7.2 Reactor Trip System

7.2.1 Description

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

7.2.1.1 System Description

The PS processes both automatic and manual RT functions. Each RT function is performed redundantly and independently in each of the four PS divisions. An RT order, produced by any two of the four divisions, results in a reactor shutdown. The functional description and architecture of the PS is described in Section 7.1.1.3.

Key process variables are continuously monitored to determine the safety status of the plant. Three categories of variables are used as inputs to automatic RT functions:

- Incore instrumentation: The self powered neutron detectors (SPND) are used as inputs to calculate variables that cannot be directly measured, such as linear power density and departure from nucleate boiling ratio (DNBR). The incore instrumentation system is described in Section 7.1.1.4.

- Excore instrumentation: The power range detectors (PRD) and intermediate range detectors (IRD) provide measurements of reactor power, and are used as inputs to RT functions that detect conditions such as high neutron flux and low doubling time. The excore instrumentation system is described in Section 7.1.1.4.

- Process instrumentation: Process instrumentation is used to measure variables such as pressure, temperature and flow. These process measurements are used directly to initiate RT or as inputs to calculations of variables that cannot be measured directly.

Any one of three diverse sets of RT devices can successfully remove power to the CRDM coils. The sets are the RT breakers, the RT contactors, and the transistors of CRDM operating coils. When an RT order is generated, the PS acts on all three sets of RT devices as described:

- RT breakers: There are four RT breakers, two each in electrical divisions 2 and 3. Each division of the PS acts on the undervoltage coil of one RT breaker. The opening of one breaker in electrical division 2 and one breaker in electrical division 3 results in reactor shutdown. The RT breakers are part of the non-Class 1E power supply (NUPS) system and are described in Section 8.3.

- RT contactors: There are 23 sets of four RT contactors. Eleven sets of contactors are in electrical division 1 and twelve sets are in division 4. Each set of contactors supplies power to four CRDMs, with the exception of one set in division 4 which supplies power to only the center CRDM. Each division of the PS opens one contactor in each of the 23 sets. Each set of contactors is arranged in a two out of four configuration, so that RT orders issued from any two PS divisions results in reactor shutdown. The RT contactors are part of the control rod drive control system which is described in Section 7.1.1.4.

- Transistors of CRDM operating coils: The transistors that control power to the CRDM operating coils are part of the CRDCS and are not safety-related trip devices. However, they are the fastest acting of the trip devices and allow the safety-related RT breakers and RT contactors to open under un-loaded conditions. Each transistor that controls power to a CRDM is de-energized based on the result of two out of four voting on the divisional RT orders from the four PS divisions.

Figure 7.2–4—Safety Related RT Devices, illustrates the arrangement and divisional assignments of the safety-related RT devices.

An automatic RT actuation is performed by the PS when selected plant parameters reach appropriate setpoints. The typical sequence performed by the PS to initiate an automatic RT is illustrated in Figure 7.2–1—Typical Reactor Trip Sequence (One Division) and is described:

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

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

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

- The RT signals of the redundant ALU in each sub-system are combined in a hardwired “functional AND gate” logic. If an RT signal is present from both redundant ALU, an RT output is generated. The RT outputs from both sub-systems in a division are combined in a hardwired “functional OR gate” logic. If either subsystem produces an RT output, a divisional RT order is propagated to the RT breakers, RT contactors and transistors of the CRDM operating coils.

Automatic RT functions that use SPND measurements as inputs utilize an additional level of computer function. This additional level consists of redundant remote acquisition units (RAU) in each division dedicated to the acquisition and distribution of the SPND measurements. The RAU in each division acquire one-fourth of the total SPND measurements and distribute those measurements to APU in all four divisions allowing for an accurate calculation over the whole reactor core in each division. Once the SPND measurements have been received by the APU, the RT function is carried out as described previously in this section for the typical RT function. Figure 7.2–2—Typical SPND-based RT Actuation illustrates the typical RT initiation sequence for SPND-based RT functions.

The capability for manual RT is available to the operator through the safety information and control system (SICS) in both the MCR and RSS. At each location, four manual RT buttons are provided to correspond to the four PS divisions. Manual RT initiation is illustrated in Figure 7.2–3—Manual RT and is also described in ANP-10281P, "U.S. EPR Digital Protection System Topical Report (Reference 1). The SICS is described in Section 7.1.1.2.

7.2.1.2 Reactor Trip Functional Description

The variables monitored by the PS are used either directly or as an input to a calculation, to detect the plant conditions which initiate reactor shutdown:

- Low departure from nucleate boiling ratio.
- High linear power density.
- High neutron flux rate of change.
- High core power level.
- Low saturation margin.
- Low reactor coolant system loop flow (two loops).
- Low-low reactor coolant system loop flow (one loop).
- Low reactor coolant pump speed.
- High neutron flux.
- Low doubling time.
- Low pressurizer pressure.
- High pressurizer pressure.
- High pressurizer level.

- Low hot leg pressure.
- Steam generator pressure drop.
- Low steam generator pressure.
- High steam generator pressure.
- Low steam generator level.
- High steam generator level.
- High containment pressure.

Each of these process conditions is determined to exist when a pre-defined or variable setpoint is exceeded by a related process parameter. The specific setpoint values are chosen to protect safety limits and support the assumptions made in the plant safety analysis as described in Chapter 15. The variables monitored for RT and their measuring ranges are listed in Table 7.2–1—Reactor Trip Variables.

In addition to the process conditions that cause RT, these safety-related signals initiate an RT:

- Safety injection system (SIS) actuation.
- Emergency feedwater system (EFWS) actuation.
- Manual RT signals from SICS.

Operating bypasses of specific RT functions are permitted when plant conditions dictate that the function is not needed, or that the function would prevent proper plant operation. These bypasses are implemented in the form of permissive signals (P#) that are generated within the PS. The logic used to generate the permissive signals is described in Section 7.2.1.3. The applicable permissive signals (if any) associated with each RT are identified in the description of each function in Section 7.2.1.2.1 through Section 7.2.1.2.22.

7.2.1.2.1 Reactor Trip on Low Departure From Nucleate Boiling Ratio

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

The DNBR calculation performed by the PS is described in Reference 3 and is based on:

- Power density distribution of the hot channel: This parameter is directly derived from the SPND measurements.
- Inlet temperature: This parameter is derived from the cold leg temperature sensors.
- Pressure: This parameter is given by the pressurizer pressure sensors.
- Core Flow Rate: This parameter is derived from the reactor coolant pump (RCP) speed sensors.

The outputs of the DNBR calculation consist of twelve DNBR values (one per SPND finger), and twelve outlet quality values (one per SPND finger). The output values are used in various combinations to generate an RT:

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

The values of the variable low DNBR setpoints depend on the number of invalidated SPND fingers. Each SPND input signal is monitored by the PS, using both inherent and engineered monitoring mechanisms, to determine the validity of the signal. A description of the inherent and engineered monitoring features utilized by TELEPERM XS is found in Reference 1 and EMF-2110(NP)(A), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," (Reference 2). If an SPND input signal is determined to be invalid, it is automatically assigned a faulty status. Additionally, if an SPND is determined to be faulty in the course of manual surveillance, the corresponding input signal is manually assigned a faulty status. Since the DNBR calculation produces its outputs on a per-finger basis (six SPND per finger), if one SPND carries a faulty status, then the entire finger is considered invalid. One of six pre-determined setpoint values is automatically selected for use based on the number of invalidated fingers. This is done for each of the three variable setpoints used in the DNBR function. The determination of setpoint values for the variable DNBR setpoints as well as the fixed high quality setpoints is described in ANF-10287P, "Incore Trip Setpoint and Transient Methodology for U.S. EPR" (Reference 3).

The rod drop (1/4) and rod drop (2/4) signals are based on the rate of change of the rod position measurements acquired by the PS. If a dropped rod is detected in one

quadrant of the core, the rod drop (1/4) signal is generated, and the corresponding setpoints are activated. If a dropped rod is detected in two or more quadrants of the core, the rod drop (2/4) signal is generated and the corresponding DNBR setpoint is activated. The logic for generation of the rod drop signals is shown in Figure 7.2–5—Low DNBR (1 of 2).

The SPND imbalance signal is generated based on an indication of asymmetrical power distribution in the core. All 72 SPND measurements are used in each PS division to detect this condition. The calculation of the SPND imbalance condition is described in Reference 3.

The P2 permissive condition bypasses the low DNBR RT function at low power levels. This bypass is automatically removed as power increases above the P2 setpoint. Generation of the P2 permissive signal is described in Section 7.2.1.3.

The logic for the low DNBR RT function is shown in Figure 7.2–6—Low DNBR (2 of 2).

7.2.1.2.2 Reactor Trip on High Linear Power Density

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

The calculation of HLPD performed by the PS uses the 72 SPND measurements as inputs. The HLPD calculation is described in Reference 3 and is performed on a per-SPND basis, resulting in 72 values of HLPD.

The second highest value of HLPD from the 72 calculated values is compared to a variable high setpoint to generate an RT. The value of the variable setpoint depends on the number of invalidated SPND measurements.

Each SPND input signal is monitored by the PS, using both inherent and engineered monitoring mechanisms, to determine the validity of the signal. A description of the inherent and engineered monitoring features utilized by TELEPERM XS is found in References 1 and 2. If an SPND input signal is determined to be invalid, it is automatically assigned a faulty status. Additionally, if an SPND is determined to be faulty in the course of manual surveillance, the corresponding input signal is manually assigned a faulty status. One of six pre-determined setpoint values is automatically selected for use based on the number of invalidated SPND. The determination of setpoint values used in the HLPD RT function is described in Reference 3.

The P2 permissive condition bypasses the HLPD RT function at low power levels. This bypass is automatically removed as power increases above the P2 setpoint. Generation of the P2 permissive signal is described in Section 7.2.1.3.

The logic for the HLPD RT function is shown in Figure 7.2–7—High Linear Power Density.

7.2.1.2.3 Reactor Trip on High Neutron Flux Rate of Change

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

The initiating signal is the derivative of neutron flux derived from measurements provided by the power range detectors (PRD). Each PS division acquires measurements from one of four pairs of PRD. Each pair consists of one measurement taken from the top half of the core, and one measurement taken from the bottom half. A calculation of nuclear power is performed in each division based on the two measurements acquired in that division:

$$Q_N = K_{CALN} * \left(K_{CAL1} * i(1) + K_{CAL2} * i(2)\right)$$

Where:

Q_N = Nuclear power expressed

i(1) = Top PRD measurement

i(2) = Bottom PRD measurement

K_{CAL1} = Calibration coefficient applied to the top measurement

K_{CAL2} = Calibration coefficient applied to the bottom measurement

K_{CALN} = Calibration coefficient applied to the sum of the calibrated top and bottom measurements

A rate/lag filter is then applied to the calculated nuclear power value to obtain a signal representative of the derivative of neutron flux. The derivative value is compared to a fixed high setpoint to generate an RT.

There are no operating bypasses associated with the high neutron flux rate of change RT. The logic for this function is shown in Figure 7.2–8—High Neutron Flux Rate of Change.

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

The RT on high core power level (HCPL) is provided to protect against an excessive reactivity addition during operation at intermediate and high power levels. This function uses an enthalpy balance to calculate core thermal power. Additionally, an

RT on low saturation margin is introduced because, in case of saturation occurring in a hot leg, the thermal core power level calculation becomes invalid.

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

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

Where:

Q_{TH}= Thermal core power

K_{CALTH}= Calibration constant

M = Mass of water in the core

H = Average specific enthalpy of the water in the core

H_{IN} = Specific enthalpy at the core inlet

H_{OUT} = Specific enthalpy at the core outlet

W_{IN}= Mass flow rate at the core inlet

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

The mass flow rate is calculated by using the enthalpy and the pressure to determine a local density, which is then multiplied by the nominal core flow rate (constant value). A three loop operating signal is used to account for the change in flow rate caused by the shutdown of an RCP. The three loop operating signal is generated as part of the low RCS flow rate RT function (refer to Section 7.2.1.2.5).

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

The resulting value of thermal core power is compared to a fixed high setpoint to generate an RT.

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

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

The resulting value of saturation margin is compared to a fixed low setpoint to generate an RT.

The P5 permissive condition bypasses both the high core power level and low saturation margin RT functions at low power levels. This bypass is automatically removed as power increases above the P5 setpoint. Generation of the P5 permissive signal is described in Section 7.2.1.3.

The logic for these functions is shown in Figure 7.2–9—High Core Power Level & Low Saturation Margin.

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

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

Four redundant flow measurements are taken in each RCS loop. Each division of the PS acquires one sensor from each loop, and each is compared to a fixed low setpoint (MIN1p). If two partial triggers are generated for one RCS loop, the flow in that loop is considered low. An additional level of two-out-of-four voting logic is then applied so that a low flow must be detected in at least two RCS loops to generate an RT. If a low flow condition is present in any one RCS loop, a three loop operating signal is generated. This signal is used to modify other PS functions which assume a nominal flow rate through the core.

The P2 permissive condition bypasses the low RCS flow rate–two loops RT function at low power levels. This bypass is automatically removed as power increases above the P2 setpoint. Generation of the P2 permissive signal is described in Section 7.2.1.3.

The logic for the low RCS flow rate RT function is shown in Figure 7.2–10—Low RCS Flow.

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

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

The 16 RCS flow sensor measurements are acquired by the PS in the manner described in Section 7.2.1.2.5. The individual flow measurements are compared to a fixed low setpoint (Min2p). If two partial triggers are generated for low-low flow in any one RCS loop, RT orders are generated.

The P3 permissive condition bypasses the low RCS flow rate–one loop RT function at low power levels. This bypass is automatically removed as power increases above the P3 setpoint. Generation of the P3 permissive signal is described in Section 7.2.1.3.

The logic for the low-low RCS flow rate RT function is shown in Figure 7.2–11—Low-Low RCS flow.

7.2.1.2.7 Reactor Trip on Low Reactor Coolant Pump Speed

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

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

The P2 permissive condition bypasses the low RCP speed RT function at low power levels. This bypass is automatically removed as power increases above the P2 setpoint. Generation of the P2 permissive signal is described in Section 7.2.1.3.

The logic for the low RCP speed RT function is shown in Figure 7.2–12—Low RCP Speed.

7.2.1.2.8 Reactor Trip on High Neutron Flux

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

To detect a high neutron flux condition, the IRD measurements are multiplied by a calibration constant, and the resulting variables are compared to a fixed high setpoint. If two out of four measurements exceed the setpoint, RT orders are generated.

The P6 permissive condition bypasses the high neutron flux RT function above a fixed core thermal power level. This bypass is automatically removed when core thermal power decreases below the P6 setpoint. Generation of the P6 permissive signal is described in Section 7.2.1.3.

The logic for the high neutron flux RT function is shown in Figure 7.2–13—High Neutron Flux.

7.2.1.2.9 Reactor Trip on Low Doubling Time

This function is provided to protect against excessive reactivity additions during reactor start-up from a sub-critical or low power start-up condition. The doubling time variable is calculated using the IRD measurements as inputs. Each division of the PS acquires the measurement from one of four IRDs.

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

$$p(t) = \frac{z(t)}{\frac{dz}{dt}(t)}$$

Where:

p(t) = doubling time.

z = ln(x).

x = measured neutron flux.

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

The P6 permissive condition bypasses the low doubling time RT function above a fixed core thermal power level. This bypass is automatically removed when core thermal power decreases below the P6 setpoint. Generation of the P6 permissive signal is described in Section 7.2.1.3.

The logic for the low doubling time RT function is shown in Figure 7.2–14—Low Doubling Time.

7.2.1.2.10 Reactor Trip on Low Pressurizer Pressure

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

The P2 permissive condition bypasses the low PZR pressure RT function at low power levels. This bypass is automatically removed as power increases above the P2 setpoint. Generation of the P2 permissive signal is described in Section 7.2.1.3.

The logic for the low PZR pressure RT function is shown in Figure 7.2–15—High Pressurizer Pressure & Low Pressurizer Pressure.

7.2.1.2.11 Reactor Trip on High Pressurizer Pressure

This function is provided to protect the integrity of the reactor coolant pressure boundary and prevent opening of the pressurizer safety relief valves in case of a RCS overpressure event. The RCS pressure variable is redundantly measured by four narrow range (NR) PZR pressure sensors. These measurements are acquired by the PS as described in Section 7.2.1.3.9 and are compared to a fixed high setpoint (Max2p). If any two of the four measurements are above the setpoint, RT orders are generated.

There are no operating bypasses associated with the high PZR pressure RT. The logic for the high PZR pressure RT function is also shown in Figure 7.2–15.

7.2.1.2.12 Reactor Trip on High Pressurizer Level

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

The P12 permissive condition bypasses the high PZR level RT function below the P12 pressure threshold. This bypass is automatically removed as pressure increases above the P12 setpoint. Generation of the P12 permissive signal is described in Section 7.2.1.3.

The logic for the high PZR level RT function is shown in Figure 7.2–16—High Pressurizer Level.

7.2.1.2.13 Reactor Trip on Low Hot Leg Pressure

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

The P12 permissive condition bypasses the low hot leg pressure RT function at low RCS pressure conditions (measured by the PZR pressure sensors). This bypass is automatically removed as pressure increases above the P12 setpoint. Generation of the P12 permissive signal is described in Section 7.2.1.3.

The logic for the low hot leg pressure RT function is shown in Figure 7.2–17—Low Hot Leg Pressure.

7.2.1.2.14 Reactor Trip on Steam Generator Pressure Drop

This function is provided to protect the integrity of the fuel in case of an overcooling event caused by an excessive increase in steam demand. The steam generator (SG) pressure variable is directly measured by four pressure sensors in each SG. Each division of the PS acquires one pressure measurement from each SG and compares them to a variable low setpoint. If two measurements from any one SG decrease below the variable setpoint, RT orders are generated.

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

There are no operating bypasses associated with the SG pressure drop RT. The logic for the SG pressure drop RT function is shown in Figure 7.2–18—SG Pressure Drop.

7.2.1.2.15 Reactor Trip on Low Steam Generator Pressure

This function is provided to protect the integrity of the fuel in case of an overcooling event caused by an excessive increase in steam demand. For smaller breaks in steam or feedwater piping, the rate of SG depressurization may not reach the setpoint for RT on SG pressure drop (refer to Section 7.2.1.2.14). Therefore, an RT on low SG pressure is used to protect the fuel in these cases. The SG pressure variable is directly measured by four pressure sensors in each SG. Each division of the PS acquires one pressure measurement from each SG and compares them to a fixed low setpoint (Min1p). If two measurements from any one SG decrease below the setpoint, RT orders are generated.

The P12 permissive condition bypasses the low SG pressure RT function at low RCS pressure conditions (measured by the PZR pressure sensors). This bypass is automatically removed as pressure increases above the P12 setpoint. Generation of the P12 permissive signal is described in Section 7.2.1.3.

The logic for the low SG pressure RT function is shown in Figure 7.2–19—Low SG Pressure.

7.2.1.2.16 Reactor Trip on High Steam Generator Pressure

This function is provided to protect the integrity of the fuel and of the SG in case of a secondary side over-pressure event. The SG pressure variable is directly measured by four pressure sensors in each SG. These measurements are acquired by the PS as described in Section 7.2.1.2.14 and are compared to a fixed high setpoint (Max1p). If two measurements from any one SG are above the setpoint, RT orders are generated.

There are no operating bypasses associated with the high SG pressure RT. The logic for the high SG pressure RT function is shown in Figure 7.2–20—High SG Pressure.

7.2.1.2.17 Reactor Trip on Low Steam Generator Level

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

The P13 permissive condition bypasses the low SG level RT function at low temperatures as measured in the hot legs. This bypass is automatically removed as hot leg temperature increases above the P13 setpoint. Generation of the P13 permissive signal is described in Section 7.2.1.3.

The logic for the low SG level RT function is shown in Figure 7.2–21—Low SG Level.

7.2.1.2.18 Reactor Trip on High Steam Generator Level

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

The SG level variable is directly measured by four (NR) level sensors in each SG. These measurements are acquired by the PS as described in Section 7.2.1.2.17 and are compared to a fixed high setpoint (Max1p). If two measurements from any one SG are above the setpoint, RT orders are generated.

The P13 permissive condition bypasses the high SG level RT function at low temperatures as measured in the hot legs. This bypass is automatically removed as hot

leg temperature increases above the P13 setpoint. Generation of the P13 permissive signal is described in Section 7.2.1.3.

The logic for the high SG level RT function is shown in Figure 7.2–22—High SG Level.

7.2.1.2.19 Reactor Trip on High Containment Pressure

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

Each division of the PS acquires one pressure measurement from each set of sensors and compares them to a fixed high setpoint (Max1p). If two measurements from either set of four pressure sensors are above the setpoint, RT orders are generated.

There are no operating bypasses associated with the high containment pressure RT. The logic for the high containment pressure RT function is shown in Figure 7.2–23—High Containment Pressure.

7.2.1.2.20 Reactor Trip on Safety Injection System Actuation

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

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

Automatic actuation of the SIS is described in Section 7.3, and the logic for generation of the SI signal is shown in Figure 7.3–2—Safety Injection Actuation. The logic combining the safety injection signal with the remainder of the RT signals is shown in Figure 7.2–24—RT Signal Generation.

7.2.1.2.21 Reactor Trip on Emergency Feedwater System Actuation

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

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

The P13 permissive condition bypasses the RT on EFWS actuation function at low temperatures as measured in the hot legs. This bypass is automatically removed as hot

leg temperature increases above the P13 setpoint. Generation of the P13 permissive signal is described in Section 7.2.1.3.

Automatic actuation of the EFWS is described in Section 7.3, and the logic for generation of the EFWS actuation signal is shown in Figure 7.3-3. The logic combining the EFWS actuation signal with the remainder of the RT signals is shown in Figure 7.2–24.

7.2.1.2.22 Manual Reactor Trip

The capability for manual RT is provided to the operator through the SICS in both the MCR and RSS. At each location, four manual RT buttons are provided to correspond to the four PS divisions. Manual RT from the MCR is hardwired to bypass the electronics of the PS and act directly on the undervoltage coils of the RT breakers. The MCR initiation signal is also acquired by the PS and processed with the automatic RT functions. Manual RT from the RSS is hardwired to bypass the electronics of the PS and act directly on the shunt trip coils of the RT breakers. Manual RT initiation is illustrated in Figure 7.2–3. Manual RT described further in Reference 1. The logic combining the manual RT signal from the MCR with the automatic RT signals is shown in Figure 7.2–24.

7.2.1.3 Permissive Signal Functional Description

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

The state of a permissive signal is defined as either validated or inhibited:

- A validated permissive signal carries a logical value of 1.
- An inhibited permissive signal carries a logical value of 0.

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

Generation of each permissive signal is described in Section 7.2.1.3.1 through Section 7.2.1.3.12. These permissive signals are generated within the PS for use in RT and engineered safety features actuation functions. Certain functions implemented in the diverse actuation system (DAS) are also subjected to the same permissive conditions. In these cases, the permissive logic used in the PS is duplicated and performed separately within the DAS.

7.2.1.3.1 P2 Permissive

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

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

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

Figure 7.2–25—P2 Permissive Logic illustrates the logic of the P2 permissive.

7.2.1.3.2 P3 Permissive

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

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

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

Figure 7.2–26—P3 Permissive Logic illustrates the logic of the P3 permissive.

7.2.1.3.3 P5 Permissive

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

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

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

Figure 7.2–27—P5 Permissive Logic illustrates the logic for the P5 permissive.

7.2.1.3.4 P6 Permissive

The P6 permissive is representative of core thermal power above a low-power setpoint value (10 percent power) corresponding to the boundary between the operating ranges of the IRDs and the PRDs.

Hot leg pressure (WR) measurements, hot leg temperature (NR) measurements, and cold leg temperature (NR) measurements are used to calculate core thermal power. These calculated core thermal power levels are compared to the setpoint. When three out of four of the calculated core thermal power levels are greater than the setpoint, the operator is prompted to manually validate the permissive.

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

Figure 7.2–28—P6 Permissive Logic illustrates the logic of the P6 permissive.

7.2.1.3.5 P7 Permissive

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

The RCP speed measurements (one per RCP) are compared to a setpoint (91percent nominal speed). When two out of four of the measurements are less than the setpoint, the permissive is validated (i.e., indicates that two or more RCPs are turned off).

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

Figure 7.2–29—P7 Permissive Logic illustrates the logic for the P7 permissive.

7.2.1.3.6 P8 Permissive

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

Rod cluster control assembly (RCCA) lower end position sensors are acquired in four different electrical divisions. For each division, when all rods in the shutdown banks reach the lower end position, a signal is generated. When two out of four of divisions indicate all rods in, the permissive is validated.

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

Figure 7.2–30—P8 Permissive Logic illustrates the logic for the P8 permissive.

7.2.1.3.7 P12 Permissive

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

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

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

Figure 7.2–31—P12 Permissive Logic illustrates the logic for the P12 Permissive.

7.2.1.3.8 P13 Permissive

The P13 permissive defines when steam generator draining and filling operations are allowed.

Hot leg temperature (WR) measurements are compared to the P13 setpoint (203 °F). When three out of four of the measurements are less than the setpoint, the operator is prompted to manually validate the permissive.

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

Figure 7.2–32—P13 Permissive Logic illustrates the logic for the P13 permissive.

7.2.1.3.9 P14 Permissive

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

Hot leg temperature (WR) and hot leg pressure (WR) measurements are each compared to a setpoint (356 °F, 464 psia). When three out of four of the hot leg temperature (WR) measurements are less than the temperature setpoint, and three out of four of the hot leg pressure measurements (WR) are less than the pressure setpoint, the operator is prompted to manually validate the permissive.

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

Figure 7.2–33—P14 Permissive Logic illustrates the logic for the P14 permissive.

7.2.1.3.10 P15 Permissive

The P15 permissive defines when SI actuation due to ΔPsat is disabled and SI actuation due to low loop level is enabled.

RCP current measurements and the same pressure and temperature measurement used in P14. RCP current measurements are each compared to a setpoint (50 percent no load current). When two out of three of the measurements for an individual pump are

less than the setpoint, a signal is generated for that pump. When signals are generated for all four pumps, a delay time is started. After the delay time has expired, and the P14 pressure and temperature conditions are satisfied, the operator is prompted to manually validate permissive P15.

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

Figure 7.2–34—P15 Permissive Logic illustrates the logic for the P15 permissive.

7.2.1.3.11 P16 Permissive

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

Hot leg pressure (WR) measurements and ΔPsat (calculated separately) are each compared to a setpoint. The following logic is used:

- Two out of four hot leg pressure measurements are less than a Setpoint (289.7 psia), and
- Two out of four the ΔPsat measurements are less than a Setpoint (73 psi), and
- RCPs indicating stopped (see P15), and
- SIS actuation followed by a delay (1.5 hours).

Once these conditions are met, the operator is prompted to manually validate the permissive.

This permissive is P-MANU with respect to validation and P-AUTO (concurrent with reactor trip reset) with respect to inhibition.

Figure 7.2–35—P16 Permissive Logic illustrates the logic for the P16 permissive.

7.2.1.3.12 P17 Permissive

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

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

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

Figure 7.2–36—P17 Permissive Logic illustrates the logic for the P17 permissive.

7.2.2 Analysis

7.2.2.1 Design Basis Information

Clause 4 of IEEE Std. 603-1998 specifies the information used to establish the design basis for safety systems. This section describes design basis information for the U.S. EPR RT function. Reactor trip is performed automatically by the PS and manually through the SICS in conjunction with PS. The design basis information related to the equipment of these safety systems, environmental conditions in which they must function, and methods used to determine their reliability is described in Section 7.1.

The design basis information below pertains to the requirements placed on the RT function and the variables monitored to initiate the RT function.

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

The design basis events 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 defined in Chapter 15. Correlation between each event and specific RT functions is found in Table 15.0-10.

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

The operating bypasses applicable to each RT function are identified in Section 7.2.1.2.1 through Section 7.2.1.2.20. 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.

7.2.2.1.3 Design Basis: Reactor Trip Input Variables (Clause 4.d of IEEE 603-1998)

Each RT function is listed in Table 15.0-7 with the relevant nominal trip setpoint, normal and degraded uncertainties, and time delays for the function. For each of these functions, Table 7.2–1 lists the input variables that are used either directly or as inputs to a calculation to initiate an RT. The range to be monitored for each of these variables is also listed in Table 7.2–1.

7.2.2.1.4 Design Basis: Manual Reactor Trip Initiation (Clause 4.e of IEEE 603-1998)

The capability for manual RT is available to the operator as described in Section 7.2.1.1. There are no operating bypasses placed on the manual RT function; it is available at any time, under any plant conditions. The variables to be displayed to the operator to use in manual RT initiation are determined as part of the methodology used for selecting Type A variables as described in Section 7.5.

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

Neutron flux varies spatially in a three dimensional manner throughout the core. Calculations used in the high linear power density and low DNBR RT functions take these spatial variations into account. The SPND are located systematically throughout the core to provide the spatially dependent neutron flux information for these calculations. Provisions are made in the RT logic to accommodate any five failed SPNDs for the HLPD function, and any number of failed SPND on up to five fingers for the low DNBR function.

Hot leg coolant thermal streaming results in radial variations of coolant temperature. Each hot leg contains four (NR) temperature sensors that are used as inputs to the high core power level and low saturation margin RT functions. The four sensors in each hot leg are mounted approximately 90 degrees apart in the cross-sectional plane of the piping to obtain a representative temperature sample. The four measurements are averaged to obtain an accurate value of hot leg temperature despite the streaming phenomenon. Provisions are made in the RT logic to detect and accommodate up to two failed sensors in a hot leg.

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

Reactor trip is initiated by the PS when selected variables exceed the associated RT setpoints. The plant conditions that define the proper completion of the RT function are defined on an event-by-event basis in the Chapter 15 analyses. The RT function is only reset (returned to normal) after manual action has been taken to close the RT breakers. Plant specific operating procedures govern the point in time when the RT breakers can be reset following an RT.

7.2.2.2 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 Reference 1 is used as the basis for the analysis. The FMEA considers each major part of the system, how it may fail, and what the effect of the failure on the system would be.

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 RT functions is summarized in this section. A summary of the effects of single failures on the ESFAS functions is provided in Section 7.3.

To define the major parts of the system for which failures are assumed, a single division of the PS is divided into functional units as described in Reference 1. The PS consists of four identical divisions, so the definition of functional units is the same for each division. The functional units that participate in the generation of automatic RT functions are:

- Remote acquisition units (RAU).
- Rod control cluster assembly units (RCCAU).
- Acquisition and processing units (APU).
- Actuation logic units (ALU).

In addition to the equipment defined as functional units of the system, certain other equipment also contributes to the automatic RT function and is analyzed as part of the system-level FMEA:

- Sensors that provide input measurements to RT functions.
- Hardwired output logic used in RT function.
- Reactor trip devices.

In order to bound the possible failures, both detected and undetected failures of sensors and digital equipment are analyzed and the worst case effect of each failure is identified. Detected failures are defined as those automatically detected by the inherent and engineered monitoring mechanisms of the system. Two types of undetected failures are analyzed. A failure denoted "undetected–spurious" is defined as a failure not automatically detected which results in a spurious partial trigger or actuation. A failure denoted "undetected–blocking" is defined as a failure not automatically detected which results in failure to issue a partial trigger or actuation when needed.

Failures in the hardwired output logic are generally not detected automatically by the PS. Therefore, only undetected single failures of these devices are considered. A failure of the output logic can result in a spurious actuation ("undetected–spurious"), or failure to actuate when needed ("undetected–blocking").

Network failures within the PS allow the receiver of data to be affected in one of three ways. First, the network failure can result in an invalid message being received. By definition, invalid messages are always detected failures, and are analyzed as single failures. Second, a network failure can result in a message received as valid that contains spurious information. This type of failure is bounded by the "undetected–spurious" failure of the sending equipment, and is therefore not considered. Third, a network failure can result in a message received as valid that fails to request an action

when one is needed. This type of failure is bounded by the "undetected–blocking" failure of the sending equipment, and is therefore not considered. Further information regarding the communication methods used and communication failure detection capabilities is found in References 1 and 2.

The architecture of the PS allows APUs and ALUs to be analyzed for single failure without regard to which specific APU or ALU in the division is the failure point. For these single failures, all functions of the system are considered affected, as every function is processed by at least one APU and two ALU in a division. Considering the effect on every function of the system bounds all cases of specific APU and ALU single failures.

When referring to the nature of a single failure, the terms "detected" and "undetected" as used in the context of the PS FMEA do not correspond to the definition of a detectable failure in IEEE 603-1998. All of the failures denoted "undetected" in the FMEA are detectable through periodic testing. The terms "detected" and "undetected", as used in the FMEA, refer to the ability of the PS to automatically detect a failure through self-surveillance.

Failures of instrument air systems are not considered in support of the PS FMEA. The ESF actuation and control functions in the U.S. EPR design do not rely on common instrument air systems.

The results of the FMEA with regard to the effects of single failures on RT functionality are summarized in Table 7.2–2—FMEA Summary for Reactor Trip

7.2.2.3 Conformance to Applicable Criteria

7.2.2.3.1 Compliance to the Single Failure Criterion (Clause 5.1 of IEEE 603-1998)

The PS maintains the ability to perform the RT function in the presence of any credible single failure of an input sensor, functional unit of the PS, or RT device. The RT function is performed in a four-fold redundant manner from sensor to actuation device.

Single failures upstream of the voting logic (sensor or APU failure) are accommodated by the voting logic. The two out of four vote in all divisions becomes either two out of three or one out of three, depending on the nature of the failure automatically detected or not. In either case, the ability to perform RT when required is retained. Certain exceptional failures that can occur upstream of the voting logic that are accommodated in other ways. For example, single failures of SPND or RCCA position measurements are accommodated by either signal selection (2^{nd} MIN or 2^{nd} MAX) or through automatic use of a more conservative trip setpoint.

Single failures at the level of the voting logic are accommodated by either redundancy within each division or redundancy across the four divisions. In case of a detected or an "undetected–spurious" failure of an ALU, the redundant ALU in the same division performs the RT function, and RT orders are still generated in all four divisions. In case of an "undetected–blocking" failure of an ALU, the affected division cannot issue RT orders, but any two of the remaining three divisions can actuate the RT function.

Single failures of RT devices are accommodated by the two out of four arrangement of the devices. A spurious opening of an RT device does not result in either spurious trip or loss of ability to trip. A failure of a single RT device to open is accommodated by the opening of any two of the other three redundant devices.

A system level FMEA is performed to verify conformance with the single failure criterion. The FMEA is described in Section 7.2.2.2, and the results are summarized in Table 7.2–2.

7.2.2.3.2 Compliance to Requirements for Quality of Components and Modules (Clause 5.3 of IEEE 603-1998 and Clause 5.3 of IEEE 7-4.3.2-2003)

Components and modules that are required to perform the RT function are classified as safety-related and are designed to Class 1E standards, and are applied in accordance with an stringent quality assurance program. Software used in the RT function is developed and applied in accordance with a safety-related software program. Further description of conformance of the PS to requirements for quality is found in Section 7.1.

7.2.2.3.3 Compliance to Requirements for Independence of the RT Function (Clauses 5.6 and 6.3 of IEEE 603-1998 and GDC 24)

Redundant portions of the PS are independent from one another so that a failure in any one portion of the system does not prevent the redundant portions from performing the RT function. Both electrical and communication independence are maintained as described in Section 7.1 and in Reference 1.

Equipment required to perform the RT function is independent from the effects of the events which the RT function mitigates. The functional units of the PS 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 described in Section 3.11 and Section 7.1.

The PS does not rely on input from any non-safety-related control system to perform the RT function. The plant accident analysis does not credit actions taken by non-safety-related control systems to improve the response of the RT function. 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 RT function is demonstrated to act independently of any non-safety-related control system. Certain sensor measurements are shared as inputs to both an RT function and a plant control function. In these cases, the measurement is acquired by the signal conditioning of the PS. The signal is multiplied and passed to the control system through an electrically isolated connection, to maintain the independence of the RT function.

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

7.2.2.3.4 Compliance to Requirements Concerning Diversity and Defense in Depth (Clause 5.16 of IEEE 603-1998)

Functional diversity for the RT function is incorporated in the EPR protection system design. The majority of anticipated operational occurrences and design basis accidents that require reactor trip are mitigated by two RT functions based on diverse measurement parameters. Each division of the PS is divided into two functionally independent subsystems for the purpose of separating the functionally diverse RT functions. The application of functional diversity in the EPR PS is described in Reference 1.

A non-safety-related diverse actuation system (DAS) is provided to perform automatic RT functions in case of the unlikely event of a common cause software failure that renders the entire PS inoperable. The hardware and software 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, the capability for manual RT is available to the operator. The manual RT from the MCR actuates the RT function in a manner separate and diverse from the automatic RT functions of the PS.

The overall U.S. EPR I&C approach to diversity and defense in depth is described in Reference 4.

7.2.2.3.5 Compliance to Requirements on System Testing and Inoperable Surveillance Requirements (Clause 5.7 of IEEE 603-1998)

The design of the PS allows for testing of the RT function while retaining the capability to perform the RT function. The majority of the components required for RT can be tested with the reactor at power. Surveillance of the PS consists of overlapping tests to verify performance of the complete RT function from sensor to RT devices.

The computerized portions of the PS are continuously monitored through self-testing during power operation. During outages, extended computer 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 RT function is still performed using the redundant input channels.

The connections between the PS output circuits and the RT devices and the RT devices themselves can be tested during power operation. One division of the PS and one redundancy of the RT devices are tested at a time to avoid spurious RT. If reactor trip orders are generated during the test, the RT is performed normally.

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

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

Implementation of safety-related I&C systems is governed by the requirements of IEEE 603-1998. Guidance on the use of digital computers in safety-related systems is provided by IEEE 7-4.3.2-2003. Conformance to these standards is described in Section 7.1.

7.2.2.3.7 Compliance to Requirements for RT Setpoint Determination (Clause 6.8 of IEEE 603-1998)

Each setpoint used to initiate an RT function is selected based on the safety limits assumed in the plant accident analysis. The RT setpoint provides margin to the safety limit and takes into account measurement uncertainties. The methodology to determine setpoints used in SPND-based RT functions is documented in Reference 3. The methodology to determine setpoints for all other RT functions is documented in Reference 5.

7.2.3 References

1. ANP-10281P, Revision 0, “U.S. EPR Digital Protection System Topical Report,” AREVA NP Inc., March 2007.

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

3. ANP-10287P, Revision 0, “Incore Trip Setpoint and Transient Methodology for U.S. EPR Topical Report,” AREVA NP Inc., November 2007.

4. ANP-10284, Revision 0, "U.S. EPR Instrumentation and Controls Diversity and Defense-in-Depth Methodology," AREVA NP Inc., June 2007.

5. ANP-10275P, Revision 0, "U.S. EPR Instrument Setpoint Methodology," AREVA NP Inc., March 2007.

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

7. IEEE 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.

Table 7.2-1—Reactor Trip Variables

Protective Function	Variables To Be Monitored	Range of Variables
High Linear Power Density	Neutron Flux-Self Powered Neutron Detectors	0–590 W/cm
Low DNBR	Neutron Flux-Self Powered Neutron Detectors	0–590 W/cm
	Cold Leg Temperature (NR)	500°F–626°F
	RCP Speed	500 -1300 rpm
	RCCA position	0–100% Insertion
	Pressurizer Pressure	1615-2515 psia
High Neutron Flux Rate of Change	Neutron Flux-Power Range Detectors	0.5–200% NP
High Core Power Level	Cold Leg Temperature (WR)	32°F - 662°F
	Hot Leg Pressure (WR)	15–3015 psia
	Hot Leg Temperature (NR)	536°F -662°F
Low Reactor Coolant Pump Speed	RCP Speed	500 -1300 rpm
Low Loop Flow Rate (two loops)	RCS Loop Flow	0–120% NF
Low-Low Loop Flow Rate (one loop)	RCS Loop Flow	0–120% NF
Low Doubling Time	Neutron Flux-Intermediate Range Detector	5 x 10E-6–60% NP
High Neutron Flux	Neutron Flux-Intermediate Range Detector	5 x 10E-6–60% NP
Low Pressurizer Pressure	Pressurizer Pressure (NR)	1615–2515 psia
High PZR Pressure	Pressurizer Pressure (NR)	1615–2515 psia
High PZR Level	Pressurizer Level	0-100% MR
Low Hot Leg Pressure	Hot Leg Pressure (WR)	15–3015 psia
Steam Generator Pressure Drop	SG Pressure	15–1615 psia
Low Steam Generator Pressure	SG Pressure	15–1615 psia
High Steam Generator Pressure	SG Pressure	15–1615 psia
Low Steam Generator Level	SG Level (NR)	0-100% MR
High Steam Generator Level	SG Level (NR)	0-100% MR
High Containment Pressure	Containment Service Compartment Pressure (NR)	-3 psig to +7 psig
	Containment Equipment Compartment Pressure	-3 psig to +7 psig
Low Saturation Margin	Cold Leg Temperature (WR)	32°F - 662°F
	Hot Leg Pressure (WR)	15–3015 psia
	Hot Leg Temperature (NR)	536°F–662°F

Notes on Table 7.2–1: NP = Nuclear Power, NF = Nominal Flow, MR = Measuring Range

Table 7.2-2—FMEA Summary for Reactor Trip
Sheet 1 of 3

Single Failure	Nature of Failure	System Response (Effect on RT Portion)	Effect on Plant
Sensor–SPND	Detected	Failed sensor marked invalid; Low DNBR and HLPD setpoint modification	None
	Undetected–Spurious	2nd MIN and 2nd MAX operations accommodate spurious measurement	None
	Undetected–Blocking	Core symmetry allows that the condition to be detected (either low DNBR or HLPD) is indicated by detectors at other locations in the core	None
Sensor–RCCA position measurement	Detected	Failed sensor marked invalid; Low DNBR setpoint value is adequate for single undetected rod insertion; inadvertent bank insertion detected by sensors in other 3 divisions	None
	Undetected–Spurious	Rod drop (1/4) signal generated; More conservative DNBR setpoint becomes valid	None
	Undetected–Blocking	Low DNBR setpoint value is adequate for single undetected rod insertion; inadvertent bank insertion detected by sensors in other 3 divisions	None
Sensor–All others	Detected	Failed sensor marked invalid; Downstream voting logic modified to 2/3	None
	Undetected–Spurious	Downstream voting logic becomes 1/3	None
	Undetected–Blocking	Downstream voting logic becomes 2/3	None
RCCAU	Detected	Rod position measurements from one quarter of the core marked invalid; Low DNBR setpoint value is adequate for single undetected rod insertion; inadvertent bank insertion detected by sensors in other 3 divisions	None
	Undetected–Spurious	RCCAU emits multiple rod drop signals spuriously; Rod drop (1/4) signal generated; More conservative DNBR setpoint is used	None
	Undetected–Blocking	Low DNBR setpoint value is adequate for single undetected rod insertion; inadvertent bank insertion detected by sensors in other 3 divisions	None

Table 7.2-2—FMEA Summary for Reactor Trip
Sheet 2 of 3

Single Failure	Nature of Failure	System Response (Effect on RT Portion)	Effect on Plant
Network RCCAU–APU	Detected	Rod position measurements from one quarter of the core marked invalid; Low DNBR setpoint value is adequate for single undetected rod insertion; inadvertent bank insertion detected by sensors in other 3 divisions	None
RAU	Detected	Redundant RAU in same division performs the function	None
	Undetected–Spurious	RAU emits multiple erroneous values which favor spurious RT	Spurious RT
	Undetected–Blocking	Redundant RAU in same division performs the function (APU selects the value between redundant RAU that favors plant safety)	None
Network RAU–APU	Detected	Redundant network associated with redundant RAU performs the function	None
APU	Detected	All signals sent from APU marked invalid; Downstream voting logic modified to 2/3	None
	Undetected–Spurious	Downstream voting logic becomes 1/3	None
	Undetected–Blocking	Downstream voting logic becomes 2/3	None
Network APU–ALU	Detected	All signals sent from APU marked invalid; Downstream voting logic modified to 2/3	None
ALU	Detected	ALU fails into state requesting RT; Redundant ALU performs the function	None
	Undetected–Spurious	ALU fails into state requesting RT; Redundant ALU performs the function	None
	Undetected–Blocking	The division cannot issue RT order; Function is performed by other 3 divisions; RT devices voting logic becomes 2/3	None
Hardwired Output Logic	Undetected–Spurious	Spurious divisional RT order issued; RT devices voting logic becomes 1/3	None
	Undetected–Blocking	The division cannot issue RT order; Function is performed by other 3 divisions; RT devices voting logic becomes 2/3	None

Table 7.2-2—FMEA Summary for Reactor Trip
Sheet 3 of 3

Single Failure	Nature of Failure	System Response (Effect on RT Portion)	Effect on Plant
Reactor Trip Device	Undetected–Spurious	One RT device is opened; Remainder of RT devices function in 1/3 configuration	None
	Undetected–Blocking	One RT device fails to open; Remainder of RT devices function in 2/3 configuration	None

Figure 7.2-1—Typical RT Actuation

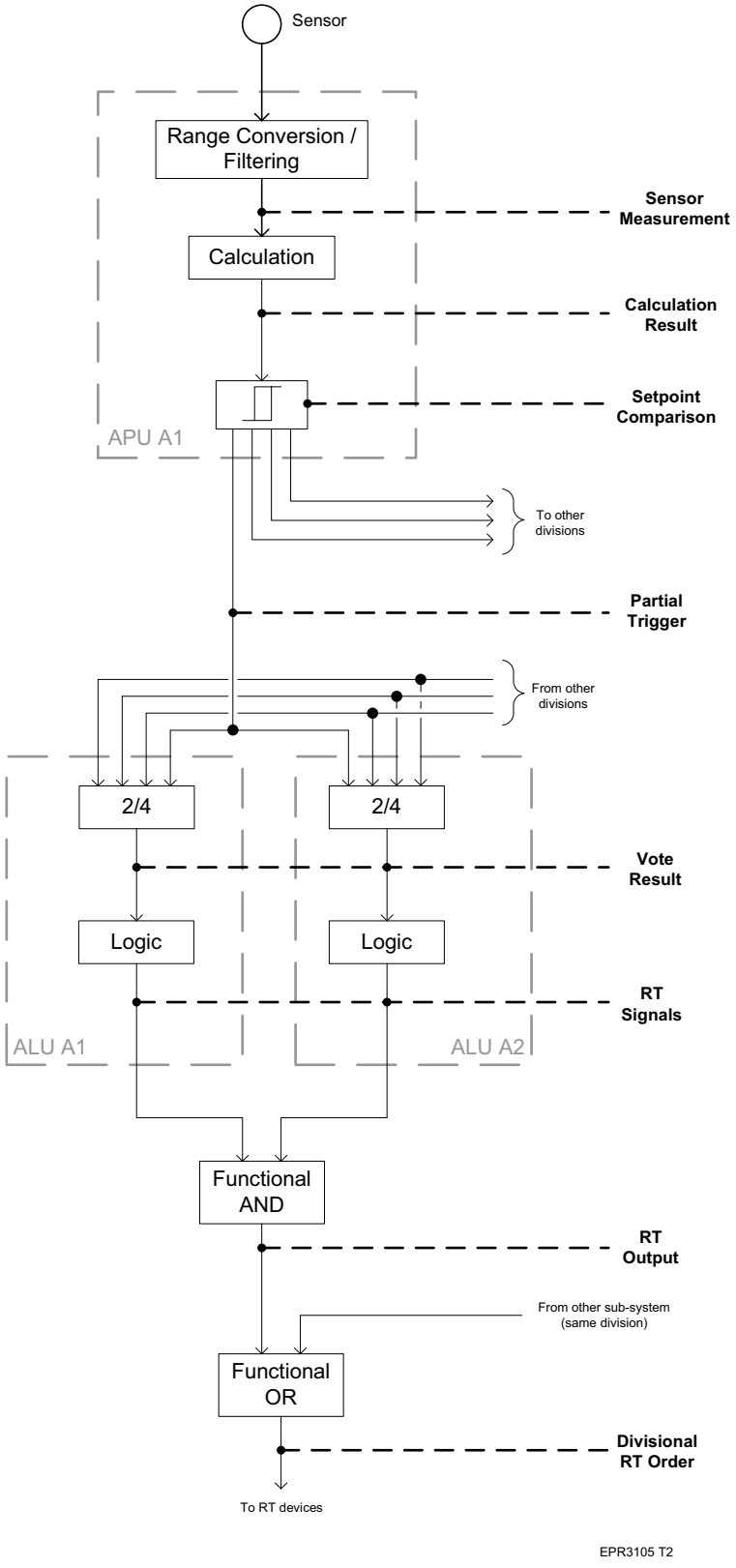

Figure 7.2-2—Typical SPND-based RT Actuation

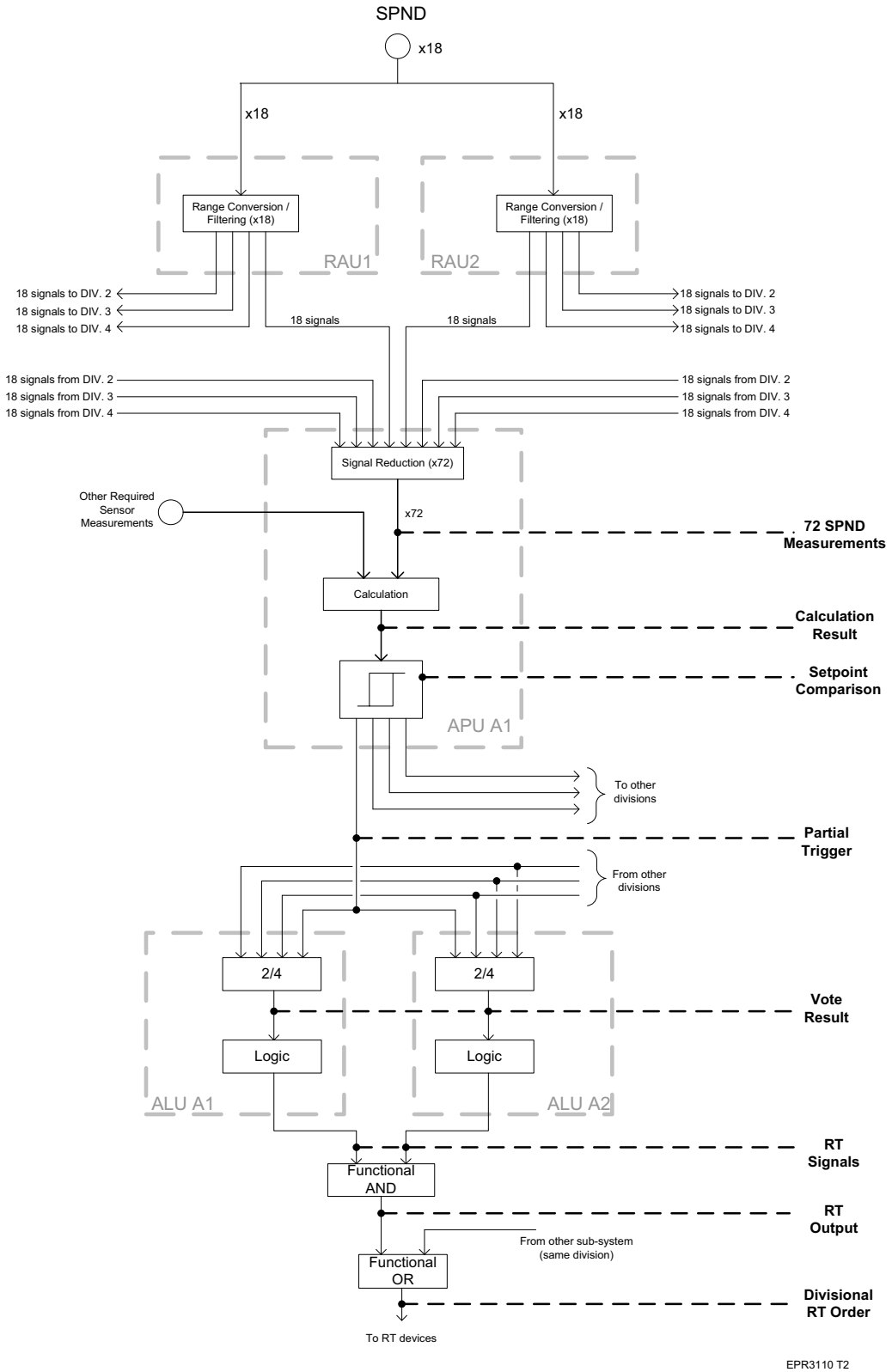

Figure 7.2-3—Manual RT