7.2 REACTOR PROTECTION SYSTEM

7.2.1 Safety Objective

The Reactor Protection System provides timely protection against the onset and consequences of conditions that threaten the integrities of the fuel barrier (uranium dioxide sealed in cladding) and the nuclear system process barrier. Excessive temperature threatens to perforate the cladding or melt the uranium dioxide. Excessive pressure threatens to rupture the nuclear system process barrier. The Reactor Protection System limits the uncontrolled release of radioactive material by terminating excessive temperature and pressure increases through the initiation of an automatic scram.

7.2.2 Safety Design Basis

1. The Reactor Protection System shall initiate, with precision and reliability, a reactor scram in time to prevent fuel damage following abnormal operational transients.

2. The Reactor Protection System shall initiate, with precision and reliability, a scram in time to prevent damage to the nuclear system process barrier as a result of internal pressure. Specifically, the Reactor Protection System shall initiate a reactor scram in time to prevent nuclear system pressure from exceeding the nuclear system pressure allowed by applicable industry codes.

3. To limit the uncontrolled release of radioactive materials from the fuel or nuclear system process barrier, the Reactor Protection System shall initiate, with precision and reliability, a reactor scram to prevent gross failure of either of these barriers.

4. To provide assurance that conditions which threaten the fuel or nuclear system process barriers are detected with sufficient timeliness and precision to fulfill safety design bases 1, 2, and 3, Reactor Protection System inputs shall be derived, to the extent feasible and practical, from variables that are true, direct measures of operational conditions.

5. To provide assurance that important variables are monitored with a precision sufficient to fulfill safety design bases 1, 2, and 3, the Reactor Protection System shall respond correctly to the sensed variables over the expected range of magnitudes and rates of change.

6. To provide assurance that important variables are monitored with a precision sufficient to fulfill safety design bases 1, 2, and 3, an adequate number of sensors shall be provided for monitoring essential variables that have spatial dependence.

7. The following bases provide assurance that the Reactor Protection System is designed with sufficient reliability to fulfill safety design bases 1, 2, and 3.

   a. No single failure within the Reactor Protection System shall prevent proper Reactor Protection System action when required to satisfy safety design basis 1, 2, and 3.

   b. Any one intentional bypass, maintenance operation, calibration operation, or test to verify operational availability shall not impair the ability of the Reactor Protection System to respond correctly.

   c. The system shall be designed for a high probability that when any monitored variable exceeds the scram setpoint, the event shall result in an automatic scram and shall not impair the ability of the system to scram as other monitored variables exceed their scram trip points.

   d. Where a plant condition that requires a reactor scram can be brought on by a failure or malfunction of a control or regulating system, and the same failure or malfunction prevents action by one or more Reactor Protection System channel(s) designed to provide protection against the unsafe condition, the remaining portions of the Reactor Protection System shall meet the requirements of safety design bases 1, 2, 3, and 7a.

   e. The power supply for the Reactor Protection System shall be arranged so that loss of one supply neither causes nor prevents a reactor scram.

   f. The system shall be designed so that, once initiated, a Reactor Protection System action goes to completion. Return to normal operation after protection system action shall require deliberate operator action.

   g. There shall be sufficient electrical and physical separation between channels and between logics monitoring the same variable to prevent environmental factors, electrical transients, and physical events from impairing the ability of the system to respond correctly.

   h. Earthquake ground motions shall not impair the ability of the Reactor Protection System to initiate a reactor scram.

8. The following bases are specified to reduce the probability that Reactor Protection System operational reliability and precision will be degraded by operator error.

a. Access to all trip settings, component calibration controls, test points, and other terminal points for equipment associated with essential monitored variables shall be under administrative control.

b. The means for manually bypassing logics, channels, or system components shall be under administrative control. If the ability to trip some essential part of the system has been bypassed, this fact is continuously indicated in the control room. Bypassing of the NMS inop trip using the Operate-Calibrate bypass switch (fiber optic bypass switch (FOBS) on Units 1, 2, and 3) shall be under Administrative control to allow functional tests of the NMS to be performed.

9. To provide the operator with means independent of the automatic scram functions to counteract conditions that threaten the fuel or nuclear system process barrier, it shall be possible for the control room operator to manually initiate a reactor scram.

10. The following bases are specified to provide the operator with the means to assess the condition of the Reactor Protection System and to identify conditions that threaten the integrities of the fuel or nuclear system process barrier.

    a. The Reactor Protection System shall be designed to provide the operator with information pertinent to the operational status of the protection system.

    b. Means shall be provided for prompt identification of channel and trip system responses.

11. It shall be possible to check the operational availability of each channel and logic.

7.2.3 Description

7.2.3.1 Identification

The Reactor Protection System includes the motor-generator power supplies with associated control and indicating equipment, sensors, relays, bypass circuitry, and switches that supply a signal to the Control Rod Drive (CRD) System to cause rapid insertion of control rods (scram) to shut down the reactor. It also includes outputs to the process computer system and annunciators. The Reactor Protection System is designed to meet the intent of the IEEE proposed criteria for nuclear power plant protection systems (IEEE-279-1971). The process computer system and annunciators are not part of the Reactor Protection System. Although scram signals

are received from the Neutron Monitoring System, this system is treated as a separate nuclear safety system in Subsection 7.5.

7.2.3.2 Power Supply

Power to each of the two reactor protection trip systems is supplied, via a separate bus, by its own high-inertia, AC motor-generator set (see Figures 7.2-1, 7.2-3, and 7.2-7c). Each generator has a voltage regulator which is designed to respond to a step-load change of 50 percent of rated load with an output voltage change of not greater than 15 percent. High inertia is provided by a flywheel. The inertia is sufficient to maintain voltage and frequency within 5 percent of rated values for at least 1.0 second following total loss of power to the drive motor. Automatic circuit protectors were added to these MG sets to provide Class 1E isolation of the RPS should the supply voltage or frequency become abnormal.

Alternate power is available to either Reactor Protection System bus from an electrical bus that can receive standby electrical power. The alternate power switch prevents simultaneously feeding both buses from the same source. The switch also prevents paralleling a motor-generator set with the alternate supply. The DC power is supplied to the backup scram valve solenoids from the plant batteries.

7.2.3.3 Physical Arrangement

Instrument piping that taps into the reactor vessel is routed through the drywell wall and terminates inside the secondary containment (Reactor Building). Reactor vessel pressure and water level information is sensed from this piping by instruments mounted on instrument racks in the Reactor Building. Valve position switches are mounted on valves from which position information is required. The sensors for Reactor Protection System signals from equipment in the Turbine Building are mounted locally in the Turbine Building. The two motor-generator sets that supply power for the Reactor Protection System are located in the Control Building in an area where they can be serviced during reactor operation. Cables from sensors, Analog Trip Unit (ATU) Cabinets, and power cables are routed to two Reactor Protection System cabinets in the Auxiliary Instrument Room, where the logic circuitry of the system is formed. One cabinet is used for each of the two trip systems. The logics of each trip system are isolated in separate bays in each cabinet, as shown in Figures 7.2-2, 7.2-8, and 7.2-9. The Reactor Protection System, except for the motor-generator sets and signals from nonseismic structures, is designed as Class I equipment to assure a safe reactor shutdown during and after seismic disturbances. The detailed requirements for Class I equipment are described in Appendix C.

7.2.3.4 Logic

The Reactor Protection System is arranged as two separately powered trip systems. Each trip system has three logics, as shown in Figure 7.2-4. Two of the logics are used to produce automatic trip signals. The remaining logic is used for a manual trip signal. The Source Range Monitoring System and mode switch in shutdown trip function actuate through the manual channel. Each of the two logics used for automatic trip signals received input signals from at least one channel for each monitored variable. Thus, two channels are required for each monitored variable to provide independent inputs to the logics of one trip system. At least four channels for each monitored variable are required for the logics of both trip systems.

As shown in Figure 7.2-5, the actuators associated with any one logic provide inputs into each of the actuator logics for the associated trip system. Thus, either of the two automatic logics associated with one trip system can produce a trip system trip. The logic is a one-out-of-two arrangement. To produce a scram, the actuator logics of both trip systems must be tripped. The overall logic of the Reactor Protection System could be termed one-out-of-two taken twice except for the Power Range Neutron Monitoring System which implements a two-out-of-four logic design.

7.2.3.5 Operation (Figures 7.2-1, 7.2-3, 7.2-4 and 7.2-7c)

To facilitate the description of the Reactor Protection System, the two trip systems are called trip system A and trip system B. The automatic logics of trip system A are logics A1 and A2; the manual logic of trip system A is logic A3. Similarly, the logics for trip system B are logics B1, B2, and B3. The actuators associated with any particular logic are identified by the logic identity (such as actuators B2) and a letter (see Figure 7.2-4). The actuator logics associated with a trip system are identified with the trip system identity (such as actuator logics A). Channels are identified by the name of the monitored variable and the logic identity with which the channel is associated (such as reactor vessel high pressure channel B1).

During normal operation, all sensor and trip contacts essential to safety are closed; channels, logics, and actuators are energized.

There are two scram pilot valves and two scram valves for each control rod. Each scram pilot valve is solenoid-operated. The solenoids are normally energized. The two scram pilot valves, associated with a control rod, control the air supply to both scram valves for that rod. With either scram pilot valve energized, air pressure holds the scram valves closed. The scram valves control the supply and discharge paths for control rod drive water. One of the scram pilot valves for each control rod is controlled by actuator logics A, the other valve by actuator logics B. There are two DC, solenoid-operated, backup scram valves which provide a second means of controlling the air supply to the scram valves for all control rods. The DC solenoid for each backup scram valve is normally deenergized. The backup scram valves are energized (initiate scram) when both trip system A and trip system B are tripped.

Whenever a channel sensor contact opens, its sensor relay deenergizes, causing contacts in the logic to open. The opening of contacts in the logic deenergizes its actuators. When deenergized, the actuators open contacts in all the actuator logics for that trip system. This action results in deenergizing the scram pilot valve solenoids associated with that trip system (one scram pilot valve solenoid for each control rod). Unless the other scram pilot valve solenoid for each rod is deenergized, the rods are not scrammed. If a trip then occurs in any of the logics of the other trip system, the remaining scram pilot valve solenoid for each rod is deenergized, venting the air pressure from the scram valves, and allowing control rod drive water to act on the control rod drive piston. Thus, all control rods are scrammed. The water displaced by the movement of each rod piston is vented into a scram discharge volume. When the solenoid for each backup scram valve is energized, the backup scram valves vent the air supply for the scram valves; this action initiates insertion of every control rod regardless of the action of the scram pilot valves.

A scram can be manually initiated. There are two scram buttons, one for logic A3 and one for logic B3. Depressing the scram button on the logic A3 deenergizes actuators A3 and opens corresponding contacts in actuator logics A. A single trip system trip is the result. To effect a manual scram, the buttons for both logic A3 and logic B3 must be depressed. By operating the manual scram button for one manual logic at a time, followed by reset of that logic, each trip system can be tested for manual scram capability. It is also possible for the control room operator to scram the reactor by interrupting power to the Reactor Protection System. This can be done by operating power supply breakers. The manual scram capability provided in the control room meets safety design basis 9.

To restore the Reactor Protection System to normal operation following any single trip system trip or scram, the actuators must be manually reset. Reset is possible only if the conditions that caused the trip or scram have been cleared, and it is accomplished by operating switches in the control room. This meets safety design basis 7f.

Whenever a Reactor Protection System sensor trips, it lights a printed annunciator window, common to all the channels for that variable, on the reactor control panel in the control room to indicate the out-of-limit variable. Each trip system lights an annunciator window indicating the trip system which has tripped.

A Reactor Protection System channel trip also sounds a buzzer or horn, which can be silenced by the operator. The annunciator window lights latch in until manually reset; reset is not possible until the condition causing the trip has been cleared. The physical positions of Reactor Protection System relays are used to identify the individual sensor that tripped in a group of sensors monitoring the same variable. The location of alarm windows provides the operator with the means to quickly

identify the cause of Reactor Protection System trips and to evaluate the threat to the fuel or nuclear system process barrier.

To provide the operator with the ability to analyze an abnormal transient during which events occur too rapidly for direct operator comprehension, all Reactor Protection System trips are recorded by an alarm typewriter controlled by the Process Computer System. All trip events are recorded. The first 40 are recorded in chronological sequence, except that events occurring within 16 milliseconds of each other are treated as having occurred simultaneously. Use of the alarm typewriter and computer is not required for plant safety, and information provided is in addition to that immediately available from other annunciators and data displays. The printout of trips is of particular usefulness in routinely verifying the proper operation of pressure, level, and valve position switches as trip points are passed during startups, shutdowns, and maintenance operations.

Reactor Protection System inputs to annunciators, recorders, and the computer are arranged so that no malfunction of the annunciating, recording, or computing equipment can functionally disable the Reactor Protection System. Signals directly from the Reactor Protection System sensors are not used as inputs to annunciating or data logging equipment. Isolation is provided between the primary signal and the information output. The arrangement of indications pertinent to the status and response of the Reactor Protection System satisfies safety design bases 10a and 10b.

7.2.3.6 Scram Functions and Bases for Trip Settings

The following discussion covers the functional considerations for the variables or conditions monitored by the Reactor Protection System. Table 7.2-1 lists the specifications for instruments providing signals for the system. Figure 7.2-6 shows the scram functions in block form.

1. Neutron Monitoring System trip--To provide protection for the fuel against high heat-generation rates, neutron flux is monitored and used to initiate a reactor scram. The Neutron Monitoring System setpoints and their bases are discussed in Subsection 7.5, "Neutron Monitoring System."

2. Nuclear system high pressure--High pressure within the nuclear system poses a direct threat of rupture to the nuclear system process barrier. A nuclear system pressure increase, while the reactor is operating, compresses the steam voids and results in a positive reactivity insertion, causing increased core heat generation that could lead to fuel failure and system overpressurization. A scram counteracts a pressure increase by quickly reducing the core fission-heat generation.

The nuclear system high-pressure scram setting is chosen slightly above the reactor vessel maximum normal operating pressure to permit normal operation without spurious scram, yet provide a wide margin to the maximum allowable nuclear system pressure. The location of the pressure measurement, as compared to the location of highest nuclear system pressure during transients, was also considered in the selection of the high-pressure scram setting. The nuclear system high-pressure scram works in conjunction with the pressure relief system in preventing nuclear system pressure from exceeding the maximum allowable pressure. This same nuclear system high-pressure scram setting also protects the core from exceeding thermal hydraulic limits as a result of pressure increases for some events that occur when the reactor is operating at less than rated power and flow.

3. Reactor vessel low water level--A low water level in the reactor vessel indicates that the reactor is in danger of being inadequately cooled. The effect of a decreasing water level while the reactor is operating at power is to decrease the reactor coolant inlet subcooling. The effect is the same as raising feedwater temperature. Should water level decrease too far, fuel damage could result as steam forms around fuel rods. A reactor scram protects the fuel by reducing the fission-heat generation within the core.

   The reactor vessel low-water-level scram setting was selected to prevent fuel damage following those abnormal operational transients caused by single equipment malfunctions or single operator errors that result in a decreasing reactor vessel water level. Specifically, the scram setting is chosen far enough below normal operational levels to avoid spurious scrams, but high enough above the top of the active fuel to assure that enough water is available to account for evaporation losses and displacements of coolant following the most severe abnormal operational transient involving a level decrease. The selected scram setting was used in the development of thermal-hydraulic limits, which set operational limits on the thermal power level for various coolant flow rates.

4. Turbine stop valve closure--Closure of the turbine stop valve with the reactor at power can result in a significant addition of positive reactivity to the core as the nuclear system pressure rise collapses steam voids. The turbine stop-valve-closure scram, which initiates a scram earlier than either the Neutron Monitoring System or nuclear system high pressure, is required to provide a satisfactory margin below core thermal hydraulic limits for this category of abnormal operational transients. The scram counteracts the addition of positive reactivity due to pressure by inserting negative reactivity with the control rods. Although the nuclear system high-pressure scram, in conjunction with the pressure relief system, is adequate to preclude overpressurizing the nuclear system, the turbine-stop-valve-closure scram provides additional margin to the nuclear system pressure limit.

The turbine stop valve closure scram setting is selected to provide the earliest positive indication of valve closure. The trip logic was chosen both to identify those situations in which a reactor scram is required for fuel protection and to allow functional testing of this scram function.

5. Turbine control valve fast closure--With the reactor and turbine-generator at power, fast closure of the turbine control valves can result in a significant addition of positive reactivity to the core as nuclear system pressure rises. The turbine-control-valve-fast-closure scram, which initiates a scram earlier than either the Neutron Monitoring System or nuclear system high pressure, is required to provide a satisfactory margin to core thermal-hydraulic limits for this category of abnormal operational transients. The scram counteracts the addition of positive reactivity due to pressure by inserting negative reactivity with the control rods. Although the nuclear system high-pressure scram, in conjunction with the pressure relief system, is adequate to preclude overpressurizing the nuclear system, the turbine control-valve-fast-closure scram provides additional margin to the nuclear system pressure limit.

   The turbine-control-valve-fast-closure scram setting is selected to provide timely indication of control-valve-fast-closure. The trip logic was chosen to identify those situations in which a reactor scram is required for fuel protection.

6. Main steam line isolation--The main-steam-line-isolation scram is provided to limit the release of fission products from the nuclear system. Automatic closure of the main-steam-line isolation valves is initiated upon conditions indicative of a steam line break. Immediate shutdown of the reactor is appropriate in such a situation. The scram initiated by main-steam-line isolation-valve closure anticipates a reactor vessel low-water-level scram. The main-steam-line-isolation scram setting is selected to give the earliest positive indication of isolation valve closure. The trip logic allows functional testing of main-steam-line-isolation trip channels with one steam line isolated.

7. Scram discharge volume high water level--The scram discharge volume receives the water displaced by the motion of the control rod drive pistons during a scram. Should the scram discharge volume fill up with water to the point where insufficient space remains for the water to be displaced should a scram be initiated, control rod movement would be hindered. To prevent this situation, the reactor is scrammed when the water level in the discharge volume attains a value high enough to verify that the volume is filling up, yet low enough to ensure that the remaining capacity in the volume can accommodate a scram.

8. Primary containment high pressure--A high pressure inside the primary containment could indicate a break in the nuclear system process barrier. It is

prudent to scram the reactor in such a situation to minimize the possibility of fuel damage and to reduce the addition of energy from the core to the coolant. The reactor vessel low-water-level scram also acts to scram the reactor for loss-of-coolant accidents. The primary containment high-pressure scram setting is selected to be as low as possible without inducing spurious scrams.

9. Main steam line high radiation--High radiation in the vicinity of the main steam lines could indicate a gross fuel failure in the core. A non-safety related high radiation trip signal results in an isolation and trip of the Mechanical Vacuum Pump only. More information on the trip setting is available in Subsection 7.12, "Process Radiation Monitoring."

10. Deleted.

11. Manual scram--To provide the operator with means to shut down the reactor, pushbuttons are located in the control room; these initiate a scram when actuated by the operator.

12. Mode switch in SHUTDOWN--The mode switch provides appropriate protective functions for the condition in which the reactor is to be operated. The reactor is to be shut down, with all control rods inserted, when the mode switch is in SHUTDOWN.

    To enforce the condition defined for the SHUTDOWN position, placing the mode switch in the SHUTDOWN position initiates a reactor scram. This scram is not considered a protective function because it is not required to protect the fuel or nuclear system process barrier, and it bears no relationship to minimizing the release of radioactive material from any barrier. The scram signal is removed after a short time delay, permitting a scram reset which restores the normal valve lineup in the control rod drive hydraulic system.

7.2.3.7 Mode Switch

A conveniently-located, multiposition, administratively-controlled mode switch is provided to select the necessary scram functions for various plant conditions. In addition to selecting scram functions from the proper sensors, the mode switch provides appropriate bypasses. The mode switch also interlocks such functions as control rod blocks and refueling equipment restrictions, which are not considered here as part of the Reactor Protection System. The switch itself is designed to provide separation between the two trip systems. The mode switch positions and their related scram functions are as follows:

a. SHUTDOWN - Initiates a reactor scram, bypasses main steam line isolation scram, and selects Neutron Monitoring System for low neutron flux level operation.

b. REFUEL - Selects Neutron Monitoring System for low neutron flux level operation (see Subsection 7.5, "Neutron Monitoring System"); bypasses main steam line isolation scram.

c. STARTUP - Selects Neutron Monitoring System scram for low neutron flux level operation (see Subsection 7.5, "Neutron Monitoring System"); bypasses main steam line isolation scram.

d. RUN - Selects Neutron Monitoring System scram for power range operation (see Subsection 7.5, "Neutron Monitoring System").

7.2.3.8 Scram Bypasses

A number of scram bypasses are provided to account for the varying protection requirements depending on reactor conditions and to allow for instrument service during reactor operations. Some bypasses are automatic, others are manual. All manual bypass switches are in the control room under the direct control of the control room operator. If the ability to trip some essential part of the system has been bypassed, this fact is continuously indicated in the control room. Bypassing of the NMS inop trip using the Operate-Calibrate bypass switch (fiber optic bypass switch (FOBS)) shall be under Administrative control to allow functional tests of the NMS to be performed.

Automatic bypass of the scram trips from main steam line isolation is provided when the mode switch is not in RUN.

The bypass allows reactor operations at low power with the main steam lines isolated and the main condenser not in operation. These conditions exist during startups (MODE 2) and certain reactivity tests during refueling (MODE 5).

The scram, initiated by placing the mode switch in SHUTDOWN, is automatically bypassed after a time delay of 2 seconds. The bypass is provided to eliminate a sustained SCRAM and to enable the SCRAM to be reset with the mode switch in SHUTDOWN. An annunciator in the control room indicates the bypassed condition.

An automatic bypass of the turbine control-valve fast-closure scram and turbine stop-valve-closure scram is effected whenever the reactor thermal power (as indicated by turbine first-stage pressure) is less than about 30 percent of its rated value. Closure of these valves from such a low initial power level does not constitute a threat to the integrity of any barrier to the release of radioactive material. Bypasses for the Neutron Monitoring System channels are described in Subsection 7.5, "Neutron Monitoring System." A manual switch located in the control room permits the operator to bypass the scram discharge-volume high-level scram trip if

the mode switch is in SHUTDOWN or REFUEL. This bypass allows the operator to reset the Reactor Protection System, so that the system is restored to its normal configuration while the operator drains the scram discharge volume. In addition to allowing the scram relays to be reset, actuating the bypass actuates the control rod block. Resetting the trip actuator opens the scram discharge volume vent and drain valves.

An annunciator in the control room indicates the bypass condition. The arrangement of bypasses meets safety design basis 8b.

7.2.3.9 Instrumentation

Channels providing inputs to the Reactor Protection System are not used for automatic control of process systems; thus, the operations of protection and process systems are separated. The Reactor Protection System instrumentation is discussed as follows:

a. Neutron Monitoring System instrumentation is described in Subsection 7.5, "Neutron Monitoring System." The IRM and APRM channels are considered part of the Neutron Monitoring System. The Neutron Monitoring System logics are considered part of the Reactor Protection System. There are four Neutron Monitoring System logics associated with each trip system of the Reactor Protection System. Each Reactor Protection System logic receives inputs from two Neutron Monitoring System logics.

   Each Neutron Monitoring System logic receives signals from one IRM channel and one APRM channel. (There are four APRMs which interface with the Reactor Protection System logic through four 2-out-of-4 trip voters. One trip voter provides divisional input into its associated RPS automatic trip logic channel.) The position of the mode switch determines which input signals will affect the output signal from the logic. The arrangement of Neutron Monitoring System logics is such that the failure of any one logic cannot prevent the initiation of a high neutron flux scram.

b. Nuclear system pressure is tapped from the reactor vessel at two separate locations. A pipe from each tap is led outside the primary containment and terminates in the Reactor Building. On Units 2 and 3, two locally mounted, nonindicating pressure transmitters monitor the pressure in each pipe. Cables from these transmitters are routed to the auxiliary instrument room. The two pairs of transmitters are physically separated. Each transmitter provides a high-pressure signal to one channel. The transmitters are arranged so that each pair provides an input to trip system A and trip system B, as shown in Figure 7.2-10. The physical separation and the signal arrangement assure that no single physical event can prevent a scram due to nuclear system high

pressure. On Unit 1, locally mounted pressure switches provide the input to the RPS logic.

c. Reactor vessel low-water-level signals are initiated from differential pressure transmitters which sense the difference between the pressure due to a constant reference column of water and the pressure due to the actual water level in the vessel. The transmitters are arranged in pairs in the same way as the nuclear system high-pressure transmitters (Figure 7.2-10). Two instrument pipelines (one above and one below the water level) attached to taps on the reactor vessel are required for the differential pressure measurement for each pair of transmitters. The two pairs of pipelines terminate outside the primary containment and inside the Reactor Building; they are physically separated from each other and tap off the reactor vessel at widely separated points. The Reactor Protection System pressure transmitters, as well as instruments for other systems, sense pressure and level from these same pipes. The physical separation and signal arrangement assure that no single physical event can prevent a scram due to reactor vessel low water level.

d. Turbine-stop-valve-closure inputs to the Reactor Protection System are from valve stem position switches mounted on the four turbine stop valves. Each of the double-pole, single-throw switches is arranged to open before the valve has closed more than 10 percent from its full-open position, providing the earliest positive indication of closure. Either of the two channels associated with one stop valve can signal valve closure, as shown in Figure 7.2-11. The logic is arranged so that closure of three or more valves initiates scram.

e. Turbine-control-valve-fast-closure inputs to the RPS are from four pressure switches which sense loss of EHC trip fluid pressure. Loss of EHC trip fluid pressure initiates control valve fast closure. One switch is mounted on each of the four control valves such that fast closure from either normal tripping or from hydraulic line failure is detected. Each pressure switch provides a signal to one of the two channels of the RPS, as shown in Figure 7.2-10. The logic is arranged so that operation of any one switch or two switches in the same channel initiates a half scram; and a simultaneous trip in each channel initiates a full reactor scram. Thus, if EHC trip fluid pressure is lost at the control valves, a turbine-control-valve-closure reactor trip signal is initiated.

f. There are eight main steam line isolation channels, two for each main steam line. Each channel senses isolation of the associated main steam line via a valve stem position switch on each isolation valve in the main steam line. The double-pole, single-throw switch on each main steam isolation valve is arranged to open before the valve has closed more than 10 percent from its full-open position providing the earliest indication of isolation. The closure of the valve in a main steam line causes both channels associated with that steam line to signal isolation. Figure 7.2-12 shows the arrangement of main

steam line isolation channels. The main-steam-line isolation-valve-closure scram function is effective only when the reactor mode switch is in RUN. The outputs from the channels are combined in Reactor Protection System logic in such a way that the isolation of three or four main steam lines (closure of one valve in each of three or more main steam lines) causes a scram. Figure 7.2-12 shows the logic arrangement. Wiring of the isolation channels from any one main steam line is physically separated in the same way that wiring to a duplicate sensor or a common process tap is separated. The effects of the logic arrangement and separation provided for the main-steam-line isolation-valve closure scram are as follows:

1. Closure of one valve for test purposes, with one steam line already isolated, without causing a scram due to valve closure,

2. Automatic scram upon isolation of three or more steam lines, and

3. No single failure can prevent an automatic scram required for fuel protection due to main steam line isolation.

g. Scram-discharge-volume high-water-level inputs to the Reactor Protection System are from four nonindicating float switches and four thermal dispersion level switches located in the Reactor Building. Each switch provides an input into one channel (Figure 7.2-10). The switches are arranged in pairs so that no single event will prevent a reactor scram due to scram-discharge-volume high-water level. With the scram setting as listed in Table 7.2-1, a scram is initiated while sufficient capacity remains in the discharge volume to accommodate a scram. Both the amount of water discharged and the volume of air trapped above the free surface during a scram were considered in selecting the trip setting.

h. On Units 2 and 3, primary containment pressure is monitored by four pressure transmitters which are mounted on instrument racks outside the drywell in the Reactor Building. Cables are routed from the transmitters to the auxiliary instrument room. Each transmitter provides an input to one channel (Figure 7.2-10). Pipes that terminate in the secondary containment (Reactor Building) connect the transmitters with the drywell interior. The transmitters are grouped in pairs, physically separated, and electrically connected to the Reactor Protection System, so that no single event will prevent a scram due to primary containment high pressure. On Unit 1, locally mounted pressure switches provide the input to the RPS logic.

i. Main steam line radiation is monitored by two gamma sensitive radiation monitors, which are discussed and evaluated in paragraph 7.12.1, "Main Steam Line Radiation Monitors."

j. Deleted.

k. Deleted.

l. Two turbine first-stage pressure transmitters are provided for each trip system to initiate the automatic bypass of the turbine-control-valve-fast-closure and turbine-stop-valve-closure scrams when the first stage pressure is below some preset fraction of rated pressure. The transmitters are arranged so that no single failure can prevent a turbine-stop-valve-closure scram or turbine-control-valve-fast-closure scram.

m. Channel and logic relays are fast-response, high-reliability relays. All Reactor Protection System relays are selected so that the continuous load will not exceed 50 percent of the continuous duty rating. Component electrical characteristics are selected so that the system response time, from the opening of a sensor contact up to and including the opening of the trip actuator contacts is less than 50 milliseconds. The time requirements for control rod movement are discussed in Subsection 3.4, "Reactivity Control Mechanical Design."

   Sensing elements are equipped with enclosures so that they can withstand conditions that may result from a steam or waterline break long enough to perform satisfactorily.

   Instruments for the Reactor Protection System (RPS) are qualified for the environment in which they are located and conditions to which they will be subjected. All RPS instruments which are located in a harsh environment as defined by the 10 CFR 50.49 Environmental Qualification Program meet the requirements to that program.

   To gain access to those calibration and trip setting controls that are located outside the control room, a cover plate, access plug, or sealing device must be removed by qualified plant personnel before any adjustment in trip settings can be effected.

7.2.3.10 Wiring

Wiring and cables for Reactor Protection System instrumentation are selected to avoid excessive deterioration due to temperature and humidity during the design life of the plant. Cables and connectors used inside the primary containment are designed for continuous operation at an ambient temperature of 150°F and a relative humidity of 99 percent.

Cables required to carry low level signals (currents of less than 1 milliampere or voltages of less than 100 millivolts) are designed and installed to eliminate, insofar

as practical, electrostatic and electromagnetic pickup from power cables and other AC or DC fields. Low level signal cables are routed separately from all power cables.

Wiring for the Reactor Protection System outside the enclosures in the control room is run in rigid metallic conduits used for no other wiring. The wires from duplicate sensors on a common process tap are run in separate conduits. Wires for sensors of different variables in the same Reactor Protection System logic may be run in the same conduit.

The scram pilot-valve solenoids are powered from eight actuator logic circuits--four circuits from trip system A and four from trip system B. The four circuits associated with any one trip system are run in separate conduits. One actuator logic circuit from each trip system may be run in the same conduit; wiring for the two solenoids associated with any one control rod may be run in the same conduit.

7.2.4 Safety Evaluation

The Reactor Protection System is designed to provide timely protection against the onset and consequences of conditions that threaten the integrities of the fuel barrier and the nuclear system process barrier. It is the objective of Section 14.0, "Plant Safety Analysis," to identify and evaluate events that challenge the fuel barrier and nuclear system process barrier. The methods of assessing barrier damage and radioactive material releases, along with the methods by which abnormal events are sought and identified, are presented in that section.

Design procedure has been to detect tentative scram trip settings that are far enough above or below normal operating levels that spurious scrams and operating inconvenience are avoided; it is then verified by analysis that the reactor fuel and nuclear system process barrier are protected as is required by the basic objective. A program is in place to determine the Analytical Limit for RPS process variables obtained by calculation and analysis to set values for scram trip point. The values shall be evaluated to ensure that it has sufficient margin from the design basis safety limit. The scrams initiated by Neutron Monitoring System variables, nuclear system high pressure, turbine stop-valve closure, turbine control-valve fast closure, and reactor vessel low-water level are sufficient to prevent excessive fuel damage following abnormal operational transients. Section 14.0, "Plant Safety Analysis," identifies and evaluates the threats to fuel damage resulting from abnormal operational events. In no case does excessive fuel damage result from abnormal operational transients. The Reactor Protection System meets the timeliness and precision requirements of safety design basis 1.

The evaluation of the scram function provided by the Neutron Monitoring System is presented in the section describing that system.

The scram initiated by nuclear system high pressure, in conjunction with the pressure relief system, is sufficient to prevent damage to the nuclear system process barrier as a result of internal pressure. For turbine-generator trips, the turbine stop-valve-closure scram and turbine control-valve-fast-closure scram provide a greater margin to the maximum allowed nuclear system pressure than would the high pressure scram alone. Section 14.0 identifies and evaluates accidents and abnormal operational events that result in nuclear system pressure increases; in no case does pressure exceed the maximum allowed nuclear system pressure. The Reactor Protection System meets the timeliness and precision requirements of safety design basis 2.

The scrams initiated by the Neutron Monitoring System, main-steam-line isolation-valve closure, and reactor vessel low water level satisfactorily limit the radiological consequences of gross failure of the fuel or nuclear system process barriers. Section 14.0 evaluates gross failures of the fuel and nuclear system process barriers; in no case does the release of radioactive material to the environs exceed the guideline values of published regulations. The Reactor Protection System meets the precision requirements of safety design basis 3.

Because the Reactor Protection System meets the timeliness and precision requirements of safety design bases 1, 2, and 3 (monitoring variables that are true, direct measures of operational conditions), it is concluded that safety design basis 4 is met.

Because the Reactor Protection System meets the precision requirements of safety design bases 1, 2, and 3 using instruments with the characteristics described in Table 7.2-1, it is concluded that safety design basis 5 is met.

Neutron flux (the Neutron Monitoring System variable) is the only essential variable of significant spatial dependence that provides inputs to the Reactor Protection System. The basis for the number and locations of neutron flux detectors is discussed in Subsection 7.5, "Neutron Monitoring System." Because the precision requirements of safety design bases 1, 2, and 3 are met using the Neutron Monitoring System as described, it is concluded that the number of sensors for spatially dependent variables satisfies safety design basis 6.

The items of safety design basis 7 specify the requirements that must be fulfilled for the Reactor Protection System to meet the reliability requirements of safety design bases 1, 2, and 3. It has already been shown in the description of the Reactor Protection System that safety design basis 7f has been met. The other requirements are fulfilled through the combination of logic arrangement, channel redundancy, wiring scheme, physical isolation, power supply redundancy, and

component environmental capabilities. The following discussion evaluates these subjects.

In terms of protection system nomenclature, the Reactor Protection System is a one-out-of-two system used twice (1 of 2 x 2) (Power Range Neutron Monitoring System inputs implement a two-out-of-four logic). Theoretically, its reliability is slightly higher than a two-out-of-three system and slightly lower than a one-out-of-two system. However, since the differences are slight, they can, in a practical sense, be neglected. The advantage of the dual trip system arrangement is that it can be tested thoroughly during reactor operation without causing a scram. This capability for a thorough testing program, which contributes significantly to increased reliability, is not possible for a one-out-of-two system.

The use of independent channels allows the system to sustain any channel failure without preventing other sensors monitoring the same variable from initiating a scram. A single sensor or channel failure will cause a single trip system trip and actuate alarms that identify the trip. The failure of two or more sensors or channels would cause either a single trip system trip, if the failures were confined to one trip system, or a reactor scram, if the failures occurred in different trip systems. Any intentional bypass, maintenance operation, calibration operation, or test, all of which result in a single trip system trip, leaves at least two channels per monitored variable capable of initiating a scram by causing a trip of the remaining trip system. The resistance to spurious scrams contributes to plant safety, because unnecessary cycling of the reactor through its operating modes would increase the probability of error or actual failure. It is concluded from the preceding paragraphs evaluating the logic, redundancy, and failure characteristics of the Reactor Protection System that the system satisfies the reliability requirement stated in safety design bases 7a and 7b.

Any actual condition in which an essential monitored variable exceeds its scram trip point is sensed by at least two independent channels in each trip system. Because only one channel must trip in each trip system to initiate a scram, the arrangement of two channels per monitored variable per trip system provides assurance that a scram will occur as any monitored variable exceeds its scram setting.

Each control rod is controlled as an individual unit. A failure of the controls for one rod would not affect other rods. The backup scram valves provide a second method of venting the air pressure from the scram valves, even if either scram pilot-valve solenoid for any control rod fails to deenergize when a scram is required. It is concluded from the evaluations in the above paragraphs that the Reactor Protection System meets safety design basis 7c.

Sensors, channels, and logics of the Reactor Protection System are not used directly for automatic control of process systems. Therefore, failure in the controls

and instrumentation of process systems cannot induce failure of any portion of the protection system. This meets safety design basis 7d.

Failure of either Reactor Protection System motor generator set would result, at worst, in a single-trip-system trip. Alternate power is available to the Reactor Protection System buses. A complete, sustained loss of electrical power to both motor-generator sets results in eventual loss of RPS instrumentation power, as delayed by the motor-generator set flywheel inertia. Loss of RPS instrumentation power initiates MSIV closure, which results in a reactor scram. This meets safety design basis 7e.

The environmental conditions in which the instruments and equipment of the Reactor Protection System must operate were considered in their design and installation. The instruments environmental requirements are based on the worst-expected environmental conditions in which the instruments must operate. All Reactor Protection System equipment that is in a harsh environment as established by the 10 CFR 50.49 Environmental Qualification Program meets the requirements of that program. The Reactor Protection System components, which are located inside the primary containment and which must function in the environment resulting from a break of the nuclear system process barrier inside the primary containment, are the condensing chambers and the inboard MSIV RPS limit switches. Special precautions are taken to ensure satisfactory operability after the accident. The condensing chambers are similar to those that have successfully undergone qualification testing in connection with other projects, and the limit switches are environmentally qualified.

The environmental capabilities of the Reactor Protection System components, combined with the previously described physical and electrical isolation of sensors and channels, satisfy safety design basis 7g.

Safe shutdown of the reactor during earthquake ground motion is assured by design of the system as a Class I system (see Appendix C) and the fail-safe characteristics of the system. The system only fails in a direction that causes a reactor scram when subjected to extremes of vibration and shock. This meets safety design basis 7h.

Calibration and test controls for the Neutron Monitoring System are located in the control room and are, because of their physical location, under the direct physical control of the control room operator. Calibration and test controls for pressure switches, level switches, and valve position switches are located on the switches themselves. These switches are located in the Turbine Building, Reactor Building, and primary containment. Electronic switches associated with RPS transmitters are located in the Control Building Auxiliary Instrument Room. To gain access to the setting controls on each switch, a cover plate or sealing device must be removed. The control room operator is responsible for granting access to the setting controls

to properly qualified plant personnel for the purpose of testing or calibration adjustments. This meets safety design basis 8a.

It has been shown in the description of the Reactor Protection System that safety design bases 8b, 9, 10a, and 10b are satisfied.

The following section covering inspection and testing of the Reactor Protection System demonstrates that safety design basis 11 is satisfied.

7.2.5 Inspection and Testing

7.2.5.1 General

The Reactor Protection System can be tested during reactor operation by five separate tests. The first of these is the manual trip actuator test. By depressing the manual scram button for one trip system, the manual logic actuators are deenergized, opening contacts in the actuator logics. After resetting the first trip system, the second trip system is tripped with the other manual scram button. The total test verifies the ability to deenergize all eight groups of button switches. Scram group indicator lights verify that the actuator contacts have opened.

The second test is the automatic actuator test, which is accomplished by operating (one at a time) the administratively-controlled test switches for each automatic logic. The switch deenergizes the actuators for that logic, causing the associated actuator contacts to open. The test verifies the ability of each logic to deenergize the actuator logics associated with the parent trip system.

The third test includes calibration of the Neutron Monitoring System. Subsection 7.5, "Neutron Monitoring System," describes the calibration procedure.

The fourth test is the single rod scram test, which verifies the capability of each rod to scram. It is accomplished by operation of toggle switches on the protection system operations panel. Timing traces can be made for each rod scrammed. Prior to the test, a physics review must be conducted to assure that the rod pattern during scram testing does not create a rod of excessive reactivity worth.

The fifth test involves the application of a test signal to each Reactor Protection System channel, in turn, and observing that a logic trip results. This test also verifies the electrical independence of the channel circuitry. The test signals can be applied to the process-type sensing instruments (pressure and differential pressure) through calibration taps. This test is performed in accordance with approved written procedures.

Reactor Protection System response times are first verified during preoperational testing and may be verified thereafter by similar tests. The elapsed times from sensor trip to each of the following events is measured:

a. Channel relay deenergized, and

b. Actuators deenergized.

The alarm typewriter provided with the process computer verifies the proper operation of many sensors during plant startups and shutdowns. Main-steam-line isolation valve position switches and turbine-stop-valve position switches can be checked in this manner. The verification provided by the alarm typewriter is not considered in the selection of test and calibration frequencies and is not required for plant safety.

The provisions for functionally testing and calibrating the Reactor Protection System meet the requirements of safety design basis 11.

Technical Specification Section 3.3.1.1 provides the technical specification associated testing requirements for the Reactor Protection System which typically includes periodic channel checks, channel functional tests, channel calibrations, and logic system functional tests. The technical specification bases provides additional details for specific surveillance requirements.

Channel functional tests verify actuation of the trip output relays or trip channels. Additionally, the associated surveillance procedures verify operation of expected alarms. Channel calibrations for pressure or level sensing instrumentation utilize standard pressure sources or calibrated water columns as the calibration reference.

7.2.5.2 Seismic Test and Analysis Results

GENERAL

NOTE: The subject topic of this section is related to the NRC Unresolved Safety Issue A-46 Program and the Seismic Analysis Program, both of which are addressed in Appendix C.