3.0 Design of Structures, Components, Equipment and Systems

3.1 Compliance with Nuclear Regulatory Commission General Design Criteria

This section addresses the U.S. EPR design compliance with the General Design Criteria (GDC) in 10 CFR 50, Appendix A, for safety-related structures, systems, and components (SSC). As presented in this section, each criterion is first quoted and then discussed in sufficient detail to demonstrate the U.S. EPR compliance with each criterion. Where additional information may be required for a complete discussion of the GDC, the appropriate sections are referenced.

3.1.1 Overall Requirements

3.1.1.1 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 functions 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."

3.1.1.1.1 U.S. EPR Compliance

The U.S. EPR Quality Assurance (QA) Plan, which has been approved by the NRC (refer to Section 17.5), provides confidence that safety-related SSC are designed to quality standards commensurate with the safety functions to be performed. Where applicable, design and fabrication are in accordance with the codes required in 10 CFR 50.55a. The QA Plan complies with the requirements of 10 CFR 50, Appendix B, and ANSI/ASME NQA-1-1994 (Reference 1). Further information on the QA program is provided in Chapter 17. A COL applicant that references the U.S. EPR design certification will identify the site-specific QA Program Plan that demonstrates compliance with GDC 1.

The SSC are classified according to their safety significance. Systems and components are classified by quality group and assigned relevant quality standards for design, fabrication, erection, and testing commensurate with their safety significance. Further information on the safety classification, quality group classification, relevant codes and

standards, and applicable quality control program for each component is provided in Section 3.2.

3.1.1.2 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 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."

3.1.1.2.1 U.S. EPR Compliance

The safety-related SSC are designed either to withstand the effects of natural phenomena without loss of the capability to perform their safety functions, or to fail in a safe condition. The nature and magnitude of the natural phenomena considered in the U.S. EPR design are described in Chapter 2. The U.S. EPR design criteria for wind, tornado, flood, and earthquakes are discussed in Section 3.3, Section 3.4, and Section 3.7, respectively.

The U.S. EPR design envelopes the natural phenomena of expected sites. The design bases for safety-related SSC reflect this envelope of natural phenomena, including appropriate combinations of the effects of normal and accident conditions. Seismic and quality group classifications, as well as other pertinent standards and information, are provided in the sections that discuss individual SSC.

3.1.1.3 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. Firefighting 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."

3.1.1.3.1 U.S. EPR Compliance

The U.S. EPR is designed for safe shutdown assuming equipment in any one fire area is rendered inoperable by fire and that re-entry into the fire area for repair and operator manual actions is not possible, as described in Section 1.2. The control room and containment are excluded from this approach. An alternate shutdown capability is provided that is physically and electrically independent of the control room. In containment, protection is provided for redundant shutdown systems, to the extent practicable, such that one shutdown division will be free of fire damage. Additionally, the design contains provisions so that smoke, hot gasses, or fire suppressant will not migrate into unaffected areas and adversely affect safe-shutdown capabilities.

As described in Section 9.5.1 safety-related SSC are designed and located to minimize the probability and effect of fires and explosions. This is accomplished in part by compartmentalizing of the plant into separate fire areas. Specifically, based on the hazards present and the need for physical separation of safety-related SSC, the plant is segregated into separate fire areas by fire-rated structural barriers (i.e., walls, floors, and ceilings). In some instances, such as the Reactor Building, fire areas may be sub-divided into fire zones, based on physical separation, location of plant equipment, or for fire hazard analysis purposes. These fire areas and zones serve the primary purpose of confining the effects of fires to a single compartment or area, thereby minimizing the potential for adverse effects from fires on redundant safety-related SSC. Outside of the control room and the Reactor Building, each of the four redundant trains of emergency core cooling is separated by three-hour rated structural fire barriers. Materials used in plant construction are noncombustible or heat resistant to the extent practicable. Walls, floors, roofs, including structural materials, suspended ceilings, thermal insulation, radiation shielding materials, and soundproofing and interior finish are noncombustible or meet applicable qualification test acceptance criteria unless otherwise justified. Concealed spaces are devoid of combustibles unless otherwise justified.

Fire protection systems include fire detection and alarm systems, fire water supply systems, and automatic and manual fire suppression systems. These systems are provided and designed using the applicable National Fire Protection Association codes and standards as guidance. Under this guidance, the plant is designed to have sufficient capacity and capability to minimize the adverse effects of fires on safety-related SSC. Failure, rupture, or inadvertent actuation of fire suppression systems does not significantly impair the safety capability of safety-related SSC.

3.1.1.4 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 (LOCA). 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."

3.1.1.4.1 U.S. EPR Compliance

Safety-related SSC are designed to accommodate the effects of, and to be compatible with, the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, which include loss-of-coolant accidents (refer to Section 3.11). These safety-related SSC are appropriately protected against dynamic effects, which include 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. Additionally, the U.S. EPR design applies the leak-before-break (LBB) methodology, as described in Section 3.6.3, to eliminate the dynamic effects of pipe rupture. Details of the design, environmental testing, and construction of safety-related SSC are included in Chapters 3, 5, 6, 7, 9, and 10.

3.1.1.5 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."

3.1.1.5.1 U.S. EPR Compliance

Since the U.S. EPR design is a single-unit station, there are no shared safety-related SSC.

3.1.2 Protection by Multiple Fission Product Barriers

3.1.2.1 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."

3.1.2.1.1 U.S. EPR Compliance

The reactor core and associated coolant, control, and protection systems are designed with appropriate margin such that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences (AOOs) and postulated accidents as defined and analyzed in Chapter 15.

For AOOs and events of lower probability of occurrence that result in a plant shutdown, shutdown capabilities will bring the plant to a subcritical condition and maintain it in a safe shutdown state through the use of safety-related equipment.

The reactor core is designed to maintain integrity over a complete range of power levels, including AOO transient conditions. The core is sized with sufficient heat transfer area and coolant flow such that specified acceptable fuel design limits are not exceeded under normal conditions or anticipated operational occurrences.

The reactor trip system is designed to actuate a reactor trip whenever necessary to prevent reactor operations from exceeding the fuel design limits. The core design together with the process and decay heat removal systems designs provide for this capability under expected conditions of normal operation. These designs include appropriate margins for uncertainties and anticipated transient situations, including the effects of the loss of reactor coolant flow, trip of the turbine-generator, loss of normal feedwater, and turbine-generator trip with loss of offsite power.

Chapter 4 describes the design bases and design evaluation of core components. Details of the control and the instrumentation design and logic of the protection systems are described in Chapter 7. The information in these chapters supports the accident analyses of Chapter 15, which shows that the acceptable fuel design limits are not exceeded conditions of normal or abnormal operation and, therefore, meet the requirements of Criterion 10.

3.1.2.2 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."

3.1.2.2.1 U.S. EPR Compliance

Whenever the reactor is critical, the negative fuel temperature effect (Doppler effect) and the operational limit on the moderator temperature coefficient of reactivity provide prompt compensatory reactivity feedback effects. The negative Doppler coefficient of reactivity is demonstrated by the inherent design, using low-enrichment fuel. The moderator temperature coefficient of reactivity is dependent upon core characteristics, such as fuel loading, the dissolved absorber (boron) concentration, and burnable poisons. Reactivity coefficients and their effects are described in Chapter 4.

3.1.2.3 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."

3.1.2.3.1 U.S. EPR Compliance

Power oscillations of the fundamental mode are inherently eliminated by negative Doppler and negative moderator temperature coefficients of reactivity. Oscillations due to xenon spatial effects in the radial, diametral, and azimuthal harmonic modes are also heavily damped due to the inherent design and due to the negative Doppler and negative moderator temperature coefficients of reactivity.

Oscillations due to xenon spatial effects may occur in the axial first harmonic mode. Using the measured axial power shape as an input, reactor trip functions are provided so that fuel design limits are not exceeded by xenon axial oscillations. Oscillations due to xenon spatial effects in axial modes higher than the first harmonic are heavily damped due to the inherent design and due to the negative Doppler coefficient of reactivity. If necessary, the operator can suppress xenon axial oscillations by control rod motions and temporary power reductions as needed to maintain axial imbalance within the limits of the Technical Specifications (i.e., imbalances which are alarmed to the operator and are within the imbalance trip setpoints).

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

3.1.2.4 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."

3.1.2.4.1 U.S. EPR Compliance

Instrumentation and controls are provided to monitor and control neutron flux, control rod position, and fluid temperatures, pressures, flows, and levels to maintain adequate plant safety. Instrumentation is provided in the reactor coolant system (RCS), steam and power conversion system, containment, engineered safety features (ESF) systems, radiological waste systems, and other auxiliaries. Parameters provided for operator use under normal operating and accident conditions are indicated in the control room.

The quantity and types of process instrumentation provide safe and orderly operation of plant systems over the full design range of the plant. These systems are described in Chapters 6, 7, 8, 9, 10, 11, and 12.

3.1.2.5 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."

3.1.2.5.1 U.S. EPR 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 with stresses within applicable limits. The pressure boundary design also considers loadings under normal operating conditions as well as abnormal loadings, such as pipe rupture and seismic loadings as described in Chapter 3. The piping is protected from overpressure by means of pressure-relieving devices as required by ASME Boiler and Pressure Vessel (BPV) Code, Section III (Reference 2). Reactor coolant pressure boundary materials and fabrication and erection techniques result in a low probability of gross rupture or significant leakage. Coolant chemistry is controlled to protect the materials of construction of the reactor coolant pressure boundary from corrosion.

The reactor coolant pressure boundary is accessible for inservice inspections to assess the structural and leaktight integrity. The details of this access are given in Chapter 5. For the reactor vessel, a material surveillance program conforming to applicable codes is provided; refer to Chapter 5 for additional details. Instrumentation is provided to detect significant leakage from the reactor coolant pressure boundary with indication in the control room as described in Chapter 5.

3.1.2.6 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."

3.1.2.6.1 U.S. EPR Compliance

Steady-state and transient analyses are performed to verify that the design conditions of the reactor coolant system and its associated auxiliary systems are not exceeded. These analyses address normal operations, including anticipated operational occurrences. Protection system setpoints and control system parameters are based on these analyses. Additionally, reactor coolant pressure boundary components have a

sufficient margin of safety through the application of proven materials and design codes, use of proven fabrication techniques, nondestructive shop testing, and integrated hydrostatic testing of assembled components. Included in reactor vessel design is consideration of the effects of radiation embrittlement; surveillance samples are provided to monitor adherence to expected conditions throughout the plant life.

Multiple safety and relief valves are provided for the reactor coolant system. These valves and their setpoints meet the ASME Code, Section III criteria for overpressure protection. Chapter 5 describes the reactor coolant system design.

3.1.2.7 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."

3.1.2.7.1 U.S. EPR Compliance

The Reactor Building consists of a cylindrical reinforced concrete outer Shield Building, a cylindrical post-tensioned concrete inner Containment Building with a 0.25 in thick steel liner, and an annular space between the two buildings. The Shield Building protects the Containment Building from external hazards. The Containment Building contains the reactor coolant system and portions of associated structures, systems, and components. In the event of a LOCA or severe accident, the Containment Building retains radioactive material and withstands the maximum pressure and temperature resulting from the release of stored energy. It is designed to sustain, without loss of required integrity, the effects of LOCAs up to and including the double-ended rupture of the largest pipe in the reactor coolant system or double-ended rupture of a steam or feedwater pipe. ESFs comprising the emergency core cooling system (ECCS) cool the reactor core and return the containment to near atmospheric pressure. The Containment Building and ESF systems are designed to contain any uncontrolled release of radioactivity. The concrete radiological shielding and the liner within the containment limit the uncontrolled release of radioactivity to the environment.

Additional information about containment design is provided in Chapters 3, 6, and 15.

3.1.2.8 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 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."

3.1.2.8.1 U.S. EPR Compliance

The onsite AC power system is designed as two separate distribution systems, a Class 1E system and a non-Class 1E system. Safety-related loads as well as select non-safety-related loads important to safety are powered from the four-division Class 1E emergency power supply system (EPSS), while remaining non-safety-related plant loads are powered from the non-Class 1E normal power supply system (NPSS). The separation of the Class 1E and non-Class 1E buses limits the effect of non-safety-related equipment on safety-related equipment.

Each EPSS division has an emergency diesel generator (EDG) as a standby power source. A loss of power or a degraded voltage condition detected at the EPSS switchgear results in automatic disconnection from the preferred power source and connection of the respective EDG. EPSS loads are automatically sequenced on each EDG so that EDG output voltage and frequency are adequately maintained while providing power to the EPSS safety-related loads.

Four Class 1E uninterruptible power supply (EUPS) divisions consisting of batteries, battery chargers, inverters, and distribution equipment provide uninterruptible power

for control and instrumentation functions. The EUPS battery chargers receive power from the diesel-backed EPSS buses. In addition to vital control and instrumentation power, the uninterruptible power supply provides power to safety-related loads that require uninterruptible power in support of performing their required safety-related functions.

Offsite power is supplied to the plant from the transmission system by at least two independent circuits through the site-specific station switchyard. Power from the switchyard to the NPSS is provided through three normal auxiliary transformers and to the EPSS through two separate emergency auxiliary transformers. Each emergency auxiliary transformer has the capacity to supply all four EPSS divisions during design basis events. Normally, each emergency auxiliary transformer supplies two EPSS divisions with offsite power. No bus transfers are required to provide power from the switchyard throughout the full range of plant operation from startup to full power operation to shutdown.

Each offsite circuit that is connected to the EPSS and the onsite power distribution system, has the capacity and capability (assuming the other power source is not functioning) to maintain fuel design limits and reactor coolant pressure boundary design conditions during anticipated operational occurrences. Additionally, either offsite power or the onsite power distribution systems can maintain core cooling, containment integrity, and other vital functions in the event of postulated accidents.

The four EPSS divisions (including respective EDGs), and EUPS divisions have sufficient independence, and redundancy to perform their safety functions assuming a single failure. Additional information on these systems is provided in Chapter 8.

3.1.2.9 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."

3.1.2.9.1 U.S. EPR Compliance

The operability and functional performance of the Class 1E onsite power distribution system components can be periodically tested; this testing includes EDGs, engineered safety feature (ESF) buses, and DC systems. The operability of these electric power

systems as a whole and under conditions as close to design as practical, including the full operational sequence that actuates these systems, can be tested.

Other plant power systems are also tested. The switchyard circuit breakers are inspected, maintained, and tested on a routine basis without affecting the rest of the system. Transmission lines and protective relays on these lines are also periodically tested. Additionally, any one of the emergency auxiliary transformers and its circuit to the Class 1E buses can be taken out of service and tested periodically. Design of the safety-related power system provides testability for transfer of power in accordance with the requirements of Criterion 18. Finally, four onsite power divisions permit periodic testing of redundant equipment while minimizing plant impact. Surveillance testing of the Class 1E distribution system components is presented in Chapter 16.

3.1.2.10 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."

3.1.2.10.1 U.S. EPR Compliance

The U.S. EPR main control room (MCR) contains the equipment and controls necessary to operate the nuclear power unit safely under normal conditions and to maintain the unit in a safe manner under accident conditions, including LOCAs. The MCR is located in a hardened concrete Safeguard Building, which is designed to withstand internal accidents as well as external hazards including aircraft hazards. Adequate concrete shielding and radiation protection are provided to prevent direct gamma radiation and inhalation doses postulated to result from a release of fission products inside the containment structure. Refer to Chapter 15 for further information on accident conditions.

The control room area ventilation system (refer to Section 9.4.1) is designed to allow access to and occupancy of the MCR 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. Fission product removal is provided by the control room area ventilation system recirculation equipment to remove iodine

and particulate matter, thereby minimizing the thyroid dose which could result from the accident. The MCR habitability features are described in Section 6.4.

If the MCR becomes inaccessible, operators can supervise and control the plant from the Remote Shutdown Station (RSS). The RSS is designed so that the plant can be brought to and maintained in a safe shutdown state. The RSS is described in Section 7.4.

3.1.3 Protection and Reactivity Control Systems

3.1.3.1 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."

3.1.3.1.1 U.S. EPR Compliance

A fully automatic protection system with redundant input channels and redundant processing is provided to cope with anticipated operational occurrences and postulated accidents in which insufficient time is available for manual corrective action. The protection system is integrated both to perform reactor trip and to actuate engineered safety features (including auxiliary support features). The response and adequacy of the protection system have been verified by the analysis of anticipated transients.

The protection system automatically initiates a reactor trip when appropriate variables monitored by the system exceed the nominal trip setpoint. Nominal trip setpoints provide an envelope of safe operating conditions with adequate margin for uncertainties so that the fuel design limits are not exceeded. When trip setpoints are exceeded, the system initiates a reactor trip by removing power to the rod drive mechanisms of the rod cluster control assemblies. This power loss causes the rods to insert by gravity, thus rapidly reducing the reactor power.

Additional information on the protection system is provided in Chapter 7.

3.1.3.2 Criterion 21 – Protection System Reliability and Testability

"The protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) 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 functions when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred."

3.1.3.2.1 U.S. EPR Compliance

The protection system is designed for high functional reliability and inservice testability. Redundant input channels, signal processing, and actuation processing are included in the design of the protection system so that no single failure prevents protection functions. If any single component or redundant portion of the protection system is removed from service, a single failure tolerant system remains intact.

The protection system design permits periodic testing of its functionality while the reactor is in operation. This design includes the capability to test redundant portions of the system independently. In cases where actuated equipment cannot be tested at power, the input channels and logic associated with the protection system, up to the final actuation device, can be tested at power. Self-monitoring functionality is also designed into the protection system and occurs continuously while the reactor is in operation. These functions detect and provide early indication of a variety of failures that may occur between periodic tests.

Chapter 7 provides additional information of the protection system reliability and testability.

3.1.3.3 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."

3.1.3.3.1 U.S. EPR Compliance

The protection system is designed so that the effects of natural phenomena, and of normal operating, maintenance, testing and postulated accident conditions do not result in loss of the protective function. Each of the four divisions of the protection system is located in a physically separate Safeguard Building, providing geographical separation diversity between divisions. Each Safeguard Building is designed to withstand the effects of natural phenomena. Redundancy and independence is designed into the protection system so that the system can perform its protective functions while one division is out of service for maintenance or testing.

Administrative controls further maintain the minimum system redundancy during maintenance and testing activities.

The protection system includes specific features that enable it to function in a postulated accident. The components of the protection system are located and qualified so that they continue to operate in the environment accompanying a postulated accident. Protection system cabinets are located so that they are unaffected by failures of pipes, vessels, tanks, pumps and valves. The geographical separation between divisions means that only one division is affected by internal hazards such as explosions or fire. The rooms that house protection system equipment are supplied by safety-related HVAC service to protect against excessive increases in temperature. Protection system components are environmentally and seismically qualified through type testing to confirm their proper operation under adverse environmental conditions. Section 3.10 and Section 3.11 provide further information on the seismic and environmental qualification of the protection system equipment.

The U.S. EPR design incorporates functional and equipment diversity to prevent loss of protective functions. Functional diversity is used within the protection system for reactor trips. Each division of the protection system contains two functionally independent subsystems. For selected design basis events, the primary reactor trip function is processed in one of these subsystems, and a second reactor trip based on diverse process measurements is processed in the other subsystem. The methodology used to determine which events are mitigated by functionally diverse reactor trips is described in Section 7.8.

The U.S. EPR includes a non-safety-related diverse actuation system which uses equipment and software separate from the protection system. This diverse system provides specific reactor trip and engineered safety features actuations to cope with postulated failures of the protection system. Additional information related to the diverse actuation system is included in Section 7.8.

3.1.3.4 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."

3.1.3.4.1 U.S. EPR Compliance

The protection system is designed to fail in a predefined safe state for the most likely failure modes. Removal of power or computer failures result in computer shutdown, and the associated outputs are de-energized. At the actuation level of the protection

system, de-energized outputs result in actuation of reactor trip and no actuation of engineered safety features.

Failures upstream of the actuation level (e.g., sensor failure, acquisition and processing computer failure, or communication failures) results in modified voting logic in the actuation level of the system. The voting logic for reactor trip actuations is modified toward actuation as a result of upstream failures. The voting logic for engineered safety features actuation is modified either toward actuation or no actuation, depending on the predefined safe state of each actuation function.

Additional information related to protection system failure handling is described in Section 7.1.

3.1.3.5 Criterion 24 – Separation of Protection and Control Systems

"The protection system shall be separated from 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."

3.1.3.5.1 U.S. EPR Compliance

The protection system is independent and separate from the control systems so that failure of any single control system component or channel does not affect the operation of the protection system. Control systems require information from the protection system to perform their control functions (including permissive status, processing results, and sensor measurements). This information is transferred to the control systems through properly isolated channels. The isolation devices for these channels are classified as part of the protection system. Minimum protection system redundancy is maintained with any portion of one division removed from service for testing or maintenance.

The protection system receives information from the non-safety-related operator interface system (permissive validation and reset of engineered safety features actuation signals). The protection system does not rely on these inputs to perform its safety function, and these inputs cannot prevent a safety function. Operator input needed for proper operation of the protection system is available through a Class 1E path which has priority over the same input from the non-safety-related system. The design of the protection system includes communication independence and electrical isolation techniques so that a failure in the non-safety-related system cannot prevent a safety function. Additional information related to protection system interfaces to control systems is found in Chapter 7.

3.1.3.6 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 control rods."

3.1.3.6.1 U.S. EPR Compliance

The protection system is designed so that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems. For instance, accidental withdrawal of a control rod or control rod bank (initiated by the rod control system) causes parameters monitored by the protection system to exceed their nominal reactor trip setpoints. The protection system responds to the exceeded setpoint by issuing reactor trip signals. The protection system then acts on the reactor trip breakers and contactors to remove power from the control rod drive system. Upon power loss, the control rods insert by gravity, regardless of movement demands from the rod control system.

The protection system is also designed so that reactivity control system malfunctions do not cause specified acceptable fuel design limits to be exceeded. Boron concentration in the chemical and volume control system (CVCS) charging lines is monitored by the protection system during shutdown, start up, and power operation. The protection system is designed to detect and terminate boron dilution due to boron control system malfunction. Chapter 7 provides further information on the protection system logic used to mitigate boron dilution events. Further information on the CVCS is provided in Section 9.3.4. Chapter 15 analyses demonstrate that specified acceptable fuel design limits are not exceeded as a result of reactivity control system malfunctions.

3.1.3.7 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."

3.1.3.7.1 U.S. EPR Compliance

Two independent reactivity control systems are provided: rod cluster control assemblies (RCCA), which are inserted into the core by gravity; and chemical shim (boric acid). During operation, the shutdown rod banks are fully withdrawn. Using the rod control system, the operator maintains a programmed average reactor temperature compensating for reactivity effects associated with scheduled and transient load changes. The shutdown rod banks and the control banks shut down the reactor with adequate margin under normal operation and anticipated operational occurrences so that specified fuel design limits are not exceeded. The most restrictive period in the core life is assumed in all analyses for this system, and the most reactive rod cluster is assumed to be in the fully withdrawn position. Boration control via the CVCS maintains the reactor in the cold shutdown state independent of the position of the control rods and can compensate for xenon burnout transients.

Further information on RCCAs is provided in Chapter 4 and Chapter 7. Boric acid concentration control is described in Section 9.3.4. Performance analyses under accident conditions are included in Section 15.0.

3.1.3.8 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."

3.1.3.8.1 U.S. EPR Compliance

The U.S. EPR makes and holds the core subcritical under any anticipated conditions and with appropriate margin for contingencies. The means to accomplish this are described in detail in Chapter 4 and Chapter 9. Combined use of the rod cluster control system and the CVCS permits the necessary shutdown margin to be maintained during long-term xenon decay and plant cooldown. The most reactive rod control cluster is assumed to be in the fully withdrawn position upon trip for this determination.

3.1.3.9 Criterion 28 – Reactivity Limits

"The reactivity control system 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 (1) 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."

3.1.3.9.1 U.S. EPR Compliance

The maximum reactivity worth of the control rods, the maximum rates of RCCA reactivity insertion, and boron removal together prevent reactivity increases from rupturing the reactor coolant system boundary or disrupting the core or vessel internals to a degree that could impair emergency core cooling. The appropriate reactivity insertion rate for the withdrawal of RCCAs and the dilution of the boric acid in the reactor coolant systems are described in Chapter 4 and Chapter 15. These chapters include graphs that show the permissible withdrawal limits and overlap of the RCCA banks as a function of power. The capability of the CVCS to avoid an inadvertent excessive rate of boron dilution is described in Chapter 9. The relationship of the reactivity insertion rates to plant safety is addressed in Chapter 15.

Core cooling capability following accidents (e.g., rod ejection, steam line break) is maintained 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 features.

3.1.3.10 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."

3.1.3.10.1 U.S. EPR Compliance

The protection and reactivity control systems accomplish their safety functions in the event of anticipated operational occurrences. Redundancy, high quality equipment, functional diversity, extensive fault detection and fault accommodation, and high quality software design processes contribute to high reliability of the protection and reactivity control systems. Further information concerning the design of the protection and reactivity control systems is found in Chapter 4 and Chapter 7.

3.1.4 Fluid Systems

3.1.4.1 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.”

3.1.4.1.1 U.S. EPR Compliance

RCS pressure boundary components are designed, fabricated, inspected, and tested in conformance with the ASME Code, Section III. Section 3.2 lists the quality group and safety classifications of the components that are included in the RCS pressure boundary. The design bases and evaluations of the RCS pressure boundary are described in Chapter 5.

Several methods are available for detecting reactor coolant leakage. In one method, the reactor vessel closure joint is provided with a temperature monitored leakoff between double gaskets. Leakage inside the reactor containment is drained to the Reactor Building sump where the level is monitored. Leakage is also detected by measuring the airborne activity of the containment. Indication of containment humidity is also available as an indirect indication of leakage. Monitoring of the inventory of reactor coolant in the system at the pressurizer, volume control tank, and coolant drain collection tank provides an indication of integrated leakage. Further information on the reactor coolant pressure boundary leakage detection system is provided in Section 5.2.5.

3.1.4.2 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."

3.1.4.2.1 U.S. EPR Compliance

Brittle fracture control of the reactor coolant pressure boundary is provided through design, material selection, and fabrication of the RCS so that the boundary behaves in a nonbrittle manner. The RCS materials that are exposed to the primary coolant are corrosion-resistant stainless steel or nickel-chrome-iron alloy. The reference temperature (RT_{NDT}) of the reactor vessel pressure boundary steel is established by Charpy V-notch and drop weight tests in accordance with 10 CFR 50, Appendix G. The fabrication and quality control techniques used in the fabrication of the RCS components and piping are governed by Reference 2 requirements (refer to Section 5.2 and Section 5.3).

Allowable pressure-temperature relationships for plant heatup and cooldown rates are calculated using methods derived from the ASME Code, Section III, Appendix G

(Reference 3). This approach specifies that allowed stress intensity factors for all vessel operating conditions will not exceed the reference critical stress intensity factor (K_{IC}) for the metal temperature at any time. Operating specifications include conservative margins for predicted changes in the RT_{NDT} due to irradiation.

3.1.4.3 Criterion 32 – Inspection of Reactor Coolant Pressure Boundary

"Components which are part of the reactor coolant pressure boundary shall be designed to permit (l) 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."

3.1.4.3.1 U.S. EPR Compliance

The design of the reactor coolant pressure boundary provides access to the entire internal surface of the reactor vessel and most external zones of the vessel. Accessible areas include the nozzle to reactor coolant piping welds, the vessel shell beneath the nozzles, the top and bottom heads, and external surfaces of the reactor coolant piping, except for the area of pipe within the primary shielding concrete. The access provided allows inspections to complement the leakage detection systems in assessing the pressure boundary integrity. The reactor coolant pressure boundary is periodically inspected under the provisions of the ASME BPV Code, Section XI (Reference 4).

The design of the reactor coolant pressure boundary piping provides accessibility to welds that require inservice inspection under the provisions of Reference 4. Removable insulation is provided at welds that require inservice inspection. The inservice inspection program for the reactor coolant pressure boundary is described in Section 5.2.4.

The material surveillance program includes conventional tensile and impact tests and fracture mechanics specimens. The observed shifts in RT_{NDT} of the core region materials with irradiation are used to confirm the allowable limits calculated for operational transients. Changes in the fracture toughness properties of the reactor vessel core region plates forging, weldments, and associated heat treated zones are monitored in accordance with 10 CFR 50, Appendix H. Samples of reactor vessel plate materials are retained and catalogued in case future engineering development shows the need for further testing.

3.1.4.4 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."

3.1.4.4.1 U.S. EPR Compliance

The pressurizer level program accommodates changes in the reactor coolant volume for normal power changes, including the transition from hot standby to full-power operation and returning to hot standby. The pressurizer also has sufficient volume to accommodate minor RCS leakage.

Safety-related RCS 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 the medium-head and low-head safety injection (MHSI and LHSI) accumulators, and the in-containment refueling water storage tank (IRWST). Long-term cooling is provided by recirculation of reactor coolant through the LHSI system. Further information on the LHSI system is provided in Section 6.3. The safety-related reactor coolant makeup relies on the Class 1E system and is designed to remain functional in spite of a single active component failure coincident with the loss of either the offsite or onsite power source.

The CVCS provides reactor coolant makeup and adjustment of the boric acid concentration. The CVCS provides two flow paths for the continuous letdown and charging of RCS water. The CVCS maintains the reactor coolant system water inventory at the desired level via the pressurizer level control system and provides reactor coolant pump seal water injection and auxiliary spray for pressurizer cooldown. The CVCS is an operational system and is not required for the mitigation of design basis accidents. However, it may be used to preclude the use of safety systems during minor transients, such as boron dilution events. The CVCS is normally in continuous operation during all modes of plant operation from normal power operation to cold shutdown. The CVCS components and valve operators are provided with emergency power and are available following a loss of onsite or offsite power. Further information on the CVCS is provided in Section 9.3.4.

3.1.4.5 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."

3.1.4.5.1 U.S. EPR Compliance

The safety injection/residual heat removal system (SIS/RHRS) provides normal shutdown cooling as well as emergency coolant injection and recirculation functions to maintain reactor core coolant inventory. This system provides decay heat removal following a LOCA. The SIS/RHRS also maintains reactor core inventory following a main steam line break.

The calculated cooling performance of the SIS/RHRS following postulated LOCAs complies with the criteria of 10 CFR 50.46. RHR is performed by forced flow with the LHSI pumps and cooling of the water taken from the hot legs via the LHSI heat exchangers. Each of the four SIS trains is provided with a separate suction connection to the In-Containment Refueling Water Storage Tank (IRWST). Guard pipes are provided for sump suction piping between the sump connection and the suction isolation valve. The sumps are provided with a series of screens that protect the SIS pumps against debris entrained in the IRWST fluid.

The SIS/RHRS trains are powered from separate emergency buses, each backed by an EDG. Thus, the SIS/RHRS is designed to remain functional in spite of a single active component failure coincident with the loss of either the offsite or onsite power source. Further information on the SIS/RHRS is provided in Section 5.4.7 and Section 6.3

The emergency feedwater system (EFWS) also supplies water to the steam generators (SG) to maintain water level and remove decay heat following the loss of normal feedwater supplies due to anticipated operational transients and design basis accident conditions. This system removes heat from the RCS, which is first transferred to the secondary side via the SGs and then discharged as steam to the condenser or via the SG main steam relief valve. Further information on the EFWS is provided in Section 10.4.

3.1.4.6 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 (l) 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."

3.1.4.6.1 U.S. EPR Compliance

For the U.S. EPR, the SIS/RHRS provides emergency core cooling. The SIS/RHRS has sufficient capacity, diversity, and independence to perform its required safety functions following transients or design basis accidents assuming a single failure in one train while a second train is out of service for maintenance. As noted in the discussion for GDC 34, the SIS/RHRS is designed to remain functional in spite of a single active component failure coincident with the loss of either the offsite or onsite power source.

The SIS/RHRS consists of four independent trains, each providing injection capability by an accumulator pressurized with nitrogen gas, a MHSI pump, and an LHSI pump. In the injection mode, the MHSI and LHSI pumps take suction from the IRWST and inject into the RCS. These pumps are located in the Safeguard Buildings. The LHSI pumps and the MHSI pumps normally inject into the cold legs. Following a cold leg break, the LHSI discharge can be switched to the hot legs to limit the boron concentration in the core, thus reducing the risk of boron precipitation in the upper part of the core. The SIS/RHRS is designed to accomplish the required safety functions even with a single failure. Further information on the SIS/RHRS is provided in Section 5.4.7 and Section 6.3

The function of the IRWST is to contain a large amount of borated water at a homogeneous concentration and temperature. It is the safety-related source of water for emergency core cooling in the event of a LOCA and is a source of water for containment cooling. During a LOCA, the IRWST collects the discharge from the RCS, allowing it to be recirculated by the SIS. Further information on the IRWST is provided in Section 6.3.

3.1.4.7 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."

3.1.4.7.1 U.S. EPR Compliance

The U.S. EPR systems that provide emergency core cooling (refer to GDC 35) are accessible for visual inspection and for nondestructive inservice inspection, as required by the ASME BPV Code Section XI (Reference 4). Components outside the containment are accessible for leak-tightness inspection during operation of the reactor.

The system piping and components are designed to permit access for periodic inspection and testing of equipment, according to the ASME Code and Technical Specifications requirements, to provide confidence in the integrity and capability of the system. Additionally, components such as pressure vessels, pumps, valves, piping, and supports are designed for accessibility for preservice inspection, as well as inservice inspection. The arrangement of the components inside their respective buildings allows access for the examinations required by Reference 4. Physical arrangement of these items provides personnel access to enable volumetric and surface examinations and provides sufficient access to supports for visual examinations.

Details of the inspection program for the U.S. EPR systems that provide emergency core cooling are described in Section 6.3.

3.1.4.8 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 (l) 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."

3.1.4.8.1 U.S. EPR Compliance

As noted in the discussion for GDC 35, the SIS/RHRS provides emergency core cooling for the U.S. EPR. The SIS/RHRS design permits the periodic inspection and testing of the appropriate system components. The testing capabilities of the system include inservice testing and inspection to confirm the structural and leak-tight integrity of various components, technical specification operability and performance of the active system components, and additional inservice testing to confirm the overall operability of the system. Inservice inspection of the SIS/RHRS can be performed periodically during power operation of the plant for the system portions outside the Reactor Building. Further information on the SIS/RHRS is provided in Section 5.4.7 and Section 6.3. For electrical power details, refer to Chapter 8.

3.1.4.9 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."

3.1.4.9.1 U.S. EPR Compliance

For the U.S. EPR, the containment heat removal function is provided by the SIS/RHRS (see Section 5.4.7 and Section 6.3). Due to its large free volume and heat capacity, the U.S. EPR containment does not rely on active systems for short-term pressure and temperature control. In a design basis accident, the LHSI/RHR heat exchanger, located outside of containment, provides long-term containment heat removal. Under design basis conditions, the LHSI draws water from the IRWST and rejects the containment heat to the plant cooling water systems through the LHSI/RHR heat exchanger before being injected into the RCS. As noted in the discussion for GDC 34, the SIS/RHRS is designed to remain functional in spite of a single active component failure coincident with the loss of either the offsite or onsite power source. Further information on the containment heat removal function is provided in Section 6.2.2.

3.1.4.10 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."

3.1.4.10.1 U.S. EPR Compliance

For the U.S. EPR, inspection of the containment heat removal function is provided as part of the ECCS function. See GDC 36 for a discussion of the ECCS inspections

3.1.4.11 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."

3.1.4.11.1 U.S. EPR Compliance

For the U.S. EPR, testing of the containment heat removal function is provided as part of the ECCS function. See GDC 37 for a discussion of testing of the ECCS.

3.1.4.12 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."

3.1.4.12.1 U.S. EPR Compliance

Several plant features serve to reduce or limit the release of fission products following a postulated accident. These systems include the containment, containment isolation system, and ESF filter systems. Further information on the U.S. EPR fission product and removal control system is provided in Section 6.5.

Fission product control for the U.S. EPR is provided via natural passive removal processes within containment and by limiting containment leakage. The passive removal processes, such as deposition and sedimentation, are evaluated based on use of an alternative source term under 10 CFR 50.67; refer to Section 6.5 for additional details. The containment and penetrations are designed to minimize overall containment leakage; refer to Section 6.2 for additional details. Combustible gas control is achieved through compliance with 10 CFR 50.44. The combustible gas control system is described in Section 6.2.5.

3.1.4.13 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."

3.1.4.13.1 U.S. EPR Compliance

The containment atmosphere cleanup systems are designed and located so that they can be inspected periodically, as required. Further information is provided in Section 6.2.5 and Section 6.5.

3.1.4.14 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."

3.1.4.14.1 U.S. EPR Compliance

The appropriate portions of the containment atmosphere cleanup system are designed to permit periodic pressure and functionality testing. 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 Section 6.2.3. Further information is provided in Section 6.2.2 and Section 6.2.5. For electrical power details, refer to Chapter 8.

3.1.4.15 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."

3.1.4.15.1 U.S. EPR Compliance

The component cooling water system (CCWS) and essential service water system (ESWS) transfer heat from plant safety-related components to the ultimate heat sink. These systems are designed to transfer their respective heat loads under anticipated normal and design basis accident conditions. Suitable redundancy, leak detection, systems interconnection, and isolation capabilities are incorporated in the design of these systems to accomplish the required safety function, assuming a single failure with either onsite or offsite power.

The CCWS consists of both a safety-related portion and a non-safety-related portion. The safety-related portion has the same number of trains as the safety systems that require cooling by the CCWS. Common headers include redundant safety-grade isolation valves and provide train separation (as required during plant transients or design basis accidents). The ESWS provides the heat sink for the CCWS and has the same number of trains as the CCWS. The CCWS and ESWS are designed to remain functional in spite of a single active component failure coincident with the loss of either the offsite or onsite power source. Further information on the CCWS and the ESWS is provided in Section 9.2.

3.1.4.16 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."

3.1.4.16.1 U.S. EPR Compliance

The integrity and capability of the CCWS and the ESWS are monitored during normal operation by alternating operation of the systems between the redundant system components. System components vital to operation are located in accessible areas, with the exception of any underground piping for the ESWS. These components have suitable manholes, handholes, inspection ports, or other appropriate design and layout features to allow periodic inspection. The integrity of any underground piping is demonstrated by pressure and functional tests. Further information on the inspection and testing requirements for the CCWS and the ESWS is provided in Section 9.2.

3.1.4.17 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 leaktight 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."

3.1.4.17.1 U.S. EPR Compliance

The component cooling system operates continuously during normal plant operation, shutdown, and under flow and pressure conditions for design accidents. A minimum of two of the four trains of cooling (including the CCWS and ESWS) are normally in operation. The ESWS distribution piping uses the service water system cooling flow during normal plant operation and at flows and pressures approximating accident

conditions. The design allows for periodic starting of the essential service water pumps and verification of the required flowpath at pressure conditions approximating the design accident conditions. These operations demonstrate the operability, performance, and structural and leak-tight integrity of cooling chain components.

The cooling water system design includes the capability for testing through the full operational sequence that brings the system into operation for reactor shutdown and for LOCAs. This capability includes operation of applicable portions of the protection system and the transfer between normal and emergency power sources. Further information on the inspection and testing requirements for the CCWS and the ESWS is provided in Section 9.2. For electrical power details, refer to Chapter 8.

3.1.5 Reactor Containment

3.1.5.1 Criterion 50 – Containment Design Basis

"The reactor containment structure, including access openings, 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 as required by § 50.44 energy from metal-water and other chemical reactions that may result from degradation but not total failure of 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."

3.1.5.1.1 U.S. EPR Compliance

The design of the U.S. EPR containment structure is based on the containment design basis accidents, which include the rupture of a reactor coolant pipe in the RCS or the rupture of a main steam line. Section 6.2 addresses the maximum pressure and temperature, the calculational model, and the input parameters for containment design basis accidents. The containment design provides margin for extra energy sources. Section 3.8 and Section 6.2 provide additional information on the containment design basis.

3.1.5.2 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."

3.1.5.2.1 U.S. EPR Compliance

The reactor containment boundary is constructed of post-tensioned concrete lined with steel. The load-carrying component is post-tensioned concrete and is designed and constructed to be serviceable and have sufficient strength to preclude failure under accident conditions in accordance with applicable codes and standards. The ferritic materials (e.g., liner, liner components, equipment hatch, air locks) exposed to the internal environment of containment are selected and designed to preclude brittle fracture for design basis loading conditions, taking into account uncertainties associated with material properties, stresses, and flaw sizes. Principal load carrying components are designed such that the probability of rapidly propagating fracture is minimized. Further information on the containment design is provided in Section 3.8 and Section 6.2.

3.1.5.3 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."

3.1.5.3.1 U.S. EPR Compliance

In accordance with the requirements of 10 CFR 50, Appendix J, the containment system design contains equipment to permit periodic integrated leakage rate tests. Section 6.2 contains the details of the periodic integrated leakage rate tests.

3.1.5.4 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."

3.1.5.4.1 U.S. EPR 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. Section 6.2 provides further information on the provisions for containment testing and inspection. Section 3.8 provides information on Seismic Category I structures.

3.1.5.5 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."

3.1.5.5.1 U.S. EPR Compliance

Piping systems that penetrate the primary reactor containment are equipped with containment isolation valves. Penetrations that must be closed for containment isolation have redundant valving. Automatic isolation valves, which do not restrict normal plant operation, are periodically tested to confirm operability. Section 6.2addresses the isolation valve arrangements.

Piping that penetrates the containment is either equipped with test connections and test vents or has other provisions to allow for periodic leak rate testing and detection in order to maintain leakage within the acceptable limit as defined by the Technical Specifications and 10 CFR 50, Appendix J. Section 7.3 provides further information on the isolation signals for piping systems that penetrate containment. Section 5.2.5 provides further information on the leakage detection systems.

The fuel transfer tube connects to the leakage exhaust system, which recovers potential leakage during normal plant operation when the transfer tube is closed and not filled with water. Manual isolation valves isolate the transfer tube in the Reactor Building and the Fuel Building. A blind flange isolates the transfer tube inside the containment, except when the reactor is shut down for refueling.

3.1.5.6 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:

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

- One locked closed 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; or

- 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 inservice inspection, protection against more severe natural phenomena, and additional isolation valves and containment, shall include consideration of the population density, use characteristics, and physical characteristics of the site environs."

3.1.5.6.1 U.S. EPR Compliance

Lines that are a part of the reactor coolant pressure boundary and penetrate the containment contain isolation valves that comply with the arrangements described in GDC 55. Section 6.2 addresses the isolation valve arrangements.

3.1.5.7 Criterion 56 – Primary Containment Isolation

"Each line that connects directly to the containment atmosphere and 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:

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

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

- One locked closed 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; or

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

3.1.5.7.1 U.S. EPR Compliance

In accordance with the acceptable arrangements described in GDC 56, lines that communicate directly with the containment atmosphere and penetrate the reactor containment are normally provided with two isolation valves in series, one inside and one outside the containment. The exception to this principle occurs in the lines from the IRWST sumps to the SIS pumps, which have only one isolation valve. In this case, a sealed envelope guard pipe contains the piping between the sump and the valve, thus providing a double leak-tight penetration barrier. This leak-tight double barrier withstands the design basis environmental conditions from the containment penetration to the containment isolation valve inside the containment; the design of this barrier takes into account a single functional or passive failure. Further information on how the containment systems meet GDC 56 is provided in Section 6.2.

3.1.5.8 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, or 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."

3.1.5.8.1 U.S. EPR Compliance

Each line that penetrates the containment and is neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere has at least one isolation valve outside containment, and located as close to the containment as practical, in accordance with the requirements of GDC 57. Section 6.2.4 provides further information on compliance with GDC 57.

3.1.6 Fuel and Reactivity Control

3.1.6.1 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 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."

3.1.6.1.1 U.S. EPR Compliance

The U.S. EPR is designed to control the release of radioactive materials in gaseous and liquid effluents and to handle radioactive solid wastes produced during normal reactor operation, which includes anticipated operational occurrences. The radioactive waste management systems are designed to minimize inadvertent releases of radioactivity from the facility and to maintain permitted radioactive waste discharges below the regulatory limits of 10 CFR 50, Appendix I, during normal operation. The radioactive waste processing system, its design criteria, and the estimated releases of radioactive effluents to the environment are described in Chapter 11.

3.1.6.2 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."

3.1.6.2.1 U.S. EPR Compliance

The fuel pool cooling and purification system consists of the fuel pool cooling system (FPCS) and the fuel pool purification system (FPPS). These systems, along with the fuel handling system, the spent fuel pool area ventilation system, and radioactive waste processing system, provide adequate safety under normal reactor operation and postulated accident conditions. Specifically, these systems include the following design capabilities:

- The FPCS provides cooling to remove residual heat from the fuel stored in the spent fuel pool. The system is designed with redundancy and testability to provide continued heat removal during normal operation, plant shutdown, refueling, and accident conditions. The FPCS is described in Section 9.1.3.

- The FPCS has two separate and independent trains located on opposite sides of the spent fuel pool. The FPPS includes two purification pumps that operate in

parallel. There are two purification paths, one is part of the FPPS and the other path utilizes the coolant purification system.

- The spent fuel pool is designed so that no postulated event could cause excessive loss-of-pool water inventory. Refer to Section 9.1 for additional information. Fuel handling and cask accidents are addressed in Section 15.7.

- Structures, components, and systems are designed and located so that appropriate periodic inspection and testing can be performed.

- Shielding is provided as described in Chapter 12. Radiation monitoring is provided as described in Chapters 11 and 12.

- Individual components that contain significant radioactivity are in confined areas adequately ventilated through appropriate filtering systems. Further information regarding the spent fuel pool area ventilation system is provided in Section 9.4.2. Information on the radioactive waste management systems is provided in Chapter 11.

3.1.6.3 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."

3.1.6.3.1 U.S. EPR Compliance

The restraints and interlocks provided for the safe handling and storage of new and spent fuel are addressed in Section 9.1. Criticality in the new and spent fuel storage areas is prevented by physical separation of fuel assemblies and the use of borated water and borated neutron absorber panels in the fuel storage pool.

3.1.6.4 Criterion 63 – Monitoring Fuel and Waste Storage

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

3.1.6.4.1 U.S. EPR Compliance

Instrumentation is provided to detect and to alarm the main control room when excessive temperature or low water level occurs in the spent fuel pool. Additionally, area radiation monitors are provided in the fuel storage area for personnel protection and general surveillance. These area monitors alarm locally and in the main control room.

The Fuel Building ventilation system provides appropriate ventilation and filtration to limit potential release of airborne radioactivity to the environment from the fuel

storage facility under normal operation and in the event of a fuel handling accident in the fuel pool area. This ventilation system is continuously monitored by gaseous, particulate, and radio-iodine radiation monitors, which alarm locally and in the MCR. Isolation dampers provide isolation of the ventilation system for specific rooms within the Fuel Building to mitigate the consequences of a fuel handling accident. Further information on the Fuel Building ventilation system is provided in Section 9.4.2.

3.1.6.5 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."

3.1.6.5.1 U.S. EPR 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 can be taken via the sampling activity monitoring system to provide data on airborne radioactive concentrations within the containment.

Facility radioactivity levels in the effluent discharge paths and in the plant environs are continuously monitored during normal and accident conditions by the plant radiation monitoring systems. Samples of the facility effluent discharge paths can be taken via the sampling system to provide data on effluent radioactivity. High radiation signal from in-containment radiation monitors causes an automatic closure of the discharge path isolation valve.

Area radiation monitors (ARM) located in the Safeguard and Radioactive Waste Processing Buildings are provided to continually monitor radiation levels in the spaces which contain components for recirculation of LOCA fluids and components for processing radioactive wastes. The ARMs also supplement the personnel and area radiation survey provisions of the U.S. EPR health physics program (described in Section 12.5). The ARMs comply with the personnel radiation protection guidelines of 10 CFR 20, 10 CFR 50, 10 CFR 70, and RG 1.97, RG 8.2, RG 8.8, and RG 8.12.

In addition to the installed detectors, the plant conducts periodic plant environmental surveillance. Measurement capability and reporting of effluents are based on the guidelines of RG 1.4 and RG 1.21, as addressed in Section 1.9 Additional information on the U.S. EPR radioactive waste management systems is provided in Chapter 11. Further information on the U.S. EPR radiation protection features is provided in Chapter 12.

3.1.7 References

1. ANSI/ASME NQA-1-1994, "Quality Assurance Program Requirements for Nuclear Facilities," American Society of Mechanical Engineers, 1994.

2. ASME Boiler and Pressure Vessel Code, Section III: "Rules for Construction of Nuclear Power Plant Components," American Society of Mechanical Engineers, 2004 (no Addenda).

3. ASME Boiler and Pressure Vessel Code, Section III, Appendix G: "Fracture Toughness Requirements," The American Society of Mechanical Engineers, 2004 (no Addenda).

4. ASME Boiler and Pressure Vessel Code, Section XI: "Rules for Inservice Inspection of Nuclear Power Plant Components," The American Society of Mechanical Engineers, 2004 (no Addenda).

Next File