7.3 Engineered Safety Features Systems

7.3.1 Description

The U.S. EPR provides safety-related instrumentation and controls to sense accident conditions and automatically initiate the engineered safety features (ESF) systems. ESF systems are automatically actuated when selected variables exceed setpoints that are indicative of conditions that require protective action. Additionally, the ability to manually initiate ESF systems is provided in the main control room (MCR). Manual system-level actuation of ESF systems initiates all actions performed by the corresponding automatic actuation, including starting auxiliary or supporting systems and performing required sequencing functions. The SICS provides controls in the MCR for the manual actuation of the ESF functions listed in Table 7.3-5—Protection System Manually Actuated Functions. Component-level control ESF system actuators is also provided in the MCR.

7.3.1.1 System Description

Automatic actuation of ESF systems and auxiliary supporting systems is performed by the protection system (PS) when selected plant parameters reach the appropriate setpoints. These automatic actuation orders are sent to the priority and actuator control system (PACS) for prioritization and interface to the actuators. An example of an ESF actuation sequence actuated by four divisions of the PS is illustrated in Figure 7.3-1 (Sheet 1), and is described as follows:

- An acquisition and processing unit (APU) in each division acquires one-fourth of the redundant sensor measurements through the signal conditioning and distribution system (SCDS) that are inputs to a given ESF actuation function.
- The APU in each division performs any required processing using the measurements acquired by that division (e.g., filtering, range conversion, calculations). The resulting variable is compared to a relevant actuation setpoint in each division. If a setpoint is breached, the APU in that division generates a partial trigger signal for the appropriate ESF function.
- The partial trigger signals from each division are sent to redundant actuation logic units (ALU) in the PS division responsible for the associated actuation. Two out of four voting is performed in each ALU on the partial trigger signals from all four divisions. If the voting logic is satisfied, an actuation order is generated.
- The actuation signals of the redundant ALU in each subsystem are combined in a hardwired “functional OR” configuration so that either redundant ALU can actuate the function.

ESF functions actuated by less than four divisions are illustrated in Figure 7.3-1 (Sheets 3 through 5).

Actuation orders are sent from the PS to the PACS priority module associated with each actuator required for the function. The exception to this is the turbine trip function. The actuation order is transmitted via hardwired connections to the turbine-generator instrumentation and control system (TG I&C) and does not involve the PACS. The connections between the PS and TG I&C are shown in Figure 7.1-27. The PS and the PACS are discussed in Section 7.1. The TG I&C system is described in Section 10.2.

The safety automation system (SAS) performs closed loop automatic controls of certain ESF systems following their actuation by the PS. These controls are described in Section 7.3.1.3. The SAS also performs functions for essential auxiliary support (EAS) systems. These are systems that provide support to the ESF systems. The EAS functions are in continuous operation and performed by the SAS. These controls are described in Section 7.3.1.4. The list of functions performed by the SAS is described in Table 7.1-5. The other functions described in Section 7.3 are done by the PS. The SAS is described in Section 7.1.

The capability for manual system-level ESF actuations is available to the operator through the safety information and control system (SICS) in the MCR. These manual actuations are acquired by the ALUs in the PS and combined with the automatic actuation logic. The manual actuations are described with the corresponding automatic function in Section 7.3.1.2.

The capability for component-level control of ESF and EAS system actuators is available to the operator on both the PICS and the SICS in the MCR. Commands from the PICS are processed by the PAS and sent to the PACS for prioritization. Commands from the SICS are sent directly to the PACS for prioritization. SICS is the safety-related actuation path and PICS is the non-safety-related actuation path. The manual system-level ESF actuation sequence is shown in Figure 7.3-1 (Sheet 2). The manual actuations are described with the corresponding automatic function in Sections 7.3.1.2.

For an extra borating system (EBS) malfunction event, the component-level controls on SICS are credited to terminate EBS. For the failure of small lines carrying primary coolant outside the Reactor Containment Building (Section 15.0.0.3.5), component-level controls from SICS are credited to isolate the failed line. Operator actions credited in mitigating accidents are addressed in Section 15.0.0.3.7.

The capability for manual reset of sense and command ESF actuation outputs is provided on the SICS. Not all ESF actuations require a manual reset. The automatic safety related actuation functions' output signals must be reset manually unless there is justification for the functions' signals being reset automatically. There are cases where a sense and command output is cleared after the PS determines that the initiating condition has cleared. The reset functionality related to each ESF actuation is

described in Section 7.3.1.2. Further description of the operation of the SICS is presented in Section 7.1.

7.3.1.2 Engineered Safety Features Actuation Functional Descriptions

7.3.1.2.1 Safety Injection System Actuation

To mitigate a loss of coolant accident (LOCA), a safety injection signal is required to actuate the appropriate ESF and support systems and to isolate non-qualified reactor coolant system (RCS) piping.

In case of a decrease in RCS water inventory due to a LOCA, the RCS is supplied by medium head safety injection (MHSI) in the high pressure phase of the event and low head safety injection (LHSI) in the low pressure phase.

The operation of the MHSI and LHSI systems is described in Section 6.3.

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

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

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

SIS actuation based on hot leg ΔP_{sat} results from the difference between measured pressure and saturation pressure being below a fixed setpoint (Min1p) in any two of the four PS divisions. The measured pressure is obtained from one pressure (wide range (WR)) measurement in each hot leg. The saturation pressure is calculated from one temperature (WR) measurement in each hot leg. This initiation parameter is used when RCS pressure is below the P12 pressure threshold and above the P15 pressure and temperature thresholds. It is bypassed above the P12 threshold and below the P15 thresholds.

SIS actuation based on hot leg loop level results from RCS water level measurements below the fixed setpoint (Min1p) in any two of the four PS divisions. One loop level measurement is taken in each of the hot legs. This initiation parameter is used below the P15 pressure and temperature thresholds with all four reactor coolant pumps

(RCP) shut down. It is bypassed above the P15 thresholds. A manual bypass of SIS actuation on low hot leg loop level is provided for protection of personnel working in the RCS components during outages.

The logic for generation of the P12 and P15 permissive signals is described in Section 7.2.1.3.7 and Section 7.2.1.3.10.

The capability for manual system-level initiation of the SIS is provided to the operator on the SICS in the MCR. This manual system-level initiation starts the four trains of safety injection as well as the associated protective actions, such as partial cooldown and reactor trip. For an SG tube rupture (SGTR) event, the operator is credited to perform a manual system-level initiation of SIS from the SICS. Four manual system-level initiation controls are provided, any two of which will start the four SIS trains.

The capability for component-level control of the SIS actuators is available to the operator on both the PICS and the SICS in the MCR. Operator actions credited in mitigating accidents are addressed in Section 15.0.0.3.7.

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

The logic for the SIS actuation function is shown in Figure 7.3-2—SIS Actuation.

7.3.1.2.2 Emergency Feedwater System Actuation

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

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

The operation of the EFWS is described in Section 10.4.9.

The U.S. EPR design uses the following initiating conditions to actuate the EFWS:

- SG level (WR) < Min2p.
- Loss of offsite power (LOOP) and SIS actuation signals generated.

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

EFWS actuation based on LOOP and SIS actuation is performed concurrently on all SGs. Generation of the SIS actuation signal is described in Section 7.3.1.2.1. Generation of the LOOP signal is described in Section 7.3.1.2.12.

In both cases, EFWS actuation is bypassed when hot leg temperature is below the P13 permissive setpoint. The bypass is automatically removed above the P13 permissive setpoint. Generation of the P13 permissive signal is discussed in Section 7.2.1.3.8.

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

When EFW actuation occurs due to LOOP and SIS actuation, the PS sends a pulse signal of limited duration to start the actuation. The duration of the pulse is long enough for the intended actions of the execute features to go to completion. The pulse function logic block is used to maintain the actuation signal until the actuator reaches its final position. Then the actuation signal is removed, and the EFW SG Level Control function maintains the level. The safety function is completed once the EFW is initiated, and the valves and pumps are in their final position/state. No reset is needed in this case, as the SG water level is already above the Min2p setpoint when the EFW actuation occurs and the safety-related SG level control loop can immediately take control of the actuators.

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

The safety-related closed loop control for SG water level following EFWS actuation is performed by the SAS. When EFWS actuation occurs, the PS signals the SAS to initiate the closed loop control. Separately, during SG water level control by the SAS,

a second closed loop control is also performed by SAS that regulates pump flow to protect the EFW pump from an overflow condition.

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

The capability for component-level control of the EFWS actuators is available to the operator on both the PICS and the SICS in the MCR. Following an FWLB, manual component-level control from the SICS is credited with redirecting the EFWS train feeding the affected SG to an intact SG. Operator actions credited in mitigating accidents are addressed in Section 15.0.0.3.7.

The functional logic for automatic actuation of the EFWS is shown in Figure 7.3-3—EFWS Actuation, Figure 7.3-6—EFWS Actuators (Div. 1&2), and Figure 7.3-7—EFWS Actuators (Div. 3&4).

The functional logic for SG water level control following EFWS actuation, and EFW pump overflow protection, is shown in Figure 7.3-4—EFWS SG Level Control and Pump Flow Protection.

7.3.1.2.3 Emergency Feedwater System Isolation

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

The operation of the EFWS is described in Section 10.4.9.

The U.S. EPR design uses the following initiating condition to isolate the EFWS:

- SG level (WR) > Max1p.
- SG isolation signal (Section 7.3.1.2.14).

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

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

Generation of the P13 signal is discussed in Section 7.2.1.3.8.

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

The capability for component-level control of the EFWS actuators is available to the operator on both the PICS and the SICS in the MCR. Following a main steam line break (MSLB), manual initiation from the SICS is credited with terminating EFWS in the affected SG. Operator actions credited in mitigating accidents are addressed in Section 15.0.0.3.7.

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

The functional logic for isolation of the EFWS is shown in Figure 7.3-5—EFWS Isolation, Figure 7.3-6—EFWS Actuators (Div. 1&2), and Figure 7.3-7—EFWS Actuators (Div. 3&4).

7.3.1.2.4 Partial Cooldown Actuation

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

The safety-related partial cooldown function consists of lowering the Max1p main steam relief isolation valve (MSRIV) opening setpoint (Section 7.3.1.2.5) according to a predefined cooldown gradient. If SG pressure exceeds the decreasing Max1p setpoint, the MSRIV is opened and the main steam relief control valve (MSRCV) is used to maintain SG pressure at the decreasing Max1p setpoint. Control of the MSRCV is described in Section 7.3.1.2.5.

The partial cooldown is preferably performed by controlling the turbine bypass valves, in a non-safety-related capacity, to a decreasing pressure setpoint that is maintained slightly lower than Max1p. During accident conditions where containment pressure is greater than Max1p and a safety injection signal is generated, the main steam isolation valves (MSIV) (including bypass piping) are closed. This prevents the use of the turbine bypass valves for partial cooldown. The operator has the capability to reset the main steam isolation signal, and further manual actions are necessary to open the MSIVs. The safety-related partial cooldown via the main steam relief train (MSRT) is

provided to cope with turbine bypass control failure, as the success of the safety injection function can depend on successful partial cooldown. Both the safety-related and non-safety-related partial cooldown are initiated by the PS. The PS detects the condition requiring partial cooldown and sends an initiation signal via an isolated hardwired connection to the process automation system (PAS). Control loops for partial cooldown via turbine bypass are performed by the PAS. The partial cooldown via turbine bypass is described in Section 7.7. The PS also sends the partial cooldown initiation signal to the safety-related SAS. Control loops for partial cooldown via MSRT are performed by the SAS.

Operation of the main steam system and main steam relief train is described in Section 10.3.

The U.S. EPR design uses the following initiating condition to actuate a partial cooldown:

- SIS actuation signal generated.

Generation of the SIS actuation signal is described in Section 7.3.1.2.1. Partial cooldown is initiated any time an SIS actuation signal occurs, except during conditions when RHR can be connected. In such conditions, the primary pressure is already low enough for MHSI to be successful and partial cooldown is not needed. For this reason, the partial cooldown actuation due to SIS actuation is bypassed below the P14 permissive pressure and temperature conditions. Generation of the P14 permissive signal is discussed in Section 7.2.1.3.9.

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

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

The functional logic for partial cooldown actuation is shown in Figure 7.3-8—Partial Cooldown Actuation.

7.3.1.2.5 Main Steam Relief Isolation Valve Opening

In case of loss of the secondary side heat sink, heat has to be removed via steam relief to the atmosphere. The four MSRTs provide this functionality. The MSRTs are also used for SG over-pressure protection to minimize the actuation of the main steam safety valves and the associated risk of the safety valves failing to re-seat. Additionally,

the MSRTs participate in the partial cooldown function (Section 7.3.1.2.4).

Operation of the main steam system (MSS) and MSRTs is described in Section 10.3.

The U.S. EPR design uses the following initiating condition to actuate MSRIV opening:

- SG pressure > Max1p.

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

- During normal operation, Max1p is maintained at one of two fixed values to provide SG overpressure protection. The higher of the two is used when RCS pressure and temperature are above the P14 permissive thresholds; the lower is used below the P14 permissive thresholds. Generation of the P14 permissive signal is discussed in Section 7.2.1.3.9.

- When a SG isolation signal is generated (Section 7.3.1.2.14), Max1p is set to a high fixed value to prevent radioactive release to the atmosphere.

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

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

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

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

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

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

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

The functional logic for formation of the MSRIV opening setpoint is shown in Figure 7.3-9—MSRT Setpoint Formation.

The functional logic for automatic opening of the MSRIV is shown in Figure 7.3-10—MSRIV Opening (Div. 1&2) and Figure 7.3-11—MSRIV Opening (Div. 3&4).

The functional logic for control of the MSRCV is shown in Figure 7.3-12—MSRCV Control.

7.3.1.2.6 Main Steam Relief Train Isolation

As described in Section 7.3.1.2.5, the MSRIV opens due to high SG pressure conditions and the MSRCV is pre-positioned appropriately based on reactor power. At 100 percent power, the MSRCV is positioned fully open. A single failure is postulated on a given MSRCV in which it is not properly pre-positioned and remains full open during a decrease in reactor power, such as following reactor trip (RT). A MSRIV opening after such a single failure could result in overcooling of the RCS. Therefore, the MSRIV and MSRCV both receive a closing order in the event of a low SG pressure condition.

Operation of the MSS and MSRT is described in Section 10.3.

The U.S. EPR design uses the following initiating condition to actuate MSRT isolation:

- SG pressure < Min3p.

The actuation order for MSRT isolation is generated when two-out-of-four SG pressure measurements on any one SG are below the Min3p setpoint. This is a train-specific actuation; only the MSRT associated with the affected SG is isolated. The MSRT isolation function is bypassed when RCS pressure is below the P12 permissive setpoint. The bypass is automatically removed when RCS pressure is above the P12 permissive setpoint. Generation of the P12 permissive signal is discussed in Section 7.2.1.3.7.

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

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

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

The functional logic for isolation of the MSRT is shown in Figure 7.3-13—MSRT Isolation.

7.3.1.2.7 Main Steam Isolation

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

Operation of the MSS is described in Section 10.3.

The U.S. EPR design uses the following initiating conditions to actuate main steam isolation:

- SG pressure drop.
- SG pressure < Min1p.
- SG isolation signal (Section 7.3.1.2.14).
- Containment equipment compartment pressure > Max1p.
- Containment service compartment pressure (NR) > Max2p.

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

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

An actuation order is also generated for main steam isolation when two-out-of-four SG pressure measurements on any one SG are below the fixed Min1p setpoint. When this condition occurs in any one SG, all four main steam trains are isolated. Main steam isolation due to low SG pressure is bypassed when RCS pressure is below the P12 permissive setpoint. The bypass is automatically removed above the P12 permissive setpoint. Generation of the P12 permissive signal is discussed in Section 7.2.1.3.7.

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

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

The capability for component-level control of the main steam and blowdown valves is available to the operator on both the PICS and the SICS in the MCR. For small main steam line breaks (MSLB) and FWLB, manual initiation from the SICS is credited with closing the main steam and blowdown valves when operating below the P12 permissive setpoint. Operator actions credited in mitigating accidents are addressed in Section 15.0.0.3.7.

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

The functional logic for automatic main steam isolation is shown in Figure 7.3-14 and Figure 7.3-15.

7.3.1.2.8 Main Feedwater Isolation

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

Operation of the MFW system is described in Section 10.4.

The U.S. EPR design uses the following initiating conditions to actuate MFW isolation:

- Initiation of RT (full load isolation).
- SG level (NR) > Max1p (full load isolation).
- SG level (NR) > Max0p for a period of time following RT (SSS isolation).
- SG pressure drop > Max2p (SSS isolation).
- SG pressure < Min2p (SSS isolation).
- SG isolation signal (Section 7.3.1.2.14).
- Containment equipment compartment pressure > Max1p (SSS isolation).
- Containment service compartment pressure (NR) > Max2p (SSS isolation).

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

Redundant to the MFW full load isolation due to RT on SG level > Max1p, a separate, SG-specific MFW full load isolation order is also generated at the Max1p setpoint to avoid SG overfill and moisture carryover. This actuation order is generated when two out of four SG level (NR) measurements on any one SG exceed the Max1p setpoint. Only the full load lines feeding the SG with the high water level are isolated due to this signal. The other full load lines are isolated on initiation of RT due to the same high level measurement. The high SG level initiation is bypassed when hot leg temperature is below the P13 permissive setpoint. The bypass is automatically removed when hot leg temperature is above the P13 permissive setpoint. Generation of the P13 permissive signal is discussed in Section 7.2.1.3.8.

Following RT on high SG level, the SG level is expected to decrease initially due to the prompt reduction in steam flow and then be maintained at a normal level by the SG level control system. A persistent high SG level may be indicative of a SGTR or a failure of the SG level control system. If the SG level remains greater than the Max0p setpoint for a fixed amount of time following RT and MFW full load isolation, MFW SSS isolation is performed. This actuation order is generated when two-out-of-four SG level (NR) measurements remain above the Max0p setpoint, following expiration of a time delay initiated by RT signal. The time delay logic block is used to isolate all main feedwater (i.e., SSS Isolation) if a high SG level (SG Level > Max0p) is present after a RT and MFW full load isolation (both on SG Level > Max1p) has occurred. The time delay is used to provide a wait time after a RT and MFW full load isolation, for the SG

level to decrease below the Max0p setpoint. If after the time delay expires, the SG level is above the Max0p setpoint, it is necessary to isolate all main feedwater. The SSS isolation is performed only on a SG in which the level remains above the Max0p setpoint. This initiation signal is bypassed when hot leg temperature is below the P13 permissive setpoint. The bypass is automatically removed when hot leg temperature is above the P13 permissive setpoint. Generation of the P13 permissive signal is discussed in Section 7.2.1.3.8.

Following a main steam or feedwater system piping failure, a complete feedwater isolation of the MFW train feeding the affected SG is desirable. In this case, MFW full load isolation occurs on all four SGs because of the reactor trip on either SG pressure drop or on SG pressure < Min1p. A MFW SSS isolation of the affected SG will occur on a more severe SG pressure drop (to mitigate fast depressurizations) or on SG pressure < Min2p (to mitigate slower depressurizations). The logic to initiate MFW isolation on SG pressure drop is the same as that described for main steam isolation on SG pressure drop described in Section 7.3.1.2.7, except that the variable low setpoint for SSS isolation is maintained below the RT and main steam isolation setpoint. The actuation order for SSS isolation due to SG pressure < Min2p is generated when two out of four SG pressure measurements on any one SG are below the Min2p setpoint. There is no operating bypass associated with SSS isolation on SG pressure drop. SSS isolation on SG pressure < Min2p is bypassed when RCS pressure is below the P12 permissive setpoint. The bypass is automatically removed when RCS pressure is above the P12 permissive setpoint. Generation of the P12 permissive signal is discussed in Section 7.2.1.3.7.

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

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

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

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

The functional logic for MFW isolation is shown in Figure 7.3-16—MFWS Isolation - Full Load, Figure 7.3-17—MFWS Isolation - SSS, Figure 7.3-18—MFW Actuators (Div. 1&2), and Figure 7.3-19—MFW Actuators (Div. 3&4).

7.3.1.2.9 Containment Isolation

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

The containment isolation actuators and their functionality are described in Section 6.2.4.

The U.S. EPR design uses the following initiating conditions to isolate the containment:

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

Stage 1 isolation is provided for a small break loss of coolant accident (SBLOCA) to isolate containment penetrations that have no active function for LOCA mitigation and to start ventilation of containment annulus. A Stage 1 containment isolation order is generated when two-out-of-four PS divisions detect high containment pressure. Either two-out-of-four equipment compartment pressure measurements exceeding the Max1p setpoint, two-out-of-four service compartment pressure (NR) measurements exceeding the Max2p setpoint, or two-out-of-four containment service compartment pressure (WR) measurements exceeding the Max3p setpoint results in Stage 1 isolation. If two-out-of-four high range containment activity sensors indicate radioactivity in containment, a Stage 1 isolation order is also generated. A safety injection actuation signal also results in a Stage 1 containment isolation actuation. To limit the peak load on the EUPS batteries and inverters, a staggered closure sequence is provided by the PS for containment isolation valves (CIVs) that receive a Stage 1 containment isolation signal and are located in the reactor containment building and powered by the EUPS. The staggering of the Stage 1 containment isolation signal is implemented through time delays in the PS. The inside CIVs that are staggered are

arranged in three groups and each group is associated with a different time delay. There is no time delay associated with an initial group of CIVs. The different grouping of CIVs is described in Section 6.2.4.2.5.

Stage 2 containment isolation order is generated when two-out-of-four service compartment pressure (WR) measurements exceed Max3p setpoint. A LOCA of sufficient size to raise containment pressure to Max3p setpoint does not require RCPs for mitigation. In fact, on a Stage 2 containment isolation signal, RCPs are tripped to limit energy input to containment, and containment penetrations for processes that support RCP operation are isolated.

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

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

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

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

Functional logic for actuation of containment isolation is shown in Figure 7.3-20—Containment Isolation.

7.3.1.2.10 Chemical and Volume Control System (CVCS) Charging Isolation

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

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

- Pressurizer Level (NR) > Max2p.

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

These CVCS charging isolation functions are bypassed when cold leg temperature is below the P17 permissive setpoint. The bypass is automatically removed above the P17 permissive setpoint. Generation of the P17 permissive signal is discussed in Section 7.2.1.3.12.

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

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

A manual reset of the sense and command outputs is not required for the CVCS charging isolation function. The outputs are automatically reset when the level measurements return below the appropriate setpoint. The pulse function logic block provides a minimum actuation output time to maintain an actuation signal, until the actuators reach their final position. A pulse order is used to provide assurance that the actions of the execute features go to completion. The automatic reset of the sense and command outputs does not result in change of state of the isolation actuators; it allows the operator to take further manual actions to change the state of individual actuators.

The functional logic for CVCS charging isolation is shown in Figure 7.3-21—CVCS Charging Isolation.

7.3.1.2.11 CVCS Isolation for Anti-Dilution

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

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

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

$$BC_P^N = \frac{R}{1+R} BC_{Inj}^N + \frac{R}{1+R} BC_P^{N-1}$$

Where:

$$R = \frac{QF_{Inj} \times \Delta t}{M_P^N}$$

And:

B_P^N = RCS boron concentration at time t_N

BC_P^{N-1} = RCS boron concentration at time t_{N-1}

BC_{Inj}^N = Boron concentration measured by the boron concentration measurement system (BCMS) in the CVCS charging line

QF_{Inj} = Measured flow in the CVCS charging line

M_p^N = Mass of reactor coolant (fixed value during power operation)

Δt = Time from N-1 to N

N = Integer

Until the boron concentration calculation has enough data to produce an output, the boron concentration measured by the BCMS in the CVCS charging line is used. This is achieved with a manual boron calculation initialization command provided in the SICS. The command lasts long enough for the boron concentration calculation to produce an output.

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

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

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

The capability for manual system-level initiation of CVCS isolation for anti-dilution on a per-division basis is provided on the SICS in the MCR. One manual system-level isolation control is provided for PS Division 1, and one control is provided for PS Division 4. The manual boron calculation initialization command is provided on the SICS in the MCR. This input is processed by the APU.

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

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

The functional logic for CVCS isolation for anti-dilution is shown in Figure 7.3-22—CVCS Isolation for Anti-Dilution.

7.3.1.2.12 Emergency Diesel Generator (EDG) Actuation

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

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

The three phases of voltage on each main MV bus are monitored by the PS to detect either a degraded voltage condition or a loss of voltage condition. If the voltage measurements for two of the three phases on a bus fall below a fixed setpoint (Min

DEGV) for a fixed amount of time and an SIS signal is received, a degraded voltage condition exists. After this fixed amount of time, if the voltage measurements for two of the three phases on a bus stay below the same fixed setpoint (Min DEGV) for an additional fixed amount of time without an SIS, a degraded voltage condition exists. If the voltage measurements for two of the three phases on a bus fall below a lower fixed setpoint (Min LOV) for a fixed amount of time, a loss of voltage condition exists. In these cases, a LOOP signal is generated within the PS which starts the corresponding EDG and begins the loading sequence. All four EDGs are also started automatically when a safety injection signal is generated, but they are not connected to the EPSS unless a LOOP signal is also generated.

The automatic EDG start and load sequence consists of the following:

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

Large electrical loads are sequenced onto the EPSS according to the diesel load steps (DLS) to maintain EDG output voltage and frequency reductions within acceptable limits. The PS performs the DLS functionality by maintaining an "off" signal to the actuators, and then removing the signal to a sub set of actuators at each load step which allows them to be re-started. Essential service water (ESW) pumps and component cooling water (CCW) pumps are automatically started as part of the load sequence regardless of whether or not they were previously running. Smaller loads that were energized before the loss of power automatically re-start when power from the EDG becomes available. The PACS module confirms that the actuator remains "off" as long as the PS signal is present. Once the PS "off" signal is removed, other systems can actuate the components.

When a LOOP signal is generated, different DLS sequences are used depending on whether or not a safety injection signal is also present. The different sequences are detailed in Table 8.3-4 through Table 8.3-7.

In absence of a safety injection signal, the CCW and ESW pumps the first two loads sequenced onto the EDG following closure of the EDG output circuit breaker. The "off" signal is removed from the safety injection components at their predefined steps, but the safety injection pumps are not started. If a safety injection signal is generated

after the LOOP-only loading sequence has begun, the sequence is stopped, the LOCA mitigation loads are started, then the LOOP-only sequence is re-entered and completed.

If a safety injection signal is present when the LOOP signal is generated, the LOCA mitigation loads are started in the first several steps of the load sequence. The other loads are then sequenced onto the EPSS according to pre-defined load steps. Upon completion of the automatic loading sequence the PS removes all "stop" signals and loads are allowed to start as their control logic permits.

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

There are two types of uses for the time delay logic block in the EDG Actuation function. The first time delay is for preventing spurious starts of the EDG on dips in the voltage. This is the time delay that is paired with each threshold logic block on the EDG Actuation logic. The operator receives an alarm if the voltage degrades for longer than the first set of time delays. The second time delay in the downstream logic allows the operator time to correct the degraded voltage condition once the operator has received an alarm. If the operator does not correct the degraded voltage condition by the time period of the second time delay, then the EDG will be started and loaded so that the electrical bus is on a known good source.

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

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

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

The functional logic used to generate an EDG actuation order is shown in Figure 7.3-23—EDG Actuation.

7.3.1.2.13 Pressurizer Safety Relief Valve Opening (Brittle Fracture Protection)

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

Operation of the PSRVs is described in Section 5.4.13.

The U.S. EPR design uses the following initiating conditions to actuate PSRV opening:

- Hot leg pressure (NR) > Max1p.
- Hot leg pressure (NR) > Max2p.

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

To avoid spurious PSRV opening during power operation, this function is automatically bypassed when cold leg temperature is above the P17 permissive setpoint. Operator action is required to remove the bypass when temperature is below the P17 permissive setpoint. Generation of the P17 permissive signal is discussed in Section 7.2.1.3.12.

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

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

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

The functional logic for automatic PSRV opening is shown in Figure 7.3-24—PSRV Opening (Brittle Fracture Protection).

7.3.1.2.14 Steam Generator Isolation

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

- MSRT opening setpoint increase.
- MSIV, MSIV bypass, and SG blowdown closure.
- MFW and SSS isolation.
- EFWS isolation (confirmatory action; EFWS should already be isolated as described in Section 7.3.1.2.3).

Operation of the main steam system is described in Section 10.3. Operation of the SG blowdown system is described in Section 10.4.8. Operation of the MFW and SSS systems is described in Section 10.4. Operation of the EFW system is described in Section 10.4.9. Main steam line activity sensor information is described in Section 11.5.4.1 and Table 11.5-1.

The U.S. EPR design uses the following initiating conditions to actuate SG isolation:

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

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

The SG isolation function is bypassed when hot leg temperature is below the P13 permissive setpoint. Generation of the P13 permissive signal is discussed in Section 7.2.1.3.8. However, when the partial cooldown actuation function is bypassed (Section 7.3.1.2.4), the SG isolation function is bypassed by association to the partial cooldown actuation signal.

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

The capability for component-level control of the actuators used in SG isolation is available to the operator on both the PICS and the SICS in the MCR. For an SGTR event, the operator is credited to perform a manual system-level initiation of SG isolation from the SICS in the MCR. Operator actions credited in mitigating accidents are addressed in Section 15.0.0.3.7.

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

The functional logic for automatic SG isolation is shown in Figure 7.3-25—SG Isolation (Div. 1&2) and in Figure 7.3-26—SG Isolation (Div. 3&4).

7.3.1.2.15 Reactor Coolant Pump Trip

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

Additionally, the RCPs are tripped on a containment isolation (Stage 2) signal.

The operation of the RCPs is described in Section 5.4.1.

The U.S. EPR design uses the following initiating conditions to actuate RCP trip:

- ΔP across RCP < Min1p and SIS actuation signal generated.
- Containment isolation (Stage 2) signal generated.

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

The parameters that result in RCP trip due to a containment isolation (stage 2) are described in Section 7.3.1.2.9.

When the conditions for RCP trip are satisfied, orders are issued to open the circuit breakers that supply power to each RCP. When the orders are issued, a time delay begins. The time delay logic block is used to delay the opening of the redundant RCP circuit breaker so that simultaneous opening of RCP circuit breakers does not cause an excessive voltage surge. When the time delay expires, an order is issued to trip the corresponding bus supply circuit breaker upstream of the RCP circuit breaker to remove power from the RCP.

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

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

The capability for component-level control for the RCP trip function is available to the operator on both the PICS and the SICS in the MCR. Following an FWLB, manual trip of two RCPs from the SICS is credited. Operator actions credited in mitigating accidents are addressed in Section 15.0.0.3.7.

When RCP trip has occurred due to low ΔP measurements, concurrent with a safety injection signal, the sense and command output can be reset manually regardless of whether or not the safety injection signal has been reset. The manual reset is available on SICS in the MCR. When RCP trip based on containment isolation (Stage 2) occurs, the RCP trip output is reset when the containment isolation (Stage 2) output is reset.

The functional logic for automatic actuation of RCP trip is shown in Figure 7.3-27—RCP Trip.

7.3.1.2.16 Main Control Room Air Conditioning System Isolation and Filtering

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

The U.S. EPR design uses the following initiating conditions to isolate and filter the MCR air conditioning system:

- MCR air intake activity > Max1p.
- Containment isolation (Stage 1) signal.

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

The parameters that result in the isolation and filtering of the MCR air conditioning system due to a containment isolation (Stage 1) are described in Sections 7.3.1.2.9.

There are no operating bypasses associated with this function.

The capability for manual system-level initiation of this function is provided on the SICS in the MCR. Two manual system-level initiation controls are provided, any one of which reconfigures both air intake paths.

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

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

The functional logic for MCR air conditioning system isolation and filtering is shown in Figure 7.3-28—MCR Air Conditioning System Isolation and Filtering.

7.3.1.2.17 Turbine Trip on Reactor Trip Initiation

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

A short delay is implemented between the RT activation and the TT demand to limit the overpressure effect. The time delay logic block is used for a loss of flow event (loss of one RCP) at 100% power that results in a Reactor Trip on Low-Low RCS Flow Rate (Figure 7.2-11). The safety analysis assumes that a turbine trip LOOP occurs and results in the loss of the three remaining operating RCPs. The time delay duration is the minimum time to delay the loss of the remaining three RCPs, to allow the trip to reduce power sufficiently, such that the loss of the remaining three RCPs does not challenge DNB limits.

The U.S. EPR design uses the following initiating condition to actuate the TT:

- RT Initiation.

The various conditions that lead to RT are described in Section 7.2.

Each divisional TT signal from the PS is sent to the TG I&C via a hardwired, isolated connection. A two-out-of-four logic is performed in each division of the TG I&C on the four PS divisional signals. These connections between the PS and TG I&C are shown in Figure 7.1-27.

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

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

Manual reset of the sense and command output for TT is available from the SICS in the MCR. A reset of the sense and command output does not result in a change of the state of the actuators; it allows the operator to take further actions to manipulate individual components as may be necessary to follow plant operating procedures.

The functional logic for turbine trip is shown in Figure 7.3-29—Turbine Trip on Reactor Trip Initiation.

7.3.1.2.18 Hydrogen Mixing Dampers Opening

This function provides convection and atmospheric mixing in the event of an AOO or PA to enable atmospheric circulation within the whole Reactor Containment Building.

The U.S. EPR design uses the following initiating conditions to open the hydrogen mixing dampers (HMD):

- Containment service compartment pressure (NR) > Max1p.
- Containment equipment compartment/containment service compartment ΔP > Max1p.

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

There are no operating bypasses associated with this function.

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

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

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

The functional logic for hydrogen mixing dampers opening is shown in Figure 7.3-30—Hydrogen Mixing Dampers Opening.

7.3.1.3 Engineered Safety Features Control Functional Descriptions

7.3.1.3.1 Annulus Ventilation System

The annulus ventilation system (AVS) accident filtration trains are used during PAs to contain leakage from the primary containment by maintaining a subatmospheric pressure in the annulus. The exhaust air from the annulus is filtered before release to the environment via the vent stack. See Section 6.2.3.2.2.2 for more information about the AVS accident trains.

Accident Filtration Train Heater Control

The AVS has a safety-related function to maintain capability of the iodine absorbers to remove iodine from the annulus exhaust air. The heaters are used to limit the relative humidity to a maximum of 70 percent in order to maintain the capability of the iodine absorbers to remove iodine from the annulus exhaust air when the AVS accident trains are in operation (RG 1.52 and ASME N509-89). The functional logic is shown in Figure 7.3-31—AVS Accident Filtration Train Heater Control.

Accident Train Switchover

The AVS has a safety-related function to maintain a negative pressure and provide exhaust filtration (GDC 16, GDC 43, Containment Leakage Testing per 10 CFR 50 Appendix J, and NRC RG 1.52 Rev 3). In case of a failure during accident operation of an operating accident filtration train, and a negative pressure is not being maintained in the annulus, operation is switched to the non-operating accident filtration train to maintain a negative pressure and provide exhaust filtration. The functional logic is shown in Figure 7.3-32—AVS Accident Train Switchover.

7.3.1.3.2 Emergency Feedwater System

Emergency Feedwater System SG Level Control

The EFWS has a safety-related function to remove residual heat via the steam generators (SG). The EFWS SG Level control function controls the level within the SG once EFWS actuation function is initiated by the PS. This function is described further in Section 7.3.1.2.2. The functional logic is shown in Figure 7.3-4—EFWS SG

Level Control and Pump Flow Protection.

Emergency Feedwater System Pump Flow Protection

The EFWS has a safety-related function to remove residual heat via the steam generators (SG). The EFWS Pump Flow Protection function controls the flow from the EFW pumps to provide protection against an overflow condition. This function is described further in Section 7.3.1.2.2. The functional logic is shown in Figure 7.3-4.

7.3.1.3.3 Main Control Room Air Conditioning System

The main control room air conditioning system (CRACS) is designed to maintain design temperature conditions for rooms within the Control Room Envelope (CRE) during normal and accident conditions. The CRACS also maintains the habitability of the MCR and associated rooms even in the case of radioactive contamination of the environment. See Section 9.4.1 for more information about the CRACS.

Iodine Filtration Train Heater Control

The CRACS has a sa safety-related function to preheat the inlet air in order to reduce the airborne moisture prior to entry into the carbon bed within the filter unit. The relative humidity is limited to a maximum of 70% in order to maintain the capability of the carbon filters to remove iodine from the annulus supply air. Carbon filter heaters shut down when the respective inlet or outlet dampers are not fully open. The heaters will turn off if the carbon filtration unit fan stops, the carbon filter inlet isolation damper is not open or the carbon filter outlet isolation damper is not open. The functional logic is shown in Figure 7.3-42—CRACS Iodine Filtration Train Heater Control.

Heater Control for Outside Inlet Air

The CRACS has a safety-related function to preheat the outside air to verify that the inlet air temperature is not less than 37°F (GDC 19). The heaters are designed to heat the outside air during cold weather conditions and to preheat the cold outside air to prevent the CRACS air handling unit chilled water cooling coils from freezing. Inlet air that bypasses the iodine filtration unit is heated by an electric heater for temperature control. Heating of the outside air is performed by multi-stage heaters located in each outside air intake duct. The functional logic is shown in Figure 7.3-43—CRACS Heater Control for Outside Inlet Air.

Pressure Control

The CRACS has a safety-related function to verify the MCR is maintained at a positive pressure with respect to the ambient air pressure in adjacent areas to prevent unfiltered in-leakage into the MCR and associated rooms (GDC 19). Differential pressure sensors sense the pressure difference between the MCR and the pressure in a

reference areas. The functional logic is shown in Figure 7.3-44—CRACS Pressure Control.

Cooler Temperature Control

The CRACS has safety-related functions that verify that the air supply temperature is maintained within the preset temperature range (GDC 19). A control signal is developed when the supply air temperature exceeds a preset temperature set point of 58°F. The control signal is used to adjust cooler outlet SCWS control valves to maintain the air supply temperature. The functional logic is shown in Figure 7.3-45—CRACS Cooler Temperature Control.

7.3.1.3.4 Main Steam System

Steam Generator MSRCV Regulation during Standby Position Control

The main steam system (MSS) has a safety-related function supporting the removal of decay heat and other residual heat from the reactor core (GDC 34). The function modulates the main steam relief control valve (MSRCV) to its standby control position, so in the event of an overpressure transient the MSRCVs will already be in its required relieving position. This function is described further in Section 7.3.1.2.5. The functional logic is shown in Figure 7.3-12—MSRCV Control

Steam Generator MSRCV Regulation during Pressure Control

The MSS has a safety-related function supporting the removal of decay heat and other residual heat from the reactor core (GDC 34). The function modulates the MSRCV to its required position in order to reduce secondary side pressure of the SGs during overpressure events. This function is described further in Section 7.3.1.2.5. The functional logic is shown in Figure 7.3-12—MSRCV Control.

7.3.1.3.5 Safeguard Building Controlled-Area Ventilation System

The safeguard building controlled-area ventilation system (SBVS) provides a suitable and controlled environment, in the mechanical areas of the safeguard buildings where ESF components are located, for personnel access and to allow safe operation of the equipment during normal plant operation, outages and under AOOs and PAs. See Section 9.4.5 for more information about the SBVS.

SIS / RHRS Pump Rooms Heat Removal

The SBVS has a safety-related function that maintains ambient conditions below the maximum limits for the rooms of the SIS/RHRS safety-related system components (GDC 60, GDC 61). The functional logic is shown in Figure 7.3-46—SBVS SIS / RHRS Pump Rooms Heat Removal.

CCWS / EFWS Valve Rooms Heat Removal

The SBVS has a safety-related function that maintains ambient conditions below the maximum limits for the rooms of the CCWS/EFWS safety-related system components (GDC 60, GDC 61). The functional logic is shown in Figure 7.3-47—SBVS CCWS / EFWS Valve Rooms Heat Removal.

Isolation of Mechanical Areas of Safeguard Building on Containment Isolation

The SBVS has a safety-related function to automatically isolate the Safeguard Building hot mechanical areas and initiate filtration of exhaust from the areas in the event of a containment isolation signal. This functional logic is shown in Figure 7.3-65—SBVS Isolation of Mechanical Areas of Safeguard Building on Containment Isolation. See Section 9.4.5.3 for more information about this function.

Iodine Filtration Train Electric Heater Control

At the start of an accident, power to both stages of the two-stage electric heater is switched on when the fans start and filter bank isolation dampers open. When the temperature downstream of the heater increases to 158°F, one stage of heater power is switched off. As the temperature downstream of the heater reaches 176°F, the second stage of the heater is also switched off. The functional logic is shown in Figure 7.3-66—SBVS Iodine Filtration Train Electric Heater Control. See Section 9.4.5.2.2 for more information about this function.

7.3.1.3.6 Safety Injection System/Residual Heat Removal System

Automatic RHRS Flow Rate Control

The SIS/RHRS has a safety-related function to provide RCS decay heat removal to reach cold shutdown, refueling modes and to control primary temperature. The function to automatically control the flow rate of the RHRS supports the safety-related function of providing decay heat removal by modulating the bypass control valve ensuring a constant flow rate through the LHSI heat exchanger. The functional logic is shown in Figure 7.3-60—SIS / RHRS Automatic RHRS Flow Rate Control.

7.3.1.4 Essential Auxiliary Support Controls Functional Descriptions

7.3.1.4.1 Component Cooling Water System

The component cooling water system (CCWS) is a closed loop cooling water system that, in conjunction with the essential water service system (ESWS) and the ultimate heat sink (UHS), removes heat generated from the plant's safety related components connected to the CCWS (GDC 44). See Section 9.2.2 for more information about the CCWS.

Common 1.b Automatic Backup Switchover of Train 1 to Train 2

The safety-related function to perform an automatic switchover from Train 1 to Train 2 verifies that the CCWS is capable of fulfilling its safety-related function to remove heat from safety-related components on the CCWS Common 1.a and 1.b headers. The functional logic is shown in Figure 7.3-33—CCWS Common 1.b and 2.b Automatic Backup Switchover.

Common 1.b Automatic Backup Switchover of Train 2 to 1

The safety-related function to perform an automatic switchover from Train 2 to Train 1 verifies that the CCWS is capable of fulfilling its safety-related function to remove heat from safety-related components on the CCWS Common 1.a and 1.b headers. The functional logic is shown in Figure 7.3-33—CCWS Common 1.b and 2.b Automatic Backup Switchover.

Common 2.b Automatic Backup Switchover of Train 3 to 4

The safety-related function to perform an automatic switchover from Train 3 to Train 4 verifies that the CCWS is capable of fulfilling its safety-related function to remove heat from safety-related components on the CCWS Common 2.a and 2.b headers. The functional logic is shown in Figure 7.3-33—CCWS Common 1.b and 2.b Automatic Backup Switchover.

Common 2.b Automatic Backup Switchover of Train 4 to 3

The safety-related function to perform an automatic switchover from Train 4 to Train 3 verifies that the CCWS is capable of fulfilling its safety-related function to remove heat from safety-related components on the CCWS Common 2.a and 2.b headers. The functional logic is shown in Figure 7.3-33—CCWS Common 1.b and 2.b Automatic Backup Switchover.

Emergency Temperature Control

The safety-related function to control the CCWS heat exchanger (HX) outlet temperature is required to maintain the temperature of the cooling water within its limits. This verifies that the CCWS is capable of fulfilling its safety-related function to remove heat from safety-related components. The functional logic is shown in Figure 7.3-34—CCWS Emergency Temperature Control.

The continuous pulse function logic block is used to close the heat exchanger bypass valve 10 percent of its 0-100 percent range at 1 minute intervals. This provides a gradual closing of the heat exchanger bypass valve and, therefore, a gradual cooling to the heat exchanger. The continuous pulse function block is initiated by a high heat exchanger temperature, and the continuous pulse is ended if the heat exchanger temperature falls below the high setpoint or the heat exchanger bypass valve is in the

fully closed position. This provides assurance that the actuation signal is maintained until the execute features go to completion.

Emergency Leak Detection

The safety-related function for emergency leak detection maintains the required cooling water inventory that supports the safety-related function to remove heat using indications to detect leaks and isolate them (GDC 44). The functional logic is shown in Figure 7.3-35—CCWS Emergency Leak Detection.

Emergency Leak Detection - Switchover Valves Leakage or Failure

The safety-related function for switchover valve leakage or failure isolates the CCWS trains from their common headers so that each train is able to provide their corresponding LHSI HX with the required flow for heat removal. Removing heat from the LHSI HX is a safety-related function. The functional logic is shown in Figure 7.3-36—CCWS Emergency Leak Detection - Switchover Valves Leakage or Failure.

SCWS Condenser Supply Water Flow Control

The CCWS has a safety-related function that controls CCWS flow to the SCWS condenser and provides a heat sink for heat rejection, therefore providing reasonable assurance that the SCWS is capable of fulfilling its safety-related functions (GDC 44). The functional logic is shown in Figure 7.3-37—SCWS Condenser Supply Water Flow Control.

7.3.1.4.2 Essential Service Water System

The essential service water system (ESWS) has a safety-related function to remove heat from safety-related components (GDC 44). See Section 9.2.1 for more information about the ESWS.

Automatic ESWS Actuation from CCWS Start

The Automatic ESWS Actuation from CCWS Start function starts the corresponding train ESWS pump so that the SCWS is capable of fulfilling its safety-related function to remove heat from the corresponding CCWS train. This function is performed as a part of the CCWS Automatic Backup Switchover function. A description of this function is in Section 7.3.1.4.1. The functional logic is shown in Figure 7.3-33—CCWS Common 1.b and 2.b Automatic Backup Switchover. See Section 9.2.1.7.1.2 for more information about this function.

ESW Flood Prevention in the Safeguard Building

In case of significant leakage from an ESWS train in a Safeguard Building, the associated motor-driven ESWS pump discharge isolation valve is automatically closed and the ESWS pump is tripped. The nuclear island drain and vent system sump level instrument in the non-controlled areas of the Safeguard Buildings isolates the affected ESWS train. The functional logic is shown in Figure 7.3-69—ESWS Flood Prevention in the Safeguard Building. See Section 9.2.1.3.5 for more information about this function.

7.3.1.4.3 Essential Service Water Pump Building Ventilation System

ESWS Pump Rooms Temperature Control

The essential service water pump building ventilation system (ESWPBVS) has a safety-related function that maintains the ESWS pump room temperature when the ESWS pumps are operating at rated load and the outside air is at maximum site design ambient temperature (GDC 4, GDC 17). The functional logic is shown in Figure 7.3-38—ESWPBVS ESWS Pump Rooms Temperature Control. See Section 9.4.11 for more information about the ESWPBVS.

7.3.1.4.4 Fuel Building Ventilation System

The fuel building ventilation system (FBVS) maintains acceptable ambient conditions in the fuel building to permit personnel access and to control airborne radioactivity in the area during normal plant operation, anticipated occurrences, and following fuel handling accidents. See Section 9.4.2 for more information about the FBVS.

Safety-Related Rooms Heater Control

The FBVS has a safety-related function that maintains the temperature in the boron rooms and surrounding extra borating system tanks to prevent crystallization in extra borating system piping (GDC 27, GDC 60, GDC 61). The functional logic is shown in Figure 7.3-39—FBVS Safety-Related Rooms Heater Control.

EBS / FPCS Pump Rooms Heat Removal

The FBVS has a safety-related function that maintains the room ambient conditions in the extra borating system pump rooms and fuel pool cooling system pump rooms (GDC 27, GDC 60, GDC 61). The functional logic is shown in Figure 7.3-40—FBVS EBS / FPCS Pump Rooms Heat Removal.

Isolation of FBVS on Containment Isolation

The FBVS has a safety-related function to automatically isolate the NABVS supply and exhaust ducts in the event of a containment isolation signal. The functional logic is shown in Figure 7.3-62—Isolation of FBVS on Containment Isolation.

Fuel Handling Accident in the Fuel Building

In the event of a fuel handling accident in the Fuel Building, the air exhaust and supply of the space above the fuel pools are isolated by closing the isolation dampers serving this room. The functional logic is shown in Figure 7.3-67—FBVS Isolation of the Fuel Pool Room. See Section 9.4.2.2.3 for more information about this function.

Fuel Handling Accident in the Containment Building

In the event of a fuel handling accident in the Containment Building, to preclude uncontrolled migration of contamination, the Fuel Building areas in front of the emergency airlock and in front of the equipment hatch are isolated by closing the air exhaust and supply dampers dedicated to these areas. The functional logic is shown in Figure 7.3-68—FBVS Isolation of the Emergency Airlock and Equipment Hatch. See Section 9.4.2.2.3 for more information about this function.

7.3.1.4.5 Fuel Pool Cooling and Purification System

FPCPS Pump Trip on Low SFP Level

The safety-related function to trip the FPC pump on low level so that the FPCPS is capable of fulfilling its safety-related function of precluding the drain down of the SFP to eliminate the potential for fuel damage and its consequences. The functional logic is shown in Figure 7.3-41—FPCPS Pump Trip on Low SFP Level. See Section 9.1.3 for more information about the FPCPS.

7.3.1.4.6 Electrical Division of Safeguard Building Ventilation System

The safeguard building ventilation system (electrical) (SBVSE) maintains acceptable ambient conditions for the safety related electrical equipment, EFW pump rooms and CCWS component rooms in the Safeguard Building during normal plant operation and accident conditions (GDC 4, GDC 17). See Section 9.4.6 for more information about the SBVSE.

Supply and Recirculation-Exhaust Air Flow Control

The SBVSE has a safety-related function to control supply, exhaust, and recirculation air flow as required to maintain ambient temperature and air quality (via filtration) within applicable limits for safety-related equipment located within the Safeguard Building areas and rooms. The pulse function logic block provides a minimum

actuation output time to maintain an actuation signal, until the actuators reach their final position. A pulse order is used to provide assurance that the actions of the execute features go to completion. The functional logic is shown in Figure 7.3-48—SBVSE Supply and Recirculation-Exhaust Air Flow Control.

Supply Fan Safe Shut-Off

An inadvertent stopping of the supply fan, due to a spurious system action, may cause the SBVSE for a given division to become inoperable. Therefore, to mitigate the risk of system spurious actions, this function is to be designated as safety-related (IEEE 603). The functional logic is shown in Figure 7.3-49—SBVSE Supply Fan Safe Shut-Off.

Recirculation Fan Safe Shut-Off

An inadvertent stopping of the recirculation/exhaust fan, due to a spurious system action, may cause the SBVSE for a given division to become inoperable. Therefore, to mitigate the risk of system spurious actions, this function is to be designated as safety-related (IEEE 603). The functional logic is shown in Figure 7.3-50—SBVSE Recirculation Fan Safe Shut-Off.

Exhaust Fan Safe Shut-Off

An inadvertent stopping of the exhaust fan, due to a spurious system action, may cause the SBVSE for a given division to become inoperable. Therefore, to mitigate the risk of system spurious actions, this function is to be designated as safety-related (IEEE 603). The functional logic is shown in Figure 7.3-51—SBVSE Exhaust Fan Safe Shut-Off.

Supply Air Temperature Heater Control

The SBVSE has a safety-related function to maintain supply air temperature (downstream of heaters) as required to maintain ambient temperature within applicable limits for safety-related equipment located within the Safeguard Building areas and rooms. The functional logic is shown in Figure 7.3-52—SBVSE Supply Air Temperature Heater Control.

Freeze Protection

The SBVSE has a safety-related function to prevent ice buildup on the louver bars (specifically, mitigating the risk of not having available makeup air). The functional logic is shown in Figure 7.3-53—SBVSE Freeze Protection.

Supply Air Temperature Control for Supply Air Cooling

The SBVSE has a safety-related function to maintain a constant air temperature, as required, to maintain ambient temperature within applicable limits for safety-related equipment located within the Safeguard Building areas and rooms. The functional

logic is shown in Figure 7.3-54—SBVSE Supply Air Temperature Control for Supply Air Cooling.

Battery Room Heater Control

The SBVSE has a safety-related function to maintain battery room ambient temperature within applicable limits. The functional logic is shown in Figure 7.3-56—SBVSE Battery Room Heater Control.

Battery Room Supply Air Temperature Control

The SBVSE has a safety-related function to maintain battery room ambient temperature within applicable limits. The functional logic is shown in Figure 7.3-57—SBVSE Battery Room Supply Air Temperature Control.

EFWS Pump Room Heat Removal

The SBVSE has a safety-related function to remove heat from the pump room and maintain room temperature within a temperature band for safety-related equipment. The functional logic is shown in Figure 7.3-58—SBVSE EFWS Pump Room Heat Removal.

CCWS Pump Room Heat Removal

The SBVSE has a safety-related function to remove heat from the applicable rooms and maintain room temperature within a temperature band for safety-related equipment. The functional logic is shown in Figure 7.3-59—SBVSE CCWS Pump Room Heat Removal.

7.3.2 Analysis

7.3.2.1 Design Basis Information

Clause 4 of IEEE Std 603-1998 (Reference 5) specifies the information used to establish the design basis for safety-related systems. This section discusses design basis information for the ESF actuation functions. These functions are performed automatically by the PS and the PACS, and manually through the SICS in conjunction with the PS and PACS. The design basis information related to the equipment of these safety-related systems, environmental conditions in which they must function, and methods used to determine their reliability are discussed in Section 7.1.

The design basis information below pertains to the requirements placed on the ESF actuation functions and the variables monitored to initiate ESF systems.

7.3.2.1.1 Design Basis: Applicable Events (Clause 4.a and 4.b of IEEE Std 603-1998)

The AOOs and PAs requiring protective action are analyzed in Chapter 15. The initiating events analyzed are listed in Table 15.0-1. The initial conditions analyzed for each event are presented in Table 15.0-6. Correlation between each event and specific ESF actuation functions is found in Table 15.0-10.

7.3.2.1.2 Design Basis: Permissive Conditions for Operating Bypasses (Clause 4.c of IEEE Std 603-1998)

The operating bypasses applicable to each ESF actuation function are identified in Section 7.3.1.2.1 through Section 7.3.1.2.18. Each operating bypass (permissive signal) is described in Section 7.2.1.3. The functional logic used to generate each operating bypass is also specified in Section 7.2.1.3.

7.3.2.1.3 Design Basis: ESF Actuation Input Variables (Clause 4.d of IEEE Std 603-1998)

Each ESF actuation function is listed in Table 15.0-8 with the relevant nominal trip setpoint, normal and degraded uncertainties, and time delays for the function. For each of these functions, Table 7.3-1—ESF Actuation Variables lists the input variables that are used either directly or as inputs to a calculation to actuate an ESF system. The range to be monitored for each of these variables is also listed in Table 7.3-1. Table 7.3-6—Engineered Safety Features Actuation System Response Times lists the response times for the ESF actuation functions. The definitions and allocation of response times are described in Section 7.1.2.

7.3.2.1.4 Design Basis: Manual ESF System Actuation (Clause 4.e of IEEE Std 603-1998)

The capability for manual system-level actuation and manual component level control of ESF actuators is available to the operator as described in Section 7.3.1.1. Manual actions credited to mitigate AOOs and PAs are identified in Section 15.0, Section 7.2, and in each credited function in Section 7.3.1.2. The variables to be displayed to the operator to use in manual ESF actuation are determined as part of the methodology used for selecting Type A PAM variables as described in Section 7.5.

7.3.2.1.5 Design Basis: Spatially Dependent Variables (Clause 4.f of IEEE Std 603-1998)

The U.S. EPR design uses no spatially dependent variables as inputs to ESF actuation functions.

7.3.2.1.6 Design Basis: Critical Points in Time or Plant Conditions (Clause 4.j of IEEE Std 603-1998)

The PS initiates operation of ESF systems when selected variables exceed the associated setpoints. The plant conditions that define the proper completion of the safety function performed by an ESF system are defined on an event-by-event basis in the Chapter 15 analyses. The actions of the execute features for an ESF actuation function are complete when, for example, a valve has reached its full open or full closed position, or required flow has been established by a pump.

The ESF actuation logic generally allows ESF actuation outputs generated by the PS to be reset after completion of the actions of the execute features. The reset of the ESF actuation signal does not result in change of state (return to normal) of the ESF actuator. Plant specific operating procedures govern the point in time when the ESF actuators can be returned to normal following their actuation.

7.3.2.2 Failure Modes and Effects Analysis

A system-level failure modes and effect analysis (FMEA) is performed on the PS to identify potential single point failures and their consequences. The architecture of the PS as defined in the U.S. EPR Protection System Technical Report (ANP-10309P) (Reference 1) is used as the basis for the analysis. The FMEA considers each major part of the system, how it may fail, and the effect of the failure on the system.

Because the PS is an integrated RT and engineered safety features actuation system (ESFAS), a single failure in the system has the potential to affect both types of functions. Therefore, a single FMEA is performed on the PS and the effects on both RT and ESFAS functions are considered. The result of the FMEA with regard to ESF actuation functions is in ANP-10309P.

7.3.2.3 Compliance with and Conformance to Applicable Criteria

7.3.2.3.1 Compliance with ESF Actuation Functions to the Single Failure Criterion (Clause 5.1 of IEEE Std 603-1998)

The PS maintains the ability to perform all ESF actuation functions in the presence of any credible single failure of an input sensor, functional unit of the PS, or PACS priority module. This is an extension of the redundancy designed into the ESF systems themselves. In general, different divisions of the PS are assigned to actuate those parts of an ESF system considered redundant to one another. Additional redundancy is designed into the PS in the form of redundant ALUs within each division, each capable of actuating one redundant portion of an ESF system.

In most cases, single failures upstream of the ALU voting logic (sensor or APU failure) are accommodated by the voting logic. The voting logic is modified to disregard the input affected by the failure and the ability to actuate based on the remaining inputs is

retained. In the case of the EDG actuation function, sensor failures are accommodated by a two-out-of-three voting logic. Failure of an APU is accommodated in the EDG actuation function by a redundant APU in the other subsystem of the same division performing the same function.

Single failures at the level of the voting logic are accommodated by both redundancy within each division and redundancy between more than one division. In all cases, either of two redundant ALUs within a division can actuate one redundant portion of an ESF function and, except for EDG actuation and EFWS isolation, at least one other division can actuate a second redundant portion of the same ESF function. In the cases of the EDG actuation and the EFWS isolation functions, either of two redundant ALU within a division can perform the voting logic and actuation portions of the functions.

Single failures of PACS priority modules are bounded by the single failure tolerance of the ESF systems themselves. An individual PACS priority module is assigned to each individual actuator so that the failure of a single PACS priority module is no different than the failure of the actuator itself.

A system level FMEA is performed to verify compliance with the single failure criterion. The FMEA is in ANP-10309P.

7.3.2.3.2 Compliance with Requirements and Conformance to Guidances for Quality of Components and Modules (Clause 5.3 of IEEE Std 603-1998 and Clause 5.3 of IEEE Std 7-4.3.2-2003)

Protection system components and modules that are required to perform ESF actuation functions are classified as safety-related, are designed to Class 1E standards, and are applied in accordance with a stringent quality assurance program. Software used to perform ESF actuation functions is developed and applied in accordance with a safety-related software program. Further discussion of compliance with requirements for quality is found in Section 7.1.

7.3.2.3.3 Compliance with Requirements for Independence of ESF and EAS Functions (Clauses 5.6 and 6.3 of IEEE Std 603-1998 and GDC 24)

Redundant portions of the PS and SAS are independent from one another so that a failure in any one portion of the system does not prevent the redundant portions from performing an ESF or EAS function. Both electrical and communication independence are maintained as described in Section 7.1 and in ANP-10309P. Section 11.2 of ANP-10309P provides information on communication independence for any system on the TXS platform.

Equipment required to perform ESF or EAS functions is independent from the effects of the events which the ESF or EAS function mitigates. The functional units of the PS and SAS are located in areas that are not subject to degraded environmental conditions

as the result of an event. Equipment located in areas subject to a degraded environment following an event (e.g., sensors) is qualified to operate as required in the expected post-event environment. Environmental qualification of instrumentation and control equipment is discussed in Section 3.11 and Section 7.1.

The PS and SAS do not rely on input from any non-safety-related control system to perform an ESF actuation function, ESF control function or EAS function. The plant accident analysis does not credit actions taken by non-safety-related control systems to improve the response of ESF or EAS functions. If a control system action can make the effects of an event more severe, then the action is assumed to occur. In this way, the ESF or EAS function is demonstrated to mitigate the event independently of any non-safety-related control system. Certain sensor measurements are shared as inputs to both an ESF or EAS function and a plant control function. In these cases, the measurement is acquired by the signal conditioning of the SCDS. The signal is multiplied and passed to the control system through an electrically isolated connection, to maintain the independence of the ESF or EAS function. Single failures of shared sensors do not impair the functioning of the control system or the ESF function.

Compliance with requirements concerning independence of safety-related instrumentation and control (I&C) systems is addressed further in Section 7.1.

7.3.2.3.4 Compliance with Requirements for Completion of Protective Action (Clauses 5.2 and 7.3 of IEEE Std 603-1998)

Once an ESF actuation function is initiated by the PS, the intended actions of the execute features proceed to completion. The return-to-normal state of ESF actuators requires deliberate operator intervention. In most cases, operator action is required to reset the actuation signal, and separate operator action is required to change the state of the actuated device. When operator action is not required to reset the actuation signal, measures are taken to prevent change in state of the actuated device until the intended actions of the execute features are completed. In many cases, the removal of the PS actuation order from the associated PACS priority module does not result in a change of state of the actuator (e.g., motor operated valves). In cases where removal of the PS actuation order from the associated PACS priority module would result in the actuator changing state (e.g., certain solenoid operators), seal-in features are incorporated in the execute features. These seal-in features allow the reset of the actuation signal while requiring additional operator action to affect the state of the actuated device.

7.3.2.3.5 Compliance with Requirements Concerning Diversity and Defense in Depth (Clause 5.16 of IEEE Std 603-1998)

A non-safety-related diverse actuation system (DAS) is provided to perform selected automatic ESF actuation functions in the unlikely event of an SWCCF failure that

renders the entire PS inoperable. The technology utilized in the DAS are diverse from that used in the PS so that the DAS cannot be subject to the same common cause failure as the PS. The functionality of the DAS is described in Section 7.1 and Section 7.8.

Additionally, manipulation of every ESF system component at the individual component level is available through a processing path completely diverse from the software-based portions of the PS.

The overall EPR I&C approach to diversity and defense in depth is described in the U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report (ANP-10304) (Reference 3).

7.3.2.3.6 Compliance with System Testing and Inoperable Surveillance Requirements (Clause 5.7 of IEEE Std 603-1998)

The design of the PS allows for testing of automatic ESF actuation functions while retaining the capability to perform the functions in response to an event requiring protective action. The majority of the PS and PACS components required for ESF actuation can be tested with the reactor at power. Surveillance of the PS consists of overlapping tests to verify performance of the ESF actuation function from sensor to PACS priority module. Surveillance of the ESF system components consists of actuating the component through the PACS priority module in a manner that overlaps the PS surveillance of the PACS priority module.

The functional units of the PS are continuously monitored through self-testing during power operation. During outages, extended self-testing is performed to verify functionality that cannot be tested with the reactor at power.

Sensors and acquisition circuits are periodically tested. The input channel to be tested is placed in a lockout condition, and the downstream voting logic is automatically modified to disregard the input being tested. The ESF actuation functions are still performed using the redundant input channels.

The connections between the PS output circuits and the PACS priority modules can be tested during power operation. One function of one division of the PS is tested at a time and the outputs of the PACS priority modules are blocked (no actuation signals can be sent) so that the actuators are not affected by the test. The PACS priority modules are blocked for five seconds and then they automatically exit the test mode and their outputs are allowed to send actuation signals. If an ESF actuation order is generated during the time that a PACS priority module is in test mode, the outputs of the PACS priority module remain blocked until the PACS priority module exits the test mode. The ESF actuation functions are still performed using the other PS divisions.

The testing of the PS is described in the U.S. EPR Protection System Surveillance Testing and TELEPERM XS Self-Monitoring Technical Report (ANP-10315P) (Reference 7).

7.3.2.3.7 Conformance to Guidance Regarding the Use of Digital Systems (IEEE Std 7-4.3.2-2003)

The automatic ESF actuation functions are implemented using the TELEPERM XS platform (Reference 2) which is approved for use in safety-related systems of nuclear power generating stations in the United States. The ESF actuation functions are implemented in an architecture designed to satisfy requirements applicable to all safety-related I&C systems.

Implementation of safety-related I&C systems is governed by the requirements of IEEE Std 603-1998 (Reference 5). Compliance with this requirement is described in Section 7.1. Guidance on the use of digital computers in safety-related systems is provided by IEEE Std 7-4.3.2-2003 (Reference 6). Conformance to this guidance is described in Section 7.1.

7.3.2.3.8 Compliance with Requirements for ESF Actuation Setpoint Determination (Clause 6.8 of IEEE Std 603-1998)

Each setpoint used to actuate an ESF system is selected based on the safety limits assumed in the plant accident analysis. The ESF actuation setpoints provide margin to the safety limit and take into account measurement uncertainties. The methodology to determine setpoints for ESF actuation functions is documented in the U.S. EPR Instrument Setpoint Topical Report (ANP-10275P-A) (Reference 4). The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

7.3.3 References

1. [*ANP-10309P, Revision 5, "U.S. EPR Protection System Technical Report," AREVA NP Inc., May 2013.*

2. *EMF-2110(NP)(A), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," Siemens Power Corporation, July 2000.*

3. *ANP-10304, Revision 6, "U.S. EPR Diversity and Defense-In-Depth Assessment Technical Report," AREVA NP Inc., May 2013.*

4. *ANP-10275P-A, Revision 0, "U.S. EPR Instrument Setpoint Methodology Topical Report," AREVA NP Inc., January 2008.*]*

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

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

7. [*ANP-10315P, Revision 2, "U.S. EPR Surveillance Testing and TELEPERM XS Self-Monitoring Technical Report," AREVA NP Inc., May 2013.*]*

Table 7.3-1—ESF Actuation Variables
Sheet 1 of 2

Protective Function	Variables To Be Monitored	Range of Variables
Safety Injection System Actuation	Pressurizer Pressure (NR)	1615-2515 psia
	Hot Leg Pressure (WR)	15-3015 psia
	Hot Leg Temperature (WR)	32-662°F
	Hot Leg Loop Level	0-30.71 in.
Reactor Coolant Pump Trip	RCP differential pressure	0-120% nominal
Emergency Feedwater System Actuation	SG Level (WR)	0-100% MR
Emergency Feedwater System Isolation	SG Level (WR)	0-100% MR
SG Isolation	Main Steam Line Activity	$1x10^{-1}$ – $1x10^{4}$ counts/ sec.
	SG Level (NR)	0-100% MR
Main Steam Relief Isolation Valve Opening	SG Pressure	15-1615 psia
Main Steam Relief Train Isolation	SG Pressure	15-1615 psia
Main Steam Isolation	SG Pressure	15-1615 psia
	Cont. Equipment Compartment Pressure	-3 to +7 psig
	Cont. Service Compartment Pressure (NR)	-3 to +7 psig
Main Feedwater Isolation	SG Level (NR)	0-100% MR
	SG Pressure	15-1615 psia
	Cont. Equipment Compartment Pressure	-3 to +7 psig
	Cont. Service Compartment Pressure (NR)	-3 to +7 psig
Containment Isolation	Cont. Service Compartment Pressure (NR)	-3 to +7 psig
	Cont. Service Compartment Pressure (WR)	-5 to +220 psig
	Cont. Equipment Compartment Pressure	-3 to +7 psig
	Containment High Range Activity	$1x10^{-1}$ – $1x10^{7}$ Rad/hr
Emergency Diesel Generator Actuation	6.9 kV Bus Voltage	0-8.625 kV
PSRV Opening	Hot Leg Pressure (NR)	0-870 psia
CVCS Charging Isolation	Pressurizer Level (NR)	0-100% MR

Table 7.3-1—ESF Actuation Variables
Sheet 2 of 2

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

NOTES

MR = Measuring Range

Table 7.3-2—Deleted

Table 7.3-3—Deleted

Table 7.3-4—Deleted

Table 7.3-5—Protection System Manually Actuated Functions

Reactor Trip
Containment Isolation (Stage 1)
Containment Isolation (Stage 2)
CVCS Charging Isolation
CVCS Isolation on Anti-Dilution Mitigation
EDG Actuation
EFWS Actuation
EFWS Isolation
Extra Borating System Isolation
Hydrogen Mixing Dampers Opening
CRACS Isolation and Filtering
Main Feedwater (MFW) Full Load Isolation
Main Steam Isolation
MSRIV Opening
MSRT Isolation
Partial Cooldown Actuation
PSRV Opening
RCP Trip
SG Isolation
SIS Actuation
Turbine Trip

Table 7.3-6—Engineered Safety Features Actuation System Response Times
Sheet 1 of 9

Function	Total Response Time (s)	T1	T2	T3	T4	T3 Definition	T4 Definition
ESFAS							
Safety Injection System Actuation							
SIS actuation on pressurizer pressure < Min3p (w/o LOOP)	16.5	0.4	1.1	0.5	14.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
SIS actuation on pressurizer pressure < Min3p (with LOOP and EDG loading)	41.5	0.4	1.1	25.5	14.5	The maximum time delay for the MCC or switchgear including EDG activities (max time delay = EDG start delay + EDG loading delay + MCC or switchgear delay). See Note 1 for more details	The maximum time delay for valve and pump actuation. See Note 2 for more details.
SIS actuation on RCS Hot Leg ΔPsat < Min1p (w/o LOOP)	15.5 plus sensor delays	0.4 (Hot leg press. WR) 4 (Hot leg temp. WR)	0.5	0.5	14.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
SIS actuation on RCS Hot Leg ΔPsat < Min1p (with LOOP including EDG loading)	40.5 plus sensor delays	0.4 (Hot leg press. WR) 4 (Hot leg temp. WR)	0.5	25.5	14.5	The maximum time delay for the MCC or switchgear including EDG activities (max time delay = EDG start delay + EDG loading delay + MCC or switchgear delay). See Note 1 for more details	The maximum time delay for valve and pump actuation. See Note 2 for more details.

Table 7.3-6—Engineered Safety Features Actuation System Response Times
Sheet 2 of 9

Function	Total Response Time (s)	T1	T2	T3	T4	T3 Definition	T4 Definition
SIS actuation on RCS Loop Level < Min1p (w/o LOOP)	16.5	1	0.5	0.5	14.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
SIS actuation on RCS Loop Level < Min1p (with LOOP and EDG loading)	41.5	1	0.5	25.5	14.5	The maximum time delay for the MCC or switchgear including EDG activities (max time delay = EDG start delay + EDG loading delay + MCC or switchgear delay). See Note 1 for more details	The maximum time delay for valve and pump actuation. See Note 2 for more details.
Emergency Feedwater System Actuation							
EFWS actuation on SG Level < Min2p (WR) (affected SG) (w/ o LOOP)	16.5	1	0.5	0.5	14.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
EFWS actuation on SG Level < Min2p (WR) (affected SG) (with LOOP including EDG loading)	61.5	1	0.5	45.5	14.5	The maximum time delay for the MCC or switchgear including EDG activities (max time delay = EDG start delay + EDG loading delay + MCC or switchgear delay). See Note 1 for more details	The maximum time delay for valve and pump actuation. See Note 2 for more details.

Table 7.3-6—Engineered Safety Features Actuation System Response Times
Sheet 3 of 9

Function	Total Response Time (s)	T1	T2	T3	T4	T3 Definition	T4 Definition
EFWS actuation on LOOP + SIS Actuation (includes EDG loading)	60	None	None	45.5	14.5	The maximum time delay for the MCC or switchgear including EDG activities (max time delay = EDG start delay + EDG loading delay + MCC or switchgear delay). See Note 1 for more details	The maximum time delay for valve and pump actuation. See Note 2 for more details.
SG blowdown isolation (affected SG)	21.5	1	0.5	0.5	19.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
EFW level control	N/A	N/A	N/A	N/A	N/A	N/A	N/A
EFWS pump overflow protection	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Emergency Feedwater System Isolation							
EFWS isolation on SG Level > Max1p (WR) (affected SG)	61.5	1	0.5	0.5	59.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
SG Isolation Signal	See SG Isolation below						
Partial Cooldown Actuation							
SIS Actuation Signal generated	None	N/A	N/A	N/A	N/A	N/A	N/A

Table 7.3-6—Engineered Safety Features Actuation System Response Times
Sheet 4 of 9

Function	Total Response Time (s)	T1	T2	T3	T4	T3 Definition	T4 Definition
MSRT Actuation							
MSRT opening (MSRIV) on SG Pressure > Max1p (affected SG)	2.7	0.4	0.5	0.1	1.7	The time required from receiving a signal from the DCS to when the relay contacts change states from normally open to normally closed, or normally closed to normally open.	The maximum time delay for valve and pump actuation. See Note 2 for more details.
MSRT isolation (MSRIV, MSRCV) on SG Pressure < Min3p (affected SG)	5.9	0.4	0.5	0.1	4.9	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
Main Steam Isolation							
MSIV closure on SG pressure drop > Max1p (all SGs)	5.9	0.4	0.5	0.5	4.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
MSIV closure on SG pressure < Min1p (all SGs)	5.9	0.4	0.5	0.5	4.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
MSIV closure on High Containment pressure	See Containment Isolation below						
SG Isolation Signal	See SG Isolation below						

Table 7.3-6—Engineered Safety Features Actuation System Response Times
Sheet 5 of 9

Function	Total Response Time (s)	T1	T2	T3	T4	T3 Definition	T4 Definition
Main Feedwater Isolation							
MFW full load isolation on Reactor Trip (all SGs)	40	None	None	0.5	39.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
MFW full load isolation on SG Level > Max1p (NR) (affected SG)	41.5	1	0.5	0.5	39.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
MFW SSS isolation on SG level > Max0p (NR) for period of time (affected SG)	21.5	1	0.5	0.5	19.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
MFW SSS isolation on SG pressure drop > Max2p (affected SG)	20.9	0.4	0.5	0.5	19.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
MFW SSS isolation on SG pressure < Min2p (affected SG)	20.9	0.4	0.5	0.5	19.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
MFW SSS isolation on High Containment pressure	See Containment Isolation function below						
SG Isolation Signal	See SG Isolation below						
Containment Isolation							
Containment equipment compartment pressure > Max1p (Stage 1)	0.9 plus T3 and T4	0.4	0.5	See Section 6.2.4	See Section 6.2.4	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
Containment service compartment pressure (NR) > Max2p (Stage 1)	0.9 plus T3 and T4	0.4	0.5	See Section 6.2.4	See Section 6.2.4	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.

Table 7.3-6—Engineered Safety Features Actuation System Response Times
Sheet 6 of 9

Function	Total Response Time (s)	T1	T2	T3	T4	T3 Definition	T4 Definition
Containment activity > Max1p (Stage 1)	5.0 plus T3 and T4	4.5	0.5	See Section 6.2.4	See Section 6.2.4	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
SIS Actuation Signal (Stage 1)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Containment service compartment pressure (WR) > Max3p (Stages 1 & 2)	0.9 plus T3 and T4	0.4	0.5	See Section 6.2.4	See Section 6.2.4	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
CVCS Charging Isolation							
CVCS charging line isolation on pressurizer level > Max2p	41.5	1	0.5	0.5	39.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
CVCS Isolation for Anti-Dilution							
Anti-Dilution (power)	105.5	65	0.5	0.5	39.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
Anti-Dilution (shutdown)	105.5	65 (Boron concentration) negligible (Cold leg temperature WR) negligible (CVCS charging line flow)	0.5	0.5	39.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.

Table 7.3-6—Engineered Safety Features Actuation System Response Times
Sheet 7 of 9

Function	Total Response Time (s)	T1	T2	T3	T4	T3 Definition	T4 Definition
Anti-Dilution (shutdown no RCPs)	105.5	65 (Boron Concentration) negligible (CVCS charging line flow)	0.5	0.5	39.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
Steam Generator Isolation							
MSRT Setpoint Increase on SG Level > Max2p + partial cooldown initiated (affected SG)	1.5	1	0.5	None	None	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
MSRT setpoint increase on high steam line activity + partial cooldown initiated (affected SG)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
MSIV closure on SG level > Max2p (NR) + partial cooldown initiated (affected SG)	6.5	1	0.5	0.5	4.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
MSIV closure on high steam line activity + partial cooldown initiated (affected SG)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
MFW SSS Isolation on SG level > Max2p (NR) + partial cooldown initiated (affected SG)	21.5	1	0.5	0.5	19.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.

Table 7.3-6—Engineered Safety Features Actuation System Response Times
Sheet 8 of 9

Function	Total Response Time (s)	T1	T2	T3	T4	T3 Definition	T4 Definition
MFW SSS isolation on high steam line activity + partial cooldown initiated (affected SG)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
EFWS isolation on SG Level (NR) > Max2p + partial cooldown initiated (affected SG)	61.5	1	0.5	0.5	59.5	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
EFWS isolation on High Steam Line Activity + partial cooldown initiated (affected SG)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Reactor Coolant Pump Trip							
RCP Trip on ΔP over RCP < Min1p + SIS signal	3.9	0.4	0.5	3	None	This is the maximum delay time from the outputs of the DCS to when the power is removed from the RCPs.	N/A
MCR AC System Isolation							
MCR air intake activity > Max1p	17	6	0.5	0.5	10	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.

Table 7.3-6—Engineered Safety Features Actuation System Response Times
Sheet 9 of 9

Function	Total Response Time (s)	T1	T2	T3	T4	T3 Definition	T4 Definition
Turbine Trip on RT							
Initiation of RT	N/A (See Note 3)	N/A	N/A (See Note 3)	N/A	N/A	N/A	N/A
EDG on LOOP or degraded voltage							
EBS							
EBS Isolation	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Hydrogen Mixing Dampers Opening							
Containment service compartment pressure (NR) > Max1p	18	0.4	0.5	0.5	16.6	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.
Containment equipment compartment/containment service compartment ΔP > Max1p	18	0.4	0.5	0.5	16.6	See Note 1	The maximum time delay for valve and pump actuation. See Note 2 for more details.

1. The maximum delay time from the input of the switchgear or MCC to the input of the motors, pumps, valves, etc. considering the shunt trip operating time, mechanism operating time, arcing time, and auxiliary relay operating time. For emergency diesel generators (EDG): The maximum time delay from when the EDGs receive the start signal to when the EDGs reach the rated load including the EDG loading.

2. The following is the T4 definition for various actuated equipment in the plant:
   For all valves (or dampers): The maximum time delay from when the valve (or damper) receives the signal from the switchgear to when the valve (or damper) goes to full open or full closed position.

   – For motor operated valves: The maximum time delay from when the motor receives the signal from the MCC to when the valve goes to full open or full closed position.

- For air-operated valves: The maximum time delay from when the valve receives the signal from the switchgear to when the valve goes to full open or full closed position. This includes the time it takes the solenoid (air supply) or pilot valve to actuate.

- For hydraulic actuated valves: The maximum time delay from when the valve receives the signal from the switchgear to when the valve goes to full open or full closed position. This includes the time it takes the solenoid (control flow of hydraulic fluid) or pilot valve to actuate.

- For pumps: The maximum time delay from when the pump receives a signal from MCC or switchgear to when the pump provides full flow.

3. The response time indicated for the Turbine Trip on RT is the minimum time based on the capability of the DCS equipment. Safety analysis requires a minimum response time of at least one second between a RT and a Turbine Trip. Therefore, a one-second time delay is implemented in the DCS software design for this function.

Figure 7.3-1—ESF Actuation
(Sheet 1 of 5)

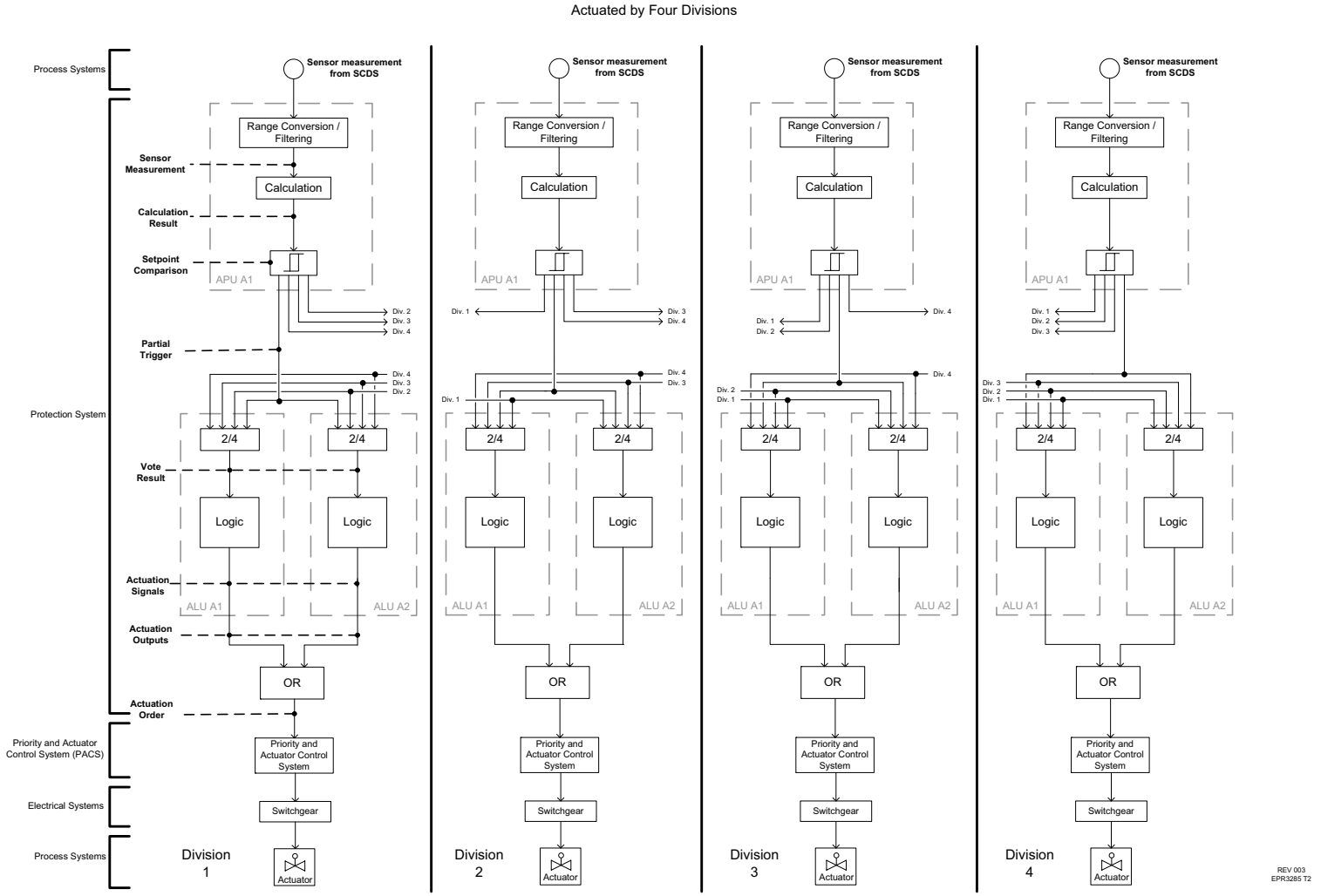
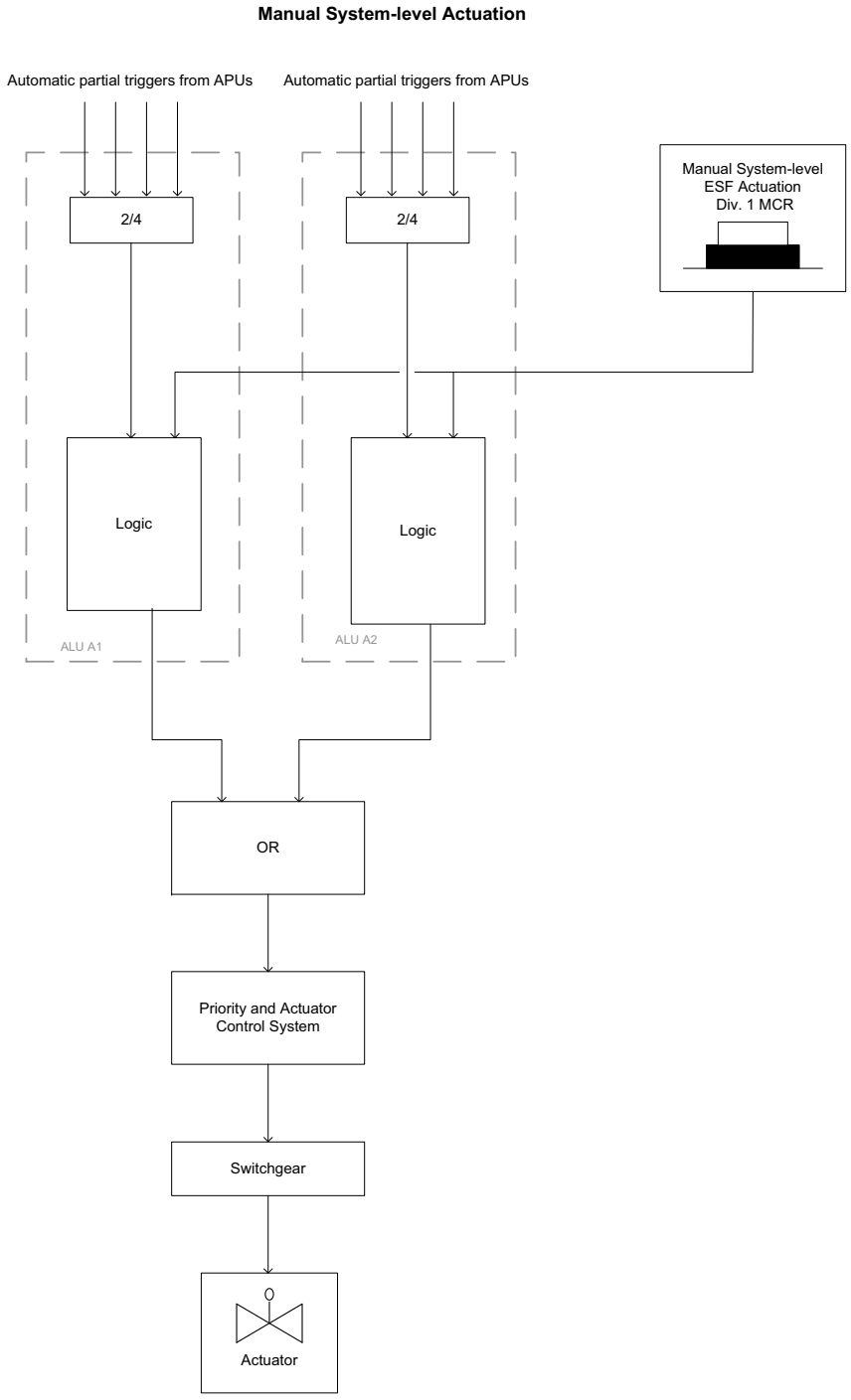


Figure 7.3-1—ESF Actuation
(Sheet 2 of 5)



EPR3286 T2

Figure 7.3-1—ESF Actuation
(Sheet 3 of 5)

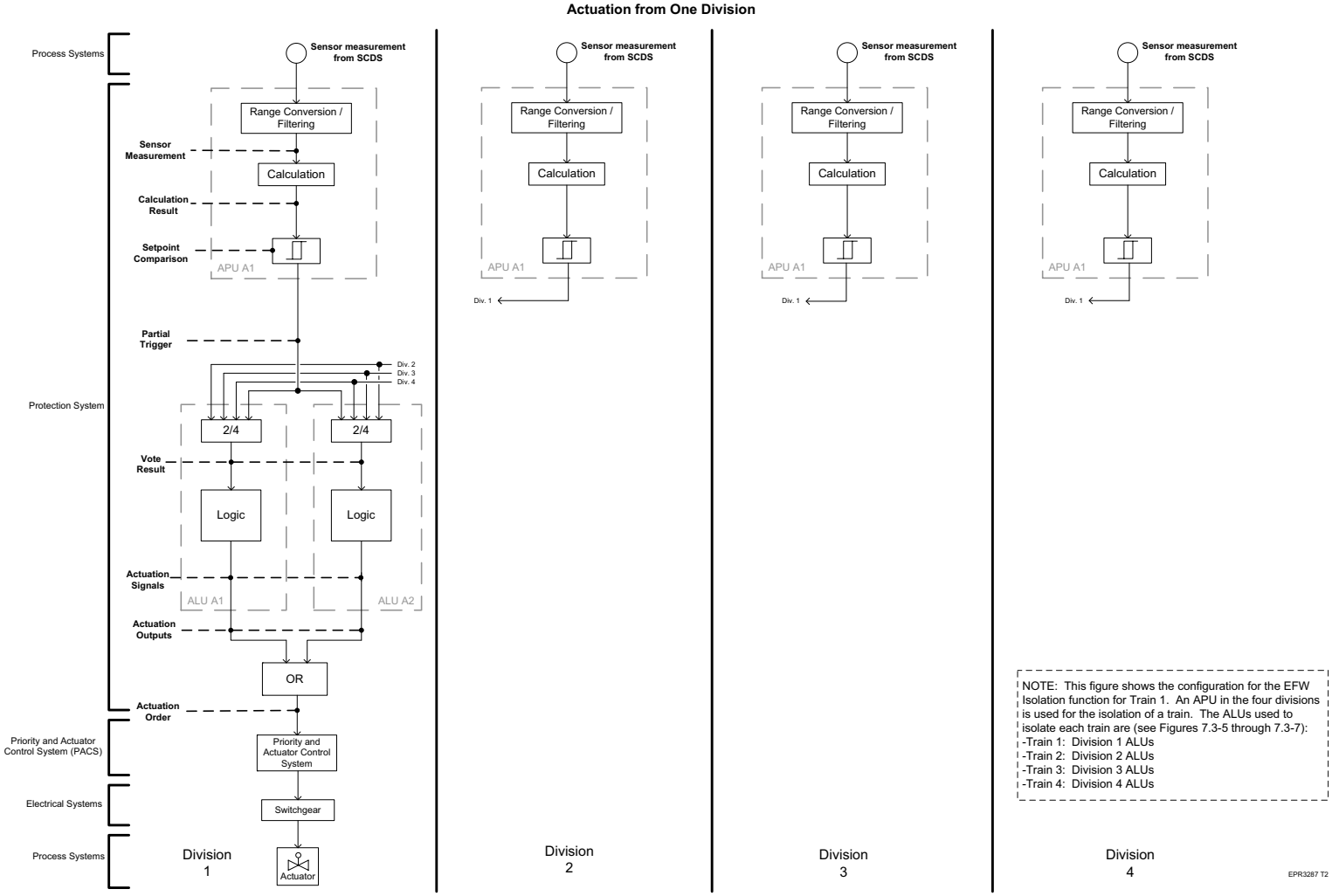


Figure 7.3-1—ESF Actuation
(Sheet 4 of 5)

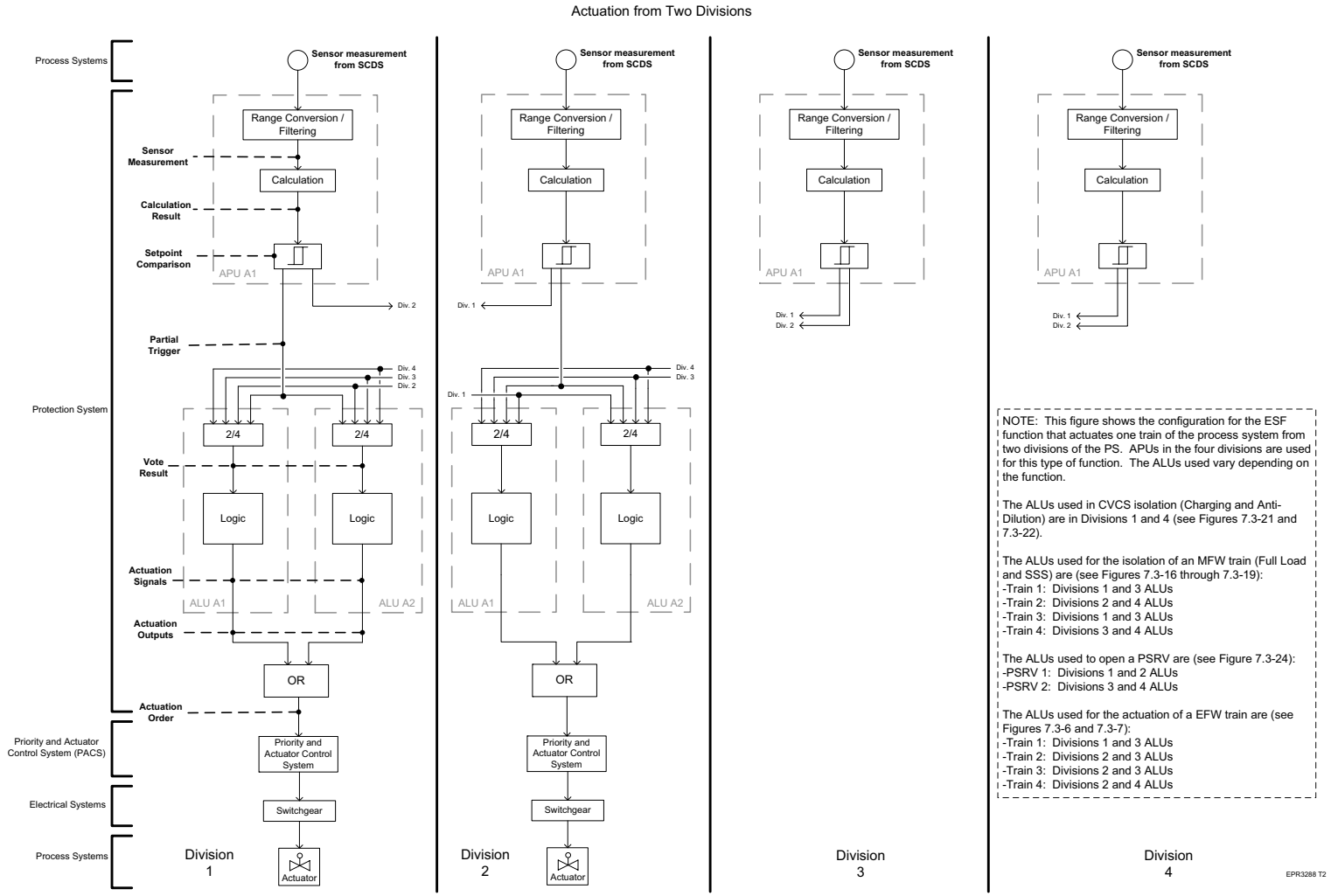
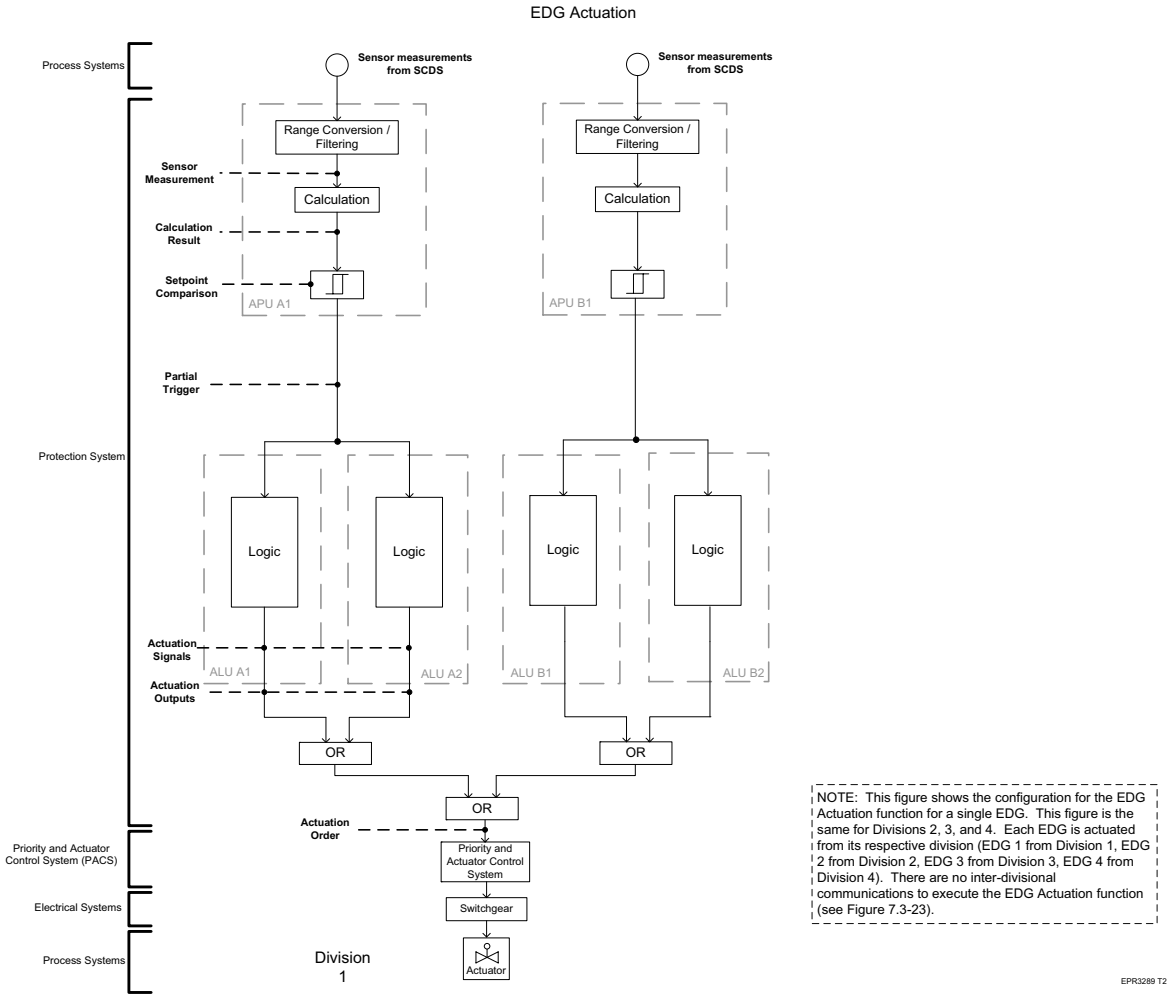


Figure 7.3-1—ESF Actuation
(Sheet 5 of 5)



Next File