Chapter 3 Design of Structures, Components, Equipment and Systems

3.1 Conformance with Nuclear Regulatory Commission General Design Criteria

This section discusses the extent to which the AP1000 design criteria for safety-related structures, systems, and components comply with 10 CFR 50, Appendix A. As presented in this section, each criterion is first quoted and then discussed. For some criteria, the AP1000 advanced passive design features are deemed to be significantly different in certain specific areas from those design features considered when the General Design Criteria were formulated. In those instances, the means by which the AP1000 design complies with the intent of the General Design Criterion is indicated. Where additional information is required for a complete discussion, the appropriate Design Control Document (DCD) sections are referenced.

3.1.1 Overall Requirements

Criterion 1 – Quality Standards and Records

Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety function to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified, as necessary, to assure a quality product, in keeping with the required safety function.

A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

AP1000 Compliance

The Quality Assurance Program for the AP1000 provides confidence that safety-related items and services are designed, procured, fabricated, inspected, and tested to quality standards commensurate with the safety-related functions to be performed. This program also applies to design services subcontracted to external organizations. The quality assurance program for erection of structures, systems, and components will be identified before the construction phase of the AP1000 project. The AP1000 quality assurance program is described in Chapter 17, including its compliance with ASME NQA-1.

Design, procurement, fabrication, inspection, and testing are performed according to recognized codes, standards, and design criteria that comply with the requirements of 10 CFR 50.55a. As necessary, supplemental standards, design criteria, and requirements are developed by the AP1000 designers. A portion of the chemical and volume control system that is defined as reactor coolant pressure boundary uses an alternate classification in conformance with the requirements of 10 CFR 50.55a(a)(3). The alternate classification is discussed in Subsection 5.2.1.3.

Appropriate records documenting that design, procurement, fabrication, inspection, and testing comply with the applicable codes, standards, and design criteria are maintained according to appropriate, applicable laws and regulations, either by or under the control of the Combined License applicant.

In the passive AP1000 design, systems necessary to provide the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, and the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures

comparable to the guideline exposures of 10 CFR 50.34 are classified as safety-related. Therefore, the AP1000 complies with the intent of Criterion 1.

The principal design criteria, design bases, codes, and standards applied to the facility are identified in Section 3.2. Additional details may be found in the pertinent sections dealing with safety-related structures, systems, and components.

Criterion 2 – Design Bases for Protection Against Natural Phenomena

Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without the loss of the capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect: (1) appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena, and (3) the importance of the safety functions to be performed.

AP1000 Compliance

The safety-related structures, systems, and components are designed to withstand the effects of natural phenomena without loss of the capability to perform their safety-related functions, or are designed such that their response or failure will be in a safe condition. Those structures, systems, and components vital to the shutdown capability of the reactor are designed to withstand the maximum probable natural phenomena at the intended site.

Accident analyses consider conservative site conditions that envelope expected sites. Appropriate combinations of structural loadings from normal, accident, and natural phenomena are considered in the plant design. The design of the plant in relationship to those natural phenomena is addressed.

Seismic and quality group classifications and other pertinent standards and information are given in the sections discussing individual structures, systems, and components as well as in Chapter 3. The nature and magnitude of the natural phenomena considered in the design of this plant are discussed in Chapter 2.

Criterion 3 – Fire Protection

Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Noncombustible and heat-resistant materials shall be used wherever practical throughout the unit, particularly in locations such as the containment and control room. Fire detection and fighting systems of appropriate capacity and capability shall be provided and designed to minimize the adverse effects of fires on structures, systems, and components important to safety. Fire fighting systems shall be designed to assure that their rupture or inadvertent operation does not significantly impair the safety capability of these structures, systems, and components.

AP1000 Compliance

The safety-related structures, systems, and components are designed to minimize the probability and effect of fires and explosions. Noncombustible and fire-resistant materials are used in the containment and main control room. Additionally noncombustible and fire-resistant materials are used on components of safety-related systems, and elsewhere in the plant where fire is a potential risk to safety-related systems.

For example, electrical cables have a fire-retardant jacketing, and fire barriers are used at fire area boundaries. The AP1000 design approach includes designing the safety-related systems with redundant divisions, and locating these redundant divisions in separate safety-related areas.

Equipment and facilities for fire protection, including detecting, alarming, and extinguishing functions, are provided to help protect both plant equipment and personnel from fire, explosion, and the resultant release of toxic vapors. Fire protection is provided by deluge systems (water spray), sprinklers, and portable extinguishers. Fire fighting systems are designed so that their rupture or inadvertent operation will not prevent safety-related systems from performing their design functions.

The following codes, guides, and standards are used as guidelines in the design of the fire protection system and equipment. The system and equipment conform to the applicable portions of the following documents:

- National Fire Protection Association Codes and Standards
- BTP-CMEB 9.5-1, "Guidelines for Fire Protection for Nuclear Power Plants," July 1981

Subsection 9.5.1 describes the AP1000 fire protection system and equipment, including conformance with the applicable portions of these codes and standards and reference to specific fire protection codes and standards.

Criterion 4 – Environmental and Missile Design Bases

Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit. However, dynamic effects associated with postulated pipe ruptures in nuclear power units may be excluded from the design basis when analyses reviewed and approved by the Commission demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping.

AP1000 Compliance

Safety-related structures, systems, and components are designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss of coolant accidents.

The AP1000 design has emphasized the minimization of missiles, pipe whip, and fluid discharge by a combination of separation of safe shutdown components and design to prevent the dynamic effects of postulated pipe ruptures based on the application of the leak-before-break approach. This analysis is discussed in Subsection 3.4.3.5 and Section 3.6.

The AP1000 structures, systems, and components are appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit. Details of the design, environmental testing, and construction of these structures, systems, and components are given in the sections that discuss individual structures, systems, and components, as well as in Sections 3.5 and 3.6.

Criterion 5 – Sharing of Structures, Systems, and Components

Structures, systems, and components important to safety shall not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and cooldown of the remaining unit.

AP1000 Compliance

The AP1000 is a single-unit plant. If more than one unit were built on the same site, none of the safety-related systems would be shared.

3.1.2 Protection by Multiple Fission Product Barriers

Criterion 10 – Reactor Design

The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.

AP1000 Compliance

The reactor core and associated coolant, control, and protection systems are designed to the following criteria:

- No fuel damage occurs during normal core operation and operational transients (Condition I) or during transient conditions arising from occurrences of moderate frequency (Condition II). For normal operation, the plant is designed to accommodate a fuel defect level of up to 0.25 percent. Fuel damage, as used here, is defined as penetration of the fission product barrier, that is, the fuel rod cladding. The small number of clad defects that may occur are within the capability of the plant cleanup system and are consistent with the plant design bases. For additional information see Section 11.1.

- The reactor can be returned to a safe shutdown state following a Condition III event, with only a small fraction of the fuel rods damaged, although sufficient fuel damage might occur to preclude the immediate resumption of operation.

- The core remains intact with acceptable heat transfer geometry following transients arising from occurrences of limiting faults (Condition IV).

The reactor protection system is designed to actuate a reactor trip whenever necessary to prevent exceeding the fuel design limits. The core design, together with the process and decay heat removal systems, provide this capability under expected conditions of normal operation, with appropriate margins for uncertainties and anticipated transient situations. This includes the effects of the loss of reactor coolant flow, trip of the turbine generator, loss of normal feedwater, and loss of both normal and preferred power sources.

Chapter 4, Reactor, describes the mechanical components of the reactor and reactor core, including the fuel rods and fuel assemblies, the mechanical design, nuclear design, and the thermal hydraulic design. Chapter 7 provides details of the control and protection systems instrumentation design and logic. This information supports the accident analyses documented in Chapter 15. The acceptable fuel design limits are not exceeded for Condition I and II events. Acceptable core cooling is provided for Condition III and IV events.

Criterion 11 – Reactor Inherent Protection

The reactor core and associated coolant systems shall be designed so that in the power-operating range the net effect of the prompt inherent nuclear feedback characteristics tends to compensate for a rapid increase in reactivity.

AP1000 Compliance

When the reactor is critical, the negative fuel temperature reactivity effects (Doppler feedback) provide prompt reactivity feedback to compensate for a rapid, uncontrolled reactivity excursion. The negative Doppler coefficient of reactivity is provided by the use of a low-enrichment fuel design. This Doppler feedback is the primary reactivity feedback mechanism to provide the inherent core reactivity protection during rapid core reactivity excursions.

For slower reactivity transients that result in moderator temperature increases, the nonpositive moderator temperature coefficient of reactivity provides compensatory reactivity feedback to help control these slower transients. The overall core design establishes a nonpositive moderator temperature coefficient of reactivity.

Chapter 4 provides information pertaining to the core design.

Criterion 12 – Suppression of Reactor Power Oscillations

The reactor core and associated coolant, control, and protection systems shall be designed to assure that power oscillations which can result in conditions exceeding specified acceptable fuel design limits are not possible or can be reliably and readily detected and suppressed.

AP1000 Compliance

Power oscillations of the fundamental mode are inherently eliminated by negative Doppler and nonpositive moderator temperature coefficients of reactivity.

Oscillations, due to xenon spatial effects, in the radial and azimuthal overtone modes are heavily damped because of the inherent design and due to the negative Doppler and nonpositive moderator temperature coefficients of reactivity.

Oscillations due to xenon spatial effects may occur in the axial first overtone mode. Reactor trip functions are provided, using the measured axial power imbalance as an input, so that the fuel design limits are not exceeded during axial xenon oscillations.

If it is necessary to maintain axial imbalance within the limits (that is, imbalances that are alarmed to the operator and are within the imbalance trip setpoints), the operator can suppress axial xenon oscillations by control rod motions or temporary power reductions or both.

Oscillations due to spatial xenon effects, in axial modes higher than the first overtone, are heavily damped because of the inherent design and the negative Doppler coefficient of reactivity.

The stability of the core against xenon-induced power oscillations and the functional requirements of instrumentation for monitoring and measuring core power distribution are discussed in Chapter 4. Details of the instrumentation design and logic are discussed in Chapter 7.

Criterion 13 – Instrumentation and Control

Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its

associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

AP1000 Compliance

Instrumentation and controls are provided to monitor and control neutron flux, control rod position, fluid temperatures, pressures, flows, and levels, as necessary, to maintain plant safety. Instrumentation is provided in the reactor coolant system, steam and power conversion system, containment, engineered safety systems, radioactive waste management systems, and other auxiliary systems.

See Section 7.5 for a discussion of indications that are required for operator use under normal operating and accident conditions. Criteria regarding layout of the controls and displays are provided in Chapter 18.

The quantity and types of process instrumentation used provide safe and orderly operation of systems over the design range of plant operations, including accident conditions.

Criterion 14 – Reactor Coolant Pressure Boundary

The reactor coolant pressure boundary shall be designed, fabricated, erected, and tested so as to have an extremely low probability of abnormal leakage, of rapidly propagating failure, and of gross rupture.

AP1000 Compliance

The reactor coolant pressure boundary is designed to accommodate the system pressures and temperatures attained under the expected modes of plant operation, including anticipated transients, while maintaining stresses within applicable limits. Consideration is given to loadings under normal operating conditions and to abnormal loadings, such as seismic loadings. The piping is protected from overpressure by means of pressure-relieving devices, as required by ASME Code, Section III. See Subsection 5.2.2 for additional information.

Reactor coolant pressure boundary materials and fabrication techniques are such that there is a low probability of gross rupture or significant leakage. The AP1000 reactor coolant system design incorporates revised pipe-break criteria (leak-before-break) to reduce or eliminate the need to consider the dynamic effects of pipe breaks. The configuration and materials of the reactor coolant system have been selected such that the pipe stresses meet the leak-before-break criteria. See Subsection 3.6.3 for additional information.

The AP1000 reactor core and reactor internals are designed to limit neutron fluence on the reactor vessel. See Section 5.4 and Chapter 4 for additional information.

The reactor vessel is manufactured from low-alloy carbon steel clad with 308L stainless steel weld overlay on wetted surfaces. The vessel shell is constructed of ring-rolled forgings that eliminate vertical weld seams. Chemical composition of the forging material is controlled to improve radiation resistance of the vessel. (See Criterion 31 for further discussion of the reactor coolant pressure boundary.)

Coolant chemistry is controlled to protect the materials of construction of the reactor coolant pressure boundary from corrosion. See Subsection 5.2.3 for additional information.

The reactor coolant pressure boundary welds are accessible for in-service inspections to assess structural and leaktight integrity. For the reactor vessel, a material surveillance program is provided. Instrumentation is provided to detect significant leakage from the reactor coolant pressure boundary, with indication in the main control room. See Subsection 5.2.4 for additional information.

A portion of the chemical and volume control system that is defined as reactor coolant pressure boundary is nonsafety-related. This portion of the system is capable of being automatically isolated by safety-related valves that are designed and qualified for the design requirements.

Criterion 15 – Reactor Coolant System Design

The reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during normal operation, including anticipated operational occurrences.

AP1000 Compliance

Steady-state and transient analyses are performed to demonstrate that reactor coolant system design conditions are not exceeded during normal operation. Protection and control setpoints are based on these analyses. See Chapter 15 for additional information.

The reactor coolant system stress analysis and the leak-before-break analyses are described in Appendices 3B and 3C. See Section 5.3 for additional information.

Two safety valves are provided for the reactor coolant system. These valves and their setpoints meet the ASME Code, Section III criteria for overpressure protection. See Subsection 5.2.2 for additional information.

Criterion 16 – Containment Design

The reactor containment and associated systems shall be provided to establish an essentially leak-tight barrier against the uncontrolled release of radioactivity to the environment and to assure that the containment design conditions important to safety are not exceeded for as long as postulated accident conditions require.

AP1000 Compliance

The containment is an integral part of the overall containment system, whose function is to contain the release of airborne radioactivity following postulated design basis accidents and to provide shielding for the reactor core and the reactor coolant system during normal operations. The containment consists of a steel containment vessel and is surrounded by a concrete shield building.

The containment vessel, which is a free-standing steel shell, is an integral part of the passive containment cooling system, whose function is to provide the safety-related ultimate heat sink for the removal of the reactor coolant system sensible heat, core decay heat, and stored energy. The containment vessel and the passive containment cooling system are designed to remove sufficient energy from the containment to prevent the containment from exceeding its design pressure following postulated design basis accidents.

The containment is designed to house the reactor coolant system and other related systems. The containment vessel functions as an essentially leaktight barrier. It is protected against postulated missiles from external sources as well as missiles produced by internal equipment failures.

Containment penetrations are isolated according to the provisions of GDCs 54, 55, 56, and 57.

Criterion 17 – Electrical Power Systems

An onsite electric power system and an offsite electric power system shall be provided to permit functioning of structures, systems, and components important to safety. The safety function for each system (assuming that the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational

occurrences and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents.

The onsite electric power supplies, including the batteries, and the onsite electric distribution system shall have sufficient independence, redundancy, and testability to perform their safety functions, assuming a single failure.

Electric power from the transmission network to the onsite electric distribution system shall be supplied by two physically independent circuits (not necessarily on separate rights-of-way) designed and located so as to minimize, to the extent practical, the likelihood of their simultaneous failure under operating and postulated accident and environmental conditions. A switchyard common to both circuits is acceptable. Each of these circuits shall be designed to be available in sufficient time, following a loss of all onsite alternating current power supplies and other offsite electric power circuit, to assure that specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded. One of these circuits shall be designed to be available within a few seconds following a loss of coolant accident to assure that core cooling, containment integrity, and other vital safety functions are maintained.

Provisions shall be included to minimize the probability of losing electric power from any of the remaining supplies as a result of, or coincident with, the loss of power generated by the nuclear power unit, the loss of power from the transmission network, or the loss of power from the onsite electric power supplies.

AP1000 Compliance

The AP1000 plant design supports an exemption to the requirement of GDC 17 for two physically independent offsite circuits by providing safety-related passive systems for core cooling and containment integrity, and multiple nonsafety-related onsite and offsite electric power sources for other functions. See Section 6.3 for additional information on the systems for core cooling.

A reliable dc power source supplied by batteries provides power for the safety-related valves and instrumentation during transient and accident conditions.

The Class 1E dc and UPS system is the only safety-related power source required to monitor and actuate the safety-related passive systems. Otherwise, the plant is designed to maintain core cooling and containment integrity, independent of nonsafety-related ac power sources indefinitely. The only electric power source necessary to accomplish these safety-related functions is the Class 1E dc and UPS power system which includes the associated safety-related 120V ac distribution switchgear.

Although the AP1000 is designed with reliable nonsafety-related offsite and onsite ac power that are normally expected to be available for important plant functions, nonsafety-related ac power is not relied upon to maintain the core cooling or containment integrity.

The nonsafety-related ac power system is designed such that plant auxiliaries can be powered from the grid under all modes of operation. During loss of offsite power, the ac power is supplied by the onsite standby diesel-generators. Preassigned loads and equipment are automatically loaded on the diesel-generators in a predetermined sequence. Additional loads can be manually added as required. The onsite standby power system is not required for safe shutdown of the plant.

Criterion 18 – Inspection and Testing of Electric Power Systems

Electric power systems important to safety shall be designed to permit appropriate periodic inspection and testing of important areas and features, such as wiring, insulation, connections, and switchboards, to assess the continuity of the systems and the condition of their components. The systems shall be designed with a capability to test periodically (1) the operability and functional

performance of the components of the systems, such as onsite power sources, relays, switches, and buses, and (2) the operability of the systems as a whole and, under conditions as close to design as practical, the full operation sequence that brings the systems into operation, including operation of applicable portions of the protection system, and the transfer of power among the nuclear power unit, the offsite power system, and the onsite power system.

AP1000 Compliance

The AP1000 is designed so that only the Class 1E dc and UPS system is required in order to initiate and actuate the systems necessary for maintaining core cooling and containment integrity. The safety-related dc power system design complies with GDC 18. Compliance with GDC 18 is achieved by designing testability and inspection capability into the system. The associated testing requirements are contained in Chapter 16.

Criterion 19 – Control Room

A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss of coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent, to any part of the body, for the duration of the accident.

Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

AP1000 Compliance

The AP1000 main control room provides the man-machine interfaces required to operate the plant safely and efficiently under normal conditions and to maintain it in a safe manner under accident conditions, including LOCAs. Simplified passive safety-related system designs are provided that do not rely upon operator action to maintain core cooling for design basis accidents. Operator action outside the main control room to mitigate the consequences of an accident is permitted.

The main control room is shielded by the containment and auxiliary building from direct gamma radiation and inhalation doses resulting from the postulated release of fission products inside containment. Refer to Chapter 15 for additional information on accident conditions. The main control room/control support area HVAC subsystem of the nuclear island nonradioactive ventilation system (VBS) allows access to and occupancy of the main control room under accident conditions as described in Subsection 9.4.1. Sufficient shielding and the main control room/control support area HVAC subsystem provide adequate protection so that personnel will not receive radiation exposure in excess of 5 rem whole-body or its equivalent to any part of the body for the duration of the accident.

If ac power is unavailable for more than 10 minutes or if "high-high" particulate, low pressurizer pressure is detected, or iodine radioactivity is detected in the main control room supply air duct, which would lead to exceeding General Design Criteria 19 operator dose limits, the protection and safety monitoring system automatically isolates the main control room and operator habitability requirements are then met by the main control room emergency habitability system (VES). The main control room emergency habitability system also allows access to and occupancy of the main control room under accident conditions. The emergency main control room habitability system is designed to satisfy seismic Category I requirements as described in Section 3.2; the system design is described in Section 6.4.

In the event that the operators are forced to abandon the main control room, a workstation is provided with remote shutdown capability. A main control room evacuation is not assumed to occur simultaneously with design basis events. The remote shutdown workstation is described in Section 7.4.

3.1.3 Protection and Reactivity Control Systems

Criterion 20 – Protection System Functions

The protection system shall be designed (1) to initiate automatically the operation of appropriate systems, including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.

AP1000 Compliance

The protection system is a microprocessor-based system that trips the reactor and actuates engineered safety features when predetermined limits are exceeded or when manually initiated.

The reactor trip portion of the protection system includes four independent, redundant, physically separated, electrically-isolated divisions. The coincidence circuits guard against the loss of protection or the generation of false protection signals due to equipment failures through the use of a two-out-of-four logic and built-in operational bypasses.

Independent, redundant, physically separated, electrically-isolated engineered safety features trains are provided. Signal conditioning for the plant sensors is provided.

See Chapter 7 for additional information concerning the design of the protection system.

Criterion 21 – Protection System Reliability and Testability

The protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (I) no single failure results in the loss of the protection function and (2) removal from service of any component or channel does not result in the loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

AP1000 Compliance

The protection system is designed for functional reliability and in-service testability. The design employs redundant logic trains and measurement and equipment diversity.

The protection system equipment includes integral testing circuits. System equipment, from input to output, in the protection cabinets and the engineered safety features cabinets, is tested. Simulated inputs replace the field signals. Outputs are monitored for validity. Manual and automatic testing is used to test the final stages of the reactor trip circuits and the reactor trip switchgear. Testing of cabinets and communications links verifies the functional operation of the equipment and the hardware. See Chapter 7 for further information concerning the test capabilities of the protection system.

Criterion 22 – Protection System Independence

The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels

do not result in the loss of the protection function or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

AP1000 Compliance

Design of the protection systems includes consideration of natural phenomena, normal maintenance, testing, and accident conditions so that the protection functions are available.

Protection system components are designed, arranged, and qualified for operation in the environment accompanying any emergency situation in which the components are required to function.

Functional diversity has been designed into the system. The extent of this functional diversity is demonstrated for a variety of postulated accidents. Diverse protection functions automatically serve to mitigate the consequences of an event. Chapter 15 identifies the primary and diverse protective functions for each of the analyzed events.

Sufficient redundancy and independence are designed into the protection systems so that no single failure or removal from service of any component or channel of a system results in loss of the protection function. Functional diversity and location diversity are designed into the system.

Automatic reactor trip is initiated by neutron flux measurements, reactor coolant system overtemperature delta-T, reactor coolant system overpower delta-T, pressurizer pressure and level measurements, reactor coolant flow, reactor coolant pump speed, reactor coolant pump bearing water temperature, and steam generator water level measurements. Trips may also be initiated manually or by a safety injection signal.

For additional information pertaining to the reactor trip logic, see Section 7.2.

High-quality components, conservative design and quality control, inspection, calibration, and tests are used to guard against common-mode failure. Qualification testing and analysis are performed on the safety-related systems to demonstrate functional operation at normal and post-accident conditions of temperature, humidity, pressure, and radiation for specified periods, as required. Typical protection system equipment is subjected to type tests under simulated seismic conditions, using conservatively large accelerations and applicable frequencies.

See Section 7.1 for additional information concerning the equipment design of the protection and safety monitoring system.

See Sections 3.10 and 3.11 for information pertaining to environmental and seismic qualification of the protection system equipment.

The AP1000 includes a nonsafety-related diverse actuation system. The diverse actuation system provides specific automatic functions including control rod insertion, turbine trip, passive residual heat removal heat exchanger actuation, core makeup tank actuation, isolation of critical containment lines, and passive containment cooling system actuation. This system is diverse and independent from the reactor protection system from sensors up to the actuation devices.

See Section 7.7 for additional information concerning the diverse actuation system.

Criterion 23 – Protection System Failure Modes

The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air) or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.

AP1000 Compliance

The protection system is designed considering the most probable failure modes of the components under various perturbations of the environment and energy sources. Reactor trip channels are designed on the deenergize-to-trip principle so that a single event (that is, loss of power) that could affect many functions at the same time causes the channels to actuate to their tripped conditions.

Criterion 24 – Separation of Protection and Control Systems

The protection system shall be separated from the control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems, leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

AP1000 Compliance

The protection system is separate and distinct from the control systems. Control systems are, in some cases, dependent on the protection system for control signals that are derived from protection system measurements, where applicable. These signals are transferred to the control system by isolation devices classified as protection components.

The adequacy of the system isolation is verified by testing under conditions of postulated credible faults. The failure of a single control system component or channel, or the failure or removal from service of a single protection system component or channel common to the control and protection system, leaves intact a system that satisfies the requirements of the protection system. The removal of a protection division from service is allowed during testing of the division.

Criterion 25 – Protection System Requirements for Reactivity Control Malfunctions

The protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of the control rods.

AP1000 Compliance

The protection system is designed to limit reactivity transients so that the fuel design limits are not exceeded. Reactor shutdown by control rod insertion is independent of the normal control functions since the trip breakers interrupt power to the rod mechanisms regardless of existing control signals. Thus, in the postulated accidental withdrawal of a control rod or control rod bank (assumed to be initiated by a control malfunction), neutron flux, temperature, pressure, level, and flow signals would be generated independently. Any of these signals (trip demands) would operate the breakers to trip the reactor.

The AP1000 is designed to automatically terminate a boron dilution during manual or automatic operation at power, and also during startup and shutdown conditions. See Chapter 7 for a discussion of the signals used in the logic to terminate a boron dilution. Subsection 9.3.6.4.5 discusses the chemical and volume control system design features for addressing boron dilution. The Chapter 15 safety analyses demonstrate that fuel design limits are not exceeded.

Criterion 26 – Reactivity Control System Redundancy and Capability

Two independent reactivity control systems of different design principles shall be provided. One of the systems shall use control rods, preferably including a positive means for inserting the rods, and shall be capable of reliably controlling reactivity changes to assure that under conditions of normal operation, including anticipated operational occurrences, and with appropriate margin for malfunctions such as stuck rods, specified acceptable fuel design limits are not exceeded. The second reactivity control system shall be capable of reliably controlling the rate of reactivity changes resulting from planned, normal power changes (including xenon burnout) to assure that the acceptable fuel design limits are not exceeded. One of the systems shall be capable of holding the reactor core subcritical under cold conditions.

AP1000 Compliance

Two reactivity control systems are provided. These are rod cluster control assemblies and gray rod assemblies, and chemical shim (boric acid). The rod cluster control and gray rod assemblies are inserted into the core by the force of gravity.

During operation, the shutdown rod banks are fully withdrawn. The control rod system automatically maintains a programmed average reactor temperature compensating for reactivity effects associated with scheduled and transient load changes. See Section 4.3 for additional information.

The shutdown and control rod banks are designed to provide reactivity margin to shut down the reactor during normal operating conditions and during anticipated operational occurrences, without exceeding specified fuel design limits. The safety analyses assume the most restrictive time in the core operating cycle and that the most reactive control rod cluster assembly is in the fully withdrawn position. See Chapter 15 for summaries of the analyses, assumptions, and results.

The safety-related passive systems provide the required boration to establish and maintain safe shutdown condition for the reactor core. See Section 6.3 for additional information.

Criterion 27 – Combined Reactivity Control Systems Capability

The reactivity control systems shall be designed to have a combined capability, in conjunction with poison addition by the emergency core cooling system, of reliably controlling reactivity changes to assure that under postulated accident conditions and with appropriate margin for stuck rods the capability to cool the core is maintained.

AP1000 Compliance

The plant is provided with the means of making and holding the core subcritical under any anticipated conditions and with appropriate margin for contingencies. Combined use of the control rod and the chemical shim control system permits the necessary shutdown margin to be maintained during long-term xenon decay and plant cooldown. The single highest worth control rod assembly is assumed to be stuck in the fully withdrawn position for this determination.

Criterion 28 – Reactivity Limits

The reactivity control systems shall be designed with appropriate limits on the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents can neither (l) result in damage to the reactor coolant pressure boundary greater than limited local yielding nor (2) sufficiently disturb the core, its support structures, or other reactor pressure vessel internals to impair significantly the capability to cool the core. These postulated reactivity accidents shall include consideration of rod ejection (unless prevented by positive means), rod dropout, steam line rupture, changes in reactor coolant temperature and pressure, and cold water addition.

AP1000 Compliance

The maximum reactivity worth of the control rods and the maximum rates of reactivity increase employing control rods and boron removal are limited by design and operating procedures.

The appropriate reactivity addition rate for the withdrawal of control rods and the dilution rate of the boric acid in the reactor coolant system are specified in the precautions, limitations, and setpoint document and the control system setpoint study. Technical specifications explicitly specify control rod bank alignment and insertion limits in addition to shutdown margin reactivity requirements.

The control rod reactivity addition rate is determined by the allowable rod control system withdrawal speed, in conjunction with the control rod worth, which varies throughout the operating cycle. The capability to change boron concentration is determined by the various plant systems that provide makeup to the reactor coolant system. The reactivity insertion rates, rod withdrawal limits, and boron dilution limits are discussed in Chapter 4.

Core cooling capability following events such as rod ejection and steam line breaks is provided by keeping the reactor coolant pressure boundary stresses within faulted condition limits, as specified by applicable ASME codes. Structural deformations are also checked and limited to values that do not jeopardize the operation of needed safety-related features.

Criterion 29 – Protection Against Anticipated Operational Occurrences

The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.

AP1000 Compliance

The protection and reactivity control systems have an extremely high probability of performing their required safety-related functions in the event of anticipated operational occurrences. High-quality equipment, diversity, and redundancy, support this probability. Loss of power to the protection system results in a reactor trip. Defense in depth is designed into AP1000 to reduce challenges to the protection and reactivity control systems.

3.1.4 Fluid Systems

Criterion 30 – Quality of Reactor Coolant Pressure Boundary

Components which are part of the reactor coolant pressure boundary shall be designed, fabricated, erected, and tested to the highest quality standards practical. Means shall be provided for detecting and, to the extent practical, identifying the location of the source of reactor coolant leakage.

AP1000 Compliance

Reactor coolant pressure boundary components are designed, fabricated, inspected, and tested in conformance with the ASME Code, Section III. A portion of the chemical and volume control system that is defined as reactor coolant pressure boundary uses an alternate classification in conformance with the requirements of 10 CFR 50.55a(a)(3). The alternate classification is discussed in Section 5.2.

Leakage detection monitoring is accomplished using instrumentation and other components of several systems. See Subsection 5.2.5 for additional information. Reactor coolant pressure boundary leakage is classified as either identified or unidentified leakage.

Auxiliary systems connected to the reactor coolant pressure boundary incorporate design and administrative provisions that limit leakage. Leakage is detected by increasing auxiliary system level,

temperature, flow, or pressure, by lifting of relief valves, or by increasing values of monitored radiation in the auxiliary system.

Leakage from the reactor coolant pressure boundary and other components not otherwise identified inside the containment will condense and flow by gravity via the floor drains and other drains to the containment sump. Leakage is indicated by an increase in the sump level.

Reactor coolant system inventory monitoring provides an indication of system leakage. The reactor coolant system inventory balance is a quantitative inventory or mass balance calculation.

Leakage from the reactor coolant pressure boundary will result in an increase in the radioactivity levels inside containment. The containment atmosphere is monitored for airborne gaseous radioactivity and F18 particulate. From the concentration of F18 particulate and the power level, reactor coolant pressure boundary leakage can be estimated.

Criterion 31 – Fracture Prevention of Reactor Coolant Pressure Boundary

The reactor coolant pressure boundary shall be designed with sufficient margin to assure that when stressed under operating, maintenance, testing, and postulated accident conditions (l) the boundary behaves in a nonbrittle manner and (2) the probability of rapidly propagating fracture is minimized. The design shall reflect consideration of service temperatures and other conditions of the boundary material under operating, maintenance, testing, and postulated accident conditions and the uncertainties in determining (l) material properties, (2) the effects of irradiation on material properties, (3) residual, steady state, and transient stresses, and (4) size of flaws.

AP1000 Compliance

Control is maintained over material selection and fabrication for the reactor coolant pressure boundary components so that the boundary behaves in a nonbrittle manner. The portion of the chemical and volume control system that uses an alternate classification is not required to meet the requirements to prevent brittle failure. The reactor coolant pressure boundary materials exposed to the coolant are corrosion-resistant stainless steel or nickel-chromium-iron alloy. The nil-ductility transition reference temperature of the reactor vessel structural steel is established by Charpy V-notch and drop weight tests in accordance with 10 CFR 50, Appendix G (Reference 1). See Section 5.3 for additional information.

The following requirements are imposed in addition to those specified by the ASME Code, Section III.

- A 100 percent volumetric ultrasonic shear wave test of reactor vessel plate and a post-hydrotest ultrasonic map of welds in the pressure vessel are required. Cladding bond ultrasonic inspection to more restrictive requirements than those specified in the ASME Code, Section III is also required in order to preclude interpretation problems during in-service inspection.

- In the surveillance programs, the evaluation of the radiation damage is based on pre-irradiation testing of Charpy V-notch and tensile specimens and post-irradiation testing of Charpy V-notch, tensile, and l/2T compact tension specimens. These programs are directed toward evaluation of the effect of radiation on the fracture toughness of reactor vessel steels based on the reference transition temperature approach and the fracture mechanics approach, and are in accordance with ASTM, E-185 (Reference 2).

- Reactor vessel core region material chemistry (copper, phosphorous, and vanadium) is controlled to reduce sensitivity to embrittlement due to irradiation over the life of the plant.

The fabrication and quality control techniques used in the fabrication of the reactor coolant system are governed by ASME Code, Section III requirements.

Allowable pressure-temperature relationships for plant heatup and cooldown rates are calculated using methods derived from the ASME Code, Section III, Appendix G. The approach specifies that the allowable stress intensity factors for vessel-operating conditions do not exceed the reference stress intensity factor for the metal temperature. Operating specifications include conservative margins for predicted changes in the material reference temperatures due to irradiation.

Criterion 32 – Inspection of Reactor Coolant Pressure Boundary

Components which are part of the reactor coolant pressure boundary shall be designed to permit (I) periodic inspection and testing of important areas and features to assess their structural and leak-tight integrity and (2) an appropriate material surveillance program for the reactor pressure vessel.

AP1000 Compliance

The design of the reactor coolant pressure boundary provides accessibility to the internal surfaces of the reactor vessel and most external zones of the vessel, including the nozzle-to-reactor coolant piping welds, the top and bottom heads, and external surfaces of the reactor coolant piping, except for the area of pipe within the primary shield concrete. The inspection capability complements the leakage detection systems in assessing the integrity of the pressure boundary components. The reactor coolant pressure boundary will be periodically inspected under the provisions of the ASME Code, Section XI. Section 5.1 provides the reactor coolant system primary loop drawings. The portion of the chemical and volume control system that uses an alternate classification is constructed to requirements that do not require in-service inspection.

Monitoring of changes in the fracture toughness properties of the reactor vessel core region plates, forgings, weldments, and associated heat-treated zones is performed according to 10 CFR 50, Appendix H. Additionally, samples of reactor vessel plate materials are retained and catalogued in case future engineering development shows the need for further testing.

The material properties surveillance program includes conventional tensile and impact tests and fracture mechanics specimens. The observed shifts in the nil-ductility transition reference temperature of the core region materials with irradiation is used to confirm the allowable limits calculated for operational transients.

The design of the reactor coolant pressure boundary piping provides for accessibility of welds requiring in-service inspection under the provisions of the ASME Code, Section XI. Removable insulation is provided at welds requiring in-service inspection. See Section 5.3 and Subsection 5.2.4 for additional information.

Criterion 33 – Reactor Coolant Makeup

A system to supply reactor coolant makeup for protection against small breaks in the reactor coolant pressure boundary shall be provided. The system safety function shall be to assure that specified acceptable fuel design limits are not exceeded as a result of reactor coolant loss due to leakage from the reactor coolant pressure boundary and rupture of small piping or other small components which are part of the boundary. The system shall be designed to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished using the piping, pumps, and valves used to maintain coolant inventory during normal reactor operation.

AP1000 Compliance

Changes in the reactor coolant volume will be accommodated by the pressurizer level program for normal power changes, including the transition from hot standby to full-power operation and returning to hot standby. In addition, the pressurizer has sufficient volume to accommodate minor reactor coolant system leakage.

Safety-related passive reactor coolant system makeup is provided to accommodate small leaks when the normal makeup system is unavailable and to accommodate larger leaks resulting from loss of coolant accidents. Safety-related reactor coolant makeup and safety injection are provided by two core makeup tanks, two accumulators, and an in-containment refueling water storage tank. Long-term cooling is provided by containment gravity recirculation of reactor coolant within containment. See Section 6.3 for additional information. The safety-related reactor coolant makeup relies on the Class 1E and UPS system. Neither onsite or offsite ac power is required.

In addition, the nonsafety-related chemical and volume control system automatically provides inventory control to accommodate minor leakage from the reactor coolant system, expansion during heatup from cold shutdown, and contraction during cooldown. This inventory control is provided by letdown and makeup connections to the chemical and volume control system purification loop. Redundant pumps with connections to redundant nonsafety-related onsite ac power are provided when offsite power is not available and these pumps can be supplied from offsite power when onsite power is not available. See Section 5.2 for additional information.

Criterion 34 – Residual Heat Removal

A system to remove residual heat shall be provided. The system safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified acceptable fuel design limits and the design conditions of the reactor coolant pressure boundary are not exceeded.

"Suitable redundancy in components and features and suitable interconnections, leak detection, and isolation capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

AP1000 Compliance

The AP1000 design satisfies the intent of GDC 34 by reducing the risk associated with loss of the decay heat removal function through a combination of safety-related passive systems, together with nonsafety-related active systems. Specific decay heat removal systems include the following:

- A safety-related passive residual heat removal heat exchanger that uses natural circulation flow and that does not require electrical power for operation
- Automatic, safety-related feed and bleed using the core makeup tanks, accumulators, and the in-containment refueling water storage tank for injection and the automatic depressurization system valves for reactor coolant system venting
- The nonsafety-related main feedwater system with motor-driven pumps supplied by the main generator or by offsite power
- The nonsafety-related startup feedwater system with motor-driven pumps supplied by offsite or onsite power, including automatic sequencing on the nonsafety-related diesel generators

- The nonsafety-related normal residual heat removal system with motor-driven pumps supplied by offsite or onsite power, including nonsafety-related diesel generators, for use at low reactor coolant system pressures

A safety-related emergency feedwater system is not required for the AP1000 design. An active safety-related residual heat removal system is not required for the AP1000.

The AP1000 passive core cooling system, in conjunction with the passive containment cooling system, provides a reliable capability for removing decay heat from the reactor core and maintains sufficient water inventory to provide adequate core cooling for an extended period of time. The system does not depend upon pumped injection or recirculation, and actuates automatically, requiring no operator actions.

The containment arrangement addresses the Regulatory Guide 1.82 issues. Functional performance of the system addresses the guidelines of Regulatory Guide 1.139, except that cooldown rate is somewhat more limited when using the passive residual heat removal equipment. See Subsection 1.9.1 for additional information.

The passive core cooling system provides both gravity injection and gravity recirculation, automatically shifting injection modes when the proper containment flood-up conditions are achieved.

The AP1000 design provides a passive decay heat removal system that functions independent of nonsafety-related ac power supplies and can accommodate single active failures. (The Class 1E dc and UPS system supplies power to the safety-related monitoring and control instrumentation.) The passive core cooling system complies with General Design Criterion 34 by providing the capability to remove decay heat without relying on nonsafety-related ac power.

Criterion 35 – Emergency Core Cooling

A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (I) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts.

Suitable redundancy in components and features and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

AP1000 Compliance

The AP1000 design provides for safety-related passive reactor coolant makeup. Core makeup tanks accommodate small leaks when the normal makeup system is unavailable and provide safety injection for small-break loss of coolant accidents. Accumulators provide the high makeup flow required for a large loss of coolant accident and initiate injection when the reactor coolant system pressure is below the static accumulator pressure during a small-break loss of coolant accident.

The in-containment refueling water storage tank, and after containment flood-up, containment recirculation capability provide the long-term source of gravity injection to the core after the reactor coolant system is depressurized. The automatic depressurization system valves provide the vent path to transfer the core decay heat to the containment and then to the ultimate heat sink.

The AP1000 design provides a passive core cooling system that functions independent of ac power supplies, assuming single active failures. The passive core cooling system does not need the

nonsafety-related diesel-generators for electrical power to either actuate or operate the various system components. Therefore, the passive core cooling system complies with the intent of GDC 35 by providing the capability for core cooling without relying on nonsafety-related ac power sources.

Criterion 36 – Inspection of Emergency Core Cooling System

The emergency core cooling system shall be designed to permit appropriate periodic inspection of important components, such as spray rings in the reactor pressure vessel, water injection nozzles, and piping, to assure the integrity and capability of the system.

AP1000 Compliance

The AP1000 design includes a passive core cooling system that provides emergency core decay heat removal, emergency reactor coolant system makeup and boration, safety injection, and containment sump pH control. The system piping and components are designed to permit access for periodic inspection and testing of equipment, according to the ASME Code and technical specification requirements, to provide confidence in the integrity and capability of the system.

The core makeup tanks, accumulators, and passive residual heat removal heat exchanger have manways which permit access for inspection and required maintenance. The in-containment refueling water storage tank design provides access for both the tank itself and for the passive residual heat removal heat exchanger, spargers, and other components located inside the tank.

In addition, the system piping provides accessibility for inspection and maintenance to the extent practical. See Section 6.3 for additional information.

Criterion 37 – Testing of Emergency Core Cooling System

The emergency core cooling system shall be designed to permit appropriate periodic pressure and functional testing to assure (I) the structural and leak-tight integrity of its components, (2) the operability and performance of the active components of the system, and (3) the operability of the system as a whole and under conditions as close to design as practical, the performance of the full operational sequence that brings the system into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.

AP1000 Compliance

The AP1000 passive core cooling system is designed to permit the periodic inspection and testing of the appropriate system components. The testing capabilities of the system including in-service testing and inspection to confirm the structural and leaktight integrity of various components, technical specification operability and performance of the active system components, and additional in-service testing to confirm the overall operability of the system.

The stage 1, 2, and 3 automatic depressurization system valves have provisions for shutdown in-service testing and at-power operability testing.

Planned shutdown testing includes operability testing of the component and system performance, including operation of applicable portions of the protection and safety monitoring system and the use of the appropriate power sources for the system.

The AP1000 design has significantly reduced the support systems required for system operation. In-service testing of the required support systems is also planned.

Criterion 38 – Containment Heat Removal System

A system to remove heat from the reactor containment shall be provided. The system safety function shall be to reduce rapidly, consistent with the functioning of other associated systems, the containment pressure and temperature following any loss of coolant accident and maintain them at acceptably low levels.

Suitable redundancy in components and features and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that for onsite electrical power system operation (assuming offsite power is not available) and for offsite electrical power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

AP1000 Compliance

The AP1000 design uses passive systems for post-loss of coolant accident core and containment heat removal and for the prevention of overpressurization failure of the containment building. Heat is transferred from the containment atmosphere to the steel containment shell by natural convection and condensation. Heat removal from the exterior of the containment shell is enhanced by a directed-flow natural convection design and a passive, external cooling water distribution system.

The AP1000 passive containment cooling system is designed with sufficient capacity to prevent the containment from exceeding its design pressure with no operator action or outside assistance for a minimum of 3 days. After 3 days, limited operator action is required.

The AP1000 passive containment cooling system consists of a steel containment shell and associated water supplies, piping, valves, and air baffle. The passive containment cooling system is a passive system that uses gravity and natural circulation as driving forces. The design of the AP1000 passive containment cooling system does not require the use of any pumps, and it functions independent of nonsafety-related ac power sources for 3 days. Therefore, the passive containment cooling system can function during loss of offsite or onsite power. GDC 38 is satisfied by using appropriate redundancy and by the design of the passive containment cooling system and its reliance on natural forces.

Criterion 39 – Inspection of Containment Heat Removal System

The containment heat removal system shall be designed to permit appropriate periodic inspection of important components, such as the torus, sumps, spray nozzles and piping, to assure the integrity and capability of the system.

AP1000 Compliance

The AP1000 design uses safety-related passive means for containment heat removal. The design of the system allows for inspection of piping, valves, the containment shell and air baffle, and other components to provide confidence in the integrity and capability of the system.

The periodic inspections specified in the ASME Code and technical specifications provide confidence that the capability of these heat removal systems is retained through plant life.

Criterion 40 – Testing of Containment Heat Removal System

The containment heat removal system shall be designed to permit appropriate periodic pressure and functional testing to assure (l) the structural and leaktight integrity of its components, (2) the operability and performance of the active components of the system, and (3) the operability of the system as a whole, and, under conditions as close to the design as practical the performance of the full operational sequence that brings the system into operation, including operation of applicable

portions of the protection system, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.

AP1000 Compliance

The AP1000 design includes a passive containment cooling system that provides containment heat removal to limit the peak containment pressure following design basis events. The system piping and components are designed to permit access for periodic inspection and testing of equipment, according to the ASME Code and technical specification requirements, to provide confidence in the integrity and capability of the system.

The passive containment cooling water storage tank design allows access for both the tank and for the various components located inside the tank.

In addition, the system piping provides accessibility for inspection and maintenance to the extent practical. See Section 6.2 for additional information.

Criterion 41 – Containment Atmosphere Cleanup

Systems to control fission products, hydrogen, oxygen, and other substances which may be released into the reactor containment shall be provided, as necessary, to reduce, consistent with the functioning of other associated systems, the concentration and quantity of fission products released to the environment following postulated accidents and to control the concentration of hydrogen or oxygen and other substances in the containment atmosphere following postulated accidents to assure that containment integrity is maintained.

Each system shall have suitable redundancy in components and features and suitable interconnections, leak detection, isolation, and containment capabilities to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) its safety function can be accomplished, assuming a single failure.

AP1000 Compliance

Fission product control for the AP1000 plant is provided via natural removal processes within containment and by limiting containment leakage. The passive removal processes such as deposition and sedimentation are evaluated based on a physically-based source term with large scale core damage. See Section 6.5 for additional details. The containment and penetration design includes features specifically designed to minimize overall containment leakage. See Subsection 6.2.3 for additional details.

The generation of hydrogen in the containment under post-accident conditions has been evaluated, and the containment hydrogen control system has been designed such that the following criteria are satisfied:

- In compliance with Section 50.44 of 10 CFR 50, means are provided to measure and control post-loss of coolant accident hydrogen concentrations.
- The combustible concentrations of hydrogen do not accumulate in the areas where unintended combustion or detonation could cause loss of containment integrity or loss of appropriate mitigating features.
- Internal passive autocatalytic recombiners are provided for hydrogen control following a design basis loss of coolant accident.

- Hydrogen igniters are provided to limit local and global hydrogen concentrations to below 10 percent following a degraded core event with the reaction of 100 percent of the zircaloy cladding.

- The concentration of uniformly distributed hydrogen produced by the equivalent of a 75 percent active fuel-clad metal water reaction does not exceed 13 percent by volume during and following a degraded core event. (The AP1000 containment volume is large enough to provide passive protection for the hydrogen produced by 75 percent zircaloy cladding reaction following a severe accident.)

- The nonsafety-related ventilation system, normally used during refueling, is designed with the capability for a controlled purge of the containment atmosphere to assist in post-accident cleanup, but is not required for hydrogen control.

Criterion 42 – Inspection of Containment Atmosphere Cleanup System

The containment atmosphere cleanup systems shall be designed to permit appropriate periodic inspection of important components such as filter frames, ducts, and piping, to assure the integrity and capability of the systems.

AP1000 Compliance

The containment atmosphere cleanup systems are designed and located so that they can be inspected periodically, as appropriate.

Criterion 43 – Testing of Containment Atmosphere Cleanup Systems

The containment atmosphere cleanup systems shall be designed to permit appropriate periodic pressure and functional testing to assure (1) the structural and leak-tight integrity of its components, (2) the operability and performance of the active components of the systems such as fans, filters, dampers, pumps, and valves, and (3) the operability of the systems as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the systems into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of associated systems.

AP1000 Compliance

The appropriate portions of the containment atmosphere cleanup system are designed to permit periodic pressure and functionality testing.

As described in GDC 41, the containment atmosphere cleanup system has no safety-related post-accident cleanup functions. Dose mitigation is passively provided by the containment isolation and integrity, natural removal processes, and limited containment leakage. Periodic containment integrity is verified in accordance with 10 CFR 50 Appendix J testing as described in Subsection 6.2.3.

Criterion 44 – Cooling Water

A system to transfer heat from structures, systems, and components important to safety to an ultimate heat sink shall be provided. The system safety function shall be to transfer the combined heat load of these structures, systems, and components under normal operating and accident conditions.

Suitable redundancy in components and features and suitable interconnections, leak detection, and isolation capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished assuming a single failure.

AP1000 Compliance

The passive containment cooling system is the ultimate heat sink for the AP1000 and does not rely upon offsite or onsite ac power sources. Heat transfer by convection from the containment shell to the atmosphere meets the intent of GDC 44. Additional information is provided in the responses for GDC 34 and GDC 38.

Criterion 45 – Inspection of Cooling Water System

The cooling water system shall be designed to permit appropriate periodic inspection of important components, such as heat exchangers and piping, to assure the integrity and capability of the system.

AP1000 Compliance

Refer to the discussion provided for GDC 39.

Criterion 46 – Testing of Cooling Water System

The cooling water system shall be designed to permit appropriate periodic pressure and functional testing to assure (1) the structural and leak-tight integrity of its components, (2) the operability and the performance of the active components of the system, and (3) the operability of the system as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the system into operation for reactor shutdown and for loss of coolant accidents, including operation of applicable portions of the protection system and the transfer between normal and emergency power sources.

AP1000 Compliance

Refer to the discussion provided for GDC 40.

3.1.5 Reactor Containment

Criterion 50 – Containment Design Basis

The reactor containment structure, including access opening, penetrations, and the containment heat removal system, shall be designed so that the containment structure and its internal compartments can accommodate, without exceeding the design leakage rate and with sufficient margin, the calculated pressure and temperature conditions resulting from any loss of coolant accident. This margin shall reflect consideration of (1) the effects of potential energy sources which have not been included in the determination of the peak conditions, such as energy in steam generators and energy from metal-water and other chemical reactions that may result from degraded emergency core cooling functioning, (2) the limited experience and experimental data available for defining accident phenomena and containment responses, and (3) the conservatism of the calculational model and input parameters.

AP1000 Compliance

The design of the containment structure is based on the containment design basis accidents, which include the rupture of a reactor coolant pipe or the rupture of a main steam or feedwater line. The maximum pressure and temperature reached, a description of the calculational model, and input parameters for a containment design basis accident are presented in Section 6.2. The containment design provides margin to the design basis limits.

Criterion 51 – Fracture Prevention of Containment Pressure Boundary

The reactor containment boundary shall be designed with sufficient margin to assure that under operating, maintenance, testing, and postulated accident conditions (1) its ferritic materials behave in

a nonbrittle manner and (2) the probability of rapidly propagating fracture is minimized. The design shall reflect consideration of service temperatures and other conditions of the containment boundary material during operation, maintenance, testing, and postulated accident conditions, and the uncertainties in determining (1) material properties, (2) residual, steady-state, and transient stresses, and (3) size of flaws.

AP1000 Compliance

Principal load-carrying components of ferritic materials of the reactor containment boundary exposed to the external environment are selected so that they behave in a nonbrittle manner and so that the probability of fracture propagation is minimized. See Subsection 3.8.2 for additional information.

Criterion 52 – Capability for Containment Leakage Rate Testing

The reactor containment and other equipment which may be subjected to containment test conditions shall be designed so that periodic integrated leakage rate testing can be conducted at containment design pressure.

AP1000 Compliance

The containment system is designed and constructed and the necessary equipment is provided to permit periodic integrated leakage rate tests according to the requirements of 10 CFR 50, Appendix J.

Criterion 53 – Provisions for Containment Testing and Inspection

The reactor containment shall be designed to permit (1) appropriate periodic inspection of all important areas, such as penetrations, (2) an appropriate surveillance program, and (3) periodic testing at containment design pressure of the leak-tightness of penetrations which have resilient seals and expansion bellows.

AP1000 Compliance

Provisions exist for conducting individual leakage rate tests on containment penetrations. Penetrations are visually inspected and pressure-tested for leak tightness at periodic intervals. Other inspections are performed as required by 10 CFR 50, Appendix J.

Criterion 54 – Piping Systems Penetrating Containment

Piping systems penetrating the primary reactor containment shall be provided with leak detection, isolation and containment capabilities having redundancy, reliability, and performance capabilities which reflect the importance to safety of isolating these piping systems. Such piping systems shall be designed with a capability to test periodically the operability of the isolation valves and associated apparatus and to determine if valve leakage is within acceptable limits.

AP1000 Compliance

Piping systems penetrating the primary reactor containment are provided with containment isolation valves. Penetrations that close for containment isolation have redundant valving. Automatic isolation valves with air-, solenoid-, or motor-operators, which do not restrict normal plant operation, are periodically tested to verify operability.

The AP1000 containment isolation design satisfies the current NRC requirements including the post-TMI requirements, as discussed in Subsection 1.9.3. In general, this means that two barriers are provided, one inside containment and the other outside containment. Usually these barriers are valves, but in some cases they are closed piping systems not connected to the reactor coolant system or to the containment atmosphere.

The AP1000 design incorporates a reduction in the number of existing penetrations. Most penetrations are normally closed. Those few that are normally open and are required to close use remotely operated valves for isolation that close automatically. See Subsection 6.2.3 for additional information.

Nonessential systems that may be normally open, such as the mini-purge system, are provided with automatic containment isolation valves that close automatically on a containment isolation signal. The containment isolation signal is actuated by the protection and safety monitoring system. See Section 7.3 for additional information.

Piping and electrical containment penetrations are equipped with test connections and test vents or have other provisions to allow periodic leak rate testing so that leakage is within the acceptable limits established in technical specifications consistent with 10 CFR 50, Appendix J.

Criterion 55 – Reactor Coolant Pressure Boundary Penetrating Containment

Each line that is part of the reactor coolant pressure boundary and that penetrates primary reactor containment shall be provided with containment isolation valves as follows, unless it can be demonstrated that the containment isolation provisions for a specific class of lines, such as instrument lines, are acceptable on some other defined basis:

1. One locked closed isolation valve inside and one locked closed isolation valve outside containment; or

2. One automatic isolation valve inside and one locked closed isolation valve outside containment; or

3. One locked closed isolation valve inside and one automatic isolation valve outside the containment. A simple check valve may not be used as the automatic isolation valve outside containment; or

4. One automatic isolation valve inside and one automatic isolation valve outside containment. A simple check valve may not be used as the automatic isolation valve outside containment.

Isolation valves outside containment shall be located as close to containment as practical and, upon loss of actuating power, automatic isolation valves shall be designed to take the position that provides greater safety.

Other appropriate requirements to minimize the probability or consequences of an accidental rupture of these lines or of lines connected to them shall be provided, as necessary, to assure adequate safety. Determination of the appropriateness of these requirements, such as higher quality in design, fabrication, and testing, additional provisions for in-service inspection, protection against more severe natural phenomena, and additional isolation valves and containment, shall include consideration of the population density, and use characteristics, and physical characteristics of the site environs.

AP1000 Compliance

Lines that penetrate containment that are connected to the reactor coolant pressure boundary are provided with containment isolation valves in accordance with one of the acceptable arrangements as described in GDC 55. Additional information is found in Subsection 6.2.3.

Criterion 56 – Primary Containment Isolation

Each line that connects directly to the containment atmosphere and penetrates the primary reactor containment shall be provided with containment isolation valves as follows, unless it can be

demonstrated that the containment isolation provisions for a specific class of lines, such as instrument lines, are acceptable on some other defined basis:

1. One locked closed isolation valve inside and one locked closed isolation valve outside the containment; or

2. One automatic isolation valve inside and one locked closed isolation valve outside the containment; or

3. One locked closed isolation valve inside and one automatic isolation valve outside the containment. A simple check valve may not be used as the automatic isolation valve outside containment; or

4. One automatic isolation valve inside and one automatic isolation valve outside the containment. A simple check valve may not be used as the automatic isolation valve outside the containment.

Isolation valves outside the containment shall be located as close to the containment as practical and, upon loss of actuating power, automatic isolation valves shall be designed to take the position that provides greater safety.

AP1000 Compliance

Lines connecting directly with the containment atmosphere and penetrating the reactor containment are normally provided with two isolation valves in series, one inside and one outside the containment, in accordance with one of the acceptable arrangements as described in GDC 56. Isolation of instrument lines for containment pressure measurement is demonstrated on a different basis and does not require isolation valves. Additional information is found in Subsection 6.2.3.

Criterion 57 – Closed System Isolation Valves

Each line that penetrates the primary reactor containment and is neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere shall have at least one containment isolation valve which shall be either automatic, locked closed, or capable of remote manual operation. This valve shall be outside the containment and located as close to the containment as practical. A simple check valve may not be used as the automatic isolation valve.

AP1000 Compliance

Lines that penetrate the containment and are neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere are considered closed systems within the containment and are equipped with at least one containment isolation valve of one of the following types:

- An automatic isolation valve (a simple check valve is not used as this automatic valve)

- A locked-closed valve

This valve is located outside the containment and as close to the containment wall as practical.

3.1.6 Fuel and Reactivity Control

Criterion 60 – Control of Releases of Radioactive Materials to the Environment

The nuclear power unit design shall include means to control suitably the release of radioactive materials in gaseous and liquid effluents and to handle radioactive solid wastes produced during

normal reactor operation, including anticipated operational occurrences. Sufficient holdup capacity shall be provided for the retention of gaseous and liquid effluents containing radioactive materials, particularly where unfavorable site environmental conditions can be expected to impose unusual operational limitations upon the release of such effluents to the environment.

AP1000 Compliance

Means are provided to control the release of radioactive materials in gaseous and liquid effluents and to handle radioactive solid wastes produced during normal reactor operation, including anticipated operational occurrences.

The radioactive waste management systems are designed to minimize the potential for an inadvertent release of radioactivity from the facility and to provide confidence that the discharge of radioactive wastes is maintained below regulatory limits of 10 CFR 50, Appendix I, during normal operation. The gaseous radwaste and liquid radwaste processing systems include continuous radiation monitoring of their discharge paths. High radiation automatically closes a discharge isolation valve. The liquid radwaste system also has provisions to prevent inadvertent siphoning of its monitor tank contents which could cause an uncontrolled discharge. The radioactive waste management systems, the design bases, and the estimated amounts of radioactive effluent releases to the environment are described in Chapter 11.

Criterion 61 – Fuel Storage and Handling and Radioactivity Control

The fuel storage and handling, radioactive waste, and other systems which may contain radioactivity shall be designed to assure adequate safety under normal and postulated accident conditions. These systems shall be designed (1) with a capability to permit appropriate periodic inspection and testing of components important to safety, (2) with suitable shielding for radiation protection, (3) with appropriate containment, confinement, and filtering systems, (4) with a residual heat removal capability having reliability and testability that reflects the importance to safety of decay heat and other residual heat removal, and (5) to prevent significant reduction in fuel storage coolant inventory under accident conditions.

AP1000 Compliance

The spent fuel pool cooling system, and the fuel handling and refueling system are designed to provide cooling and shielding for the fuel assemblies stored in the spent fuel pit and to provide purification of the water in the pit. The system design provides adequate safety under normal and postulated accident conditions.

The spent fuel pool cooling system normal system operation is described in Subsection 9.1.3. Sampling of the spent fuel pool water for gross activity, tritium, and particulate matter is conducted periodically. The concentration of tritium in the spent fuel pool water is maintained at less than 0.5 microcuries per gram to provide confidence that the airborne concentration of tritium in the fuel handling area is within the limits specified in 10 CFR 20, Appendix B. See Subsection 12.2.2 for additional information.

The spent fuel pool is designed so that a water level is maintained above the spent fuel assemblies for at least 72 hours following a loss of the spent fuel pool cooling system, without ac power. See Subsection 9.1.2 for additional information.

The spent fuel pool cooling system maintains the water in the in-containment refueling water storage tank consistent with activity requirements of the water in the refueling cavity during a refueling. Two spent fuel pool cooling filters are provided, one downstream of each demineralizer in the purification branch line of each mechanical train. The filters are sized to collect particulates and suspended solids passed by the demineralizer.

The AP1000 spent fuel pool cooling system is not required to operate to mitigate design basis events. In the event the spent fuel pool cooling system is unavailable, the spent fuel pool cooling is provided by the heat capacity of the water in the pool and in the passive sources of makeup water.

Normal HVAC to the spent fuel pool area is provided by a subsystem of the radiologically controlled area ventilation system described in Subsection 9.4.3. No credit is taken for this system in evaluation of fuel handling accidents discussed in Subsection 15.7.4.

Connections to the spent fuel pool are provided at an elevation that prevents inadvertent draining of the water in the pool to an unacceptable level.

The design of spent fuel storage pool and the spent fuel pool cooling system satisfies GDC 61. See Subsection 9.1.3 for additional information.

Criterion 62 – Prevention of Criticality in Fuel Storage and Handling

Criticality in the fuel storage and handling system shall be prevented by physical systems or processes, preferably by use of geometrically safe configurations.

AP1000 Compliance

The restraints, interlocks, and physical arrangement provided for the safe handling and storage of new and spent fuel are discussed in Section 9.1. The spent fuel assemblies are stored in the spent fuel pit until fission product activity is low enough to permit shipment.

Criterion 63 – Monitoring Fuel and Waste Storage

Appropriate systems shall be provided in the fuel storage and radioactive waste systems and associated handling areas (1) to detect conditions that may result in the loss of residual heat removal capability and excessive radiation levels and (2) to initiate appropriate safety actions.

AP1000 Compliance

Instrumentation is provided to monitor spent fuel storage pool temperature and water level. Indication and alarms are provided in the main control room. Area radiation monitoring is provided in the fuel storage area for personnel protection and general surveillance. The area monitor alarms locally and in the main control room.

If radiation levels in the ventilation effluent reach a predetermined point, an alarm is actuated in the main control room, and the ventilation discharge path is automatically transferred through filter absorber units that provide filtration before discharge from the plant vent.

Criterion 64 – Monitoring Radioactivity Releases

Means shall be provided for monitoring the reactor containment atmosphere, spaces containing components for recirculation of loss of coolant accident fluids, effluent discharge paths, and the plant environs for radioactivity that may be released from normal operations, including anticipated operational occurrences, and from postulated accidents.

AP1000 Compliance

The containment atmosphere is monitored during normal and transient operations by the containment gaseous radiation monitors. Under accident conditions, samples of the containment atmosphere taken via the sampling system provide data on airborne radioactive concentrations within the containment.

No reactor coolant fluids are required to be recirculated outside of containment following an accident. Radioactivity levels contained in the facility effluent and discharge paths and in the plant environs are monitored during normal and accident conditions by the plant radiation monitoring systems. High radiation in a discharge path causes automatic closure of the discharge isolation valve.

Area radiation monitors (ARMs) are provided to supplement the personnel and area radiation survey provisions of the AP1000 health physics program described in Section 12.5 and to comply with the personnel radiation protection guidelines of 10 CFR 20, 10 CFR 50, 10 CFR 70, and Regulatory Guides 1.97, 8.2, 8.8, and 8.12. In addition to the installed detectors, periodic plant environmental surveillance is established.

Measurement capability and reporting of effluents are based on the guidelines of Regulatory Guides 1.4 and 1.21, as discussed in Subsection 1.9.1. Additional information is contained in Chapters 11 and 12.

3.1.7 Combined License Information

This section contained no requirement for additional information.

3.1.8 References

1. 10 CFR 50, Appendix G, "Fracture Toughness Requirements."

2. American Society of Testing Materials E-185, Standard Recommended Practice for Surveillance Test for Nuclear Reactor Vessels, and the requirements for 10 CFR 50, Appendix H, "Reactor Vessel Material Surveillance Program Requirements."