TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

8.0 INSTRUMENTATION AND CONTROL SYSTEMS

Learning Objectives:

1. State the purposes of the following:

    a. Safety Information and Control System,
    b. Process Information and Control System,
    c. Protection System,
    d. Process Automation System, and
    e. Diverse Actuation System.

2. Describe the major differences between the control and instrumentation system design of the US-EPR and those of currently operating PWRs.

8.1 Introduction

The US-EPR implements a modern instrumentation and control (I&C) design. The US-EPR I&C systems implement these design features to optimize overall plant safety:

- Use of state-of-the-art I&C technology: The I&C design maximizes the use of programmable electronic I&C technology. Many features of this technology provide overall improvements in plant safety. These features include continuous online self-testing and diagnostics that allow early detection of failures and improved human-machine interfaces (HMIs) using video display units that provide an integrated view of process-system status to the operators.

- Robust I&C architecture design: The I&C architecture implements several design principles such as defense in depth, diversity, redundancy, independence, and priority to optimize plant safety. These principles are applied so that the impact of failures is minimized and that the required safety functions are executed when required.

- Automation of plant operation: A high degree of automation is implemented to improve plant operation, to reduce operator burden, and to improve situational awareness during normal and accident conditions. For design-basis events, safety functions required during the first 30 minutes are automated.

- State-of-the-art design for human factors: The I&C design is integrated with human factors engineering principles for improved human reliability and overall plant safety.

The primary I&C systems used for control and monitoring in the plant are collectively referred to as the distributed control system (DCS). The DCS performs the majority of signal input processing, automation, operator interface, annunciation of abnormal process conditions, and actuator output functions in the plant. The DCS implements functional requirements specified by the various plant mechanical and electrical systems, provided in the following list:

- Process control and limitation functions,
- Reactor trip functions,
- Engineered safety feature (ESF) actuation functions,
- Safety control and interlock functions,
- Severe accident control functions,
- Diverse reactor trip and ESF actuation functions,
- Process indications, post-accident monitoring (PAM) indications, and severe accident indications, and
- Alarms.

Black-box I&C systems in the plant include dedicated systems for specific functions, such as the acquisition and processing of neutron flux measurements. I&C equipment is also contained in mechanical and electrical systems. This equipment includes instrumentation and black boxes for packaged equipment, such as emergency diesel generators (EDGs).

The safety-related I&C systems use proprietary, time-triggered operating systems that do not rely on hardware and interrupt only on cyclic processing of the software. Because there are no process-driven interrupts, every operation is cyclic and predictive; this feature verifies that the output of messages on network links prevents collision.

The hardware components only read the incoming memory buffer or generate a packet to send only when the operating system generates the order. The cyclic operations of the processing units verify that the operator does not simultaneously perform a reading and writing operation.

The protection portions, as well as certain nonsafety-related portions, of the US-EPR I&C design incorporate the TELEPERM XS (TXS) platform, designed by the Siemens Power Corporation. TXS is a digital I&C platform that has been specifically designed and qualified for use in nuclear safety-related applications. The TXS platform is described in Topical Report EMF-2110(NP)(A).

TXS is a distributed, redundant computer system. The US-EPR application consists of four independent redundant data-processing paths (channels), each with two or three layers of operation and running asynchronous with respect to each other. Layers of operation include signal acquisition, data-processing, and actuation signal voting. The communication between redundant channels uses end-to-end fiber-optic cable connections.

The signal-acquisition layer in each channel acquires analog and binary input signals from sensors in the plant (such as for temperature, pressure, and level measurements). Each signal acquisition computer distributes its acquired and preprocessed input signals to the data-processing computer in the next layer.

The data-processing computers perform signal processing for plant protective functions such as signal online validation, limit value monitoring, and closed-loop control calculations. Each data-processing computer then sends its outputs to all of the independent voter computer units (two per channel, eight total).

The signal online validation uses a second-minimum (or second-maximum) principle. For a redundant measurement system, each protection channel compares the second lowest measurement to the low setpoint value and then determines the partial trip status of that channel for a "low trip" parameter. Similarly, it compares the second highest measurement to the high setpoint value and then determines the partial trip status of that channel for a "high trip" parameter. This method will reject an outlying signal and thereby minimize inadvertent trips.

In the voter computers, the outputs of the data-processing computers of the redundant channels are processed together. A voter computer controls a set of actuators. Each voter receives the actuation signal from each of the redundant data-processing computers. The voter's task is to compare this redundant information, using simple two-out-of-four logic, and to compute a validated (voted) actuating signal, which is used for actuating the end devices.

Because of advances in technology and the rapid obsolescence of components, the various modules described in EMF-2110(NP)(A) will be modified and upgraded over time, and new modules will be developed.

8.2 Instrumentation and Control Architecture Overview

8.2.1 Human-Machine Interface Systems

8.2.1.1 Safety Information and Control System

The safety information and control system (SICS) is provided as a safety-related HMI and is specifically designed to provide the operator with the necessary inventory of controls and indications in the main control room (MCR) and in the remote shutdown station (RSS) for the following:

- Mitigation of anticipated operational occurrences (AOOs) and postulated accidents (MCR),
- Reaching and maintaining safe shutdown (MCR and RSS),
- Mitigation of AOOs and postulate accidents concurrent with a common-cause failure of the protection system (MCR), and
- Mitigation of severe accidents (MCR).

The SICS controls in the MCR are not normally used by the operator. The SICS is used for manual implementation of reactor trips, ESF actuations, and permissives, and when the process information and control system (PICS) is unavailable. The SICS in the RSS provides controls not available in the PICS in the RSS to reach and maintain safe shutdown following an evacuation of the MCR.

Table 8-1 shows the functions of the SICS.

The required controls and indications of the SICS are implemented with dedicated, hardwired I&C equipment. Additionally, as part of the SICS a subset of plant parameters is duplicated on the nonsafety-related qualified display system (QDS). The nonsafety-related QDS is capable of trending of information, including Type A,

B, and C post-accident-monitoring variables, needed to provide situational awareness by the operator. Each QDS subsystem receives input only from the four divisions of the protection system. Isolation between the protection system and the QDS is provided by the protection system.

The SICS is implemented with various types of I&C technology to support its functions. Manual controls are implemented with buttons and switches. Indications are provided via digital indicators. A limited number of indications are provided on the QDS for situational awareness. The QDS consists of a display, computer, and input devices such as a touch screen or trackball.

The safety-related portion of the SICS is powered from the Class 1E uninterruptible power supply system (EUPS). The EUPS provides backup power with two-hour batteries and the emergency diesel generators (EDGs) in the case of a loss of offsite power (LOOP). In the event of a station blackout (SBO), the EUPS has the capability of receiving power from the station blackout diesel generators (SBODGs).

The nonsafety-related portion of the SICS is powered from the 12-hour uninterruptible power supply system (12UPS). The 12UPS provides backup power with 12-hour batteries and the SBODGs during a LOOP.

8.2.1.2 Process Information and Control System

The nonsafety-related PICS is a modern HMI. The operator primarily uses the PICS to control the plant during normal, abnormal, and accident operation. There are a limited number of controls for the protection system, the safety automation system (SAS), and the diverse actuation system (DAS) that are only available in the SICS. PICS equipment is provided in both the MCR and the RSS. Monitoring-only capabilities are provided in the technical support center (TSC) for support of emergency-response operations.

The PICS is classified as nonsafety related, augmented quality. Table 8-1 shows the functions of the PICS.

The PICS consists of gateways, servers, operator workstations, plant overview panels, and firewalls.

Redundant gateways are provided for communication with the protection system, SAS, reactor control, surveillance, and limitation system (RCSLS), and turbine-generator I&C system (TG I&CS). The PICS receives unidirectional signals from the protection system and SAS to receive status information on those systems. The PICS communicates bi-directionally with the RCSLS and TG I&CS for control of reactivity control systems and the turbine-generator, respectively.

Servers are provided for data exchange between the automation bus and the HMI bus. The servers perform functions such as data message validation, short term data storage, and alarm management. Redundant servers are provided so that the PICS remains operational in the case of a failure of a single server. Multiple sets of redundant servers may be used to subdivide functionality (e.g., control and indication, alarm, historical data keeping, etc).

PICS workstations with control and monitoring capabilities are located in the MCR and the RSS. Normally, the operator displays in the RSS are in supervisory mode (view only) to prevent plant control until authorized in accordance with plant procedures. Operator displays are provided in the TSC with monitoring-only capabilities to assist in plant emergency response.

Plant overview panels are provided in the MCR and other locations, such as the TSC, as desired. These are wide-screen displays that are capable of providing continuously visible information to the operator.

The PICS is implemented with an industrial I&C platform. The servers consist of industrial computers. Operator workstations typically consist of computers, displays, and input devices (i.e., computer mice and keyboards). The operator may use several monitors that share input devices. These monitors display different plant functions, and the display content is interchangeable. The plant overview panels constitute a set of large panels that display an overview of plant and system status. Equipment such as network switches and electrical and fiber-optic cable are provided to support data communications. The PICS equipment is capable of trending information to provide situational awareness by the operator. In addition, the PICS has recording capability so that historical data can be recalled by the operator.

The plant annunciator is integrated into the PICS operating and monitoring system. Special screens display and organize alarms and warnings based on their status and relative levels of importance. An alarm hierarchy with a color coding system is used to immediately alert the operator of the importance of alarms based on the impact of the alarming conditions on plant safety.

The PICS is used to control both safety-related (via the process automation system [PAS] and the priority and actuator control system [PACS]) and nonsafety-related process systems. The PICS implements these measures to preclude spurious actuation of plant equipment:

- Operation of plant equipment is performed using a two-step process. A single mouse click on a component is followed by a verification step requiring a second single mouse click, so that a single inadvertent action by the operator does not result in a command signal.

- Touch screen displays are not used.

The PICS is powered from the 12UPS.

8.2.2 Automation Systems

8.2.2.1 Protection System

The safety-related protection system (PS) is an integrated reactor protection system (RPS) and ESF actuation system. The PS detects plant conditions that indicate the occurrence of an AOO or postulated accident, and it actuates the safety-related process systems required to mitigate the event.

Table 8-1 shows the functions of the PS.

The PS is organized into four redundant, independent divisions located in separate safeguard buildings. Each division contains two functionally independent subsystems (A and B). These subsystems are used to implement functional diversity for reactor trip functions.

The PS consists of acquisition and processing units, actuation logic units, monitoring service interfaces (MSIs), gateways, and service units. It is implemented with the TXS I&C platform and is powered from the EUPS.

8.2.2.2 Safety Automation System

The safety automation system is a Class 1E control system. The SAS performs automatic and manual grouped control functions to provide safety-related controls during normal operations, to mitigate the effects of AOOs and postulated accidents, and to achieve and maintain safe shutdown.

The SAS is classified as safety related. Table 8-1 shows its functions.

The SAS is organized into four independent divisions located in the safeguard buildings, emergency power generating buildings, and essential service water pump buildings.

The SAS consists of control units, MSIs, gateways, and service units. The control units execute the logic for the assigned automatic and manual grouped control functions. The control units acquire inputs from the signal conditioning and distribution system (SCDS), the PS, or the SICS via hardwired connections. Hardwired outputs from the control units are sent to the PACS for signal prioritization and drive actuation. Hardwired outputs may also be sent to the PAS to coordinate logic for related actuators within the PAS. Data are sent from the control units to the MSIs for display in the SICS, or via the MSIs and redundant gateways for display in the PICS.

The SAS is implemented with the TXS I&C platform and is powered from the EUPS.

8.2.2.3 Priority and Actuator Control System

The PACS is a safety-related system that performs prioritization of signals from different I&C systems, drive actuation, and the monitoring of plant actuators.

Table 8-1 shows the functions of the PACS.

Figure 8-2 provides a functional representation of the PACS. The PACS is organized into four independent divisions located in the safeguard buildings, emergency power generating buildings, and essential service water pump buildings. In each division, there is safety-related and nonsafety-related PACS equipment to interface with safety-related and nonsafety-related actuators, respectively. The safety-related PACS equipment and the nonsafety-related PACS equipment are located in separate cabinets.

The PACS is composed of priority and communication modules. One priority module and one communication module are provided for each actuator/black box. The PACS includes qualified isolation devices as needed. Fiber-optic cable is used for the data connection between the PAS and the PACS.

The PACS receives actuation orders sent by the various systems of the DCS for prioritization. Signals are sent either via hardwired connections or via a dedicated data connection to the PAS. Interfaces with actuation devices and actuated equipment (e.g., switchgear, torque and limit switches) are via hardwired connections. Priority between actuation requests from the various DCS systems is established by wiring the inputs using priority principles. The following systems inputs to the PACS are listed in order of priority:

- PS,
- DAS,
- SAS,
- SICS, and
- PAS.

The DAS is given a higher priority than the SAS because it is a functional substitute to the PS and is needed at this level of priority to verify proper operation of SAS functions on a software common-cause failure of the PS.

The safety-related PACS equipment is powered from the EUPS. The nonsafety-related PACS equipment in the safeguard buildings is powered from the 12UPS. The nonsafety-related PACS equipment in the emergency power generating buildings and the essential service water pump buildings is powered from uninterruptible power supplies (UPSs) and diesel-backed sources.

8.2.2.4 Reactor Control, Surveillance, and Limitation System

The nonsafety-related RCSLS performs reactivity-related control and limitation functions.

The RCSLS is organized into four divisions located in separate safeguard buildings. It is implemented with the TXS I&C platform and is powered from the 12UPS.

8.2.2.5 Process Automation System

The nonsafety-related PAS is the main automation and control system for the plant. The PAS provides controls for both safety-related and nonsafety-related equipment. The PAS only implements nonsafety-related or noncredited control functions for safety-related systems. The SAS is provided to perform safety-related, credited control functions for safety-related process systems.

Table 8-1 shows the functions of the PAS.

The PAS is comprised of four divisions located in the Nuclear Island in the following buildings:

- Safeguard buildings,
- Emergency power generating buildings,
- Essential service water pump buildings,
- Nuclear auxiliary building (division 4 only), and
- Radioactive waste building (division 4 only).

In addition, the PAS includes two trains that are located in the switchgear buildings and the circulating water cooling tower structure.

The PAS implements redundant control units to perform its functions. The number of redundant control units is dependent on the sizing of the PAS. The control units acquire hardwired signals directly from the SCDS, DAS, PS, SAS, RCSLS, field sensors, or black boxes. Outputs are sent to nonsafety-related actuators directly or to the PACS. Interfaces are also provided to the TG I&CS for turbine-generator operation. The control units interface with the PICS via the plant data network for manual commands and the display of information.

The PAS is implemented with an industrial, commercial-grade digital I&C platform that is diverse from the TXS hardware and software.

The PAS is powered in the safeguard buildings from the 12UPS, in the turbine building from the non-Class 1E uninterruptible power supply system, and in other buildings from UPSs and diesel-backed sources.

8.2.2.6 Diverse Actuation System

The DAS is the I&C system that is provided to mitigate an AOO or postulated accident concurrent with a common-cause failure of the PS. In order to be sufficiently diverse from the PS, the DAS is required to be constituted of electrical, electronic, or programmable electronic I&C technology other than microprocessor-based technology.

The DAS is classified as nonsafety related, augmented quality. Table 8-1 shows its functions.

The DAS is organized into four redundant divisions located in separate safeguard buildings. Each division of the DAS contains a diverse actuation unit (DAU). Hardwired signals are acquired from the SCDS and compared to setpoints. Hardwired connections are provided to share trip requests, and two-out-of-four voting is performed in each DAU. Outputs are sent to the reactor trip breakers, control rod drive control system (CRDCS), TG I&CS, and PACS via hardwired connections. Signals are also sent to the PAS to display information in the PICS and to coordinate logic as necessary. This logic is not relied upon to mitigate an AOO or postulated accident concurrent with a common-cause failure of the PS.

The DAUs interface with the SICS via hardwired connections to receive manual system-level commands and to display information.

The DAS is powered from the 12UPS.

8.2.2.7 Signal Conditioning and Distribution System

The SCDS is a safety-related system that performs signal conditioning and distribution of signals from sensors or black boxes. Table 8-1 shows its functions.

The SCDS is organized into four independent divisions located in the safeguard buildings, emergency power generating buildings, and essential service water pump buildings. In each division, safety-related and nonsafety-related SCDS equipment interfaces with safety-related and nonsafety-related sensors, respectively. The safety-related SCDS equipment and nonsafety-related SCDS equipment are located in separate cabinets.

The SCDS is composed of noncomputerized signal conditioning modules and signal distribution modules that are part of the TXS platform. Multiple signal conditioning modules or signal distribution modules may be used for a particular signal, depending on the required conditioning and the number of DCS systems to which the output signal is required to go.

The SCDS receives hardwired signal inputs from sensors or black boxes. The SCDS sends hardwired signal outputs to the SICS, DAS, PS, SAS, RCSLS, and PAS as needed. Outputs from safety-related SCDS equipment to nonsafety-related DCS systems are electrically isolated by the signal distribution modules.

The SCDS is implemented with TXS signal conditioning and distribution equipment. The signal conditioning and distribution modules are diverse from the digital TXS function processors, and they are simple devices that are not considered susceptible to software common-cause failure.

The safety-related SCDS equipment is powered from the EUPS, the nonsafety-related SCDS equipment in the safeguard buildings is powered from the 12UPS, and the remaining nonsafety-related equipment is powered from UPSs and diesel-backed sources.

8.2.3 Black-Box I&C Systems

8.2.3.1 Control Rod Drive Control System

The CRDCS is classified as nonsafety-related.

The CRDCS controls the actuation of the 89 rod cluster control assemblies (RCCAs) in the reactor vessel. The CRDCS accomplishes this task by controlling the currents to the individual coils of the control rod drive mechanisms (CRDMs) to move the corresponding RCCAs. The CRDCS also sends feedback signals to the RCSLS for the generation of digital rod position indications.

The CRDCS receives dc power from the NUPS to move and hold the CRDMs. The reactor trip breakers are upstream of the CRDMs.

Within the CRDCS, the safety-related trip contactor modules interrupt power to the CRDMs when a trip signal is received from the PS. Each set of trip contactors gets

a signal from each division of the PS; each set is arranged to implement two-out-of-four logic. The contactor modules are environmentally qualified for seismic effects and for electromagnetic and radio-frequency interference.

The DAS provides a reactor trip signal to the CRDCS in the case of an AOO or postulated accident concurrent with a common-cause failure of the PS. The reactor trip signal is sent to the control logic to drop the rods in a diverse manner from that effected by the trip contactors.

8.2.3.2 Incore Instrumentation System

The safety-related incore instrumentation system (ICIS) measures certain in-vessel parameters. The ICIS consists of safety-related and nonsafety-related equipment.

The ICIS consists of:

- Self-powered neutron detectors (SPNDs) (safety-related except for test equipment),
- Aeroball measurement system (AMS) (nonsafety-related),
- Fixed core-outlet-thermocouple (COT) measurement system (safety-related), and
- Reactor pressure vessel dome temperature (RPVDT) measurement system (nonsafety-related).

Seventy-two SPNDs continuously measure the neutron flux at given positions in the core to provide information about the three-dimensional flux distribution. The AMS is used to calibrate the SPNDs at regular intervals.

The COTs continuously measure fuel assembly outlet temperatures. The fixed thermocouples are placed in selected fuel assemblies. The core outlet temperature is used to determine the saturation margin (ΔT_{sat}) at the core exit and to provide information about the radial temperature distribution in the core and average temperature in the reactor coolant system (RCS). There are a total of 36 COTs. The COTs are arranged with three thermocouples (two narrow-range thermocouples and one wide-range thermocouple) within each of the twelve SPND finger assemblies.

The RPVDT measurement system continuously measures the temperature within the reactor dome. The sensing elements are thermocouples. The RPVDT instrumentation provides temperature signals from the top-level, mid-level, and bottom-level measurement regions of the dome. The measurements of fluid temperature in the RPV dome provide information to the operator during normal and emergency operations if they are available (although not required for post-accident monitoring).

8.2.3.3 Excore Instrumentation System

The safety-related excore instrumentation system (EIS) monitors neutron flux during power and shutdown modes of operation. Because it is not possible to measure the entire operating range of reactor power with a single set of instruments, three ranges of detection are used:

- Power range – uses uncompensated, boron-lined ionization chambers,
- Intermediate range – uses gamma-compensated, boron-lined ionization chambers, and
- Source range – uses boron-lined proportional counters.

These ranges provide coverage from shutdown conditions to about 200% reactor power. Overlaps between measuring ranges allow operation of two ranges during transitions in power levels.

Eight power range detectors cover the upper three decades up to 200% reactor power. Two detectors are located in each of four radial locations around the core (45°, 135°, 225°, 315°). The two detectors at each location measure the upper and lower portions of the core for monitoring and control of axial flux distributions.

Four intermediate range detectors monitor a little more than seven decades up to at least 60% of full power, with an overlapping of the source range by about 2.5 decades. They are located in the same radial locations as the power range detectors.

Three source range detectors are provided at three radial locations around the core (0°, 90°, 270°). The source range detectors monitor the lower six decades.

8.2.3.4 Turbine-Generator Instrumentation and Control System

The turbine-generator I&C system (TG I&CS) regulates the operation of the turbine-generator for power generation. It provides speed and load control, as well as control of turbine-generator auxiliaries. The TG I&C also performs a turbine trip when requested by either the PS or the DAS.

8.2.3.5 Rod Position Measurement System

The rod position measurement system (RPMS) is classified as safety related.

The RPMS measures the positions of the RCCAs located in the reactor vessel and provides the measurements for control andindication to the operator.

Each rod position sensor is comprised of one primary and three secondary coils, which are part of the CRDM. Two of the secondary coils, called auxiliary secondary coils, indicate the rod at its lowest or highest end position. The third secondary coil, or main secondary coil, indicates the entire range of RCCA travel. The analog position measurement of the RCCA is derived from the magnetic coupling through the control rod between the primary coil and the secondary coils. The auxiliary secondary coil signals determine the extreme positions of the drive rod.

The RPMS is arranged in four divisions located in the four safeguard buildings. Each of divisions 1, 2, and 3 processes measurement for 22 RCCAs, and division 4 processes measurements for 23 RCCAs, for a total of 89 RCCA position measurements.

8.2.3.6 Miscellaneous Process Interface Systems

The following is a list of additional process-interface systems:

- Boron concentration measurement system,
- Radiation monitoring system,
- Hydrogen monitoring system,
- Reactor pressure vessel level measurement system,
- Seismic monitoring system,
- Loose parts monitoring system,
- Vibration monitoring system,
- Fatigue monitoring system, and
- Leak detection system.

8.3 Reactor Trips

The US-EPR provides safety-related instrumentation and controls to sense accident conditions requiring protective action and to automatically initiate a reactor trip. The protection system initiates automatic trips to rapidly introduce negative reactivity to the core to mitigate the effects of anticipated operational occurrences and postulated accidents, and to prevent acceptable fuel design limits from being exceeded. The PS automatically initiates trips when selected variables exceed setpoints that are indicative of conditions which require protective action. Additionally, the ability to manually initiate the reactor trip function is provided in the main control room and the remote shutdown station. Initiation of the trip function results in the removal of electrical power from the control rod drive mechanism coils, allowing the rods to fall by gravity into the core.

8.3.1 System Description

The PS processes both automatic and manual trip functions. Each trip function is performed redundantly and independently in each of the four PS divisions. A reactor trip order, produced by at least any two of the four divisions, results in a reactor shutdown. Key process variables are continuously monitored to determine the safety status of the plant. There are three sources of variables used as inputs to automatic trip functions:

- Incore instrumentation: The self-powered neutron detectors provide inputs to calculate variables that cannot be directly measured, such as linear power density and departure from nucleate boiling ratio (DNBR).

- Excore instrumentation: The power range detectors and intermediate range detectors provide measurements of reactor power, which are used as inputs to trip functions such as high neutron flux and low doubling time.

- Process instrumentation: Process instrumentation is used to measure variables such as pressure, temperature and flow. These process measurements are used

directly to initiate trips or as inputs to calculations of variables that cannot be measured directly.

Either of two diverse sets of reactor trip devices can successfully remove power to the CRDM coils. These sets are the reactor trip breakers and the reactor trip contactors. When a trip order is generated, the PS acts on the trip devices as described below:

- Reactor trip breakers: There are four trip breakers, two each in electrical divisions 2 and 3. Each division of the PS acts on the undervoltage coil of one trip breaker. The opening of at least one breaker in electrical division 2 and of at least one breaker in electrical division 3 results in reactor shutdown. The trip breakers are part of the non-Class 1E power supply system.

- Reactor trip contactors: There are 23 sets of four trip contactors. Eleven sets of contactors are in electrical division 1, and twelve sets are in division 4. Each set of contactors supplies power to four CRDMs, with the exception of one set in division 4, which supplies power to only the center CRDM. Each division of the PS opens one contactor in each of the 23 sets. Each set of contactors is arranged in a two-out-of-four configuration, so that trip orders issued from any two PS divisions result in reactor shutdown. The trip contactors are part of the control rod drive control system.

Figure 8-3 illustrates the arrangement and divisional assignments of the safety-related trip devices.

An automatic trip actuation is performed by the PS when a selected plant parameter reaches an appropriate setpoint. The typical sequence performed by the PS to initiate an automatic trip is illustrated in Figure 8-4 and is described as follows:

- An acquisition and processing unit (APU) in each division of the PS acquires through the SCDS one fourth of the redundant sensor measurements that are inputs to a given trip function.

- The APU in each division performs any required processing or calculations using the input measurements, and compares the resulting variable to a relevant setpoint. If a setpoint is breached, a partial trigger signal is generated.

- The partial trigger signals generated in each PS division are sent to redundant actuation logic units (ALUs) in all four divisions (four per division, grouped into two subsystems of two ALUs), where two-out-of-four logic is performed. If partial triggers are present from two divisions, the ALUs in all four divisions generate trip signals.

- The trip signals from the redundant ALUs in each subsystem are combined in a hardwired “functional-AND” logic. If a trip signal is present from both redundant ALUs, a trip output is generated. The trip outputs from both subsystems in a division are combined in a hardwired “functional-OR” logic. If either subsystem of a division produces a trip output, a divisional trip order is propagated to the trip breakers and trip contactors.

The capability for manual reactor trip is available to the operator through the safety information and control system in both the MCR and the RSS. Each location provides four manual trip buttons, which correspond to the four PS divisions. Manual trip initiation is illustrated in Figure 8-5 and is also described in ANP-10309P, "U.S. EPR Digital Protection System Technical Report." The SICS is described in section 8.2.

8.3.2 Reactor Trip Initiating Signals

When any of the following conditions is determined by the PS, it initiates a reactor trip:

- Low departure from nucleate boiling ratio (DNBR),
- High linear power density,
- High neutron flux rate of change,
- High core power level,
- Low saturation margin,
- Low reactor coolant system (RCS) flow rate (two loops),
- Low-low RCS flow rate (one loop),
- Low reactor coolant pump speed,
- High neutron flux,
- Low doubling time,
- Low pressurizer pressure,
- High pressurizer pressure,
- High pressurizer level,
- Low hot leg pressure,
- Steam generator pressure drop,
- Low steam generator pressure,
- High steam generator pressure,
- Low steam generator level,
- High steam generator level, and
- High containment pressure.

Each of these process conditions is determined to exist when a predefined or variable setpoint is exceeded by a related process parameter. The specific setpoint values are chosen to protect safety limits and to support the assumptions made in the plant safety analysis. The variables monitored for reactor trips and their measuring ranges are listed in Table 8-2. In addition to the process conditions that cause trips, these safety-related signals initiate a reactor trip:

- Safety injection system (SIS) actuation,
- Emergency feedwater system (EFWS) actuation, and
- Manual reactor trip signals from the SICS.

The trip functions are listed in Table 8-3.

Operating bypasses of specific trip functions are permitted when plant conditions dictate that the function is not needed, or that the function would prevent proper plant operation. These bypasses are implemented in the form of permissive signals

(P#) that are generated within the PS. The applicable permissive signals (if any) associated with each trip are identified in the description of each function in the following subsections.

8.3.2.1 Reactor Trip on Low Departure from Nucleate Boiling Ratio

The low DNBR trip is provided to protect the fuel against the risk of departure from nucleate boiling (DNB) during events that lead to a decrease of the DNBR value. Online calculations in the PS are used to construct variables representative of the DNBR phenomenon.

The DNBR calculation performed by the PS is based on:

- Power density distribution of the hot channel: This parameter is directly derived from the SPND measurements.
- Inlet temperature: This parameter is derived from the cold leg temperature sensors.
- Pressure: This parameter is derived from the pressurizer pressure sensors.
- Core flow rate: This parameter is derived from the reactor coolant pump (RCP) speed sensors.
- Three-loop operating signal: This signal is generated as part of the low RCS flow rate trip function (refer to section 8.3.2.5). The signal accounts for the change in RCS flow rate caused by the shutdown of an RCP.

The outputs of the DNBR calculation consist of twelve DNBR values (one per SPND finger), and twelve outlet quality values (one per SPND finger). The output values are used in various combinations to determine whether a reactor trip is necessary:

- Second lowest DNBR value compared to a variable low setpoint,
- Lowest DNBR value compared to a variable low setpoint that is only valid when either a rod drop (1/4) signal or SPND imbalance signal is present,
- Lowest DNBR value compared to a variable low setpoint that is only valid when a rod drop (2/4) signal is present,
- Second highest quality value compared to a fixed high setpoint, and
- Highest quality value compared to a fixed high setpoint that is only valid when either a rod drop (1/4) signal or SPND imbalance signal is present.
-

The values of the variable low DNBR setpoints depend on the number of invalidated SPND fingers. Each SPND input signal is monitored by the PS, using both inherent and engineered monitoring mechanisms, to determine the validity of the signal. If an SPND input signal is determined to be invalid, it is automatically assigned a faulty status. Additionally, if an SPND is determined to be faulty in the course of manual surveillance, the corresponding input signal is manually assigned a faulty status via the service unit. Since the DNBR calculation produces its outputs on a per-finger basis (six SPND per finger), if one SPND carries a faulty status, then the entire finger is considered invalid. One of six predetermined setpoint values is automatically selected for use based on the number of invalidated fingers. This is done for each of the three variable setpoints used in the DNBR function. The determination of setpoint values for the variable DNBR setpoints and for the fixed

high quality setpoints is described in ANF-10287P, “Incore Trip Setpoint and Transient Methodology for U.S. EPR.”

The rod drop (1/4) and rod drop (2/4) signals are based on the rates of change of the analog rod position measurements acquired by the PS. If a dropped rod is detected in one quadrant of the core, the rod drop (1/4) signal is generated, and the corresponding setpoints are activated. If a dropped rod is detected in two or more quadrants of the core, the rod drop (2/4) signal is generated, and the corresponding DNBR setpoint is activated.

The SPND imbalance signal is generated based on an indication of asymmetrical power distribution in the core. All 72 SPND measurements are used in each PS division to detect this condition.

The P2 permissive condition bypasses the low DNBR trip function at low power levels. This bypass is automatically removed as power increases above the P2 permissive setpoint.

8.3.2.2 Reactor Trip on High Linear Power Density

The high linear power density (HLPD) trip function is provided to protect the fuel against melting at the center of a fuel pellet during events which lead to an increase of linear power density in the core.

The calculation of HLPD performed by the PS uses the 72 SPND measurements as inputs. The HLPD calculation is performed on a per-SPND basis, resulting in 72 values of HLPD.

The second highest value of HLPD from the 72 calculated values is compared to a variable high setpoint (Max LPD) to generate a trip. The value of the variable setpoint depends on the number of invalidated SPND measurements.

Each SPND input signal is monitored by the PS, using both inherent and engineered monitoring mechanisms, to determine the validity of the signal. If an SPND input signal is determined to be invalid, it is automatically assigned a faulty status via the service unit. If the number of invalidated SPNDs is above a fixed setpoint (Max1p), a trip signal is generated. Additionally, if an SPND is determined to be faulty in the course of manual surveillance, the corresponding input signal is manually assigned a faulty status. One of six predetermined setpoint values is automatically selected for use based on the number of invalidated SPND inputs.

The P2 permissive condition bypasses the HLPD trip function at low power levels. This bypass is automatically removed as power increases above the P2 permissive setpoint.

8.3.2.3 Reactor Trip on High Neutron Flux Rate of Change

The high neutron flux rate of change trip function is provided to protect against an excessive reactivity increase. Specifically, the main objective of the function is to cope with a fast reactivity insertion such as that resulting from a rod ejection event.

The initiating signal is the derivative of neutron flux derived from measurements provided by the power range detectors. Each PS division acquires measurements from one of four pairs of detectors. Each pair consists of one measurement taken from the top half of the core, and one measurement taken from the bottom half. A calculation of nuclear power is performed in each division, based on the sum of the two detector measurements and the application of appropriate calibration coefficients. A rate/lag filter is then applied to the calculated nuclear power value to obtain a signal representative of the derivative of neutron flux. The derivative value is compared to a fixed high setpoint (Max QROC) to generate a reactor trip.

There are no operating bypasses associated with the high neutron flux rate of change trip.

8.3.2.4 Reactor Trip on High Core Power Level or Low Saturation Margin

The trip on high core power level (HCPL) is provided to protect against an excessive reactivity addition during operation at intermediate and high power levels. This function uses an enthalpy balance to calculate core thermal power. Additionally, a trip on low saturation margin is introduced because, in the case of saturation occurring in a hot leg, the core thermal power level calculation becomes invalid.

The core thermal power level is calculated based on the principles of conservation of energy and mass:

$$Q_{TH} = K_{CALTH} * W_{IN} * (H_{OUT} - H_{IN}) - H_{OUT} * \frac{dM}{dt} + \frac{d(M * H)}{dt}$$

Where:

Q_{TH}= Core thermal power,
K_{CALTH}= Calibration constant,
M = Mass of water in the core,
H = Average specific enthalpy of water in the core,
H_{IN} = Specific enthalpy at the core inlet,
H_{OUT} = Specific enthalpy at the core outlet, and
W_{IN}= Mass flow rate at the core inlet.

The enthalpies are calculated based on the cold leg wide-range (WR) temperature, the hot leg narrow-range (NR) temperature, and the hot leg WR pressure.

The mass flow rate is calculated by using the enthalpy and the pressure to determine a local density, which is then multiplied by the nominal core flow rate (constant value). A three-loop operating signal is used to account for the change in flow rate caused by the shutdown of an RCP. The three-loop operating signal is generated as part of the low RCS flow rate reactor trip function.

The mass of water in the core is calculated by using the average enthalpy and the pressure to determine an average density, which is then multiplied by the volume of the core (constant value).

The resulting value of core thermal power is compared to a fixed high setpoint (Max CPL) to generate a trip.

To determine the saturation margin value, the liquid saturation enthalpy (H_{SAT}) is calculated as a function of measured hot leg pressure, and the specific enthalpy at the core outlet (H_{OUT}) is calculated as a function of measured pressure and temperature at the core outlet. The saturation margin (DH_{SAT}), is then determined according to:

$$DH_{SAT} = H_{SAT} - H_{OUT}$$

The resulting value of saturation margin is compared to a fixed low setpoint (Min SAT) to generate a trip.

The P5 permissive condition bypasses both the high core power level and low saturation margin trip functions at low power levels. This bypass is automatically removed as power increases above the P5 permissive setpoint.

8.3.2.5 Reactor Trip on Low Reactor Coolant System Flow Rate – Two Loops

This function is provided to prevent a deviation from an adequate DNBR and to prevent the loss of sufficient heat removal from the reactor coolant system. A reactor trip is ordered when a low flow rate is detected in two RCS loops.

Four redundant flow measurements are obtained in each RCS loop. Each division of the PS acquires one flow sensor measurement from each loop, and each is compared to a fixed low setpoint (Min1p). If two partial triggers are generated for one RCS loop, the flow in that loop is considered low. An additional level of two-out-of-four voting logic is then applied so that a low flow must be detected in at least two RCS loops to generate a trip. If a low flow condition is present in any one RCS loop, a three-loop operating signal is generated. This signal is used to modify other PS functions which assume a nominal flow rate through the core.

The P2 permissive condition bypasses the low RCS flow rate – two loops trip function at low power levels. This bypass is automatically removed as power increases above the P2 permissive setpoint.

8.3.2.6 Reactor Trip on Low-Low Loop Flow Rate – One Loop

This function is provided to prevent a deviation from an adequate DNBR and to prevent the loss of sufficient heat removal from the RCS. A reactor trip is ordered when a low-low flow rate is detected in one RCS loop.

The 16 RCS flow sensor measurements are acquired by the PS in the manner described above. Each individual flow measurement is compared to a fixed low setpoint (Min2p). If two partial triggers are generated for a low-low flow rate in any one RCS loop, trip orders are generated.

The P3 permissive condition bypasses the low RCS flow rate – one loop trip function at low power levels. This bypass is automatically removed as power increases above the P3 permissive setpoint.

8.3.2.7 Reactor Trip on Low Reactor Coolant Pump Speed

This function protects against a loss of forced flow in the RCS due to events affecting the electrical supply of all four reactor coolant pumps. The loss of four RCPs is detected based on measurements of RCP speed (one measurement per pump).

Each PS division acquires the speed measurement from one RCP and compares it to a fixed low setpoint (Min RCPS). If any two of the four speed measurements decrease below the setpoint, trip orders are generated.

The P2 permissive condition bypasses the low RCP speed trip function at low power levels. This bypass is automatically removed as power increases above the P2 permissive setpoint.

8.3.2.8 Reactor Trip on High Neutron Flux

This function is provided to protect against excessive reactivity additions during a reactor startup from a subcritical or low power startup condition. The neutron flux variable is directly derived from the measurements of the intermediate range detectors. Each division of the PS acquires the measurement from one of four detectors.

To detect a high neutron flux condition, the detector measurements are multiplied by a calibration constant, and the resulting variables are compared to a fixed high setpoint (Max NF). If two out of four measurements exceed the setpoint, trip orders are generated.

The P6 permissive condition bypasses the high neutron flux trip function above a fixed core thermal power level. This bypass is automatically removed when core thermal power decreases below the P6 permissive setpoint.

8.3.2.9 Reactor Trip on Low Doubling Time

This function is provided to protect against excessive reactivity additions during a reactor startup from a subcritical or low power startup condition. The doubling-time variable is calculated using the intermediate range detector measurements as inputs. Each division of the PS acquires the measurement from one of four detectors.

To detect a low doubling-time condition, the detector measurements are used to calculate the neutron flux doubling time according to the concept:

$P(t) = P_0 e^{t/\tau}$

Where:

P(t) = Reactor power as a function of time,
P_0 = Initial reactor power,
t = Time during the transient in seconds, and
τ = Reactor period in seconds.

To determine the time to double the power, set $P(t) = 2P_0$ and $t = t_D$ (doubling time):

$2P_0 = P_0 e^{t_D/\tau}$, and solving for t_D:

$t_D = \tau \ln 2$.

If any two of the four PS divisions determine that a low doubling time condition is present, reactor trip orders are generated.

The P6 permissive condition bypasses the low doubling time trip function above a fixed core thermal power level. This bypass is automatically removed when core thermal power decreases below the P6 permissive setpoint.

8.3.2.10 Reactor Trip on Low Pressurizer Pressure

This function is provided to protect the integrity of the fuel in the case of an RCS depressurization that could lead to excessive boiling and saturated steam conditions in the core. The RCS pressure variable is redundantly measured by four NR pressurizer pressure sensors. Each division of the PS acquires one of the four pressure measurements and compares it to a fixed low setpoint (Min2p). If any two of the four measurements are below the setpoint, trip orders are generated.

The P2 permissive condition bypasses the low pressurizer pressure trip function at low power levels. This bypass is automatically removed as power increases above the P2 permissive setpoint.

8.3.2.11 Reactor Trip on High Pressurizer Pressure

This function is provided to protect the integrity of the reactor coolant pressure boundary and to prevent the opening of the pressurizer safety relief valves in the case of an RCS overpressure event. The RCS pressure variable is redundantly measured by four NR pressurizer pressure sensors. These measurements are acquired by the PS and are compared to a fixed high setpoint (Max2p). If any two of the four measurements are above the setpoint, trip orders are generated.

There are no operating bypasses associated with the high pressurizer pressure trip.

8.3.2.12 Reactor Trip on High Pressurizer Level

This function is provided to avoid overfilling the pressurizer in the case of a control system malfunction leading to an excessive increase in pressurizer water inventory. The pressurizer level variable is redundantly measured by four NR pressurizer level sensors. Each division of the PS acquires one of the four level measurements and compares it to a fixed high setpoint (Max1p). If any two of the four measurements are above the setpoint, trip orders are generated.

The P12 permissive condition bypasses the high pressurizer level trip function below the P12 pressure threshold. This bypass is automatically removed as pressure increases above the P12 permisive setpoint.

8.3.2.13 Reactor Trip on Low Hot Leg Pressure

This function is provided to protect the integrity of the fuel in the case of an RCS depressurization that could lead to excessive boiling and saturated steam conditions in the core. The RCS pressure variable is directly measured by four WR hot leg pressure sensors (one per hot leg). Each division of the PS acquires one of the four pressure measurements and compares it to a fixed low setpoint (Min1p). If any two of the four measurements are below the setpoint, trip orders are generated.

The P12 permissive condition bypasses the low hot leg pressure trip function at low RCS pressure conditions (measured by the pressurizer pressure sensors). This bypass is automatically removed as pressure increases above the P12 permissive setpoint.

8.3.2.14 Reactor Trip on Steam Generator Pressure Drop

This function is provided to protect the integrity of the fuel in the case of an overcooling event caused by an excessive increase in steam demand, or to adapt the reactor power to the capacity of the safety systems in case of an event that causes a decrease in heat removal by the secondary system. The steam generator (SG) pressure variable is directly measured by four pressure sensors in each SG. Each division of the PS acquires one pressure measurement from each SG and compares it to a variable low setpoint. If two measurements from any one SG decrease below the variable setpoint, trip orders are generated.

The condition to be detected is an SG pressure drop greater than a specified value (Max1p). This is accomplished by using a variable low setpoint. The value of the variable setpoint is maintained lower than the measured pressure by a fixed amount, with a limitation placed on the rate of decrease of the setpoint value. The measured pressure will only fall below the setpoint if it decreases at a rate greater than that of the rate-limited setpoint for a given amount of time.

There are no operating bypasses associated with the SG pressure drop trip.

8.3.2.15 Reactor Trip on Low Steam Generator Pressure

This function is provided to protect the integrity of the fuel in the case of an overcooling event caused by an excessive increase in steam demand. For smaller breaks in steam or feedwater piping, the rate of SG depressurization may not reach the setpoint for a trip on SG pressure drop. Therefore, a trip on low SG pressure is used to protect the fuel in these cases. The SG pressure variable is directly measured by four pressure sensors in each SG. Each division of the PS acquires one pressure measurement from each SG and compares it to a fixed low setpoint (Min1p). If two measurements from any one SG decrease below the setpoint, trip orders are generated.

The P12 permissive condition bypasses the low SG pressure trip function at low RCS pressure conditions. This bypass is automatically removed as pressure increases above the P12 permissive setpoint.

8.3.2.16 Reactor Trip on High Steam Generator Pressure

This function is provided to protect the integrity of the fuel and of the SG in the case of a secondary-side overpressure event. The SG pressure variable is directly measured by four pressure sensors in each SG. These measurements are acquired by the PS and are compared to a fixed high setpoint (Max1p). If two measurements from any one SG are above the setpoint, trip orders are generated.

There are no operating bypasses associated with the high SG pressure trip.

8.3.2.17 Reactor Trip on Low Steam Generator Level

This function is provided to protect the integrity of the fuel in the case of a steam demand versus feedwater flow mismatch caused by a control system malfunction or a break in feedwater piping. The SG level variable is directly measured by four NR level sensors in each SG. Each division of the PS acquires one level measurement from each SG and compares it to a fixed low setpoint (Min1p). If two measurements from any one SG decrease below the setpoint, trip orders are generated.

The P13 permissive condition bypasses the low SG level trip function at low temperatures, as measured in the hot legs. This bypass is automatically removed as hot leg temperature increases above the P13 permissive setpoint.

8.3.2.18 Reactor Trip on High Steam Generator Level

This function is provided to protect the integrity of the fuel in the case of a main feedwater control malfunction that causes an increase in feedwater flow resulting in RCS overcooling and a reactivity insertion. This function also protects the turbine from moisture carryover in the case of excessive feedwater addition or a rising SG water level due to a tube rupture.

The SG level variable is directly measured by four NR level sensors in each SG. These measurements are acquired by the PS and are compared to a fixed high setpoint (Max1p). If two measurements from any one SG are above the setpoint, trip orders are generated.

The P13 permissive condition bypasses the high SG level trip function at low temperatures, as measured in the hot legs. This bypass is automatically removed as hot leg temperature increases above the P13 permissive setpoint.

8.3.2.19 Reactor Trip on High Containment Pressure

This function is provided to protect the integrity of the containment during any event leading to water or steam discharge into the containment. The containment pressure variable is directly measured by two sets of four redundant pressure sensors. One set of four measures the pressure in the containment equipment

compartments. The other set of four measures the pressure in the containment service compartments.

Each division of the PS acquires one pressure measurement from each set of sensors. The containment service compartment pressure measurements are compared to a fixed high setpoint (Max2p), and the containment equipment compartment pressure measurements are compared to another fixed high setpoint (Max1p). If two measurements from either set of four pressure sensors are above the setpoint, trip orders are generated.

There are no operating bypasses associated with the high containment pressure reactor trip.

8.3.2.20 Reactor Trip on Safety Injection System Actuation

This function is provided to trip the reactor when an SIS is actuated by the PS. In each division of the PS, when a safety injection (SI) signal is generated, a reactor trip order is also generated in the same division.

There are no operating bypasses associated with this function; any automatic SI actuation will result in a trip.

8.3.2.21 Reactor Trip on Emergency Feedwater System Actuation – Low SG Level

This function is provided to trip the reactor when the emergency feedwater system is actuated by the PS due to low SG level.

In each division of the PS, when an EFWS actuation signal is generated due to low SG level (regardless of the EFWS train to be initiated), a trip signal is also generated in the same division.

The P13 permissive condition bypasses the reactor trip on EFWS actuation – low SG level function at low temperatures, as measured in the hot legs. This bypass is automatically removed as hot leg temperature increases above the P13 permissive setpoint.

8.3.2.22 Manual Reactor Trip

The capability for a manual reactor trip is provided to the operator through the SICS in both the MCR and the RSS. Each location provides four manual trip buttons, corresponding to the four PS divisions. Any two of four manual trip buttons together will actuate a reactor trip. The manual trip from the MCR is hardwired to bypass the APUs and ALUs of the PS and to act directly on the undervoltage coils of the trip breakers. The MCR and RSS manual trip initiation signals are also acquired by the PS and processed with the automatic trip functions.

For the steam generator tube rupture event, a manual reactor trip is credited to trip the reactor when the chemical and volume control system is operating.

8.3.3 Permissive Signals

Permissive signals are used to enable, disable or modify the operation of reactor trip and engineered safety features actuation functions based on plant conditions.

The state of a permissive signal is defined as either validated or inhibited. The validation or inhibition of permissive signals is defined as one of two types, depending on whether the state of the permissive is set automatically or manually. Those that are automatically validated or inhibited based on the corresponding plant condition are defined as P-AUTO. If an operator action is required to either validate or inhibit the permissive after the corresponding plant condition is satisfied, the permissive is defined as P-MANU. The operator may validate or inhibit manual permissives from the SICS.

The generation of the permissive signals is described below. These permissive signals are generated within the PS for use in reactor trip and engineered safety features actuation functions. Certain functions implemented in the diverse actuation system are also subjected to the same permissive conditions. In these cases, the permissive logic used in the PS is duplicated and performed separately within the DAS.

P2 Permissive

The P2 permissive is representative of power range neutron flux measurements higher than a low-power setpoint value (10 percent power). The P2 permissive setpoint value corresponds to the value below which transients do not lead to a risk of DNB.

To generate the permissive, neutron flux measurements from the power range detectors are compared to the setpoint. When two out of four measurements are greater than the setpoint, the permissive is validated. Otherwise, it is inhibited.

This permissive is P-AUTO with respect to validation and inhibition.

P3 Permissive

The P3 permissive is representative of power range neutron flux measurements higher than an intermediate power setpoint value (70 percent power). The P3 permissive setpoint value corresponds to the value below which loss of one reactor coolant pump does not lead to a risk of DNB.

To generate the permissive, neutron flux measurements from the detectors are compared to the setpoint. When two out of four measurements are greater than the setpoint, the permissive is validated. Otherwise, it is inhibited.

This permissive is P-AUTO with respect to validation and inhibition.

P5 Permissive

The P5 permissive is representative of intermediate range neutron flux measurements above a low power setpoint value (10^{-5}% power). The P5 permissive setpoint value corresponds to the boundary between the operating ranges of the source range detectors and the intermediate range detectors.

To generate the permissive, neutron flux measurements from the intermediate range detectors are compared to the setpoint. When two out of four of the measurements are greater than the setpoint, the permissive is validated. Otherwise, it is inhibited.

This permissive is P-AUTO with respect to validation and inhibition.

P6 Permissive

The P6 permissive is representative of core thermal power above a low power setpoint value (10% power) corresponding to the boundary between the operating ranges of the intermediate range and the power range detectors.

Hot leg pressure WR measurements, hot leg temperature NR measurements, and cold leg temperature NR measurements are used to calculate core thermal power. A three-loop operating signal is used to account for the change in flow rate caused by the shutdown of an RCP. The three-loop operating signal is generated as part of the low RCS flow rate trip function (refer to section 8.3.2.5). These calculated core thermal power levels are compared to the setpoint. When three out of four of the calculated core thermal power levels are greater than the setpoint, the operator is prompted to manually validate the permissive.

This permissive is P-MANU with respect to validation and P-AUTO with respect to inhibition.

P7 Permissive

The P7 permissive defines when reactor coolant pumps are no longer in operation.

RCP speed and breaker positions are monitored to determine whether an RCP is off. If at least two out of four of the following conditions are true, then an “RCP OFF” signal is generated for that pump:

- The RCP breaker is in the open position.
- The RCP bus breaker is in the open position.
- The first RCP speed measurement is less than or equal to a setpoint (90%).
- The second RCP speed measurement is less than or equal to a setpoint (90%).

When “RCP OFF” signals are generated for all four pumps, a delay time is started. After the delay time has expired, the permissive is validated.

This permissive is P-AUTO with respect to validation and inhibition.

P8 Permissive

The P8 permissive defines the shutdown state with all rods in (ARI).

Outputs from the rod cluster control assembly analog rod position sensors are acquired in the four electrical divisions. For each division, when all rods in the shutdown banks are less than the P8 permissive setpoint (two in.), a signal is generated. When two out of four of divisions indicate all rods in, the permissive is validated.

This permissive is P-AUTO with respect to validation and inhibition.

P12 Permissive

The P12 permissive defines the transition from hot shutdown to cold shutdown with respect to RCS pressure.

Pressurizer pressure NR measurements are compared to the P12 permissive setpoint (2005 psia). When three out of four of the measurements are less than the setpoint, the operator is prompted to manually validate the permissive.

This permissive is P-MANU with respect to validation and P-AUTO with respect to inhibition.

P13 Permissive

The P13 permissive facilitates plant heatup and cooldown by disabling certain engineered safety features functions.

Hot leg temperature WR measurements are compared to the P13 permissive setpoint (200°F). When three out of four of the measurements are less than the setpoint, the operator is prompted to manually validate the permissive.

This permissive is P-MANU with respect to validation and P-AUTO with respect to inhibition.

P14 Permissive

The P14 permissive defines when the residual heat removal (RHR) system is allowed to be connected to the RCS.

Hot leg temperature WR and hot leg pressure WR measurements are each compared to a setpoint (350°F, 464 psia). When two out of four of the hot leg temperature measurements are less than the temperature setpoint, and two out of four of the hot leg pressure measurements are less than the pressure setpoint, the operator is prompted to manually validate the permissive.

This permissive is P-MANU with respect to validation and inhibition.

P15 Permissive

The P15 permissive defines when SI actuation due to ΔP_{sat} is disabled and when SI actuation due to low loop level is enabled.

The same pressure and temperature measurement used for the P14 permissive are used for this permissive. RCP speed and breaker positions are monitored to determine whether an RCP is off. If at least two out of four of the following conditions are true, then an "RCP OFF" signal is generated for that pump:

- The RCP breaker is in the open position.
- The RCP bus breaker is in the open position.
- The first RCP speed measurement is less than or equal to a setpoint (90%).
- The second RCP speed measurement is less than or equal to a setpoint (90%).

When "RCP OFF" signals are generated for all four pumps, a delay time is started. After the delay time has expired, and the P14 permissive pressure and temperature conditions are satisfied, the operator is prompted to manually validate the P15 permissive.

This permissive is P-MANU with respect to validation and P-AUTO with respect to inhibition.

P16 Permissive

The P16 permissive defines when the SIS may be aligned from cold leg injection to hot leg injection.

Hot leg pressure WR measurements are compared to a setpoint (289.7 psia). When two out of four of the hot leg pressure measurements are less than the setpoint, the operator is prompted to manually validate the permissive.

This permissive is P-MANU with respect to validation and P-MANU (concurrent with reactor trip reset or hot leg pressure > 289.7 psia) with respect to inhibition.

P17 Permissive

The P17 permissive corresponds to the temperature conditions at which brittle fracture protection is required.

Cold leg temperature WR measurements are compared to a setpoint (248°F). When three out of four measurements are less than the setpoint, the operator is prompted to manually validate the permissive.

This permissive is P-MANU with respect to validation and P-AUTO with respect to inhibition.

8.4 Engineered Safety Features Actuations

The US-EPR provides safety-related instrumentation and controls to sense accident conditions and to automatically initiate the engineered safety features systems. ESF systems are automatically actuated when selected variables exceed setpoints that are indicative of conditions which require protective action. Additionally, the ability to manually initiate ESF systems is provided in the main control room. Manual system-level actuation of ESF systems initiates all actions performed by the corresponding automatic actuation, including starting auxiliary or supporting systems and performing required sequencing functions. Component-level control of ESF system actuators is also provided in the main control room.

8.4.1 System Description

Automatic actuation of ESF systems and auxiliary supporting systems is performed by the protection system when selected plant parameters reach the appropriate setpoints. These automatic actuation orders are sent to the priority and actuator control system for prioritization and interface to the actuators. An example of an ESF actuation sequence actuated by four division of the protection system is illustrated in Figure 8-6, and is described as follows:

- An acquisition and processing unit in each division acquires, through the signal conditioning and distribution system, one fourth of the redundant sensor measurements that are inputs to a given ESF actuation function.

- The APU in each division performs any required processing using the measurements acquired by that division (e.g., filtering, range conversion, calculations). The resulting variable is compared to a relevant actuation setpoint in each division. If a setpoint is breached, the APU in that division generates a partial trigger signal for the appropriate ESF function.

- The partial trigger signals from each division are sent to redundant actuation logic units in the PS division responsible for the associated actuation. Two-out-of-four voting is performed in each ALU on the partial trigger signals from all four divisions. If the voting logic is satisfied, an actuation order is generated.

- The actuation signals of the redundant ALUs in each division are combined in a hardwired “functional OR” configuration so that either redundant unit can actuate the function.

Actuation orders are sent from the PS to the PACS priority module associated with each actuator required for the function. The exception to this is the turbine trip function. The actuation order is transmitted via hardwired connections to the turbine-generator instrumentation and control system and does not involve the PACS. The PS and the PACS are discussed in section 8.2.

The safety automation system performs closed-loop automatic controls of certain ESF systems following their actuation by the PS. These controls are described in the following sections. The SAS is described in section 8.2.

The capability for manual system-level ESF actuations is available to the operator through the safety information and control system in the MCR. These manual actuations are acquired by the ALUs in the protection system and combined with the automatic actuation logic. The manual actuations are described with the corresponding automatic functions in the following sections.

The capability for component-level control of ESF system actuators is available to the operator via both the PICS and the SICS in the MCR. Commands from the PICS are processed by the PAS and sent to the PACS for prioritization. Commands from the SICS are sent directly to the PACS for prioritization. Actuation via the SICS is the safety-related actuation path, and actuation via the PICS is the nonsafety-related actuation path. The manual actuations are described with the corresponding automatic functions in the following sections.

The capability for manual reset of sense-and-command ESF actuation outputs is provided in the SICS. Not all ESF actuations require a manual reset. There are cases where a sense-and-command output is cleared after the PS determines that the initiating condition has cleared. The reset functionality related to the ESF actuations is described in the following sections. Further description of the operation of the PICS and SICS is presented in section 8.2.

8.4.2 Engineered Safety Features Actuation Functional Descriptions

The variables monitored for the ESF actuations and their measuring ranges are listed in Table 8-4. The actuation functions are listed in Table 8-5.

8.4.2.1 Safety Injection System Actuation

To mitigate a loss-of-coolant accident (LOCA), a safety injection signal is required to actuate the appropriate ESF and support systems and to isolate nonqualified reactor coolant system piping. In the case of a decrease in RCS water inventory due to a LOCA, the RCS is supplied by medium head safety injection (MHSI) in the high pressure phase of the event and by low head safety injection (LHSI) in the low pressure phase.

The US-EPR design provides for automatic generation of the safety injection signal during all modes of plant operation by utilizing three different initiation parameters, depending on the current plant state:

- Pressurizer pressure < Min3p,
- Hot leg ΔP_{sat} < Min1p, and
- Hot leg loop level < Min1p.

Safety injection system actuation based on pressurizer pressure results from narrow-range pressurizer pressure measurements below a fixed setpoint (Min3p) in any two of the four PS divisions. This initiation parameter is active above the P12 permissive pressure threshold and is bypassed below the P12 permissive setpoint.

SIS actuation based on hot leg ΔP_{sat} results from the difference between measured pressure and saturation pressure being below a fixed setpoint (Min1p) in any two of

the four PS divisions. The measured pressure is obtained from one wide-range pressure measurement in each hot leg. The saturation pressure is calculated from one WR temperature measurement in each hot leg. This initiation parameter is active when RCS pressure is below the P12 permissive pressure threshold and when RCS conditions are above the P15 permissive pressure and temperature thresholds. It is bypassed above the P12 permissive threshold and below the P15 permissive thresholds.

SIS actuation based on hot leg loop level results from RCS water level measurements below a fixed setpoint (Min1p) in any two of the four PS divisions. One loop level measurement is taken in each of the hot legs. This initiation parameter is active below the P15 permissive pressure and temperature thresholds with all four reactor coolant pumps shut down. It is bypassed above the P15 permissive thresholds. A manual bypass of SIS actuation on low hot leg loop level is provided for the protection of personnel working on RCS components during outages.

The capability for manual system-level initiation of the SIS is provided to the operator by the SICS in the MCR. This manual initiation starts the four trains of safety injection as well as the associated protective actions, such as partial cooldown and reactor trip. Four manual system-level initiation controls are provided; any two start the four SIS trains.

The capability for component-level control of the SIS actuators is available to the operator via both the PICS and the SICS in the MCR.

Reset of the SIS actuation sense-and-command output is available from the SICS in the MCR and the RSS. A reset of the SIS actuation output does not result in stopping the actions of the SIS actuators; it allows the operator to take further actions to stop specific trains of safety injection or to manipulate individual components as necessary to follow plant operating procedures.

8.4.2.2 Emergency Feedwater System Actuation

To mitigate the effects of a loss-of-main-feedwater (MFW) event, the emergency feedwater system is actuated as a safety-related means to remove residual heat via the steam generators. A number of failure mechanisms can result in a loss of MFW (e.g., feedwater line break, loss of offsite power, feedwater pump failure). Regardless of the initiating event, a low SG level condition is characteristic of a loss of MFW, and is used to actuate the EFWS.

An anticipatory EFWS actuation is also included to cope with the possibility of a LOOP concurrent with a LOCA, to enhance natural circulation cooldown.

The US-EPR design uses the following initiating conditions to actuate the EFWS:

- SG wide-range level < Min2p, and
- LOOP and SIS actuation signals generated.

EFWS actuation based on low SG level is performed on a per-SG basis. The actuation order is generated when two of four WR level measurements are below the Min2p setpoint in any one SG. Only the EFWS train corresponding to the SG with the low level condition is actuated.

EFWS actuation based on LOOP and SIS actuation is performed concurrently on all SGs.

In both cases, EFWS actuation is bypassed when hot leg temperature is below the P13 permissive setpoint. The bypass is automatically removed above the P13 permissive setpoint.

When EFWS actuation occurs due to a low SG level, the sense-and-command actuation output is reset automatically when the SG level again exceeds the Min2p setpoint. The actuation is reset so that the safety-related SG level control loop, performed by the SAS, can control the actuators needed to maintain the correct water level in the SG. Additionally, the capability for manual reset of the EFWS actuation signal is available, on a per-train basis, from the SICS in the MCR and the RSS. The manual reset does not result in stopping the EFWS actuation; it allows the operator to take further manual actions to stop the actuation.

When EFWS actuation occurs due to LOOP and SIS actuation, the PS sends a pulse signal of limited duration to start the actuation. The duration of the pulse is long enough for the intended actions of the execute features to go to completion. No reset is needed in this case, as the SG water level is already above the Min2p setpoint when the EFW actuation occurs, and the safety-related SG level control loop can immediately take control of the actuators.

The EFWS SG level control and EFWS pump flow protection functions provide the EFWS control valves with position correction signals as needed. The actual SG level and EFWS pump discharge flow are compared to their respective setpoints. A proportional plus integral (PI) step controller sends a close or open signal, depending on the valve position, to maintain the SG level and EFWS pump discharge flow parameters at their respective setpoints.

The safety-related closed-loop control for SG water level following EFWS actuation is performed by the SAS. When EFWS actuation occurs, the PS signals the SAS to initiate the closed-loop control. Separately, during SG water level control by the SAS, the SAS also performs a second closed-loop control that regulates pump flow to protect the EFW pump from an overflow condition.

The capability for manual system-level initiation of the EFWS on a per-train basis is provided by the SICS in the MCR. Three manual initiation controls are provided per EFW train. One-out-of-two logic applies to two of these controls to start the EFW pump, open the associated EFW valves, and isolate the SG blowdown line. The third control is used only to close SG blowdown isolation valves that are redundant to those closed by the first two controls.

The capability for component-level control of the EFWS actuators is available to the operator via both the PICS and the SICS in the MCR.

8.4.2.3 Emergency Feedwater System Isolation

To mitigate the effects of a steam generator tube rupture (SGTR), the EFWS is isolated when an SG level reaches a high level setpoint to avoid SG overfill and potential radioactive water discharge via the main steam relief train.

The US-EPR design uses the following initiating conditions to isolate the EFWS:

- SG wide-range level > Max1p, and
- SG isolation signal.

EFWS isolation based on SG level is performed on a per-SG basis. The actuation order is generated when two of four WR level measurements are above the Max1p setpoint in any one SG. Only the EFWS train corresponding to the SG with the high level condition is isolated.

EFWS isolation is bypassed when hot leg temperature is below the P13 permissive setpoint. The bypass is automatically removed above the P13 permissive setpoint.

The capability for manual system-level EFWS isolation on a per-train basis is provided to the operator by the SICS in the MCR. Two manual isolation controls are provided per EFWS train. Either of these two controls actuates the isolation function.

The capability for component-level control of the EFWS actuators is available to the operator via both the PICS and the SICS in the MCR.

The sense-and-command output to isolate the EFWS can be reset manually from the SICS in the MCR and the RSS. Reset of the sense-and-command output does not result in opening the EFWS isolation valves; it allows the operator to take further manual actions to open the valves. The manual reset is only allowed after the SG level returns to below the Max1p setpoint.

8.4.2.4 Partial Cooldown Actuation

When a safety injection signal is generated, it is necessary to perform a secondary-side partial cooldown to lower the RCS pressure to a point where MHSI is effective. This is necessary due to the MHSI shutoff-head discharge pressure possibly being lower than the nominal RCS pressure.

The safety-related partial cooldown function consists of lowering the Max1p main steam relief isolation valve (MSRIV) opening setpoint according to a predefined cooldown gradient. If SG pressure exceeds the decreasing Max1p setpoint, the MSRIVs are opened, and the main steam relief control valves (MSRCVs) operate to maintain SG pressure at the decreasing Max1p setpoint.

The partial cooldown is preferably performed by controlling the turbine bypass valves, in a nonsafety-related capacity, at a decreasing pressure setpoint that is maintained slightly lower than Max1p. The safety-related partial cooldown via the main steam relief trains (MSRTs) is provided to cope with turbine bypass control

failure, as the success of the safety injection function can depend on successful partial cooldown. Both the safety- and nonsafety-related partial cooldowns are initiated by the PS. The PS detects the condition requiring partial cooldown and sends an initiation signal via an isolated hardwired connection to the process automation system. Control loops for partial cooldown via turbine bypass are performed by the PAS. The PS also sends the partial cooldown initiation signal to the safety-related SAS. Control loops for partial cooldown via the MSRTs are performed by the SAS.

The US-EPR design uses the following initiating condition to actuate a partial cooldown:

- SIS actuation signal generated.

Partial cooldown is initiated any time an SIS actuation signal occurs, except during conditions when the RHR system can be connected. In such conditions, the primary pressure is already low enough for MHSI to be successful, and partial cooldown is not needed. For this reason, the partial cooldown actuation due to SIS actuation is bypassed below the P14 permissive pressure and temperature conditions.

The capability for manual system-level actuation of partial cooldown is provided by the SICS in the MCR. This manual initiation starts the partial cooldown via all four main steam trains if the P14 permissive is inhibited and the reactor is tripped. Four manual initiation controls are provided; any two start the partial cooldown.

When the Max1p setpoint has reached a predefined value, a partial cooldown finished signal is generated, and the sense-and-command output to actuate partial cooldown is reset automatically. The partial-cooldown-finished signal can then be reset manually from the SICS in the MCR.

8.4.2.5 Main Steam Relief Isolation Valve Opening

In the case of a loss of the secondary-side heat sink, decay heat has to be removed via steam relief to the atmosphere. The four MSRTs provide this functionality. The MSRTs also provide SG overpressure protection to minimize the actuation of the main steam safety valves and the associated risk of the safety valves failing to reseat. Additionally, the MSRTs participate in the partial cooldown function.
The US-EPR design uses the following initiating condition to actuate MSRIV opening:

- SG pressure > Max1p.

The actuation order for MSRIV opening is generated when two out of four SG pressure measurements on any one SG exceed the variable Max1p setpoint. This is a loop-specific actuation; only the MSRIV associated with the affected SG is opened. Four different conditions determine the value of Max1p that is used:

- During normal operation, Max1p is maintained at one of two fixed values to provide SG overpressure protection. The higher of the two is used when RCS

pressure and temperature are above the P14 permissive thresholds; the lower is used below the P14 permissive thresholds.

- When an SG isolation signal is generated, Max1p is set to a high fixed value to limit radioactive release to the atmosphere.

- During partial cooldown, Max1p decreases according to a predefined schedule.

- When partial cooldown is finished, Max1p is maintained at a fixed value for all SGs for which an SG isolation signal is not present.

Whenever the Max1p setpoint is exceeded and the MSRIV opens, the MSRCV is modulated by a closed-loop control to maintain SG pressure at the Max1p setpoint. This SAS-performed control uses the difference between measured SG pressure and the Max1p value to determine the control valve position. When the MSRIV is not open, the MSRCV is continuously controlled by the SAS based on reactor power. This is a prepositioning function that allows the MSRCV to be in a reasonable position when the MSRIV receives a protection order to open.

The MSRCV control function provides the MRSCV with a position-correction signal as needed. The actual MSRCV position is compared to the programmed position based on the plant condition. The PI step controller sends a close or open signal, as needed, depending on the actual valve position.

The capability for manual system-level opening of the MSRIV on a per-train basis is provided by the SICS in the MCR. Two manual initiation controls are provided per MSRIV. Either of these two controls opens the desired MSRIV.

The capability for component-level control of the MSRIV actuators is available to the operator via both the PICS and the SICS in the MCR.

The sense-and-command output to open an MSRIV can be reset manually from the SICS in the MCR and the RSS. Reset of the sense-and-command output does not result in closure of the MSRIV; it allows the operator to take further manual action to close the valve.

8.4.2.6 Main Steam Relief Train Isolation

As described above, the MSRIV opens due to high SG pressure conditions, and the MSRCV is prepositioned appropriately based on reactor power. At 100% power, the MSRCV is positioned fully open. A single failure is postulated for a given MSRCV in which it is not properly prepositioned and remains fully open during a decrease in reactor power, such as following a reactor trip. An MSRIV opening after such a single failure could result in the overcooling of the RCS . Therefore, the MSRIV and MSRCV both receive a closing order in the event of a low SG pressure condition.

The US-EPR design uses the following initiating condition to actuate MSRT isolation:

- SG pressure < Min3p.

The actuation order for MSRT isolation is generated when two out of four SG pressure measurements on any one SG are below the Min3p setpoint. This is a train-specific actuation; only the MSRT associated with the affected SG is isolated. The MSRT isolation function is bypassed when RCS pressure is below the P12 permissive setpoint. The bypass is automatically removed when RCS pressure is above the P12 permissive setpoint.

The capability for manual system-level isolation of the MSRT on a per-train basis is provided by the SICS in the MCR. Two manual isolation controls are provided per MSRT. Either of these two controls isolates the desired MSRT.

The capability for component-level control of the MSRT actuators is available to the operator via both the PICS and the SICS in the MCR.

The sense-and-command output to isolate the MSRT can be reset manually from the SICS in the MCR and the RSS. Reset of the sense-and-command output does not result in opening the MSRT; it allows the operator to take further manual action to open the valves.

8.4.2.7 Main Steam Isolation

In the case of a steam or feedwater system piping failure, a depressurization of the affected SG is anticipated. In order to limit the overcooling transient and to limit energy release into the containment, a main steam isolation signal is generated for an SG pressure drop at greater than an allowed rate for a large pipe failure, and also for an SG pressure less than a fixed low setpoint for a small steam line failure. The actions that result from a main steam isolation signal are MSIV closure, MSIV bypass line closure, and SG blowdown line closure.

The US-EPR design uses the following initiating conditions to actuate main steam isolation:

- SG pressure drop,
- SG pressure < Min1p,
- SG isolation signal,
- Containment equipment compartment pressure > Max1p, and
- Containment service compartment narrow-range pressure > Max2p.

An actuation order is generated for main steam isolation when two out of four SG pressure measurements on any one SG decrease faster than the specified allowable rate. When this condition occurs in any one SG, all four main steam trains are isolated. An SG pressure drop is detected by using a variable low setpoint equal to the actual SG pressure minus a fixed value, with a limitation placed on the rate of decrease of the setpoint. The maximum value of the setpoint is also limited in order to avoid MSIV closure during an SG pressure decrease following reactor and turbine trips, which could result in an SG overpressure condition.

There are no permissive conditions associated with main steam isolation due to SG pressure drop; this initiation parameter is active for all plant operating conditions.

An actuation order is also generated for main steam isolation when two out of four SG pressure measurements on any one SG are below the fixed Min1p setpoint. When this condition occurs in any one SG, all four main steam trains are isolated. Main steam isolation due to low SG pressure is bypassed when RCS pressure is below the P12 permissive setpoint. The bypass is automatically removed above the P12 permissive setpoint.

An actuation order is generated for main steam isolation when two out of four PS divisions detect high containment pressure. Either two out of four equipment compartment pressure measurements exceeding the Max1p setpoint, or two out of four service compartment pressure (NR) measurements exceeding the Max2p setpoint results in main steam isolation. There are no operating bypasses associated with main steam isolation on high containment pressure.

The capability for manual system-level actuation of main steam isolation is provided by the SICS in the MCR. This manual initiation isolates all four main steam lines. Four manual system-level initiation controls are provided, any two of which will actuate the main steam isolation.

The capability for component-level control of the main steam and blowdown valves is available to the operator via both the PICS and the SICS in the MCR.

The sense-and-command output for main steam isolation can be reset manually from the SICS in the MCR. Reset of the sense-and-command output does not result in opening the associated valves; it allows the operator to take further manual actions to open the valves.

8.4.2.8 Main Feedwater Isolation

To protect against a loss of SG level control arising from an SGTR, pipe fault, or level control malfunction, and to prevent overcooling of the RCS following a reactor trip, isolation of the main feedwater (MFW) system is performed. The MFW isolation is actuated in two steps, full-load isolation and startup-and-shutdown-system (SSS) isolation, depending upon the severity of the SG level deviation. For a given SG, the SSS isolation includes the closure of the MFW isolation valve, which prevents full-load as well as SSS feedwater flow.

The US-EPR design uses the following initiating conditions to actuate MFW isolation:

- Initiation of reactor trip (full-load isolation),
- SG level NR > Max1p (full-load isolation),
- SG level NR > Max0p for a period of time following reactor trip (SSS isolation),
- SG pressure drop > Max2p (SSS isolation),
- SG pressure < Min2p (SSS isolation),
- SG isolation signal,
- Containment equipment compartment pressure > Max1p (SSS isolation), and
- Containment service compartment pressure NR > Max2p (SSS isolation).

Following a reactor trip, the full-load isolation of MFW to all four SGs is required to avoid RCS overcooling, which could result in a return to critical conditions with a potential power excursion. This MFW isolation secures the full-load flow paths and allows for SG level control by the low-load valves, in the absence of close commands for the low-load valves.

Redundant to the MFW full-load isolation due to reactor trip, a separate, SG-specific MFW full-load isolation order is also generated at the Max1p setpoint to avoid SG overfill and moisture carryover. This actuation order is generated when two out of four NR SG level measurements on any one SG exceed the Max1p setpoint. Only the full-load line feeding the SG with the high water level is isolated due to this signal. The other full-load lines are isolated on the initiation of a reactor trip due to the same high level measurement. The high SG level initiation is bypassed when hot leg temperature is below the P13 permissive setpoint. The bypass is automatically removed when hot leg temperature is above the P13 permissive setpoint.

Following a reactor trip on high SG level, the SG level is expected to decrease initially due to the prompt reduction in steam flow and then to be maintained at a normal level by the SG level control system. A persistent high SG level may be indicative of an SGTR or a failure of the SG level control system. If the SG level remains greater than the Max0p setpoint for a fixed amount of time following reactor trip and MFW full-load isolation, MFW SSS isolation is performed. This actuation order is generated when two out of four NR SG level measurements remain above the Max0p setpoint, following expiration of a time delay initiated by the reactor-trip signal. The SSS isolation is performed only for an SG in which the level remains above the Max0p setpoint. This initiation signal is bypassed when hot leg temperature is below the P13 permissive setpoint. The bypass is automatically removed when hot leg temperature is above the P13 permissive setpoint.

Following a main steam or feedwater system piping failure, a complete feedwater isolation of the MFW train feeding the affected SG is desirable. In this case, MFW full-load isolation occurs on all four steam generators because of the reactor trip on either SG pressure drop or on SG pressure < Min1p. Additionally, an MFW SSS isolation of the affected SG occurs on a more severe SG pressure drop to mitigate fast depressurizations, and on SG pressure < Min2p to mitigate slower depressurizations. The logic to initiate MFW isolation on SG pressure drop is the same as that described for main steam isolation on SG pressure drop, except that the variable low setpoint for SSS isolation is maintained below the reactor-trip and main-steam-isolation setpoint. The actuation order for SSS isolation due to SG pressure < Min2p is generated when two out of four SG pressure measurements on any one SG are below the Min2p setpoint. There is no operating bypass associated with SSS isolation on SG pressure drop. SSS isolation on SG pressure < Min2p is bypassed when RCS pressure is below the P12 permissive setpoint. The bypass is automatically removed when RCS pressure is above the P12 permissive setpoint.

An actuation order is generated for SSS isolation when two out of four PS divisions detect high containment pressure. Either two of four equipment compartment pressure measurements exceeding the Max1p setpoint, or twoof four service compartment pressure NR measurements exceeding the Max2p setpoint results in

SSS isolation. There are no operating bypasses associated with SSS isolation on high containment pressure.

The capability for manual system-level isolation of MFW on a per-train basis is provided by the SICS in the MCR. This manual initiation isolates both full-load and SSS lines to the desired SG. Two manual system-level isolation controls are provided per MFW train. Either of the two controls isolates the MFW train.

The capability for component-level control of the MFW actuators is available to the operator via both the PICS and the SICS in the MCR.

The sense-and-command outputs for MFW isolation can be reset manually from the SICS in the MCR. Reset of the sense-and-command output does not result in opening the associated valves; it allows the operator to take further manual actions to open the valves.

8.4.2.9 Containment Isolation

During a LOCA, radioactive coolant is released into the containment. Therefore, the containment has to be isolated in order to prevent activity release to the environment. The US-EPR provides containment isolation in two stages, based on the size of the break, to isolate nonessential components. Containment pressure measurements and high-range activity monitors are used to initiate containment isolation and to determine which stage is actuated. Additionally, containment isolation is actuated any time a safety injection actuation signal is generated.

The US-EPR design uses the following initiating conditions to isolate the containment:

- Containment equipment compartment pressure > Max1p (stage 1),
- Containment service compartment pressure NR > Max2p (stage 1).
- Containment activity > Max1p (stage 1),
- SIS actuation signal (stage 1), and
- Containment service compartment pressure WR > Max3p (stages 1 and 2).

The stage-one isolation is provided for a small-break loss of coolant accident (SBLOCA) to isolate containment penetrations which have no active function for LOCA mitigation and to start ventilation of the containment annulus. A stage-one containment isolation order is generated when two out of four PS divisions detect high containment pressure. Either two out of four equipment compartment pressure measurements exceeding the Max1p setpoint, two out of four NR service compartment pressure measurements exceeding the Max2p setpoint, or two out of four WR containment service compartment pressure measurements exceeding the Max3p setpoint results in stage-one isolation. If two out of four high-range containment activity sensors indicate high radioactivity in the containment, a stage-one isolation order is also generated. A safety injection actuation signal also results in a stage-one containment isolation actuation.

The stage-two containment isolation order is generated when two out of four WR service compartment pressure measurements exceed the Max3p setpoint. A LOCA

of sufficient size to raise containment pressure to the Max3p setpoint does not require RCPs for mitigation. In fact, on a stage-two containment isolation signal, RCPs are tripped to limit the energy input to the containment, and containment penetrations for processes that support RCP operation are isolated.

There are no operating bypasses associated with containment isolation. This function is available during all plant conditions.

The capability for manual system-level initiation of containment isolation on a per-stage basis is provided by the SICS in the MCR. Four manual isolation controls are provided for each stage. Any two of the four controls actuate the appropriate stage of containment isolation.

The capability for component-level control of the containment isolation actuators is available to the operator via both the PICS and the SICS in the MCR.

The sense-and-command outputs for containment isolation can be reset manually from the SICS in the MCR. Reset of the sense-and-command outputs does not result in changing the state of the containment isolation actuators; it allows the operator to take further manual actions to change the state of individual actuators.

8.4.2.10 Chemical and Volume Control System Charging Isolation

A malfunction of the chemical and volume control system (CVCS) could result in overfilling the pressurizer and opening the pressurizer safety relief valves (PSRVs). Isolation of the CVCS is therefore required when the pressurizer water level increases inadvertently.

This isolation is performed by closure of redundant isolation valves. The following initiating condition is used to perform the CVCS charging isolation:

- Pressurizer level NR > Max2p.

If two out of four level measurements exceed the Max2p setpoint, orders are generated to isolate the CVCS charging flow and auxiliary spray.

The CVCS charging isolation function is bypassed when cold leg temperature is below the P17 permissive setpoint. The bypass is automatically removed above the P17 permissive setpoint.

The capability for manual system-level initiation of CVCS charging isolation on a per-division basis is provided by the SICS in the MCR. One manual system-level isolation control is provided for PS division 1, and one control is provided for PS division 4.

The capability for component-level control of the CVCS actuators for CVCS charging isolation is available to the operator via both the PICS and the SICS in the MCR.

A manual reset of the sense-and-command outputs is not required for the CVCS charging isolation function. The outputs are automatically reset when the level

measurements return below the appropriate setpoint. A pulse order is used to provide assurance that the actions of the execute features go to completion. The automatic reset of the sense-and-command outputs does not result in changing the state of the isolation actuators; it allows the operator to take further manual actions to change the state of individual actuators.

8.4.2.11 CVCS Isolation for Anti-Dilution

To mitigate the risk of dilution of the RCS boron concentration, a CVCS isolation is required to secure potential dilution flow paths. This function provides protection during all plant conditions by using different combinations of input signals depending on the current plant state. The function actuation is divided among plant states as follows:

- Power operation (above the P8 permissive),
- Shutdown conditions with RCPs in operation (below the P8permissive and above the P7 permissive), and
- Shutdown conditions without RCPs in operation (below the P7 permissive).

An online calculation of the boron concentration in the RCS is performed during power operation based on the boron concentration measurement in the CVCS charging line and the measured CVCS charging flow. The calculated boron concentration is compared to a fixed setpoint corresponding to the critical boron concentration of the core at hot zero power with the highest worth rod not inserted.

In shutdown conditions with RCPs in operation, a similar calculation, with the addition of wide-range cold leg temperature measurements, is used. The cold leg temperature is used to determine the mass of reactor coolant and the value to be used for the actuation setpoint. The determination of reactor coolant mass is made according to a lookup table with linear interpolation between eight pairs (cold leg temperature, RCS mass). The setpoint determination is also made based on a lookup table with linear interpolation between eight pairs (cold leg temperature, setpoint value). The selected setpoint represents the critical boron concentration of the current shutdown condition as dictated by cold leg temperature.

In shutdown conditions without RCPs in operation, the measured boron concentration is simply compared to a fixed setpoint. This setpoint represents the boron concentration required under outage conditions, minus a built-in margin to prevent spurious actuations.

Regardless of the current operating conditions, if any two of the four PS divisions determine that dilution is occurring, redundant valves downstream of the volume control tank are closed. This isolates the main CVCS source of dilution. Additionally, the CVCS letdown isolation valve is closed.

The capability for manual system-level initiation of CVCS isolation for anti-dilution on a per-division basis is provided by the SICS in the MCR. One manual isolation control is provided for PS division 1, and one control is provided for PS division 4.

The capability for component-level control of the CVCS actuators for CVCS isolation for anti-dilution is available to the operator from both the PICS and the SICS in the MCR.

The sense-and-command outputs for CVCS isolation for anti-dilution can be reset manually from the SICS in the MCR. Reset of the sense-and-command outputs does not result in changing the state of the isolation valves; it allows the operator to take further manual actions to change the state of individual actuators.

8.4.2.12 Emergency Diesel Generator Actuation

During normal plant operation, the electrical power for the safety-related loads is provided by dedicated offsite emergency auxiliary transformers (EATs) for distribution to the emergency power supply system (EPSS). To mitigate the effects of a loss of offsite power, each division of the EPSS is provided an EDG as a standby source to supply electrical power to the necessary loads.

The EPSS consists of different voltage levels: medium voltage (MV) for large safety-related loads, and low voltage for other loads. Each of the four main MV distribution buses that provide power to the four divisions of the EPSS has a normal connection to one of the two dedicated EATs, but can be alternately supplied from the other dedicated EAT or from the EDG for that division.

The three phases of voltage on each main MV bus are monitored by the PS to detect either a degraded voltage condition or a loss-of-voltage condition. There are two degraded voltage conditions: (1) the voltage measurements for two of the three phases on a bus fall below a fixed setpoint (Min DEGV) for a fixed amount of time and an SIS actuation signal is received, and (2) the voltage measurements for two of the three phases on a bus stay below the same fixed setpoint (Min DEGV) for a longer fixed amount of time without an SIS actuation signal. If the voltage measurements for two of the three phases on a bus fall below a lower fixed setpoint (Min LOV) for a fixed amount of time, a loss-of-voltage condition exists. In these cases, a LOOP signal is generated within the PS, which starts the corresponding EDG and begins the loading sequence. All four EDGs are also started automatically when a safety injection signal is generated, but they are not connected to the EPSS unless a LOOP signal is also generated.

The automatic EDG start and load sequence (for a particular EPSS division) consists of the following:

- That division's MV bus is monitored for proper voltage, and if a degraded voltage condition or loss-of-voltage condition exists, a LOOP signal is generated.
- The EDG is started.
- The EPSS is isolated from the division's preferred sources of power.
- The large loads are removed from the EPSS.
- The EDG is connected to the EPSS.
- The loads are sequenced onto the EPSS.

In general, smaller loads that were energized before the loss of power automatically restart when power from the EDG becomes available. This functionality is provided

by the priority modules associated with each actuator. Large electrical loads are sequenced onto the EPSS according to diesel load steps (DLSs) to maintain EDG output voltage and frequency reductions within acceptable limits. The PS performs the DLS functionality by first maintaining an “off” signal to the actuators, and then removing the signal to a subset of actuators at each load step, which allows them to be restarted. CVCS charging pumps are not restarted automatically regardless of whether they were previously running. Essential service water (ESW) and component cooling water (CCW) pumps are automatically started as part of the load sequence regardless of whether they were previously running.

When a LOOP signal is generated, different DLS sequences are used depending on whether a safety injection signal is also present.

In the absence of a safety injection signal, the CCW and ESW pumps are started as part of the first two load steps. The “off” signal is removed from the safety injection components at their predefined steps, but the safety injection pumps are not started. If a safety injection signal is generated after the LOOP-only loading sequence has begun, the sequence is stopped, the LOCA mitigation loads are started, and then the LOOP-only sequence is re-entered and completed.

If a safety injection signal is present when the LOOP signal is generated, the LOCA mitigation loads are started in the first several steps of the load sequence. The other loads are then sequenced onto the EPSS according to predefined load steps.

The EDG actuation function is implemented in the PS architecture differently than the remainder of the ESF actuation functions. The three phases of voltage measurement for any one electrical division are acquired by the corresponding PS division. The processing and actuation of the related EDG are also carried out completely within the same PS division. For the actuation of any one EDG, redundancy within the PS is obtained by utilizing the functionally independent subsystems within each division. Both subsystems within a division acquire the voltage measurements, and either subsystem can actuate the same EDG. For this function, the two ALUs within each subsystem are combined in a “functional AND” logic. The results of the “functional AND” logic in each subsystem are combined in a “functional OR” logic, so that either subsystem within a division can start the corresponding EDG.

The capability for manual system-level startup of EDGs on a per-EDG basis is provided by the SICS in the MCR. Two manual controls are provided per EDG. Either of the two controls starts the desired EDG.

The capability for component-level control of the EDG is available to the operator from both the PICS and the SICS in the MCR.

The sense-and-command outputs for EDG actuation can be manually reset from the SICS in the MCR. Reset of the sense-and-command outputs does not result in changing the state of the actuators; it allows the operator to take further manual actions to change the state of individual actuators.

8.4.2.13 Pressurizer Relief Valve Opening (Brittle Fracture Protection)

The integrity of the reactor pressure vessel must be protected under all plant conditions. During normal power operation, overpressure protection is provided by three spring-loaded PSRVs. At low coolant temperatures, the cylindrical part of the vessel could fail by brittle fracture before the design pressure of the RCS is reached. In cold operating conditions, low-temperature overpressure protection (LTOP) is provided by opening two of the three PSRVs via redundant electrical solenoid valves.

The US-EPR design uses the following initiating conditions to actuate PSRV opening:

- Hot leg NR pressure > Max1p, and
- Hot leg NR pressure > Max2p.

PSRV opening orders are generated when two out of four NR hot leg pressure measurements are above either setpoint. The setpoints are staggered, with Max1p < Max2p. One PSRV is opened at each setpoint. Each division of the PS actuates one solenoid valve.

To avoid spurious PSRV opening during power operation, this function is automatically bypassed when cold leg temperature is above the P17 permissive setpoint. Operator action is required to remove the bypass when temperature is below the P17 permissive setpoint.

The capability for manual system-level PSRV opening on a per-PSRV basis is provided to the operator by the SICS in the MCR. Two manual initiation controls are provided per PSRV, both of which must be activated to open a PSRV.

The capability for component-level control of the PSRV redundant solenoid valves is available to the operator from both the PICS and the SICS in the MCR.

No manual reset of the PSRV opening sense-and-command output is required. The output is automatically reset when the hot leg pressure measurements return within an acceptable range. Reset of the sense-and-command output results in valve closure.

8.4.2.14 Steam Generator Isolation

In the case of an SGTR, a partial cooldown is initiated to depressurize the RCS to the point where MHSI becomes effective. The SG containing the tube rupture is isolated after the partial cooldown is initiated if a high SG level or high main steam activity level is detected. The isolation prevents the release of contaminated fluid from the affected SG and prevents other water sources from adding to the uncontrolled SG level increase. SG isolation consists of the following main actions:

- MSRT opening setpoint increase,
- MSIV, MSIV bypass, and SG blowdown closure,
- MFW and SSS isolation, and

- EFWS isolation (confirmatory action; the EFWS should already be isolated as described in a previous section).

The US-EPR design uses the following initiating conditions to actuate SG isolation:

- Partial cooldown actuated and SG NR level > Max2p, and
- Partial cooldown actuated and main steam activity > Max1p.

SG isolation orders are generated when two out of four SG NR level measurements on any one SG exceed the Max2p setpoint and partial cooldown has been actuated. The same isolation orders are generated when two out of four main steam activity measurements on any one SG exceed the Max1p setpoint and partial cooldown has been actuated. In both cases, only the affected SG is isolated, and the partial cooldown function is performed via the remaining SGs.

The SG Isolation function is bypassed when hot leg temperature is below the P13 permissive setpoint. However, when the partial cooldown actuation function is bypassed, the SG isolation function is bypassed by its association to the partial cooldown actuation signal.

The capability for manual system-level initiation of SG isolation on a per-SG basis is provided by the SICS in the MCR. Four manual initiation controls are provided per SG, any two of which will isolate the desired SG.

The capability for component-level control of the actuators used in SG isolation is available to the operator from both the PICS and the SICS in the MCR.

Reset of the SG isolation sense-and-command output is available from the SICS in the MCR and the RSS. A reset of the sense-and-command output does not result in changing the state of the isolation actuators; it allows the operator to take further actions to manipulate individual components as may be necessary to follow plant operating procedures.

8.4.2.15 Reactor Coolant Pump Trip

In the case of an SBLOCA, RCPs are tripped when conditions indicate that two-phase flow is present. They are tripped because the RCPs may subsequently be lost due to cavitation or operation in a degraded environment. Forced convection of the two-phase flow increases the mass lost via the break. If the RCPs are permitted to operate for an extended period of time in this condition and then are shut down, an inadequate core cooling condition may occur due to insufficient liquid inventory as the two phases separate. For this reason, an automatic RCP trip is provided early after two-phase flow is indicated, while the void fraction is still relatively low, to enhance long-term accident mitigation and to minimize the potential for RCS mass depletion.

Additionally, the RCPs are tripped on a containment isolation stage-two signal.

The US-EPR design uses the following initiating conditions to actuate an RCP trip:

- ΔP across RCPs < Min1p and SIS actuation signal generated, and
- Stage-two containment isolation signal generated.

The RCP trip based on differential pressure across the RCPs results from one of two ΔP measurements below the Min1p setpoint on any two of the four RCPs. A safety injection signal also must be present in addition to the low ΔP condition for this actuation to occur. This reduces the possibility of a spurious RCP trip.

The parameters that result in an RCP trip due to a stage-two containment isolation are described in a previous section.

When the conditions for RCP trip are satisfied, orders are issued to open the circuit breakers that supply power to the RCPs. When the orders are issued, a time delay begins. When the time delay expires, an order is issued to trip the corresponding bus supply circuit breaker upstream of the RCP circuit breaker to remove power from the RCP.

There are no operating bypasses associated with the RCP trip function.

The capability for manual system-level RCP trip on a per-pump basis is provided to the operator by the SICS in the MCR. Two initiation controls are provided for each pump. Either of the controls trips the desired RCP.

The capability for component-level control for the RCP trip function is available to the operator from both the PICS and the SICS in the MCR.

When an RCP trip has occurred due to low ΔP measurements, concurrent with a safety injection signal, the sense-and-command output can be reset manually, regardless of whether the safety injection signal has been reset. The manual reset is available from the SICS in the MCR. When an RCP trip based on stage-two containment isolation occurs, the RCP trip output is reset when the stage-two containment isolation output is reset.

8.4.2.16 Main Control Room Air Conditioning System Isolation and Filtering

This function is provided to maintain the habitability of the MCR during anticipated operational occurrences (AOOs) and postulated accidents when the MCR and associated rooms become vulnerable to a radioactive environment.

The US-EPR design uses the following initiating conditions to isolate and filter the MCR air conditioning system:

- MCR air intake activity > Max1p, and
- Stage-one containment isolation signal.

High radioactivity is detected by two sensors located in each of two MCR air intake ducts (four sensors total). If any one out of the four sensors detects activity, orders are generated by the PS to isolate both intakes and to reroute the air flow path through iodine filtering units.

The parameters that result in the isolation and filtering of the MCR air conditioning system due to a stage-one containment isolation are described in a previous section.

There are no operating bypasses associated with this function.

The capability for manual system-level initiation of this function is provided by the SICS in the MCR. Two manual initiation controls are provided; either reconfigures both air intake paths.

The capability for component-level control of the actuators for this function is available to the operator from both the PICS and the SICS in the MCR.

Reset of the MCR air intake reconfiguration sense-and-command outputs is available from the SICS in the MCR. A reset of the sense-and-command output does not result in changing the state of the actuators; it allows the operator to take further actions to manipulate individual components as may be necessary to follow plant operating procedures.

8.4.2.17 Turbine Trip on Reactor Trip Initiation

A turbine trip is required following any reactor trip in order to avoid a mismatch between primary and secondary power, which would result in an excessive RCS cooldown with a potential inadvertent return to critical conditions and power excursion.

A short delay is implemented between the reactor trip activation and the turbine trip demand to limit the overpressure effect.

The US-EPR design uses the following initiating condition to actuate the turbine trip:

- Confirmation of reactor trip initiation.

The various conditions that lead to a reactor trip are described in previous sections in this chapter.

Each divisional turbine trip signal from the PS is sent to the TG I&CS via a hardwired, isolated connection. Two-out-of-four logic is performed in each division of the TG I&C on the four PS divisional signals.

The capability for manual system-level initiation of a turbine trip is provided by the SICS in the MCR. Four manual initiation controls are provided; the activation of any two of the four results in a turbine trip.

The capability for component-level control for the turbine trip function is available to the operator from both the PICS and the SICS in the MCR.

Manual reset of the sense-and-command output for turbine trip is available from the SICS in the MCR. A reset of the sense-and-command output does not result in changing the state of the actuators; it allows the operator to take further actions to

manipulate individual components as may be necessary to follow plant operating procedures.

8.4.2.18 Hydrogen Mixing Dampers Opening

This function provides convection and atmospheric mixing in the event of an AOO or postulated accident to enable atmospheric circulation within the whole reactor containment building.

The US-EPR design uses the following initiating conditions to open the hydrogen mixing dampers (HMDs):

- Containment service compartment NR pressure > Max1p, and
- Containment equipment compartment/containment service compartment ΔP > Max1p.

If two out of four containment service compartment NR pressure measurements exceed the Max1p setpoint, then orders are generated by the PS to open the HMDs. Additionally, the HMDs are opened if the differential pressure between the service compartment and the equipment compartment exceeds the Max1p setpoint. This differential pressure is detected by eight differential pressure measurements (two in each division of the PS). If two out of eight equipment compartment/service compartment ΔP measurements exceed the Max1p setpoint, then orders are generated by the PS to open the HMDs.

There are no operating bypasses associated with this function.

The capability for manual system-level initiation of this function is provided from the SICS in the MCR. Four manual system-level initiation controls are provided, any two of which will open the HMDs.

The capability for component-level control for the HMD opening function is available to the operator from both the PICS and the SICS in the MCR.

Reset of the hydrogen mixing dampers opening sense-and-command outputs is available from the SICS in the MCR. A reset of the sense-and-command output does not result in changing the state of the actuators; it allows the operator to take further actions to manipulate individual components as may be necessary to follow plant operating procedures.

8.5 Control Systems

8.5.1 Design Objectives

The general objectives of the nonsafety-related instrumentation and control systems are:

- To make sure the major process variables of the nuclear steam supply system (NSSS) are kept in predefined and allowed ranges during normal power operation.

- To limit the variation of process parameters during normal operation in such a way that the initial conditions for operation are met at the onset of AOOs and postulated accidents as assumed in the safety analyses.

- To minimize the need for protective actions and thus to increase plant availability.

- To provide the reactor operator with monitoring instrumentation that indicates the required input and output control parameters of the systems and to provide the operator with the capability of assuming manual control of the systems.

8.5.2 Control System Descriptions

The following sections describe the US-EPR I&C features associated with the control of nonsafety-related functions.

8.5.2.1 Core Control

The I&C systems that provide core-control functions are the reactor control, surveillance, and limitation system, the process information and control system, and the control rod drive control system. The architecture of the RCSLS, the PICS, and the CRDCS is described in Section 8.2.

The RCSLS receives input signals from the SCDS and implements the automation-level I&C functions related to core control. The SCDS provides the instrumentation interface to the RCSLS. The PICS interfaces with the RCSLS to provide the operator with control and monitoring capability for the core control functions. The architecture of the SCDS is described in Section 8.2.

The CRDCS controls the actuation of the 89 rod cluster control assemblies (RCCA) in the reactor vessel. The RCSLS logic transmits the direction of movement (i.e., withdrawal or insertion), the speed of movement, and drop and hold information to the rod control units of the CRDCS. Each rod control unit generates the cycling sequence input to the corresponding CRDCS coil modules in order to control the rod speed and movement for one RCCA. The coil modules control the amount of current applied to the operating coils (i.e. lift coil, movable gripper coil and stationery gripper coil) of the control rod drive mechanism (CRDM) in order to move the corresponding RCCA. A feedback signal is sent from the rod control unit to the RCSLS. This feedback signal is used by the RCSL to generate a digital position indication of the RCCA and is based on the number of rod movement steps sent from the CRDCS to the operating coils of the CRDM. Figure 8-8 indicates that the RCCA maximum speed withdrawal rate is 75 steps/min. Because each rod movement step equals 0.393 in., the maximum withdrawal rate of an RCCA is 29.48 in./min, which is less than the maximum allowed 30 in./min.

The rod position measurement system uses, for each RCCA, analog rod position measurement coils located within the CRDM to provide an indication of RCCA

position that is separate from the position signal developed by the rod control unit of the CRDCS.

Adjustments to boron concentration levels in the reactor coolant system provide another means of core control. Boron addition and dilution demand signals are generated by RCSLS and are sent to the chemical and volume control system for the average coolant temperature (ACT) control function.

ACT Control Using Rod Motion

The ACT control function is designed to maintain a programmed average RCS average temperature (T_{avg}) by regulating core power. The T_{avg} program is shown in Figure 8-7. The ACT control is the predominant function of core control. The control logic consists of the following four main elements:

- The mismatch between turbine generator load and reactor power (i.e., feed-forward power imbalance),
- The formation of the ACT control setpoint based on power level,
- The difference between the measured average RCS temperature and the desired average temperature (i.e., temperature error), and
- The relationship between the sum of the two error signals and the resulting rod movement actuation requests.

The ACT setpoint serves as an input to determine the temperature error. The setpoint is programmed with power.

The ACT control function consists of two main error signal channels which are summed to provide a total error input signal to the rod speed control program. The rod speed program is shown in Figure 8-8. The rods that are used to perform this function are designated as control bank rods that move into or out of the core in a prescribed manner, referred to as sequence and overlap, that is followed during insertion or withdrawal. The signal output of the rod speed program is a digital pulse that determines both rod stepping speed and direction (i.e., insertion or withdrawal). The two error channels are:

- Average temperature error: Difference between the second-highest (auctioneered) measured loop T_{avg} and the ACT setpoint, and
- Power imbalance feed-forward error: Mismatch between turbine generator load and reactor power.

The power imbalance feed-forward error signal and the temperature error signal are combined additively to produce a total error signal. This total error signal is the output that determines whether the control rods need to be inserted or withdrawn and the speed at which the movement needs to occur. If the total error is negative, rods are withdrawn. If the total error is positive, rods are inserted. The rod speed control program determines the rod movement as a function of total temperature error.

At or near full power operation, the ACT control function uses boron addition and dilution batches as final control elements.

ACT Control Using Boration and Dilution

Rod movements are used to respond to rapid temperature deviations in the RCS or to a rapid generator power increase or decrease. For small, long-lasting temperature deviations that occur due to fuel burnup at or near full power, the ACT control function uses boron addition and dilution batches in order to avoid rod movement. ACT control using boron or dilution batches does not consider the power imbalance feed-forward signal and only corrects an average temperature error that has existed for a predetermined period of time. Boration or dilution batches will occur within the dead bands shown in Figure 8-8. If the total error is negative, a dilution batch will be requested. If the total error is positive, a boron addition batch will be requested. Dilution or boration batches are not permitted by this function when rods are moving and for a time after rods have moved. Dilution or boration batches are not permitted by this function when the axial power distribution is not within predetermined limits. Dilution or boration batches are subordinate to the actions of the AO control function described below.

The transition from the neutron flux control function to the ACT control function occurs at 25% reactor power.

Neutron Flux Control

The neutron flux control function is designed to control reactor power (i.e., neutron flux) during startup and shutdown operations, while the secondary pressure is controlled with the turbine bypass system (TBS). This function simplifies constant power operation and facilitates the operator tasks during the startup of the turbine and the synchronization of the generator with the grid.

In the neutron flux control mode, the control bank movements operate in the same way as under ACT control (i.e., with sequence and overlap). The neutron flux control acts on the rod control banks in the same way as the ACT control function. The neutron flux deviation is appropriately amplified to give an output signal corresponding to that from the ACT control. The neutron flux control setpoint can be adjusted manually by the operator using the PICS.

When the reactor is at hot shutdown with all the banks inserted, the operator begins the first stage of the startup by withdrawing the shutdown and control banks. The withdrawal sequence requires that the shutdown banks are withdrawn to their all-rods-out (ARO) position before control banks are withdrawn.

During startup (i.e., after exceeding the low reactor power permissive P5) and shutdown operation, the reactor power (i.e., neutron flux) can be controlled in conjunction with the main steam (MS) pressure control using the turbine bypass valves. The neutron flux control function blocks turbine synchronization at power levels less than a setpoint on increasing reactor power, and blocks power reductions below a setpoint until the turbine is tripped on decreasing reactor power.

Axial Offset Control

The AO control function is designed to maintain core axial power within analyzed limits. AO is a measure of the axial power distribution in the core. Extreme shifts in power distributions have an adverse impact on accident analysis results.

The AO control strategy works in conjunction with ACT control to restore the AO to within prescribed limits.

Above a predetermined power level, the AO control can be activated. If the AO exceeds a power-dependent positive value, a dilution batch is requested. This effectively raises the core-wide power and average coolant temperature, which causes the ACT control to insert rods, thereby correcting the AO. If the AO exceeds a power-dependent negative value, a boration batch is requested. This effectively lowers the core-wide power and average coolant temperature, which causes the ACT control to withdraw rods and correct the AO.

Partial Trips

Each of the following conditions causes a partial trip (the dropping of a subset of the control rods into the core):

- Loss of one RCP,
- Loss of one MFW pump,
- Load rejection or turbine trip,
- High linear power density, and
- Low DNBR.

8.5.2.2 Plant Control

RCS Pressure Control

The RCS pressure control maintains the RCS pressure within allowable limits in Modes 1 through 5. When in the automatic control mode, the RCS pressure control maintains the primary pressure at a setpoint value in steady-state operation and within an allowable range around its setpoint (i.e., control band) during transients, including startup and cooldown operations. Figure 8-9 indicates the control band relative to other RCS pressure setpoints.

When the automatic heatup and cooldown mode is selected, the RCS pressure control has an automatically generated temperature-dependent setpoint. The automatic heatup and cooldown mode is selected during operation in Modes 2 and 3. The primary pressure is required to stay in an allowable range around the automatically generated setpoint. If the pressure drifts from the limits of the setpoint, the Max2 sliding pressure limitation function is actuated. If the pressure progresses further from the temperature-dependent setpoint to the high pressure (HP) or low pressure (LP) locking setpoints, the automatic heatup and cooldown is interrupted, and an alarm is sent to the PICS.

RCS pressure control is performed by actuating pressurizer (PZR) heaters or PZR normal spray.

The manual control mode allows manual setpoint control and manual control of the actuators.

Pressurizer Level Control

The PZR level control provides:

- Sufficient RCS water inventory for cooling and for proper control of RCS pressure.

- A sufficient steam volume in the PZR to accommodate an insurge into the PZR from the RCS without causing an excessive pressure increase for normal operating transients. There is also sufficient water mass to accommodate an outsurge from the PZR to the RCS without causing an excessive pressure decrease.

The function of the PZR level control is to maintain the PZR level at a setpoint value in steady-state operation and within an allowable range around its setpoint during normal operational situations, including startup and cooldown. When in the automatic control mode, the PZR level control channel makes sure that the PZR level remains within given limits (i.e., control band) around the setpoint. Figure 8-10 indicates the control band relative to other PZR level setpoints.

The PZR level control monitors the PZR level for deviations from its setpoint during operation in Modes 1 through 4, and based on mode changes, actuates different control valves at the pressure-reducing stations located in the CVCS letdown lines.

The manual control mode allows manual setpoint control and manual control of the pressure-reducing valve actuators.

Steam Generator Level Control

The steam generator water level control automatically maintains SG level by matching feedwater flow to steam demand. The level can also be controlled manually.

This SG level control I&C function provides the following:

- Sufficient water level for heat removal from the primary to secondary side, and
- Minimization of moisture carryover to the turbine.

The SG level control I&C function maintains the SG level at a setpoint value in steady-state operation during heatup and cooldown (Modes 1 through 4), and within allowable limits (the control band) during normal operational transients. Figure 8-11 illustrates the control band relative to other SG level setpoints.

This function acts on the following valves in the main feedwater system (MFWS) to control SG water level in a particular SG:

- Full load control valve,
- Low load control valve, and
- Very low load control valve.

Main Steam Pressure Control

The purpose of the MS pressure control function is to provide MS overpressure control and limitation in case of load reduction due to load steps, load ramps, or load rejection. MS pressure is controlled by automatically modulating the turbine bypass valves.

During normal power operation, this function is realized by maintaining a floating MS pressure setpoint above the measured MS pressure. As the measured pressure changes, the setpoint changes accordingly. However, a limitation is placed on the rate of change of the setpoint so that if the measured pressure increases at a rate greater than the limitation of the floating setpoint, the turbine bypass valves are opened. The turbine bypass valves close and are prevented from opening on high condenser backpressure or high hotwell level.

During plant heatup and cooldown operations, the operator can adjust a target pressure setpoint which is adapted with a limited temperature gradient. Based on the target pressure setpoint, the turbine bypass valves control MS pressure and thus reactor coolant temperature. Locking logic is provided to interrupt the automatic heatup or cooldown process when RCS parameters deviate from their setpoint thresholds.

When a partial cooldown is initiated, the MS pressure follows a specific partial cooldown setpoint, which has priority over all other setpoints and locking signals.

Following a reactor trip, in order to avoid primary overcooling, the MS pressure setpoint is immediately set to a fixed maximum pressure setpoint.

8.6 Diverse I&C Systems

The safety instrumentation and control systems that execute automatic reactor trip and engineered safety feature actuation and control functions for accident mitigation are described in sections 8.3 and 8.4. These systems are designed to perform the required safety functions in the event of a single random failure. The DCS design can also withstand software common-cause failure (SWCCF) that prevents the PS from performing its functions. The design has sufficient diversity and defense in depth to tolerate an AOO or postulated accident concurrent with an SWCCF of the PS.

This section describes the I&C systems and functional requirements credited for mitigating these events.

8.6.1 Systems Providing Diverse Performance of Safety Functions

Safety Information and Control System: The SICS provides the ability to manually trip the reactor and to initiate system-level safety functions via the DAS with equipment that is not affected by a software CCF of the safety-related I&C systems.

Diverse Actuation System: The DAS executes manual functions initiated from the SICS and automatic functions to mitigate an ATWS or SWCCF of the PS. The DAS is diverse from the PS.

The DAS executes the automatic reactor trip, ESF actuation, and alarm and display functions listed below. Sensor information is acquired by the DAS from the SCDS via hardwired signals that are not affected by a software CCF. The DAS also processes certain manual system-level actuations of critical safety functions, as described below.

For reactor trip functions, outputs from the DAS are sent to the shunt trip coils of the trip breakers, which are a diverse means of opening the breakers from the undervoltage coils affected by the PS. Outputs are also sent to the rod control units of the CRDCS to interrupt power to the CRDM coils; this constitutes a diverse means of dropping the control rods from the reactor trip contactors which are de-energized by the PS. The DAS outputs are energized to actuate. This design is diverse from the PS outputs, which are de-energized to actuate.

For ESF actuations, outputs from the DAS are sent directly to the PACS. This path is not affected by a software CCF of the PS. Outputs for turbine trips are sent directly to the turbine-generator I&C system via hardwired connections (one per division). The TG I&CS performs two-out-of-four voting logic on the turbine trip signals.

The following features are implemented so that the automatic DAS functions do not interfere with PS actuations under normal circumstances and so that the PS is given the opportunity to actuate before the DAS:

- DAS setpoints are selected to provide reasonable assurance that they will be reached after corresponding PS setpoints are reached.

- Voting logic within the DAS is such that single failures do not result in spurious actuations of the automatic DAS functions.

- Priority logic within the PACS dictates that in the case of conflicting orders between the PS and the DAS, the PS orders have a higher priority (the priority rules are described in section 8.2).

The DAS functions are designed so that once initiated, they proceed to completion.

Alarms and indications are processed by the DAS and sent to the PICS (via the PAS) and SICS for display. The DAS provides accurate status information to the operator in the main control room on the PICS (via the PAS) and on the SICS. This

includes system operational status (i.e., bypass, initiate, standby, normal), power availability, and any system faults or messages pertinent to plant operation.

Priority and Actuator Control System: The PACS supports the execution of automatic and manual functions required to mitigate an ATWS and a software CCF of the PS. The PACS is diverse in operation from the PS. The PACS is not part of the actuation path for the reactor trip function.

The PACS receives actuation orders from the various I&C systems and sends the order of highest priority to the plant actuators. The priority modules in the PACS are not subject to SWCCF by virtue of 100 percent combinatorial, proof-of-design testing.

Signal Conditioning and Distribution System: The SCDS provides conditioned signals from sensors and black boxes to multiple DCS systems for further processing. The outputs of the SCDS are hardwired, are sent independently to each system, and are not affected by a SWCCF of the PS.

The SCDS is also connected directly to the SICS via hardwire for the display of certain sensor information. The display of this information is not affected by a SWCCF of the PS.

8.6.2 Functional Descriptions

8.6.2.1 Automatic DAS Functions

The following automatic DAS functions are provided to mitigate an AOO or postulated accident concurrent with a CCF of the PS:

- Reactor trip on low SG pressure,
- Reactor trip on low SG level,
- Reactor trip on high SG level,
- Reactor trip on low RCS flow (two loops),
- Reactor trip on low-low RCS flow (one loop),
- Reactor trip on high neutron flux (power range),
- Reactor trip on low hot leg pressure,
- Reactor trip on high pressurizer pressure,
- Turbine trip on reactor trip,
- EFWS actuation on low SG level,
- SIS actuation on low pressurizer pressure,
- Main steam isolation on low SG pressure,
- Containment isolation on high activity,
- MFW isolation on low SG pressure,
- MFW isolation on high SG level,
- Opening of containment hydrogen mixing dampers on high containment pressure or high containment compartments differential pressure, and
- Starting of SBODGs.

8.6.2.2 DAS Permissives

Permissive signals are used to enable, disable, or modify the operation of DAS reactor trip and ESF actuation functions based on plant conditions. The state of a permissive signal is defined either as validated or inhibited. There are two Permissives, D2 and D3, which are implemented in the DAS.

D2 Permissive

The D2 permissive is intended, during normal operation, to allow the plant to reach a shutdown state without inadvertent DAS function actuation. The D2 permissive is provided with the same excore power measurements as the PS P2 permissive. The D2 permissive is validated when the indicated power is higher than its setpoint of 10% nominal power. The validation of the D2 permissive follows the same two-out-of-four logic as the P2 permissive.

The D2 permissive is automatically validated when the power increases above 10% and can be manually inhibited when the power is below the setpoint. The validation of the D2 permissive automatically enables all of the DAS functions except the reactor trip on low-low RCS flow (one loop). The inhibition of the D2 permissive automatically disables all of the DAS functions with the same exception.

D3 Permissive

The D3 permissive is intended to prevent a full reactor trip actuation following a partial reactor trip due to the loss of one RCP. The D3 permissive is provided with the same excore power measurements as the PS P3 permissive. The D3 permissive is automatically validated when the indicated power is higher than its setpoint of 70% nominal power. The validation of the D3 permissive follows the same two-out-of-four logic as the P3 permissive.

The D3 permissive is automatically validated when the power increases above 70% and automatically inhibited when the power decreases below 70%. The validation of the D3 permissive automatically enables the reactor trip on low-low RCS flow (one loop). The inhibition of the D3 permissive automatically disables that trip.

8.6.2.3 Manual Functions

The following manual functions are provided to mitigate an AOO or postulated accident concurrent with a SWCCF of the PS. The allocation of the function within the DCS design is provided.

- Manual reactor trip (SICS/DAS/PACS),
- Manual EDG start (SICS/PACS),
- Manual control of components to support diesel generator loading (emergency diesel generators or SBOs) (SICS/PACS)
- Manual EFW actuation (SICS/DAS/PACS)
- Manual operation of EFW for long-term SG level control (SICS/PACS),
- Manual safety injection switchover to hot leg injection (SICS/PACS),
- Manual MSIV closure (SICS/PACS),

- Manual feedwater isolation (MFW and EFW) (SICS/PACS),
- Manual initiation of medium head safety injection (MHSI) (SICS/DAS/PACS),
- Manual control of MHSI (SICS/PACS),
- Manually extension of partial cooldown (SICS/PACS),
- Manual depressurization of the RCS with pressurizer sprays (SICS/PACS),
- Manual actuation of the extra borating system (SICS/PACS),
- Manual control room HVAC reconfiguration (SICS/PACS),
- Manual CVCS isolation (SICS/PACS),
- Manual MSRT control (SICS/PACS),
- Manual stage 1 containment isolation (SICS/DAS/PACS), and
- Manual opening of containment hydrogen mixing dampers (SICS/DAS/PACS).

8.6.2.4 Indications and Alarms

The following indications and alarms are processed by the SCDS and provided to the operator on the PICS and SICS:

Post-Accident Monitoring Variables: The operator is provided with indications to monitor the plant following an actuation by the DAS. The SICS acquires type A, B, and C post-accident monitoring variables from the SCDS. The SCDS processes the information and sends it to the SICS for display to the operator.

Indication and Alarm of DAS Status: When an automatic reactor trip or ESF actuation is performed by the DAS, alarms are generated and sent to the PICS (via the PAS) and the SICS to alert the operator.

Table 8-1 Distributed Control System Functional Requirements Matrix

Functional Requirements	DCS System								
	SICS	PICS	DAS	PS	SAS	RCSLS	PAS	SCDS	PACS
Process Control Functions									
Non-reactivity related		X					X	X	X
Reactivity related (with rods)		X				X		X	
Reactivity related (without rods)[1]		X				X	X	X	X
Process Limitation Functions									
Non-reactivity related		X					X	X	X
Reactivity related (with rods)		X				X		X	
Reactivity related (without rods)[1]		X				X	X	X	X
Reactor Trip	X			X				X	
ESF Actuation	X			X				X	X
Safety Control-									
Automatic[2]	X				X			X	X
Manual grouped control[3]	X	X			X		X		X
Manual component control[4]	X	X					X		X
Safety Interlocks[5,6]	X			X	X			X	X
Severe Accident Controls[7]	X	X					X		X
Diverse Reactor Trip	X		X					X	
Diverse ESF Actuation	X		X					X	X
Process Indications[8]		X					X	X	X
PAM Indications									
PAM type A[9]	X	X					X	X	X
PAM type B[9]	X	X					X	X	X
PAM type C[9]	X	X					X	X	X
PAM type D		X					X		
PAM type E		X					X		
Severe Accident Indications[10]	X	X					X	X	X
Alarms[11]	X	X	X	X	X	X	X	X	

Notes:

1. Process control and limitation functions that are reactivity related and command actuators other than control rods (e.g., reactor boron water makeup) are allocated to the RCSLS and PAS. The RCSLS performs the bulk of the logic, and then sends the specific actuator command (i.e., open/close) to the PAS. This provides a common actuator interface from the PICS.

2. Safety automatic control functions are allocated to the SICS if an operator interface is needed for the function (e.g., auto/manual transfer).

3. Safety-related manual grouped controls are allocated to two different paths, which are: (a) SICS >> SAS >> PACS (credited path), (b) PICS >> PAS >> PACS (duplicated path provided so that the operator can perform these functions from the PICS).

4. Safety-related manual component controls are allocated to two different paths, which are: (a) SICS >> PACS (credited path), (b) PICS >> PAS >> PACS (duplicated path provided so that the operator can perform these functions from the PICS).

5. Safety interlock functions are allocated to the SICS if an operator interface is needed for the function (e.g., validating a permissive to enable an interlock).

6. The interlock is allocated to the PS if it relies on a permissive that resides in the PS (e.g., P14 permissive for RHR interlock). Otherwise, the interlock is allocated to the SAS. This minimizes wiring between the PS and SAS.

7. Severe accident controls are allocated to two different paths, which are: (a)SICS >> PACS (credited path), (b) PICS >> PAS >> PACS (duplicated path provided so that the operator can perform these functions from the PICS).

8. Process indications are routed as follows: (a) PAS >> PICS (path used if the signal is needed only in the PAS), (b) SCDS or PACS (for actuator feedback) >> PAS >> PICS >> (path used if the signal is needed in multiple DCS systems).

9. PAM Type A-C indications are allocated to two different paths, which are: (a) SCDS or PACS (for actuator feedback) >> SICS (credited path), (b) SCDS or PACS (for actuator feedback) >> PAS >> PICS (duplicated path provided so that the operator can monitor these parameters from the PICS).

10. Severe accident indications are allocated to two different paths, which are: (a) SCDS or PACS (for actuator feedback) >> SICS (credited path), (b) SCDS or PACS (for actuator feedback) >> PAS >> PICS (duplicated path provided so that the operator can monitor these parameters from the PICS).

11. Alarms provided in the PICS are generated in the PS, SAS, RCSLS, DAS (sent to the PAS via a hardwired link), or PAS. A limited number of alarms are provided in the SICS are generated in the DAS, PS, or SAS.

Table 8-2 Reactor Trip Variables

Protective Function	Variable to be Monitored	Range of Variable
High Linear Power Density	Neutron Flux-Self Powered Neutron Detectors	0–590 W/cm
Low DNBR	Neutron Flux-Self Powered Neutron Detectors	0–590 W/cm
	Cold Leg Temperature (NR)	500°F–626°F
	RCP Speed	800 -1600 rpm
	RCS Loop Flow	0-120% NF
	RCCA position	0–100% Insertion
	Pressurizer Pressure (NR)	1615-2515 psia
High Neutron Flux Rate of Change	Neutron Flux-Power Range Detectors	0.5–200% NP
High Core Power Level	Cold Leg Temperature (WR)	32°F - 662°F
	Hot Leg Pressure (WR)	15–3015 psia
	Hot Leg Temperature (NR)	536°F -662°F
	RCS Loop Flow	0-120% NF
Low Reactor Coolant Pump Speed	RCP Speed	800 -1600 rpm
Low RCS Flow Rate (two loops)	RCS Loop Flow	0–120% NF
Low-Low RCS Flow Rate (one loop)	RCS Loop Flow	0–120% NF
Low Doubling Time	Neutron Flux-Intermediate Range Detectors	5 x 10E-6–60% NP
High Neutron Flux	Neutron Flux-Intermediate Range Detectors	5 x 10E-6–60% NP
Low Pressurizer Pressure	Pressurizer Pressure (NR)	1615–2515 psia
High Pressurizer Pressure	Pressurizer Pressure (NR)	1615–2515 psia
High Pressurizer Level	Pressurizer Level (NR)	0-100% MR
Low Hot Leg Pressure	Hot Leg Pressure (WR)	15–3015 psia
Steam Generator Pressure Drop	SG Pressure	15–1615 psia
Low Steam Generator Pressure	SG Pressure	15–1615 psia
High Steam Generator Pressure	SG Pressure	15–1615 psia
Low Steam Generator Level	SG Level (NR)	0-100% MR
High Steam Generator Level	SG Level (NR)	0-100% MR
High Containment Pressure	Containment Service Compartment Pressure (NR)	-3 psig to +7 psig
	Containment Equipment Compartment Pressure	-3 psig to +7 psig
Low Saturation Margin	Cold Leg Temperature (WR)	32°F - 662°F
	Hot Leg Pressure (WR)	15–3015 psia
	Hot Leg Temperature (NR)	536°F–662°F
	RCS Loop Flow	0-120% NF

Notes: NP = nuclear power, NF = nominal flow, MR = measuring range

Table 8-3 (page 1 of 2)
Reactor Trip Functions

----------REVIEWER'S NOTE----------
[Reviewers Note: The values specified in brackets in the Limiting Trip Setpoint column are included for reviewer information only. A plant-specific setpoint study will be conducted. The values in Limiting Trip Setpoint column will then be replaced after the completion of this study.]

TRIP / ACTUATION FUNCTION / PERMISSIVE	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	MINIMUM REQUIRED FOR FUNCTIONAL CAPABILITY[a]	LIMITING TRIP SETPOINT / DESIGN LIMIT	CONDITION
A. REACTOR TRIP				
1.a. Low Departure from Nucleate Boiling Ratio (DNBR)	1[d]	3 divisions	[(e) [b)(c)]]	H
1.b. Low DNBR and (Imbalance or Rod Drop (1/4))	1[d]	3 divisions	[(e)[b)(c)]]	H
1.c. Low DNBR and Rod Drop (2/4)	1[d]	3 divisions	[(e)[b)(c)]]	H
1.d. Low DNBR - High Quality	1[d]	3 divisions	[(e)[b)(c)]]	H
1.e. Low DNBR - High Quality and (Imbalance or Rod Drop (1/4))	1[d]	3 divisions	[(e)[b)(c)]]	H
2. High Linear Power Density	1[d]	3 divisions	[(e)[b)(c)]]	H
3. High Neutron Flux Rate of Change (Power Range)	1,2,3[f]	3 divisions	[11% RTP[b)(c)]]	K
4. High Core Power Level	1,2[g]	3 divisions	[105% RTP[b)(c)]]	J
5. Low Saturation Margin	1,2[g]	3 divisions	[30 Btu/lb[b)(c)]]	J
6.a. Low-Low Reactor Coolant System (RCS) Loop Flow Rate in One Loop	1[h]	3 divisions	[54% Nominal Flow[b)(c)]]	G

(a) A division is OPERABLE provided: a) the minimum sensors required for functional capability for all sensors providing input to the Trip/Actuation Function/Permissive are OPERABLE; and b) the associated signal processors are OPERABLE.

(b) If the as-found setpoint is outside its predefined as-found tolerance, then the Trip/Actuation Function shall be evaluated to verify that it is functioning as required before returning the Trip/Actuation Function to service.

(c) The setpoint shall be reset to a value that is within the as-left tolerance around the Nominal Trip Setpoint (NTSP) at the completion of the surveillance; otherwise, the division shall be declared inoperable. Setpoints more conservative than the LTSP are acceptable provided that the as-found and as-left tolerances apply to the actual setpoint implemented in the Surveillance procedures to confirm Trip/Actuation Function performance. The methodologies used to determine the as-found and the as-left tolerances are specified in a document controlled under 10 CFR 50.59.

(d) With Permissive P2 validated.

(e) As specified in the COLR.

(f) With the RCSL System capable of withdrawing a RCCA or one or more RCCAs not fully inserted.

(g) With Permissive P5 validated.

(h) With Permissive P3 validated.

Table 8-3 (page 2 of 2)
Reactor Trip Functions

	TRIP / ACTUATION FUNCTION / PERMISSIVE	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	MINIMUM REQUIRED FOR FUNCTIONAL CAPABILITY[a]	LIMITING TRIP SETPOINT / DESIGN LIMIT	CONDITION
6.b.	Low RCS Loop Flow Rate in Two Loops	1[d]	3 divisions	[90% Nominal Flow[b][c]]	H
7.	Low Reactor Coolant Pump (RCP) Speed	1[d]	3 divisions	[93% Nominal Speed[b][c]]	H
8.	High Neutron Flux (Intermediate Range)	1[i],2,3[f]	3 divisions	[25% RTP[b][c]]	K
9.	Low Doubling Time (Intermediate Range)	1[i],2,3[f]	3 divisions	[20 Sec.[b][c]]	K
10.	Low Pressurizer Pressure	1[d]	3 divisions	[2005 psia[b][c]]	H
11.	High Pressurizer Pressure	1,2	3 divisions	[2415 psia[b][c]]	J
12.	High Pressurizer Level	1,2	3 divisions	[75% Measuring Range[b][c]]	J
13.	Low Hot Leg Pressure	1,2,3[f][j]	3 divisions	[2005 psia[b][c]]	L
14.	Steam Generator (SG) Pressure Drop	1,2,3[f]	3 divisions	[29 psi/min; 102 psi<steady state; Max 1088 psia[b][c]]	K
15.	Low SG Pressure	1,2,3[f][j]	3 divisions	[725 psia[b][c]]	L
16.	High SG Pressure	1	3 divisions	[1385 psia[b][c]]	I
17.	Low SG Level	1,2	3 divisions	[20% Narrow Range[b][c]]	J
18.	High SG Level	1,2	3 divisions	[69% Narrow Range[b][c]]	J
19.	High Containment Pressure	1,2,3,4	3 divisions	[18.7 psia[b][c]]	K

(a) A division is OPERABLE provided: a) the minimum sensors required for functional capability for all sensors providing input to the Trip/Actuation Function/Permissive are OPERABLE; and b) the associated signal processors are OPERABLE.

(b) If the as-found setpoint is outside its predefined as-found tolerance, then the Trip/Actuation Function shall be evaluated to verify that it is functioning as required before returning the Trip/Actuation Function to service.

(c) The setpoint shall be reset to a value that is within the as-left tolerance around the Nominal Trip Setpoint (NTSP) at the completion of the surveillance; otherwise, the division shall be declared inoperable. Setpoints more conservative than the LTSP are acceptable provided that the as-found and as-left tolerances apply to the actual setpoint implemented in the Surveillance procedures to confirm Trip/Actuation Function performance. The methodologies used to determine the as-found and the as-left tolerances are specified in a document controlled under 10 CFR 50.59.

(d) With Permissive P2 validated.

(f) With the RCSL System capable of withdrawing a RCCA or one or more RCCAs not fully inserted.

(i) Less than or equal to 10% RTP.

(j) With Permissive P12 inhibited.

Table 8-4 ESF Actuation Variables (sheet 1 of 2)

Protective Function	Variable To Be Monitored	Range of Variable
Safety Injection System Actuation	Pressurizer Pressure (NR)	1615-2515 psia
	Hot Leg Pressure (WR)	15-3015 psia
	Hot Leg Temperature (WR)	32-662°F
	Hot Leg Loop Level	0-30.71 in.
Reactor Coolant Pump Trip	RCP differential pressure	0-120% nominal
Emergency Feedwater System Actuation	SG Level (WR)	0-100% MR
Emergency Feedwater System Isolation	SG Level (WR)	0-100% MR
SG Isolation	Main Steam Line Activity	1x10-1 – 1x104 counts/ sec.
	SG Level (NR)	0-100% MR
Main Steam Relief Isolation Valve Opening	SG Pressure	15-1615 psia
Main Steam Relief Train Isolation	SG Pressure	15-1615 psia
Main Steam Isolation	SG Pressure	15-1615 psia
	Cont. Equipment Compartment Pressure	-3 to +7 psig
	Cont. Service Compartment Pressure (NR)	-3 to +7 psig
Main Feedwater Isolation	SG Level (NR)	0-100% MR
	SG Pressure	15-1615 psia
	Cont. Equipment Compartment Pressure	-3 to +7 psig
	Cont. Service Compartment Pressure (NR)	-3 to +7 psig
Containment Isolation	Cont. Service Compartment Pressure (NR)	-3 to +7 psig
	Cont. Service Compartment Pressure (WR)	-5 to +220 psig
	Cont. Equipment Compartment Pressure	-3 to +7 psig
	Containment High Range Activity	1x10-1 – 1x107 Rad/hr
Emergency Diesel Generator Actuation	6.9 kV Bus Voltage	0-8.625 kV
PSRV Opening	Hot Leg Pressure (NR)	0-870 psia
CVCS Charging Isolation	Pressurizer Level (NR)	0-100% MR

Table 8-4 ESF Actuation Variables (sheet 2 of 2)

Protective Function	Variable To Be Monitored	Range of Variable
CVCS Isolation for Anti-Dilution	Boron Concentration	0-5000 ppm
	Boron Temperature	32-212°F
	CVCS Charging Flow	0-320,000 lb/hr
	Cold Leg Temperature (WR)	32-662°F
MCR Air Conditioning System Isolation and Filtering	MCR Air Intake Duct Activity	$1x10^{-5}$ – $1x10^{1}$ Rad/hr
Turbine Trip	RT Breaker Position	Open/Closed
Hydrogen Mixing Dampers Opening	Cont. Service Compartment Pressure (NR)	-3 to +7 psig
	Cont. Equipment Compartment and Cont. Service Compartment Differential Pressure	-7.25 to +7.25 psi

Table 8-5 (page 1 of 5)
ESF Actuation Functions

	TRIP / ACTUATION FUNCTION / PERMISSIVE	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	MINIMUM REQUIRED FOR FUNCTIONAL CAPABILITY[a]	LIMITING TRIP SETPOINT / DESIGN LIMIT	CONDITION
B.	ENGINEERED SAFETY FEATURES ACTUATION SYSTEM (ESFAS) SIGNALS				
1.	Turbine Trip on Reactor Trip (RT)	1	3 divisions	[Reactor Trip for 1 sec.]	I
2.a.	Main Feedwater Full Load Isolation on Reactor Trip (All SGs)	1,2[k],3[k]	3 divisions	NA	M
2.b.	Main Feedwater Full Load Isolation on High SG Level (Affected SGs)	1,2[k],3[k]	3 divisions	[69% Narrow Range[b][c]]	M
2.c.	Startup and Shutdown Feedwater Isolation on SG Pressure Drop (Affected SGs)	1,2[l],3[l]	3 divisions	[29 psi/min; 247 psi<steady state; Max 943 psia[b][c]]	M
2.d.	Startup and Shutdown Feedwater Isolation on Low SG Pressure (Affected SGs)	1,2[l],3[j][l]	3 divisions	[580 psia[b][c]]	L
2.e.	Startup and Shutdown Feedwater Isolation on High SG Level for Period of Time (Affected SGs)	1,2[l],3[l]	3 divisions	[65% Narrow Range for 10 sec.[b][c]]	M
3.a.	SIS Actuation on Low Pressurizer Pressure	1,2,3[j]	3 divisions	[1668 psia[b][c]]	L
3.b.	SIS Actuation on Low Delta P_{sat}	3[m],4[n]	3 divisions	[220 psi[b][c]]	O

(a) A division is OPERABLE provided: a) the minimum sensors required for functional capability for all sensors providing input to the Trip/Actuation Function/Permissive are OPERABLE; and b) the associated signal processors are OPERABLE.

(b) If the as-found setpoint is outside its predefined as-found tolerance, then the Trip/Actuation Function shall be evaluated to verify that it is functioning as required before returning the Trip/Actuation Function to service.

(c) The setpoint shall be reset to a value that is within the as-left tolerance around the Nominal Trip Setpoint (NTSP) at the completion of the surveillance; otherwise, the division shall be declared inoperable. Setpoints more conservative than the LTSP are acceptable provided that the as-found and as-left tolerances apply to the actual setpoint implemented in the Surveillance procedures to confirm Trip/Actuation Function performance. The methodologies used to determine the as-found and the as-left tolerances are specified in a document controlled under 10 CFR 50.59.

(j) With Permissive P12 inhibited.

(k) Except when all MFW full load lines are isolated.

(l) Except when all MFW full load and low load lines are isolated.

(m) With Permissive P12 validated.

(n) With Permissive P15 inhibited.

Table 8-5 (page 2 of 5)
ESF Actuation Functions

	TRIP / ACTUATION FUNCTION / PERMISSIVE	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	MINIMUM REQUIRED FOR FUNCTIONAL CAPABILITY[a]	LIMITING TRIP SETPOINT / DESIGN LIMIT	CONDITION
3.c	SIS Actuation on Low RCS Loop Level	4[o]	3 divisions	[18.9 in.[b][c]]	O
		5,6	2 divisions		R
4.	RCP Trip on Low Delta Pressure across RCP with SIS Actuation	1,2,3,4	3 divisions	[80% Nominal Pressure[b][c]]	N
5.	Partial Cooldown Actuation on SIS Actuation	1,2,3	3 divisions	NA	M
6.a.	Emergency Feedwater System (EFWS) Actuation on Low-Low SG Level (Affected SGs)	1,2,3	3 divisions	[40% Wide Range[b][c]]	M
6.b.	EFWS Actuation on Loss of Offsite Power (LOOP) and SIS Actuation (All SGs)	1,2	3 divisions	NA	J
7.a.	Main Steam Relief Train (MSRT) Actuation on High SG Pressure (Affected SG)	1,2,3,4[p]	3 divisions	[1385 psia[b][c]]	N
7.b.	MSRT Isolation on Low SG Pressure (Affected SG)	1,2,3[j]	3 divisions	[580 psia[b][c]]	L
8.a.	Main Steam Isolation Valve (MSIV) Isolation on SG Pressure Drop (All SGs)	1,2,3[q]	3 divisions	[29 psi/min; 102 psi<steady state; Max 1088 psia[b][c]]	M
8.b.	MSIV Isolation on Low SG Pressure (All SGs)	1,2,3[j][q]	3 divisions	[725 psia[b][c]]	L

(a) A division is OPERABLE provided: a) the minimum sensors required for functional capability for all sensors providing input to the Trip/Actuation Function/Permissive are OPERABLE; and b) the associated signal processors are OPERABLE.

(b) If the as-found setpoint is outside its predefined as-found tolerance, then the Trip/Actuation Function shall be evaluated to verify that it is functioning as required before returning the Trip/Actuation Function to service.

(c) The setpoint shall be reset to a value that is within the as-left tolerance around the Nominal Trip Setpoint (NTSP) at the completion of the surveillance; otherwise, the division shall be declared inoperable. Setpoints more conservative than the LTSP are acceptable provided that the as-found and as-left tolerances apply to the actual setpoint implemented in the Surveillance procedures to confirm Trip/Actuation Function performance. The methodologies used to determine the as-found and the as-left tolerances are specified in a document controlled under 10 CFR 50.59.

(j) With Permissive P12 inhibited.

(o) With Permissive P15 validated.

(p) When the SGs are relied upon for heat removal.

(q) Except when all MSIVs are closed.

Table 8-5 (page 3 of 5)
ESF Actuation Functions

TRIP / ACTUATION FUNCTION / PERMISSIVE	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	MINIMUM REQUIRED FOR FUNCTIONAL CAPABILITY[a]	LIMITING TRIP SETPOINT / DESIGN LIMIT	CONDITION
9.a. Containment Isolation (Stage 1) on High Containment Pressure	1,2,3,4	3 divisions	[18.7 psia[b)(c)]]	N
9.b. Containment Isolation (Stage 1) on SIS Actuation	1,2,3,4	3 divisions	NA	N
9.c. Containment Isolation (Stage 2) on High-High Containment Pressure	1,2,3,4	3 divisions	[≤ 36.3 psia[b)(c)]]	N
9.d. Containment Isolation (Stage 1) on High Containment Radiation	1,2,3,4	3 divisions	[≤ 100 x background[b)(c)]]	N
10.a. Emergency Diesel Generator (EDG) Start on Degraded Grid Voltage	1,2,3,4	4 divisions	[≥ 6210 V and ≤ 6350 V; ≥ 7 sec. and ≤ 11 sec. w/SIS, ≥ 270 sec. and ≤ 300 sec. wo/SIS[b)(c)]]	P
	5,6,(r)	2 divisions		P
10.b. EDG Start on LOOP	1,2,3,4	4 divisions	[≥ 4830 V and ≤ 4970 V; ≥ 0.4 sec. and ≤ 0.6 sec.[b)(c)]]	P
	5,6,(r)	2 divisions		P
11.a. Chemical and Volume Control System (CVCS) Charging Line Isolation on High-High Pressurizer Level	1,2,3,4[s]	3 divisions	[80% Measuring Range[b)(c)]]	N
11.b. CVCS Isolation on Anti-Dilution Mitigation (ADM) at Shutdown Conditions (RCP not operating)	3[t],4[t]	3 divisions	[927 ppm[b)(c)]]	O
	5[t],6	2 divisions		Q

(a) A division is OPERABLE provided: a) the minimum sensors required for functional capability for all sensors providing input to the Trip/Actuation Function/Permissive are OPERABLE; and b) the associated signal processors are OPERABLE.

(b) If the as-found setpoint is outside its predefined as-found tolerance, then the Trip/Actuation Function shall be evaluated to verify that it is functioning as required before returning the Trip/Actuation Function to service.

(c) The setpoint shall be reset to a value that is within the as-left tolerance around the Nominal Trip Setpoint (NTSP) at the completion of the surveillance; otherwise, the division shall be declared inoperable. Setpoints more conservative than the LTSP are acceptable provided that the as-found and as-left tolerances apply to the actual setpoint implemented in the Surveillance procedures to confirm Trip/Actuation Function performance. The methodologies used to determine the as-found and the as-left tolerances are specified in a document controlled under 10 CFR 50.59.

(r) During movement of irradiated fuel assemblies.

(s) With permissive P17 inhibited.

(t) With Permissive P7 validated (no RCPs in operation).

Table 8-5 (page 4 of 5)
ESF Actuation Functions

TRIP / ACTUATION FUNCTION / PERMISSIVE	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	MINIMUM REQUIRED FOR FUNCTIONAL CAPABILITY[a]	LIMITING TRIP SETPOINT / DESIGN LIMIT	CONDITION
11.c. CVCS Isolation on ADM at Standard Shutdown Conditions	3[u],4[u]	3 divisions	[(e)[b)(c)]]	O
	5[u]	2 divisions		Q
11.d CVCS Isolation on ADM at Power	1,2	3 divisions	[(e)[b)(c)]]	J
12.a. Pressurizer Safety Relief Valve (PSRV) Actuation - First Valve	4[v]	3 divisions	[(w)]	S
	5[v],6[v]	2 divisions		S
12.b. PSRV Actuation - Second Valve	4[v]	3 divisions	[(w)]	S
	5[v],6[v]	2 divisions		S
13. Control Room Heating, Ventilation, and Air Conditioning Reconfiguration to Recirculation Mode on High Intake Activity	1,2,3,4	3 divisions	[≤ 3 x background[b)(c)]]	T
	5,6,(r)	2 divisions		T
C. PERMISSIVES				
P2 - Flux (Power Range) Measurement Higher than First Threshold	1 (≥ 10% RTP)	3 divisions	[10% RTP]	H
P3 - Flux (Power Range) Measurement Higher than Second Threshold	1 (≥ 70% RTP)	3 divisions	[70% RTP]	G
P5 - Flux (Intermediate Range) Measurement Higher than Threshold	1,2 (≥ 10^{-5}% RTP)	3 divisions	[10^{-5}% RTP]	J

(a) A division is OPERABLE provided: a) the minimum sensors required for functional capability for all sensors providing input to the Trip/Actuation Function/Permissive are OPERABLE; and b) the associated signal processors are OPERABLE.

(b) If the as-found setpoint is outside its predefined as-found tolerance, then the Trip/Actuation Function shall be evaluated to verify that it is functioning as required before returning the Trip/Actuation Function to service.

(c) The setpoint shall be reset to a value that is within the as-left tolerance around the Nominal Trip Setpoint (NTSP) at the completion of the surveillance; otherwise, the division shall be declared inoperable. Setpoints more conservative than the LTSP are acceptable provided that the as-found and as-left tolerances apply to the actual setpoint implemented in the Surveillance procedures to confirm Trip/Actuation Function performance. The methodologies used to determine the as-found and the as-left tolerances are specified in a document controlled under 10 CFR 50.59.

(e) As specified in the COLR.

(r) During movement of irradiated fuel assemblies.

(u) With Permissive P7 inhibited (one or more RCPs in operation).

(v) When PSRV OPERABILITY is required by LCO 3.4.11.

(w) As specified in the Pressure Temperature Limits Report.

Table 8-5 (page 5 of 5)
ESF Actuation Functions

TRIP / ACTUATION FUNCTION / PERMISSIVE	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	MINIMUM REQUIRED FOR FUNCTIONAL CAPABILITY[a]	LIMITING TRIP SETPOINT / DESIGN LIMIT	CONDITION
P7 - RCP Not in Operation	3[t],4[t]	3 divisions	[50% no load current]	O
	5[t],6[t]	2 divisions		Q
P8 - Shutdown Rod Cluster Control Assembly Position Lower than Threshold	3[u],4[u]	3 divisions	[All rods in]	O
	5[u]	2 divisions		Q
P12 - Pressurizer Pressure Lower than Threshold	3 (RCS < 2005 psia),4[n]	3 divisions	[2005 psia]	O
P14 - Hot Leg Pressure and Hot Leg Temperature Lower than Thresholds	1,2,3,4[p]	3 divisions	[350°F and 464 psia]	N
P15 - Hot Leg Pressure and Hot Leg Temperature Lower than Thresholds and RCPs Shutdown	4	3 divisions	[350°F, 464 psia, and 50% no load current]	O
	5, 6	2 divisions		R
P16 - Hot Leg Pressure and Delta P_{sat} Lower than Thresholds, RCP Not in Operation, and Time Elapsed since Safety Injection start	1, 2, 3, 4	3 divisions	[290 psia, P_{sat} 73 psi, 50% no load current, and 1.5 hrs post-SI]	N
P17 - Cold Leg Temperature Lower than Threshold	4[v]	3 divisions	[248°F]	S
	5[v],6[v]	2 divisions		S

(a) A division is OPERABLE provided: a) the minimum sensors required for functional capability for all sensors providing input to the Trip/Actuation Function/Permissive are OPERABLE; and b) the associated signal processors are OPERABLE.

(b) If the as-found setpoint is outside its predefined as-found tolerance, then the Trip/Actuation Function shall be evaluated to verify that it is functioning as required before returning the Trip/Actuation Function to service.

(c) The setpoint shall be reset to a value that is within the as-left tolerance around the Nominal Trip Setpoint (NTSP) at the completion of the surveillance; otherwise, the division shall be declared inoperable. Setpoints more conservative than the LTSP are acceptable provided that the as-found and as-left tolerances apply to the actual setpoint implemented in the Surveillance procedures to confirm Trip/Actuation Function performance. The methodologies used to determine the as-found and the as-left tolerances are specified in a document controlled under 10 CFR 50.59.

(n) With Permissive P15 inhibited.

(p) When the SGs are relied upon for heat removal.

(t) With Permissive P7 validated (no RCPs in operation).

(u) With Permissive P7 inhibited (one or more RCPs in operation).

(v) When PSRV OPERABILITY required by LCO 3.4.11.