

CHAPTER 19

PROBABILISTIC RISK ASSESSMENT

19.1 Introduction

Part 52 of the 10 Code of Federal Regulations requires that a probabilistic risk assessment (PRA) be submitted as a part of an application for design certification. The PRA provides an evaluation of the design, including plant, containment, and typical site analyses that consider both internal and external events.

The AP600 design process included a risk assessment of the design prior to being finalized to optimize the plant with respect to safety. Westinghouse accomplished this by committing to the early application of probabilistic analysis techniques in the AP600 design process. This work resulted in information used in the selection of design alternatives, with a goal that the overall level of safety of the completed design exceed design objectives.

19.1.1 Background and Overview

The Westinghouse AP600 PRA program was completed in three phases. Phase 1 involved the development of a scoping study based on the AP600 conceptual design. It resulted in a preliminary but mostly complete set of PRA models that provided bounding or conservative estimates of plant risk. These models were used to develop insights that contributed to the plant design process. Through the interactions between the PRA analysts and the AP600 design engineers, the Phase 1 effort resulted in:

- Identification of core damage sequences for detailed analysis and understanding of plant response
- Better understanding of the contribution of various design features to the prevention and mitigation of severe accidents
- Important design changes and more stringent requirements for some components

Phase 2 of the PRA focused on enhancing the existing models to better reflect the plant design, which had evolved since Phase 1 was begun, and on confirming the continuing validity of assumptions made during Phase 1. In addition, the key assumptions and ground rules specified in the Advanced Light Water Reactor Utility Requirements Document (ALWR URD) (Reference 19.1-1) were incorporated in the Phase 2 study.

Phase 3 included design changes since Phase 2 and additional design information. Examples of the information added during Phase 3 include the following:

- Sections to address the probabilistic evaluations under Regulatory Treatment of Nonsafety Systems (RTNSS)

- Results and insights from a substantial success criteria analysis that included extensive thermal/hydraulic computer code modeling
- Revised definitions and plant response models for loss-of-coolant accidents (LOCAs) to incorporate insights gained from the additional success criteria thermal/hydraulic analysis
- Information and, in some cases, revised models, in response to requests for additional information (RAIs) received from the NRC.

Because Phase 3 was conducted over an extended period of time, the final PRA updates address many of the questions raised by the NRC during the reviews of prior updates. There was close coordination and interaction between the AP600 designers and the PRA analysts, and review of the PRA submittal documents by Westinghouse management.

19.1.2 Objectives

The objectives of the AP600 PRA are to:

- Provide an integrated view of the AP600 behavior in response to transients and accidents, including severe accidents
- Satisfy the NRC regulatory requirements that a design-specific PRA be conducted as part of the application for design certification (10 CFR 52.47(a)(i)(v))
- Demonstrate that the design meets the proposed safety goals for core damage frequency and large fission product releases
- Construct a PRA Level 1 (core damage frequency), Level 2 (large release frequency), and Level 3 (offsite dose) model that is consistent with the AP600 design configuration and operation requirements and the ALWR URD requirements on PRA methodology (Reference 19.1-1)
- Demonstrate that the AP600 nonsafety-related systems are not required to meet the NRC safety goals.
- Demonstrate the low vulnerability and insensitivity of the AP600 design to human interaction
- Provide input to the design process (that is, provide a tool to investigate detailed design solutions and operational strategies to optimize AP600 safety)
- Demonstrate compliance with the hydrogen control criteria set forth in 10 CFR 50.34(f)(2)(ix)
- Serve as a basis for an accident management program

19.1.3 Technical Scope

The technical tasks for the AP600 PRA are defined in the following categories:

- Level 1 Analysis for Internal Events
- Level 2 Analysis for Internal Events
- Level 3 Analysis for Internal Events
- Sensitivity, Importance, and Uncertainty Analyses for Internal Events
- Shutdown Analysis
- External Events Analysis
- Sensitivity study to support Regulatory Treatment of Nonsafety Systems resolution

The ALWR URD document serves as the base document to define the source of data.

The Level 1 analysis includes:

- Internal initiating events evaluation
- Event tree and success criteria analyses
- Plant systems analysis using fault tree models
- Common cause failure and human reliability analyses
- Data analysis
- Fault tree and event tree quantification to calculate the core damage frequency

The Level 2 analysis includes:

- An evaluation of severe accident phenomena and fission product source terms
- Modeling of the containment event tree and associated success criteria
- Analysis of hydrogen burning and mixing

The Level 3 analysis is an offsite dose evaluation.

The low power and shutdown analysis includes:

- Level 1 shutdown assessment
- Level 2 shutdown assessment

External events analyses include:

- Internal fire analysis
- Internal flooding analysis
- Seismic margin analysis

19.1.4 Project Methodology Overview

Guidelines have been developed for the major tasks. These guidelines provide homogeneity among similar tasks that are performed by different analysts (such as fault tree construction) and to standardize the methodology for selected tasks (such as human reliability or common cause failure analysis).

The major activities performed during this study include:

- Initiating event and event tree analysis - Evaluations are performed to identify a comprehensive set of initiating events. This evaluation includes review of pressurized water reactor (PWR) operating experience, past PRAs, and consideration of AP600-specific features. For each initiating event category, an event tree is constructed to model the accident sequences that may result.
- Success criteria - Extensive analyses are performed with MAAP4 (Reference 19.1-2), NOTRUMP, and other codes to determine the success criteria for system mitigation following initiating events.
- Analysis of individual systems - Qualitative analysis and fault tree construction are performed for safety-related and nonsafety-related front-line systems and supporting systems that contribute to prevention or mitigation of severe accident events. The analysis identifies the importance of each component for each system.
- Human reliability analysis - A detailed human reliability analysis is performed, with emphasis on the evaluation of the effect of single operator decisions on more than one system.
- Common cause failure analysis - An analysis is performed to identify and model the dependencies (common cause failures), both internal to individual systems and among systems, that use similar components exposed to similar environments.
- Severe accident analysis - Analyses are performed with the MAAP4 code to study the progression of severe accident sequences and to define the radionuclide source terms.
- Dose evaluation - The dose at the plant site boundary for the various fission product release categories are calculated.
- Hydrogen control analysis - Analyses to demonstrate the effectiveness of the hydrogen igniters are carried out using the MAAP4 code.
- Shutdown analysis - The frequency of core damage and of large release are quantified for low power and shutdown conditions.
- Fire and flood analyses - Internal fire and internal flood risk analyses evaluate potential vulnerabilities within the plant.

- Seismic margin analysis - Seismic margin methodology is used to identify potential seismic vulnerabilities and to assess the margin beyond the design-level safe shutdown earthquake.
- Assembly of results - The frequency of the dose at the site boundary exceeding a certain level is obtained by combining the results of the core damage analysis, severe accident analysis, and dose analysis.

19.1.5 Results

The AP600 PRA is an integrated view of the AP600 behavior in response to transients and accidents, including severe accidents.

The AP600 core damage frequency for internal events from at-power conditions is extremely low. The core damage frequency calculated for internal events at shutdown conditions is also very low. The combined core damage frequency from internal events at power and at shutdown conditions meets the NRC and URD safety goals with substantial margin.

The AP600 large release frequency of the dose at the site boundary exceeding 1 rem effective dose equivalent in 24 hours after core damage for internal events from at-power conditions is very low. The AP600 large release frequency calculated for internal events at shutdown conditions is also very low. Like the core damage frequency, the combined large release frequency from internal events at power and at shutdown conditions meets the NRC safety goals with substantial margin.

There are no nonsafety-related systems in the AP600 that have a high risk importance. A sensitivity analysis shows the core damage frequency and large release frequency for the AP600 is lower than those measured for current generation plants without any credit for the mitigation abilities of the AP600 nonsafety systems.

There are no critical operator actions in the AP600 PRA analyses. The core damage frequency remains relatively small even if all operator actions are assumed to fail. Only a small improvement in the core damage frequency can be realized by improving the reliability of the plant operators.

The AP600 containment is capable of providing an effective barrier to the release of fission-products to the environment and includes effective hydrogen control measures. The AP600 design meets the criteria in 10 CFR 50.34(f)(2)(ix).

These results demonstrate that the AP600 meets and exceeds the design goals specified in Section 19.1.2.

Insights regarding the AP600, derived from or verified by this PRA, include:

- Passive safety-related systems eliminates the dependence of safety-related system operation on ac electric power and compressed air. This significantly reduces the core damage frequency resulting from a loss of offsite power or station blackout event.
- Reactor coolant pump seal loss-of-coolant accidents are eliminated because of the use of canned motor reactor coolant pumps.
- Simplified passive safety-related systems reduce the need for, and importance of, operator action.
- The analysis shows that many of the events, which in the past, were leading contributors to the risk of nuclear power plants, are not as significant for the AP600. The contribution of interfacing systems loss-of-coolant accidents, which are typically the highest risk severe accident sequences, is made insignificant by the design of the AP600.
- The ability to flood the reactor cavity is an important contributor to maintaining a low release frequency for AP600. This feature and the design of the reactor insulation that provides for cooling of the reactor vessel keeps a damaged core inside the reactor vessel. This reduces the potential for ex-vessel severe accident events.
- The AP600 design provides a passive means of maintaining the containment integrity by removing decay heat from the containment with water on the containment shell or through air cooling. This cooling ability reduces the potential of containment failure due to overpressurization after severe accident.
- The AP600 containment design enhances the deposition of aerosols before they are released to the environment and reduces the potential environmental effects of a severe accident that has failed the containment.

19.1.6 Plant Definition

19.1.6.1 General Description

See Chapter 1.

19.1.6.2 AP600 Design Improvement as a Result of Probabilistic Risk Assessment Studies

Several design improvements are incorporated based on the results of the PRA and other design analyses. The plant design evolved throughout the PRA program. Interaction between design engineers and the PRA analysts influenced the final plant design.

The most significant design changes prompted by the PRA are:

- In the first three stages of the automatic depressurization system (ADS), both series motor-operated valves are closed during normal operation instead of one closed/one open. This reduces the frequency of spurious actuation of the automatic depressurization system.
- The number and size of the fourth-stage automatic depressurization system valves has been increased. In the event of a small loss-of-coolant accident, this modification provides a redundant and diverse path for depressurization in case of common cause failure of the motor-operated valves in the first three stages of the automatic depressurization system.
- The diverse actuation system is provided to automatically actuate selected systems such as the passive residual heat removal, core makeup tank, passive containment cooling system, reactor trip, and containment isolation. In addition, the system provides alarms and information to the main control room for manual actuation of these systems.

Diversity is provided in the diverse actuation system by using components that are diverse from the microprocessor-based components used in the protection and safety monitoring system and the plant control system. This reduces the importance of potential common cause failures (both hardware and software) of microprocessor-based components of the protection and safety monitoring system and the plant control system that process information and provide for actuation of safety-related and nonsafety-related accident mitigation systems.

The diversified functions are selected on the basis of PRA insights to reduce the core damage frequency and to reduce the conditional probability of large-release frequency, given core damage.

- Manual actuation of the normal residual heat removal system (RNS) can be accomplished from the main control room. The normal residual heat removal system provides a diverse means of coolant injection in case of failure of the check valves of the in-containment refueling water storage tank. An emergency operating procedure requires aligning the normal residual heat removal system when the automatic depressurization system is actuated.
- Two parallel paths, each containing a squib valve and a check valve in series, are used for gravity injection from the in-containment refueling water storage tank. This improves the in-containment refueling water storage tank reliability for the case of single valve failure during a safety injection line break event, or for the case of common cause failure of the two check valves in other events requiring full reactor depressurization.
- The check valves in the core makeup tank injection lines are designed so that they remain in the open position during the plant normal operation. This design eliminates opening failures and common cause failures with the accumulator check valves.

- The automatic depressurization system is automatically actuated during a transient event with loss of both secondary side heat removal and passive residual heat removal capability. This is accomplished by the provision to automatically actuate the core makeup tanks on low steam generator level and high hot leg temperature signals. Core makeup tank injection subsequently causes actuation of the automatic depressurization system. This improvement reduces the importance of the operator actions.
- Automatic opening of the motor-operated valves of the in-containment refueling water storage tank injection line occurs on a low hot leg water level signal. These valves are closed during shutdown conditions, such as mid-loop and vessel-flange operation, when the reactor coolant system is at atmospheric pressure. This also reduces the importance of operator action on these events.
- Alarms are provided in the main control room to inform the operator of mispositioned isolation valves of the passive core cooling systems that have remote manual control capability. This reduces the probability of valve mispositioning.
- Protection system logic is adopted to preclude steam generator overfilling during a steam generator tube rupture event. This reduces the need for full reactor depressurization and, therefore, reduces the frequency of core damage for steam generator tube rupture events with the containment bypassed.
- The capability to manually actuate the draining of in-containment refueling water storage tank water into the reactor cavity is provided. This is incorporated to address a core damage event in which the injection of in-containment refueling water storage tank water to the reactor vessel fails. This drained water cools the core debris inside the reactor vessel, removing the heat through the reactor vessel wall, avoiding failure of the reactor vessel.

19.1.7 References

- 19.1-1 Advanced Light Water Reactor Requirements Document, Volume III, Appendix A to Chapter 1, "PRA Key Assumptions and Groundrules," Revisions 5 and 6, December 1993.
- 19.1-2 EPRI MAAP 4.0 Users Manual.

19.2 Internal Initiating Events

This section intentionally blank.

19.3 Modeling of Special Initiators

This section intentionally blank.

19.4 Event Tree Models

This section intentionally blank.

19.5 Support Systems

This section intentionally blank.

19.6 Success Criteria Analysis

This section intentionally blank.

19.7 Fault Tree Guidelines

This section intentionally blank.

19.8 Passive Core Cooling System - Passive Residual Heat Removal

See subsection 6.3.1.1.1.

19.9 Passive Core Cooling System - Core Makeup Tanks

See subsections 5.4.13 and 6.3.2.2.1.

19.10 Passive Core Cooling System - Accumulator

See subsection 6.3.2.2.2.

19.11 Passive Core Cooling System - Automatic Depressurization System

See subsections 5.4.6 and 6.3.2.2.8.5.

19.12 Passive Core Cooling System - In-Containment Refueling Water Storage Tank

See subsection 6.3.2.2.3.

19.13 Passive Containment Cooling

See subsection 6.2.2.

19.14 Main and Startup Feedwater System

See Section 10.3 and subsection 10.4.9.