7.6 Interlock Systems Important to Safety

7.6.1 Description

This section describes the interlock functions important to safety that reduce the probability of occurrence of specific events, or maintain safety systems in a state that provides reasonable assurance of their availability. These interlocks are provided by instrumentation and control (I&C) functions designed to:

- Prevent over-pressurization of the residual heat removal (RHR) system when reactor coolant system (RCS) pressure and temperature are higher than the allowable values for RHR connection.
- Maintain the availability of the safety injection (SI) accumulators above specific RCS pressure conditions.
- Maintain separation between redundant component cooling water system (CCWS) trains.
- Prevent over-pressurization of the RCS and connected RHR system in case of SI actuation during low temperature operations.

7.6.1.1 System Description

The control logic for these interlock functions is processed by the protection system (PS), with the exception of the interlocks to maintain separation between redundant CCWS trains. The control logic for the CCWS interlocks is processed by the safety automation system (SAS). The relevant control logic for each function is described in Section 7.6.1.2.

When plant conditions dictate that an interlock be activated, the interlock signal is sent from the PS or SAS to the priority and actuator control system (PACS). While the interlock signal is present, the PACS prevents an override of the interlock by actuation or control orders having a lower priority than the interlock function. When plant conditions are such that an interlock can be removed, the PS or SAS removes the interlock signal and the PACS allows the actuator to be influenced by other control systems. Further discussion of the operation of the PACS is presented in Section 7.1.

The capability to perform manual actions related to these interlocks (i.e., inhibition or validation of permissive signal status) is provided on the safety information and control system (SICS).

7.6.1.2 Functional Descriptions

7.6.1.2.1 RHR Suction Valve Interlocks

There are four 100 percent low head safety injection (LHSI) trains that can be aligned to perform the RHR function. Each train has connections to the hot and cold legs of an RCS loop. The RHR function is performed by forced flow with the LHSI pumps taking suction from the hot legs, cooling the water via the LHSI heat exchangers, and injecting into the cold legs.

The operation of the LHSI and RHR systems is described in Section 5.4.7.

In RHR mode, each LHSI train takes suction from its respective hot leg through two motor operated isolation valves in series (first and second RHR reactor coolant pressure boundary (RCPB) isolation valves). These isolation valves are interlocked to prevent their opening when RCS pressure and temperature have not decreased below acceptable values. These acceptable values are the P14 permissive pressure and temperature thresholds.

When RCS pressure and temperature are above the P14 permissive threshold, the PS provides constant signals to hold the RHR RCPB isolation valves closed. After pressure and temperature decrease below the thresholds, the operator is prompted to manually validate P14 permissive which allows the isolation valves to be opened to connect RHR. This safety-related interlock prevents the RHR system from being exposed to pressures and temperatures beyond its design condition.

Generation of the P14 permissive signal is described in Section 7.2.1.3.9.

Two redundant actuation logic units (ALU) within a PS division each send the interlock signal to one isolation valve in each of two RHR trains (i.e., PS Division 1 holds closed a single valve on Train 1 and a single valve on Train 2. Division 2 of the PS holds closed a single valve on Train 2 and a single valve on Train 1). This arrangement precludes a single failure from allowing opening of both interlocked isolation valves on any one RHR train. Additionally, no single failure can prevent the operator from aligning the isolation valves, on at least one suction line, for RHR after RCS pressure and temperature requirements are satisfied.

Independence and diversity are provided between the interlocks of the two valves on each suction line to prevent their opening unless RCS pressure and temperature are below the RHR system design pressure. Independence is maintained between the two divisions of the PS that each provide the interlock to one of the two valves. Measures used to establish independence between redundant safety divisions are described in Section 7.1. Diversity is achieved by the fact that both RCS pressure and temperature measurements must be below the P14 permissive threshold values before the valves can be opened. Additionally, the operator is prompted to manually validate or inhibit the P14 permissive, providing a third diverse condition that must be satisfied to allow valve opening.

Another safety-related interlock prevents the opening of the RHR RCPB isolation valves, unless the LHSI suction isolation valve is closed. This prevents the LHSI suction from the IRWST from being exposed to the higher pressures of the RCS. The functional logic for this RHR isolation valve interlock is shown in Figure 7.6-11—RHR Isolation Valves Interlock.

When RHR is connected, an inadvertent increase in RCS pressure does not result in an automatic signal to close the RHR RCPB isolation valves. However, the following design features prevent an increasing pressure from exceeding the RHR system design pressure:

- Interlock holding the MHSI large miniflow lines open (see Section 7.6.1.2.6).
- Pressurizer safety relief valves operating in their LTOP mode (see Section 7.3.1.2.13).
- Spring loaded safety valves on the RHR suction lines.

During an intentional increase in pressure, when RCS temperature and pressure exceed the P14 permissive setpoint, the operator is prompted to manually inhibit the P14 permissive, and is then allowed to close the RHR RCPB isolation valves.

The operational status of the PS on a divisional basis is provided to the operator. Indications and alarms are provided to the operator regarding the state of the P14 permissive signal. Additionally, the following indications are provided to the operator to verify correct operation of the interlock:

- Open or closed position of first RHR RCPB isolation valve (each train).
- Open or closed position of second RHR RCPB isolation valve (each train).

7.6.1.2.2 Safety Injection Accumulator Interlocks

There are four accumulators, one associated with each of the four independent SIS trains. Borated water is injected into the RCS from the accumulators when RCS pressure falls below the internal pressure of the accumulators.

The operation of the SI accumulators is described in Section 6.3.

Each accumulator is connected to the cold leg injection line of its respective RCS loop through two check valves and a motor operated isolation valve in series. Each isolation valve is interlocked to remain fully open above a specified RCS pressure value in Modes 1, 2, 3, and 4. This pressure value is the P12 permissive threshold. The accumulators are used to provide safety injection into the RCS during higher pressures.

At higher pressures (above P12 permissive value), the P12 inhibited signal is used to hold open the accumulator isolation valves. At lower pressures (below P12 permissive value), the open signal from the PS is removed and the operator can manually close the isolation valves. Isolation of the accumulator is necessary to prevent discharge of the accumulator at lower pressures.

Generation of the P12 permissive signal is described in Section 7.2.1.3.7.

Normally, the operator fully opens the isolation valves when RCS pressure exceeds accumulator pressure. Regardless, when RCS pressure increases above the P12 permissive threshold, the PS provides automatic signals to open the accumulator isolation valves. Once the isolation valves are verified to be in the fully open position, control power is removed from the valves to prevent inadvertent closure. During a normal decrease in pressure, power is restored to the valves at a point in time determined by the operating procedures. Then, after RCS pressure decreases below the P12 permissive threshold, the operator is prompted to manually validate the P12 permissive, which allows the isolation valves to be closed before RCS pressure is reduced below the accumulator pressure in Mode 4.

A pressure region exists below the P12 permissive pressure threshold where the accumulators are required to be available but Plant Technical Specifications allow an accumulator isolation valve to be closed for a short period of time. To accommodate operation in this pressure region, an automatic 'open' signal is sent to the accumulator isolation valves when an SIS actuation occurs. The SIS actuation function is described in Section 7.3.1.2.1.

When the RCS is depressurized upon entry into Mode 5, the accumulators are depressurized or maintained at a low pressure so they can be used as an RCS makeup source in response to an extended loss of AC power (ELAP) event. To respond to an ELAP event, the accumulator isolation valves are partially opened and repositioned as necessary to throttle makeup water to the RCS.

Two redundant ALUs within a division send the automatic opening signal through a "functional OR" logic to the isolation valve of the corresponding accumulator (i.e., PS Division 1 opens the isolation valve related to the Train 1 accumulator). This arrangement precludes a single actuator logic unit (ALU) failure from preventing the opening of a valve. Any other single failure which could prevent opening of a valve, such as failure of a PACS module or of the valve itself, is detected immediately by failure of the valve to open. Corrective actions can then be taken before continued increase in pressure.

The operational status of the PS on a divisional basis is provided to the operator. Indications and alarms are provided to the operator regarding the state of the P12 permissive signal. Additionally, the following indications are provided to the operator to verify correct operation of the interlock:

- Pressure and level of each accumulator.
- Percent open or closed position of each accumulator isolation valve.

7.6.1.2.3 CCWS Valves Interlocks

The CCWS is comprised of four closed-loop, safety-related supply trains that function to cool and transfer heat load from safety-related users to the emergency service water system (ultimate heat sink). The common loads cooled by the CCWS consist of two separate sets, referred to as Common-1 and Common-2. The Common-1 header is supplied by either CCWS Train 1 or Train 2 while the Common-2 header is supplied by either CCWS Train 3 or Train 4. Each common header is further divided into two sub-headers designated as Common 1a and 1b or Common 2a and 2b.

The operation of the CCWS is described in Section 9.2.2.

Switchover Valves Interlock

Interlocks are provided so that no two redundant CCWS trains are connected to the same common header at the same time. Each CCWS train is provided with four switchover valves to perform the required train separation. This safety-related interlock provides independence between redundant CCWS trains, such that if a failure occurs (e.g., pipe break) both redundant trains are not compromised.

CCWS Train 1 has a single valve on the supply side and a single valve on the return side of Common 1a. Train 2 also has a single valve on both the supply and return sides of Common 1a. These valves are interlocked so that both valves (supply and return) on Train 1 must be closed before either valve on Train 2 can be opened. Likewise, both valves on Train 2 must be closed before either valve on Train 1 can be opened. The same valve arrangement and interlocks are provided relative to Common 1b to provide separation between Trains 1 and 2, and on Common 2a and 2b to provide separation between Trains 3 and 4. The functional logic for the switchover valve interlock is shown in Figure 7.6-1—CCWS Switchover Valves Interlock.

The interlock functions maintaining separation between redundant CCWS trains are performed by the SAS. Each switchover valve is assigned to a SAS division based on the CCWS train it belongs to (i.e., switchover valves on Train 1 are assigned to SAS Division 1). Each division of SAS acquires position information from the valves to which it is assigned, and controls those same valves. In any SAS division, the information about the position of valves in other trains that is needed to control a switchover valve is provided via network connection by the SAS division which acquires the information. For example, the positions of the Train 2 valves on the supply and return of Common 1a are acquired by SAS Division 2. This information is provided via a network connection to SAS Division 1 to perform the interlock function for the Train 1 valves on the supply and return of Common 1a.

RCP Thermal Barrier Containment Isolation Valves Interlock and RCP Thermal Barrier Containment Isolation Valves Opening Interlock

Another interlocking function is required concerning the cooling paths of the Common 1b and Common 2b headers for the reactor coolant pump (RCP) thermal barriers. Either the Common 1b or 2b header can provide cooling to the RCP thermal barriers. To maintain strict CCWS train separation, one of the supply containment isolation valves (CIV) and one of the return CIVs on the RCP thermal barriers cooling path must be closed on the header being removed from service (1b or 2b) prior to opening the CIVs on the header being placed in service (2b or 1b, respectively). The functional logic for the CIV interlock is shown in Figure 7.6-2—CCWS RCP Thermal Barrier Containment Isolation Valves Interlock. This safety-related interlock provides independence between redundant CCWS trains, such that if a failure occurs (e.g. pipe break) both redundant trains are not compromised.

An interlock function is required to open the CIVs on the common header removed from service (1b or 2b) when a CIV on the common header in service (2b or 1b, respectively) is closed. The functional logic for the CIV opening interlock is shown in Figure 7.6-12—CCWS RCP Thermal Barrier Containment Isolation Valves Opening Interlock. This safety-related interlock ensures that during a failure that causes the CIVs of the train in service to close, the redundant train's CIVs open to provide cooling to the RCP thermal barriers. During a manual switchover, if a CIV on the common header coming into service fails to open, then plant operating procedures require the CIVs to be realigned back to the initial configuration before switchover.

The interlock functions concerning the CIVs are also performed by the SAS. The CIVs are assigned to SAS divisions for control based on which electrical division provides power to the valves (i.e., valves powered by electrical Division 1 are controlled by SAS Division 1). The closed position indications of the CIVs on Common 1b are used to allow opening of the CIVs on Common 2b, and the closed position indication of the CIVs in Common 2b are used to allow the opening of the CIVs on Common 1b.

Redundant SAS controllers are provided in each division, and redundant networks are used between the divisions so that no single failure within the SAS can result in inadvertent connection or closure of redundant CCWS trains. Each valve is equipped with redundant open/closed position sensors so that a single sensor failure does not result in inadvertent connection of redundant CCWS trains. While each switchover valve is controlled by one SAS division, PACS modules in multiple divisions, acting on multiple solenoid devices, are required in order to change the position of a switchover valve. Therefore, a single PACS module failure does not result in inadvertent connection of redundant CCWS trains. For the CIV interlock, redundancy is obtained through the use of inner and outer CIVs, each controlled by a different division of SAS.

The single failure tolerance of the CCWS with respect to availability of the required cooling function is encompassed within the redundancy of the mechanical system design, as described in Section 9.2.2, and the two SAS CU pairs per division for the function.

The pulse function logic block is used so that once an operating common header is isolated, a momentary signal opens the standby common header and isolates the rest of the operating common header. This provides a momentary signal to switchover from an operating common header to the standby common header. The momentary signal's duration maintains an actuation signal, until the actuators reach their final position. A momentary signal is used to prevent concurrent and conflicting signals to the actuators between the CCWS RCP Thermal Opening function and the CCWS RCP Thermal Barrier Containment Isolation Valves Interlock for maintaining independence between the CCW trains feeding the RCP thermal barrier. A pulse order is used to provide assurance that a complete switchover between common headers occurs.

The following indications are provided to the operator relative to these interlocks:

- Indication of open or closed position of each interlocked valve.
- Alarm indicating position conflict between supply and return switchover valve of the same CCWS train relative to the same common header.
- Alarm indicating position conflict between CIVs of the same common header.
- Alarm indicating connection of two CCWS trains to the same common header.

7.6.1.2.4 IRWSTS Boundary Isolation for Preserving IRWST Water Inventory Interlock

The IRWST has a safety-related function to isolate the IRWST for purposes of preserving the IRWST water inventory to support the safety-related function of controlling core reactivity (via safety injection) by closing the IRWST isolation valves. This preserves IRWST inventory for long-term availability of safety injection, given a pipe failure in a connected non-safety related system. The functional logic is shown in Figure 7.6-4—IRWSTS Boundary Isolation for Preserving IRWST Water Inventory Interlock.

7.6.1.2.5 Safety Chilled Water System Interlocks

The SCWS has the following safety-related functions:

1. Transfer of heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions,
2. Component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power,

3. The capability to isolate components, systems, or piping, if required, so system safety functions are not compromised.

These safety-related automatic switchover functions provide that during a failure that prevents the train in service from transferring heat loads, the redundant train turns on to transfer the heat loads from the safety-related SSC. The pulse function logic block is used so that the circulating pumps are started and run to full speed, before the actuation signal is removed. A pulse order is used to provide assurance that the actions of the execute features go to completion. The time delay logic block is used to start the pumps in a sequenced fashion (one pump at a time); so that they are running at full speed before they are loaded to the system. The following automatic switchover functions verify that the SCWS is capable of fulfilling the safety-related functions in compliance with GDC 44:

- SCWS Train 1 to Train 2 Switchover on Train 1 Loss of Pump:

  The functional logic is shown in Figure 7.6-5—SCWS Train 1 to Train 2 Switchover on Train 1 Loss of Pump / Loss of Chiller / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock.

- SCWS Train 2 to Train 1 Switchover on Train 2 Loss of Pump:

  The functional logic is shown in Figure 7.6-6—SCWS Train 2 to Train 1 Switchover on Train 2 Loss of Pump / Loss of Chiller / Loss of UHS-CCWS / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock.

- SCWS Train 3 to Train 4 Switchover on Train 3 Loss of Pump:

  The functional logic is shown in Figure 7.6-7—SCWS Train 3 to Train 4 Switchover on Train 3 Loss of Pump / Loss of Chiller / Loss of UHS-CCWS / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock.

- SCWS Train 4 to Train 3 Switchover on Train 4 Loss of Pump:

  The functional logic is shown in Figure 7.6-8—SCWS Train 4 to Train 3 Switchover on Train 4 Loss of Pump / Loss of Chiller / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock.

- SCWS Train 1 to Train 2 Switchover on Train 1 Loss of Chiller:

  The functional logic is shown in Figure 7.6-5—SCWS Train 1 to Train 2 Switchover on Train 1 Loss of Pump / Loss of Chiller / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock.

- SCWS Train 2 to Train 1 Switchover on Train 2 Loss of Chiller:

  The functional logic is shown in Figure 7.6-6—SCWS Train 2 to Train 1 Switchover on Train 2 Loss of Pump / Loss of Chiller / Loss of UHS-CCWS / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock.

- SCWS Train 3 to Train 4 Switchover on Train 3 Loss of Chiller:

  The functional logic is shown in Figure 7.6-7—SCWS Train 3 to Train 4 Switchover on Train 3 Loss of Pump / Loss of Chiller / Loss of UHS-CCWS / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock.

- SCWS Train 4 to Train 3 Switchover on Train 4 Loss of Chiller:

  The functional logic is shown in Figure 7.6-8—SCWS Train 4 to Train 3 Switchover on Train 4 Loss of Pump / Loss of Chiller / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock.

- SCWS Train 1 to Train 2 Switchover on Train 1 LOOP Re-Start Failure:

  The functional logic is shown in Figure 7.6-5—SCWS Train 1 to Train 2 Switchover on Train 1 Loss of Pump / Loss of Chiller / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock.

- SCWS Train 2 to Train 1 Switchover on Train 2 LOOP Re-Start Failure:

  The functional logic is shown in Figure 7.6-6—SCWS Train 2 to Train 1 Switchover on Train 2 Loss of Pump / Loss of Chiller / Loss of UHS-CCWS / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock.

- SCWS Train 3 to Train 4 Switchover on Train 3 LOOP Re-Start Failure:

  The functional logic is shown in Figure 7.6-7—SCWS Train 3 to Train 4 Switchover on Train 3 Loss of Pump / Loss of Chiller / Loss of UHS-CCWS / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock.

- SCWS Train 4 to Train 3 Switchover on Train 4 LOOP Re-Start Failure:

  The functional logic is shown in Figure 7.6-8—SCWS Train 4 to Train 3 Switchover on Train 4 Loss of Pump / Loss of Chiller / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock.

The following automatic control function verifies that the SCWS is capable of fulfilling its safety-related functions in compliance with GDC 44:

- SCWS Chiller Evaporator Water Flow Control for Trains 1 and 4 to prevent freezing at the evaporator coil:

  The functional logic is shown in Figures 7.6-5 through 7.6-8.

7.6.1.2.6 Interlocks to Provide Low Temperature Over-Pressure Protection

Section 5.2.2 describes LTOP for the U.S. EPR design. Low temperature RCPB overpressure events include mass input events and heat input events. A start of four medium head safety injection (MHSI) pumps with one large miniflow line isolation valve failed into the closed position is the limiting case.

The MHSI pumps are used to inject borated water from the in-containment refueling water storage tank (IRWST) into the cold legs when a safety injection signal is present. A large miniflow line branches off from the discharge side of each MHSI pump and provides a path, through a motor operated isolation valve, to the IRWST. These isolation valves are interlocked in the open position during low temperature operations to reduce the MHSI injection pressure.

The interlock holding open the MHSI large miniflow valves serves two purposes:

- Protection against brittle fracture of the reactor pressure vessel (RPV).
- Protection of the RHR system from over-pressurization when it is connected to the RCS.

Brittle Fracture Protection:

The pressurizer safety relief valves (PSRVs) ultimately provide protection against brittle fracture of the RPV. However, the PSRV setpoints and sizing are based on the pressure and flow rates of four MHSI pumps, with one large miniflow valve failed closed, injecting into the RCS. For this reason, below the P17 permissive temperature threshold, the large miniflow line isolation valves are interlocked in the open position to make brittle fracture protection via the PSRVs effective. Actuation of the PSRVs by the PS in an LTOP capacity is described in Section 7.3.

RHR System Protection:

The RHR system can only be connected to the RCS below the P14 permissive RCS temperature threshold. Below the P14 permissive temperature, over-pressure protection of the RHR system is provided differently in two different RCS temperature regimes, as described below. In both temperature regimes, a start of four MHSI pumps with one MHSI large miniflow line isolation valve failed into the closed position is representative of the limiting pressure addition event.

P14 temperature > RCS temperature > P17 temperature

When the P14 permissive is validated and one or more trains of RHR are connected to the RCS, the MHSI large miniflow valves are interlocked in the open position. The RHR spring-loaded safety valves along with the interlock holding the large miniflow valves open provide overpressure protection of the RHR system in this temperature regime.

During the postulated pressure addition event, by the time RCS pressure reaches the RHR safety valve opening setpoint, the three MHSI pumps with open large miniflow valves are no longer able to inject due to a higher RCS pressure caused by the single MHSI pump with its large miniflow valve closed. Therefore the other three MHSI pumps re-circulate through their miniflow lines to the IRWST. This leaves the one

MHSI pump with its (failed) closed large miniflow valve injecting into the RCS. The RHR spring loaded safety valves are sized based on the pressure and flow rate of one MHSI pump, with large miniflow line isolated, injecting into the RCS while RHR is connected.

P17 temperature > RCS temperature

When the P17 permissive is validated, the MHSI large miniflow valves are interlocked in the open position. The PSRVs operating in their LTOP mode along with the interlock holding the large miniflow valves open provide over-pressure protection of the RHR system in this temperature regime.

The LTOP setpoints for opening of PSRVs are lower than the RHR spring-loaded safety valve setpoints. Therefore, during the postulated pressure addition event, the PSRVs relieve pressure before the design pressure of the connected RHR system is reached. The PSRV setpoints and sizing are based on the pressure and flow rate of four MHSI pumps, with one miniflow line isolated, injecting into the RCS. Actuation of the PSRVs by the PS in an LTOP capacity is described in Section 7.3.

Generation of the P14 and P17 permissive signals is described in Sections 7.2.1.2.9 and 7.2.1.3.12.

The logic for the MHSI large miniflow valves interlock between P14 and P17 permissives is shown in Figure 7.6-3. RHR isolation valves interlock is shown in Figure 7.6-11.

Two redundant ALUs within a PS division each send the interlock signal to the large miniflow line isolation valve of one MHSI train. This arrangement precludes a single ALU failure from preventing the opening of a valve. The failure of a single PACS module or of a single valve results in one MHSI large miniflow line being isolated, which is accounted for in the design of the RHR safety valves and PSRVs as previously described.

Additionally, no single failure can prevent the isolation valve from being closed on at least one MHSI injection path during power operation when maximum MHSI discharge pressure is required.

The operational status of the PS on a divisional basis is provided to the operator. Indications and alarms are provided to the operator regarding the state of the P14 and P17 permissives. Additionally, the following indications are provided to the operator to verify correct operation of the interlock:

- Open or closed position of each MHSI large miniflow line isolation valve (each train).

- Status of MHSI pump (on or off, each train).
- Open or closed position of each isolation valve as shown in Figure 7.6-3.

7.6.2 Analysis

The analysis provided in this section pertains to the I&C functionality related to interlocks important to safety, or supports U.S. EPR compliance with requirements at the plant level. Compliance of specific mechanical configurations, valves and piping with applicable codes and standards is addressed in the appropriate sections identified in Section 7.6.1.

7.6.2.1 Compliance with Applicable Criteria

7.6.2.1.1 Compliance with the Single Failure Criterion (Clause 5.1 of IEEE Std 603-1998)

The interlocks important to safety are designed to satisfy the single failure criteria. Specific aspects of single failure accommodation are described as part of the functional description of each interlock in Section 7.6.1.2. Accommodation of single failures at the system level for the PS, SAS, and PACS is described in Section 7.1.

Accommodation of single failures at the system level for the mechanical safety systems described in this chapter is addressed in the relevant sections identified in Section 7.6.1.2.

7.6.2.1.2 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)

Components and modules that are required to perform the interlocking functions described in this section are classified as safety-related. They are designed to Class 1E standards and are applied in accordance with a quality assurance program. Software used in these functions is developed and applied in accordance with ANP-10272-A (Reference 3). Further discussion of safety-related I&C system compliance with requirements for quality is found in Section 7.1.

7.6.2.1.3 Compliance with Requirements for Independence (Clauses 5.6 and 6.3 of IEEE Std 603-1998)

Redundant divisions of the safety-related I&C systems are independent from one another so that a failure in any one portion of the system does not prevent the redundant portions from performing their function. Both electrical and communication independence are maintained as described in Section 7.1.

I&C equipment required to perform the interlock functions described in this section is independent from the effects of anticipated operational occurrences and postulated accidents. The safety-related I&C systems are located in areas that are not subject to degraded environmental conditions as the result of an event. Equipment that may be located in areas subject to a degraded environment is required to be qualified to operate in the expected post-event conditions. 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 non-safety-related systems to perform the interlock functions described in this section. Certain sensor measurements are used as inputs to both a safety-related interlock function, and a non-safety-related control function performed by a non-safety-related I&C system. In these cases, the signal conditioning and distribution system (SCDS) is provided to condition (if necessary) and distribute signal inputs needed within multiple distributed control system (DCS) subsystems.

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

Surveillance of the safety-related I&C systems consists of overlapping tests to verify performance of the interlock function from sensor to PACS module.

Sensors and acquisition circuits are periodically tested. The input channel to be tested is placed in a lockout condition, and the downstream logic is automatically modified to disregard the input under test and maintain the interlock function in its current state.

The functional unit of the safety-related systems 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.

With respect to the connections between the output circuits of the PS and SAS, and the PACS modules, and to the actuators themselves, surveillance of interlocking functions during power operations can be satisfied by observing the correct interlocked position of the actuators.

The safety-related I&C systems are designed to provide bypassed and inoperable status information to the operator. Sufficient indications are provided to the operator to evaluate the status of each interlock as described in the relevant functional descriptions in Section 7.6.1.2.

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

The interlock functions described in this section are implemented in I&C systems using the TELEPERM XS platform, which is approved for use in safety-related systems of nuclear power generating stations in the United States. These systems are implemented in architectures designed to satisfy requirements applicable to digital safety-related I&C systems.

Implementation of safety-related I&C systems is governed by the requirements of IEEE Std 603-1998 (Reference 1). Compliance with this requirement is described in Section 7.1. Guidance on the use of digital computers in safety systems is provided by IEEE Std 7-4.3.2-2003 (Reference 2). Conformance to this guidance is described in Section 7.1.

7.6.3 References

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

2. 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.

3. [*ANP-10272-A, Revision 3, “Software Program Manual TELEPERM XS™ Safety Systems Topical Report,” AREVA NP Inc., July 2011.*]*

Next File