7.6 Interlock Systems Important to Safety

This section discusses interlock systems which operate to reduce the probability of occurrence of specific events or to verify the state of a safety system. These include interlocks to prevent overpressurization of low-pressure systems and interlocks to verify availability of engineered safety features.

7.6.1 Prevention of Overpressurization of Low-Pressure Systems

7.6.1.1 Description of Normal Residual Heat Removal Isolation Valve Interlocks

An interlock is provided for the normally closed, motor-operated normal residual heat removal system (RNS) inner and outer suction isolation valves. The interlock prevents the suction valves for the normal residual heat removal system from being opened by operator action unless the reactor coolant system pressure is less than a preset pressure and both the suction and discharge valves for the in-containment refueling water storage tank are in a closed position.

There are two parallel sets of two motor-operated valves in series in the normal residual heat removal system pumps suction line from the reactor coolant system hot leg. The two valves nearest the reactor coolant system are designated as the inner isolation valves. The two valves nearest the normal residual heat removal system pumps are designated as the outer isolation valves. Logic for the outer valves is similar to that provided for the inner isolation valves, except that equipment diversity is provided by virtue of the fact that the pressure transmitters used for valve interlocks on the inner valves are diverse from the pressure transmitters used for the outer valve interlocks. Typically, this diversity is achieved by procuring wide range pressure transmitters either with similar measurement principles from different vendors, or with different measurement principles (from either the same or different vendors).

Each valve is interlocked so that it cannot be opened unless the reactor coolant system pressure is below a preset pressure. This interlock prevents the valve from being opened (from the main control room or the remote shutdown workstation) when the reactor coolant system pressure is above the normal residual heat removal system design pressure.

Figure 7.2-1, Sheet 18 illustrates the interlock logic that applies to these valves. The logic, shown on Sheet 18, is replicated twice, once for each parallel path. This interlock logic prevents the two series isolation valves from being opened while the reactor coolant system is pressurized above a set pressure.

The valves may be closed by operator action from the main control room at any time. To prevent an inadvertent closure of these valves, no auto-closure interlock that would close the valves on high reactor coolant system pressure is included.

The normal residual heat removal system relief valves provide adequate system pressure protection for conditions after the valves have been opened. (This is discussed in subsection 5.2.2.1). Alarms are provided in the main control room and on the remote shutdown workstation to alert the operator if reactor coolant system pressure exceeds the normal residual heat removal system design pressure after the valves are opened.

7.6.1.2 Analysis of Normal Residual Heat Removal Valve Interlocks

IEEE 603-1991 and IEEE 338-1987 criteria do not apply to the normal residual heat removal isolation valve interlocks. Their function is not required during, or after, a design basis event. However, because of the possible severity of the consequences of loss of function, the requirements of IEEE 603-1991 are applied with the following comments:

- For the purpose of applying IEEE 603-1991, the protection system is the two parallel sets of two valves in series and the components of their interlock circuitry. The inner valve is powered by a separate power supply from the outer valve of each series combination.

- Online testability; IEEE 603-1991, Paragraph 5.7: The pressure interlock signals and logic are tested on line to the maximum extent possible without adversely affecting safety. This test includes the initiating signals for the interlocks from the protection and safety monitoring system cabinets.

- IEEE 603-1991, Paragraph 6.8.2: This requirement does not apply, as the setpoints are independent of mode of operation and are not changed.

7.6.2 Availability of Engineered Safety Features

7.6.2.1 Passive Residual Heat Removal Heat Exchanger Inlet Isolation Valve

The passive core cooling system passive residual heat removal heat exchanger inlet line includes a normally open motor-operated isolation valve that can be manually controlled from either the main control room or the remote shutdown workstation. The generation of the confirmatory open signal to this valve is described in subsection 7.3.1.2.7.

The use of a confirmatory open signal to this valve provides a means to automatically override bypass features that are provided to allow this isolation valve to be closed for short periods of time. As a result of the confirmatory open signal, isolation of the passive residual heat removal heat exchanger inlet line, for short periods of time during modes of plant operation when the passive residual heat removal heat exchanger is required to be operable, is acceptable.

The operation of the valve is controlled by an actuation control circuit that functions in the following manner:

- The control circuit has an automatic operation function that is normally enabled. It allows the valve to automatically open upon receipt of the confirmatory open signal, in case the valve is closed.

- The control circuit has a valve open actuation function that opens the valve when a control switch on the operator workstation is manually actuated. Once the operation is complete, the control circuit returns to automatic operation.

- The control circuit has a valve close actuation function that closes the valve when a control switch on the operator workstation is manually actuated. This function is required when performing periodic operability testing of the passive residual heat removal heat exchanger discharge valves when the reactor is operating. Once the manual operation is complete, the control circuit returns to automatic operation.

- The control circuit has a valve maintain closed actuation function to provide an administratively controlled manual block of the automatic opening of the valve. This function allows the valve to be maintained closed if needed for leakage isolation. The maximum permissible time that a passive residual heat removal heat exchanger inlet isolation valve can be closed is specified in technical specifications. An alarm is actuated when the maintain closed function is instated.

The valve is interlocked so that:

- If the maintain closed actuation has not been manually initiated, it opens automatically on receipt of a confirmatory open signal with the control circuit in automatic control or during the manual valve close function.

- It cannot be manually closed when a confirmatory open signal is present.

During plant operation and shutdown, the passive residual heat removal heat exchanger inlet isolation valve is open. To prevent an inadvertent closure of the valve, redundant output cards are used in the protection and safety monitoring system cabinet. Power to this valve is normally locked out at power to prevent a fire-induced spurious closing.

Figure 7.2-1, sheet 17 illustrates the interlock logic which applies to the passive residual heat removal heat exchanger inlet isolation valve.

This normally open motor-operated valve has alarms, indicating valve mispositioning (with regard to their passive core cooling function). The alarm actuates in the main control room and the remote shutdown workstation.

An alarm actuates for the passive residual heat removal heat exchanger inlet isolation valve under the following conditions when the passive residual heat removal heat exchanger is required:

- Sensors on the motor operator for the valve indicate when the valve is not fully open.

- Redundant sensors on the valve stem indicate when the valve is not fully open.

7.6.2.2 Core Makeup Tank Cold Leg Balance Line Isolation Valves

Each core makeup tank has a cold leg balance line which is provided with a normally open, motor-operated, isolation valve. The balance line isolation valves, for each core makeup tank, may be manually controlled from either the main control room or the remote shutdown workstation. The generation of the confirmatory open signal to these valves is described in subsection 7.3.1.2.3.

A confirmatory open signal to these valves automatically overrides any bypass features that are provided to allow the balance line isolation valve to be closed for short periods of time. As a result of the confirmatory open signal, isolation of the core makeup tank cold leg balance line to permit inservice testing of the core makeup tank discharge valves, is acceptable.

The operation of each valve is controlled by an actuation control circuit that functions in the following manner:

- The control circuit has an automatic operation function that automatically opens the valve upon receipt of the confirmatory open signal, in case the valve is closed.

- The control circuit has a valve open actuation function that opens the valve when a control switch on the operator workstation is manually actuated. Once the operation is complete, the control circuit returns to automatic operation.

- The control circuit has a valve close actuation function that closes the valve when a control switch on the operator workstation is manually actuated. This function is provided for performing periodic operability tests of the core makeup tank discharge valves when the reactor is operating. Once the manual operation is complete, the control circuit returns to automatic operation.

- The control circuit has a valve maintain closed actuation function to provide an administratively controlled manual block of the automatic opening of the valve when the pressurizer level is greater than the P-12 interlock. This function allows the valve to be maintained closed if needed for leakage isolation. The maximum permissible time that a core makeup tank cold leg balance line isolation valve can be closed is specified in technical specifications. An alarm is actuated when the maintain closed function is instated.

Each valve is interlocked so that:

- It receives a confirmatory open signal automatically whenever the pressurizer water level increases above the P-12 interlock.

- It cannot be manually closed when a confirmatory open signal is present.

During power and shutdown operations, the core makeup tank cold leg balance line isolation valve remains open. To prevent an inadvertent closure of the valve, redundant output cards are used in the protection and safety monitoring system cabinet. As a result, it is not necessary to lock out control circuit power.

Figure 7.2-1, sheet 17 illustrates the interlock logic which applies to the cold leg balance line isolation valves on each of the two core makeup tanks. The logic shown on sheet 17 is replicated for each core makeup tank.

These normally open motor-operated valves have alarms, indicating valve mispositioning (with regard to their passive core cooling function). The alarms actuate in the main control room and the remote shutdown workstation.

An alarm actuates for a core makeup tank cold leg balance line isolation valve under the following conditions when the core makeup tank is required to be operable:

- Sensors on the motor operator for the valve indicate when the valve is not fully open.

- Redundant position sensors indicate when the valve is not fully open.

7.6.2.3 Interlocks for the Accumulator Isolation Valve and IRWST Discharge Valve

The accumulator isolation and in-containment refueling water storage tank injection isolation valves are safety-related in order to retain their pressure boundary and remain in their open position. The accumulator isolation and in-containment refueling water storage tank injection valve operators are nonsafety-related since the valves are not required to change position to mitigate an accident. The DCD Chapter 15 safety analyses assume that these valves are not subject to valve mispositioning (prior to an accident) or spurious closure (during an accident). Valve mispositioning and spurious closure are prevented by the following:

- The Technical Specifications, Section 16.1, require these valves to be open and power locked out whenever these injection paths are required to be available. The accumulators are required to be available when the reactor coolant system pressure is above 1000 psig. Both in-containment refueling water storage tank injection lines are required to be available in Modes 1, 2, 3, and 4. One in-containment refueling water storage tank injection line is required to be available in Mode 5 and in Mode 6.

- The Technical Specifications, Section 16.1, require verification that the motor-operated valves are open every 12 hours. They also require verification that power is removed every 31 days.

- With power locked out, redundant (nonsafety-related) valve position indication is provided in the main control room and remote shutdown workstation. Valve position indication and alarm are provided to alert the operator if these valves are mispositioned. These indications are powered by different nonsafety-related power supplies.

In addition, the valves have a confirmatory open signal during an accident (safeguards actuation signal for accumulator motor-operated valves and automatic depressurization system stage 4 signal for in-containment refueling water storage tank motor-operated valves). The valves also have an automatic open signal when their close permissives (P-11 for accumulator motor-operated valves and P-12 for in-containment refueling water storage tank motor-operated valves) clear during plant startup. The confirmatory open and the automatic open control signals are provided to the valve operator by the nonsafety-related plant control system.

7.6.3 Combined License Information

This section has no requirement for information to be provided in support of the Combined License application.