## 7.4 Systems Required For Safe Shutdown

To achieve a safe shutdown configuration, the appropriate alignment of systems is required to implement the following functions associated with attaining and maintaining a safe shutdown condition:

- Reactivity control.
- Reactor coolant makeup.
- Reactor coolant system pressure control.
- Decay heat removal.
- Process monitoring.

The definition of safe shutdown, the criteria applicable to the shutdown, and the equipment that can be utilized to reach safe shutdown are different depending on the scenario. This section provides information on components and systems that are used to achieve safe shutdown for specific scenarios.

- Cold shutdown using only safety-related equipment to shutdown the plant in accordance with BTP 5-4 (Reference 2).
- Cold shutdown post-fire in accordance with RG 1.189.
- Hot shutdown required during and following a station blackout (SBO) in accordance with 10 CFR 50.63 and in accordance with RG 1.155.

Section 7.4.1 describes the systems necessary to achieve safe shutdown, including the instrumentation and control (I&C) systems that are associated with the safe shutdown functions. Several systems can perform a safe shutdown function. Section 7.4.1 also notes the description of these systems and their associated I&C references.

### 7.4.1 Description

#### 7.4.1.1 I&C Systems Associated with Safe Shutdown

Engineered safety features (ESF) are used to achieve and maintain safe shutdown. The actuation of the ESF is performed by the protection system (PS). The I&C that perform ESF actuation are described in Section 7.3. The safety automation system (SAS) automatically controls the safety-related systems once those systems are actuated by the PS. The SAS provides grouped commands execution initiated from the safety information and control system (SICS). This is designed to provide control of the safety-related systems that are needed to reach safe shutdown of the plant.

The priority and actuator control system (PACS) controls safety-related components associated with safe shutdown. The functions performed by the PACS are described in

Section 7.1.1.4.3. The manual functions needed for safe shutdown functions are duplicated in the process information and control system (PICS) and the process automation system (PAS). The SICS is directly hardwired to PACS for the component-level manual commands.

The human machine interface (HMI) is the PICS and SICS. Monitoring and control of the safety-related systems are both available in the main control room (MCR) and the remote shutdown station (RSS). The operator uses the PICS as the primary HMI in the MCR and RSS to mitigate the event and to achieve and maintain safe shutdown (e.g. manual component level control, manual grouped controls, indications, alarms). The PICS and PAS are credited in the RSS for manual grouped controls, manual component level controls, indications, and alarms. Because the PICS does not send commands to the diverse actuation system (DAS), PS, or SAS, there are some functions that the operator must perform using the SICS from the MCR. These include:

- Manual actuation of reactor trip (RT) and ESF actuation (as required).
- Manual reset of ESF actuation functions.
- Validating or inhibiting of DAS and PS permissives as needed to transition the plant to safe shutdown.
- Interfacing with automatic functions within SAS (e.g., auto/manual switchover) as needed.

The SICS inventory in the RSS consists of the following controls that are unavailable on PICS but are needed to achieve and maintain safe shutdown:

- RT.
- P12 permissive (switches safety injection (SI) modes, bypasses main steam relief train (MSRT) isolation, main steam isolation, main feedwater startup and shutdown system (SSS) isolation functions, and SI accumulator valve interlock bypass).
- P14 permissive (partial cooldown operating bypass, setpoint change for MSRT opening residual heat removal (RHR) interlock).
- P15 permissive (SI mode switching).
- P17 permissive (pressurizer safety relief valve opening operating bypass, large miniflow line interlock).
- SIS actuation reset.
- Emergency feedwater system (EFWS) actuation reset.
- EFWS isolation reset.

- MSRIV opening reset.
- MSRT isolation reset.
- SG isolation reset.

### 7.4.1.2 Safe Shutdown Using Safety-Related Systems and Equipment

The plant is designed so that it can be taken from normal operating conditions to cold shutdown from the MCR using only safety-related systems in accordance with BTP 5-4. The safety-related systems and equipment, that with proper alignment are capable of achieving a safe shutdown of the plant, are described in Section 7.4.1.2.1 through Section 7.4.1.2.13. These systems satisfy GDC 1, GDC 2, GDC 3, and GDC 4.

The systems and equipment described in Section 7.4.1.2.1 through Section 7.4.1.2.13 are capable of bringing the plant to a cold shutdown condition, with only offsite or onsite power available along with the most limiting single failure. The entire shutdown procedure is completed from the MCR.

#### 7.4.1.2.1 Emergency Feedwater System

The emergency feedwater system (EFWS) provides a safety-related means of supplying feedwater to the steam generators (SG) for decay heat removal. This system is capable of maintaining hot standby and facilitating a plant cooldown. The I&C associated with the EFWS are described in Section 10.4.9.

#### 7.4.1.2.2 Main Steam System

The main steam system (MSS) contains the MSRT. The MSRT provides secondary side pressure control capability. The MSRT valves are located outside of containment upstream of the main steam isolation valves (MSIV). These valves are used to remove decay heat via the SGs in the event the condenser is unavailable (including loss of power), and to dissipate the heat to atmosphere. The MSRT may be used to cool and depressurize the reactor coolant system (RCS) to conditions necessary to initiate residual heat removal. The MSS contains the MSIVs and associated bypass valves that are necessary to isolate the secondary plant and to allow decay heat removal by the MSRT. The I&C associated with the MSS are described in Section 10.3.

#### 7.4.1.2.3 Medium Head Safety Injection

The safety injection system (SIS) contains medium head safety injection (MHSI) pumps that are capable of providing negative reactivity by the injection of highly borated water into the RCS from the in-containment refueling water storage tank (IRWST). The MHSI pumps may be used to add boron to the RCS during hot shutdown and cold shutdown phases, if the extra borating system (EBS) is unavailable. The I&C associated with the MHSI pumps and IRWST are described in Section 6.3.

#### 7.4.1.2.4 Extra Borating System

The EBS provides negative reactivity by injecting highly borated water into the RCS during the cooldown from the controlled state to the safe shutdown state to achieve core shutdown margin. The I&C associated with the EBS are described in Section 6.8.

#### 7.4.1.2.5 Residual Heat Removal System

The residual heat removal system (RHRS) provides the residual heat removal needed to reach cold shutdown and to control the primary temperature during cold shutdown. The I&C associated with the RHRS are described in Section 5.4.7.

#### 7.4.1.2.6 Excore Instrumentation System

The neutron flux range of measurement cannot be covered with sufficient accuracy by a single detector system. The range is subdivided into three overlapping ranges; source range, intermediate range, and power range. The source range monitors the lower six decades of neutron flux and is used to diagnose the plant status with regard to criticality in shutdown states.

#### 7.4.1.2.7 Reactor Coolant System

The RCS transfers heat from the core to the SGs to allow cooldown and depressurization of the RCS. Once the appropriate RCS temperature and pressure are met, connection of the RHRS to the RCS is allowed for further cooldown of the plant. The RCS provides the interface between the core and the RHRS for decay heat removal. Section 5.4 describes the components of the RCS.

#### 7.4.1.2.8 Emergency Diesel Generators and Auxiliaries

Four emergency diesel generators (EDG) (one per division) provide a reliable power source capable of starting and supplying necessary loads required to safely shut down and maintain a shutdown condition during a loss of offsite power (LOOP). The diesel generator (DG) fuel oil storage and transfer system, the DG cooling water system, the DG starting air system, the DG lubricating oil system, and the DG air intake and exhaust system are required to support EDG operation.

The I&C associated with the DG auxiliaries are described in Section 9.5.

#### 7.4.1.2.9 Essential Service Water System

The essential service water system (ESWS) transfers heat from the component cooling water system (CCWS) to the ultimate heat sink. The I&C associated with the ESWS are described in Section 9.2.1.

#### 7.4.1.2.10 Component Cooling Water System

The CCWS is an intermediate cooling system between safety-related loads and the ESWS. The CCWS transfers heat from plant safety-related and non-safety-related components to the ESWS. The I&C associated with the CCWS are described in Section 9.2.2.

#### 7.4.1.2.11 Safety Chilled Water System

The safety chilled water system (SCWS) provides chilled water for heating, ventilation, and air conditioning (HVAC) heat removal to safety-related room cooling units and cooling to Train 1 and Train 4 of the RHRS. Refer to Section 5.4.7 for more information on cooling water supplies to the RHRS. The I&C associated with the SCWS are described in Section 9.2.8.

#### 7.4.1.2.12 Heating Ventilation and Air Conditioning Systems

The HVAC systems provide ambient temperature control for the systems and components that are necessary for safe shutdown. These are the HVAC systems required for safe shutdown:

- MCR air conditioning system.
- Fuel building ventilation system.
- Safeguard building controlled-area ventilation system.
- Electrical division of safeguard building ventilation system.
- Emergency power generating building ventilation system.
- Emergency service water pump building ventilation system.
- Annulus ventilation system.

The I&C associated with the HVAC systems are described in Sections 6.2.3 and 9.4.

#### 7.4.1.2.13 Power Distribution System

The power distribution system distributes the available power (onsite or offsite) to the loads required for safe shutdown. Section 8.3 describes the buses required for operation of the safety-related equipment necessary for shutdown of the plant.

### 7.4.1.3 Post-fire Safe Shutdown Systems

The selection of post-fire safe shutdown systems is based on meeting the guidance of RG 1.189. The following assumptions, based on RG 1.189, were made in the selection process:

- All equipment in one fire area (except for the MCR and containment) is rendered inoperable by fire.

- Re-entry to the fire area for repair or operator actions is not possible.

The fire protection analysis described in Appendix 9A confirms the plant capability to safely reach cold shutdown following a fire. The systems described in Section 7.4.1.2 and the additional systems listed in Section 7.4.1.3.1 through Section 7.4.1.3.3 were identified as post-fire safe shutdown systems.

#### 7.4.1.3.1 Main Feedwater System

Associated circuits of concern were identified when selecting post-fire safe shutdown systems. These circuits are non-safety-related or safety-related circuits that could adversely affect the identified shutdown equipment by feeding back potentially disabling conditions. One of these disabling conditions is spurious operation of the main feedwater pumps caused by fire damage to the power circuit of these pumps. In the event that spurious operation of the main feedwater pumps occur, capability to isolate the main feedwater system is provided to prevent possible overcooling of the steam generator (SG).

#### 7.4.1.3.2 Chemical and Volume Control System

The chemical and volume control system (CVCS) is a non-safety-related system that provides reactivity control and reactor coolant makeup water. Reactivity control is possible through the injection of borated water through the CVCS charging lines. The CVCS is an alternate to the safety-related systems in Section 7.4.1.2 that provides reactivity control and reactor coolant makeup water. The I&C associated with the CVCS are described in Section 9.3.4.

#### 7.4.1.3.3 Fuel Pool Cooling and Purification System

The spent fuel pool cooling and purification system (FPCPS) provides cooling to the spent fuel pool to remove decay heat during normal operation, plant shutdown, and accident conditions. The FPCPS is included as a post-fire shutdown system because fires in the spent fuel areas must be considered. The I&C associated with the FPCPS are described in Section 9.1.3.

#### 7.4.1.3.4 Remote Shutdown Station

The RSS provides an independent alternative shutdown capability that is physically and electrically independent of the MCR.

The RSS is a control center located in Safeguard Building 3 near the MCR. It contains the equipment necessary to bring the plant to a safe shutdown state during an event requiring evacuation of the MCR, in conjunction with:

- A single failure of a system, structure, or component required to bring the plant to safe shutdown (in the event of a fire, no additional single failure, unrelated to the damage caused by the fire, is considered).

- A sustained loss of either onsite or offsite AC power.

The RSS contains both the PICS and the SICS. The PICS provides most of the necessary controls for safe shutdown. The SICS controls are only those controls needed to achieve safe shutdown that are unavailable on the PICS. These SICS controls are listed in Section 7.4.1.1. Therefore, the RSS, using PICS and SICS, provides all the displays and controls necessary to reach and maintain safe shutdown. The architecture of the SICS and PICS is described in Section 7.1. Communication equipment is described in Section 9.5.2.

The displays and controls in the RSS to allow the monitoring and control of the following safe shutdown functions during a postulated fire in the MCR or during an event that could cause the MCR to become uninhabitable, coupled with a single failure:

- Reactivity control.

- Reactor coolant makeup.

- Reactor coolant system pressure control.

- Decay heat removal.

- Control and monitoring of safety support systems for the above functions, as well as essential service water, component cooling water, and onsite power including the emergency diesel generators.

The physical layout of the RSS and equipment located in it is taken into consideration in the human factors engineering program described in Chapter 18.

In the event of a condition requiring MCR evacuation, operators will transfer control from the MCR to the RSS via the MCR-RSS transfer switches, which are located in the RSS. MCR actions required per procedures to transfer control to the RSS can be accomplished during a rapid evacuation of the MCR. Communications equipment is provided to support the transfer. If the MCR requires evacuation, the following actions are taken:

- Perform an RT (from the MCR if time allows, from the RSS if there is not enough time).

- Log out of the PICS workstations in the MCR (if time allows).

- Transition to the RSS.

- Actuate the MCR-RSS transfer switches, which performs the following actions:
  - Disables diverse actuation system (DAS) outputs so that no DAS functions (automatic or manual) are operable.
  - Disables manual controls for PS, SAS and PACS from the MCR.
  - Disables the ability of the PICS workstations in the MCR to communicate to the RCSL and PAS.
  - Enables manual controls for PS in the RSS.
- Log into the PICS workstations in the RSS.
- Take actions as needed to reach and maintain hot standby with the PICS.

If the MCR will be unavailable for an extended period of time, the operator will use the PICS as well as the necessary permissives and ESF resets, if necessary, on the SICS to reach and maintain cold shutdown.

The RSS is only utilized following an evacuation of the MCR. No actions are required from the RSS during normal operation.

The MCR-RSS transfer switches maintain divisional independence, so that an electrical failure in one safety division cannot affect another safety division. Additionally, the MCR-RSS transfer switches cannot be disabled by a single active failure coincident with a LOOP. Access to the MCR-RSS transfer switches results in annunciation of an alarm in the MCR. The MCR-RSS transfer switches are key-locked.

Displays in the MCR and RSS contain real-time plant data prior to, during, and after control transfer from one station to the other. The RSS data are populated from the same information buses that supply data to the MCR. During the time that control is transferred from the MCR to the RSS or vice versa, data are not lost or interrupted. An indication on the PICS and SICS shows that RSS control has been established.

#### 7.4.1.4 Station Blackout Safe Shutdown

The SBO safe shutdown equipment are predicated on fulfilling those functions delineated by 10 CFR 50.63 and RG 1.155 to take the plant from normal operating conditions to hot shutdown from the MCR. Section 8.4 describes the systems and equipment, including I&C systems necessary for achieving safe shutdown.

## 7.4.2 Analysis

### 7.4.2.1 Compliance with General Design Criteria

Compliance with these GDC, applicable to safe shutdown systems, is described in Section 7.1:

- GDC 2, Design Bases for Protection against Natural Phenomena.
- GDC 4, Environmental and Missile Design Bases.
- GDC 13, Instrumentation and Control.
- GDC 19, Control Room.
- GDC 24, Separation of Protection and Control Systems.
- GDC 34, Residual Heat Removal.
- GDC 35, Emergency Core Cooling.
- GDC 38, Containment Heat Removal.

### 7.4.2.2 Compliance with 10 CFR 50.55 a(h) and IEEE Std 603

10 CFR 50.55 a(h) requires safety-related systems to meet the requirements of IEEE Std 603-1991. This section addresses the following IEEE Std 603-1998 (Reference 1) requirements, as they pertain to particular safety-related I&C systems used for safe shutdown. An alternative request to use IEEE Std 603-1998 in lieu of IEEE Std 603-1991 is described in Section 7.1.

- Independence.
- Use of digital systems.
- Single failure.
- Testing.

#### 7.4.2.2.1 Independence

The safety-related I&C systems that are used for safe shutdown are designed to meet IEEE Std 603-1998, Clause 5.6, “Independence,” and IEEE Std 603-1998, Clause 6.3, “Interaction Between the Sense and Command Features and Other Systems” subject to the alternative request described in Section 7.1. Independence provisions and measures are implemented between the redundant divisions of the SCDS, PS, SAS, and the SICS. In addition, independence provisions and measures between the safety-related I&C systems and the other I&C systems make sure that possible interdependence between the safety-related I&C systems and other I&C systems does

not prevent the execution of safety-related functions. Safety-related I&C systems do not depend on non-safety-related I&C systems for their safety functions. Independence of the safety-related I&C systems is addressed in Section 7.1.

#### 7.4.2.2.2 Use of Digital Systems

The safety-related I&C systems utilize digital I&C. They are implemented using the TELEPERM XS platform which is approved for use in safety-related systems of nuclear power generating stations in the United States. These digital systems are implemented in architectures designed to satisfy requirements applicable to all safety-related I&C systems, digital or otherwise.

The IEEE Std 603-1998 contains the requirements that govern the implementation of safety-related I&C systems. Compliance with these requirements is addressed in Section 7.1. IEEE Std 7-4.3.2-2003 (Reference 3) contains the guidance that governs the use of digital computers in safety-related systems. Conformance to this guidance is addressed in Section 7.1.

#### 7.4.2.2.3 Single Failure Criterion

The four divisions of the safety-related I&C systems are physically separated and electrically isolated. Each division controls one of the four redundant divisions - fluid, mechanical, electrical and I&C. Consequently the safety function supported by the four redundant divisions can be performed even in case of a single failure in the I&C divisions. In the case of the EBS, only two divisions exist. One division of the EBS is controlled by Division 1 of the SAS and the other division is controlled by Division 4 of the SAS. A single failure in the EBS system or in the SAS will not prevent the execution of safety functions of the EBS.

The RSS is located in separate physical locations other than the MCR. The MCR-RSS transfer switches will disable MCR controls and enable control functions from the RSS. The MCR-RSS transfer switches also provide isolation between the RSS and the MCR. Therefore, no single credible event will cause the MCR to be evacuated and cause the RSS to malfunction.

A failure within the safety-related I&C systems will not lead to anticipated operational occurrences or postulated accidents even during maintenance or periodic testing.

#### 7.4.2.2.4 Testing

Self and periodic testing of the safety-related I&C systems is implemented to detect failures that could prevent the execution of the safety-related functions.

Measures are taken to detect and identify failures during reactor operation in order to avoid long periods of operation with degraded safety-related I&C systems, structures,

and components which might lead to a loss of function due to an accumulation of failures.

### 7.4.2.3 Remote Shutdown Capability

The RSS provides the capability to remotely shutdown the plant. The MCR-RSS transfer switches are located in a separate fire area than the MCR to allow transfer of control without entry into the MCR. Alarms in the MCR will alert operators that control is transferred to the RSS. Parameter indications common to both the MCR and RSS are maintained throughout the transfer of control.

The RSS contains controls and indications that will allow the operators to control and monitor the safe shutdown systems. Controls and indications of permissive signals are provided in the RSS. The capability to manually validate permissives allows the operator to enable or disable protective functions that may be necessary for proper shut down of the plant. Sections 7.4.1.1 and 7.4.1.3.4 also provide information on RSS capability.

Administrative controls are provided to prevent unauthorized access to the RSS. The MCR-RSS transfer switches are key locked. Keys are maintained by appropriate plant personnel.

### 7.4.2.4 Loss of Plant Instrument Air Systems

The safety-related I&C necessary for safe shutdown are not reliant on instrument air. Any devices that use instrument air fail in a safe position upon loss of air. Section 9.3.1 describes the plant instrument air system.

### 7.4.2.5 Loss of Cooling Water to Vital Equipment

Cooling water systems required for safe shutdown are addressed in Section 7.4.1.2.9 through Section 7.4.1.2.11.

### 7.4.2.6 Turbine Trip and Plant Load Rejection

Safe shutdown capability is provided in the event of a LOOP associated with a turbine trip or plant load rejection. The EDGs will provide power to the safe shutdown system components and I&C systems in the event of a LOOP.

## 7.4.3 References

1. IEEE Std 603-1998, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 1998.

2. NUREG-0800, BTP 5-4, “Design Requirements of the Residual Heat Removal System,” U.S. Nuclear Regulatory Commission, Rev. 3, March 2007.

3. IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.