7.4 Systems Required for Safe Shutdown

Systems to establish safe shutdown conditions perform two basic functions. First, they provide the necessary reactivity control to maintain the core in a subcritical condition. Boration capability is provided to compensate for xenon decay and to maintain the required core shutdown margin. Second, these systems must provide residual heat removal capability to maintain adequate core cooling.

The designation of systems required for safe shutdown depends on identifying those systems that provide the following capabilities for maintaining a safe shutdown:

- Decay heat removal
- Reactor coolant system inventory control
- Reactor coolant system pressure control
- Reactivity control

There are two different safe shutdown conditions that are expected following a transient or accident condition. Short-term safe shutdown refers to the plant conditions from the start of an event until about 36 hours later. Long-term safe shutdown refers to the plant conditions after this 36-hour period.

The short-term safe shutdown conditions include maintaining the reactor subcritical, the reactor coolant average temperature less than or equal to no load temperature, and adequate coolant inventory and core cooling. These shutdown conditions shall be achieved following any of the design basis events using safety-related equipment. The specific safe shutdown condition achieved is a function of the particular accident sequence.

The long-term safe shutdown conditions are the same as the short-term conditions except that the coolant temperature shall be less than 420°F. This long-term condition must be achieved within 36 hours and maintained indefinitely using safety-related equipment.

There are no systems specifically and solely dedicated as safe shutdown systems. However, there are a number of plant systems that are available to establish and maintain safe shutdown conditions. Normally, in the event of a turbine or reactor trip, nonsafety-related plant systems automatically function to place the plant in short-term safe shutdown, as described in subsection 7.4.1.2. During the short-term safe shutdown condition, an adequate heat sink is provided to remove reactor core residual heat and boration control is available. Redundancy of systems and components is provided to enable continued maintenance of the short-term safe shutdown condition. Additional redundant nonsafety-related systems are normally available to manually perform a plant depressurization and cooldown.

The engineered safety systems are designed to establish and maintain safe shutdown conditions for the plant. Nonsafety-related systems are not required for safe shutdown of the plant.

This section focuses on safety-related systems used to establish and maintain safe shutdown conditions. The discussion of safe shutdown does not include accident response and/or mitigation since the standard review plan for this section addresses safe shutdown not related to accident

mitigation. However, safe shutdown conditions are also established and maintained by these safety-related systems following accident conditions. For example, the control rods are released to initially place the plant in a shutdown condition to mitigate the consequences of various accidents. The passive core cooling system, on the other hand, is used to provide core cooling in an accident, but it is also one of the principal systems used for safe shutdown. Only those specific engineered safety systems listed in Table 7.4-1 are used to establish and maintain safe shutdown of the plant. These engineered safety systems automatically function to place the plant in a safe shutdown condition without operator action.

The instrumentation functions necessary for safe shutdown are available through instrumentation channels associated with the safety-related systems in the primary plant. These channels automatically actuate the protective functions provided by the safety-related systems. Manual actuation of the associated safety-related systems is also provided.

The instrumentation systems discussed in this section are those which are required during nonaccident conditions to align the safety-related systems and perform the specified safe shutdown functions.

The specific systems available for safe shutdown are discussed in subsection 7.4.2 and are listed in Table 7.4-1.

Maintenance of safe shutdown conditions with these systems, and the associated instrumentation and controls, includes consideration of the accident consequences that might challenge safe shutdown conditions. The accident consequences that are germane are those that tend to degrade the capabilities for coolant circulation, boration, heat removal, and depressurization. Safe shutdown is achieved following any of the accidents analyzed in Chapter 15. The specific safe shutdown condition reached is a function of the particular accident sequence.

The instrumentation and controls discussed in subsection 7.4.1 are used to control and/or monitor shutdown. These safety-related systems allow the maintenance of safe shutdown, even under accident conditions that tend toward a return to criticality or a loss of heat sink.

In addition to the operation of safety-related systems used for safe shutdown, as described in subsection 7.4.1, the following are part of the safe shutdown provisions:

- The turbine is tripped. (This can be accomplished at the turbine as well as from the main control room.)

- The reactor is tripped. (This can be accomplished at the reactor trip switchgear as well as from the main control room.)

- Support of engineered safety systems actuation is provided by safety-related onsite dc power.

7.4.1 Safe Shutdown

7.4.1.1 Safe Shutdown Using Safety-Related Systems

The following describes the process that establishes safe shutdown conditions for the plant, using the safety-related systems, and no operator action. The reactor coolant system is assumed to be intact for this discussion of safe shutdown.

Since this discussion only considers the use of safety-related systems, offsite electrical power sources are assumed to be lost at the start of the event. This results in a loss of the reactor coolant pumps. Even though the reactor coolant pumps are tripped during the initiation of certain engineered safety system actuation, it is assumed that no engineered safety system actuation signal is generated for this initiating event. With loss of the reactor coolant pumps, reactor coolant system natural circulation flow initiates and transfers core heat to the steam generators. Since feedwater flow is lost, the existing steam generator water inventory provides initial decay heat removal capability.

The initial loss of main ac power results in the Class 1E dc batteries automatically supplying power to the Class 1E dc power distribution network and the four Class 1E 120 Vac instrumentation divisions via the inverters.

The initial response of the passive safety systems is to actuate the passive residual heat removal heat exchanger due to low steam generator water level. The passive residual heat removal heat exchanger removes decay heat from the core by transferring this heat to the in-containment refueling water storage tank.

The passive residual heat removal heat exchanger removes core decay heat, cooling the reactor coolant system. As reactor coolant system cooldown continues, the reactor coolant system pressure decreases due to contraction of the reactor coolant system inventory since the pressurizer heaters are de-energized. An engineered safety system actuation signal occurs when reactor coolant system pressure decreases below a setpoint. This actuates the core makeup tanks, if they had not been previously actuated due to low pressurizer level. The core makeup tanks provide borated water injection to the reactor coolant system.

The engineered safety system actuation signal generated on low pressurizer pressure also actuates containment isolation. This prevents loss of water inventory from containment and permits indefinite operation of the passive residual heat removal heat exchanger and the in-containment refueling water storage tank.

The in-containment refueling water storage tank starts to boil about one to two hours after passive residual heat removal operation is initiated. Once boiling occurs, the in-containment refueling water storage tank begins steaming to containment, transferring heat to the air flowing on the outside of the containment shell. As steaming to containment continues, containment pressure slowly increases. As containment pressure slowly increases, an engineered safety system actuation signal is generated on containment high pressure, resulting in the initiation of passive containment cooling. This provides water flow on the outside of the containment shell to improve the heat removal performance from containment through evaporative cooling to the outside air.

A gutter located at the operating deck elevation collects condensate from the inside of the containment shell. Valves located in drain lines from the gutter to the containment waste sump close on a passive residual heat removal heat exchanger actuation signal. This action diverts the condensate to the in-containment refueling water storage tank. The system indefinitely provides core decay heat removal in this configuration without a significant increase in the containment water level.

Once the reactor coolant system and the safety systems are in this configuration, the plant is in a stable shutdown condition. The reactor coolant system temperatures and pressures continue to slowly decrease. The passive residual heat removal heat exchanger cools the reactor coolant system to 420°F in 36 hours.

Operation in this configuration may be limited in time duration by reactor coolant system leakage. The core makeup tanks can only supply a limited amount of makeup in the event there is reactor coolant system leakage. Eventually the volume of the water in the core makeup tanks will decrease to the first stage automatic depressurization setpoint. The time to reach this setpoint depends upon the reactor coolant system leak rate and the reactor coolant cooldown.

The Class 1E dc batteries that power the automatic depressurization system valves provide power for at least 24 hours. There is a timer that measures the time that ac power sources are unavailable. This timer provides for automatic actuation of the automatic depressurization system before the Class 1E dc batteries are discharged. The emergency response guidelines direct the operator to assess the need for automatic depressurization before the timer completes its count (approximately 22 hours). The operator assessment includes consideration for a visible refueling water storage tank level, full core makeup tanks, and a high and stable in-containment refueling water storage tank level. If automatic depressurization is not needed, the operator is directed to de-energize all loads on the Class 1E dc batteries. This action preserves the capability for the operator to initiate automatic depressurization at a later time.

The automatic depressurization system can be manually initiated by the operator at any time, but no operator action is needed to provide safe shutdown conditions. Once the automatic depressurization system sequence initiates, the plant automatically transitions to lower pressure and temperature conditions that establish and maintain long-term safe shutdown of the plant.

When the automatic depressurization system is actuated, the first stage depressurization valves open and the reactor coolant system depressurization starts. The second and third stage depressurization valves open in sequence, based on automatic timers that are started upon the actuation of the first stage depressurization valves. As reactor coolant inventory continues to be lost, the core makeup tanks continue to inject. If the volume of the water in the core makeup tanks decrease to the fourth stage automatic depressurization setpoint, the fourth stage depressurization valves open. The water and steam vented from the reactor coolant system initially flows into the in-containment refueling water storage tank and overflows into the refueling canal. Eventually this overflows into the reactor vessel cavity, where any moisture from the fourth stage automatic depressurization system valves also collects from discharge in the loop compartments. This overflow initiates the floodup of containment, along with condensate from the containment shell and other cool surfaces in containment.

As the reactor coolant system pressure decreases, the accumulators inject borated water into the reactor coolant system. After the fourth stage automatic depressurization system valves open, the reactor coolant system pressure is reduced sufficiently so that in-containment refueling water storage tank injection can begin as the core makeup tanks empty.

The drain down of the in-containment refueling water storage tank is relatively slow, depending on the injection rates and the reactor coolant system pressure. As the in-containment refueling water storage tank continues to inject, the containment floodup also continues and eventually the floodup volume is sufficient to initiate flow from the recirculation sump.

As the reactor coolant system voids during the cooldown and depressurization process, water flow through the passive residual heat removal heat exchanger is replaced by steam flow, which also provides core cooling. As the in-containment refueling water storage tank empties and uncovers the passive residual heat removal heat exchanger, heat transfer via this path decreases. Eventually, the passive residual heat removal heat exchanger is uncovered, heat removal by the passive residual heat removal heat exchanger stops, and decay heat is removed by automatic depressurization system venting.

The final long-term safe shutdown plant conditions are maintained with the reactor coolant system depressurized to about 10 psig at saturated conditions, venting steam through the automatic depressurization system valves to containment, with heat transferred to the outside atmosphere via the passive containment cooling system. With containment isolation established, the water inventory inside containment provides an indefinite cooling water supply for core decay heat removal.

7.4.1.2 Safe Shutdown Using Safety-Related and Nonsafety-Related Systems

This subsection describes situations where nonsafety-related features of the plant are used together with safety-related systems to establish safe shutdown conditions. As discussed in subsection 7.4.1.1, the AP1000 can be placed in a safe shutdown condition and maintained there using safety-related systems and no operator actions. Section 6.3 provides additional discussion of these situations.

Following passive residual heat removal heat exchanger actuation, the in-containment refueling water storage tank heats up and starts to boil after several hours of operation. If normal steam generator heat removal is not re-established, the operators align the normal residual heat removal system to cool the in-containment refueling water storage tank. This operation prevents significant steaming to the containment.

In case the automatic depresurization system is actuated, the operators align the normal residual heat removal system to provide injection to the reactor coolant system. This action causes the core makeup tank level to remain above the fourth stage valve actuation setpoint and prevents significant steaming to and flooding of the containment.

7.4.1.3 Safe Shutdown Using Nonsafety-Related Systems

This subsection describes the process to establish and maintain safe shutdown conditions using the nonsafety-related systems. As discussed in Section 7.4, the review of the plant safe shutdown capability, including the capabilities provided by the nonsafety-related systems, does not include accident response or mitigation. The nonsafety-related systems normally used to support plant shutdown operations are expected to be available. Offsite power is also expected to be available to support safe shutdown operations, although the nonsafety-related systems can establish and maintain safe shutdown conditions using only onsite electrical power.

For the purposes of this discussion, the nonsafety-related system operation following a reactor trip is described. As assumed in the discussion in subsection 7.4.1.1 on safe shutdown using safety-related systems, the reactor coolant system is assumed to be intact during plant safe shutdown operations.

The nonsafety-related systems and equipment used to establish and maintain safe shutdown conditions are the same systems and equipment that are operated during normal plant startup and shutdown evolutions. The safe shutdown capability using the safety-related systems, described in subsection 7.4.1.1, is only expected to be used in the event that the nonsafety-related systems are not available.

The nonsafety-related systems operate to establish and maintain safe shutdown conditions by providing the safe shutdown functions described in Section 7.4, except that reactivity control is only needed for long-term safe shutdown. If offsite power is available, the operation of these nonsafety-related systems is automatic.

The nonsafety-related systems actuate to establish and maintain the short-term safe shutdown conditions. The systems can also establish and maintain long-term safe shutdown conditions within the time limits discussed in Section 7.4. The operational philosophy following any event is to maintain appropriate safe shutdown conditions based on the duration of the shutdown, until the plant is able to re-start.

Cold shutdown conditions would only be established if it becomes necessary for equipment repair or due to limitations of the nonsafety-related systems in maintaining safe shutdown conditions (such as feedwater system water inventory). This philosophy reduces unnecessary challenges to plant safety due to the transition from operating systems to infrequently-operated standby systems.

Normally, offsite electrical power is available and the nonsafety-related systems automatically maintain short-term safe shutdown conditions as follows:

- Reactor coolant system forced flow to the steam generators by the reactor coolant pumps
- Feedwater from the main or startup feedwater systems
- Heat removal by the steam generators to the main condenser using turbine bypass valves
- Condenser heat removal provided by the main circulating water system

- Reactor coolant system inventory and boration control by the chemical and volume control system

- Reactor coolant system pressure control using pressurizer heaters and normal spray

If offsite power is not available, the reactor coolant pumps, main feedwater pumps, and main circulating water pumps will not be operating. However, the nonsafety-related systems maintain short-term safe shutdown conditions without offsite electrical power as follows:

- Electrical power provided to the required nonsafety-related systems by the diesel-generators of the onsite standby power system

- Heat removal by the steam generators directly to the atmosphere through the power-operated relief valves

- Feedwater from the startup feedwater system

- Reactor coolant system flow to the steam generators via natural circulation

- Reactor coolant system inventory and boration control by the chemical and volume control system

- Reactor coolant system pressure control using pressurizer heaters and auxiliary spray

In case the main feedwater is unavailable, the initial response of the nonsafety-related systems following a reactor trip is to automatically actuate the startup feedwater system, on low steam generator water level, to provide decay heat removal. The steam generators can remove decay heat from the core by either forced or natural circulation in the reactor coolant system. If offsite electrical power is available, the reactor coolant pumps continue to provide forced circulation in the reactor coolant system and the circulating water system continues to operate to provide a heat sink for the steam discharged from the steam generators to the main condenser.

With offsite power and the main condenser available, the turbine bypass valves automatically actuate after the reactor trip to control reactor coolant system temperature, based on the pre-set steam generator pressure control set point that is normally established for standby turbine bypass valve operation. The main feedwater system or the startup feedwater system automatically maintains steam generator water level as the turbine bypass valves continue to throttle steam flow to match the decreasing core decay heat levels. The pressurizer heaters and spray automatically maintain reactor coolant system subcooling with pressure at normal reactor coolant system conditions.

The chemical and volume control system makeup pumps automatically actuate as required to provide borated makeup water to maintain pressurizer level in the programmed band for no-load conditions. The makeup source is the boric acid tank which provides long-term reactivity control. The makeup pumps are expected to operate infrequently during these conditions to compensate for normal reactor coolant system inventory losses such as valve leakage.

Operation of the nonsafety-related systems in this mode maintains short-term safe shutdown conditions and reactor coolant system temperature and pressure remain near no-load conditions. If it becomes necessary to perform a plant cooldown and depressurization to establish long-term safe shutdown conditions, the nonsafety-related systems are used, following the normal plant cooldown procedures. Manual boration to the cold shutdown boron concentration is provided by the chemical and volume control system by initiating reactor coolant system letdown in combination with makeup pump operation. After the boration is completed and letdown is secured, the makeup pumps automatically maintain reactor coolant system inventory throughout the remainder of the cooldown process.

After the required boration is completed the turbine bypass valves are used to initiate the cooldown, with manual control of pressurizer heaters and spray to maintain the reactor coolant system pressure, temperature, and cooldown rate within the limits specified in the technical specifications. The main feedwater system automatically provides feedwater and maintains steam generator level throughout the cooldown process.

When the reactor coolant system temperature and pressure are reduced to within the capabilities of the normal residual heat removal system, at approximately 350°F and 400 psig, the system is manually aligned to the reactor coolant system and started to continue the cooldown process. The final long-term safe shutdown conditions established would be dependent upon the specific maintenance required.

The use of the nonsafety-related systems and equipment for both short-term and long-term safe shutdown also requires the operation of associated support systems. These normally operating support systems include component cooling water, chilled water, compressed air, area ventilation, and nonsafety-related instrumentation and control power. These systems are started as required following a loss of offsite power, once the nonsafety-related diesel-generators are started.

If offsite electrical power is unavailable, the nonsafety-related systems actuate to establish and maintain safe shutdown conditions. There are some differences in the decay heat discharge flow path and the reactor coolant system remains at a slightly higher temperature resulting from the natural circulation flow conditions. With the loss of offsite electrical power, the nonsafety-related diesel-generators provide electrical power for the required nonsafety-related equipment. However, the reactor coolant pumps, main feedwater pumps, and main circulating water pumps are not available. Therefore, core decay heat is transferred to the steam generators using natural circulation in the reactor coolant system, the startup feedwater pumps supply the steam generators, and the steam generators discharge directly to the atmosphere to remove decay heat.

When offsite electrical power is unavailable, reactor coolant temperature is automatically maintained by the steam generator atmospheric power-operated relief valves instead of the turbine bypass valves. The steam generator power-operated relief valves maintain a pre-set steam generator pressure by throttling the steam discharged directly from the steam generators to the atmosphere. The relief valve operation maintains a slightly higher steam generator pressure than the pressure maintained with turbine bypass valve standby operation, resulting in a slight increase in the reactor coolant system temperature. The automatic operation of the startup feedwater subsystem maintains steam generator inventory with the pumps powered from the diesel-

generators. In addition, the direct discharge of steam to the atmosphere prevents condensate recovery, which limits the water inventory for the startup feedwater system.

Following a loss of offsite power, the reactor coolant system temperature is slightly higher than for a reactor trip when offsite electrical power is available, resulting from natural circulation flow and steam generator power-operated relief valve operation. Since the transition to natural circulation flow is relatively slow, the reactor coolant system pressure remains stable without operator action. Operator action is not required to maintain reactor coolant system pressure.

Without offsite electrical power, the pressurizer heaters are manually re-energized after the diesel-generators start. Without reactor coolant pump operation, normal pressurizer spray is unavailable to counteract system pressure increases. Therefore, auxiliary spray provided by the chemical and volume control system makeup pumps is manually initiated to decrease reactor coolant system pressure, if necessary. The operation of the chemical and volume control system makeup pumps to maintain reactor coolant system inventory is similar to their operation when offsite power is available, except that the pumps are manually controlled and powered from the diesel-generators.

The nonsafety-related systems are normally expected to maintain short-term safe shutdown conditions when offsite power is not available. If it is required to establish long-term safe shutdown conditions for equipment maintenance, the cooldown would normally be delayed until offsite power is recovered.

However, the nonsafety-related systems can be used to perform a natural circulation cooldown, if necessary. When performing a natural circulation plant cooldown and depressurization, the operation of the nonsafety-related systems is similar to the normal cooldown operation except that they are powered from the diesel-generators. The primary difference in operation is the use of the steam generator power-operated relief valves to control the cooldown process.

7.4.2 Safe Shutdown Systems

To effect a safe shutdown, with safety-related systems, the plant is initially brought to a stable condition with heat removal provided by the passive residual heat removal heat exchanger. For safe shutdown conditions, control is possible from either the main control room or the remote shutdown workstation. To accomplish a safe shutdown, the functions required are: coolant circulation, boration, heat removal, and depressurization. The portions of the protection and safety monitoring system required to achieve the safe shutdown condition are described in Sections 7.2 and 7.3. The minimum systems required to maintain safe shutdown conditions under a nonaccident condition are listed and discussed in the following paragraphs.

7.4.2.1 Passive Core Cooling System

A description of the passive core cooling system and its operation is provided in Section 6.3. The passive residual heat removal heat exchanger, the core makeup tanks, the in-containment refueling water storage tank, the containment recirculation, and the automatic depressurization system actuate automatically. They can also be manually initiated. Actuation controls are located at the remote shutdown workstation as well as in the main control room.

The safety injection flow from the accumulators, initiates automatically by the reactor coolant system depressurization process. The operation of the accumulator is integrated with the automatic actuation of the other passive core cooling subsystems.

7.4.2.2 Passive Containment Cooling System

A description of the passive containment cooling system and its operation is provided in subsection 6.2.2. The passive containment cooling system actuates automatically. It also can be manually initiated. Actuation controls are located at the remote shutdown workstation as well as in the main control room.

7.4.2.3 Containment Isolation

A description of containment isolation valves and their operation is provided in various subsections. Each system that has piping that penetrates the containment vessel and therefore, requires containment isolation valves is discussed in its own subsection. Most of these systems are nonsafety-related; however, the containment isolation valves and the associated piping are safety-related and automatically close on a safeguards actuation (S) signal. The containment isolation system is discussed in subsection 6.2.3.

7.4.2.4 Reactor Coolant System Circulation

The preferred method of coolant circulation is forced circulation with the reactor coolant pumps supplying the driving head. Upon the loss of main ac power, or when the reactor coolant pumps are tripped during engineered safety system actuation, the reactor coolant pumps are not available. However, the reactor coolant system is designed to provide sufficient natural circulation to achieve safe shutdown conditions with the steam generators and passive residual heat removal heat exchanger removing decay heat. Natural circulation flow is verified by monitoring the reactor coolant system temperatures.

7.4.2.5 Other Systems Required for Safe Shutdown

The other safety-related equipment and systems used to maintain the plant in safe shutdown are identified in Table 7.4-1. They are also listed below, with a reference to the respective section or subsection which discusses their operation in more detail:

- Protection and safety monitoring system — Sections 7.2, 7.3, and 7.5
- Class 1E dc and UPS system — Subsection 8.3.2

These systems are either normally operating or they start automatically when required. The instrumentation for these systems is described in the particular section containing the system description.

The monitoring instrumentation available in the main control room for safe shutdown is safety-related and is part of the protection and safety monitoring system. The instrumentation available for safe shutdown monitoring is listed in Section 7.5.

7.4.3 Safe Shutdown from Outside the Main Control Room

7.4.3.1 Description

If temporary evacuation of the main control room is required because of some abnormal main control room condition, the operators can establish and maintain safe shutdown conditions for the plant from outside the main control room through the use of controls and monitoring located at the remote shutdown workstation. Safe shutdown is a stable plant condition that can be maintained for an extended period of time. In the event that access to the main control room is restricted, the plant is maintained in safe shutdown until the main control room can be re-entered.

7.4.3.1.1 Remote Shutdown Room/Remote Shutdown Workstation

Safe shutdown can be established and maintained from the remote shutdown room. The I&C equipment in the room is collectively referred to as the remote shutdown workstation. The workstation is designed to allow control of a shutdown following an evacuation of the control room, coincident with the loss of offsite power and a single active failure. No other design basis event is postulated. Subsection 9.5.1 provides a discussion of shutdown in the event of a fire. The design basis for the remote shutdown workstation does not require safety-related displays, alarms, and controls.

The remote shutdown workstation contains nonsafety controls, displays, and alarms for the safety-related equipment required to establish and maintain safe shutdown. Additionally, control of nonsafety-related components is available.

The remote shutdown workstation includes operator workstations that are similar to the operator workstations in the main control room and are designed to the same standards. The remote shutdown workstation also includes dedicated nonsafety controls that provide the minimum inventory of controls listed in Table 18.12.2-1. The dedicated nonsafety controls interface to the plant safety and monitoring system via qualified isolators within that system.

The operator workstations have the same capabilities as the reactor operator's workstation in the main control room. The displays and alarms listed in Table 18.12.2-1 are retrievable from the operator workstations. Subsection 18.12.3 provides more discussion on the remote shutdown workstation displays, alarms, and controls.

The remote shutdown workstation is provided for use only following an evacuation of the main control room. No actions are anticipated from the remote shutdown workstation during normal, routine shutdown, refueling, or maintenance operations.

The remote shutdown workstation has sufficient communication circuits to allow the operator to effectively establish safe shutdown conditions. As detailed in subsection 9.5.2, communication is available between the following stations:

- Main control room
- Remote shutdown workstation

- Onsite technical support center
- Diesel generator local control station

Operator control capability at the remote shutdown workstation is normally disabled, and operator control functions are normally performed from workstations located inside the main control room; however, operator control capability can be transferred from the main control room workstations to the remote shutdown workstation if the control room requires evacuation. Procedures will instruct the operator to trip the reactor prior to evacuating the control room and transferring control to the remote shutdown workstation. This operator control transfer capability cannot be disabled by any single active failure coincident with the loss of offsite power.

The control transfer function is implemented by multiple transfer switches. Each individual transfer switch is associated with only a single safety-related or single nonsafety-related group. These switches are located behind an unlocked access panel. Entry into this access panel will result in alarms at the main control room and remote shutdown workstation. The access panel is located within a fire zone which is separate from the main control room. Actuation of these transfer switches results in additional alarms at the main control room and remote shutdown workstation, the activation of operator control capability from the remote workstation, and the deactivation of operator control capability from the main control room workstations. This deactivation of operator control capability includes deactivation of all operator control capability provided by the soft control devices described in subsection 7.1.3.3 and deactivation of all operator control capability provided by dedicated switches. This includes deactivation of operator control capability using manual actuation functions provided by the diverse actuation system as described in subsection 7.7.1.11. The manual reactor trip switches located in the main control room are not affected by this control transfer function. The operator displays, located in the main control room and on the remote shutdown workstation, are also not affected by this control transfer function. The displays on the remote shutdown workstation are operational during normal operation (from the main control room) so that they can be used with no delay if transfer to the remote shutdown workstation is required.

7.4.3.1.2 Controls at Other Locations

In addition to the controls and indicators provided at the remote shutdown workstation, the following controls are provided outside the main control room:

- Reactor trip capability at the reactor trip switchgear
- Turbine trip capability at the turbine
- Start/stop controls for the diesel generators, located at each diesel generator local control panel
- Local control at motor control centers and electrical switchgear.

7.4.3.1.3 Design Bases Information

According to GDC 19, the capability of establishing a shutdown condition and maintaining the station in a safe status in that mode is an essential function. The controls and indications necessary for this function are identified in subsection 7.4.2. To provide the availability of the remote shutdown workstation after control room evacuation, the following design features are provided:

- The remote shutdown workstation conforms with the guidelines provided by ANSI 58.6 1996 (Reference 1).
- The remote shutdown workstation achieves and maintains safe shutdown conditions from full power conditions and maintains safe shutdown conditions thereafter.
- The remote shutdown workstation achieves safe shutdown when offsite power is available and when offsite power is not available.
- The remote shutdown workstation operates safety-related systems, independent from the main control room.
- The remote shutdown workstation is designed with redundancy. When a random event, such as a fire, or an allowable technical specification maintenance results in one safety-related division being unavailable, a single failure in a redundant division is not postulated. When a random event other than fire causes a main control room evacuation, a coincident single failure in the safety systems controlled from the remote shutdown workstation is considered.
- Access to the remote shutdown workstation is under administrative control.

7.4.3.2 Analysis

The analysis of the systems required for safe shutdown is provided in subsection 7.4.1. The following discussion is limited to the remote shutdown workstation.

Conformance to NRC General Design Criteria

General Design Criterion 19 – The remote shutdown workstation provides adequate controls and indications located outside the main control room to establish and maintain the reactor and the reactor coolant system in a safe shutdown condition in the event that the main control room must be evacuated.

Conformance to NRC Regulatory Guides

Regulatory Guide 1.22 – The remote shutdown workstation is tested periodically during station operation.

Regulatory Guide 1.29 – The remote shutdown workstation is designed as seismic Category II to prevent compromising the function of safety-related devices during or after a safe shutdown earthquake.

Conformance to IEEE 603-1991

The remote shutdown workstation and the design features which provide for the transfer of control capability from the main control room to the remote shutdown workstation conform to applicable portions of IEEE 603-1991. The circuits which perform the control transfer function are designed so that a single failure does not prevent maintaining safe shutdown. This is accomplished by redundant components in the systems required for safe shutdown, using independent safety-related power divisions.

To prevent interaction between the redundant systems, the redundant control channels are wired independently and are separated from each other. Nonsafety-related circuits available for (but not required for) safe shutdown are electrically isolated from safety-related circuits.

7.4.4 Combined License Information

This section has no requirement for information to be provided in support of the Combined License application.

7.4.5 References

1. ANSI 58.6 1996, "Criteria for Remote Shutdown for Light Water Reactors."

Table 7.4-1

SYSTEMS REQUIRED FOR SAFE SHUTDOWN

Protection and Safety Monitoring System
Passive Core Cooling System
Passive Residual Heat Removal Heat Exchanger
Core Makeup Tanks
Accumulators
In-Containment Refueling Water Storage Tank
Containment Sump Recirculation
Automatic Depressurization Valves
Passive Containment Cooling System
Class 1E dc and UPS System
Containment Isolation Valves
Reactor System
Control Rods