1. INTRODUCTION AND GENERAL DISCUSSION

1.1 Introduction

On March 28, 2002, Westinghouse Electric Company (hereinafter referred to as Westinghouse or the applicant) tendered its application for certification of the AP1000 standard nuclear reactor design with the U.S. Nuclear Regulatory Commission (the NRC or Commission). The applicant submitted this application in accordance with Title 10 of the Code of Federal Regulations (10 CFR) Part 52, Subpart B, "Standard Design Certifications," and 10 CFR Part 52, Appendix O, "Standardization of Design: Staff Review of Standard Designs." The application included the AP1000 Design Control Document (DCD) and the AP1000 Probabilistic Risk Assessment (PRA). The NRC formally accepted the application as a docketed application for design certification (Docket No. 52-006) on June 25, 2002. Information submitted before that date is associated with Project No. 711.

The applicant originally submitted the AP1000 DCD on March 28, 2002. The DCD information is divided into two categories, denoted as Tier 1 and Tier 2. Tier 1 means the portion of the generic design-related information that is proposed for approval and certification, including, among other things, the inspections, tests, analyses and acceptance criteria (ITAAC). Tier 2 means the portion of the generic design-related information proposed for approval but not certification. Tier 2 information includes, among other things, a description of the design of the facility required for a final safety analysis report by 10 CFR 50.34. Subsequently, the applicant supplemented the information in the DCD by providing revisions to that document. The applicant submitted the most recent version, DCD Revision 14, to the Commission on September 7, 2004. Similarly, the applicant originally submitted the PRA on March 28, 2002. The most recent revision of this report, Revision 8, was submitted by letter dated August 2, 2004. In addition, throughout the course of the review, the NRC staff (staff) requested that the applicant submit additional information to clarify the description of the AP1000 design. Some of the applicant's responses to these requests for additional information (RAIs) are discussed throughout this report. Appendix E to this report provides a listing of the issuance and response dates for each RAI the staff submitted to the applicant. The DCD, PRA, Tier 1 information, and all other pertinent information and materials are available for public inspection at the NRC Public Document Room and the Agencywide Documents Access and Management System Public Electronic Reading Room (ADAMS).

This final safety evaluation report (FSER) summarizes the staff's safety review of the AP1000 design against the requirements of 10 CFR Part 52, Subpart B, and delineates the scope of the technical details considered in evaluating the proposed design. In addition, this FSER documents the resolution of the open and confirmatory items identified in the draft safety evaluation report (DSER) for the AP1000 design, issued on June 16, 2003. Appendix G to this report includes a copy of the report by the Advisory Committee on Reactor Safeguards (ACRS) required by 10 CFR 52.53, "Referral to the ACRS."

As described above, the applicant supplemented the information in the DCD by providing revisions to the document. The staff's review of these revisions to determined their impact on the conclusions in this FSER was Open Item 1.1-1 in the DSER. The staff has completed its review of the most recent version of the DCD, as documented throughout this report, and for the reasons set forth herein, finds it to be acceptable. Therefore, Open Item 1.1-1 is resolved.

Sections 1.2 and 1.3 of this report summarize the AP1000 design. Section 1.4 of this report identifies the agents and contractors who provided design services to the applicant or other support for the design. Section 1.5 of this report provides a discussion of the principal matters that the staff reviewed.

1.1.1 Metrication

This report conforms to the Commission's policy statement on metrication published in the Federal Register on June 19, 1996. Therefore, all measures are expressed as metric units, followed by English units in parentheses. The unit of air volume flow was converted from standard cubic feet per minute at 14.7 psia and 68 °F to standard cubic meters per hour at 760 mmHg and 0 °C.

1.1.2 Proprietary Information

This report references several Westinghouse reports. Some of these reports contain information that the applicant requested be held exempt from public disclosure, as provided by 10 CFR 2.790, "Public Inspections, Exemptions, Requests for Withholding." For each such report, the applicant provided a nonproprietary version, similar in content except for the omission of the proprietary information. The staff predicated its findings on the proprietary versions of these documents, which are primarily referenced throughout this report.

1.1.3 Combined License Applicants Referencing the AP1000 Design

Applicants who reference the AP1000 standard design in the future for specific facilities will retain architect-engineers, constructors, and consultants, as needed. As part of its review of an application for a combined license (COL) referencing the AP1000 design, the staff will evaluate, for each plant-specific application, the technical competence of the COL applicant and its contractors to manage, design, construct, and operate a nuclear power plant. COL applicants will also be subject to the requirements of 10 CFR Part 52, Subpart C, "Combined Licenses," and any requirements resulting from the staff's review of this standard design. Throughout the DCD, the applicant identified matters to be addressed by plant-specific applicants as "Combined License Information." This report refers to such matters as "COL Action Items" throughout. Appendix F to this report provides a cross-reference between the COL action items identified in this report and the COL information referred to in the DCD.

1.1.4 Additional Information

Appendix A to this report provides a chronology of the principal actions, submittals, and amendments related to the processing of the AP1000 application. Appendix B of this report provides a list of references identified in this report. Appendix C of this report provides a list containing definitions of the acronyms and abbreviations used throughout this report. Appendix D of this report lists the principal technical reviewers who evaluated the AP1000 design. Appendix E of this report provides an index of the staff's RAIs and the applicant's responses. Appendix F of this report provides a cross-reference of the COL information in the DCD, FSER, and COL action items. Appendix G of this report includes a copy of the letter received from the ACRS providing the results of its review of the AP1000 design.

The NRC licensing project managers assigned to the AP1000 standard design review are Mr. John P. Segala, Mr. Joseph Colaccino, Mr. Steven D. Bloom, and Ms. Lauren M. Quinones-Navarro. They may be reached by calling (301) 415-7000, or by writing to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, DC 20555-0001.

1.2 General Design Description

1.2.1 Scope of the AP1000 Design

The requirement that governs the scope of the AP1000 design can be found in 10 CFR 52.47(b)(2)(i)(A)(4), which requires that an applicant for certification provide a complete design scope, except for site-specific elements. Therefore, the scope of the AP1000 design must include all of the plant structures, systems, and components that can affect the safe operation of the plant, except for its site-specific elements. The applicant described the AP1000 standard design scope in DCD Tier 2, Section 1.8, “Interfaces for Standard Design,” including the site-specific elements that are either partially or wholly outside of the standard design scope. The applicant also described interface requirements (see DCD Tier 2, Table 1.8-1, “Summary of AP1000 Plant Interfaces with Remainder of Plant”) and representative conceptual designs, as required by 10 CFR 52.47(a)(1)(vii) and 10 CFR 52.47(a)(1)(ix), respectively.

1.2.2 Summary of the AP1000 Design

The AP1000 design has a nuclear steam supply system (NSSS) power rating of 3415 megawatt thermal (MWt), with an electrical output of at least 1000 megawatt electric (MWe). The plant is designated for rated performance with up to 10 percent of the steam generator (SG) tubes plugged and with a maximum hot-leg temperature of 321.1 °C (610 °F). The plant is designed to accept a step-load increase or decrease of 10 percent between 25- and 100-percent power without reactor trip or steam dump system actuation, provided that the rated power level is not exceeded. In DCD Tier 2, Section 1.2, “General Plant Description,” the applicant also indicated that the plant is designed to accept a 100-percent load rejection from full power to house loads without a reactor trip or operation of the pressurizer or SG safety valves. The goal for the overall plant availability is projected to be greater than 90 percent, considering all forced and planned outages, with a rate of less than one unplanned reactor trip per year. The applicant stated that the plant has a design objective of 60 years without a planned replacement of the reactor vessel. However, the design does provide for replaceability of other major components, including the SG. The following is a general description of the AP1000 design. Subsequent sections of this report provide detailed descriptions of the individual systems that make up the AP1000 design.

1.2.2.1 Reactor Coolant System Design

The AP1000 reactor coolant system (RCS) is designed to effectively remove or enable removal of heat from the reactor during all modes of operation, including shutdown and accident conditions.

The system consists of two heat transfer circuits, each with the following components:

- an SG
- two reactor coolant pumps (RCPs)
- a single hot-leg
- two cold-legs

In addition, the system includes a pressurizer, interconnecting piping, valves, and the instrumentation necessary for operational control and safeguards actuation. All of the system equipment is located within the reactor containment. Figure 1.2-1 of this report shows a diagram of the AP1000 RCS.

Operation of the pressurizer controls the reactor system pressure. The spring-loaded safety valves installed on the pressurizer provide overpressure protection for the RCS. These safety valves discharge to the containment atmosphere. The valves for the first three stages of automatic depressurization are also mounted on the pressurizer. These valves discharge steam through spargers to the in-containment refueling water storage tank (IRWST) of the passive core cooling system (PXS). The discharged steam is condensed and cooled by mixing with water in the tank.

The following auxiliary systems interface with the RCS:

- chemical and volume control system (CVS)
- component cooling water system
- liquid radwaste system
- primary sampling system
- PXS
- spent fuel pit cooling system
- SG system

1.2.2.2 Reactor Design

An AP1000 fuel assembly consists of 264 fuel rods in a 17x17 square array. The fuel grids consist of an eggcrate arrangement of interlocked straps that maintains lateral spacing between the rods. The fuel rods consist of enriched uranium, in the form of cylindrical pellets of uranium dioxide, contained in ZIRLO tubing. The tubing is plugged with seals welded at the ends to encapsulate the fuel. An axial blanket comprised of fuel pellets with reduced enrichment may be placed at each end of the enriched fuel pellet stack to reduce the neutron leakage and improve fuel utilization. Other types of fuel rods may be used to varying degrees within some fuel assemblies. One type uses an integral fuel burnable absorber containing a thin boride coating on the surface of the fuel pellets. Another type uses fuel pellets containing gadolinium oxide mixed with uranium oxide. The boride-coated fuel pellets and gadolinium oxide/uranium oxide fuel pellets provide burnable absorber integral to the fuel.

The applicant stated that the reactor core is designed for an 18-month fuel cycle. A core design is maintained for projected fuel cycles. The reactor core is located low in the vessel to minimize core temperature during a postulated loss-of-coolant accident (LOCA). The core is designed to have a moderator temperature coefficient that is nonpositive over the entire fuel cycle and at any power level, with the reactor coolant at the normal operating temperature. The core design provides an adequate margin so that departure from nucleate boiling will not occur with a 95 percent probability and 95 percent confidence basis for all Condition I and II events. No vessel penetrations exist below the top of the core because the AP1000 does not use bottom-mounted in-core instrumentation. In addition, the design employs an integrated head package that consists of the following components:

- control rod drive mechanisms
- integrated head cooling fans
- instrument columns
- insulation
- seismic support
- package lift rig

A permanent, welded-seal ring provides the seal between the vessel flange and the refueling cavity floor.

1.2.2.3 Steam Generator Design

The AP1000 design uses the Model Delta 125 SG, which employs thermally treated, nickel-chromium-iron Alloy 690 tubes and a steam separator area sludge trap with clean-out provisions. The channel head is designed to directly attach the two RCPs, and to allow both manual and robotic access for inspection, plugging, sleeving, and nozzle dam placement operations.

1.2.2.4 Reactor Coolant Pump Design

The four AP1000 RCPs are hermetically sealed canned pumps. Two RCPs are attached directly to the SG channel head with the motor located below the channel head to simplify the loop piping and eliminate fuel uncovery during postulated small-break LOCA scenarios. Each RCP includes sufficient internal rotating inertia to permit coastdown to avoid departure from nucleate boiling following a postulated loss-of-coolant flow accident. Each pump impeller and diffuser vane is ground and polished to minimize radioactive crud deposition and maximize pump efficiency. The RCPs are designed such that they are not damaged due to a loss of all cooling water for the period up to and including a safety-related pump trip on high-bearing water temperature. This automatic protection is provided to protect the RCPs from an extended loss of coolant water.

1.2.2.5 Pressurizer and Loop Arrangement

The pressurizer is a vertical, cylindrical vessel with hemispherical top and bottom heads. One spray nozzle and two nozzles for connecting the safety and depressurization valve inlet headers are located in the top head. Electrical heaters are installed through the bottom head. The piping layouts for the AP1000 are designed to provide adequate thermal expansion flexibility, assuming a fixed vessel and a free-floating SG/RCP support system. The reactor coolant loop and surge line piping are designed to leak-before-break criteria. The pressurizer itself is designed such that the power-operated relief valve function is neither required nor provided, given the AP1000 design spray flow rates.

1.2.2.6 Steam and Power Conversion System Design

Turbine Generator

The AP1000 turbine generator design consists of a double-flow, high-pressure cylinder (high-pressure turbine) and three double-flow, low-pressure cylinders (low-pressure turbines) that exhaust to the condenser. It is a six-flow, tandem-compound, 1800-rpm machine. The turbine system includes the following components:

- stop, control, and intercept valves directly attached to the turbine and in the steam-flow path
- crossover and cross under piping between the turbine cylinders and the moisture separator reheaters

The high-pressure turbine has extraction connections for one stage of feedwater heating, and its exhaust provides steam for one stage of feedwater heating in the deaerator. The low-pressure turbines have extraction connections for four stages of feedwater heating.

Two moisture separator reheaters are located between the high-pressure turbine exhaust and the low-pressure turbine inlet. The moisture separator reheater, an integral component of the turbine system, extracts moisture from the steam and then reheats the steam to improve turbine system performance. The reheater has two stages of reheat.

The turbine is oriented in a manner that minimizes potential interactions between turbine missiles and safety-related structures and components.

Main Steam System

The main steam system is designed to supply steam from the SG to the high-pressure turbine over a range of flows and pressures for the entire plant operating range. The main steam system is also designed to dissipate the heat generated by the NSSS to the condenser through the steam dump valves, or to the atmosphere through power-operated atmospheric relief valves or spring-loaded main steam safety valves, when either the turbine generator or the condenser is not available. There are two steam headers, with each one utilizing six SG safety valves.

Main Feedwater and Condensate System

The main feedwater system is designed to supply the SGs with adequate feedwater during all modes of plant operation, including transient conditions. The condensate system is designed to condense and collect steam from the low-pressure turbines and turbine bypass systems, and then to transfer this condensate from the main condenser to the deaerator. The applicant stated that the main feedwater and condensate systems are designed for increased availability and improved dissolved oxygen control.

1.2.2.7 Engineered Safeguards Systems Design

The engineered safeguards systems include the following systems and components. Figure 1.2-2 of this report shows some of the passive safety features, including the containment, the passive containment cooling system (PCS), and the PXS.

- The containment vessel is a free-standing, cylindrical steel vessel. Its engineered safety feature (ESF) function is to contain the release of radioactivity following a postulated design-basis accident (DBA). The containment vessel provides shielding for the reactor core and the RCS during normal operation. It also functions as the safety-related ultimate heat sink for the removal of the RCS sensible heat, core decay heat, and stored energy.

- The PCS consists of the following components:

  - a passive containment cooling water storage tank that is incorporated in the shield building structure above the containment

  - an air baffle that is located between the steel containment vessel and the concrete shield building

  - air inlet and exhaust paths that are incorporated in the shield building structure

  - a water distribution system

  - an ancillary water storage tank and two recirculation pumps for onsite storage of additional PCS cooling water

  Upon actuation, the PCS delivers water to the top, external surface of the steel containment shell, which forms a film of water over the dome and side walls of the containment structure. Air is induced to flow over the containment as it is heated, causing a chimney effect. This air flow and cooling water evaporation removes the heat generated within the containment and expels it to the outside air. The applicant stated that the PCS maintains the containment pressure and temperature within the appropriate design limits for both DBA and severe accident scenarios. Figure 1.2-3 of this report shows the PCS.

- The major function of the containment isolation system is to provide containment isolation to allow the normal or emergency passage of fluids through the containment boundary while preserving the integrity of the containment boundary. This function prevents or limits the escape of fission products that may result from postulated accidents. In the event of an accident, the containment isolation provisions are designed so that fluid lines penetrating the primary containment boundary are isolated. The containment isolation system consists of the piping, valves, and actuators that isolate the containment.

C The containment hydrogen control system controls the hydrogen concentration in the containment so that containment integrity is not endangered. It consists of the hydrogen monitoring system, passive autocatalytic hydrogen recombiners, and hydrogen ignitors.

C The PXS provides emergency core cooling following postulated design-basis events. The PXS is comprised of the following components:

– two core makeup tanks
– two accumulators
– the IRWST
– a passive residual heat removal (PRHR) heat exchanger
– pH adjustment baskets
– associated piping and valves

C The automatic depressurization system (ADS), which is part of the RCS, provides important passive core cooling functions by depressurizing the RCS. The PXS system provides emergency core cooling following a postulated DBA by providing (1) RCS makeup water and boration when the normal makeup supply is lost or insufficient, (2) safety injection to the RCS to ensure adequate core cooling during a postulated DBA, and (3) core decay heat removal during transients and accidents. Figure 1.2-4 of this report shows the safety injection systems.

C The main control room (MCR) emergency habitability system is comprised of a set of storage tanks connected to a main and an alternate air delivery line. Components common to both lines include a manual isolation valve, a pressure-regulating valve, and a flow metering orifice. This system is designed to provide the ventilation and pressurization needed to maintain a habitable environment in the MCR for 72 hours following any DBA.

In DCD Tier 2, Section 1.2.1.4.1, “Engineered Safeguards Systems Design,” the applicant stated that the engineered safeguards systems are designed to mitigate the consequences of DBAs with a single failure. With the exception of the MCR emergency habitability system, the passive safety systems are designed to cool the RCS from normal operating temperatures to safe-shutdown conditions. In addition, all of these systems are designed to maximize the use of natural driving forces, such as pressurized nitrogen, gravity flow, and natural circulation flow. They do not rely on active components such as pumps, fans, or diesel generators to function. These systems do, however, use valves to initially align the safety systems when activated. In addition, the safety systems are designed to function without safety-related support systems, such as alternating current; component cooling water; service water; or heating, ventilation, and air conditioning (HVAC).

The design of the AP1000 minimizes the number and complexity of operator actions needed to control the safety systems. To meet this objective, the approach was to eliminate the action, rather than automating it.

The automatic RCS depressurization feature included in the design meets the following criteria:

C The reliability (redundancy and diversity) of the ADS valves and controls satisfies the single-failure criterion as well as the failure tolerance called for by the low core melt frequency goals.

- The design provides for both real demands (i.e., RCS leaks and failure of the CVS makeup pumps) and spurious instrumentation signals. The probability of significant flooding of the containment due to the use of the ADS is less than once in 600 years.

The design is such that, for small-break LOCA up to 20.32 cm (8 in.) in diameter, the core remains covered.

Non-Safety-Related Systems Designs

The applicant stated that the non-safety-related systems used in the AP1000 are not relied on to provide safety functions needed to mitigate DBAs. The AP1000 includes active systems that provide defense-in-depth (DID) (or investment protection) capabilities for RCS makeup and decay heat removal. These active systems are the first line of defense to reduce challenges to the passive systems in the event of transients or plant upsets. Most active systems in the AP1000 are designated as non-safety-related.

Examples of non-safety-related systems that provide DID capabilities for the AP1000 design include the CVS, normal residual heat removal system, and the startup (backup) feedwater system. For these DID systems to operate, the associated systems and structures to support these functions must also be operable, including the non-safety-related standby diesel generators, the component cooling water system, and the service water system. The AP1000 also includes other active systems, designated as non-safety-related, such as the HVAC system which removes heat from the instrumentation and control (I&C) cabinet rooms and the MCR to limit challenges to the passive safety capabilities for these functions.

In existing plants, as well as in the evolutionary advanced light-water reactor (ALWR) designs, many of these active systems are designated as safety-related. However, by virtue of their designation in the AP1000 design as non-safety-related, credit is generally not taken for the active systems in DCD Tier 2, Chapter 15, “Accident Analyses,” licensing DBA analyses, except in certain cases in which operation of a non-safety-related system could make an accident worse.

The residual uncertainties associated with passive safety system performance increase the importance of active non-safety-related systems in providing DID functions to the passive systems. These active systems are not required to meet all of the criteria imposed on safety-related systems, but the staff does expects a high level of confidence that active systems which have a significant safety role will be available when challenged. As discussed in SECY-94-084, “Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Design,” issued March 28, 1994, a process was developed for maintaining appropriate regulatory oversight of these active systems in passive ALWR designs. In a staff requirements memorandum (SRM) dated June 30, 1994, the Commission approved the recommendations made in SECY-94-084 concerning the issue of regulatory treatment of non-safety-related systems (RTNSS). Chapter 22 of this report summarizes the staff’s evaluation of RTNSS.

1.2.2.8 Instrumentation and Control System and Electrical System Designs

Introduction

Control and Protection Systems Designs

The AP1000 control and protection systems are significantly different from I&C systems in operating reactor designs. In particular, the AP1000 employs digital, microprocessor-based I&C systems, instead of the analog electronics, relay logic, and hard-wired systems currently used in most operating plants. In DCD Tier 2, Section 1.2.1.5.1, “Control and Protection Systems Design,” the applicant stated that the design of the control and protection systems ensures that a single failure in the I&C system will not result in a reactor trip or ESF actuation during normal operation. As compared to currently operating plants, the design is intended to reduce the potential for a reactor trip and a safeguards actuation because of failures in the reactor control or protection systems.

The AP1000 design minimizes the number of measured plant variables used for reactor trip and for safeguards actuation relative to currently operating plants. The margin between the normal operating condition and the protection system setpoints is increased relative to currently operating plants. The potential for interaction between the protection and safety monitoring system (PMS) and the plant control system is reduced, relative to currently operating plants by incorporating a signal selector function that selects signals for control and for protection.

The AP1000 I&C systems are comprised of the following major systems:

- PMS
- special monitoring system (SMS)
- plant control system (PLS)
- diverse actuation system (DAS)
- operation and control centers system (OCS)
- data and display processing system (DDS)
- incore instrumentation system (IIS)

The PMS monitors plant processes using a variety of sensors; performs calculations, comparisons, and logic functions based on those sensor inputs; and actuates a variety of equipment. The PMS provides the safety-related functions necessary to control the plant during normal operation, to shut down the plant, and to maintain the plant in a safe-shutdown condition. The PMS is also used to operate safety-related systems and components.

The SMS consists of specialized subsystems that interface with the I&C architecture to provide diagnostic and long-term monitoring functions.

The PLS (1) controls and coordinates the plant during start-up, ascent to power, power operation, and shutdown conditions, (2) integrates the automatic and manual control of the reactor, reactor coolant, and various reactor support processes for specified normal and off-normal conditions, (3) controls the non-safety-related decay heat removal systems during shutdown, and (4) permits the operator to control plant components from the MCR or remote shutdown workstation.

The DAS provides a backup to the PMS for some specific diverse automatic actuation and provides diverse indications and controls to assist in operator manual actions. The DAS is a

DID system that is also designed to provide essential protection functions in the event of a postulated common-mode failure of the PMS.

The OCS includes the complete operational scope of the MCR, remote shutdown workstation, technical support center, local control stations, and the emergency operations facility.

The DDS comprises the equipment used for processing data that result in non-safety-related alarms and displays for both normal and emergency plant operations.

The IIS provides a three-dimensional flux map of the reactor core. It also provides the PMS with in-core thermocouple signals to monitor the adequacy of postaccident core cooling.

Alternating and Direct Current Power Designs

All safety-related electrical power is provided from the Class 1E direct current (dc) power system. The AP1000 does not include a separate safety-related alternating current (ac) power system. Safety-related dc power is provided to support reactor trip and engineered safeguards actuation. Batteries are sized to provide the necessary dc power and uninterruptable ac power for items such as PMS system actuation; control room functions including habitability; actuation of dc-powered valves in the passive safety systems; and containment isolation.

Main Control Room Design

The MCR controls the plant during normal and anticipated transients, as well as DBAs. It includes indications and controls that are capable of monitoring and controlling the plant safety systems and the non-safety-related control systems. The MCR contains the safety-related I&C to allow the operator to achieve and maintain safe shutdown following any DBA.

During normal operation, the MCR is serviced by redundant, non-safety-related power sources and HVAC systems. In the event that either the normal power source or the HVAC system becomes unavailable, the applicant has stated that passive systems (batteries and compressed air) will be available to support MCR operation for up to three days. The safety-related power sources and passive cooling system are designed to provide a habitable environment for the operating staff, assuming that no ac power is available. By using a passive cooling system, the safety-related instrumentation (equipment racks) is maintained at acceptable ambient conditions for three days following a loss of all ac power. After three days, it will be possible to continue operation with the control room cooled and ventilated by the natural circulation of outside air.

The operators can transfer control from the MCR to the remote shutdown workstation should the MCR become uninhabitable. The remote shutdown workstation contains the safety-related indications and controls that allow an operator to achieve and maintain safe shutdown of the plant following an event when the MCR is unavailable.

1.2.2.9 Plant Arrangement

The AP1000 plant is arranged with the following principal building structures:

- the nuclear island
- the turbine building
- the annex building
- the diesel generator building
- the radwaste building

The nuclear island is structurally designed to meet seismic Category I requirements in accordance with the guidance in Regulatory Guide 1.29, “Seismic Design Classification.” The nuclear island consists of the following buildings:

- a free-standing steel containment building
- a concrete shield building
- an auxiliary building

The nuclear island is designed to withstand the effects of postulated internal events such as fires and flooding without loss of capability to perform safety functions.

Figure 1.2-5 of this report shows the AP1000 building layout.

The containment building is the containment vessel and the structures contained within the containment vessel. The shield building comprises the structure and annulus area that surrounds the containment building. The containment building is an integral part of the overall containment system, which contains the release of airborne radioactivity following a postulated DBA and provides shielding for the RCS during normal operations. The containment and shield buildings are an integral part of the PCS. The auxiliary building protects and separates all of the seismic Category I mechanical and electrical equipment located outside the containment building. The auxiliary building contains the MCR, I&C systems, dc system, fuel handling area, mechanical equipment areas, containment penetration areas, and main steam and feedwater isolation valve compartments.

The turbine building houses the main turbine, generator, and associated fluid and electrical systems. It also houses the makeup water purification system. No safety-related equipment is located in the turbine building.

The annex building serves as the main personnel entrance to the power generation complex. The building includes the health physics area, the non-Class 1E ac and dc electric power systems, the ancillary diesel generators and their fuel supply, other electrical equipment, the technical support center, and various HVAC systems. No safety-related equipment is located in the annex building.

The diesel generator building houses two diesel generators and their associated HVAC equipment. No safety-related equipment is located in the diesel generator building. The building is a nonseismic structure designed for wind and seismic loads in accordance with the Uniform Building Code.

The radwaste building contains facilities for segregated storage of various categories of waste prior to processing, for processing by mobile systems, and for storing processed waste in shipping and disposal containers. No safety-related equipment is located in the radwaste building. It is a nonseismic structure designed for wind and seismic loads in accordance with the Uniform Building Code. The foundation for the building is a reinforced concrete mat on grade.

The overall plant arrangement utilizes building configurations and structural designs to minimize the building volumes and quantities of bulk materials (concrete, structural steel, and rebar), consistent with safety, operational, maintenance, and structural needs. The plant arrangement provides separation between safety-related and non-safety-related systems to preclude adverse interaction between safety-related and non-safety-related equipment. Separation between redundant, safety-related equipment and systems provides confidence that the safety design functions of the AP1000 can be performed. In general, this separation is achieved by partitioning an area with concrete walls.

1.3 <u>Comparison with Similar Facility Designs</u>

The AP1000 standard design contains many features that are not found in currently operating reactor designs. For example, a variety of engineering and operational improvements provide additional safety margins and address Commission policy statements regarding severe accidents, safety goals, and standardization. The most significant improvement to the design is the use of safety systems that rely on passive means, such as gravity, natural circulation, condensation and evaporation, and stored energy, for accident prevention and mitigation. DCD Tier 2, Table 1.3-1, “AP1000 Plant Comparison with Similar Facilities,” provides a detailed comparison of the principal design features of the AP1000 standard design with the certified AP600 design and a typical two-loop plant.

1.4 <u>Identification of Agents and Contractors</u>

Westinghouse is the principal AP1000 designer. The following organizations provided the principal subcontracting services for the design of the AP1000:

- Avondale Industries, Incorporated
- Bechtel North American Power Corporation
- Burns & Roe Company
- Chicago Bridge & Iron Services, Inc.
- MK-Ferguson Company
- Southern Electric International

Westinghouse received additional support from the following organizations:

- SOPREN/ANSALDO of Italy
- University of Western Ontario of Canada
- Ente Nazionale per l'Energia Eletrica (ENEL) of Italy
- Badan Tenaga Nuklir Nasional (BATAN) of Indonesia
- Ente per le Nuove tecnologie, l'Energie e l'Ambiente (ENEA) of Italy
- Badan Pengkajian dan Penerapan Teknologi (BPPT) of Indonesia
- FIATof Italy

- INITEC of Spain
- Asociacion Espanola de la Industria Electrica (UNESA) of Spain
- Union Temporal Empresas (UTE) of Spain
- Perusahaan Listrik Negara/Badan Pengkajian dan Penerapan Teknologi (PLN/BPPT) of Indonesia
- Oregon State University
- Electricité de France (EdF)
- Shanghai Nuclear Engineering Research & Design Institute (SNERDI) of China
- Mitsubishi Heavy Industries (MHI) of Japan
- Unterausschuss Kernenergie (UAK) of Switzerland
- Desarrollo Tecnologico Nuclear (DTN) of Spain
- Fortum of Finland

1.5 Summary of Principal Review Matters

The procedure for certifying a design is conducted in accordance with the requirements of 10 CFR Part 52, Subpart B, and is carried out in two stages. The technical review stage is initiated by an application filed in accordance with the requirements of 10 CFR 52.45, “Filing of Applications.” This stage continues with reviews by the NRC staff and the ACRS and ends with the issuance of an FSER that discusses the staff’s conclusions related to the acceptability of the design. The administrative review stage begins with the publication of a Federal Register notice that initiates rulemaking, in accordance with 10 CFR 52.51, “Administrative Review of Applications,” and includes a proposed standard design certification rule. The rulemaking culminates with the denial of the application or the issuance of a design certification rule.

The staff performed its technical review of Westinghouse’s application for certification of the AP1000 standard design in accordance with the requirements of 10 CFR Part 52, Sections 52.47, “Contents of Applications”; 52.48, “Standards for Review of Applications”; and 52.53. The staff evaluated the technical information required by 10 CFR 52.47(a)(1)(i) and provided by the applicant, in accordance with NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants.” That evaluation is the subject of this report.

In addition to these safety standards, the staff followed Commission guidance provided in the SRMs for all applicable Commission papers, including those referenced throughout this report. In particular, SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” issued April 2, 1993; SECY-94-084, and SECY-95-132, “Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs (SECY-94-084),” issued May 22, 1995, identify staff positions generic to passive light-water reactor (LWR) design certification policy issues. SECY-96-128, “Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design,” issued June 12, 1996; SECY-97-044, “Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design,” issued February 19, 1997; and SECY-98-161, “The Westinghouse AP600 Standard Design as it Relates to the Fire Protection and the Spent Fuel Pool Cooling Systems,” issued July 1, 1998, identify staff positions on issues specific to the AP600 design. In SRMs dated July 21, 1993, June 30, 1994, June 28, 1995, January 15, 1997, and June 30, 1997, the

Commission provided its guidance on these matters as they pertain to passive plant designs. Unless otherwise noted, the staff reviewed the AP1000 application using the newest codes and standards endorsed by the NRC.

Chapter 20 of this report discusses the staff's evaluation of the technically relevant unresolved safety issues, generic safety issues, and Three Mile Island requirements (10 CFR 52.47(a)(1)(ii) and (iv)). Chapter 2 of this report presents the staff's evaluation of the site parameters postulated for the design as required by 10 CFR 52.47(a)(1)(iii). Section 19.1 of this report summarizes the staff's evaluation of the design-specific PRA (10 CFR 52.47(a)(1)(v)), and Section 14.3 of this report provides the evaluation of the ITAAC required by 10 CFR 52.47(a)(1)(vi).

Selected chapters of this report, particularly Chapter 14, discuss the staff's evaluation of the interface requirements and representative conceptual designs (10 CFR 52.47(a)(1)(vii) through (ix)). The staff also implemented the Commission's Severe Accident Policy Statement, dated August 8, 1985, and the Commission's SRMs related to SECY-90-016, "Evolutionary Light Water Reactor (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements," issued January 12, 1990; SECY-93-087; SECY-94-084; SECY-95-132; SECY-96-128; and SECY-97-044, in its resolution of severe accident issues. Section 19.2 of this report discusses the staff's evaluation of severe accident issues.

The regulations in 10 CFR 52.47(a)(2) describe the level of design information needed to certify a standard design. In addition, the February 15, 1991, SRM associated with SECY-90-377, "Requirements for Design Certification Under 10 CFR Part 52," issued November 8, 1990, sets forth the Commission's position on the level of design information required for a certification application. The staff followed this guidance in preparing this report. The staff also followed the guidance of SECY-92-053, "Use of Design Acceptance Criteria During 10 CFR Part 52 Design Certification Reviews," issued February 19, 1992, and SECY-02-0059, "Use of Design Acceptance Criteria for AP1000 Standard Plant Design," issued April 1, 2002. To allow for the use of rapidly developing technology, the staff based its safety determinations on design acceptance criteria (DAC) for certain technical areas. The DAC are part of the Tier 1 information proposed for the AP1000 design. Section 14.3 of this report includes the staff's evaluation of the Tier 1 information, including DAC and ITAAC.

As part of its technical review, the staff issued numerous RAIs to gain sufficient bases for its safety findings, thereby meeting the requirement in 10 CFR 52.47(a)(3) to advise the applicant on whether additional technical information required submission. Appendix E of this report provides an index of the applicant's responses to these RAIs.

Section 1.2.1 of this report discusses the scope of the design to be certified. Because of the unique nature of the AP1000 design, the applicant implemented an extensive testing program to provide data on the passive safeguards systems. These data validate the safety analysis methods and computer codes and provide information to assess the design margins in the passive safety system performance. Chapter 21 of this report discusses the staff's evaluation of the testing program required pursuant to 10 CFR 52.47(b)(2). Because the AP1000 is designed as a single unit (i.e., no safety systems will be shared at a multi-unit site), 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 5, "Sharing of Structures, Systems, and

Components," and 10 CFR 52.47(b)(3) do not apply to this design. Any applicant wishing to construct multiple units at a single site will be required to address these regulations in its application.

In DCD Tier 2, Section 1.2.1.1.2, the applicant states that the plant design objective is 60 years. Throughout this report the staff makes reference to the applicant's 60 year design objective. These statements, however, do not affect the bases of the staff's evaluation. In accordance with the Atomic Energy Act of 1954, as amended, and 10 CFR 50.51(a), the staff based its review on a license duration of 40 years.

1.6 Summary of Open Items

As a result of the staff's review of Westinghouse's application for certification of the AP1000 design (including any additional information provided to the NRC through April 21, 2003), the staff identified several issues that remained open at the time the DSER was issued. In addition, the staff identified additional issues after the issuance of the DSER. The staff considers an issue to be open if the applicant has not provided requested information and the staff is unaware of what will ultimately be included in the applicant's response. Each open item was assigned a unique identifying number which indicates the section in this report where it is described. For example, Open Item 4.4-1 is discussed in Section 4.4 of this report.

The DSER was issued with 174 open items. When the FSER was prepared, the staff discovered Open Item 3.7.2-1 had not been included in DSER Section 1.6, "Summary of Open Items." After issuance of the DSER, two new issues were identified through discussions with the ACRS, Open Items 5.2.3-2 and 5.2.3-3. In addition, 28 issues connected to Open Item 14.2-1 were identified during the supplemental review concerning the initial plant test program. This report includes a discussion of these open items. As set forth throughout this report, all open items have been resolved.

1.7 Summary of Confirmatory Items

The NRC staff's review of Westinghouse's application for certification of the AP1000 design, as documented in the DSER, identified several confirmatory items. An item is identified as confirmatory if the staff and Westinghouse have agreed on a resolution of a particular item, but the resolution has not yet been formally documented in the DCD. Each confirmatory item was assigned a unique identifying number. The number indicates the section in this report where the confirmatory item is described. For example, Confirmatory Item 7.2.3-1 is discussed in Section 7.2.3 of this report.

The DSER was issued with 27 confirmatory items. After issuance of the DSER, two additional confirmatory items were identified, Confirmatory Items 3.8.2.6-1 and 3.8.5.5-3. This report includes a discussion of these confirmatory items. As set forth throughout this report, all confirmatory items have been resolved.

1.8 Index of Exemptions

In accordance with 10 CFR 52.48, the staff used the current regulations in 10 CFR Part 20, “Standards for Protection Against Radiation”; Part 50, “Domestic Licensing of Production and Utilization Facilities”; Part 73, “Physical Protection of Plants and Materials”; and Part 100, “Reactor Site Criteria”; in reviewing Westinghouse’s application for certification of the AP1000 design. During this review, the staff recognized that the application of certain regulations to the AP1000 design would not serve the underlying purpose of the rule, or would not be necessary to achieve the underlying purpose of the rule.

In a letter dated December 3, 2002, Westinghouse submitted a list of exemption requests. These exemptions are discussed in the sections of this report listed below.

Section	Exemption
8.2.3.2	Exemption from GDC 17, “Electric Power Systems,” requirement for a physically independent circuit (i.e., a second off-site electrical power source)
15.2.9	Exemption from 10 CFR 50.62, “Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants,” requirement for automatic startup of auxiliary feedwater system
18.8.2.3	Exemption from 10 CFR 50.34(f)(2)(iv) requirements for safety parameter display console

1.9 Index of Tier 2* Information

The NRC staff has determined that certain changes to or departures from information in the DCD that are proposed by an applicant or licensee who references the certified AP1000 design will require NRC approval before the change can be implemented, in accordance with the design certification rule. This information will be referred to as Tier 2* in the proposed design certification rule. At the time the DSER was issued, the staff had not completed its review of the Tier 2* information pertaining to the AP1000 design. This was Open Item 1.9-1 in the DSER.

DCD Introduction Table 1-1, “Index of AP1000 Tier 2 Information Requiring NRC Approval for Change,” provides a list of the items designated as Tier 2* information. The staff has now completed its review of the Tier 2* information pertaining to the AP1000 design. For the reasons set forth throughout this report regarding Tier 2* information, the staff finds such information acceptable. Therefore, Open Item 1.9-1 is resolved.

1.10 COL Action Items

COL applicants and licensees referencing the certified AP1000 standard design must satisfy the requirements and commitments identified in the DCD, which is the controlling document used in the certification of the AP1000 design. In addition, the AP1000 DCD identifies certain general commitments as “Combined License Information Items,” and in this report as “COL Action Items.” These COL action items relate to programs, procedures, and issues that are outside the scope of the certified design review. These COL action items do not establish requirements;

rather, they identify an acceptable set of information to be included in a plant-specific safety report. An applicant for a COL must address each of these items in its application. It may deviate from or omit these items, provided that the deviation or omission is identified and justified in the plant-specific safety report.

Westinghouse included a summary of COL action items in DCD Tier 2, Table 1.8-2, “Summary of AP1000 Standard Plant Combined License Information Items,” and provided an explanation of the items in the applicable sections of the DCD. At the time the DSER was issued, the staff had not completed its review and cross-reference of the COL action items. This was Open Item 1.10-1 in the DSER.

In addition, the staff identified a number of new COL action items as a result of its review. These are highlighted throughout this report. The applicant revised the DCD to incorporate these new COL action items. The staff reviewed the revised DCD and found it to be acceptable. Appendix F to this report provides a cross-reference between the COL action items identified in this report and the COL information referred to in the DCD. Therefore, Open Item 1.10-1 is resolved.

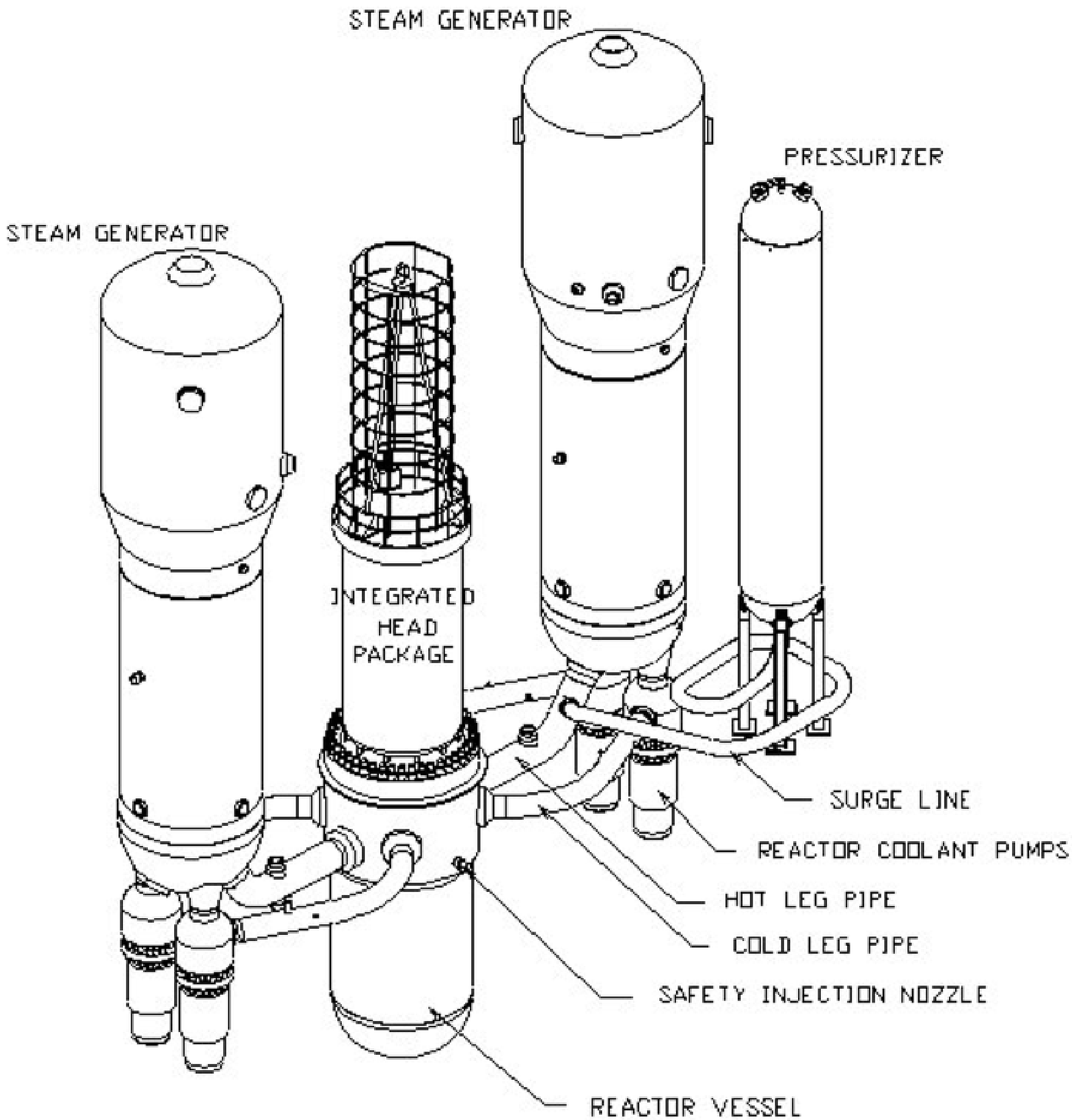

Figure 1.2-1 AP1000 Reactor Coolant System

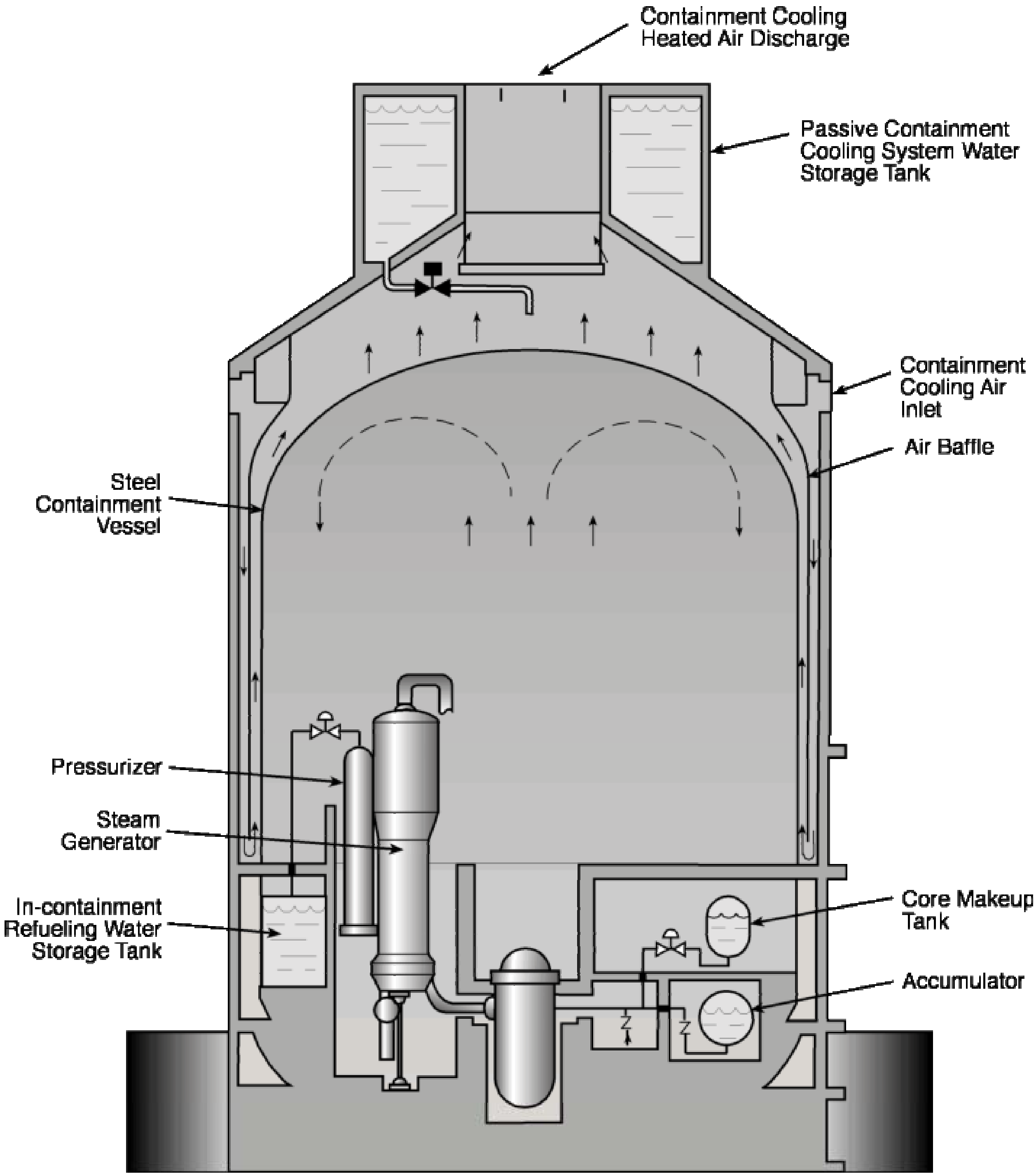

Figure 1.2-2 AP1000 Passive Safety Injection System Post-LOCA, Long Term Cooling

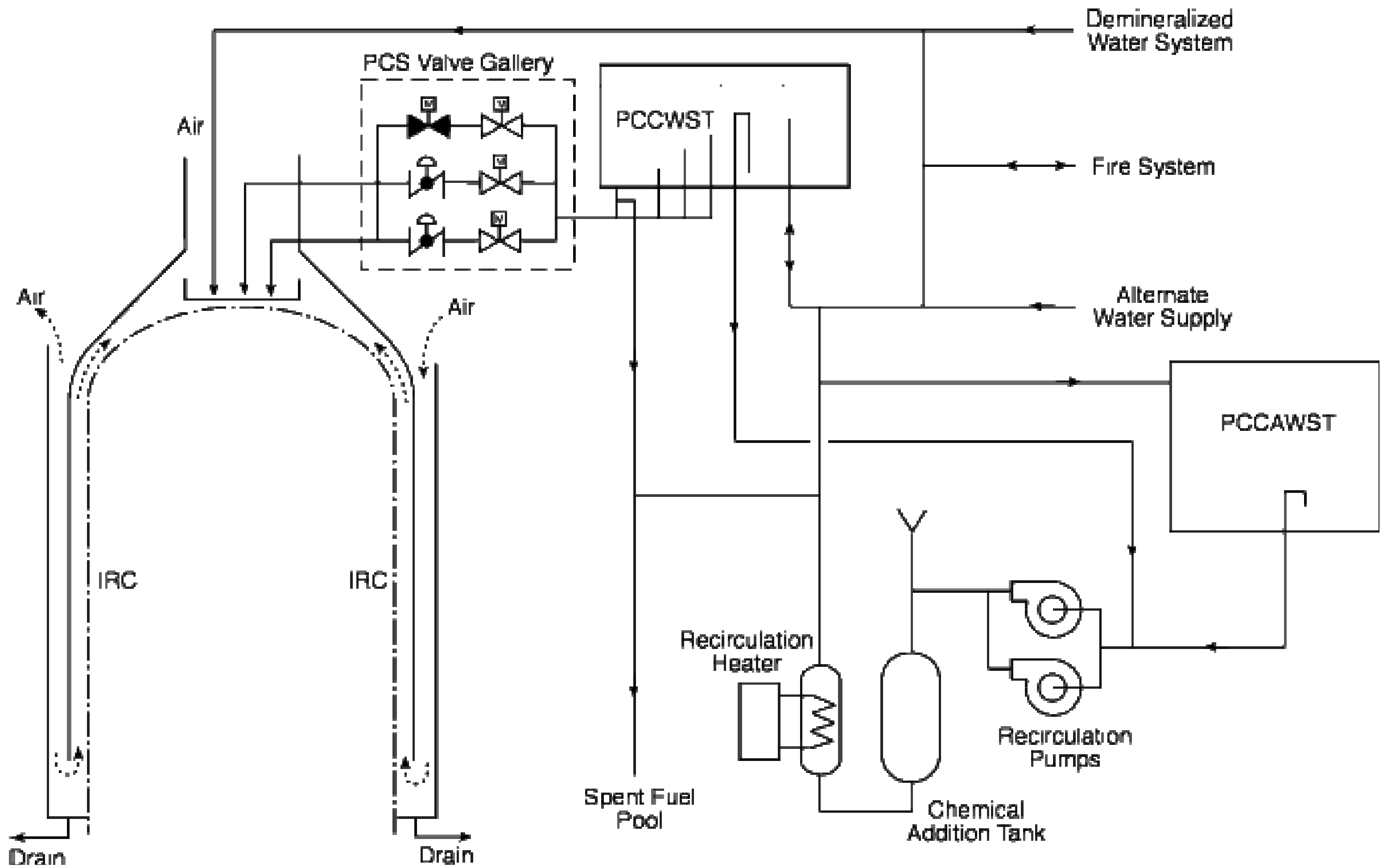

Figure 1.2-3 AP1000 Passive Containment Cooling System

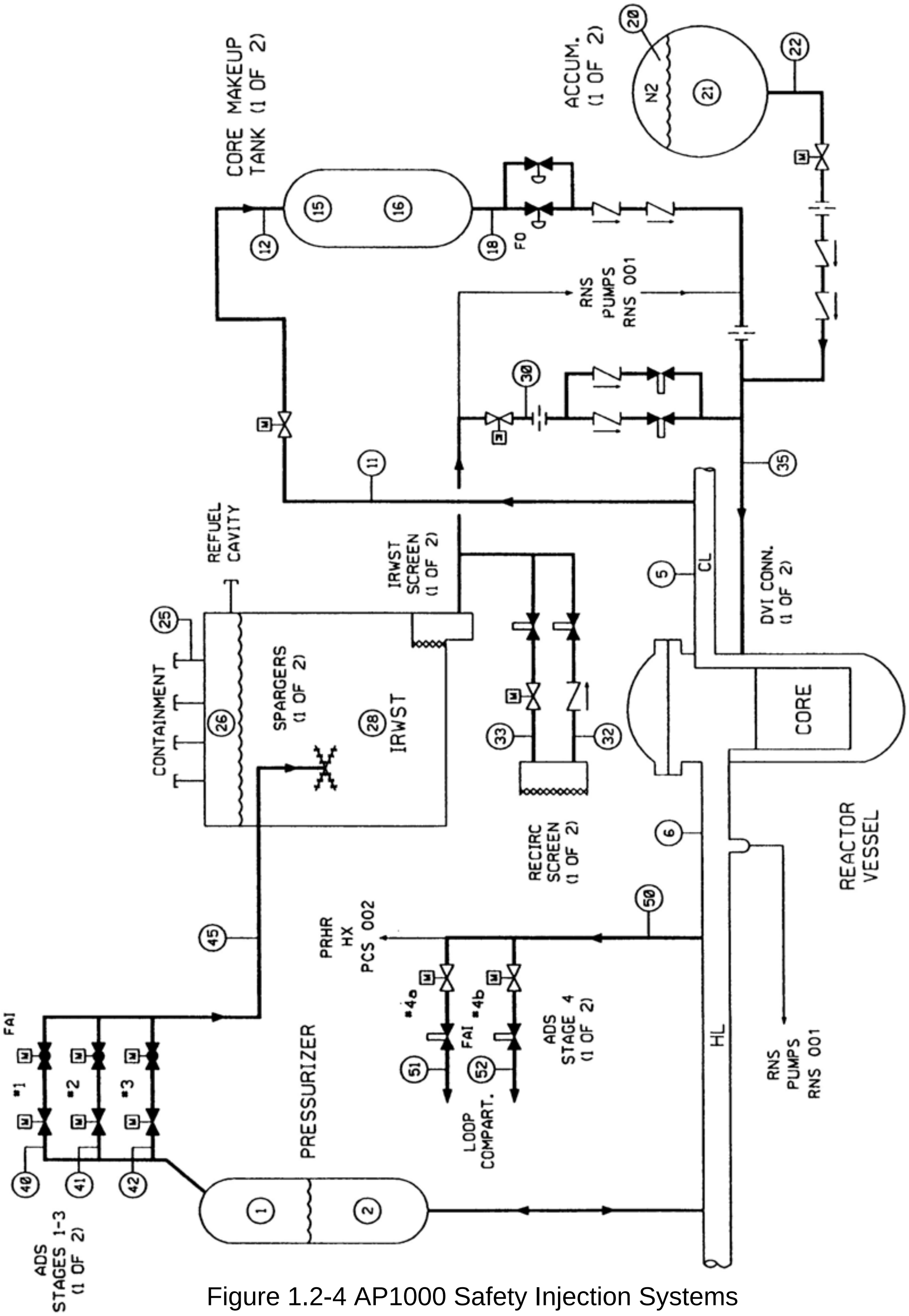

Figure 1.2-4 AP1000 Safety Injection Systems

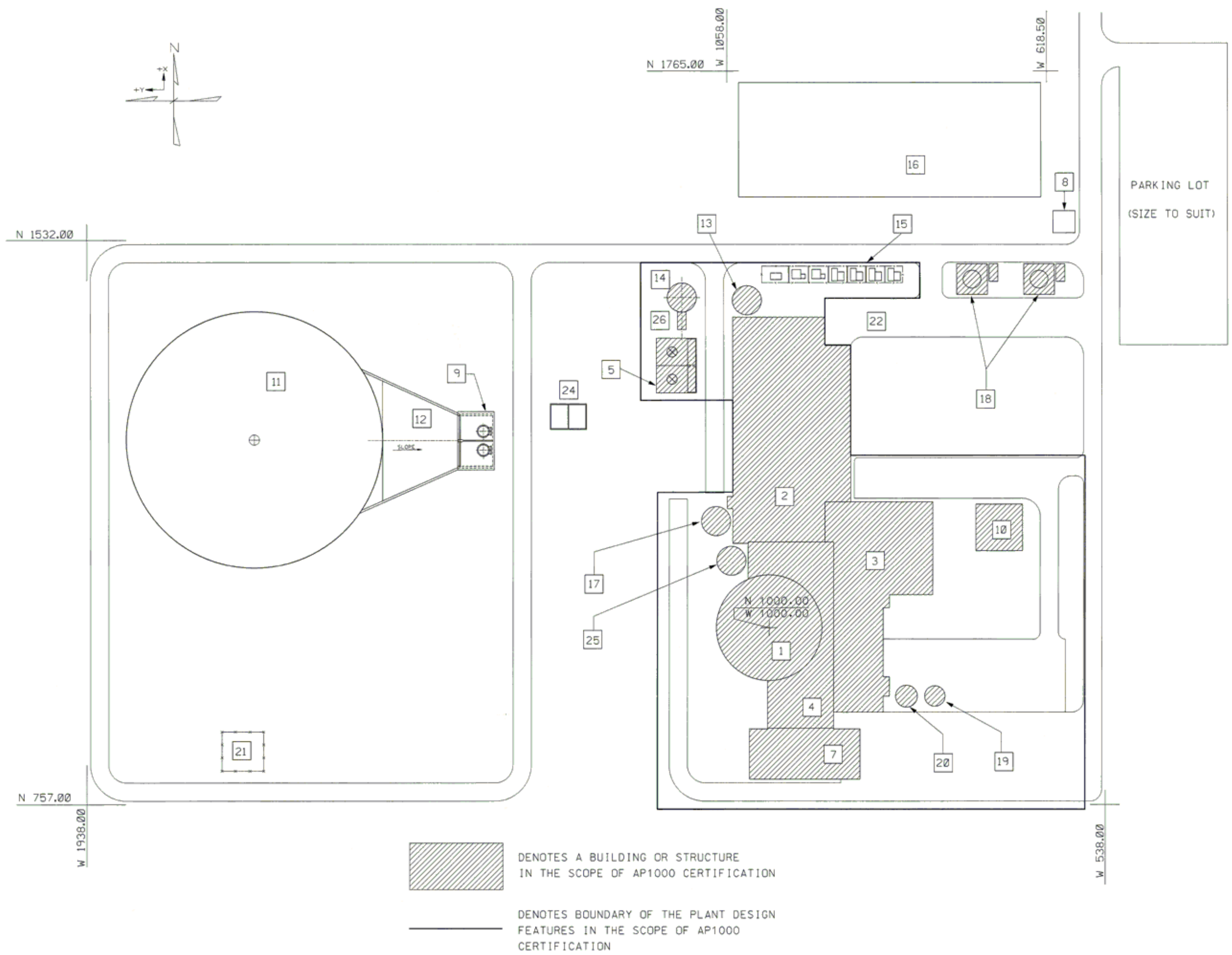

Figure 1.2-5
Layout

AP1000 Plant
(Sheet 1 of 2)

Figure 1.2-5 AP1000 Plant Layout
(Sheet 2 of 2)

1. Containment/Shield Building
2. Turbine Building
3. Annex Building
4. Auxiliary Building
5. Service Water System Cooling Towers
7. Radwaste Building
8. Plant Entrance
9. Circulating Water Pump Intake Structure
10. Diesel Generator Building
11. Circulating Water System Cooling Tower
12. Circulating Water System Intake Canal
13. Fire Water/Clearwell Storage Tank
14. Fire Water Storage Tank
15. Transformer Area
16. Switchyard
17. Condensate Storage Tank
18. Diesel Generator Fuel Oil Storage Tank
19. Demineralized Water Storage Tank
20. Boric Acid Storage Tank
21. Hydrogen Storage Tank Area
22. Turbine Building Laydown Area
24. Waste Water Retention Basin
25. Passive Containment Cooling Ancillary Water Storage Tank
26. Diesel-Driven Fire Pump/Enclosure