
| Noble Metals | 0.00 | 0.00 | 0.0025 | 0.0025 |
| Lanthanides | 0.00 | 0.00 | 0.0002 | 0.0002 |
| Cerium Group | 0.00 | 0.00 | 0.0005 | 0.0005 |

Table 1 shows that an initial, instantaneous, release of a set of nuclides was simulated for the AP600 at 10 minutes. All other releases are made over a time-span. At 40 and 118 minutes, both the AP600 and the AP1000 have equivalent cumulative releases. The higher dose rate values for the AP1000 up to 118 minutes reflect the higher power rating and containment volume. After 118 minutes, no more releases are simulated for the AP1000, while they continue for the AP600. The cumulative release for all nuclides of the AP600 are larger than the AP1000 (except for the "Noble Gasses" which are equal). The higher doses for the AP600 (after approximately 3 hours) are attributable to the higher total releases.

**Design Control Document (DCD) Revision:**

None

**PRA Revision:**

None

# AP1000 DESIGN CERTIFICATION REVIEW

## Response to Request For Additional Information

RAI Number: 720.085

***Question:***

The AP600 in-vessel steam explosion analysis neglects the possibility of initially small FCIs (with little energetic potential) being a driver for larger melt crucible failures that would increase the melt pour rate. How were these events considered or bounded for the RPV survival in-vessel? Please elaborate.

**Westinghouse Response:**

The response to this question is based on the following key factors:

a) The reactor vessel lower internals assembly, which includes the core barrel and core support plate, are at the time of interest, still integral and structurally strong. These constitute the outer envelope of the crucible that contains the melt. Only the uppermost area has melted, but we are interested in the lower part. Also, the lower support structure is integral and structurally strong.

b) The downcomer cross sectional area is nearly 4 $m^2$ and allows relatively free venting up and through the cold legs. This would prevent pressurization during premixing. Also in the event of any significant interaction, with sustained pressures capable to set the lower boundary of the crucible (the crusts), or the crucible as a whole, in motion, this vent area would allow large quantities of lower plenum water to be dispersed, together with venting steam, upwards. Note, in this respect, that only a fraction (-30%) of the core support plate area is open (the flow holes), and also, the inertia mass of the whole lower internals assembly (containing the melt), is at least one order of magnitude greater than any lower plenum water mass coupled in the interaction. This means any pressure developed in between these two masses would tend to expel the water rather than move the core.

c) To fail the lower boundary of the crucible (the crusts), pressure must be applied from below that is high enough and sustained enough to cause motion. This can only be done by forcing water on to this boundary, and this can arise only from a sustained strong interaction in the lower plenum. But an immediate consequence of this is also that another melt-water interaction boundary is formed, at the failing lower boundary of the crucible. This would tend to be self-limiting, as the developing pressure creates a local expansion zone, that again venting downwards, expelling lower plenum water, in a manner that precedes the downward relocation of the melt that would eventually occur. Note that this interaction zone would also contain melt, which would be expelled downwards as well, sustaining the removal of lower plenum water.

d) Throughout all these interactions the structures mentioned under (a) would effectively maintain the retentive property of the crucible, while the core support plate and the internal support structures would effectively prevent a fall-back, gross, contact mechanism. Rather, the fallback would be arrested, and any melt relocation has to occur by gravity, through the holes on the core support plate.

e) By that time hardly any water would have been left in the lower plenum to receive the melt for an explosive interaction. No mechanism that would violate lower head integrity is seen.

**Design Control Document (DCD) Revision:**

None

**PRA Revision:**

None

# AP1000 DESIGN CERTIFICATION REVIEW

## Response to Request For Additional Information

RAI Number: 720.086

***Question:***

The initial AP600 in-vessel steam explosion analysis for the premixing phase of the FCI was limited to times shorter than 1 second, and the triggering time was much shorter than 1 second. The fuel-coolant mixture will naturally attain an optimum set of conditions that would then cause an optimal set of energetics. Please address the ways in which this has been accounted for in the AP1000.

**Westinghouse Response:**

The AP600 In-Vessel Explosion (IVE) assessment (DOE/ID-10541) indicated that voiding so significantly "dampened" the premixtures that it was not possible to trigger energetic explosions even with microinteractions. This voiding increased (in saturated water) with time as the quantity of melt in the pool increased, so that an "optimal" was found to occur at some early time, less than 1 second. Since the key condition (lower plenum water saturation) in the AP1000 is the same as for AP600, the previous IVE results are directly applicable. Please also note that the localized pour at a few hundreds of kg/s is also applicable here.

Work carried out since that time by the authors of DOE/ID-10541 has not lead to any reasons to change the above conclusion.

**Design Control Document (DCD) Revision:**

None

**PRA Revision:**

None

# AP1000 DESIGN CERTIFICATION REVIEW

## Response to Request For Additional Information

RAI Number: 720.097

***Question:***

(Related to AP1000 RAI 720.024) In the AP1000 PRA, Table 6-1, there are 2 bases designated as "M" and "P" for success criteria which are not defined. Please, provide the missing definitions. Also, there are multiple success criteria basis provided for some of the event cases. Please, provide the logic behind, and the decision making process for using a multiple criteria basis.

**Westinghouse Response:**

Table 6-1 has been updated to provide the reference to the analysis or justification that is the basis for declaring the event to be a success for AP1000.

**Design Control Document (DCD) Revision:**

None

**PRA Revision:**

The revised section 6.4 and table 6-1 will be included in the next revision of the AP1000 PRA (see RAI 720.023).