CHAPTER 03 – DESIGN OF STRUCTURES, SYSTEMS, COMPONENTS, AND EQUIPMENT

3.1 Conformance with Nuclear Regulatory Commission General Design Criteria

3.1.1 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."

Response:

The structures, systems, and components (SSCs) described in the Design Control Document (DCD) are classified according to their importance to safety, including the prevention and mitigation of accidents using the classification system described in ANSI/ANS 51.1 (Reference 1). Each component is given a safety class designation. The codes, standards, and quality control applicable to each component and safety class designation are identified in Section 3.2. The design and fabrication of SSCs conform to 10 CFR 50.55a (Reference 2) as applicable. The quality assurance program conforms to the requirements of 10 CFR 50, Appendix B (Reference 3), and is addressed in Section 17.3. Chapter 14 describes the initial tests and operations that are conducted on installed equipment to provide reasonable assurance that the performance of the equipment is commensurate with the importance of the safety function.

The design, fabrication, and quality programs for components not included in the American National Standards Institute (ANSI) classification system are governed by industry codes

appropriate to the application. Additional details are described in the relevant DCD sections.

3.1.2 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 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."

Response:

The SSCs important to safety are designed to accommodate, without loss of capability, the effects of the design basis natural phenomena along with appropriate combinations of normal and accident conditions, as described in this chapter. Additional design information is provided in the sections that describe the individual SSCs.

3.1.3 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."

Response:

The pressure boundary components and structures and the attendant auxiliary systems in the APR1400 design scope are designed to minimize the probability and effects of fires and explosions. High-grade noncombustible and fire-resistant materials are used for components located in the containment, components of engineered safety feature systems, and throughout the plant wherever practical. The fire protection system is described in Subsection 9.5.1.

3.1.4 Criterion 4 – Environmental and Dynamic Effects Design Bases

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

Response:

SSCs important to safety are designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including a LOCA as described in Section 3.11.

Where appropriate, design bases include design requirements that provide reasonable assurance that SSCs are appropriately protected against dynamic effects such as missiles, pipe whipping, fluid discharges that could result from equipment failures, postulated accidents, and events and conditions outside the nuclear power plant.

The design concept of leak-before-break (LBB) is applied to the reactor coolant piping including surge line, safety injection, and shutdown cooling piping inside containment. The LBB concept eliminates the dynamic effects of postulated pipe ruptures from the design basis and is carried out in accordance with SRP 3.6.3 (Reference 4) and NUREG-1061 (Reference 5) Volume 3. The applications of LBB provisions are described in Subsection 3.6.3.

3.1.5 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 units."

Response:

SSCs that perform safety-related functions are not shared between two units because the APR1400 is a single-unit plant.

3.1.6 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."

Response:

Specified acceptable fuel design limits (SAFDLs) are described in Subsection 4.4.1. Operation within the limiting conditions for operation (LCOs) specified by the Technical Specifications keeps the reactor fuel within the SAFDLs for normal operation, including anticipated operational occurrences (AOOs).

The plant is designed so that operation within the LCOs and limiting safety system settings (LSSSs) prescribed in the Technical Specifications results in confidence that SAFDLs are

not exceeded as a result of an AOO. Operator action, aided by control systems and monitored by plant instrumentation, maintains the plant within LCO limits during normal operation.

Additional information is provided in the following sections:

a. Section 4.2, Fuel System Design

b. Chapter 5, Reactor Coolant System and Connecting Systems

c. Subsection 5.4.7, Shutdown Cooling System

d. Section 7.2, Reactor Trip System

e. Chapter 15, Transient and Accident Analyses

f. Chapter 16, Technical Specifications

3.1.7 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."

Response:

In the power operating range, the combined response of the fuel temperature coefficient (FTC), moderator temperature coefficient (MTC), moderator void coefficient, and moderator pressure coefficient to an increase in reactor power is a decrease in reactivity (i.e., the inherent nuclear feedback characteristics are not positive).

The reactivity coefficients for this reactor are described in Subsection 4.3.1.4.

3.1.8 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."

Response:

Total reactor power oscillations of the fundamental mode stability is provided by the negative power coefficient of reactivity (GDC 11, Subsection 3.1.7) and the coolant temperature program maintained by regulating rods. Power level is continuously monitored by neutron flux detectors (Chapter 7).

Power distribution oscillations are detected by neutron flux detectors. Axial mode oscillations are suppressed by means of part-strength or full-strength neutron absorber rods. All other modes of oscillation are expected to be convergent. Monitoring and protective requirements imposed by GDC 10 and 20 are described in Subsections 3.1.6 and 3.1.16 and Chapter 4.

3.1.9 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."

Response:

Instrumentation is provided to monitor significant process variables that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary (RCPB), and their associated systems. Controls are provided for the purpose of maintaining these variables within the limits prescribed for safe operation.

Instrumentation and control for the containment and its associated systems are described in Chapters 6 through 12. The principal process variables to be monitored and controlled are:

a. Neutron flux level (reactor power)

b. Control element assembly (CEA) positions

c. Neutron flux distribution (at various axial positions)

d. Reactor coolant temperature and pressure

e. Reactor coolant pump (RCP) speed

f. Pressurizer (PZR) level

g. Steam generator (SG) level and pressure

The departure from nucleate boiling ratio (DNBR) margin and local power density (LPD) margin (kW/cm) are also monitored.

The plant protection system (PPS) consists of the reactor protection system (RPS) and engineered safety features actuation system (ESFAS). The RPS is designed to monitor nuclear steam supply system (NSSS) operating conditions and initiate reliable and rapid reactor shutdown if monitored variables or combinations of monitored variables deviate from the permissible operating range to a degree that a safety limit may be reached. The ESFAS is designed to monitor plant variables and to actuate ESF systems during a design basis event (DBE).

The following systems and equipment are provided to monitor and maintain control over the fission process during transient and steady-state periods over the life of the core:

a. Redundant channels of ex-core nuclear instrumentation as the primary means of monitoring the fission process for protection, control, and low power operation

b. Redundant and diverse CEA position-indicating systems

c. Manual and automatic control of reactor power by means of CEAs

d. Manual regulation of boron concentration in the reactor coolant

e. A boronometer to determine boron concentration in the reactor coolant by neutron absorption as a backup to routine sampling and analysis

f. In-core instrumentation, provided to supplement information on core power distribution and enable calibration of ex-core flux detectors

The non-nuclear instrumentation measures temperatures, pressures, flows, and levels in the reactor coolant, main steam, and auxiliary systems and is used to maintain these variables within the prescribed limits. The instrumentation and control (I&C) systems are described in Chapter 7. The boronometer is described in Subsections 7.7.1.1 and 9.3.4.2. The process radiation monitor is described in Subsection 9.3.4.2.

When a variable is to be monitored during and after a DBE, in addition to normal operation, the event analysis results are used to provide reasonable assurance that the instruments provided cover the range anticipated for the event conditions.

3.1.10 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."

Response:

The RCPB is defined in accordance with 10 CFR 50.2 and ANSI/ANS 51.1, as described in the response to GDC 55, Subsection 3.1.48.

Reactor coolant system (RCS) components are designed to meet the requirements of ASME Section III. To establish operating pressure and temperature limitations during startup and shutdown of the RCS, the fracture toughness rules defined in ASME Section III are followed. Quality control, inspection, and testing are performed as required by ASME

Section III and allowable reactor pressure-temperature operations are specified to provide reasonable assurance of the integrity of the RCS.

The RCPB is designed to accommodate the system pressures and temperatures attained under all expected modes of unit operation, including anticipated transients, and maintain the stresses within applicable limits.

Piping and equipment pressure parts of the RCPB are assembled and erected by welding unless applicable codes permit flanged or screwed joints. Welding procedures that produce welds of complete fusion and free of unacceptable defects are followed. All welding procedures, welders, and welding machine operators are qualified in accordance with the requirements of ASME Section IX for the materials to be welded. Qualification records, including the results of the procedure and performance qualification tests and identification symbols assigned to each welder, are maintained.

The pressure boundary has provisions for in-service inspection in accordance with ASME Section XI to provide reasonable assurance of the continuance of the structural and leak-tight integrity of the boundary, as described in the response to GDC 32, Subsection 3.1.28. For the reactor vessel, a material surveillance program conforming to the requirements of 10 CFR 50, Appendix H, is provided.

3.1.11 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 any condition of normal operation, including anticipated operational occurrences."

Response:

The design criteria and bases for the RCPB are described in the response to GDC 14.

The operating conditions for normal steady-state and transient plant operations are established conservatively. Normal operating limits are selected so that an adequate margin exists between normal operating limits and design limits. The plant control

systems are designed to provide reasonable assurance that plant variables are maintained well within established operating limits. The plant transient response characteristics and pressure and temperature distributions during normal operations are considered in the design as well as the accuracy and response of the instruments and controls. These design techniques provide reasonable assurance that a satisfactory margin is maintained between normal operating conditions, including design transients, and design limits for the RCPB.

Plant control systems function to minimize the deviations from normal operating limits in the event of AOOs. When the control system is inadequate or fails to respond upon demand, the plant protection system starts functioning to mitigate the consequences of such events.

The plant protection system functions to mitigate the consequences in the event of accidents. Analyses show that design limits for the RCPB are not exceeded in the event of any ANSI/ANS 51.1-1983 conditions.

3.1.12 Criterion 16 – Containment Design

"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."

Response:

The containment design incorporates a post-tensioned concrete containment with a steel liner to enclose the nuclear steam supply system completely. The containment system is designed to protect the public from the consequences of a LOCA, based on the equivalent energy release of a postulated break of reactor coolant piping up to and including a double-ended break of the largest reactor coolant pipe.

The containment building and the associated engineered safety feature systems are designed to safely withstand all internal and external environmental conditions that may reasonably be expected to occur during the life of the plant, including both short- and long-term effects of a LOCA.

The design criteria and methods of analysis for the containment structure are described in Subsections 3.8.1 and 3.8.2. The leak-tightness of the containment system and short- and long-term performance following a LOCA are described in Section 6.2.

3.1.13 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 the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents.

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

Electric power from the transmission network to the onsite electric distribution system shall be supplied by two physically independent circuits (not necessarily on separate rights of way) designed and located so as to minimize to the extent practical the likelihood of their simultaneous failure under operating and postulated accident and environmental conditions. A switchyard common to both circuits is acceptable. Each of these circuits shall be designed to be available in sufficient time following a loss of all onsite alternating current power supplies and the 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."

Response:

The APR1400 design is provided with an onsite electric power system and an offsite electric power system to permit functioning of SSCs important to safety in compliance with the requirements of this GDC, as described in Chapter 8.

The onsite electric power system consists of separate, redundant, and independent distribution systems and dedicated power supplies with sufficient capacity, capability, and testability to perform associated safety functions assuming a single failure.

The offsite electric power is supplied to the plant from the transmission network by at least two independent circuits through the site-specific switchyard. Each circuit is immediately available and has sufficient capacity and capability to perform the associated safety function.

Provisions are made 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.

3.1.14 Criterion 18 – Inspection and Testing of Electrical 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."

Response:

Electrical power systems important to safety are 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 to detect deterioration, if any, of their components. Capability is provided to periodically test the operability and functional performance of the system components. The diesel generator sets are started and loaded periodically on a routine basis, and relays, switches, and buses are inspected and tested for operation and availability.

Transfer from normal to emergency sources of power is performed to check system operability and the full operational sequence that brings the systems into operation.

Further information is provided in Subsections 8.3.1 and 8.3.2 and in Chapter 16.

3.1.15 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.

Applicants for and holders of construction permits and operating licenses under this part who apply on or after January 10, 1997, applicants for design approvals or certifications under part 52 of this chapter who apply on or after January 10, 1997, applicants for and holders of combined licenses or manufacturing licenses under part 52 of this chapter who do not reference a standard design approval or certification, or holders of operating licenses using an alternative source term under § 50.67, shall meet the requirements of this criterion, except that with regard to control room access and occupancy, adequate radiation protection

shall be provided to ensure that radiation exposures shall not exceed 0.05 Sv (5 rem) total effective dose equivalent (TEDE) as defined in § 50.2 for the duration of the accident."

Response:

All control and monitoring equipment necessary to operate or shut the unit down and maintain safe control of the facility is located in the main control room (MCR).

The design of the MCR permits safe occupancy during abnormal conditions. The use of non-combustible and fire-retardant materials in the construction of the MCR, the limitation of combustible supplies, the location of firefighting equipment, and the continuous presence of a trained operator minimize the possibility that the MCR will become uninhabitable. Radiation exposure levels following design-basis accidents are maintained below allowable levels by proper design of shielding and ventilation. The MCR ventilation system is designed to allow access to occupancy of the MCR under accident conditions without personnel receiving radiation exposures in excess of 0.05 Sv (5 rem) TEDE during the accident. Fission product removal is performed by the MCR heating, ventilation and air conditioning (HVAC) system to remove iodine and particle matter, thereby minimizing the dose that could result from the accident. Radiation detectors and alarms are provided. MCR habitability features are described in Section 6.4. Emergency lighting is described in Subsection 9.5.3.

If the MCR is inaccessible, alternate local controls and instruments are available for equipment required to establish and maintain a hot standby condition, as well as cold shutdown. Hot and cold shutdown capability is addressed in Section 7.4 for the systems required for safe shutdown. The MCR is described in Subsection 7.7.1.2. Human factors issues are addressed in Chapter 18.

Radiation protection for the plant's control facilities is addressed in Section 6.4 and Chapter 2.

3.1.16 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."

Response:

A plant protection system (PPS), consisting of a reactor protection system (RPS) and an engineered safety features actuation system (ESFAS), is provided. The RPS automatically initiates a reactor trip when any of the monitored process variables reach a trip setpoint. The ESFAS automatically actuates engineered safety feature (ESF) systems and their support systems when any of the monitored process variables reach a predetermined setpoint.

The trip setpoints of the RPS are selected to provide reasonable assurance that DBEs that are expected to occur once or more during the life of the nuclear generating station do not cause the violation of SAFDLs. The reactor trips also help the ESF systems in mitigating the consequences of DBEs that are expected to occur once during the life of several plants as well as arbitrary combinations of unplanned events and degraded systems that are never expected to occur, to within acceptable limits.

Reactor trip is accomplished by de-energizing the control element drive mechanism (CEDM) coils through the interruption of the CEDM power supply either automatically or manually. The CEDM power supply is a pair of full-capacity motor-generator sets. The path to the CEDMs is interrupted by opening the reactor trip switchgear. With the CEDM coils de-energized, the CEAs are released to drop into the core by gravity, rapidly inserting negative reactivity to shut the reactor down. The CEDMs are addressed in Subsection 3.9.4 and specific reactor trips are addressed in Section 7.2.

The ESF systems are actuated to minimize the effects of incidents that could occur. Controls are provided for manual actuation of the ESF system. The ESF systems are addressed in Chapter 6. The process variables that automatically actuate the ESF system and the logic for the ESFAS are addressed in Section 7.3.

The SAFDLs on linear heat rate and DNBR are intended to enforce the principal thermal hydraulic design bases given in Subsection 4.4.1 (i.e., the avoidance of thermally induced fuel damage during normal steady-state operations and AOOs).

3.1.17 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 loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred."

Response:

The protection system is designed to comply with the requirements of IEEE Std. 603-1991 (Reference 6) and other standards, as noted in Subsection 7.1.2. No credible single failure will result in a loss of the protection function. The protection channels are independent with respect to wire routing, sensor mounting, and supply of power.

Each channel of the protection system, including the sensors up to the reactor trip switchgear system (RTSS) and ESFAS actuation devices, is capable of being checked during reactor operation. Process sensors of each channel in the protection systems are checked by comparison of the redundant process sensor values using the discrete indications and alarms in the MCR, as described in Subsection 7.7.1.2.

To minimize an inadvertent actuation of an ESF system or an inadvertent reactor trip, the protection systems use a coincidence of two-out-of-four logic to operate. The channel being testing is bypassed so the protection system converts to a two-out-of-three logic. This allows periodic testing and the operation of various protective functions without a loss of the protection function.

3.1.18 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 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."

Response:

The protection systems conform to the independence requirements of IEEE Std. 603-1991. Four independent measurement channels, complete with sensors, sensor power supplies, signal conditioning units, and bistable trip functions, are provided for each protective parameter monitored by the protection systems, except for the CEA position sensors that are two-fold redundant. The measurement channels are provided with a high degree of independence by separate connection of the channel sensors to the process systems. Refer to Chapter 7 for a more detailed description of the protection systems.

Power to the protection system channels is provided by independent vital bus power supply systems. The power supply systems are described in Subsection 8.3.2.

Functional diversity is incorporated into the system design to prevent a loss of the protective function. When an RPS trip function is required, it is frequently backed up by other trip functions. The ESFAS actuation signals are used to actuate two or four independent ESF trains.

The diverse protection system augments reactor trip and auxiliary feedwater system (AFWS) actuation by using separate and diverse non-Class 1E trip logic from that used by the plant protection system.

The design goals are accomplished without excessive complexity by using only four channels for each parameter. This allows for testing and maintenance of a channel without reducing the system to a single channel for trip, which would make the system susceptible to spurious trip or actuation signals.

Environmental and seismic qualifications are also performed using type tests, specific equipment tests, appropriate analyses, or prior operating experience. Further information is provided in Sections 3.10 and 3.11.

3.1.19 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, radiation) are experienced."

Response:

The plant protection system trip channels are designed to fail into a safe state or into a state established as acceptable in the event of loss of power supply. A failure is assumed to occur in only one channel (i.e., a single failure). This channel can be placed into bypass, which places the RPS/ESFAS local coincidence logic into a two-out-of-three configuration. Refer to Sections 7.2 and 7.3 for information on the failure modes and effects analysis.

A loss of power to CEDM coils would cause the CEAs to insert into the core. Redundancy, channel independence, and separation are incorporated into the protection system design to minimize the possibility of the loss of a protective function. The loss of offsite power would cause the standby diesel electric generators to start and energize the ESF trains with actuation signals present.

3.1.20 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."

Response:

Protection system components and control system components are electrically and functionally isolated from each other. Further details are provided in Sections 7.2, 7.3, and 7.7.

Isolation devices provide reasonable assurance that when protection signals are used by non-safety systems and non-safety signals are used by safety systems, credible single failures in the non-safety system do not degrade the performance of the safety system. In addition to the electrical and physical isolations, functional isolation between non-safety systems and safety systems is provided. The functional isolation is provided by priority logics in the safety systems or by signal selector logic in the non-safety systems. The priority logics provide reasonable assurance that safety actuation signals, both automatic and manual (system level and component level), override all control signals from the non-safety systems. Signal selection logic in the control system prevents erroneous control actions due to single sensor failures. Eliminating these erroneous control actions prevents challenges to the protection system while it is degraded due to the same sensor failure.

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

3.1.21 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."

Response:

Shutdown of the reactor is accomplished by the opening of the reactor trip switchgear system (RTSS) circuit breakers, which interrupts power to the CEDM coils. Actuation of the circuit breakers is independent of any existing control signals.

The protection systems are designed such that SAFDLs are not exceeded for any single malfunction of the reactivity control systems, including the withdrawal of a single full- or part-strength CEA. Analyses of possible reactivity control system malfunctions are described in Chapter 15.

3.1.22 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 acceptable fuel design limits are not exceeded. One of the systems shall be capable of holding the reactor core subcritical under cold conditions."

Response:

Two independent reactivity control systems of different design principles are provided. The first system, using control element assemblies (CEAs), includes a passive means (gravity) for inserting CEAs and is capable of reliably controlling reactivity changes to provide reasonable assurance that under conditions of normal operation, including AOOs, SAFDLs are not exceeded. The CEAs can be mechanically driven into the core.

The appropriate margin for stuck rods is provided by assuming in the analyses of AOOs that the highest worth CEA does not fall into the core.

The second system, using neutron absorbing soluble boron, is capable of reliably compensating for the rate of reactivity changes resulting from planned normal power changes (including xenon burnup) such that SAFDLs are not exceeded. This system is capable of holding the reactor subcritical under cold conditions.

Either system is able to insert negative reactivity at a rate sufficient to prevent exceeding SAFDLs as the result of a power change (i.e., positive reactivity added by xenon burnup).

3.1.23 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."

Response:

Dissolved boron addition capability provided by the safety injection system (SIS) (Chapter 6) in conjunction with the CEAs is such that under postulated accident conditions (Chapter 15), even with the CEA of highest worth stuck out of the core, adequate reactivity control is available to maintain short- and long-term core cooling.

3.1.24 Criterion 28 – Reactivity Limits

"The reactivity control systems shall be designed with appropriate limits on the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents can neither (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."

Response:

The bases for CEA design include providing reasonable assurance that the reactivity worth of any one CEA is not greater than a preselected maximum value. The CEAs are divided into two sets, a shutdown set and a regulating set, further subdivided into groups as necessary. Administrative procedures and interlocks provide reasonable assurance that only one group is withdrawn at a time, and that regulating groups are withdrawn only after shutdown groups are fully withdrawn. The regulating groups are programmed to move in sequence and within limits that prevent the rate of reactivity addition and the worth of individual CEAs from exceeding limiting values.

The maximum rate of reactivity addition that can be produced by the chemical and volume control system (CVCS) is too low to induce pressure forces significant enough to rupture the RCPB or disturb the reactor vessel internals.

The RCPB (Chapter 5) and reactor internals (Chapter 4) are designed to appropriate codes (e.g., the response to Criterion 14) and accommodate the static and dynamic loads associated with an inadvertent, sudden release of energy such as that resulting from a CEA ejection or steam line break (Chapter 15) without rupture and with limited deformation so that core cooling capability is not impaired.

3.1.25 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."

Response:

Plant events, designated in ANSI/ANS 51.1, have been carefully considered in the design of the protection and reactivity control systems. Redundancy, independence, and testability have been considered in the design. These considerations, coupled with careful component selection, overall system testing, and adherence to detailed quality assurance requirements, provide reasonable assurance that protection and reactivity control systems will accomplish their safety functions in the event of AOOs.

Refer to Chapter 7 for detailed descriptions of the protection systems and Chapter 17 for description of design quality assurance. DBE analysis is addressed in Chapter 15.

3.1.26 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."

Response:

RCPB components are designed, fabricated, erected, and tested in accordance with ASME Section III. All components are classified safety Class 1 or 2 in accordance with ANSI/ANS 51.1-1983 and undergo all quality assurance measures that are appropriate for the respective classification.

Means are provided for identifying the source of reactor coolant leakage, which includes detection of leakage to systems connected to the RCPB as well as leakage from the boundary into the containment.

Instrumentation is provided to indicate and record makeup flow rates to the primary water system. This instrumentation permits detection of both suddenly occurring and gradually increasing leaks. Leakage detection methods are described in Subsection 5.2.5.1.

3.1.27 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 (1) 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 (1) material properties, (2) the effects of irradiation on material properties, (3) residual, steady state and transient stresses, and (4) size of flaws."

Response:

All the RCPB components are designed and constructed in accordance with ASME Section III and comply with test and inspection requirements of these codes. The test and inspection requirements provide reasonable assurance that flaw sizes are limited so that the probability of failure by rapid propagation is extremely remote. Particular emphasis is placed on the quality control applied to the reactor vessel, on which tests and inspections exceeding ASME Code requirements are performed. The tests and inspections performed on the reactor vessel are described in Subsection 5.3.1.3.

Carbon and low-alloy steel materials that form part of the RPCB are tested in accordance with fracture toughness requirements for materials in ASME Section III. Nonductile failure prevention is reasonably assured by adhering to the relevant sections of the ASME Code.

Excessive embrittlement of the reactor vessel material due to neutron irradiation is prevented by providing an annulus of coolant water between the reactor core and the vessel. In addition, to minimize the effects of irradiation on material toughness properties of core beltline materials, restrictions on upper limits for residual elements that directly influence the reference temperature nil-ductility transition (RT_{NDT}) shift are required by design specification. Specifically, upper limits are placed on copper, nickel, phosphorous, sulfur, and vanadium.

The maximum integrated fast neutron exposure of the reactor vessel wall opposite the midplane of the core is less than 9.5×10^{19} n/cm^2. This value assumes a 60-year design life and a 93 percent plant capacity factor. The maximum expected increase in transition temperature for vessel weld materials is approximately 31.4 °C (56.5 °F) provided that weld metal is conservatively assumed to be exposed to the peak value of neutron fluence, 9.5×10^{19} n/cm^2. Actual locations of welds are outside the active core region. The actual change in material toughness properties due to irradiation is verified periodically during plant lifetime by a material surveillance program. Based on the initial RT_{NDT} of archive pressure vessel beltline material, which is –23.3 °C (–10 °F) or less, operating restrictions are applied as necessary to limit vessel stresses.

The thermal stresses induced by the injection of cold water into the vessel following a LOCA have been examined. Analyses have shown that there is no gross yielding across the vessel wall when using the minimum specified yield strength in ASME Section III.

3.1.28 Criterion 32 – Inspection of Reactor Coolant Pressure Boundary

"Components which are part of the reactor coolant pressure boundary shall be designed to permit (1) periodic inspection and testing of important areas and features to assess their structural and leaktight integrity, and (2) an appropriate material surveillance program for the reactor pressure vessel."

Response:

Provisions have been made in the design for inspection, testing, and surveillance of the RCS boundary as required by ASME Section XI. The system designer recommends a reactor vessel surveillance program to the owner. The reactor vessel surveillance program provided to the owner conforms to 10 CFR 50, Appendix H. Sample pieces taken from the same material used in fabrication of the reactor vessel are installed between the core and the vessel inside wall. These samples are removed and tested by the owner at intervals during vessel life to provide an indication of the extent of the neutron embrittlement of the vessel wall. Charpy tests are performed on the samples to develop a Charpy transition curve. By comparing this curve with the Charpy curve and drop weight test results for specimens taken at the beginning of the vessel life, the change of RT_{NDT} is determined and operating procedures adjusted as required. Further details are provided in Chapter 5.

3.1.29 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."

Response:

Reactor coolant makeup during normal operation is provided by the CVCS. The two charging pumps can be powered from either onsite or offsite power sources. The system is described in Subsection 9.3.4. The CVCS has the capability of replacing the flow loss to the containment due to leaks in small reactor coolant lines such as instrument and sample lines. These lines have 5.56 mm (7/32 in) diameter by 25.4 mm (1 in) long flow-restricting devices to limit loss of RCS coolant due to postulated pipe breaks in RCS piping.

The CVCS is not required to perform any safety-related function, such as accident mitigation or safe shutdown. This does not, however, compromise the defense-in-depth provided by the system as the normal means of maintaining RCS inventory and primary water chemistry. The CVCS is essential to day-to-day plant operations and has been provided with a high degree of reliability and redundancy, and is designed in accordance with accepted industry standards and quality assurance commensurate with its importance to plant operation. Design criteria, including ASME Code classification assignments, are in accordance with ANSI/ANS 51.1, which requires that portions of the CVCS in the RCPB, all portions that provide reasonable assurance of containment isolation and reactor coolant normal makeup, have a rigorous safety classification in accordance with the functional performance requirements.

3.1.30 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."

Response:

Residual heat removal capability is provided by the shutdown cooling system (SCS) for reactor coolant temperature and pressure less than 176.7 °C (350 °F) and 31.6 kg/cm^{2}A (450 psia). For temperatures greater than 176.7 °C (350 °F), this function is provided by the SGs. The AFWS provides a dedicated, independent, safety-related means of supplying feedwater (FW) to the SGs for removal of heat and prevention of reactor core uncovery. The design incorporates sufficient redundancy, interconnections, leak detection, and isolation capability to provide reasonable assurance that the residual heat removal function can be accomplished, assuming a single active failure. Within appropriate design limits, either system can remove fission product decay heat at a rate that SAFDLs and the design conditions of the RCPB are not exceeded.

The SCS and SG auxiliaries are designed to operate from offsite or from onsite power sources.

Further description of the SCS is provided in Subsection 5.4.7, and further description of the steam and power conversion system is provided in Chaper 10.

3.1.31 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 (1) 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."

Response:

Emergency core cooling is provided by the SIS as described in Section 6.3. The system is designed to provide cooling water to limit peak clad temperature to less than 1,204 °C (2,200 °F), to remove heat at a rate sufficient to maintain the fuel in a coolable geometry and to provide reasonable assurance that zirconium-water reaction is limited to a negligible amount (less than one percent) following a loss-of-coolant accident, including breaks in the pipe in the reactor coolant pressure boundary up to and including a break size equivalent to the double-ended rupture of the largest pipe in the RCS. Performance of the emergency core cooling system (ECCS) has been analyzed using the evaluation models complying with the requirements of 10 CFR 50.46(a)(1), and performance has been verified adequate to meet the criteria prescribed in 10 CFR 50.46(b).

The system design includes provisions to provide reasonable assurance that the required safety functions are accomplished with either onsite or offsite electrical power, assuming a single failure of any component which is qualified as described below.

The single failure may be an active failure[1] during the short-term cooling phase of safety injection or an active or limited leakage passive failure[2] during the long-term cooling phase of safety injection.

Although the SIS is designed to accommodate a limited leakage passive failure during the long-term cooling phase, it does not accommodate arbitrary large leakage passive failures, such as the complete double-ended severance of piping, which are extremely low probability events.

---

[1] An active failure is a malfunction, excluding passive failure, of a component that relies on mechanical movement to complete its intended function upon demand. Examples of active failures include the failure of a valve to move to its correct position, or the failure of a pump, fan, or diesel generator to start. Spurious action of a powered component originating within the actuation system or its supporting systems shall be regarded as an active failure, unless specific design features or operating restrictions preclude such spurious action.

[2] A passive failure is defined as the blockage of a process flow path or a breach in the integrity of a component or piping (e.g., piping failure). Refer to Subsection 6.3.2.5.4 for a description of a limited-leakage passive failure of the SIS.

3.1.32 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."

Response:

The SIS is designed to facilitate access to all critical components. All pumps, heat exchangers, valves, and piping external to the containment structure are readily accessible for periodic inspection to provide reasonable assurance of system leak-tight integrity. Valves, piping, and tanks inside the containment may be inspected for leak-tightness during plant shutdowns for refueling and maintenance.

Reactor vessel internal structures, reactor coolant piping, and water injection nozzles are designed to permit visual inspection for wear due to erosion, corrosion, or vibration and nondestructive inspection techniques where applicable and desirable.

Descriptions of the inspection program are provided in Chapters 5, 6, and 16.

3.1.33 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 (1) 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 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."

Response:

The SIS is provided with testing capability to demonstrate system and component operability. Testing can be conducted during normal plant operation with the test facilities

arranged not to interfere with the performance of the systems or with the initiation of control circuits, as described in Section 6.3 and Chapter 14. During in-service testing, testing is performed to confirm that the SI pump return line to the in-containment refueling water storage tank (IRWST) allows each SI pump to be operated at rated flow.

3.1.34 Criterion 38 – Containment Heat Removal

"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 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."

Response:

The containment spray system (CSS) consists of two independent divisions. Each division consists of a containment spray pump, a containment spray heat exchanger, a containment spray pump miniflow heat exchanger, a containment spray header, and associated piping and valves. The heat removal capacity of each division is sufficient to keep the containment pressure and temperature below design conditions for any break size in the RCS piping up to and including a double-ended break of the largest reactor coolant pipe, with an unobstructed discharge from both ends.

The CSS takes suction borated water from the in-containment refueling water storage tank (IRWST), which is located in the containment. Borated water is sprayed downward by the CSS from the upper regions of the containment to cool the containment atmosphere. The removed heat is transferred by the component cooling water via the CSS heat exchangers to the ultimate heat sink (UHS).

Suitable redundancy in components and features is designed into the CSS to maintain the pressure and temperature conditions below containment design conditions even in the event of a single failure including the loss of onsite or offsite electrical power.

The CSS is supplied from separate Class 1E buses and receives electrical power from electrically independent and redundant emergency power supply systems as well as offsite power suplies.

The CSS is described further in Subsections 6.2.2 and 6.5.2. Electrical power supplies are described further in Subsections 8.2 and 8.3.

3.1.35 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."

Response:

Inspections of the CSS are conducted to confirm the integrity and capability and provide reasonable assurance of the system. All essential equipment of the CSS is located outside the containment, except for spray headers, nozzles, containment sump, IRWST, and associated piping. These components include two containment spray pumps, two containment spray pump miniflow heat exchangers, two containment spray heat exchangers, and independent containment spray headers.

The detailed arrangement and layout of system piping, pumps, heat exchangers, and valves provide the separation, availability, and accessibility required for periodic inspection. Nozzle inspection capability is provided as well.

The CSS is described further in Subsections 6.2.2 and 6.5.2.

3.1.36 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 (1) 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."

Response:

The containment heat removal system is arranged so that components can be tested periodically for operability. The operational tests are performed to verify the proper operation of CSS and include the calibration of instrumentation, verification of adequate pump performance, verification of the operability of all associated valves, and verification that the spray headers and spray nozzles are free of obstructions. Testing can be conducted during normal plant operation with the system configured to not interfere with the performance of the initiation of control circuits, as described in Subsection 6.2.2.

All components of the CSS are hydrostatically tested in the manufacturer's shop. A hydrostatic test is performed in the field to verify the leaktightness of the system.

The performance testing of containment spray pumps is conducted at some time other than refueling. The pumps are aligned to take suction from and return flow to the IRWST. Flow and head are recorded by the installed instrumentation.

Actuator-operated valves can be tested from the control room and operation verified by observing control room indication.

The valves on the inlets and outlets of the containment spray pumps can be tested to provide reasonable assurance that the valves operate properly.

3.1.37 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 quality 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."

Response:

The CSS and containment hydrogen control system are provided to control fission products, hydrogen, oxygen, and other substances that may be released into the containment. The CSS is an automatically actuated ESF system that provides heat removal and fission product removal following a LOCA. The fission products are removed to reduce activity at the site boundary by the CSS and the post-accident pH of the sprayed fluid is controlled by using trisodium phosphate (TSP). The CSS consists of two independent divisions that are supplied power from separate Class 1E buses and has sufficient redundancy to perform its safety functions. The CSS is designed so that a single failure coincident with a loss of offsite power does not prevent performance of the safety function.

Passive autocatalytic recombiners (PARs), which have 200 percent of required capacity, are located in containment and preclude hydrogen concentration buildup to detonable levels.

The systems are described in detail in Subsections 6.2.5 and 6.5.2.

3.1.38 Criterion 42 – Inspection of Containment Atmosphere Cleanup Systems

"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."

Response:

The containment atmosphere cleanup systems are designed and located so that they can be inspected periodically as required. Inspection of the CSS function relative to iodine removal is treated as described in GDC 39.

All major active components of the containment atmosphere cleanup systems are located outside containment and are readily accessible for periodic inspection.

The inspection and surveilance program for the containment hydrogen control system is described further in Subsection 6.2.5.

3.1.39 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 leaktight 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."

Response:

Testing of the CSS is conducted to provide reasonable assurance of structural and leaktight integrity and operability and performance in accordance with GDC 40. In addition, performance testing is conducted on CSS components. These tests are normally conducted while the plant is operating. System design includes provisions to prevent accidental containment spray during component testing. The test for the CSS is described further in Subsections 6.2.2 and 6.5.2

The containment hydrogen control system is designed to permit periodic testing for confirming the continued operability. Testing may be conducted during normal plant

operation or shutdown. The test for the containment hydrogen control system is described in Subsection 6.2.5 for details.

3.1.40 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."

Response:

The cooling water systems, which function to remove the combined heat load from safety-related systems and components under normal operating and accident conditions, are the component cooling water system (CCWS) and the essential service water system (ESWS). The CCWS is a closed-loop system that removes heat from nuclear safety-related and potentially radioactive systems. The ESWS removes heat from the CCWS and transfers it to the environment through the UHS.

Suitable redundancy, systems interconnection, leak detection, and isolation capabilities are incorporated into the design of these systems to provide reasonable assurance of the required safety function, assuming a single failure with available onsite or offsite power.

The CCWS and the ESWS are described in Subsections 9.2.2 and 9.2.1, respectively.

3.1.41 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."

Response:

Components of these systems 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 during normal power operation as well as by pressure and functional tests. The inspection and testing requirements for the CCWS and the ESWS are described in Subsections 9.2.2 and 9.2.1, respectively.

3.1.42 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."

Response:

The design provides for periodic testing of the cooling water systems for operability and functional performance.

The manufacturer is required to conduct performance tests of the components. An initial system flow test demonstrates proper functioning of the system. Thereafter, periodic tests provide reasonable assurance that components are functioning properly.

Cooling water system valves can be connected to the preferred power source at any time during reactor operation to demonstrate operability. The system is operated normally, thereby demonstrating operability. Remotely operated valves are exercised and actuation circuits are tested. Automatic actuation circuitry, valves, and pump breakers can also be checked when integrated system tests are performed during a planned cooldown of the RCS. Provisions have been made to permit periodic leakage tests to verify the continued leak-tight integrity of the systems. The inspection and testing requirements for the CCWS and the ESWS are provided in Subsections 9.2.2 and 9.2.1, respectively.

3.1.43 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."

Response:

The containment structure, including access openings and penetrations, is designed to accommodate, without exceeding the design leak rate, the transient peak pressure and temperature associated with a LOCA up to and including a double-ended rupture of the largest reactor coolant pipe.

The containment structure and ESF systems have been evaluated for various combinations of energy release. The analysis accounts for system thermal and chemical energy, and for nuclear decay heat. The SIS is designed such that no single active failure could result in significant metal-water reaction, as described in Subsection 6.2.1.

The containment heat removal system is described in Subsection 6.2.1. Further information is provided in Subsections 3.8.1 and 3.8.2.

3.1.44 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."

Response:

The containment's ferrite materials are selected to provide reasonable assurance that their temperature under normal operating and testing conditions is at least 16.7 °C (30 °F) above the nil-ductility transition temperature (NDTT). Detailed stress analyses of the containment liner anchors are conducted under normal and postulated accident conditions.

Further details regarding ferrite materials used in the containment and associated design requirements are described in Subsections 3.8.1, 3.8.2, and 6.1.1.

3.1.45 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."

Response:

Criterion 52 is complied with the plant design. The provision for testing in conformance with this criterion and the provisions for conformance to 10 CFR 50, Appendix J, are described in Subsection 6.2.6.1. Containment design relative to test pressure is described in Subsection 3.8.1.3.

3.1.46 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 leaktightness of penetrations which have resilient seals and expansion bellows."

Response:

The containment design permits access to penetrations and other important areas for implementation of the surveillance program described in Chapter 16. Penetrations with resilient seals and bellows are visually inspected and pressure tested periodically for leak-tightness according to the Technical Specifications. Leakage rate testing is described in Subsection 6.2.6.

3.1.47 Criterion 54 – Piping Systems Penetrating Containment

"Piping systems penetrating 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."

Response:

Piping systems that penetrate containment are designed to provide the required isolation and testing capabilities. These piping systems are provided with test connections to allow periodic leak detection tests to provide reasonable assurance that the leakage is within the acceptable limits of 10 CFR 50, Appendix J, and Chapter 16.

The ESFAS circuitry provides the means for testing isolation valve operability.

The fuel transfer tube is not classified as a fluid system penetration. The blind flange and the portion of the transfer tube inside the containment are an extension of the containment

boundary. The blind flange isolates the transfer tube at all times, except when the reactor is shut down for refueling. This assembly is a penetration in the same sense as the equipment hatches and personnel locks.

Subsection 6.2.4 addresses penetration design. Additional information is given in the responses to GDC 55, 56, and 57 (Subsections 3.1.48 through 3.1.50).

3.1.48 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:

a. One locked closed isolation valve inside and one locked closed isolation valve outside containment.

b. One automatic isolation valve inside and one locked closed isolation valve outside containment.

c. 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.

d. 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."

Response:

All RCPB lines penetrating containment meet the isolation criteria of GDC 55 using the following basis for specific lines in addition to those noted above:

a. Safety injection lines, as shown in Figure 6.3.2-1, are used to mitigate the consequences of accidents and therefore do not receive an automatic closure signal and are not locked closed.

b. When in shutdown cooling mode, the shutdown cooling system is an extension of the RCPB and is isolated from the environment by two isolation valves in series.

c. The charging and seal injection lines shown in Figure 9.3.4-1 have automatic valves outside containment that do not receive a closure signal (CIAS) because it is desirable to maintain charging and seal injection flow as long as the charging pumps are in operation.

d. Special cases are described in Subsection 6.2.4.

3.1.49 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:

a. One locked closed isolation valve inside and one locked closed isolation valve outside containment.

b. One automatic isolation valve inside and one locked closed isolation valve outside containment.

c. 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.

d. 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."

Response:

Fluid systems comply with the requirements of GDC 56 with the following exceptions:

a. Lines that connect directly to the containment atmosphere and are used for mitigating the effects of accidents are connected to a closed piping system outside containment, which is isolated from the environment in accordance with the requirements of GDC 55.

b. In addition, the capability for remote double isolation at the containment boundary is provided in accordance with GDC 56.

c. Special cases are described in Subsection 6.2.4.

3.1.50 Criterion 57 – Closed System Isolation Valves

"Each line that penetrates 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 containment and

located as close to the containment as practical. A simple check valve may not be used as the automatic isolation valve."

Response:

The system complies with the requirements of GDC 57 as described in Subsection 6.2.4.

3.1.51 Criterion 60 – Control of Releases of Radioactive Material 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."

Response:

The sources and expected quantities of radioactive materials produced during normal reactor operation, including AOOs, are presented in Chapter 11. The radioactive waste systems to suitably control the release of these materials in gaseous and liquid effluents and handle radioactive solid wastes are described in Sections 11.2 through 11.4.

3.1.52 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."

Response:

The spent fuel cooling and cleanup system, fuel handling system, building ventilation systems for radiation control areas, and radioactive waste management systems are designed to provide reasonable assurance of adequate safety under normal and postulated accident conditions.

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

Information on shielding is provided in Section 12.3. Radiation monitoring is described in Section 11.5 and Subsection 12.3.4.

The individual components that contain radioactivity are located in confined areas and ventilated through appropriate filtering systems. Information on radioactive waste management systems is provided in Chapter 11.

The spent fuel pool cooling and cleanup system provides cooling to remove residual heat from the fuel stored in the spent fuel pool. The system is designed with redundant and testable features to provide reasonable assurance of continuous heat removal. The spent fuel pool cooling and cleanup system is described in Subsection 9.1.3.

The spent fuel pool is designed in accordance with seismic Category I requirements so that no postulated accident can cause excessive loss of coolant inventory.

3.1.53 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."

Response:

The restraints and interlocks provided for safe handling and storage of new and spent fuel are described in Section 9.1.

The fuel handling area is laid out to preclude the spent fuel shipping cask from traversing the spent fuel storage pool.

Design of the new and spent fuel racks provides reasonable assurance of an effective multiplication factor (K_{eff}) of less than 0.95 for spent fuel racks and new fuel racks when flooded with pure, unborated water and 0.98 for the new fuel racks even in the optimum moderating condition.

Criticality in the fuel storage area is prevented by the physical separation of fuel assemblies, the fixed neutron absorber attached on the spent fuel rack wall, and the presence of borated water in the fuel storage pool.

3.1.54 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."

Response:

Instrumentation is provided to monitor the spent fuel pool (SFP) water level and water temperature continuously, and their indications and annunciations are provided in the main control room (MCR). Two redundant safety-related fuel handling area radiation monitors are provided to monitor SFP area radioactivity continuously, and their indications and annunciations are provided in the MCR. In case of an inadvertent release of radioactivity, the area radiation monitor generates local and MCR alarms and an engineered safety features actuation signal (ESFAS) fuel handling area emergency ventilation actuation signal as required for the appropriate safety actions. Information on the ESFAS is provided in

Section 7.3, and information on the fuel storage area radiation monitoring system is provided in Subsection 9.4.2.

3.1.55 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."

Response

The reactor containment atmosphere is continuously sampled and monitored for any radioactivity that is released from normal operations (including AOOs) by a continuous air monitoring system located outside the containment. A separate system is provided to enable collection and analysis of grab samples of the containment atmosphere during normal operations and accident conditions. Area monitors such as high range ion chambers are located inside the containment to measure radiation levels from normal and accident conditions.

Gamma and beta scintillators are located outside the containment for containment air monitoring.

Spaces containing components for recirculation of loss-of-coolant accident fluids and areas contiguous to the containment structure are monitored for airborne radioactivity by systems that sample and monitor the air exhausted from the associated areas. The systems consist of continuous air monitors, duct radiation monitors, and air samplers to enable the collection of samples of exhaust air for laboratory analysis during normal and accident conditions.

Effluent discharge paths and plant environs from the facility are continuously monitored for radioactivity during normal operations with continuous air and liquid monitoring systems. Sampling provisions are included to allow sample collection for analysis during normal operations and accident conditions. Extended range noble gas monitors are provided to

allow for continuous monitoring during accident conditions. The systems provided for monitoring radioactive releases from the facility are described in Sections 11.5 and 12.3.

3.1.56 Combined License Information

No COL information is required with regard to Section 3.1.

3.1.57 References

1. ANSI/ANS 51.1-1983, "American National Standard Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plant," 1983, withdrawn 1998.

2. 10 CFR 50.55a, "Codes and Standards."

3. 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants."

4. Standard Review Plan 3.6.3, "Leak-Before-Break Evaluation Procedures," Rev. 1 NUREG-0800, U.S. Nuclear Regulatory Commission, March 2007.

5. U.S. Nuclear Regulatory Commission, "Evaluation of Potential for Pipe Breaks," NUREG-1061, Volume 3, Washington DC, USA, November 1984.

6. IEEE Std. 603, "IEEE Standard Critetia for Safety Systems for Nuclear Power Generating Stations," 1991.