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. Protection and Safety Monitoring System,
    b. Reactor Trip System,
    c. Engineered Safety Features Actuation System,
    d. Plant Control and Monitoring System, and
    e. Diverse Actuation System.

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

8.1 Introduction

The instrumentation and control (I&C) systems provide the capability to control and to regulate the plant systems manually and automatically during normal plant operation, and provide reactor protection against unsafe plant operation. The primary purpose of the I&C systems is to provide automatic protection and to exercise proper control against unsafe and improper reactor operation during steady-state and transient power operations. The system also provides initiating signals to actuate safety functions, which are assigned to mitigate the consequences of faulted conditions and to ensure safe shutdown. Safety functions are those actions required to achieve the system responses assumed in the safety analyses and those credited to achieve safe shutdown of the plant. The I&C system is primarily a digital system with the exception of the analog diverse actuation system (DAS). The overall I&C architecture for the US-APWR is shown in Figure 8-1.

The general specifications of the overall I&C system are summarized as follows:

A. Main control board (refer to Figure 8-2)

- Fully computerized,
- Safety visual display units (VDUs) and nonsafety operational VDUs,
- Large display panel (LDP), and
- Minimal conventional switches, only for regulatory compliance.

B. Safety-related I&C

- Fully digital Mitsubishi Electric Total Advanced Controller (MELTAC) platform,
- Four-train redundant reactor protection system (RPS),
- Four-train redundant engineered safety features actuation system (ESFAS),
- Four-train redundant safety logic system (SLS) for component control,
- Four-train redundant safety-grade human-system interface system (HSIS), and
- Conventional switches (for train-level manual actuation).

C. Nonsafety-related I&C

- Fully digital, except for analog DAS,
- MELTAC platform,
- Duplex redundant digital architecture for each control and process monitoring subsystem, and
- Analog DAS.

D. Data communication

- Fully multiplexed, including Class 1E signals,
- Multi-drop data bus and serial data link, and
- Fiber-optics communication networks.

All nuclear steam supply systems and other I&C systems are designed and manufactured by Mitsubishi Heavy Industries (MHI). The I&C systems for the US-APWR are essentially the same as the I&C systems for new plants in Japan, including the Japanese advanced pressurized water reactor (APWR), and systems currently installed and being implemented for plant modernization in Japan.

8.2 Instrumentation and Control Architecture Overview

The overall I&C system (Figure 8-1) consists of the safety-related protection and safety monitoring system (PSMS) with the safety-related portion of the HSIS, the nonsafety-related plant control and monitoring system (PCMS), the nonsafety-related DAS, and the nonsafety-related portion of the HSIS. The HSIS consists of safety-related safety VDUs, post-accident monitoring (PAM), nonsafety-related operational VDUs, and the nonsafety-related LDP for normal plant operation. The safety VDUs and operational VDUs are located on both the operator console (OC) in the main control room (MCR) and the remote shutdown console (RSC) in the remote shutdown room (RSR). Operational VDUs are also provided for information only (i.e., no control capability) at the technical support center (TSC). Information to support emergency response operations (the same as that provided on operational VDUs) is provided at the emergency operations facility (EOF).

8.2.1 Protection and Safety Monitoring System

The safety-related PSMS with safety-related portion of the HSIS consists of:

- RPS,
- ESFAS and SLS,
- Conventional switches (train level), and
- Safety VDUs - part of the safety-related HSIS for manual operation and monitoring of critical safety functions, including PAM.

Safety functions are those actions required to achieve the system responses assumed in the safety analyses, and those credited to achieve safe shutdown of the plant. Some safety functions are automatically initiated by the PSMS. These same safety functions may also be manually initiated and monitored by operators using the

HSIS. The HSIS is also used to manually initiate other safety functions that do not require time critical actuation and safety functions credited for safe shutdown. After manual initiation from the HSIS, all safety functions are executed by the PSMS. The HSIS also provides all plant information to operators, including critical parameters required for post-accident conditions. The HSIS includes both safety and nonsafety sections.

Each of the PSMS trains is powered from two Class 1E power sources. These sources are uninterruptible power supplies (UPSs) backed up by Class 1E station batteries and by the Class 1E gas turbine generators (GTGs).

Reactor Trip System

The safety systems automatically trip the reactor and initiate engineered safety features (ESFs) (if required) whenever predetermined limits are approached. The RPS maintains surveillance on nuclear and process variables which are related to equipment mechanical limitations, such as pressure, and on variables that directly affect the heat transfer capability of the reactor, such as the reactor coolant flow and temperature. When a limit is approached, the RPS initiates the signal to open the reactor trip breakers (RTBs). This action removes power from the control rod drive mechanism (CRDM) coils, permitting the rods to fall by gravity into the core. This rapid negative reactivity insertion will cause the reactor to shut down.

Engineered Safety Features Actuation

The occurrence of a postulated accident (PA), such as a loss-of-coolant accident (LOCA) or a steam line break, requires a reactor trip plus actuation of one or more ESFs in order to prevent or mitigate damage to the core and reactor coolant system (RCS) and to ensure containment integrity.

The RPS will determine if setpoints are being approached for selected plant parameters. If setpoints are approached, the RPS will process signals through logic functions, to respond properly to the various conditions.

Once the required logic is generated, the RPS will send signals to the ESFAS, which combines signals from all four RPS trains in two-out-of-four voting logic. Once the ESFAS receives the appropriate voting logic combination, it sends signals to the SLS to actuate appropriate ESF components for protective action. The ESFAS also receives signals from conventional switches on the OC for train-level manual actuation of ESF systems.

In the event of a loss of offsite power (LOOP) and/or PA, ESF loads are connected to the emergency power buses in a predetermined sequence by the load sequencing function, provided by the ESFAS and SLS. There are two types of load sequencing: one for LOOP and the other for emergency core cooling system (ECCS) actuation concurrent with LOOP.

The ESFAS also receives interlock signals from the RPS, such as the P-4 interlock, which indicates the reactor trip. Interlocks are developed redundantly within each

RPS train. The RPS will send interlock signals to the ESFAS, which combines signals from all four RPS trains in two-out-of-four voting logic.

The SLS receives ESF system level actuation demand signals and LOOP load sequencing signals for the safety components from the ESFAS. The SLS also receives manual component level control signals from the OC (safety VDUs and operational VDUs). This system performs the component-level control logic for safety actuators (e.g., motor-operated valves [MOVs], solenoid-operated valves, switchgears).

Post-Accident Monitoring

The purpose of displaying PAM parameters is to assist MCR personnel in evaluating the safety status of the plant. In accordance with RG 1.97, PAM Type A, B, and C variables have redundant instrumentation and can be displayed on at least two redundant safety VDUs. Type A and B parameters are continuously displayed on the LDP and are continuously available on a safety VDU, or can be retrieved immediately.

8.2.2 Plant Control and Monitoring System

The function of the nonsafety PCMS is to establish and maintain the plant operating conditions within prescribed limits. The PCMS includes the reactor control system, the balance of plant (BOP) control system, the incore instrumentation system, the nonsafety part of the HSIS, and other I&C systems.

Each system within the PCMS has redundant controllers powered by separate non-Class 1E UPSs. These UPSs are backed up by station batteries and by the alternate ac power sources.

8.2.3 Diverse Actuation System

The nonsafety-related DAS monitors and controls safety and nonsafety systems required for coping with anticipated operational occurrences (AOOs) and PAs concurrent with a common-cause failure (CCF) that disables all functions of the PSMS and PCMS. The DAS includes automated actuations and manual controls.

8.2.4 Data Communication Systems

The data communication system (DCS) consists of the plant-wide unit bus, the safety bus for each PSMS train, and the maintenance networks for the PSMS trains and for the PCMS (five maintenance networks total). The DCS also contains data links for point-to-point communication and an input/output (I/O) bus for each controller. This includes information and controls for the MCR, RSR, and TSC (monitoring only at the TSC). The DCS interfaces with the station bus, which is an information technology network (i.e., not I&C). The station bus provides information to plant personnel and to the EOF. Figure 8-1 shows the major components of the DCS within the overall I&C architecture.

8.2.5 Defense in Depth and Diversity

The architecture of the overall I&C system is based on the defense-in-depth and diversity concepts. These concepts define four echelons of defense. These echelons are the control system, the reactor trip system, the engineered safety features actuation system, and monitoring and indicators. Separation of functions and diversity of functions between these echelons minimize the potential for CCFs. In addition, the software applied for the PSMS has high integrity due to design simplicity and a comprehensive software quality program including independent verification and validation (V&V).

The conventional, analog, and hardwired DAS is provided to accommodate beyond-design-basis CCFs that could adversely affect all safety and nonsafety control systems within all echelons. The DAS provides automated actuation of time-critical safety functions. In addition, the DAS allows the operator to monitor critical safety functions and to manually actuate safety process systems, using equipment that is diverse from the PSMS and PCMS.

8.3 Reactor Trips

8.3.1 System Description

The reactor trip (RT) system, which achieves all RT functions, consists of the following Class 1E systems:

- Safety sensors,
- RPS,
- RTBs, and
- Safety-grade HSIS.

Figure 8-3 shows the RPS configuration.

The RPS automatically trips the reactor to ensure that specified acceptable fuel design limits are not exceeded. Fuel design limits are defined by several considerations, such as mechanical/hydraulic limitations on equipment and heat transfer phenomena. The RPS maintains surveillance of process variables which affect equipment mechanical limitations, such as pressure, and also of variables that are direct measurements of the heat transfer capability of the reactor, such as reactor coolant flow and reactor coolant temperature. Other parameters utilized in the RPS are calculated indirectly from combinations of process variables, such as ΔT (i.e., reactor coolant hot leg temperature [T_{hot}] – reactor coolant cold leg temperature [T_{cold}]). Whenever a direct process measurement or calculated variable exceeds a setpoint, the reactor is shut down in order to protect against either gross damage to the fuel cladding or a loss of system integrity, which could lead to the release of radioactive fission products into the containment vessel (C/V).

To initiate a reactor trip, the RPS interfaces with the following equipment:

- Sensors and manual inputs, and
- RTBs.

The RPS consists of four redundant and independent trains. Four redundant measurements using sensors from the four separate trains are made for each variable used for reactor trip. This applies to all measurements with the exception of source range and intermediate range nuclear instrumentation outputs and main turbine stop valve positions, which only have two associated trains. Selected analog measurements are converted to digital form by analog-to-digital converters within the four trains of the RPS. When a monitored signal requires signal conditioning, it is applied prior to its conversion to digital form. Following necessary calculations and processing, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for a given parameter is generated if one train's measurement exceeds its limit. Each train sends its own partial trip signal to each of the other three trains over isolated serial data links. The RPS will generate a RT signal if two or more trains of the same variable are in the partial trip state. The RPS sends system status and process data to the nonsafety-related part of the HSIS and the PCMS via the unit bus. The RPS also receives operator bypass and reset signals, which are not required for safety, from the HSIS via the unit bus.

8.3.1.1 Functional Performance

The RT system automatically initiates an appropriate reactor trip:

- To protect fuel design limits for AOOs,
- To limit core damage for PAs, and
- So that the energy generated in the core is compatible with the design provisions to protect the reactor coolant pressure boundary for limiting fault conditions.

The RT system initiates a turbine trip signal whenever a reactor trip is initiated. This function prevents the reactivity insertion that would otherwise result from an excessive reactor coolant system cooldown and thus avoids an unnecessary actuation by the ESFAS. The RT system provides for manual initiation of a reactor trip by operator action.

8.3.1.2 Reactor Trip Logic

Each train of the RPS consists of two separate digital controllers to achieve defense in depth through functional diversity. Two different parameters are monitored by the separate sensors that interface with two separate digital controllers within the RPS. Each of the controllers processes these inputs to generate reactor trip and/or ESF actuation signals. This two-fold diversity is duplicated in each redundant RPS train. The processing of diverse parameters results in functional redundancy within each RPS train. Functional diversity provides two separate methods of detecting the same abnormal plant condition for specific AOOs and specific PAs, which helps to minimize the potential for CCF concurrent with these specific events. Each functionally diverse digital controller within a train can initiate a reactor trip. The RT signal from each of the four RPS trains is sent to a corresponding RT actuation train. Each of the four RT actuation trains consists of two RTBs. The reactor is tripped when two or more RT actuation trains receive an RT signal. When a limit is

approached, the RPS initiates signals to open the RTBs. This action removes power to the CRDM coils, permitting the control rods to fall by gravity into the core. This rapid negative reactivity insertion causes the reactor to shut down.

Figure 8-4 illustrates the configuration of the RTBs. The breakers are located in two fire-protected areas. Breakers with a "1" designation are located in one room. Breakers with a "2" designation are located in the second room. This configuration ensures that a fire in one room does not prevent a reactor trip. The cables of each train are isolated for fire. The isolation between trains A and B and between trains C and D is based on IEEE Std. 384-1992, including minimum distance and barriers. Isolation between trains A/B and trains C/D is by separate fire areas. The logic functions within the RPS are limited to bistable calculations and voting for RT actuation. Each train performs 2-out-of- 4 voting logic for like-sensor coincidence to actuate trip signals to the four trains of the RTBs. Each train also includes a hardwired manual switch on the OC that directly actuates the RTBs. Each switch bypasses the associated RPS digital controller. The trip demand, whether generated manually or automatically, initiates the following actions: 1) it de-energizes the undervoltage trip attachments on the RTBs, and 2) it energizes the shunt trip devices on the RTBs. Either action causes the breakers to trip.

The RPS is a microprocessor-based digital system that achieves high reliability through segmentation of primary and backup trip/actuation functions, use of four redundant trains, failed equipment bypass functions, and microprocessor self-diagnostics, including data communications. The system also includes features to allow for manual periodic testing of functions that are not automatically tested by the self-diagnostics, such as the opening of RTBs. Manual periodic tests can be conducted with the plant on-line and without jeopardy of spurious trips due to single failure(s) during testing.

8.3.1.3 Reactor Trip Variables

The following variables and signals are monitored to generate reactor trip signals. Some of the variables are used by multiple safety functions and nonsafety control functions.

- Neutron flux (source range, intermediate range and power range, neutron flux rate for power range),
- Reactor coolant cold leg and hot leg temperature (T_{cold} and T_{hot}),
- Pressurizer pressure,
- Pressurizer water level,
- Reactor coolant flow,
- Reactor coolant pump (RCP) speed,
- Steam generator (SG) water level,
- ECCS actuation signal,
- Manual RT actuation signal, and
- Turbine trip signal.

8.3.2 Reactor Trip Initiating Signals

The following subsections describe the specific reactor trip functions, which are grouped according to their protection function. The complete list of RT initiating signals is provided in Table 8-1. The initiating signals are included in the reactor trip functional diagram, Figure 8-5. Table 8-2 provides the range, accuracy, response time, and setpoint for each RT variable. Permissives associated with the RPS are described in Table 8-3. Table 8-4 shows diverse parameters in two separate controller groups.

8.3.2.1 Nuclear Startup Protection Trips

High Source Range Neutron Flux Trip

The high source range neutron flux trip provides protection during reactor startup and plant shutdown. An operating bypass may be manually initiated when the neutron flux is above the P-6 setpoint value (intermediate range), which also de-energizes the high voltage power supply to the source range neutron flux detectors. This trip is automatically bypassed by the power range neutron flux interlock P-10. The bypass automatically resets to reactivate the trip function when the intermediate range neutron flux decreases below the P-6 reset point.

Due to the limited duration of reactor startup and shutdown, there are only two source range instrument channels, trains A and D. The train A source range neutron flux detector interfaces with RPS trains A and B. The train D source range neutron flux detector interfaces with RPS trains C and D. Interfaces to RPS trains B and C are via isolated digital data links.

The source range and intermediate range neutron flux signals from the train A detectors are sent to the RPS controllers of train A and B through analog circuits installed in the train A nuclear instrumentation system (NIS) cabinet and compared with trip setpoints in each train's controller. The signals from the train A NIS cabinet to the train B RPS cabinet are isolated in the train B RPS cabinet. In the case of the train D detectors, the neutron flux signals are sent to the train C and D controllers. The results of the comparison with trip setpoints in train D are sent to train A, and the trip signals of train A (train A partial trip) are generated as a result of one-out-of-two logic. The train D trip signals are generated by the same logic. Similarly, the results of the comparison with trip setpoints in train C are sent to train B, and the trip signals of train B (train B partial trip) are generated as a result of one-out-of-two logic. The train C trip signals are generated by the same logic. The results of the one-out-of-two logic may be bypassed by the following operating bypass signals: (1) P-6 allows the source range neutron flux trip manual operating bypass, (2) P-10 allows the source range neutron flux trip automatic operating bypass, and (3) P-10 allows then intermediate range trip manual operating bypass.

Similar trip logic functions are processed in each train. The partial trip signal from each train is sent to each trip breaker of the corresponding train, and a two-out-of-four voting logic is implemented.

High Intermediate Range Neutron Flux Trip

This trip provides protection during reactor startup and shutdown. It can be manually bypassed if the power range channels are above 10 percent power (P-10). This operating bypass is automatically reset to reactivate the trip function when the power range channels indicate less than the reset point for P-10.

Due to the limited duration of reactor startup and shutdown, there are only two intermediate range instrument channels, trains A and D. The train A intermediate range neutron flux detector interfaces with RPS trains A and B. The train D intermediate range neutron flux detector interfaces with RPS trains C and D. Interfaces to RPS trains B and C are by isolated digital data links.

As described above for the high source range neutron flux trip, the results of the comparison with trip setpoints in train D are sent to train A, and a trip signal from train A (train A partial trip) is generated as a result of 1-out-of-2 logic. A train D trip signal is generated by the same logic. Similar 1-out-of-2 logic is performed in trains B and C with neutron flux signals obtained from trains A and D.

High Power Range Neutron Flux Trip (Low Setpoint)

This parameter trips the reactor when two of the four power range channels exceed the trip setpoint. This trip provides protection during startup. It can be manually bypassed when the power range channels are above 10 percent power (P-10). This operating bypass automatically resets to reactivate the trip function when the power range channels indicate less than the reset point for P-10. This operating bypass action is indicated in the MCR.

8.3.2.2 Nuclear Overpower Protection Trips

Four power range nuclear instrumentation detectors are installed in vertical orientations at the four corners of the core. Each power range neutron flux detector assembly consists of an upper-half detector and a lower-half detector. Each detector assembly has a total active length that covers almost the full active fuel length. The detectors are used to measure power level, axial flux difference, and radial quadrant power tilt.

The basic power range signals are:

- A signal from the upper half of each power range neutron flux detector, which corresponds to the neutron flux in the upper section (four signals total), and

- A signal from the lower half of each power range neutron flux detector, which corresponds to the neutron flux in the lower section (four signals total).

The following variables are derived from these basic signals:

- Nuclear power, derived from the average of the upper and lower signals, and
- Axial flux difference, derived from the upper-half flux minus the lower-half flux.

The remaining RT signals derived from the power range nuclear instrumentation are described in the subsections below.

High Power Range Neutron Flux Trip (High Setpoint)

This parameter trips the reactor when two of the four power range channels exceed the trip setpoint. This trip provides protection against excessive core power generation during normal plant operation, and is always active.

High Power Range Positive Flux Rate Trip

This trip protects the reactor when a sudden abnormal increase in power occurs in two out of the four power range channels. It is always active. A channel is tripped when rate sensitive circuits in the channel detect a rate of change in nuclear power above the trip setpoint value. The channel trip is latched such that the partial trip signal does not disappear when the rate of change in power goes below the trip setpoint value. Once latched, the channel can only be reset from the MCR by manual action. This manual action can only be completed after the rate of change in power goes below the trip setpoint value.

High Power Range Neutron Flux Negative Rate

This trip protects the reactor when a sudden abnormal radial power distribution occurs with two or more dropped control rods. An RT is initiated when two out of the four power range channels detect a negative flux rate exceeding the setpoint. The trip is always active. A channel is tripped when rate sensitive circuits in the channel detect a rate of change in nuclear power greater in magnitude than the setpoint value. The channel trip is latched such that the partial trip signal does not disappear when the rate of change in power reduces to below the setpoint value. Once latched, the channel can only be reset from the MCR by manual action. This manual action can only be completed after the negative flux rate becomes lesser in magnitude than the trip setpoint value.

8.3.2.3 Core Heat Removal Protection Trips

Overtemperature ΔT Trip

This trip provides protection to prevent a departure from nucleate boiling (DNB) or the development of core-exit boiling (hot-leg boiling). The setpoints for the DNB limit and the core-exit boiling limit are continuously and individually calculated by the RPS using specific algorithms. The lower value of these two setpoints is used as the overtemperature ΔT trip setpoint.

The DNB protection setpoint is calculated as a function of pressurizer pressure (P_{PZR}), reactor coolant system average temperature (T_{avg}), and axial flux difference (ΔI). An increase in ΔI beyond a predefined deadband results in a decrease in the trip setpoint. The core-exit boiling protection setpoint is calculated as a function of T_{avg} and P_{PZR}. A reactor trip is initiated when the loop ΔT ($T_{hot} – T_{cold}$) in at least two of the four loops exceeds the setpoint.

Overpower ΔT Trip

This trip provides protection against excessive power. The setpoint for this trip is continuously calculated by the RPS using a specific algorithm.

The overpower ΔT trip setpoint is calculated as a function of T_{avg} and ΔI. An increase in ΔI beyond a predefined deadband results in a decrease in the trip setpoint. A reactor trip is initiated when the loop ΔT in at least two of the four loops exceeds the setpoint.

Low Reactor Coolant Flow Trip

This trip protects the reactor in the event of low reactor coolant flow in one or more loops. An RT is initiated when two out of four flow sensors indicate low reactor coolant flow in any loop. This trip is automatically bypassed when reactor power is below the P-7 permissive setpoint, as indicated by power range neutron flux and turbine inlet pressure. The operating bypass is automatically removed when reactor power is above the P-7 permissive setpoint.

Low Reactor Coolant Pump Speed Trip

This trip protects the reactor core in the event of loss of flow in all loops by tripping the reactor when the speed of two out of four RCPs falls below the setpoint. RCP speed is measured by an electro-magnetic speed detector. This trip is automatically bypassed by permissive P-7. The operating bypass is automatically removed when reactor power is above the P-7 permissive setpoint.

Low Pressurizer Pressure Trip

This trip protects the reactor against low pressure, which could lead to DNB. An RT is initiated when two out of four pressurizer pressure channels fall below the low setpoint. This trip is automatically bypassed when reactor power (turbine inlet pressure and power range neutron flux) is below the P-7 permissive setpoint. The operating bypass is automatically removed when reactor power is above the P-7 permissive setpoint.

8.3.2.4 Primary Overpressure Protection Trips

High Pressurizer Pressure Trip

This trip protects the RCS against system overpressure. The trip signal is generated when two out of four pressurizer pressure channels exceed the trip setpoint. There are no operating bypasses associated with this trip.

High Pressurizer Water Level Trip

This trip prevents water relief through the pressurizer relief valves for system overpressurization. The trip signal is generated when two out of four pressurizer water level channels exceed the trip setpoint. This trip is automatically bypassed

when reactor power is below the P-7 permissive. This operating bypass is automatically removed when reactor power is above the P-7 setpoint.

8.3.2.5 Loss of Heat Sink Protection Trip

The low SG water level trip protects the reactor from the loss of its heat sink in the event of a loss of feedwater to the SGs. The trip signal is generated when two out of four water level sensors, in any SG, monitor water level at or below its trip setpoint. There are no operating bypasses associated with this RT.

8.3.2.6 Excessive Cooldown Protection Trip

The high-high SG water level trip protects the reactor from excessive cooldown in the event of excessive feedwater addition to the SGs, and prevents damage to the main turbine by water induction. The trip signal is generated when two out of four water level sensors in any SG exceed the setpoint. This trip is automatically bypassed when reactor power is below the P-7 permissive. This operating bypass is automatically removed when reactor power is above the P-7 setpoint.

8.3.2.7 Emergency Core Cooling System Actuation Trip

A trip signal is initiated from each RPS train with actuation of its respective ECCS train, manually or automatically. This trip protects the core against a loss-of-coolant accident or a steam line break.

8.3.2.8 Turbine Trip

An RT on turbine trip is an anticipatory trip that is not credited in the safety analysis. Therefore, this is not a safety function, but it is designed to be highly reliable. Even though the turbine-trip sensors are located in an area that is not seismically qualified (the turbine building), the effects of credible failures in this area could not be propagated back to the RPS and degrade the RPS performance or reliability. An RT is initiated by either of the following two diverse turbine trip signals:

Main Turbine Stop Valves Closed

The RT signal is generated within each RPS train when that train receives signals indicating that all four main turbine stop valves are closed. As for all other trips, an RT is generated when two out of four RPS trains have detected this condition.

The two limit switches on each main turbine stop valve interface with RPS trains A and D, as associated circuits. RPS train A routes the limit switch signals to trains B, C, and D. RPS train D retransmits the limit switch signals to trains A, B, and C. Train interfaces are by isolated digital data links.

The main turbine stop valve limit switch inputs can be individually bypassed in each RPS train to permit channel testing. This maintenance bypass condition is displayed in the MCR. This trip is automatically bypassed by permissive P-7 for power levels lower than the P-7 setpoint. The operating bypass is automatically removed above the P-7 power level.

Low Turbine Emergency Trip Oil Pressure

The turbine emergency trip oil pressure trip signal is generated when the oil pressures from two out of four oil pressure channels are below the trip setpoint. Four oil pressure signals are independently interfaced to each train of the RPS as associated circuits. This trip is automatically bypassed by permissive P-7 for power levels lower than the P-7 setpoint. The operating bypass is automatically removed above the P-7 power level.

8.3.3 Manual Control and Actuated Devices

In addition to the automatic trips, operators can trip the RTBs using conventional, fixed-position, hardwired switches on the OC. There is one switch for each RT actuation train. Actions by the undervoltage trip and shunt trip attachments to trip the reactor are discussed in subsection 8.3.1.2. There are no operating bypasses associated with the manual RT.

8.3.4 Bypasses (Permissives)

Automatic and manual operating bypasses are provided to bypass certain protective actions that would otherwise prevent modes of operation such as startup. Automatic and manual operating bypasses are described in the subsections below.

8.3.4.1 Automatic Operating Bypasses

Some operating bypasses are automatically initiated separately within each PSMS train when the plant process permissive condition is sensed by the PSMS input channel(s). The automatically initiated operating bypasses for the RPS are as follows:

- The high source range neutron flux trip is bypassed automatically by power range neutron flux (P-10).
- The low reactor coolant flow trip is bypassed automatically during low power conditions (P-7).
- The low RCP speed trip is bypassed automatically during low power conditions (P-7).
- The low pressurizer pressure trip is bypassed automatically during low power conditions (P-7).
- The high pressurizer water level trip is bypassed automatically during low power conditions (P-7).
- The high-high SG water level trip is bypassed automatically during low power conditions (P-7).
- The reactor trip on turbine trip is bypassed automatically during low power conditions (P-7).

All automatically initiated operating bypasses are automatically removed when the plant moves to an operating condition in which the protective action would be required if an accident occurred. Refer to Table 8-3.

8.3.4.2 Manual Operating Bypasses

Some operating bypasses must be manually initiated. These operating bypasses can be manually initiated separately within each PSMS division when the plant process permissive condition is sensed by the PSMS input channel(s). The manually initiated operating bypasses for the RPS are as follows:

- The high source range neutron flux trip is bypassed manually with high intermediate range neutron flux (P-6).
- The high intermediate range neutron flux trip is bypassed manually with high power range neutron flux (P-10).
- The high power range neutron flux (low setpoint) trip is bypassed manually with high power range neutron flux (P-10).

All operating bypasses, either manually or automatically initiated, are automatically removed when the plant moves to an operating regime in which the protective action would be required if an accident occurred. Status indication is provided in the MCR for all operating bypasses.

8.4 Engineered Safety Features Actuations

8.4.1 System Description

The equipment involved in actuating ESF systems consists of:

- Safety sensors,
- RPS,
- ESFAS,
- SLS,
- Safety-grade HSIS, which includes processors and VDUs common to both RPS and ESFAS, and
- Conventional safety-related switches (for system-related actuation).

Figure 8-6 shows the overall configuration for the ESFAS and the SLS.

ESF systems provide I&C functions to sense accident conditions and initiate the operation of necessary ESF system components to mitigate accident conditions in a timely manner. The occurrence of a PA, such as a LOCA or a steam line break, requires an RT plus actuation of one or more ESF systems in order to mitigate the consequences. The RPS receives signals from various sensors and transmitters. The RPS then determines if the setpoints are being exceeded, and if they are, the RPS combines the signals into logic matrices indicative of primary or secondary system boundary ruptures. Once the required logic combination is completed, the RPS sends ESF actuation signals to each train of the ESFAS. Each train of the ESFAS combines the signals from all RPS trains using 2-out-of-4 voting logic to actuate its respective train of the SLS.

Actuated and/or realigned ESF systems include the ECCS, containment isolation systems, the containment spray system (CSS), the emergency feedwater system

(EFWS), the annulus emergency exhaust system, and the MCR heating, ventilation, and air conditioning (HVAC) system. These systems, their subsystems, and/or their components are actuated by the appropriate ESFAS signals as necessary to mitigate specific accident/event condition(s). Examples of actuations by the ESFAS include ECCS actuation, main steam line isolation, containment spray (CS) actuation, containment isolation, emergency feedwater (EFW) actuation, MCR isolation, emergency generator startup, essential service water system (ESWS) actuation, and RT (at the train level). Individual ESF systems can be manually actuated from the MCR.

The following equipment is involved in ESF actuations:

- Process variable sensors.

- The RPS for processing process input signals and voting to determine the need for system-level ESF actuation.

- The ESFAS for voting logic, which combines signals from all RPS trains and generates train-level actuation signals to the SLS. The ESFAS also sequences the actuation of plant components to avoid overloading plant electrical systems during LOOP conditions.

- The SLS to distribute train-level actuation signals from the ESFAS to the control logic for designated plant components.

- Systems and components associated with ESF systems.

- Safety VDU processors and safety VDUs to provide manual component-level control of plant components after initial automatic actuation by the ESFAS. Safety VDUs also provide resets for ESFAS actuations.

- Conventional switches for manual initiation at the train level

The ESFAS and SLS send system status and process data, which are not required for safety, to the HSIS and PCMS via the unit bus. The ESFAS and SLS also receive manual component control and reset signals, which are not required for safety, from the HSIS via the unit bus.

8.4.1.1 ESF System-Level Logic

There are four trains for the ESF system in the US-APWR design. The system-level ESF actuation signals from all four RPS trains are transmitted over isolated data links to an ESFAS controller in each train of the ESF system. Each ESFAS controller consists of a duplex architecture using dual central processing units (CPUs) to enhance reliability. The RPS provides bistable calculations and voting logic to the ESFAS for ESF actuation. Two-out-of-four coincidence voting logic is performed within each train through the redundant subsystems within each ESFAS controller. Each ESFAS subsystem generates a train-level ESF actuation signal when the required two-out-of-four coincidence is met from the four RPS actuation signals. System-level ESF manual actuation signals are hardwired from

conventional switches located on the OC. These signals are also processed by the logic in each redundant subsystem of each ESFAS train to generate the same train-level ESF actuation signal. Train-level manual actuation signals are generated for each ESFAS signal from separate switches for each ESFAS train. To avoid spurious actuation from a single contact or signal path failure, each switch contains two contacts that are interfaced to two separate digital inputs. Each ESFAS subsystem processes these signals through redundant train-level manual actuation with two-out-of-two logic.

Whether automatically or manually initiated, train-level ESF actuation signals are transmitted from both subsystems of the ESFAS controller to the corresponding train of the SLS. The number of ESFAS trains that generate train-level ESF actuation signals corresponds to the number of mechanical ESF trains being actuated.

The ESFAS also provides automatic load sequencing for the Class 1E GTGs to accommodate the site LOOP event. Each ESFAS train monitors three undervoltage inputs, using two-out-of-three logic, to detect a loss of power condition for its respective train, and generates a LOOP signal. Upon detecting a loss of power, the ESFAS starts the Class 1E GTG for its train and disconnects the loads for its train from the electrical bus. Once the Class 1E GTG is capable of accepting loads, the ESFAS sequences the loads for its train back onto the electrical bus in an order appropriate for the current train-level ESF actuation signal(s). The ESFAS sequencing logic accommodates ESF actuation signals occurring prior to or during a loading sequence. The ESFAS load sequencing function is independent for each train. The ESFAS also provides automatic load sequencing for ESF components when they are actuated during normal power conditions (i.e., no LOOP).

Safety-related components are manually loaded on the nonsafety alternate ac power sources from the SLS during a station blackout (which includes the loss of the Class 1E GTG power sources).

8.4.1.2 ESF Component-Level Logic

The SLS controls safety-related plant components in all trains based on ESF actuation signals, process instrumentation, and component-level manual actions from the operational VDUs and safety VDUs.

There are four SLS trains in the US-APWR design. The SLS consists of multiple controllers in each train. Plant process systems are assigned to controllers based on consideration of maintenance, potential SLS equipment failures, and optimization of controller performance. In general, complete plant process systems are assigned to a single controller. Multiple process systems are assigned to the same controller, or a single process system is assigned to multiple controllers, only if the plant effects of controller failure and maintenance are demonstrated to be acceptable, based on the failure-modes-and-effects analysis.

Each train of the SLS receives ESF system-level actuation demand signals and load sequencing signals from its respective train of the ESFAS. The SLS also receives manual component-level control signals from the OC and RSC (safety VDUs and operational VDUs). The SLS also receives process signals from the RPS for

interlocks and controls of plant process systems. The system performs the component-level control logic for safety actuators (e.g., MOVs, solenoid-operated valves, and switchgears).

The SLS controllers for each train are located in separate I&C rooms. The system has conventional I/O portions and I/O portions with priority logic to accommodate signals from the DAS. All SLS I/O modules are located within Class 1E I&C equipment rooms and Class 1E electrical rooms, which have mild environment conditions maintained by the safety ventilation system at all times.

The SLS is a microprocessor-based system that achieves high reliability through redundancy within each train and microprocessor self-diagnostics, including data communications. The system also includes features to allow periodic testing of functions that are not automatically tested by the self-diagnostics, such as final actuation of safety components. Manual periodic tests can be conducted with the plant on-line and without the risk of spurious system level actuation due to single failures during testing.

To enhance reliability, each SLS controller consists of a duplex architecture using redundant CPUs operating in a redundant parallel configuration. Each controller of the duplex architecture receives ESF actuation signals and load sequencing signals from the corresponding duplex controller of the ESFAS. The SLS also includes I/O modules mounted in I/O chassis. These I/O chassis can be located within the same cabinet as the controllers, or remotely in separate cabinets that are distributed throughout the plant to reduce the lengths of cables from the process components or instruments to the I/O chassis. Signals from each SLS controller in the duplex architecture are combined in the output modules using one-out-of-two logic for control of plant components to the desired safety state. The SLS I/O modules include contact-input-conversion devices and power-interface devices. Each power interface module receives input signals and controls the actuation device (such as a motor starter, switchgear, etc.). The actuation device, in turn, controls motive power to the final ESF component. Each train of the SLS thus interfaces the PSMS to a train of the ESF equipment.

Each controller has multiple I/O chassis, each chassis has multiple I/O modules, and each I/O module accommodates one or more process interfaces. The plant process interfaces are assigned to I/O modules/chassis with consideration of maintenance and potential SLS equipment failures. Acceptable plant-level effects for failure or maintenance of any I/O module or any I/O chassis are demonstrated. I/O modules are duplicated within a single SLS train if a single failure of the I/O module causes a spurious reactor trip.

The ESFAS provides all the system-level ESF actuation logic, including the automatic load sequencing for the Class 1E GTGs. Whether automatically or manually generated, train-level ESF actuation signals are transmitted from each ESFAS train to the corresponding train of the SLS. Within the SLS, the train-level ESF actuation signals are then broken down to component actuation signals to actuate all components associated with an ESF function. The logic within each train of the SLS accomplishes this function and performs the necessary interlocking to ensure that components are properly aligned for safety.

The SLS also controls ESF components, such as the EFW control valve, based on manual component-level controls from operational VDUs and safety VDUs, including all components required for credited manual operator actions. To ensure spurious command signals from operational VDUs cannot adversely affect multiple safety divisions, all safety components controlled by the PSMS, regardless of their positions under normal operating conditions, are commanded to the correct safety positions by automatic safety interlocks or automatic ESFAS actuation signals.

8.4.1.3 Engineered Safety Features

For the US-APWR design, the ESF systems consist of the ECCS, containment isolation systems, CSS, EFWS, annulus emergency exhaust system, and MCR HVAC system. The ESFAS activates the required components to mitigate plant conditions relating to the occurrence of specific credible limiting fault(s). Limiting faults include LOCA; large or small steam line break; LOOP; LOCA followed by LOOP, LOOP followed by LOCA, or both occurring together; control rod ejection; SG tube rupture; and all credible accidents in which radioactive fission products could be released from the RCS.

8.4.1.4 Process Variables Monitored for ESF Actuations

The following variables and signals are monitored for generating ESF actuation signals to initiate various required ESF systems. Some of the variables are used by multiple safety functions and nonsafety control functions.

- Pressurizer pressure,
- Pressurizer water level,
- Main steam line pressure,
- SG water level,
- Containment pressure,
- Containment high-range area radiation,
- MCR outside air intake radiation,
- Main feedwater (MFW) pumps trip signal,
- RT signal (P-4 interlock),
- LOOP signal, and
- Reactor coolant cold leg and hot leg temperatures (T_{avg} signal).

8.4.2 ESF Initiating Signals, Logic, Actuation Devices, and Manual Controls

The following subsections provide functional descriptions of ESF actuation signals, actuated systems/components, and the initiating logic for actuating the ESF functions. The complete list of ESF actuation signals is provided in Table 8-5. Table 8-6 provides the range, accuracy, response time, and setpoint for each actuation variable.

Except as noted in specific sections below, all actuation signals are latched at the train level, whether automatically or manually initiated, and require manual reset. Latching ensures that the protective action goes to completion and ensures that components remain in their safety positions after the process returns to its pre-trip

condition. A manual reset can only be initiated after the process returns to its pre-trip condition.

Except as noted in specific sections below, each description is for one train and is applicable to all four trains. All manual actuations, bypasses, overrides, and resets are initiated separately for each train.

8.4.2.1 Emergency Core Cooling Actuation

An ESF actuation signal for the ECCS function is generated when any of the following initiating signals are present. The logic for this actuation circuit is shown in Figure 8-7.

- Manual actuation,

- Low pressurizer pressure, generated when 2 out of 4 signals for low pressurizer pressure are present and the pressurizer pressure ECCS actuation bypass is not activated,

- Low main steam line pressure, generated when 2 out of 4 signals for low pressure in any one of the four steam lines are present and the main steam line pressure ECCS actuation bypass is not active, and

- High containment pressure, generated when 2 out of 4 signals for high containment pressure are present. There is no operating bypass associated with this ECCS actuation signal.

The low pressurizer pressure ECCS actuation bypass and low main steam line pressure ECCS actuation bypass can be activated manually only when the pressurizer pressure interlock P-11 is present (i.e., when the pressurizer pressure signal is lower than the P-11 setpoint). These manually initiated operating bypasses are automatically removed when the pressurizer pressure signal is higher than the P-11 setpoint.

An activated ECCS signal is latched separately for each train and cannot be manually overridden for 160 seconds. After the ECCS actuation is manually overridden, the override is automatically removed when the P-4 RT interlock clears (i.e., the RTBs are re-closed). An ECCS actuation signal cannot be manually reset for 160 seconds after actuation and until the initiating signals have cleared.

An ECCS actuation signal aligns the ESF system valves (e.g., containment isolation valves, EFW valves) and starts the ESF system pumps and fans required to mitigate the specific accident and/or AOO conditions. An ECCS actuation signal results in the following actions:

- All Class 1E RCP breakers (one breaker in the Class 1E electrical room and one in the turbine building electrical room for each RCP) are tripped in 15 seconds if the P-4 RT interlock is present. The P-4 interlock is generated when breaker open status signals are received from any combination of RTBs that would result in an RT.

- Emergency generators are started. The ECCS actuation signal starts the emergency power sources.

- Safety injection pumps are started.

- Reactor trip. An RT is initiated by the ECCS actuation signal; refer to section 8.3.

- Main feedwater isolation.

- Emergency feedwater actuation.

- Containment isolation phase A.

- Containment purge isolation.

- Hydrogen igniter actuation. This is a nonsafety function. Isolation is provided within the PSMS for this function.

- MCR isolation.

- ESWS actuation.

The ECCS actuation signal also initiates automatic load sequencing.

The P-4 interlock is generated independently in each RPS division. Each RPS train receives status signals from the RTBs in its own train. RTB status signals are interfaced between RPS trains through the same fiber-optic data links used for all RPS partial trip signals. P-4 interlocks from each RPS train are interfaced to each ESFAS train through 2-out-of-4 logic.

8.4.2.2 Main Steam Line Isolation

There are only two ESFAS trains for main steam line isolation, A and D.

An ESF actuation signal for the main steam isolation function is generated when any of the following initiating signals are present.

- Manual actuation,

- High-high containment pressure, generated when 2 out of 4 signals for high-high containment pressure are present,

- Low main steam line pressure, generated when 2 out of 4 signals for low main steam line pressure are present in any one of the four steam lines and the low main steam line pressure ECCS actuation bypass is not activated, and

- High main steam line pressure negative rate, generated when 2 out of 4 signals for high main steam line pressure negative rate are present in any one of the four steam lines. The high main steam line pressure negative rate trip is only active when the low main steam line pressure trip is inactive.

Once the main steam line isolation signal is generated, it is latched and can only be reset by manual action. This signal initiates closure of the main steam isolation valves and associated bypass valves for all four loops.

8.4.2.3 Containment Spray Actuation

An ESF actuation signal for the CS actuation function is generated when any of the following initiating signals are present.

- High-3 containment pressure, the result of 2 out of 4 signals from high-3 containment pressure, and

- Manual actuation. Unlike other manual actuations, which are actuated by a single switch for each train, the manual actuation signal for each CS train is activated when two out of two CS manual controls are operated concurrently.

8.4.2.4 Containment Isolation Phase A

An ESF actuation signal for the containment isolation phase A function is generated when any of the following initiating signals are present.

- ECCS actuation, and
- Manual actuation.

For any single containment penetration, isolation can be accomplished by either of two redundant trains. There are only two ESFAS trains for containment isolation phase A, A and D.

8.4.2.5 Containment Isolation Phase B

An ESF actuation signal for the containment isolation phase B function is generated when any of the following initiating signals are present.

- High-3 containment pressure, the result of 2 out of 4 signals from high-3 containment pressure, and

- Manual CS actuation.

For any single containment penetration, isolation can be accomplished by either of two redundant trains. All containment isolation functions are distributed among all four ESFAS trains.

8.4.2.6 Containment Purge Isolation

An ESF actuation signal for the containment purge isolation function is generated when any of the following initiating signals are present.

- ECCS actuation,

- High containment high-range area radiation, the result of two out of four signals for high containment radiation,

- Manual containment isolation phase A actuation, and

- Manual CS actuation.

For any single containment penetration, isolation can be accomplished by either of two redundant trains. There are only two ESFAS trains for containment purge isolation, A and D.

8.4.2.7 MCR Isolation

An ESF actuation signal for this function is generated when any of the following initiating signals are present.

- Manual actuation,

- ECCS actuation, and

- High MCR outside air intake radiation. There are six MCR outside air intake radiation monitors (two gas monitors, two iodine monitors, and two particulate monitors) interfaced separately to RPS trains A and D. RPS trains A and D provide separate bistable setpoint comparison functions for each monitor. These bistable output signals are distributed from RPS trains A and D to each of the four ESFAS trains. Within each of the four ESFAS trains, the MCR isolation signal is actuated on a signal from either the A or the D train detector using one-out-of-two logic for each type of monitor.

8.4.2.8 Main Feedwater Isolation

Main Feedwater Regulation Valve Closure

An ESF actuation signal for MFW regulation valve closure is generated when the following signal is present.

- Low T_{avg} in any two out of four loops with the P-4 interlock active.

The MFW regulation valve closure signal initiates closure of all MFW regulation valves.

Main Feedwater Isolation

An ESF actuation signal for MFW isolation is generated when any of the following signals are present.

- Manual actuation,
- ECCS actuation, and
- High-high SG water level (high-high water level in any of the SGs).

The bypass signal from the MFW isolation bypass control switch (operating bypass) can be activated only when the pressurizer pressure P-11 interlock is present (i.e., when the pressurizer pressure signal is lower than the P-11 setpoint). This operating bypass is automatically removed on deactivation of the P-11 interlock (i.e., when the pressurizer pressure signal is above the P-11 setpoint). This bypass function bypasses the MFW isolation signal for all MFW pumps, all MFW isolation valves, and all SG water filling control valves.

A signal for MFW isolation initiates the following:

- Trip all MFW pumps,
- Close all MFW isolation valves,
- Close all SG water filling control valves,
- Close all MFW bypass regulation valves, and
- Close all MFW regulation valves.

The actuation signals to trip the nonsafety-related MFW pumps are electrically isolated in the SLS via power interface modules.

8.4.2.9 Emergency Feedwater Actuation

An ESF actuation signal for EFW actuation is generated when any of the following initiating signals are present.

- Manual actuation,

- Low SG water level (low water level in any SG, based on two out of four signals),

- ECCS actuation,

- LOOP signal, and

- MFW pumps trip. EFW actuation on a trip of all MFW pumps is an anticipatory function that is not credited in the safety analysis. Therefore, this is not a safety function, but it is designed to be highly reliable. Isolation is provided within the PSMS for this function. Redundant trip signals for each MFW pump are interfaced from the PCMS to the PSMS via the unit bus. Since these nonsafety signals can only result in a safety actuation, there is no potential for adverse interaction with the safety function. Since actuation requires signals from all four MFW pumps, there is minimal potential for spurious actuation.

An EFW actuation signal initiates the following:

- Starting EFW pumps. The train A actuating signal starts the train A EFW pump. Likewise, trains B through D start their corresponding EFW pumps.

- Closing the SG blowdown isolation valves and sample line valves of all SGs.

- Opening EFW isolation valves.

8.4.2.10 Emergency Feedwater Isolation

There are four emergency feedwater isolation signals, one for each loop (SG). The following description is for loop A. All loops are identical.

There are two separate ESFAS trains for the emergency feedwater isolation valves for each SG (there are two isolation valves per SG).

An ESF actuation signal for emergency feedwater isolation (loop A) is generated when any of the following initiating signals are present.

- Manual actuation;

- Loop A low main steam line pressure, generated when two out of four main steam line pressure signals from SG A indicate low pressure, there is no low main steam line pressure EFW isolation block signal from any other SG loop (B, C, or D), and there is no EFW bypass control (operating bypass); and

- Loop A high SG water level, generated when there are two out of four high SG water level signals from SG A (with time delay), there is no loop A low main steam line pressure signal, the reactor is tripped (the P-4 interlock is active) and there is no EFW isolation bypass control (operating bypass).

The EFW isolation bypass control can be manually actuated when the low pressurizer pressure P-11 interlock is present. This operating bypass is automatically removed by the P-11 interlock when pressurizer pressure rises above the P-11 setpoint. The EFW isolation bypass control is common to all SG loops, whereas there are separate EFW isolation bypass controls for each ESFAS train.

8.4.2.11 CVCS Isolation

There are two ESFAS trains for chemical and volume control system (CVCS) isolation, train A and train D.

The ESF actuation signal for the CVCS isolation function is generated when any of the following initiating signals are present. The signal is latched.

- Manual actuation, and

- High pressurizer water level, generated when two out of four signals are present for high pressurizer water level, and the high pressurizer water level CVCS isolation bypass control (operating bypass) is not present.

The CVCS isolation bypass control (operating bypass) can only be actuated when the P-11 interlock is active. This operating bypass is automatically removed by the P-11 interlock when pressurizer pressure rises above the P-11 setpoint.

8.4.3 Bypasses and Overrides

Automatic and manual operating bypasses are provided to block certain protective actions that would otherwise prevent modes of operations such as startup. Automatic and manual bypasses are described in the following subsections.

8.4.3.1 Automatic Operating Bypasses

These operating bypasses are automatically initiated separately within each PSMS division when the plant process permissive condition is sensed by the PSMS input channel(s). The following is a list of automatically initiated operating bypasses:

- The high main steam line pressure negative rate initiating signal for main steam line isolation is automatically bypassed when the P-11 interlock clears (when pressurizer pressure is above the setpoint). This bypass can be manually removed when P-11 is present (pressurizer pressure is below the setpoint).
- When the P-4 interlock is absent (RTBs closed) the low T_{avg} initiating signal for main feedwater isolation (for closing all main feedwater valves) is automatically bypassed. This operating bypass is automatically removed when the P-4 interlock is present (RTBs open).

8.4.3.2 Manual Operating Bypasses

Some operating bypasses must be manually initiated. These operating bypasses can be manually initiated separately within each PSMS train when the plant process permissive condition is sensed by the PSMS input channel(s). The following is a list of manually initiated operating bypasses:

- The low pressurizer pressure initiating signal for the ECCS actuation function can be manually bypassed only when the P-11 interlock is present (pressurizer pressure is below the setpoint). This operating bypass is automatically removed when the P-11 interlock clears (when pressurizer pressure is above the setpoint).

- The low main steam line pressure initiating signal for the ECCS actuation function and main steam line isolation function can be manually bypassed only when the P-11 interlock is present (pressurizer pressure is below the setpoint). This operating bypass is automatically removed when the P-11 interlock clears. When this operating bypass is active, the high main steam line pressure negative rate trip is enabled.

- The MFW isolation function can be bypassed manually only when the P-11 interlock is present. This operating bypass is automatically removed when the P-11 interlock clears.

- The EFW isolation function actuated by low main steam line pressure can be manually bypassed if the P-11 interlock is present. This operating bypass is automatically removed when the P-11 interlock clears.

- The manual bypass for the high pressurizer water level initiation signal for CVCS isolation can only be actuated when the P-11 interlock is present. This operating bypass is automatically removed when the P-11 interlock clears.

All operating bypasses, either manually or automatically initiated, are automatically removed when the plant moves to an operating condition for which the protective action would be required if an accident occurred. Status indication is provided in the MCR for all operating bypasses.

8.4.3.3 Manual Overrides

Manual overrides must be manually initiated. These manual overrides can be manually initiated separately within each PSMS train when the plant process permissive condition is sensed by the PSMS input channel(s). The following is a list of train-level manually initiated overrides:

- An ECCS actuation can be manually overridden at the train level when the P- 4 interlock is present (RTBs open). This manual override is automatically removed when the P-4 interlock clears (RTBs closed).

- The block cooldown turbine bypass valve actuation by low-low T_{avg} may be manually overridden at the system level. This manual override cannot be initiated until after automatic system-level actuation. The manual override may be manually reset by the operator at any time, and it is automatically reset when the low-low T_{avg} initiation signal returns to normal. This signal blocks the "cooldown" turbine bypass valves.

8.5 Control Systems

8.5.1 Introduction

The function of the US-APWR control systems not required for safety is to establish and maintain the plant operating conditions within prescribed limits. These control systems improve plant safety by minimizing the frequency of required protection responses and relieve the operator from routine tasks.

The control functions not required for safety are implemented by the PCMS. The PCMS regulates conditions in the plant automatically in response to changing plant conditions and changes in plant load demand. These operating conditions include the following:

- Step load changes of plus or minus 10% while operating in the range of 15 to 100% of full power,

- Ramp load changes of plus or minus 5% per minute while operating in the range of 15 to 100% of full power (subject to core power distribution limits), and

- Full load rejection from 100% power.

These capabilities are accomplished without a reactor trip. A full load rejection is an event in which the main generator is cut off from the transmission system by a tripping of the main transformer breaker or the switchgear breaker without causing a turbine trip. In a load rejection scenario, the turbine governor valves are immediately fully closed, and the turbine bypass valves are opened fully, dumping the excess steam to the condenser. Reactor power is decreased by the automatic insertion of the control rods.

The PCMS and PSMS utilize the same basic software, and both utilize the MELTAC digital platform. Maximum utilization of a common digital platform throughout a nuclear plant reduces maintenance, training, and changes due to obsolescence, thereby minimizing the potential for human error. The potential for common-cause failure (CCF) in these systems is minimized by the following:

- Simplicity of the basic design,
- Maturity of the MELTAC platform,
- Design processes, including the elevated quality programs, applied to both systems, and
- Significant functional diversity within the numerous computers that compose these systems.

Regardless of this very low potential for CCF, the DAS is provided to accommodate beyond-design-basis CCFs that could adversely affect the PSMS and PCMS concurrent with an AOO or PA.

8.5.2 Control System Descriptions

The following sections describe the US-APWR control functions not required for safety that can affect the performance of the critical safety functions. The rod control system, pressurizer pressure control system, pressurizer water level control system, steam generator water level control system, and turbine bypass control system are all considered to be parts of the reactor control system shown in Figure 8-1.

8.5.2.1 Rod Control System

The rod control function controls the reactor coolant average temperature (T_{avg}) by sending control signals to the CRDM control system to adjust control rod bank positions. For any RCS loop, the T_{avg} is the average value of the reactor coolant hot-leg and cold-leg temperatures.

The difference between (1) the programmed reference temperature (which is based on turbine inlet pressure) and (2) the selected lead/lag compensated value of the T_{avg} signal from one of the four reactor coolant loops becomes the primary demand signal for rod control. This primary demand signal is further varied using an additional control input signal, which is derived from the reactor power versus turbine load mismatch. This mismatch signal improves system performance by enhancing response and reducing transient peaks. The programmed coolant temperature increases linearly with turbine load from the zero-power to the full-power condition. As the temperature difference increases, the demanded rod speed also increases.

A deadband is included in the system to preclude rod motion when the temperature error is within the deadband.

The T_{avg} input signals for the rod control function are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains, corresponding to each RPS loop, are processed through the signal select algorithm (SSA) within the PCMS before being used for the rod control function.

The output signals from the rod control function of the PCMS are interfaced to the CRDM control system via the data links.

The PCMS provides the following HSI signals for the rod control function:

- Rod control auto/manual - Allows transfer between the automatic control mode of the control rod control banks by the rod control system and the manual control mode.

- Control rod bank selector - Allows selection of the desired control rod bank for manual motion demand when in the manual mode.

- Control rod lift coil disconnection selector - Allows the interruption of lift coil power for a selected control rod for certain test and maintenance conditions.

- Rods out/in - Allows manual control of control rod banks and individual control rods at a fixed speed when in the manual mode.

Interlocks

Interlocks are provided to prevent abnormal power and temperature conditions that could result from excessive control rod withdrawal initiated either by a control system malfunction or by an operator violation of operating procedures. Refer to Table 8-7. These interlocks are generated by the following signals:

- Power range neutron flux,
- Intermediate range neutron flux,
- Overpower ΔT,
- Overtemperature ΔT,
- Turbine inlet pressure, and
- Control rod bank D position.

To generate these interlocks the PCMS receives input signals from the RPS via the unit bus. Within the PCMS, signals from each of the four RPS trains are processed through the SSA within the PCMS before being used to generate these interlocks. All interlocks block automatic or manual control rod withdrawal. These interlocks are provided from the reactor control section of the PCMS to the control rod drive mechanism control system.

Control Rod Drive Mechanism Control System

The CRDM control system in the PCMS adjusts the positions of the control rod banks in the reactor core. Each control rod bank is divided into two or more groups to obtain small incremental reactivity changes per step. The control rod groups within the same bank are moved such that the relative positions of the groups do not differ by more than one step. Each control rod in a group is paralleled so that rods of the same group move simultaneously.

Power to the CRDMs is supplied by two motor generator sets operating from two separate 480-V, three-phase buses. Each synchronous generator is driven by an induction motor. The ac power is distributed to the CRDM control system power cabinet through the RTBs.

The CRDM control system consists of a logic cabinet and a power cabinet, both located in close proximity to the CRDM motor generator sets. The PCMS controller group of the CRDM control system is located within the logic cabinet. The controller group controls solid-state CRDM power supplies that are located in the power cabinet.

Manual control is provided from the OC to move individual control rods or entire control rod banks in or out of the core. The control rod speed for manual control is fixed at approximately 48 steps per minute.

The CRDM control system provides control for control rod shutdown banks and control rod control banks. The four control rod shutdown banks are manually withdrawn to the full-out position prior to the reactor becoming critical. The control rod shutdown banks are always in the fully withdrawn position until the reactor is tripped or shut down. The four control rod control banks are positioned to control reactor power after the control rod shutdown banks are fully withdrawn. The control rod control banks may be manually controlled or automatically controlled by the rod control function. In the manual mode, control banks may be moved individually or in a predetermined overlap sequence. In the automatic mode, the control banks are withdrawn or inserted in the same predetermined overlapped sequence.

The following is a summary of the control rod control bank sequencing characteristics:

- The control rod control banks are programmed so that rod withdrawal is sequenced in a predetermined order. The programmed insertion sequence is the opposite of the withdrawal sequence. That is, the last inserted bank will be the first withdrawn.

- The control rod control bank withdrawals are programmed such that, when the first bank reaches a preset position, the next bank begins to move out simultaneously with the first bank. This preset position is predetermined by the maximum allowable overlap between the banks. This withdrawal sequence continues until the reactor reaches a desired power level. The control bank insertion sequence is the opposite of the withdrawal sequence.

- Overlap between successive control rod control banks is adjustable from 0 to 50%.

While in the automatic mode, the rod control function can vary the rod speed demand. The variable speed control function allows small changes in reactivity at low speed. This permits fine control of reactor coolant temperature. The variable speed control function allows large changes in reactivity at high speed. This permits control of reactor coolant temperature for transients such as large load rejections.

An RT signal opens the RTBs, thereby causing the control rod shutdown banks and the control rod control banks to fall into the core by gravity.

The CRDM control system generates control rod position demand signals for display on operational VDUs. The demand position accuracy is ± 0 steps. This zero-step accuracy is due to the fact that the demand is generated in the digital controller in the control system, and the readout is indicated in the operational VDU through the unit bus. The CRDM control system counts the motion demand signals during bank or individual rod motion to provide a digital readout of the demanded position. The control rod position demand signals are used to generate alarms for incorrect control bank overlap and sequencing, and control rod bank insertion limit alarms.

Control Rod Bank Insertion Limit Alarms

The PCMS generates control rod bank insertion limit alarms to alert the operator to excessive rod insertion. The alarms prompt the operator to manually terminate rod insertion and possibly to adjust the required boron concentration of the reactor coolant. The control rod bank insertion limit alarm setpoints ensure sufficient core reactivity shutdown margin following an RT to accommodate all accident conditions.

The following two control rod bank insertion limit alarms are provided for each control rod control bank:

- A "low" alarm warns the operator that the rod insertion limits are being approached, and

- A "low-low" alarm warns the operator that the rod insertion limits have been reached.

The control rod bank insertion limit alarm setpoints are calculated from reactor power, as measured by the core ΔT. The control rod bank demand position is compared to the respective alarm setpoints.

These alarm limits ensure that an adequate shutdown margin is maintained for all accident conditions. The control rod insertion limit alarm setpoint also provides a limit on the maximum inserted rod worth for the hypothetical rod ejection event. Insertion limits provide confidence that acceptable nuclear peaking factors are always maintained. The allowable rod insertion limits are increased (the rods must be withdrawn further) with increasing power because the amount of shutdown reactivity required for the design shutdown margin following a reactor trip increases with increasing power.

The reactor control system in the PCMS receives rod position signals from the CRDM control system based on control rod demand position. ΔT input signals for control rod bank insertion limits are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS divisions, corresponding to each RPS loop, are processed through the SSA within the PCMS before being used for control rod bank insertion limits.

Control Rod Position Monitoring

The reactor control system in the PCMS receives signals from the rod position indication (RPI) system. The RPI system provides individual position indication for each control rod. The RPI system measures the position of each control rod using a detector consisting of discrete coils mounted outside the control rod pressure housing. These coils are located axially along the pressure housing. The RPI coils magnetically sense the movement of the rod drive shaft. The accuracy of the digital RPI is ± 12 steps.

Alarms are generated if any control rod shutdown bank is detected to have left its fully withdrawn position, or if any control rods are detected at the bottom position, except as part of the normal insertion sequence. An alarm is also generated whenever the position of an individual rod deviates from the other rods in the bank by a preset limit. The alarm is set to accommodate appropriate core design limits, including an allowance for instrument error.

8.5.2.2 Pressurizer Pressure Control System

The pressurizer pressure control function maintains the pressurizer pressure at its nominal operating value during normal operation and transients.

During normal plant operation, the primary system pressure is monitored and controlled to prevent pressure from increasing to a limit where actuation of the PSMS is required to prevent design limits from being encroached. Additionally, the primary system pressure is prevented from decreasing to a value that may encroach on thermal design limits.

The pressurizer pressure control function is designed to provide the stable and accurate control of pressure at its predetermined setpoint. Small or slowly varying changes in pressure are regulated by modulation of the proportional heaters. Reset (integral) action is included to maintain pressure at its setpoint. A fast pressure increase is controlled by reducing the proportional heater output and by actuating pressurizer spray. Spray continues until pressure decreases to a point at which the proportional heaters alone can regulate pressure.

For normal transients, including a full load rejection, the pressurizer pressure control function acts promptly to prevent pressurizer pressure from reaching the high pressure RT setpoint. A decrease in pressure, greater than that which can be handled by the proportional heaters only, results in the actuation of the backup heaters. These backup heaters are switched off automatically when the proportional heaters alone are able to restore the pressure to setpoint. During normal steady-state plant operation, proportional heater output is regulated to compensate for

pressurizer heat loss. During normal transient operation, the pressure is regulated to provide adequate margin to actuation of ESF systems or a reactor trip.

The automatic pressure control function can be manually selected by the operator when nominal pressure is established during plant startup. The automatic pressure control function can be maintained from 0 to 100% power.

Pressurizer pressure input signals for pressurizer pressure control are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains are processed through the SSA within the PCMS before being used for the pressurizer pressure control function. Pressurizer pressure control function output signals are provided from the PCMS to switchgear for the backup heaters, power controllers for the proportional heaters, and electropneumatic positioners for the pressurizer spray valves.

8.5.2.3 Pressurizer Water Level Control System

The pressurizer water level control function maintains pressurizer water level at its programmed value. The programmed value is determined as a function of reactor coolant T_{avg} to minimize charging and letdown control operations. This arrangement minimizes potential challenges to protection system actuation during normal operational transients.

The pressurizer provides a reservoir for the RCS inventory changes that occur due to changes in reactor coolant density. As the reactor coolant temperature is increased from hot zero-load to full-load values, the RCS fluid expands. The pressurizer water level control system adjusts letdown and charging flow to allow the pressurizer to absorb this change.

The pressurizer water level control function provides a stable and accurate method of pressurizer water level control at the prescribed setpoint value, which is programmed with T_{avg}. Automatic level control may be manually selected at the point in the startup evolution at which the hot zero-load level is established. Automatic pressurizer water level control can be maintained from 0 to 100% power.

The pressurizer water level input signals for pressurizer water level control are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains are processed through the SSA within the PCMS before being used for the pressurizer water level control function. Tavg input signals for pressurizer water level control are also interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains, corresponding to each RPS loop, are processed through the SSA within the PCMS before being used for pressurizer water level control. The pressurizer water level control function output signals are provided from the PCMS to electropneumatic positioners for the charging flow control valve.

8.5.2.4 Steam Generator Water Level Control System

The water levels in the shell sides of the steam generators are maintained by the SG water level control function at a predetermined setpoint. During normal plant transients, the SG water level is controlled to prevent an undesirable reactor trip.

Three modes of the SG water level control function are provided:

- During normal power operation, three-element feedwater control regulates MFW flow into each SG via the MFW line with the MFW regulation valve by continuously comparing the SG water level signal to the fixed level reference, and by comparing the MFW flow signal to the steam flow signal.

- During low-power operation, two-element feedwater control regulates MFW flow into each SG with the MFW bypass regulation valve (bypassing the MFW regulation valve) by continuously comparing the SG water level signal to the fixed level reference, and by adding the level error to the reactor coolant ΔT

- During hot standby operation, single-element feedwater control regulates MFW flow into each SG with the SG water filling control valve (bypassing both the MFW regulation valve and the MFW bypass regulation valve) by continuously comparing the SG water level signal to the fixed level reference.

The transition from the MFW bypass regulation valve to the MFW regulation valve during low-power startup operation, or the transition from the MFW regulation valve to the MFW bypass regulation valve during low power shutdown operation, can be done automatically or manually. Tracking is provided to allow a smooth transition between manual and automatic control. The transition from the SG water filling control valve to the MFW bypass regulation valve during low-power startup operation is manual.

The SG water level control function is separate for each SG; the following description is applicable to each SG:

The SG water level input signals for the SG water level control function are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains are processed through the SSA within the PCMS before being used for SG water level control. ΔT input signals for the SG water level control function are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains, corresponding to each RPS loop, are processed through the SSA within the PCMS before being used for the SG water level control function.

Redundant main steam flow and MFW flow input signals are interfaced directly to the PCMS. For main steam line flow, the PCMS validates these signals by cross-checking the signals between two SG loops. For MFW flow, the PCMS validates these signals by cross-checking to the main steam line flow in the same loop. After the input signals are validated, the PCMS selects the higher of the two valid inputs for use in the SG water level control function. Inputs determined to be invalid are not included in this selection.

The SG water level control function output signals are provided from the reactor control system in the PCMS to electropneumatic positioners for all MFW regulation valves described above.

8.5.2.5 Turbine Bypass Control System

During startup and shutdown conditions, when steam flow is blocked to the main turbine generator, the turbine bypass control function is used to bypass steam to the condenser. During normal operation, the turbine bypass control function is in a standby condition to modulate the bypass valves to maintain T_{avg}. Following a sudden loss of load, the turbine bypass control function prevents a reactor trip by opening the turbine bypass valves to dump excess steam from the SGs to the condenser. For all operating modes, the turbine bypass control function prevents lifting the main steam safety valves. The functional operation of the turbine bypass control system for each plant operating mode is described in the following sections.

The turbine bypass control function input signals for turbine inlet pressure, T_{avg}, and power range neutron flux are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains are processed through the SSA within the PCMS before being used for the turbine bypass control function. Also, the turbine bypass control function input signals for the turbine trip signal are interfaced from the RPS to the PCMS via the unit bus.

The turbine bypass control function input signals for steam header pressure signals, condenser available signals, and condensate booster pump status are interfaced directly from nonsafety field instrumentation to the PCMS.

The turbine bypass control function output signals are provided from the reactor control system in the PCMS to electropneumatic positioners and trip-open solenoids for the turbine bypass valves.

Plant Startup and Shutdown

During a plant startup or shutdown, the difference between measured steam header pressure and a pressure setpoint is used to generate a turbine bypass demand signal. This mode is used for low-power conditions (up through turbine synchronization). This mode is also used during a plant cooldown for decay heat removal between hot standby and entry conditions for the RHR system.

The steam header pressure control mode is manually selected by the operator. The pressure setpoint is manually adjusted by the operator to obtain the desired reactor coolant temperature.

Normal Operation

In this mode, the turbine bypass control function is in a standby condition. Once actuated, the system modulates the turbine bypass valves to control T_{avg} at a reference temperature derived from turbine inlet pressure.

Load Rejection

The US-APWR is designed to sustain a full load rejection without generating an RT, opening atmospheric steam relief valves, or actuating pressurizer or main steam line safety relief valve(s).

A full load rejection is an event in which the main generator is cut off from the transmission system by tripping either the main transformer breaker or the switchgear breaker without causing a turbine trip or a main generator trip. In this scenario, the main turbine control valves are immediately fully closed, and four banks of turbine bypass valves are tripped opened to fully dump excess steam to the condenser.

During such an event, reactor power is decreased by automatic insertion of control rods. The automatic turbine bypass control function, in conjunction with other control systems, is provided to accommodate this abnormal load rejection and to reduce the effects of the transient imposed on the RCS. By bypassing main steam to the condenser, an artificial load is maintained on the primary system. This artificial load makes up the difference between the reactor power and the turbine load for load rejections.

The turbine bypass control function is sized to pass approximately 68% of nominal steam flow at nominal steam pressure. This capacity, in conjunction with the response of the rod control system, is sufficient to handle load rejections equivalent to a step load decrease of 100% of the rated load.

The turbine bypass control function prevents a large increase in reactor coolant temperature following a large, sudden load decrease. The error signal is the sum of (1) the difference between the lead-lag compensated selected T_{avg} and the reference T_{avg} (designated as T_{ref}), which is based on turbine inlet pressure, and (2) the difference between the nuclear power signal and the turbine inlet pressure. The lead-lag compensation for the T_{avg} signal compensates for lags in the plant thermal response and in valve positioning. The addition of the difference between the nuclear power signal and the turbine inlet pressure with a rate-lag compensation allows for a decrease in gain in the load rejection controller, thereby increasing stability.

Following a sudden load decrease, T_{ref} and turbine inlet pressure immediately decrease, and T_{avg} tends to increase. This generates an immediate demand signal for the turbine bypass control function. Following the initial trip opening, the error signal reduces in magnitude, indicating that the T_{avg} is reduced toward the reference T_{avg} and that power range neuron flux is reduced by the insertion of control rods. At this point, the turbine bypass valves are modulated in the closed direction, and the rod control function commands the control rods to insert in a controlled manner to reduce the reactor power to match the turbine load. On a load rejection resulting in a turbine runback, the turbine bypass terminates when (1) the reactor power matches the turbine load and (2) the temperature error is within the maneuvering capability of the control rods. On a grid disconnect, the turbine bypass control function modulates the bypass valves in the closed direction in response to the control rods reducing nuclear power to approximately 15% power. At this point, the rod control function is transferred to the manual mode, the operator maintains nuclear power, and the plant stabilizes in preparation for a turbine-generator restart and/or grid synchronization with the turbine bypass valves partially open.

Turbine Trip

For the US-APWR, a turbine trip leads to a reactor trip, and a reactor trip leads to a turbine trip. Following a turbine trip, the load rejection control function is defeated, and the turbine trip control function becomes active. The demand signal for the turbine bypass control function is the error signal between the lead-lag compensated T_{avg} and the no-load reference T_{avg}. When the error signal exceeds a predetermined setpoint, two banks of the turbine bypass valves are tripped opened in a prescribed sequence. As the error signal reduces in magnitude, indicating that the T_{avg} is being reduced toward the reference no-load value, the turbine bypass valves are modulated in the closed direction. This action regulates the rate of decay heat removal and establishes the equilibrium hot shutdown condition.

Turbine Bypass Interlocks

Low-low T_{avg} turbine bypass block: The turbine bypass control functions are prevented by this interlock from the PSMS, in which SLS trains A and D control redundant non-Class 1E permissive solenoids on each turbine bypass valve. An excessive primary cooldown is blocked by this function.

Loss-of-load interlock: The actuation of turbine bypass on small load perturbations is prevented by an independent load rejection sensing circuit. This circuit senses the rate of decrease in the turbine load as detected by turbine inlet pressure. It unblocks the turbine bypass valves only when the rate of load rejection exceeds the preset values corresponding to a 10% step load decrease or a sustained ramp load decrease of 5% per minute. The unblocking of the turbine bypass valves is latched to enable the load rejection operating mode. This latch is manually reset by the operator after plant stabilization using the loss-of-load reset switch.

Condenser-not-available interlock: This nonsafety interlock is implemented in the PSMS to simplify the interface with the non-Class 1E turbine bypass valve permissive solenoids used for the T_{avg} interlock described above. Turbine bypass valve permissive solenoids are controlled by the PSMS to achieve a high reliability for blocking the turbine bypass function

These interlocks improve the potential for preventing inadvertent turbine bypass actuations that may be generated due to failures in the PCMS turbine bypass control group.

8.5.2.6 Turbine Electrohydraulic Governor Control System

The turbine electrohydraulic governor control system (EHGS) in the PCMS provides the following functions for control of the turbine generator:

- Speed control,
- Load control,
- Overspeed protection, and
- Automatic turbine startup control.

8.6 Diverse Actuation System

8.6.1 Overview

The DAS is the nonsafety diverse instrumentation and control system for the US-APWR design. The DAS provides monitoring, control, and actuation of safety and nonsafety systems required to cope with abnormal plant conditions concurrent with a CCF that disables all functions of the PSMS and the PCMS. The DAS includes an automatic actuation function, HSI functions located at the diverse HSI panel (DHP), and interfaces with the PSMS and the PCMS. The DAS can be used to maintain all critical safety functions and to achieve hot standby.

The DAS design consists of conventional equipment that is totally diverse and independent from the MELTAC platforms of the PSMS and PCMS, so that a beyond-design-basis CCF in these digital systems will not impair the DAS functions. In addition, the DAS includes internal redundancy to prevent spurious actuation of automatic and manual functions due to a single component failure. The DAS is also designed to prevent spurious actuations due to postulated earthquakes and postulated fires. The DAS interfaces with the safety process inputs and outputs of the SLS are isolated within these safety systems. In addition, hardwired Class 1E logic within the SLS (not affected by a CCF) ensures that control commands which correspond to the desired safety function always have priority, regardless of where they originate (DAS or SLS). Therefore, there is no adverse interaction of the DAS with safety functions and no erroneous signals resulting from a CCF in the SLS that can prevent the safety function.

Within the DAS, manual actuation is provided for systems which maintain all critical safety functions (refer to Table 8-8). For conditions in which there is insufficient time for manual operator action, the DAS provides automatic actuation of the required plant safety functions needed for accident mitigation. Key parameter indications, diverse audible and visual alarms, and provisions for manual controls are located in a dedicated independent DHP located in the MCR. Conventional hardwired logic hardware and relays for automatic actuation are installed in two diverse automatic actuation cabinets (DAACs), each located in a separate room. Each DAAC is powered by a separate non-Class 1E uninterruptible power supply (UPS). During plant on-line operation, the system can be tested manually without causing component actuation that would disturb plant operations.

Since the DAS is a nonsafety system, it does not need to meet the single-failure criterion for actuation. The DAS subsystems are arranged in a two-out-of-two configuration to ensure that the DAS can sustain one random component failure without spurious actuation of either manual or automatic functions. A spurious actuation of a single component due to a single failure in an SLS power interface module has been considered in the plant safety analysis.

The two DAAC subsystems actuate all required plant components to achieve the required safety function. With regard to the number of actuated plant components, the DAS design generally does not consider additional single failures. For example, for a given set of containment isolation valves, only one of the two valves is actuated. This nonredundant configuration is considered in determining the

allowable out-of-service time for plant equipment in the technical specifications. However, the numbers of safety injection and EFW pumps started by the DAS do consider an out-of-service condition. In addition, unavailability of the main steam depressurization valve of an impaired steam line is considered. The DAS actuates all four safety injection or EFW pumps and opens all four main steam depressurization valves for operability, while three constitutes the minimum required.

8.6.2 System Description

The DAS consists of manual HSI functions and automatic actuation functions. These functions are located in the DHP and the DAACs, respectively. In addition, the DAS includes interfacing connections with the PSMS and CRDM motor generator sets. The DAS receives inputs from qualified analog isolators located in the RPS or directly from plant components. The DAS provides outputs which interface to the SLS power interface modules via qualified isolators located in the SLS or directly to plant components.

Once actuated, either manually or automatically, the DAS signals are latched at the system level. This feature ensures that all DAS functions actuate to completion. The DAS latches can be reset from the defeat switch located on the OC.

8.6.2.1 Diverse HSI Panel

The DHP, located in the MCR, consists of conventional hardwired switches, conventional indicators for key parameters of all critical safety functions, and audible and visual alarms. The DHP-installed equipment is used for manual control and actuations credited in the defense-in-depth and diversity coping analysis. The actuation status of each safety system actuated from the DHP can be confirmed by monitoring the safety function process parameters displayed on the DHP. The DHP is powered by a non-Class 1E UPS.

Manual Actuation Switches

System-level manual actuation is provided on the DHP for all automated functions and for systems required to maintain critical safety functions, which may not be automatically actuated. The following manual actuations are provided from conventional switches on the DHP (see Table 8-8, Figure 8-8):

- Reactor trip/turbine trip/MFW isolation: one switch,
- EFW actuation: one switch,
- ECCS: one switch,
- Containment isolation: one switch,
- EFW isolation and flow control: four switches (one per SG),
- Control of main steam depressurization valves: four switches (one per SG), and
- Control of safety depressurization valve: one switch.

To prevent spurious actuation due to a failure of any of the above switches, a separate manual actuation permissive switch is provided. This is referred to as the “Permissive Switch for DAS HSI.” The permissive switch is located in the MCR, but it is physically separated from the DHP to minimize the effects of fire propagation.

The DAS permissive switch is powered by a non-Class 1E UPS that is separate from the power to the DHP. Signals from the manual actuation switches and the permissive switch are interfaced separately from the MCR to each DAAC. To prevent spurious DAS actuation due to an MCR fire, all DAS manual actuation signals are blocked when the MCR/RSR transfer is activated.

The manual actuation switches listed above provide the capability to maintain all critical safety functions and to achieve hot standby. Hot standby can be maintained for an extended period of time by direct operation of local power distribution and switching devices that are not affected by the CCF in the PSMS.

Alarms

When the DAS system-level actuation signal is generated for (1) reactor trip, turbine trip, and MFW isolation, or (2) EFW actuation, a summary alarm for the actuated functions is also actuated on the DHP. The diverse audible alarm is activated to notify the operators. The first-out alarm panel on the DHP indicates the specific input parameter that has caused the system-level actuation.

Failure information about the DAS, such as power supply failure or module de-energization or removal, is alarmed as a “DAS failure summary alarm” on the alarm VDU in the MCR. The DHP also provides a summary alarm for RCS leakage as described below. High main steam radiation (N-16) and high-high steam generator water level are alarmed and indicated on the DHP.

Indicators

The analog indicators provided on the DHP are sufficient to support all manual control actions which provide the capability to maintain all critical safety functions and to achieve and maintain hot standby.

8.6.2.2 Diverse Automatic Actuation Cabinets

Each DAAC provides for the automatic actuation of critical systems, which are required to be actuated within 10 minutes of event initiation. The defense-in-depth and diversity coping analysis provides justification for manual operator actions credited after 10 minutes.

Safety sensors selected for DAS input are interfaced from within the PSMS or PCMS input modules. These input modules utilize analog distribution modules and isolation modules that connect the input signals to the DAS prior to any digital processing. Therefore, a software CCF within the PSMS or PCMS does not affect the DAS automation function or the display of plant parameters on the DHP.

The DAS has two analog-logic subsystems; each is located in one of the two DAACs. Within each DAAC, input signals are compared to their setpoint values. If a monitored value exceeds its setpoint, a partial trip/actuation signal is generated. RT signals and/or ESF actuation signals are generated from each DAAC through the two-out-of-four voting logic performed on its input signals.

The DAS actuation signals from both DAAC subsystems are configured at their destination using two-out-of-two voting to execute an RT or actuation of ESF systems.

The monitored signals are isolated from the PSMS and interfaced to the separate subsystem in each DAAC. The process variables monitored for automatic actuation functions are (1) pressurizer pressure (4 channels each for low and high pressure signals) and (2) SG water level (4 channels, one per SG for low level signals).

The numbers of channels required for each automatic actuation function are based on the following considerations:

- No single failure spuriously actuates the DAS.

- Unlimited bypass of a single channel does not cause the DAS automatic function to be inoperable, prevent decisions regarding credited manual actions, or prevent the monitoring of critical safety functions.

The defeat switch can be manually actuated during plant heatup or cooldown conditions to prevent actuation of the DAS when it is not needed. This is an administratively controlled operating bypass.
The DAACs are located in separate Class 1E electrical rooms and qualified as Seismic Category II.

Reactor Trip, Turbine Trip and Main Feedwater Isolation

The reactor and turbine are tripped, and MFW isolation is automatically actuated by the following signals:

- Low pressurizer pressure: two-out-of-four voting logic of the four pressurizer pressure low signals,

- High pressurizer pressure: two-out-of-four voting logic of the four pressurizer pressure high signals, and

- Low SG water level: two-out-of-four voting logic of the four SG water level low signals, one from each SG.

These automatic actuations are illustrated in the DAS functional diagram, Figure 8-8.

Each of the four pressurizer pressure signals is interfaced from one of the four PSMS trains. This configuration allows the DAS to meet the target reliability of the probabilistic risk assessment with one channel continuously bypassed or inoperable.

To support the single-failure criterion for all PSMS functions, there are four SG water level signals (one per train) for each SG. However, for the DAS, which does not need to meet the single-failure criterion, only one water level signal is required from each SG.

The reactor trip is actuated by tripping the nonsafety CRDM motor generator sets. This action de-energizes the CRDMs by a means that is diverse from opening the RTBs and thereby releases the control rods for gravity insertion into the reactor core. Diversity from the PSMS is maintained from sensor inputs to final actuators.
The turbine trip is actuated by opening the solenoid valves for turbine trip. Diversity from the RT function in the PSMS is maintained from sensor inputs up to the power interface modules.

The MFW isolation is actuated by closing the MFW regulation valves. Diversity from the feedwater isolation function in the PSMS is maintained from sensor inputs up to the power interface modules.

These DAS actuation functions are automatically blocked when both of the following conditions are established:

- Status signals are received indicating that the minimum combination of RTBs have opened for the RT function. This is referred to as the P-4 interlock. The logic for the P-4 interlock is the same as in the PSMS. The P-4 interlock is processed independently in each DAAC. Signals from all RTBs are interfaced from the PSMS, prior to any software processing, to each DAAC.

- The turbine trip signal, based on low emergency trip oil pressure, is generated.

Emergency Feedwater Actuation

EFW is automatically actuated on a low SG water level signal. Two-out-of-four voting logic is utilized for the low SG water level signals, one from each SG. This automatic actuation is illustrated in the DAS functional diagram, Figure 8-8.

The interfaces and configuration of the SG water level signals is as described above. Diversity from the EFW actuation function in the PSMS is maintained from sensor inputs to the power interface modules. This automatic DAS EFW function is automatically blocked when status signals are received indicating that the PSMS EFW function has actuated correctly. Correct actuation is indicated when two out of four status signals are received from limit-switch contacts on the steam inlet valves to the turbine-driven EFW pumps and from auxiliary contacts on the motor starters controlling the motor-driven EFW pumps. The EFW pump status signals are interfaced from the PSMS, prior to any software processing, to each DAAC.

Table 8-1 Reactor Trip Signals

Actuation Signal	Number of Sensors, Switches, or Signals	Division Trip Actuation Logic	Permissives and Bypasses
High Source Range Neutron Flux	2 Neutron Detectors	1/2	P-6, P-10
High Intermediate Range Neutron Flux	2 Neutron Detectors	1/2	P-10
High Power Range Neutron Flux (low setpoint)	4 Neutron Detectors	2/4	P-10
High Power Range Neutron Flux (high setpoint)		2/4	None
High Power Range Neutron Flux Positive Rate		2/4	None
High Power Range Neutron Flux Negative Rate		2/4	None
Over Temperature Δ T	1 Composite Signal per RCS Loop	2/4	None
Over Power Δ T	1 Composite Signal per RCS Loop	2/4	None
Low Reactor Coolant Flow	4 Flow Sensors per RCS Loop	2/4 per RCS Loop	P-7
Low RCP Speed	1 Speed Sensor per RCP	2/4	P-7
Low Pressurizer Pressure	4 Pressure Sensors	2/4	P-7
High Pressurizer Pressure		2/4	None
High Pressurizer Water Level	4 Level Sensors	2/4	P-7
Low SG Water Level	4 Level Sensors per SG	2/4 per SG	None
High-High SG Water Level		2/4 per SG	P-7
Manual Reactor Trip	1 Switch per Train	1/1	None
ECCS Actuation	Valid Signal	N/A	None
Turbine Trip	Valid Signal	N/A	P-7

Table 8-2 Reactor Trip Variables, Ranges, Accuracies, Response Times, and Setpoints (Nominal) (Sheet 1 of 3)

RT Function	Variables to be monitored	Range of Variables	Instrument Accuracy*1,2	Response Time*1,2	Setpoint*3
High Source Range Neutron Flux	Neutron Flux	6 decades of neutron flux	5% of span	0.6 sec	1E+5 cps
High Intermediate Range Neutron Flux	Neutron Flux	Approximately 8 decades of neutron flux overlapping source range by approximately 2 decades and including 100% RTP	10% RTP*4	0.6 sec	25% RTP
High Power Range Neutron Flux (low setpoint)	Neutron Flux	1 to 120% RTP	4% RTP	0.6 sec	25% RTP
High Power Range Neutron Flux (high setpoint)	Neutron Flux	1 to 120% RTP	4% RTP	0.6 sec	109% RTP
High Power Range Neutron Flux Positive Rate	Neutron Flux	1 to 120% RTP	2% RTP	0.6 sec	10% RTP
High Power Range Neutron Flux Negative Rate	Neutron Flux	1 to 120% RTP	2% RTP	0.6 sec	7% RTP
Over Temperature ΔT (DNB Protection) Δ T (Exit Boiling Limiting)	(a) Δ T	0 to 150%	Total 5.6% RTP Total 9.4% RTP	Total 6.0 sec Total 6.0 sec	109.8% RTP 195.9*5% RTP
	(b) Reactor Coolant Cold Leg Temperature (T_{cold})	510 to 630°F			
	(c) Reactor Coolant Hot Leg Temperature (T_{hot})	530 to 650°F			
	(d) Pressurizer Pressure	1700 to 2500 psig			
	(e) Neutron Flux (difference between top and bottom power range neutron flux detectors)	-60 to +60% (ΔI)			

Table 8-2 Reactor Trip Variables, Ranges, Accuracies, Response Times, and Setpoints (Nominal) (Sheet 2 of 3)

RT Function	Variables to be monitored	Range of Variables	Instrument Accuracy*[1,2]	Response Time*[1,2]	Setpoint*[3]
Over Power ΔT	(a) ΔT	0 to 150%	Total 5.2% RTP	Total 6.0 sec	110.6*[5]% RTP
	(b) Reactor Coolant Cold Leg Temperature (T_{cold})	510 to 630°F			
	(c) Reactor Coolant Hot Leg Temperature (T_{hot})	530 to 650°F			
	(d) Neutron Flux (difference between top and bottom power range neutron flux detectors)	-60 to +60% (ΔI)			
Low Reactor Coolant Flow	Reacter Coolant Flow	0 to 120% of rated flow	3% of rated flow	1.8 sec	90% of rated flow
Low RCP Speed	RCP Speed	0 to 120% of rated pump speed	0.5% of rated pump speed	0.6 sec	95.5% rated pump speed
Low Pressurizer Pressure	Pressurizer Pressure	1700 to 2500 psig	2.5% of span	1.8 sec	1865 psig
High Pressurizer Pressure	Pressurizer Pressure	1700 to 2500 psig	2.5% of span	1.8 sec	2385 psig
High Pressurizer Water Level	Pressurizer Water Level	0 to 100% of span	3% of span	1.8 sec	92% of span
Low SG Water Level	SG Water Level	0 to 100% of span (narrow range taps)	3% of span	1.8 sec	13% of span
High-High SG Water Level	SG Water Level	0 to 100% of span (narrow range taps)	3% of span	1.8 sec	70% of span
Manual Reactor Trip Actuation	Switch Position	N/A	N/A	N/A	N/A
ECCS Actuation	Pressurizer Pressure	1700 to 2500 psig	2.5% of span	3.3 sec	1765 psig
	Main Steam Line Pressure	0 to 1400 psig	3% of span	3.3 sec	525 psig
	Containment Pressure	-7 to 80 psig	2.8% of span	3.3 sec	6.8 psig

Table 8-2 Reactor Trip Variables, Ranges, Accuracies, Response Times, and Setpoints (Nominal) (Sheet 3 of 3)

RT Function	Variables to be monitored	Range of Variables	Instrument Accuracy*[1,2]	Response Time*[1,2]	Setpoint*[3]
Turbine Trip	Turbine Emergency Trip Oil Pressure	0 to 3500psig	2% of span	1.0 sec	1000 psig
	Main Turbine Stop Valve Position	N/A	N/A	1.0 sec	5% open

Note:
1. Instrument accuracy and response time calculation methodology refer to Subsection 7.2.2.7.
2. Instrument accuracies and response times will be decided to take into account the specification of instruments.
3. Setpoints will be adjusted to compensate for loop accuracy.
4. Rated thermal power
5. This is nominal value. Calculation formulas are shown in Figure 7.2-2 sheet 5.

Table 8-3 RT and ESF Permissives, Bypasses and Interlocks (Sheet 1 of 3)

Designation		RT and/or ESF	Function	Activation or De-activation Setpoint*[1]
P-4	Reactor Trip (RTB open)	RT, ESF	(a) Permit manual rest of ECCS to block automatic actuation of ECCS while RTBs are open. (b) Permit low T_{avg} MFW regulation valve closure. (c) Initiate turbine trip. (d) Permit high SG water level EFW isolation (e) Permit RCP trip by ECCS signal.	-
P-6	Intermediate Range Neutron Flux Above or Below Setpoint	RT	Above setpoint Permit manual operating bypass for high source range neutron flux reactor trip. Below setpoint Remove manual operating bypass for high source range neutron flux reactor trip.	1E-10 A*[2]
P-7	Turbine Inlet Pressure (P-13) or Power Range Neutron Flux (P-10) Above Setpoint or Turbine Inlet Pressure (P-13) and Power Range Neutron Flux (P-10) Below Setpoint	RT	Above setpoint (a) Remove operating bypass for low pressurizer pressure reactor trip. (b) Remove operating bypass for low reactor coolant flow reactor trip. (c) Remove operating bypass for low RCP speed reactor trip. (d) Remove operating bypass for high pressurizer water level reactor trip. (e) Remove operating bypass for high-high SG water level reactor trip. (f) Remove operating bypass for reactor trip by turbine trip. Below setpoint (a) Initiate operating bypass for low pressurizer pressure reactor trip. (b) Initiate operating bypass for low reactor coolant flow reactor trip. (c) Initiate operating bypass for low RCP speed reactor trip. (d) Initiate operating bypass for high pressurizer water level reactor trip. (e) Initiate operating bypass for high-high SG water level reactor trip. (f) Initiate operating bypass for reactor trip by turbine trip.	N/A

Table 8-3 RT and ESF Permissives, Bypasses and Interlocks (Sheet 2 of 3)

Designation		RT and/or ESF	Function	Activation or De-activation Setpoint*[1]
P-10	Power Range Neutron Flux Above or Below Setpoint	RT	Above setpoint (a) Initiate operating bypass for high source range neutron flux reactor trip. (b) Permit manual operating bypass for high intermediate range neutron flux reactor trip (c) Permit manual operating bypass for high power range neutron flux (low setpoint) reactor trip. Below setpoint (a) Permit to reset operating bypass for high source range neutron flux reactor trip. (b) Remove manual operating bypass for high intermediate range neutron flux reactor trip. (c) Remove manual operating bypass for high power range neutron flux (low setpoint) reactor trip.	10% RTP*[3]
P-11	Pressurizer Pressure Above or Below Setpoint	ESF	Below setpoint (a) Permit manual operating bypass for low pressurizer pressure ECCS actuation. (b) Permit manual operating bypass for high-high SG water level MFW isolation function for all MFW pumps, all MFW isolation valves, and all SG water filling control valves. (c) Permit manual operating bypass for high pressurizer water level CVCS isolation. (d) Permit manual operating bypass for EFW isolation. (e) Permit manual operating bypass for low main steam line pressure ECCS actuation. (f) Permit high main steam line pressure negative rate main steam line isolation function. (g) Permit manual operating bypass for low main steam line pressure main steam line isolation. Above setpoint (a) Remove manual operating bypass for low pressurizer pressure ECCS actuation. (b) Remove manual operating bypass for high-high SG water level MFW isolation function for all MFW pumps, all MFW isolation valves, and all SG water filling control valves. (c) Remove manual operating bypass for high pressurizer water level CVCS. (d) Remove manual operating bypass for EFW isolation. (e) Remove manual operating bypass for low main steam line pressure ECCS actuation. (f) Initiate operating bypass for high main steam line pressure negative rate main steam isolation.	1915 psig

Table 8-3 RT and ESF Permissives, Bypasses and Interlocks (Sheet 3 of 3)

Designation		RT and/or ESF	Function	Activation or De-activation Setpoint*[1]
P-11 (continued)	Pressurizer Pressure Above or Below Setpoint (continued)	ESF (continued)	(g) Remove manual operating bypass for low main steam line pressure main steam line isolation.	1915 psig
P-13	Turbine Inlet Pressure Below Setpoint	RT	Generate P-7 along with P-10	10% Turbine Power

Note:
1. Default lockup is 1.0% of rated value.
2. Default lockup of this value is 50% of setpoint value.
3. Default lockup of this value is 2.0% rated thermal power (RTP).

Table 8-4 Diverse Parameters in Two Separate Controller Groups

Group 1	Group 2	Remark
Over Power Δ T*[6] High Power Range Neutron Flux Rate	High Power Range Neutron Flux	Over Power Protection*[1]
Low RCP Speed Over Temperature Δ T	Low Reactor Coolant Flow Low Pressurizer Pressure	Core Heat Removal Protection*[2]
Low SG Water Level High Pressurizer Water Level	High Pressurizer Pressure	Loss of Heat Sink Protection*[3]
High Source Range Neutron Flux High Intermediate Range Neutron Flux	High Power Range Neutron Flux (Low Setpoint)	Nuclear Startup Protection*[4]
High Pressurizer Water Level	High Pressurizer Pressure	Primary Over Pressure Protection*[5]

Note:
1. Example of design basis event in the safety analysis is "Uncontrolled Control Rod Assembly Withdrawal at Power."
2. Example of design basis event in the safety analysis is "Loss of Forced Reactor Coolant Flow Including Trip of Pump Motor."
3. Example of design basis event in the safety analysis is "Feedwater System Pipe Break Inside and Outside Containment."
4. Example of design basis event in the safety analysis is "Uncontrolled Control Rod assembly Withdrawal from a Subcritical or Low Power Startup Condition, or Spectrum of Rod Ejection Accident."
5. Example of design basis event in the safety analysis is "Loss of External Electrical Load or Turbine Trip."
6. Overpower ΔT also has a function of Core Heat Removal Protection in conjunction with Overtemperature ΔT, although the primary function of Overpower ΔT is Overpower Protection.

Table 8-5 Engineered Safety Features Actuation Signals (Sheet 1 of 2)

Actuation Signal	Number of Sensors, Switches, or Signals	Actuation Logic	Permissives and Bypasses For Permissives and Bypasses Refer Table 7.2-4
1. Emergency Core Cooling System - Logic diagram Figure 7.2-2 Sheet 11			
Low Pressurizer Pressure	4 Pressure Sensors (Shared with RT)	2/4	Operating bypass permitted while P-11 is active, automatically unbypassed by inactive P-11.
Low Main Steam Line Pressure	4 Pressure Sensors per Steam Line	2/4 per Steam Line	Operating bypass permitted while P-11 is active, automatically unbypassed by inactive P-11.
High Containment Pressure	4 Pressure Sensors	2/4	None
Manual Actuation	1 Switch per Train	1/1	Can be manually reset to block re-initiation of ECCS signal while P-4 is active. This block is automatically removed when P-4 becomes inactive.
2. Containment Spray - Logic diagram Figure 7.2-2 Sheet 12			
High-3 Containment Pressure	4 Pressure Sensors (Shared with ECCS)	2/4	None
Manual Actuation	2 Switches per Train	2/2	None
3. Main Control Room Isolation - Logic diagram Figure 7.2-2 Sheet 12			
MCR Outside Air Intake Radiation	2 Gas Radiation Detectors	1/2	None
	2 Iodine Radiation Detectors	1/2	None
	2 Particulate Radiation Detectors	1/2	None
ECCS Actuation	Valid ECCS Signal	1/1	None
Manual Actuation	1 Switch per Train	1/1	None
4. Containment Purge Isolation - Logic diagram Figure 7.2-2 Sheet 12			
Containment High Range Area Radiation	4 Radiation Detectors	2/4	None
ECCS Actuation	Valid ECCS signal	1/1	None
Manual Containment Isolation	1 Switch per Train	1/1	None
Manual CS Actuation	2 Switches per Train	2/2	None
5. Containment Isolation Phase A - Logic diagram Figure 7.2-2 Sheet 12			
ECCS Actuation	Valid ECCS Signal	1/1	None
Manual Actuation	1 Switch per train	1/1	None
6. Containment Isolation Phase B - Logic diagram Figure 7.2-2 Sheet 12			
High-3 Containment Pressure	4 Pressure Sensors (Shared with ECCS)	2/4	None
Manual CS Actuation	2 Switches per train	2/2	None

Table 8-5 Engineered Safety Features Actuation Signals (Sheet 2 of 2)

Actuation Signal	Number of Sensors, Switches, or Signals	Actuation Logic	Permissives and Bypasses For Permissives and Bypasses Refer Table 7.2-4
7A. Main Feedwater Regulation Valve Closure Figure 7.2-2 Sheet 10			
Low T_{avg} coincident with RT (P-4)	4 Temperature Sensors (T_{avg}) (Shared with RT)	2/4	None
	1Signal per Train (P-4)	1/1	None
7B. Main Feedwater Isolation Figure 7.2-2 Sheet 10			
High-High SG Water Level	4 Level Sensors per SG (Shared with RT)	2/4 per SG	None
ECCS Actuation	Valid ECCS signal	1/1	None
Manual Actuation	2 Switches	1/2 per Valve	None
8. Main Steam Line Isolation - Logic diagram Figure 7.2-2 Sheet 9			
Low Main Steam Line Pressure	4 Pressure Sensors per Steam Line (Shared with ECCS)	2/4 per Steam Line	Operating bypass permitted while P-11 is active, automatically unbypassed by inactive P-11.
High Main Steam Line Pressure Negative Rate		2/4 per Steam Line	Operating bypass of unblock permitted while P-11 is active, automatically blocked by inactive P-11.
High-High Containment Pressure	4 Pressure Sensors (Shared with ECCS)	2/4	None
Manual Actuation	2 Switches	1/2 per Valve	None
9. Emergency Feedwater Actuation - Logic diagram Figure 7.2-2 Sheet 7			
Low SG Water Level	4 Level Sensors per SG (Shared with RT)	2/4 per SG	None
ECCS actuation	Valid ECCS signal	1/1	None
LOOP signal	Valid Blackout signal	1/1	None
MFW Pumps tripped	All pumps trip signal	1/1	None
Manual Actuation	1 Switch per train	1/1	None
10 Emergency Feedwater Isolation - Logic diagram Figure 7.2-2 Sheet 8			
High SG Water Level	4 Level Sensors per SG (Shared with RT)	2/4 per SG	Permitted while P-4 is active Automatically blocked while steam line pressure is low Operating bypass permitted while P-11 is active, automatically unbypassed by inactive P-11.
Low Main Steam Line Pressure	4 Pressure Sensors per Steam Line (Shared with ECCS)	2/4 per Steam Line	Automatically blocked while EFW Isolation signal from other SG is initiated.
Manual Actuation	2 Switches per SG	1/2 per SG	None
11. CVCS Isolation - Logic Diagram Figure 7.2-2 Sheet 6			
High Pressurizer Water Level	4 Level Sensors (Shared with RT)	2/4	Operating bypass permitted while P-11 is active, automatically unbypassed by inactive P-11.
Manual Actuation	1 Switch per train	1/1	None

Table 8-6 Engineered Safety Features Actuation Variables, Ranges, Accuracies, Response Times, and Setpoints (Nominal) (Sheet 1 of 2)

ESF Function	Variables to be monitored	Range of Variables	Instrument Accuracy*[1,2]	Response Time*[1,2,3]	Setpoint*[4]
Emergency Core Cooling System Actuation					
(a) Low Pressurizer Pressure	Pressurizer Pressure	1700 to 2500 psig	2.5% of span	3.0 sec	1765 psig
(b) Low Main Steam Line Pressure	Main Steam Line Pressure	0 to 1400 psig	3% of span	3.0 sec	525 psig
(c) High Containment Pressure	Containment Pressure	-7 to 80 psig	2.8% of span	3.0 sec	6.8 psig
Containment Spray					
High-3 Containment Pressure	Containment Pressure	-7 to 80 psig	2.8% of span	3.0 sec	34.0 psig
Main Control Room Isolation					
High MCR Outside Air Intake Radiation	MCR Gas Radiation	1E-7 to 1E-2 µCi/cc	6% of span	60 sec	2E-6 µCi/cc
	MCR Iodine Radiation	1E-11 to 1E-5 µCi/cc	6% of span	60 sec	8E-10 µCi/cc
	MCR Particulate Radiation	1E-12 to 1E-7 µCi/cc	6% of span	60 sec	8E-10 µCi/cc
Containment Purge Isolation					
High Containment High Range Area Radiation	Containment Area Radiation	1 to 1E+7 R/h	6% of span	15 sec	100 R/h
Main Feedwater Isolation					
(a) High-High SG Water Level	SG Water Level	0 to 100% of span (narrow range taps)	3% of span	3.0 sec	70% of span
(b) Low T_{avg} coincident with RT (P-4)	Reactor Coolant Temperature	530 to 630 °F	2.0 °F	8.0 sec	564 °F
Main Steam Line Isolation					
(a) Low Main Steam Line Pressure	Main Steam Line Pressure	0 to 1400 psig	3% of span	3.0 sec	525 psig
(b) High Main Steam Line Pressure Negative Rate	Main Steam Line Pressure	0 to 1400 psig	3% of span	3.0 sec	100 psi
(c) High-High Containment Pressure	Containment Pressure	-7 to 80 psig	2.8% of span	3.0 sec	22.7 psig

Table 8-6 Engineered Safety Features Actuation Variables, Ranges, Accuracies, Response Times, and Setpoints (Nominal) (Sheet 2 of 2)

ESF Function	Variables to be monitored	Range of Variables	Instrument Accuracy*[1,2]	Response Time*[1,2,3]	Setpoint*[4]
Emergency Feedwater Actuation					
Low SG Water Level	SG Water Level	0 to 100% of span (narrow range taps)	3% of span	3.0 sec	13% of span
LOOP Signal	LOOP Signal	0 to 8.25 kV	1.5% of span	3.0 sec	4727 V with ≤ 0.8 sec time delay
Emergency Feedwater Isolation					
(a)High SG Water Level	SG Water Level	0 to 100% of span (narrow Range taps)	3% of span	3.0 sec	50% of span
(b)Low Main Steam Line Pressure	Main Steam Line Pressure	0 to 1400 psig	3% of span	3.0 sec	525 psig
CVCS Isolation					
High Pressurizer Water Level	Pressurizer Water Level	0 to 100% of span	3% of span	3.0 sec	92% of span

Note:
1. Instrument accuracy and response time calculation methodology refer to Subsection 7.2.2.7.
2. Instrument accuracies and response times will be decided to take into account the specification of instruments.
3. Additional time during LOOP is referred to Chapter 8.
4. Setpoints will be adjusted to compensate for loop accuracy.

Table 8-7 Rod Control System Interlocks

Designation	Derivation	Function
C-1	1-out-of-2 Intermediate Range Neutron Flux above setpoint	Blocks automatic and manual control rod withdrawal
C-2	1-out-of-4 Power Range Neutron Flux above setpoint	Blocks automatic and manual control rod withdrawal
C-3	2-out-of-4 Over Temperature ΔT above setpoint	Blocks automatic and manual control rod withdrawal
		Actuates turbine runback via load reference
C-4	2-out-of-4 Over Power ΔT above setpoint	Blocks automatic and manual control rod withdrawal
		Actuates turbine runback via load Reference
C-5	Turbine Inlet Pressure (output of signal selector) below setpoint	Blocks automatic control rod Withdrawal

Table 8-8 Diverse Actuation Signals

Actuation Signal	Number of Sensors or Switches	Actuation Logic	Permissives and Bypasses
1. Reactor Trip, Turbine Trip and MFW Isolation			
Low Pressurizer Pressure	4 Pressure Sensors	2/4	Manually bypassed by the actuation of a dedicated hardwired switch on the OC during plant startup and shutdown. Blocked by P-4.
High Pressurizer Pressure	4 Pressure Sensors	2/4	Manually bypassed by the actuation of a dedicated hardwired switch on the OC during plant startup and shutdown. Blocked by P-4.
Low SG Water Level	1 Level Sensor per SG) (Shared with EFW Actuation)	2/4	Manually bypassed by the actuation of a dedicated hardwired switch on the OC during plant startup and shutdown. Blocked by P-4.
Manual Actuation	1 Switch	1/1	None
2. Emergency Feedwater Actuation			
Low SG Water Level	1 Level Sensor per SG (Shared with reactor trip, turbine trip and MFW isolation)	2/4	Manually bypassed by the actuation of a dedicated hardwired switch on the OC during plant startup and shutdown. Blocked by 2-out-of-4 signal of EFW Pump operation signals.
Manual actuation	1 Switch	1/1	None
3. ECCS Actuation			
Manual Actuation	1 Switch	1/1	None
4. Containment Isolation			
Manual actuation	1 Switch	1/1	None
5. Open/Close Emergency Feedwater Control Valves			
Manual Actuation	1 Switch per SG	1/1	None
6. Open/Close Safety Depressurization Valve			
Manual Actuation	1 Switch	1/1	None
7. Open/Close Main Steam Depressurization Valves			
Manual Actuation	1 Switch per SG	1/1	None