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 AP1000 design process includes a risk assessment of the design prior to being finalized to optimize the plant with respect to safety. Westinghouse accomplishes this by committing to the early application of probabilistic analysis techniques in the AP1000 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 exceeds design objectives.

19.1.1 Background and Overview

The AP1000 PRA was developed to support the application for Design Certification of the AP1000 nuclear plant. The AP1000 design is based extensively on the AP600 standard nuclear plant that received Design Certification in December 1999. The AP600 PRA, which was reviewed by the US NRC in detail during the seven-year review of the AP600, is used as the starting point for the AP1000 PRA. Since the configuration of the AP1000 reactor and safety systems is the same as the AP600, the AP600 PRA is used as the basis of the AP1000 PRA with relevant changes implemented in the model to reflect the AP1000 design changes. AP1000 plant-specific T&H analyses are performed in order to determine the system success criteria. The core damage frequency and large release frequency are calculated for internal events. The external events and shutdown models are also assessed to derive plant insights and plant risk conclusions.

The purpose of the PRA is to provide inputs to the optimization of the AP1000 design and to verify that the US NRC PRA safety goals have been satisfied. As in the AP600, the PRA is being performed interactively with the design, analysis and operating procedures. The PRA results show that there are only minor impacts on the PRA results compared to AP600, and that the very low risk of the AP600 has been maintained in the AP1000; the AP1000 PRA meets the US NRC safety goals with significant margin. Insights from the analysis are provided discussing the effect on the PRA of differences between the AP600 and the AP1000 designs.

19.1.2 Objectives

The objectives of the AP1000 PRA are to:

- Provide an integrated view of the AP1000 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 AP1000 design configuration and operation requirements and the ALWR URD requirements on PRA methodology (Reference 19.1-1)

- Demonstrate the low vulnerability and insensitivity of the AP1000 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 AP1000 safety)

- Demonstrate compliance with the hydrogen control criteria set forth in 10 CFR 50.44

- Serve as a basis for an accident management program

19.1.3 Technical Scope

The technical tasks for the AP1000 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 Risk Assessment
- External Events Risk Assessment

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.

External events analyses include:

- Internal fire assessment
- Internal flooding assessment
- Seismic margin assessment
- High winds assessment
- External flooding assessment
- Transportation and nearby facility accident assessment

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 AP1000-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 assessment - The frequency of core damage is assessed for low power and shutdown conditions.

- Fire and flood assessment - Internal fire and internal flood risk assessment evaluate potential vulnerabilities within the plant.

- Seismic margin assessment - 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 AP1000 PRA is an integrated view of the AP1000 behavior in response to transients and accidents, including severe accidents.

The AP1000 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 AP1000 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. 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.

In the AP600 licensing process, an initial set of sensitivity analyses were made to assess the importance of non-safety related systems. Later on, this exercise grew into a full-fledged PRA model which was named the focused PRA. The focused PRA was performed to assess the importance of the nonsafety-related systems. The results of the focused PRA (Reference 19.1-3) demonstrated that the AP600 passive plant design was able to meet the NRC safety goals crediting only safety-related equipment, with no credit for any of the nonsafety-related systems. To resolve the regulatory treatment of nonsafety-related systems, Westinghouse and the NRC agreed to availability controls of selected nonsafety-related systems for the purposes of providing defense-in-depth as well as investment protection.

The AP1000 PRA demonstrates a very similar low risk profile for the AP1000 as for the AP600. Sensitivity studies performed for the AP1000 demonstrates that no nonsafety-related system is of high risk importance. The same nonsafety-related system availability controls adopted for the AP600 will be applied to the AP1000 for the purpose of providing defense-in-depth and investment protection and are discussed in DCD Section 16.3.

There are no critical operator actions in the AP1000 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 AP1000 containment is capable of providing an effective barrier to the release of fission-products to the environment and includes effective hydrogen control measures. The AP1000 design meets the criteria in 10 CFR 50.44.

These results demonstrate that the AP1000 meets and exceeds the design goals specified in Section 19.1.2.

Insights regarding the AP1000, derived from or verified by this PRA, include:

- Passive safety-related systems eliminate 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 sealless 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 AP1000. 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 AP1000.

- The ability to flood the reactor cavity is an important contributor to maintaining a low release frequency for AP1000. This feature and the design of the reactor insulation that provides for cooling of the reactor vessel keep a damaged core inside the reactor vessel. This reduces the potential for ex-vessel severe accident events.

- The AP1000 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 AP1000 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 AP1000 Design Improvement as a Result of Probabilistic Risk Assessment Studies

Design improvements were incorporated in the AP600 design based on the results of the AP600 PRA and other design analyses and are discussed in Reference 19.1-3. These improvements have been retained in the AP1000 design. Additional design changes have been incorporated in the AP1000 as a result of the AP1000 PRA. The most significant design changes prompted by the AP1000 PRA are:

- Two recirculation lines, each containing a motor-operated valve and a squib valve or a check valve and a squib valve in series, are used to provide recirculation flow from containment sump to the core through direct vessel injection line. Diversity is provided in the actuation by using diverse squib valves. The motor-operated valve is designed so that it remains open in case of failure.

- Three parallel supply lines allow water flow from PCCWST to the containment shell. Diversity is provided in the actuation by using motor-operated valves for one path.

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.

19.1-3 AP600 PRA.

19.2 Internal Initiating Events

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.3 Modeling of Special Initiators

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.4 Event Tree Models

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.5 Support Systems

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.6 Success Criteria Analysis

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.7 Fault Tree Guidelines

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

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 subsection 10.4.9.