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 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., acknowledgement of permissive signal status) is provided on both the process information and control system (PICS) and the safety information and control system (SICS). Manual actions taken from the SICS have priority over those from the PICS as described in Section 7.1.

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 permissive P14 pressure and temperature thresholds.

When RCS pressure or temperature is above the P14 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 acknowledge P14 which allows the isolation valves to be opened to connect RHR.

Generation of the P14 permissive signal is described in Section 7.2.1.3.

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 holds closed a single valve on train one and a single valve on train two. Division two of the PS holds closed a single valve on train two and a single valve on train one). 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 is 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 pressure and temperature measurements must be below the P14 setpoint values before the valves can be opened. Additionally, the operator is prompted to acknowledge the P14 condition, providing a third diverse condition that must be satisfied to allow valve opening.

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 pressurizer safety relief valves (PSRV) operating in their low temperature overpressure protection (LTOP) mode (Section 7.3.1.2.13), and spring loaded safety valves on the RHR suction lines prevent the increasing pressure from exceeding the RHR system design pressure. During an intentional increase in pressure, when either RCS temperature or pressure exceed the P14 setpoint, the operator is prompted to acknowledge P14, 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

permissive P14 signal. Additionally, the following indications are provided to the operator to verify correct operation of the interlock:

- Open or closed position of 1st RHR RCPB isolation valve (each train).
- Open or closed position of 2nd 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 open above a specified RCS pressure value. This pressure value is the permissive P12 threshold.

Generation of the P12 permissive signal is described in Section 7.2.1.3.

When RCS pressure increases above the P12 threshold, the PS provides automatic signals to open the accumulator isolation valves. Once the valves are verified to be in the 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 threshold, the operator is prompted to manually acknowledge P12 which allows the isolation valves to be closed.

Two redundant ALU within a division send the automatic opening signal to the isolation valve of the corresponding accumulator (i.e., PS division one 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 priority actuation and control (PAC) 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.
- Open or closed position of each accumulator isolation valve.

7.6.1.2.3 Interlocks Isolating Redundant CCWS Trains

The CCWS is comprised of four closed-loop, safety-related supply trains that function to cool and transfer heat load from safety users to the 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 CCW train one or train two while the Common-2 header is supplied by either CCW train three or train four. 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.

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.

CCWS train one has a single valve on the supply side and a single valve on the return side of Common 1a. Train two 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 one must be closed before either valve on train two can be opened. Likewise, both valves on train two must be closed before either valve on train one can be opened. The same valve arrangement and interlocks are provided relative to Common 1b to provide separation between trains one and two, and on Common 2a and 2b to provide separation between trains three and four.

Another interlocking function is required concerning the cooling paths of the Common 1b and Common 2b headers toward the reactor coolant pump (RCP) thermal barriers. Either the Common 1b or 2b headers can provide cooling to the RCP thermal barriers. To maintain strict CCWS train separation, the containment isolation valves (CIV) on the RCP thermal barriers cooling path on the supply and return side of Common 1b cannot be opened unless the CIVs on both the supply and return side of Common 2b are closed, and vice versa.

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 one are assigned to SAS division one). 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 two valves on the supply and return of Common 1a are acquired by SAS division two. This information is transmitted to SAS division one to perform the interlock function for the train one valves on the supply and return of Common 1a.

The interlock function concerning the CIVs is also performed by the SAS, but is only performed in divisions one and four. 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 one are controlled by SAS division one). The closed

position indications of the CIVs on common-1b are used to allow opening of the CIVs on Common 1a, and vice versa.

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 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 I&C division, multiple PAC modules in that division, acting on multiple solenoid devices, are required in order to change the position of a switchover valve. Therefore, a single PAC 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 I&C.

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.

The following indications are provided to the operator relative to this interlock:

- 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 Interlocks to Provide Low Temperature Over-Pressure Protection

Low temperature RCPB overpressure events include mass input events and heat input events. Section 5.2.2 describes LTOP for the U.S. EPR design. An interlock is provided to support brittle fracture protection in case of a safety injection actuation during low temperature operation.

The medium head safety injection (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. Below the P17 temperature threshold, the large miniflow line isolation valves are interlocked in the open position to limit the discharge pressure of the MHSI pumps. This provides protection against a fast increase in RCS pressure during cold conditions. When the P17 signal is present the PS maintains an open order, with highest priority, to all four large miniflow lines to prevent their inadvertent closure.

Generation of the P17 permissive signal is described in Section 7.2.1.3.

Two redundant ALU 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 is accommodated by PSRVs operating in their LTOP mode. The PSRVs provide adequate brittle fracture protection following the start of four MHSI pumps with any one large miniflow line in the closed position.

Actuation of the pressurizer safety relief valves by the PS in a LTOP capacity is described in Section 7.3.

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 P17. 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).

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 or 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 to Applicable Criteria

7.6.2.1.1 Compliance to 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 to Requirements for Quality of Components and Modules (Clause 5.3 of IEEE Std 603-1998 and Clause 5.3 of IEEE 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 stringent quality assurance program.

Software used in these functions is developed and applied in accordance with a safety related software program. Further discussion of safety related I&C system conformance to requirements for quality is found in Section 7.1.

7.6.2.1.3 Compliance to 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 design basis events. The computerized portions of the safety 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 (e.g., sensors) 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 measurement is acquired by the signal conditioning of the safety related system, is multiplied, and then passed to the non-safety related system through an electrically isolated connection.

7.6.2.1.4 Compliance to Requirements for System Testing and Inoperable Surveillance

Surveillance of the safety related I&C systems consists of overlapping tests to verify performance of the interlock function from sensor to PAC 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 computerized portions of the safety systems 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.

With respect to the connections between the output circuits of the PS and the PAC 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 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 systems of nuclear power generating stations in the United States. These systems are implemented in architectures 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 Std 603-1998 (Reference 1). Guidance on the use of digital computers in safety systems is provided by IEEE 7-4.3.2-2003 (Reference 2). Conformance to these standards 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 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.