7.1 INTRODUCTION

The Plant systems are instrumented to provide information on Plant conditions at selected locations, to protect equipment and personnel from undesirable conditions, and to control the Plant during start-up, operation, and shutdown. The principal control station for the Plant is in the control room.

The Plant will be started up and shut down by manual control. In the power range, the operator will maintain manual control of reactivity at all times. Annunciation, indication and recording will alert the operator and provide data on Plant conditions.

Major portions of the instrumentation and controls essential to Plant safety (Class 1E and safety related as discussed in Section 8.1) are located in the control room. The instrumentation is arranged in groups on the control boards so that when corrective action is required, all pertinent indicators, recorders and controllers are within easy reach of the operator. The control board consists of a control console and duplex vertical panels. Visible alarms with audible signals, located on the super-structure over the main control board, annunciate and identify abnormal operating conditions. A telephone system provides both intraplant and external communication. The control room is kept at a controlled temperature which is well within the design ambient temperature requirements of the instruments (Reference Section 6.10, Control Room Habitability).

All instrumentation and control equipment is made from highly reliable components. Environmental and seismic qualification of the instrumentation have been the subject of various reports (see Subsections 8.1.3, 8.1.4 and Class 1E classification in Section 5.2).

The protection instrumentation consists of independent multiple channels to ensure system flexibility while maintaining Plant safety at all times. A highly reliable source (Class 1E as discussed in Section 8.1) of electrical power is provided to ensure safe and reliable Plant operation.

The reactor operates within limits as a result of its inherent characteristics, the instrumentation and controls, the reactivity controls, and by operational procedures and administrative controls. Potential departures from these limits are audibly and visibly annunciated in the control room. A Reactor Protective System designed to protect the core initiates reactor trips.

This chapter describes safety-related as well as major nonsafety-related instrumentation and controls for systems described in other chapters. Special nonsafety-related instrumentation systems such as radiation monitoring, leak detection, fire detection and meteorological instrumentation are outlined in other chapters.

7.2 REACTOR PROTECTIVE SYSTEM

7.2.1 GENERAL

The Reactor Protective System (RPS) is a Class 1E system (with the exception of the clutch power supplies) and is comprised of the sensor instrumentation, amplifiers, trip units, logic circuits, actuation circuits and other equipment as required to monitor selected nuclear steam supply system conditions, and is designed to reliably effect a rapid reactor shutdown (scram) if any one or combination of conditions deviates from a preselected operating range. The system functions to protect the reactor core.

The RPS controls are housed in four cabinets in the control room. The cabinets consist of the following components:

Four (4) Trip-Inhibit Switch Panel Assemblies

Four (4) Trip-Unit Assemblies (One for each channel A,B,C,D)

Twenty Eight (28) Bistable Trip Units (Seven in each channel)

Sixteen (16) Auxiliary Trip Units (Four in each channel)

Four (4) RPS Power Supply Assemblies

Four (4) Clutch Power Supply Assemblies

Four (4) RPS Bin Assemblies

Four (4) Trip Unit Interconnection Modules

One (1) Rod Drop Test Panel

Four (4) Auxiliary Logic Module Assemblies

Four (4) RPS Test Panel Modules

The following components are also part of the RPS cabinets and are part of the nuclear instrumentation described in Section 7.6:

Two (2) Nuclear Instrument Source/Wide Range Drawer Assemblies

Four (4) Power Range Safety Drawer Assemblies

One (1) Comparator Averager Assembly

Finally, a set of annunciators (non-class 1E) are also located on the above cabinets for operator convenience. An extension of the RPS is housed in an additional panel, also in the control room. This panel contains:

Four (4) Thermal Margin Monitors

Four (4) Reactor Power Calibration and Indication Assemblies

Another panel in the control room (C12) contains:

Four (4) pressure switch alarms (dual output each, one for PORV logic, one for ATWS logic)

7.2.2 DESIGN BASES

The RPS is designed under the following bases to assure adequate protection for the reactor core:

1. Instrumentation and controls for this Plant conform to the provisions of the General Design Criteria as indicated in Section 5.1 and to IEEE 279-1971.

2. No single component failure will prevent safety action.

3. Four independent measurement channels complete with sensors, sensor power supply units, amplifiers and trip units are provided for each safety parameter with the exception of loss of load and rate trips.

4. The channels are provided with a high degree of independence by separate connection of the sensors to the process systems and of the channels to preferred power supply buses. Separate raceways are used to ensure independence from cable faults.

5. The four normal measurement channels provide trip signals to four independent trip paths.

6. A trip signal from any two-out-of-four protective channels causes a reactor trip.

7. When one of the four channels is taken out of service for maintenance, the protective system logic can be changed to a two-out-of-three coincidence for a reactor trip by bypassing the removed channel. If the bypass is not effected, the out-of-service channel assumes a tripped condition, which results in a one-out-of-three channel logic.

8. The protective system ac power is supplied from four separate buses.

9. Open circuit, or loss of power supply of the channel logic, initiates an alarm and a channel trip.

10. All measurement channels and trip logic matrices assume the nonconducting state to provide a tripping function.

11. The RPS can be tested during reactor operation and when shut down.

12. The manual trip is totally independent of the automatic trip system.

13. Trip signals are preceded by alarms to alert the operator to undesirable operating conditions in cases where the operator could avert a reactor trip.

14. The RPS components are independent from the control channels.

15. Zero power mode bypass and low power nuclear channels bypass interlocks are provided with the same independence and single failures protection design as the trip circuits.

16. A diverse reactor trip to satisfy the 10CFR50.62 ATWS (Anticipated Transient Without SCRAM) rule was installed in 1990 (Reference 14). This trip uses a 2/4 pressurizer high pressure trip which is set higher than the normal pressurizer high trip. When one of the four signals of the ATWS trip is physically removed for maintenance, or any other reason, the protective system logic becomes 2/3.

The high pressurizer pressure trip modules are set up to trip at 2375 $\pm$25 psia. This makes it secondary to the RPS trips which actuate at 2255 $\pm$22 psia. Pressurizer safety relief valves are set at 2500, 2540, and 2580 psia. The set points for the modules were specifically chosen to avoid overlap with either RPS trips or safety relief valves.

This modification was approved by the NRC by SER on December 5, 1989. It also covers diverse circuitry for both turbine trip and initiation of an auxiliary feedwater pump.

As shown in Figures 7-1 and 7-2, the RPS consists of four trip paths operating through coincidence logic to maintain power to, or remove it from, the control rod drive (CRD) clutches. Four independent measurement channels normally monitor each safety parameter. Individual channel trips occur when the measurement reaches a preselected value. A typical measurement channel functional diagram is shown in Figure 7-3. The channel trips are combined in multiple two-out-of-four logic. Each two-out-of-four logic system provides trip signals to one-out-of-six logic units, each of which causes a direct trip of the contactors in the ac supply to the CRD clutch power supplies. The common sides of the clutch power supplies are ungrounded.

Reactor trip is accomplished by de-energizing the magnetic clutch holding coils and releasing the full-length control rods to drop into the core. The four partial-length control rods are not equipped with magnetic clutches and are described in Chapter 3.

7.2.3 REACTOR PROTECTIVE SYSTEM ACTIONS

Rapid reactor shutdown is effected on the following conditions:

7.2.3.1 High Rate-of-Change of Power

A reactor trip for high rate-of-change of reactor power (neutron flux) is provided to protect the reactor against an uncontrolled control rod withdrawal while the core is critical but at very low power levels.

The rate-of-change of power is normally monitored at startup by two source range indications of the source/wide range nuclear instrumentation as discussed in Section 7.6.2.2.

A reactor trip is initiated if the rate-of-change of reactor power exceeds 2.6 decades per minute (dpm), over a range of about 10^{-4}% to 15% full power, by either of the two wide-range portions of the source/wide range nuclear instrumentation channels. The trip signal is automatically bypassed below 10^{-4}% and above 15% full power. Alarms for high rate-of-change of power are initiated at 1.5 dpm over the operating range of 10^{-4}% to 15% full power. {In addition, manual rod withdrawal prohibit (between approximately 10^{-4}% and 15% full power from the two wide-range channels) prevents all regulating rods from being withdrawn, but does not prevent insertion.}

Above 15% power the high rate-of-change of power trip unit is switched by the 15% bistable in the power range safety channels to perform Axial Shape Index (ASI) alarm functions. This function is derived in the thermal margin monitor using maximum selected power (Q_2) from either ΔT power (B) or calorimetric nuclear power (ϕ). As shown in Figure 7-7, the maximum power (Q_2) is used to determine a set point which is then compared with axial offset (Y) (see Subsection 7.2.3.5) to generate an alarm. The ASI alarm is applicable for positive as well as negative values and indicates that an axial offset administrative limit has been breached. The ASI alarm is used to monitor and protect the reactor from axial power distributions outside analyzed limits.

7.2.3.2 Variable High Power

A reactor trip using a variable high power (VHP) trip of the thermal margin monitors is provided to shut down the reactor when the indicated neutron power or thermal power (maximum selected) exceeds a predetermined value. This trip is available at full or part loop operation and is independent of power level or pump configuration. The high power trip signals are initiated by two-out-of-four coincidence logic from the four thermal margin monitors. During normal full power Plant operation with all coolant pumps operating, reactor trips are initiated when the reactor core power level exceeds a nominal value of 106.5% of indicated full power; this trip level represents a reactor power of no greater than 113.4% of full power when instrument and calorimetric errors are taken into account. Provisions are made in the thermal margin monitor to select VHP set points for three primary coolant pump operation.

The variable high power function is enabled at approximately 30% power with the variable trip set point set at 15% (Reference 15). Each increase of power level requires reset action of all four thermal margin monitor VHPT functions prior to the trip set point for continued escalation up to a maximum of 106.5% power. The maximum allowable value of the VHPT is defined in the Technical Specifications as 109.4% of Rated Thermal Power. Upon power descension, the VHP trips and pretrips automatically decrease maintaining the predetermined set point margins. The pretrip alarms provide annunciation in addition to rod withdrawal prohibit signals. A block diagram of VHP is illustrated in Figure 7-7.

The neutron flux at the excore detectors for a given reactor power level is affected by control rod position, radial core power distribution, and average coolant temperature. These effects are compensated for by performing periodic Plant heat balances and adjusting the calibration of the power range channels accordingly. Between secondary heat balances, an alarm has been added for operator convenience which indicates when power based on steam generator ΔT measurement is different than that based upon neutron monitoring by greater than a predetermined amount. The difference between the PCS hot and cold leg temperatures is compared to a power range safety channel output. This difference is displayed on a meter relay for each channel, and the difference alarmed when it exceeds a preset adjustable value. The alarm incorporates a time delay of up to eighteen seconds to dampen the effect of PCS flow oscillation on PCS elements. The meter relays and the associated calibration controls are located on the front of the reactor power calibration cabinet panel in the control room. The thermal power (B) is calculated in each of the four thermal margin monitors.

The thermal power signal (B) is then sent to the power comparator unit where it is subtracted from the nuclear power signal received from a power range safety channel. This difference may be either positive or negative and is sent to an indicating meter relay. The meter relay is equipped with adjustable high- and low-set points. When the absolute value of the deviation signal reaches the set point, an alarm is sounded on the Reactor Protective System alarm panel and a light is lit adjacent to the meter relay.

Periodic calibration of the system can be performed using a secondary Plant heat balance to determine actual reactor power. The nuclear power calibrate potentiometers and thermal margin monitor adjustable constants for ΔT power will be used to adjust these outputs to agree with the secondary Plant heat balance.

7.2.3.3 Low Primary Coolant Flow

A reactor trip is provided to protect the core from a power to flow mismatch. There are four primary coolant pumps, with flow in each measured by sensing differential pressure between the coolant pump suction line and the primary coolant input line to the associated steam generator. The flow measurement signals are provided by summing the output of the differential pressure transmitters to provide an indication of total coolant flow through the reactor. A reactor trip is initiated by two-out-of-four coincidence logic from either of the four independent measuring channels when the flow function falls below a preselected value.

Provisions are made in the Reactor Protective System to permit operation at reduced power if one pump is taken out of service. For this mode of operation, the low flow trip points are changed manually at the RPS bistable trip units to the allowable values for the selected pump condition, thus providing a positive means of assuring that the more restrictive settings are used.

Pretrip alarms provide indication of degrading coolant flow prior to the four pump trip set point, or three pump trip set point.

A key-operated bypass switch ("Zero Power Mode Bypass" switch, see Subsection 7.2.5.2) allows this trip to be bypassed for subcritical testing of control rod drive mechanisms. The trip bypass is automatically reset above 10^{-4}% full power.

7.2.3.4 High Pressurizer Pressure

A reactor trip for high pressurizer pressure is provided to prevent excessive blowdown of the Primary Coolant System by relief action through the safety valves.

The trip signals are provided by four narrow range independent pressure transducers measuring the pressurizer pressure. A typical channel diagram is shown on Figure 7-3.

A reactor trip is initiated by two-out-of-four coincidence logic from the four independent measuring channels if the pressurizer pressure exceeds a preset pressure ($\leq$ 2,255 psia). A diverse reactor trip was added in 1990 to provide a two out of four coincidence pressurizer high pressure trip from four independent measuring channels if the pressurizer pressure exceeds a preset pressure (>2375 psia). See Figures 7-4 and 7-5. Since no credit is taken for the relief capacity of the primary coolant power-operated relief valves in Chapter 14, the Plant operates with these valves isolated due to leakage problems.

Pretrip alarms are initiated if the pressurizer pressure exceeds a preset pressure (2,205 psia).

7.2.3.5 Thermal Margin/Low Pressure

A reactor trip is initiated by a continuously computed function of core power, reactor coolant maximum inlet temperature, core coolant system pressure and axial shape index to prevent reactor conditions from violating a minimum departure from nucleate boiling ratio (DNBR).

$P_{Var} = \lambda Q_{DNB} + \beta T_{IN} + \gamma$

Where: λ, β and γ are constants, T_{IN} is measured reactor inlet temperature, and

$Q_{DNB} = QR_1 * QA$

Where:

QA = F (Y)
Y = Axial Offset
QR_1 = F (Q_1)
Q_1 = Max (ϕ or B)
B = ΔT Power
ϕ = Adjusted Nuclear Power

Figure 7-7 is a simplified functional diagram of this system. The signal representing core power (Q_1) is the auctioneered highest of the neutron flux power (ϕ) and the ΔT power (B) signal. This signal is used to calculate QR_1. The measured axial shape index signal (Y), which includes the adjustment for shape annealing and represents the peripheral axial shape index, is used to calculate QA. The QA, QR_1 and constant λ are multiplied together to generate a signal representing the first term in the P_{Var} equation.

The signal (T_{Cal}) representing reactor coolant inlet temperature (T_{IN}) is the highest measured cold leg temperature (T_C). The second term in the P_{Var} equation is then the product of constant β and T_{Cal}. The third term is constant γ. These three terms are summed to produce P_{Var}. This limit is then compared to a fixed low pressure trip limit (P_{Min}). The auctioneered highest of these signals (P_{Var} and P_{Min}) becomes the trip limit (P_{Trip}). P_{Trip} is compared to the measured reactor coolant pressure and a trip signal is generated in the RPS trip unit when P is less than or equal to P_{Trip}. A pretrip alarm is also generated when P is less than or equal to the pretrip setting $P_{Trip} + \Delta P$.

The logic shown in Figure 7-7 is for Channel A. There are three other functionally identical channels; B, C and D. The output of the TM/LP trip unit bistable is connected to the Reactor Protective System as shown on Figure 7-2.

A key-operated bypass switch ("Zero Power Mode Bypass" switch, see Subsection 7.2.5.2) allows this trip to be bypassed at low power level. The trip bypass is automatically reset above 10^{-4}% full power.

7.2.3.6 Loss of Load

A reactor trip will automatically be initiated after a turbine trip occurs. A turbine low auto stop oil condition occurs with all types of turbine trips. The reactor trip will be initiated when the turbine auto stop oil pressure decreases, causing contacts in the auto stop oil pressure switches to close and, via two out of three logic, energize two turbine trip auxiliary relays (see Figure 7-14, Sheet 2).

Each relay will provide a reactor trip signal to two of four protective system channels.

The loss of load reactor trip is an anticipatory trip which is not required to protect the reactor since the primary trip is high primary system pressure. As such, its measuring channels components are not required to be Class 1E and its circuits need not meet IEEE 279-1971. This trip is automatically bypassed when three of four power range safety channels indicate power is below 17% full power (see Subsection 7.2.5.2).

Isolation of Nonclass 1E turbine trip circuits from the Class 1E Reactor Protective System is provided by the turbine trip relays (see Subsection 7.2.9).

7.2.3.7 Low Steam Generator Water Level

Low steam generator downcomer water levels will cause a loss-of-heat-removal capability from the Primary Coolant System.

A reactor trip signal is initiated by two-out-of-four logic from four independent downcomer level differential pressure transmitters on each steam generator. A 25.9% narrow range minimum trip setting assures that the heat transfer surface (tubes) are covered with water when the reactor is critical. The 25.9% level corresponds to the location of the feed ring. Pretrip alarms are actuated to provide for annunciation of approach to reactor trip conditions.

7.2.3.8 Low Steam Generator Pressure

A reactor trip on low steam generator secondary pressure is provided to protect against excessively high steam flow caused by a steam line break. The trip set point is $\geq$ 500 psia.

An abnormally high main steam flow from either steam generator will cause the secondary pressure to drop rapidly.

Four pressure transmitters on each steam generator actuate trip units which are connected in a two-out-of-four logic to initiate the reactor protective action if the steam generator pressure drops below a preselected value. Signals from two of the four indicating meter relays from either steam generator will close the main steam isolation valves on both steam generators. Pretrip alarms are also provided.

A key-operated bypass switch ("Zero Power Mode Bypass" switch, see Subsection 7.2.5.2) allows the reactor trip to be bypassed. This trip bypass is automatically reset above 10^{-4}% full power.

7.2.3.9 Containment High Pressure

A reactor trip is initiated on high containment pressure.

Four independent pressure switches actuate trip units which are connected in a two-out-of-four coincidence logic to initiate the reactor protective action when the containment pressure reaches 3.7 psig.

This reactor trip is in addition to the thermal margin/low-pressure trip to ensure that the reactor is tripped before the safety injection and containment spray are initiated (see Subsection 7.3.3.2).

Containment high-pressure circuitry related to the RPS does not involve any pretrip actions. A pretrip alarm of 0.9 psig is initiated through containment pressure indications in the control room.

7.2.3.10 Manual Trip

A manual reactor trip is provided to permit the operators to trip the reactor (see Figure 7-1). Manual actuation of either of two independent reactor trip push-button switches in the main control room causes direct interruption of the ac power to the dc power supplies feeding the CRDM electromagnetic clutches.

One manual trip push button interrupts the control power to the holding coils of four contactors whose contacts break ac power to the clutch power supplies. The second push button interrupts power to the undervoltage coils of two circuit breakers which disconnect all ac power to the clutch power supplies. This system ensures diverse means of trip actuation.

7.2.4 SIGNAL GENERATION

Four instrument channels are used to generate the signals necessary to initiate the automatic reactor trip action except for the loss of load and high neutron flux rate-of-change trips where one and two measuring channels, respectively, are used. The signal cable routing and readout drawer locations in the RPS cabinets are separated and isolated to provide channel independence.

1. The high rate-of-change of neutron flux signals is generated by the two wide-range measuring channels (Figure 7-8) which monitor the flux from source level to 200% of full power. These channels receive signals from flux monitors in the biological shield around the reactor (refer to Section 7.6 for details).

2. The high neutron flux signals are supplied by four linear flux measuring channels (Figure 7-9) covering the flux range from 0% to 125% full power. These channels receive signals from ion chambers which monitor the full length of the core and are located in the biological shield around the reactor (refer to Section 7.6 for details).

3. The primary coolant pressure, flow, thermal margin, steam generator pressure and water level, and containment pressure trips are each actuated from signals generated by separate sets of sensors. The primary coolant pressure is measured in the pressurizer, flow is measured by monitoring the pressure difference across the steam generators, thermal measurements are taken from the reactor inlet and outlet piping in each loop and combined with primary coolant pressure, axial shape and power to determine thermal margin, steam generator water level and pressure are monitored in each steam generator, and containment pressure is obtained via appropriate pressure sensors (refer to Section 7.6 for details).

4. The electronic sensors (transmitters) are located in the air room inside containment with physical separation provided between each channel. The output of each transmitter is an ungrounded current loop (see typical loop, Figure 7-3) supplying signal receivers and trip units.

5. The trip units have three isolated outputs which feed the logic matrices. Additional outputs feed the pretrip alarm, the trip alarm, the SOE Node and the critical function multiplexor (see Subsection 7.6.2.5). Provisions are also made for test inputs to the trip units for normal protective system testing and are described in Subsection 7.2.6. The protective system outputs referred to here are connected into logic matrices as shown in Figure 7-2.

7.2.5 LOGIC OPERATION

7.2.5.1 Trip Logic (See Figure 7-2)

The instrument channels which supply protective action, operate channel trip units in the corresponding channel cabinet of the Reactor Protective System; each unit includes three electromagnetically actuated relays and associated contacts. Four units are actuated for each trip condition, eg, high primary coolant pressure. The relays in each unit are numbered one, two and three. Each relay has a single-pole, double-throw (SPDT) contact. The normally open contacts of the No l relays in the Channels A and B trip units are connected into a two-out-of-two logic ladder matrix. (The normally open contacts are used for the logic ladders so that the relays are energized and the contacts closed under operating conditions.) The respective No 2 and No 3 relay contacts are similarly connected into separate logic ladder matrices. With the Channels C and D trip units arranged in a similar manner, there are a total of six independent matrices. These logic ladders are designated the AB, AC, AD, BC, BD and CD logic trips.

The output of each logic ladder is a logic trip set of four electromagnetically actuated relays. Each relay in these sets has an SPDT contact. The contacts from one relay of the set from each logic ladder output are placed in series with corresponding contacts from the remaining sets in each of the four trip paths. Each of these paths is the power supply line to a power trip relay which interrupts the power to the CRDM clutches. De-energizing of any one power trip relay interrupts (opens) one trip path and effects a one half trip. De-energizing any set of logic trip relays (which results from trip action of any two channels through a ladder matrix) causes an interruption of all trip paths and a full trip.

The functions of Reactor Protective System Relays Kl, K2, K3 and K4 shown on Figure 7-1 are listed in Table 7-1.

7.2.5.2 Trip Bypass Logic

Four different types of trip bypasses (or inhibits), as discussed below, are used in the Reactor Protective System. An annunciator indicates the presence of any trip bypass.

Testing Bypass - The first of these bypasses ("Test Bypass") is used when it is desired to physically remove an individual trip unit from the system, or when calibration or servicing of a trip channel could cause an inadvertent trip. A key lock bypass switch is located above each trip unit. The key cannot be removed in the bypass position. Each trip bypass (high power, low pressure, etc) has a different lock cylinder combination; however, corresponding trips in each of the four protective channels have the same cylinder combination. Since only one key for each type trip is provided, an operator cannot bypass more than one channel at a time. Duplication of keys is prevented by using "ACE" type round key locks. Turning the key lock switch closes three separate contacts in parallel with the three normally open trip contacts of the trip unit. A light above the bypass switch indicates that the trip channel has been bypassed.

During the bypass condition, the system logic reverts from 2/4 channels required for trip to 2/3 channels required for trip. The Reactor Protective System continues to provide protective function in the event of a single failure in one of the unbypassed channels.

Nuclear Channel Bypass - The second type of trip bypass ("Nuclear Channel Bypass") is an automatic bypass. This is used in two cases where a bypass is required during start-up or shutdown. The high rate-of-change of power signal is bypassed when the reactor power is below 10^{-4}% of full power or above 13% of full power. The Technical Specifications require that the loss-of-load trip be bypassed during reactor start-up when power is below 17% of full power. This requirement is conservatively implemented in plant operating procedures with the loss-of-load trip being bypassed when power is less than 15%. Bypassing is automatically accomplished by contacts operated from the wide range portion of a nuclear instrumentation channel for the high rate-of-change of power bypass at 10^{-4}% full power and by contacts from the power range safety channel for the loss-of-load bypass when power is below 15% full power. When power level is such that a bypass is required, contacts in parallel with the trip contact to the input of the high rate-of-change of power and the loss-of-load auxiliary trip units prevent reactor trip. The bypasses are arranged so that a given power range channel bypasses the corresponding rate-of-change power trip channel above 13% of full power, removes the bypass for loss of load above 17% of full power and enables the local power density alarm function of the rate-of-change auxiliary trip unit (K25 relays on Figure 7-10). A single wide range section of a nuclear instrumentation source/wide range channel feeds two rate-of-change of power level bypass circuits, each bypass circuit in turn bypasses a single rate-of-change of power trip channel (K26 relays on Figure 7-10). Removal of a power range safety channel or a wide range channel results in removal of the bypasses associated with that channel.

Zero Power Mode Bypass - The third type of trip bypass ("Zero Power Mode Bypass") is required when the Plant is shut down to permit maintenance or shutdown operation. This bypass is manually initiated when it is desired to raise the control rods for control rod drop testing or to assure a reserve shutdown margin during low power testing.

This bypass is effective for the following trips: low flow, low pressure SG No 1 and 2, and TM/low pressure.

This bypass is automatically removed by contacts operated from the wide-range logarithmic nuclear instrumentation channel when reactor power increases above 10^{-4}% full power; each wide-range logarithmic channel resets two RPS trip channels.

Four key lock switches, one located in each cabinet, control the initiation of the bypass. Each switch controls the initiation of the bypass for that cabinet. All four switches must be turned to make the bypass fully effective. This method of initiating the bypass was selected because four bypass switches, one in each protective channel cabinet of the Reactor Protective System, allow for complete channel separation as required by IEEE 279-1971.

Operation of a given bypass switch is shown in Figure 7-11. The bypass switch applies +15 V to an integrated circuit that drives the trip relays in the trip unit. The trip unit will remain in the untripped condition, regardless of the input signal level, as long as the +15 V is applied to the integrated circuit. Normally open contacts in series with the bypass switch allow auto bypass removal. Operation of the pretrip alarms is unaffected by the bypass switch.

ATWS System Bypass - The fourth type of trip bypass (ATWS system high pressurizer pressure trip) is necessary to permit maintenance on the ATWS trip system. This bypass is manually initiated from the control room via key switch HS-0102D on panel C12. The alarm for this bypass annunciates on the C06 panel.

7.2.5.3 CRDM Clutch Power Circuitry (See Figure 7-1)

The CRDM clutches are separated into two groups. The clutches in each group are supplied in parallel with low-voltage dc power by an ungrounded feed line. Two ac to dc converters supply each feed line so that one converter being cut off does not cause release of the clutches. The converters on each side are each supplied by a line from a preferred ac bus to assure a continued source of power. Each line passes through two interrupters (each actuated by a separate trip path) in series so that, although both ac lines must be de-energized to release the clutches, there are two separate means of interrupting each line. This arrangement provides means for the testing of the protective system including Relays Kl, K2, K3 and K4.

7.2.6 TESTING

Provisions are made for testing of the Reactor Protective System while the reactor is at operating power levels or when shut down. These tests cover the trip paths from sensor, to the output to the final CRDM clutches. The testing system is completely isolated from the protective system circuitry itself. Failure of any part of the testing system does not prevent proper operation of the trip circuitry. The system test does not prevent the protection function.

In response to Generic Letter 83-28 regarding the ATWS events at Salem Nuclear Power Plant, seven Safety Evaluation Reports (SERs) were written in response to inputs regarding testing of the RPS. The SERs concluded that the Palisades' design meets the requirements of Generic Letter 83-28.

Isolation of the testing circuitry is accomplished with an isolated test power supply and double coil relays. One coil is normally used in the protective system circuitry and the other coil is used in the testing system circuit. The double coil relays permit system testing without bypassing or inhibiting protective functions. Depending on the relay action required, the coil in the testing circuit, which is used to provide a magnetic flux in the relay core, aids or bucks the magnetic flux produced by the coil in the circuit of the protection system. This feature allows all trip test switches to be located in the circuitry of the test system, thus providing complete isolation of the two systems.

During reactor operation, the measuring channels are checked by comparing the outputs of similar channels and cross-checking with related measurements. The trip units are tested by inserting a voltmeter in the circuit, noting the signal level, and initiating a test input which is also indicated on the voltmeter. This provides the necessary overlap in the testing process and also enables the test to establish that the trip can be effected within the required tolerances. The test signal is provided to the trip unit signal input circuit by an internal test signal generator which is incorporated in the test features of the RPS power supply. With the test signal generator functioning, a trip unit is selected for test and the test signal is increased or decreased (depending upon the type of trip unit) by depressing the manual test switch. The test circuit permits various rates-of-change of the signal tested by the coarse and fine adjustments of the test signal generator. Trip action (opening) of each of the trip unit relays is indicated by individual lights on the front of the trip unit. The pretrip alarm action is indicated by a separate light.

The sets of logic trip relays at the output of each coincidence logic matrix are tested one at a time. The test circuits in the logic permit only one pair of coincidence matrix logic relays to be tripped while one set of matrix output relays can be held at the same time; the application of hold power to one set of matrix output relays denies the power source to the other sets. In testing a logic trip set, eg, AB, a holding current is initiated in the test coils of the logic trip relays by turning the matrix relay trip test switch to "off" and depressing the matrix logic AB test push-button switch. Operation of the matrix trip test switch de-energizes a parallel pair of trip unit relays. With the ladder-logic relay contacts open, the logic trip relays may be de-energized one at a time (by rotating the matrix-relay-trip test switch) to initiate a half-trip. Indicator lights on the trip unit relay coils and on the dc power supply ac feed lines provide verification that coil operation and half-trip conditions have occurred.

The capability to test the RPS Relays Kl through K4 associated with the RPS "trip/reset" function has been provided as described in Subsection 7.2.5.3. The nuclear channel bypass relays (K25 and K26), and their contacts described in Subsections 7.2.5.2, 7.6.2.2 and Figure 7-10, can be tested with the reactor at power. The K25 and K26 relay can be tested as part of the normal Reactor Protective System tests by varying the wide-range logarithmic channel output above and below 10^{-4}% full power and the power range safety channel output above and below 15% full power. In order to verify the loss-of-load trip function (see Subsection 7.2.3.6), the manual turbine trip button can be used to energize the turbine trip relays while the unit is shut down.

7.2.7 EFFECTS OF FAILURES

The Reactor Protective System is designed and arranged to perform its function with single failures. Some of the faults and their effects are described below. The word "ungrounded" is used in several of the faults. Ungrounded is taken to mean that adequate impedance exists between the signal common and earth ground such that a single short from the signal common to the earth ground would result in a change in signal level which is within the tolerances of the loop accuracy analysis or would result in a change in signal level that does not render the circuit incapable of performing its safety function.

Analog portion:

1. A loss of signal in a channel initiates channel trip action for all trips except high rate-of-change of power, high-power level and high-pressurizer pressure. Although high-pressurizer pressure will not trip, the loss of signal will cause a thermal margin/low-pressure trip.

2. Shorting of the signal leads to each other, has the same effect as a loss of signal. Shorting the leads to an ungrounded voltage source, has no effect since the signal circuit is ungrounded.

3. Single grounds on the signal circuit have no effect. Double grounds would tend to cause the channel to fail in the safe direction.

4. Open circuit of the signal leads has the same effect as a loss of signal.

5a. TMM VHPT function will cause a VHPT trip when power removed from TMM.

Logic portion:

5b. Inadvertent operation of the relay contacts in the matrices can be identified by the indicating lights.

6. Shorting of the pairs of contacts in the matrices prevents the trip relay sets from being released. Such shorts are detectable in the testing process by observing that the trip relay sets cannot be dropped out. Testing is accomplished by successive opening of the matrix pairs.

7. Shorting of the matrices to an external voltage has no effect since the matrix is ungrounded. The testing process will indicate accidental application of potential to the matrix.

8. The logic matrices will each be supplied by two power sources. Single loss of power source has no effect. Loss of power to a logic matrix initiates a trip condition.

9. Failure of a trip relay set to actuate has no effect since there are six sets in series in the trip action and any one initiating trip action will cause the action to be completed.

10. The failure of one power trip relay in the power supply circuit has no effect since either of the two relays in series will provide the necessary action.

11. Single grounds in the power trip relay circuits have no effect since the circuit is ungrounded by a local isolating transformer. Local ground detectors also indicate should an accidental ground occur. Double grounds would cause the circuits to fail in the safe direction.

12. The ac circuit supplying power to the clutch power supplies is fed from an isolation transformer with a center tap grounded through a resistance to assure that single grounds will not prevent system action. The circuit has a local ground detection system. The supply transformer center tap ground is used in a ground detection system to identify local ground and shorts around the power trip relay contacts when the relays are de-energized.

13. The dc clutch power supply circuits operate ungrounded so that single grounds have no effect. The clutches are supplied in two groups by separate pairs of power supplies to further reduce the possibility of clutches being improperly held. The clutch impedances and load requirements are such that the application of any other local available voltage will not prevent clutch release, eg, connection of the clutch supply circuit to the battery distribution circuit would cause the distribution circuit fuse to blow due to excessive current drain. Connection to a 115 volt ac circuit would have similar effects. Connection to available low-voltage dc, such as the nuclear instrumentation power supplies, would have no effect since these power supplies have insufficient capacity to supply the load.

Diversity of Trip Functions

Several Reactor Protective System functions back each other up for tripping the reactor. An example is high pressurizer pressure and thermal margin/ low-pressure trips.

Because the Technical Specifications permit operation with only two operable channels (if one of the inoperable channels is tripped), there are several scenarios in which the high-pressure trip could fail. The most simple of these is to fail the 125v DC bus which is assumed to be common to the two preferred AC buses that feed the remaining channels. Alternatively, assuming one of the four Reactor Protective System channels is bypassed but not tripped (operating in a two-out-of-three logic arrangement for reactor trip) and assuming the single failure of one 125v DC bus causes failure of two preferred AC buses that are needed to generate two high-pressure trip signals, the high pressurizer pressure reactor trip would not occur if required. However, the failure of two pressurizer pressure channels would also cause a thermal margin/low-pressure trip and thus protection of the reactor would still be maintained.

Other diversity features are described in Reference 1 and protect against common mode failures affecting similar components. In addition to the RPS diversities described in Reference 1 a diverse reactor trip based on pressurizer high pressure 2 out of 4 logic was added during the 1990 refueling outage as part of the ATWS rule (10CFR50.62).

7.2.8 POWER SOURCES

The power for the Reactor Protective System is supplied from four separate independent preferred ac buses. Each preferred bus is supplied from the battery system through an inverter to assure an uninterrupted, transient-free source of power (refer to Section 8.4).

Each preferred bus also has provision for connection to an instrument ac bus to permit servicing of the inverters.

The distribution circuits to the preferred buses are provided with circuit protective devices to assure that individual circuit faults are isolated.

For additional information on power sources for the Reactor Protective System, see Chapter 8.

7.2.9 PHYSICAL SEPARATION AND ELECTRICAL ISOLATION

7.2.9.1 Physical Separation

The sensors for the Reactor Protective System are located in the air room inside the containment building and physically separated to assure channel separation. The air room permits access to the sensors while the Plant is at power. The process transmitters located inside the containment, which are required for short-term operation following a design basis accident (DBA), are rated and have been tested under simulated DBA conditions (see Subsection 6.1.3.2) and have been tested for the safe shutdown earthquake (see Section 5.7). The routing of cables from these transmitters is arranged so that the cables are separated from each other and from power cabling to reduce the danger of common event failures. This includes separation at the containment penetration areas. More detail on cable installation is discussed in Section 8.5. In the control room, the four nuclear instrumentation and protective system trip channels are located in individual compartments. Mechanical and thermal barriers between these compartments reduce the possibility of common event failure and meet the intent of IEEE 384-1977 for interfaces with nonsafety-related systems as detailed in the following subsection.

7.2.9.2 Electrical Isolation

This subsection evaluates the adequacy of the Reactor Protective System electrical isolation from interfacing nonsafety-related systems. Such interfaces are intended to meet IEEE 384-1977 and 10 CFR 50 Appendix A, General Design Criterion 24, "Separation of Protection and Control Systems."

RPS interfaces are outlined in Figure 7-12. The Plant Process Computer (PPC) SOE Node inputs are located in the cable spreading room (see Subsection 7.6.2.5). The CFMS input cabinets and the PPC SPI Node are located in the main control room area (see Subsections 7.6.2.5 and 7.6.2.3, respectively). Other RPS outputs to nonsafety-related circuits (meters, recorders) go to control boards in the main control room (see Subsection 7.6.2). Four basic types of isolation devices are used for isolation: optical isolators, thermistors/Zener diodes, operational amplifiers and resistors.

1. Analog RPS Outputs to SOE Node

Isolation for the RPS analog signals to the SOE Node is achieved by 100 kohm resistors in the analog signal circuits. See Figure 7-12 for analog signals involved.

The isolation method is considered adequate because:

a. There are four channels for each of the analog signals. If an isolation device fails and takes out one channel, the RPS will still operate properly on two-out-of-three logic.

b. All the analog signals interfacing with the SOE Node are on Channel A. Therefore, it is highly unlikely that the SOE Node could cause interchannel failures by tying two different channels together to completely eliminate the voting logic and thus inhibit a signal from reaching the RPS.

c. Each channel's power supply bus is alarmed to indicate if a problem exists on a particular channel so that it can be isolated and analyzed.

2. Digital RPS Outputs to PPC SOE Node

Isolation for the RPS digital signals to the SOE Node is achieved by individual relay contacts in the RPS which is an acceptable form of isolation.

3. Analog RPS Outputs to PPC SPI Node

The neutron flux start-up rate of change of power is fed to the PPC SPI Node via an operational amplifier as isolation buffer. The operational amplifier includes common mode rejection and fused output for protection against high voltage or excessive load. As such, it is considered adequate as an isolation device.

Analog outputs to the PPC SPI Node use 100 kohm resistors as an isolation device. Engineering analyses, conducted in accordance with IEEE 384-1977, show that these resistors are adequate to protect the RPS from any short circuit, open circuit and application of the maximum voltage present on the nonsafety-related side of the resistors. As such, these resistors are qualified as isolation devices.

4. Analog RPS Outputs to Critical Function Multiplexor

The upper and lower power range neutron flux signals are fed to the Critical Function Multiplexor via an operational amplifier as an isolation buffer. The operational amplifier is the same device as described in the above section. This signal is also isolated at the Critical Function Multiplexor input at the signal termination isolation cabinets which have qualified isolation devices per IEEE 384-1977.

5. Other RPS Outputs

Circuits other than those identified on Figure 7-12 (and other than the Critical Function Multiplexor) go to remote meters and auxiliary circuits from the power range safety channels and are isolated by operational amplifiers with 10 kohm resistors at the inverting and noninverting inputs.

7.2.10 REACTOR TRIP AND PRETRIP SET POINTS

The Reactor Protective System trip set points are provided in the Technical Specifications; pretrip set points are determined by operating experience and are controlled administratively.

7.3 ENGINEERED SAFEGUARDS CONTROLS

7.3.1 INTRODUCTION

The engineered safeguards controls consist of equipment to monitor and select the available power sources and to initiate operation of certain load groups, and will initiate containment isolation when required. The system is designed on a two-independent-channel basis with each channel capable of initiating the safeguards equipment load groups to meet the minimum requirements to safely shut down the reactor and provide all functions necessary to operate the system associated with the Plant's capability to cope with abnormal events. The system is provided with the necessary redundant circuitry and physical isolation so that a single failure within the system will not prevent the proper system action when required in accordance with IEEE 279-1971 and 10 CFR 50, Appendix A, General Design Criteria 22 and 24. The control equipment is designed to withstand seismic loads described in Section 5.7 and is designed for Class 1E service. The system is provided with test facilities and alarms to alert the operator when certain components trip or malfunction or are not available or operable. The controls are interlocked to automatically provide the sequence of operations required to initiate engineered safeguards system operation with or without offsite power.

Certain critical parameters have four sensors utilizing a two-out-of-four logic to provide reliable operation with a minimum of spurious activations. Initiation level settings and their bases are provided in the Technical Specifications. The four sensors are physically isolated and operation of any two out of four will initiate the appropriate engineered safeguards action. This action is provided by combining the four sensors into relay matrices which provide dual-channel initiation signals. Actuation Channel A has all odd numbered relays. Channel B has all even numbered relays. Channel A receives its power from preferred ac Panel Y10; Channel B from Panel Y20 (see Section 8.3). Instruments Channel C has odd numbered devices and Instruments Channel D has even numbered devices. Channel C receives its power from preferred ac power Panel Y30; Channel D from Panel Y40. Physical separation between channels is maintained in the control panels to meet the intent of IEEE 384-1977 by locating devices in individual groups and providing barriers between groups. The cables for the two groups of channels (A/C and B/D) are run in separate raceways (see Section 8.5 for odd/even, left/right channels separation criteria).

Testing of major portions of the engineered safeguards control circuits is accomplished while the Plant is at power. More extensive circuit sequence and load testing may be done with the reactor shut down. The test circuits are designed to test the redundant circuits separately so that the correct operation of each circuit may be verified by either equipment operation or by sequence lights. The test circuit design is such that, should an accident occur while testing is in progress, the test will not interfere with initiation of the safeguards equipment required.

7.3.2 SAFETY INJECTION SYSTEM CONTROL CIRCUITS AND EQUIPMENT INITIATION

7.3.2.1 Design Basis

The control system is designed to automatically initiate the necessary engineered safeguards equipment upon a safety injection signal (SIS) with or without offsite power available. To assure reliability, the control system is designed on a two-channel concept with each channel initiating the operation of separate and redundant engineered safeguards load groups. The control system will function at all times and will operate in any mode of reactor operation.

7.3.2.2 Description and Operation

Description - The Safety Injection System logic is shown on Figure 7-13 and control schematics are shown on Figures 7-15 through 7-23.

Two independent and isolated circuits each initiate operation of redundant engineered safeguards equipment. These control circuits monitor whether offsite and/or emergency power is available and select load groups in accordance with the available power supply.

The safety injection signal is derived from pressurizer low-low pressure or containment high pressure. The pressurizer low-low pressure signal is derived from four pressure sensors installed on the pressurizer. Each sensor supplies a pressurizer pressure signal to a pressure indicator/alarm instrument (Figure 7-15). Each pressure instrument is connected to a latching-type auxiliary relay. The containment pressure signal is derived from four containment pressure sensors. Each containment pressure sensor is connected to a latching-type auxiliary relay. One pressure sensor and associated pressure instrument, as well as one containment pressure sensor, are supplied from each of the four preferred ac sources.

Either two out of four pressurizer low-low pressure or two out of four containment high-pressure signals initiate the SIS signal which, in turn, actuates two safety injection control circuits, each of which is supplied by a separate preferred ac source.

Within each control circuit, relays are provided to initiate redundant devices so that individual relay failure will not cause a complete circuit failure. Actuation of each safety injection control circuit can be performed manually via a safety injection initiate push button, one push button for each safety injection circuit. The SIS relay logic circuits control the loading sequence in duplicate control circuits. Failure of the control power on any one redundant circuit will be annunciated in the control room.

Containment spray activation requires the containment high-pressure signal to ensure the containment is sprayed only when needed (see Subsection 7.3.3).

If an SIS is accompanied by a loss of offsite power, the load sequencers will be initiated. There are two of these sequencers with each connected to a separate control circuit. The sequencers load the required equipment in sequence on the emergency generators so as to not exceed the emergency generators' capacity (see Section 8.4).

Operation - These circuits are safeguards circuits and operate only during shutdown or accident conditions. They have no function while the Plant is under normal operation. The shutdown sequence will vary depending on the presence or absence of an SIS signal and offsite power availability.

Shutdown Upon a Reactor Trip With Offsite Power Available - If no SIS condition exists at the time of the reactor trip, all auxiliary equipment will continue to operate from the offsite power source. Plant shutdown will be performed as necessary by the operator.

Shutdown Upon a Reactor Trip Without Offsite Power - Upon loss of offsite power during normal operation, each emergency generator will be started through its own separate control circuit. The emergency generator start is dependent upon undervoltage on the engineered safeguard buses (see Section 8.6). The bus loads will be shed by the pre-diesel load shedding relays. When the pre-diesel load shed relays have operated and the emergency generator voltage reaches a preset value, the buses will then be energized from the emergency generators. The sequencers will be energized to automatically start required normal shutdown equipment.

Safety Injection With Offsite Power Available - If offsite power is available at the time of initiation of the SIS, the SIS relays will initiate the simultaneous start of the engineered safeguards equipment.

Safety Injection Without Offsite Power - If offsite power fails, all loads will be shed at the time the diesel generators receive an automatic start signal. With load shedding completed, the diesel generator breakers will close automatically when generator voltage approaches a normal operating value. Closing of the breakers will reset the load shedding signals and start the sequencers. The sequencers will initiate operation of the engineered safeguards equipment required for design basis accident response.

Safety Injection System Block During Normal Shutdown - In order to avoid initiating operation of SIS equipment when the Primary Coolant System is depressurized, the SIS circuits must be blocked. Blocking is manual and is effective only when three of the four pressurizer pressure sensors are between the low-pressure and the low-low-pressure set points.

After the Primary Coolant System is placed back in service and the pressurizer pressure is restored to normal, the safety injection circuit block will be automatically reset when two or more of the four pressurizer pressure sensors detect normal operating pressure.

Testing - The availability of the control circuits may be tested at any time. Testing of these circuits will initiate the safeguards equipment unless their operation would adversely affect the normal Plant operation. A test sequence light indicator is provided to show that the initiating signal has energized the control circuit of the specific engineered safeguards equipment where either operation is not desirable during the test or equipment is already in operation. See Subsection 7.3.5 for further details on testing of the SIS.

7.3.2.3 Design Analysis

Reliability of the Safety Injection System control circuits is assured by redundant and diverse circuits, each initiating operation of redundant load groups. Diversity of initiation is provided by using two physically independent and diverse parameters (pressurizer and containment pressure) sensing an LOCA to activate SIS. Failure of control power to any one of the pressurizer low-pressure or containment high-pressure circuits will cause the circuit to fail in an SIS initiation signal mode. Failure of control power on any one redundant circuit will be annunciated.

7.3.3 CONTAINMENT HIGH PRESSURE AND HIGH RADIATION

7.3.3.1 Design Basis

The containment isolation control system is designed to isolate the containment upon occurrence of either containment high pressure or containment high radiation. The Containment Spray System is initiated upon containment high-pressure signal. The system is also designed to prevent inadvertent opening of the containment isolation valves.

The control system is designed on a two-channel concept with redundancy and physical separation. Each channel is capable of initiating containment isolation and operation of certain engineered safeguards.

7.3.3.2 Description and Operation

Description - The containment high-pressure and radiation control logic is shown on Figures 7-24, 7-25 and typical schematics on Figures 7-26 through 7-29.

One containment radiation monitor is located adjacent to each containment air cooler where radioiodines would condense along with water vapor in the event of relatively minor breaches of primary system integrity. Radiation monitor locations in the lower level of containment also allow for response from abnormal sump or 590-foot level water accumulations of radioactive coolant. Such conditions could be hypothesized for rupture of a letdown line after cooling by the letdown heat exchanger, leakage or overflow of the primary system drain tank, etc. In order to ensure ability to isolate containment on the premise that significant core damage might occur without loss of coolant, the location of two of the radiation monitors is also in the direct path of radiation emanating from abnormal concentrations of fission products passing through the letdown heat exchanger.

The sensors for containment pressure are located in the auxiliary building next to the containment building and in separate rooms to ensure channel separation.

Refer to Chapter 8, Subsection 8.1.3 for details of environment qualifications for the containment isolation instrumentation channels.

The controls consist of two independent and isolated groups of circuits. The four radiation sensors and four pressure sensors are each connected to an auxiliary relay. Four separate control circuits each consisting of one pressure and one radiation level sensor and their two auxiliary relays are connected to separate preferred ac buses. There are two separate initiation circuits which consist of two-out-of-four logic matrices and necessary auxiliary relays.

The containment isolation valves operate from the 125 volt dc source and are normally energized. It requires two high-radiation or two high-pressure signals to close the isolation valves. This prevents spurious signals from causing containment isolation.

Refueling accident high-radiation monitors are also provided in each of the two initiation circuits. These initiation circuits function on a one-out-of-two trip logic. Key switches are provided to lock in the monitors during refueling operations.

Operation - Coincident two-out-of-four high-radiation or two-out-of-four high-containment pressure signals from the auxiliary relays will trigger an alarm in the main control room, close all containment isolation valves not required for engineered safeguards except the component cooling line valves which are closed only by containment high pressure, and will isolate the control room ventilation system (see Section 9.8). High radiation detected by the refueling accident high-radiation monitors will also close all containment isolation valves not required for engineered safeguards when locked in by the respective refueling monitor key switches.

Coincident two-out-of-four high-radiation or two-out-of-four high-containment pressure signals from the auxiliary relays locks in the high-pressure and high-radiation circuits, respectively.

In order to deisolate the containment, the high-pressure and high-radiation circuits must be manually reset. At least three out of four pressure sensors must sense normal pressure, three out of four radiation sensors must sense normal radiation level or the refueling accident high-radiation monitors (when locked in) must sense normal radiation level before the operator can reset the pressure isolation circuits or the radiation isolation circuits. In accordance with NUREG-0578/0737, resetting the isolation circuits will not result in automatically opening the containment isolation valves; the operator must manually reopen each valve by placing each valve's hand switch from the "Open" position to the "Close" position and back to the "Open" position again. Resetting containment high-pressure will result in the component cooling line valves to reopen.

Containment high-pressure signal will initiate SIS, and start containment spray.

Containment high-pressure signal will also initiate a reactor trip with a two-out-of-four logic. This trip is in addition to the thermal margin/low-pressure trip (see Subsection 7.2.3.5) to ensure that the reactor is tripped before SIS and containment spray is initiated.

Containment high-pressure (CHP) signal will initiate closure of the main steam isolation valves to reduce the inventory blowdown from the intact steam generator in the case of a main steam line break, reducing the peak containment pressure and temperature as required in the accident analysis. CHP also closes the main and bypass feedwater regulating valves (Modification FC-906-1990). See Subsection 7.5.1.3.

Testing - The containment high-pressure detectors and auxiliary relays can be tested at power without actuating containment isolation by tripping one out of the four local pressure switches. Actuation of the auxiliary relay is annunciated in the control room. The detectors and auxiliary relays for containment high radiation are tested at power by using an internal test feature of the radiation monitor.

Testing the containment isolation circuits is done only during shutdown. RO-12, “Containment High Pressure (CHP) and Spray System Tests,” functionally tests the CHP circuitry. Pressure is applied to two of the CHP pressure switches to simulate containment high pressure. All twelve 2/4 combinations (six left channel and six right channel) are tested separately. For the first test on each channel, proper operation is verified by verifying the following:

Containment Isolation Signal	-	Annunciator Lit
Containment Isolation	-	Valves Close
SIS Signal	-	Voltage Signal
Containment Spray System	-	Valves Open and Pumps Receive Start Signal
Control Room Ventilation	-	CR Air Filter Fans Start

The remaining five tests on each channel are performed in the same manner. However, only one component from each CHP relay is verified to operate properly. Actuation of containment isolation from the high-radiation channels is done by actuating the monitor by a radiation source thereby causing an actuation of the system. SIS is not actuated during this test. One of two redundant switches located in the control room, turned to test position, may be operated at a time to de-energize two of the four containment high-pressure channels which will cause containment isolation, initiate SIS, close feedwater regulating valves and start the containment spray pumps. The spray valves will not open in test position; if spray valves are not both closed fully, the spray pumps cannot be started in test position. The containment spray valves can be manually opened by means of their individual hand switches located in the control room. This second necessary manual operation to initiate the spray system will prevent inadvertent spraying inside containment with borated water.

Further information on testing of the above circuits is provided in Subsection 7.3.5.

7.3.3.3 Design Analysis

Reliability is assured by the redundancy and diversity in the initiating control circuits, in the design of the individual isolation valve control circuits and in the Containment Spray System and air cooler system control circuits.

The containment isolation signal receives diverse inputs from containment high-pressure and containment high-radiation signals. Diversity is ensured by the amount and location of containment radiation monitors ensuring effectiveness toward containment isolation in all postulated accident modes. This effectiveness has been verified by actual testing for the case of core damage assuming 1% failed fuel without LOCA (see Reference 2).

The containment isolation valves are closed following an isolation signal such that deliberate operator action is required to reopen the penetration (NUREG-0578, Paragraph 2.1.4).

The containment isolation signal is not received by essential systems. Essential systems are those critical to the immediate mitigation of any event that results in automatic containment isolation. Essential systems provide Primary Coolant System inventory and pressure control, reactivity control, core cooling, secondary heat sink, containment cooling (depressurization) and safe shutdown. Essential systems must be available in response to accident parameters without operator action and, therefore, should not be automatically isolated as part of the Containment Isolation System.

The essential systems are (Chapters 6, 9 and 10):

High-Pressure Safety Injection

Low-Pressure Safety Injection

Containment Spray (including recirculation)

Containment Critical Service Water

Charging

Auxiliary Feedwater

Main Steam

Note that main steam isolation will occur on containment high pressure or steam generator low pressure (see Subsection 7.2.3.8) based on containment pressurization considerations for a steam line break.

Nonessential systems receive the containment isolation signal, with two exceptions: instrument air and main feedwater. In both of these cases, isolation is affected in a way which is functionally equivalent to automatic containment isolation. Instrument air is at a higher pressure than containment pressure under LOCA conditions. Both instrument air and main feedwater have check valves prior to entering containment. Note that component cooling water provides cooling for primary coolant pump seals and isolates on containment high pressure only. Although not part of the isolation system, the feedwater regulating valves will also close on CHP due to a 1990 modification.

Failure in control source power to the pressure/radiation sensor relay circuit or to the redundant initiating circuit causes the circuit to fail in a mode to initiate isolation. Loss of control power will be annunciated in the control room, but isolation will not be effected unless a second failure occurs. Failure of source power to the control circuit of any isolation valve or failure of the pilot valve solenoid of an isolation valve will cause that isolation valve to close.

7.3.4 SAFETY INJECTION AND REFUELING WATER TANK LOW LEVEL

7.3.4.1 Design Basis

The SIRW tank low-level control system (recirculation actuation system (RAS)) is designed to transfer the suction of the safety injection and containment spray pumps to the containment sump when the SIRW tank is essentially empty, and to perform the functions required to recirculate and cool the water which has accumulated in the containment building sump, for post-accident cooling of the core. In the recirculation mode, it automatically provides component cooling water to the shell side of the shutdown cooling heat exchangers. The circuit is designed on a two-channel concept in accordance with IEEE 279-1971 with each channel initiating the operation of separate and redundant hydraulic loops.

7.3.4.2 Description and Operation

Description - The SIRW tank level control logic is shown on Figure 7-30 and typical schematics are shown on Figures 7-26, 7-31 and 7-32.

The SIRW tank is provided with four level switches to detect low level with each connected to an auxiliary relay from separate preferred ac supplies.

A separate circuit is provided for control of the safety injection recirculation valves associated with one recirculation loop consistent with the two-channel concept. In addition, each circuit controls the operation of:

- the component cooling water valves to each of the component cooling water heat exchangers,
- the service water valve for service water from each of the component cooling water heat exchangers, and
- tripping the low pressure safety injection pumps.
- throttling the containment spray valves CV-3001 and CV-3002.

A separate circuit is provided for the opening enable of the high pressure safety injection subcooling valve (CV-3071) and closing enable of the spray header isolation valve (CV-3001), if containment sump valve (CV-3030) does not open.

Operation - The low-level control circuits have no normal or shutdown cooling operating function and will operate only after the SIRW tank has been essentially emptied. Coincident one-out-of-two (taken twice) low-level signals will automatically initiate the necessary valve operations to permit operation of the two recirculation loops and trip both low-pressure safety injection pumps to protect the pumps from low suction pressure. A manual bypass is provided so that the low-pressure safety injection pumps may be restarted if the operators deem this necessary for long-term core cooling.

A key switch is provided for each of the low-level control circuits. The switch contacts are in parallel with the SIRW tank low-level contacts, such that the minimum LPSI pump recirculation valves CV-3027 and CV-3056 may be closed without having low level in the SIRW tank. This operation is annunciated. The valves will not close if their control switch is in the "Open" position.

Testing - The RAS control circuit may be tested while the Plant is shut down. This test will initiate the operation of the valves and the trip signal of both LP safety injection pumps.

The test may be initiated by the test switches provided in the control room, simulating level switch actuation, or may be initiated by actuating the level switches mounted at the SIRW tank. Operation of one of the two redundant three-position test switches on the control panel will de-energize two level switch auxiliary relay circuits and provide a one-out-of-two (taken twice) low-level signal which will initiate operation of the valves. This circuit will be maintained (sealed in) until the test switch is moved to the reset position. Releasing the test switch from reset will conclude the test and valve operators will return to the normal positions.

In addition, the valve operation may be manually tested individually with valve control switches.

Further information on SIRW tank low-level control circuits testing can be found in Subsection 7.3.5.

7.3.4.3 Design Analysis

Reliability of the low-level control (recirculation actuation system (RAS)) is assured by redundant control circuits, each controlling a redundant recirculation loop and cooling system valves. Each of the redundant control circuits is supplied from a separate preferred ac source. Failure of the power source in any one of the level switch circuits will cause the circuit to fail in a mode to initiate recirculation. Manual activation is also available from the control room using pump and valve control switches. Override of the RAS is annunciated.

7.3.5 ENGINEERED SAFEGUARDS TESTING

7.3.5.1 Design Bases

The engineered safeguards testing features, method and program meet 10 CFR 50, Appendix A, General Design Criterion 37; NRC Branch Technical Position ICSB 25; Regulatory Guide 1.22; and Standard Review Plan (NUREG-75/087).

Response time testing of engineered safeguards is consistent with the requirements of 10 CFR 50, Appendix A, General Design Criterion 21; Section 3.9 of IEEE 279-1971; and IEEE 338-1977.

The engineered safeguard functional testing program also demonstrates the full-functional operability and independence of the onsite power sources (see Section 8.4) and is performed during shutdown. This testing program simulates loss of offsite power in conjunction with a simulated safety injection actuation signal and simulates interruption and subsequent reconnection of onsite power sources. Steps are included to verify the proper operation of the load-shed system, load-shed bypass when the emergency diesel generators are supplying power to their respective buses and that there is no adverse interaction between the onsite and offsite power sources.

7.3.5.2 Testing Description

The details of the testing program, methods and acceptance criteria are provided in Appendix 7A.

7.4 OTHER SAFETY RELATED PROTECTION, CONTROL AND DISPLAY SYSTEMS

While the Reactor Protective System protects against reactor core damage and the engineered safeguards controls protect against a loss of coolant incident, other safety related (Class 1E service) control and instrumentation systems ensure a safe shutdown of the Plant, protection of primary coolant fluid boundaries, mitigation of anticipated events such as loss of feedwater and uncontrolled release of radioactive effluents. In addition, Plant parameters critical to safety are monitored with Class 1E instruments to ensure the operator can act in a timely fashion during abnormal conditions.

7.4.1 REACTOR SHUTDOWN CONTROLS

Refer to Section 7.7.4 and the Fire Safety Analyses (Section 9.6.3) for information concerning reactor shutdown controls.

7.4.2 PRIMARY COOLANT BOUNDARIES PROTECTION

Leak detection from the Primary Coolant System is described in Chapter 4 and is considered as nonsafety related. The primary coolant safety valves are the protective devices with coolant at normal pressure. The following identifies and describes the safety related control and instrumentation provided to protect primary coolant fluid system boundaries during off-normal anticipated condition.

7.4.2.1 Primary Coolant Overpressure Protection System

1. Design Bases

   Without a low temperature overpressure protection system, pressure transients in the Primary Coolant System initiated while operating at low temperatures are not protected against and there are no pressure relief devices to prevent these transients from exceeding the Technical Specifications limits as required by 10 CFR 50, Appendix G pressure-temperature limits. The reactor has a pressure limit in excess of 2,500 psia above 430°F, but has a much lower limit at 200°F (see Technical Specifications limit in LCO 3.4.3). The code safety valves with settings in the 2,500 psia range would not be able to relieve a pressure transient at low Primary Coolant System temperature without the limits of the Technical Specifications being violated.

The Technical Specifications pressure limit drops off rapidly at lower temperatures because the reactor vessel material and welds have significantly less toughness at lower temperatures and are therefore more susceptible to flaw-induced failure. In addition, factors such as copper content in welds and neutron fluence levels affect the material toughness and contribute to the reduction in safety margin to vessel failure at low temperature conditions.

The Primary Coolant System Low temperature overpressurization subsystem (LTOP) has been designed to provide automatic pressure relief of the Primary Coolant System at temperatures lower than 430°F. This is not a set point, set points are defined in Figure 4-15. An exemption from the requirements of 10CFR50.60 has been granted by the NRC such that in determining the setpoint for LTOP events, the ASME Section III, Appendix G curves for P/T limits are not exceeded by more than 10% (Reference 17). The current LTOP setpoint limit curve incorporates the 10% factor. New P/T limit curves were generated using the latest ASME Code methodology which does not include the 10% allowance (Reference 20). The new P/T curves were not instituted, but instead the existing P/T limit curves were compared to the new curves and it was determined that adequate margin exists, such that the existing curves can continue to be used through the period of extended operation.

In order to prevent overpressurization of the Shutdown Cooling System, the LTOP will be placed in service whenever this system is not isolated from the Primary Coolant System. This additional requirement precludes conditions that could lead to a loss of coolant incident outside containment as identified in Regulatory Guide 1.139.

It is also noted that, following a loss of offsite power, which is an anticipated operational occurrence (AOO), "feed and bleed" mode of Primary Coolant System operation may be used to remove decay heat from the reactor. In order to satisfy the basic requirements for safety equipment used in mitigation of AOOs, the OPS mechanical components, valves, etc, are CP Co Design Class 1.

2. Design Description

Two redundant and separate overpressurization protection channels are provided. Each channel consists of a CP Co Design Class 1 power-operated relief valve (PORV), a CP Co Design Class l PORV isolation (block) valve, valve actuators, position indications, a Class 1E primary coolant narrow range pressure sensor, and related instrumentation and controls. Pressure relief is accomplished by the automatic opening of the power-operated relief valves. Each PORV has sufficient capacity to protect the Primary Coolant System from overpressurization at lower temperatures. Limiting transients that each PORV is capable of handling are: (1) the start of an idle primary

coolant pump when secondary water in the steam generator is up to 100°F hotter than the Primary Coolant System cold leg temperatures; and (2) the start of an HPSI pump when the system is in the water solid condition.

Each pressure relief valve is blocked by an individual block valve. The PORVs are solenoid operated and designed to fail closed, while the block valves are motor operated (fail as is). Direct indication of PORV position is provided in the control room using acoustic sensors. The block valves, controlled by hand switches in the control room are also provided with a direct valve position indication. The PORVs block valves are closed in normal operation. The pressurizer safety valves are provided with similar acoustic sensors for direct valve position indication in the control room.

Power for the PORVs and their respective block valves is supplied by Class 1E MCC-1 for one channel and Class 1E MCC-2 for the other. All valves may be operated with either offsite or onsite power. The initiation channels are fed from redundant preferred ac power sources.

Three annunciators are provided for interface of the system with the operator. The first annunciator advises the operator of five conditions:

1. PCS temperature of 460°F with PORV block valves closed as a signal to arm the system

2. Loss of control power

3. Microprocessor failure

4. Inputs out of range

5. LTOP/SDC switch failure

The second signals an approaching high-pressure condition. The third annunciator advises the operator that PCS pressure has exceeded the trip setpoint as shown on Figure 4-15 and the PORVs should have opened.

A separate key-operated switch, concurrently with a switch opening the associated block valve, is provided for arming each channel. Indicator lights in each channel have been provided on the control room panel to inform the operator that (1) the block valves are open (white light), (2) the system is in the SDC mode (amber light), and (3) the overpressurization system has been activated (red light).

Testing - Refer to the Plant Technical Specifications.

3. Design Evaluation

The Primary Coolant System overpressure protection subsystem design meets the following requirements:

a. Operator Action - No credit is taken for operator action until 10 minutes after the operator is aware, through an activation alarm, that a pressure transient is in progress.

b. Single Failure Criterion - The primary coolant overpressure protection system is designed to protect the reactor vessel given a single failure in addition to the event that initiated the pressure transient. The power-operated relief valves and their associated block valves are powered from Class 1E 480 volt buses to allow emergency power for these valves.

c. Testability - The system is tested on a periodic basis per Technical Specifications.

d. Seismic and IEEE 279 Criteria - The electrical and instrumentation equipment meets IEEE 279-1971 criteria. The system is not vulnerable to a failure mode that would both initiate a pressure transient and disable the overpressure mitigating system. Such events as loss of instrument air and loss of offsite power have been considered.

e. Environment Qualification - The narrow range primary coolant pressure channels equipment is qualified to IEEE 323 including post-LOCA environment for equipment inside containment.

f. Operator Interfaces - The electrical instrumentation and control system provides a variety of alarms to alert the operator to (1) properly enable the low temperature overpressure protection system at the proper temperature during cooldown, (2) indicate if a pressure transient is occurring, and (3) indicate system problems due to loss of control power, microprocessor failure, inputs out of range and LTOP/SDC switch failure.

g. Interlocks - Additionally, the electrical system provides positive assurance that the block valve upstream of each PORV is open when the system is enabled by wiring its position into the enable alarm. The enable alarm is not permitted to be activated until the temperature is less than 460°F.

7.4.2.2 Other Primary Coolant Boundaries Protection

1. Primary Coolant vs LPSI System

   A high-low pressure interface, in which the low-pressure system must be isolated from the high-pressure system when the high-pressure system is at rated pressure, exists in the shutdown cooling line connecting the Primary Coolant System to the suction of the low-pressure safety injection pumps. Isolation is provided by two valves in series. Except for the areas of penetration into containment, the power and control circuits of both valves are routed through the same fire areas. To preclude the possibility of fire damage to the control circuitry of the shutdown cooling valves resulting in opening operations of both valves, an operating procedure is provided requiring the valves to be checked closed and the operating power disconnected from both before pressurizing the primary system greater than 260 psig.

2. Primary Coolant vs Gas Vent System

   The primary coolant gas vent system allows the control room operator to remotely vent either the reactor vessel head space or the pressurizer vapor space (see supplemental details in Chapter 4). The vented vapor is released to the pressurizer quench tank for small quantities of vapor or to the containment atmosphere for large quantities. The vent isolation valves (remotely controlled) are series redundant with Class 1E controls and power including a separate key-operated control switch for each valve to ensure the primary coolant boundaries are maintained. The vent isolation valves are also parallel redundant to reduce the probability of a vent path failing to open since the valves are fail-close type in the event of loss of power. The valves and their controls are qualified to IEEE 332-1972 for inside containment devices, IEEE 344-1975 (seismic event) and IEEE 323-1974 (environmental and qualified life considerations) for all components. The isolation/opening controls meet IEEE 279-1971 including testability, using individual test and open/closed indication for each valve.

7.4.3 AUXILIARY FEEDWATER CONTROLS

For the safety-related portion of the auxiliary feedwater (AFW) system, the controls became Class 1E and automatic in response to NUREG-0578/0737. Alternate locations for controls were the result of the Systematic Evaluation Program of the Palisades Plant and compliance with Appendix R of 10 CFR 50. Compliance with Appendix R has since been replaced by compliance with National Fire Protection Association (NFPA) 805.

7.4.3.1 Auxiliary Feedwater Initiation

1. Design Bases

   Without an automatic initiation of the safety-related portion of the Auxiliary Feedwater System, the operator would have 17 minutes to restore flow to the steam generators upon loss of main feedwater to avoid opening of the primary coolant power-operated relief valves resulting in a small loss of primary coolant incident. Since the loss of main feedwater is considered as an anticipated operational occurrence, NUREG-0578 (Paragraph 2.1.7a) followed by NUREG-0737 (Section II.E.1.2) have required the installation of a Class 1E automatic initiation of the auxiliary feedwater pumps meeting IEEE 279-1971 criteria, assuring restoration of flow to the steam generators independent of operator action. Specific design criteria used in the design were to be as follows:

   a. Delivery of AFW minimum required flow to the steam generators must occur within 120 seconds of the Auxiliary Feedwater Actuation Signal for AFW Pumps P-8A and P-8C.

   b. The AFW pumps must be able to be started manually with or without the auto-start signal present.

   c. All circuits within the control system must meet IEEE 279-1971 including capability for on-line testing and a two-out-of-three (2/3) coincidence logic for low suction trip of the pumps.

   d. The circuits and instruments utilized must be powered from Class 1E power sources that meet the power redundancy requirements.

   e. 10 CFR 50, Appendix A, General Design Criteria 13, 20 and 34 are relevant to this system.

   f. 10 CFR 50, Appendix R, and 10 CFR 50.48 are to be met.

Review of the above criteria centered on potential common mode failures associated with the location of the existing AFW pumps (as of 1981) in a single room. Design modifications were performed in 1983 to incorporate a third AFW pump from the original design of two (one electric and one turbine driven) in a location physically separate from the other two pumps.

During the 1990 refueling outage, to meet the criteria defined in 10CFR50.62, the ATWS rule, an auto start of the turbine driven auxiliary feedwater pump on loss of dc control power was added.

During the 2018 refueling outage, a fourth AFW pump, P-8D, was installed to address postulated fire scenarios in rooms where the cables for the other three AFW pumps are routed. Such fire scenarios may result in a loss of the safety-related AFW trains, due to combinations of fire-induced cable and component failures, random failures, and failures of operators to take appropriate actions. In these scenarios, pump P-8D, which is diesel-driven and manually operated, is available to provide auxiliary feedwater to the steam generators.

2. Design Description

The safety-related portion of the Auxiliary Feedwater System utilizes two motor-driven pumps and one turbine-driven pump to feed the steam generators (Chapter 10). One or more of these pumps are started manually when required. In addition, one of the motor-driven pumps is automatically started upon low steam generator level. The second motor-driven pump is started in the case of failure of the first pump. If these pumps fail to establish flow or are tripped for any reason, the turbine-driven pump is then automatically started. Refer to the logic symbols of Figures 7-33 through 7-35 for reading the figures corresponding to this subsection.

Motor-Driven AFW Pumps Controls - Loss of main feedwater to the steam generators is indicated and annunciated in the control room by one of the following:

a. Closing of both the high- and low-pressure trip valves on each of the main feedwater pump drive turbines

b. Low main feedwater flow to the main feedwater pumps

c. Low steam generator level (pretrip)

If no action by the operator is performed, low-level signals from two-out-of-four (2/4) steam generator level sensors on an OR logic between the two steam generators energize a timer relay if the motor-driven AFW pumps mode selector switches are in the "Auto" position (Figures 7-36 through 7-39). Upon completion of the timing

cycle, the timer contacts actuate closing of the motor-driven AFW Pump A circuit breaker provided offsite or onsite standby (emergency generator) power is available. If offsite power is unavailable, the auto start is blocked until the normal shutdown or DBA sequencer allows loading the pump motor onto the emergency generator. The motor-driven AFW Pump C is called to start if Pump A circuit breaker trips or AFW flow does not materialize. The AFW low flow initiation logic is one-out-of-two (1/2) derived from redundant Class 1E voltage-type flow switches (Figures 7-43 and 7-44).

The 2/4 initiation logic is derived from current-type level switches installed in the redundant Class 1E Reactor Protective System steam generator level input channels (Section 7.2 and Figure 7-36). The mode selector switch position off the "Auto" position is indicated as an off-normal condition on the main control panel.

Manual trip of the pump can be accomplished by the circuit breaker control switch regardless of the presence of the automatic start signal. Automatic tripping will occur on pump low suction pressure via a two-out-of-three (2/3) logic from redundant Class 1E pressure sensors on the pump suction (Figures 7-41 and 7-42), or upon operation of the pump circuit breaker electrical protection (overcurrent/ground fault), or upon a load shed signal (Section 8.6). These trip functions are in force regardless of the presence of the automatic start signal. The 2/3 logic output will be sealed in, and the seal-in will be removed by manual closing of the pump circuit breaker.

Turbine-Driven AFW Pump Controls - A similar automatic start system is provided for this pump except that the timer for this system has a longer time delay setting to ensure the motor-driven pumps have had a chance to start and establish the auxiliary feedwater flow (Figures 7-36, 7-37 and 7-40).

An occurrence of low flow in either AFW line to the steam generators or motor-driven Pump C trip, together with a time delayed auto-start signal for the turbine-driven pump will open the turbine drive Steam Supply Valve B and start the pump. The steam supply valve control switch must be in the "Auto" position for the auto-start signal to be effective.

The AFW low flow initiation logic is one-out-of-two (1/2) derived from redundant Class 1E voltage-type flow switches (Figures 7-43 and 7-44). The Steam Inlet Valve B control switch position off the "Auto" position is indicated as an off-normal condition on the main control panel.

In the case of a successful start of one of the motor-driven pumps, the start of the turbine-driven pump is overridden by the reset of the AFW discharge line flow switches on a two-out-of-two (2/2) basis.

Manual starting of the turbine-driven pump can be accomplished at any time by its steam inlet valve control switch "Open" position. Manual trip can also be accomplished at any time by the same switch in the "Close" position. The control switch position in "Close" is indicated on the main control panel as an off-normal condition.

Automatic tripping of the pump will occur on pump low suction pressure with the same circuit as the motor-driven pump (P-8A) via a two-out-of-three logic. This trip function is in force regardless of the presence of the automatic start signal. The trip function is not in force for operation of the valve from the C150 panel or upon loss of DC control power to panel D11 (ATWS). The 2/3 logic output will be sealed in, and the seal-in will be removed by manual closing of the pump turbine Steam Supply Valve B. Steam supply valve A is also tripped on pump low suction pressure. This is a manually opened valve only. The 2/3 logic output will also be sealed in and the seal-in will be removed by manually closing the pump turbine steam inlet valve A.

A diverse system has been added to automatically start the turbine driven pump on loss of dc control power to panel D11 (ATWS system, 10CFR50.62). This automatic start is annunciated on the control room panel C06 (ATWS TROUBLE/TRIP).

Operation - The AFW automatic initiation system is placed in operation when the Primary Coolant System is heated above 300°F. Operation of the system is normally from the control room; if the control room becomes unavailable, manual controls can be taken over from the Auxiliary Shutdown Control Panel C-150 (see Subsections 7.4.1 and 7.7.4). The AFW automatic initiation system status is annunciated on the main control board (Figures 7-51 and 7-52).

Testing - Both the motor-driven and the turbine-driven AFW pumps' automatic initiation circuits are individually tested from the main control room according to Technical Specifications requirements. After a start test switch (one for each pump) has been turned to the "Test" position, a status light indicates the test status and the test signal passes through the automatic initiation circuit, including the timers, and starts the applicable pump. The test signal is sent into the circuit after the steam generator low-level signals logic, and in the case of the turbine-driven pump, after the AFW low-flow signals.

The steam generator low-level signals logic (Figure 7-37) is provided with test push buttons for test of the coincidence logic and bistable trip modules.

The entire automatic initiation circuit is tested on line and the pumps themselves are tested on line by the test switches. Water is delivered

to the steam generators during the test, thus checking the suction pressure and discharge flow switches operation. The steam generator level signals are checked as a part of the Reactor Protective System input channels test.

The nonsafety-related AFW pump P-8D can be manually started at either the pump or at a station located in the north heating boiler room. The manual controls for AFW supply flow to the steam generators are located in the atmospheric dump valve missile shield room, in close proximity of the main control room for enhanced communications during a postulated fire scenario.

3. Design Evaluation

The automatic AFW initiation system for the safety-related portion of the AFW system meets all the criteria of NUREG-0578/0737 and IEEE 279-1971.

The automatic start signal originates from independent steam generators low-level switches on a 2/4 logic from either steam generator. These two logic signals are independent and diverse. All components of the initiating logics are Class 1E. Initiating signals and circuits are powered from Class 1E preferred ac or 125 volt dc sources. The motor-driven Pump A circuit and the turbine-driven pump are considered as a "left" channel while the motor-driven Pump C is considered a "right" channel. One low steam generator level logic circuit is powered from the "left" channel preferred ac power supplies while the other logic circuit is powered from the "right" channel. Loss of power to either logic circuit does not result in AFW pump start and leaves one circuit available for activation. Loss of one 125 volt dc power to a pump control circuit channel leaves one pump start available. Electric power for motor-driven Pump A is supplied by 2,400 volt Bus 1C while Pump C power is from 2,400 volt Bus 1D, respectively, left and right channels. The electrical equipment and instrument channels are then powered from emergency buses which meet the power redundancy requirements set forth in NRC BTP ASB 10-1.

The two-out-of-three low-suction pressure pump trip eliminates the possibility of an incorrect trip of both pumps due to failure of a single pressure switch. These trip logic components are themselves Class 1E and the three sensing channels meet IEEE 279-1971.

Automatic/manual initiation requirements of IEEE 279-1971 are met as described earlier including ability to start the pumps regardless of auto-start system status and testability.

The ATWS system for automatic start of the turbine driven pump is a non-1E system as defined by 10CFR50.62. However the equipment in

the area of CV-0522B was purchased and installed as 1E equipment and it was mounted seismically.

The motor-driven AFW pumps are redundant to each other and to the turbine-driven pump to the extent that each pump is capable of supplying the auxiliary feedwater flow requirements to remove decay heat from the primary system and maintain the reactor in a safe condition.

The reliability of the system has been verified by a failure mode and effects analysis (see Reference 4). In addition, manual controls located outside the control room, in accordance with 10 CFR 50.48, have been provided.

In the case of offsite power loss as sensed by auxiliary contacts from the offsite power incoming circuit breakers (both open), the auto start of the motor-driven AFW pumps are included in the emergency generator's DBA and normal shutdown sequence. The turbine-driven pump will also be available in this case since all support equipment is powered directly or indirectly from the station batteries.

Instrumentation and control devices are qualified to IEEE 344-1975 and Regulatory Guide 1.100 seismic design requirements (deviations from the seismic design class are presented in Reference 5) and to IEEE 323-1974 and Regulatory Guide 1.89 environment and life qualifications requirements. Compliance with IEEE 279-1971 is summarized as follows:

a. No single component failure will prevent the auto-start signal from being initiated for at least one AFW pump.

b. Four independent steam generator level measurement channels complete with sensors, sensor power supply units, indicators and level switches are provided for each steam generator (diverse parameters).

c. The channels are provided with a high degree of independence by separate connections of the sensors to the process system and of the channels to preferred power supply buses. Separate raceways, conduits and junction boxes are used to ensure independence from cable faults.

d. The four normal (narrow-range) steam generator level measurement channels provide initiation signals to four independent initiation paths.

e. Elimination of spurious activation is provided by the 2/4 logic and the built-in time delays for actuation.

f. When one of the four channels is taken out of service for maintenance, the initiation logic reverts to either a 2/3 coincidence or a 1/3 coincidence.

g. The auto-start system instrument channels power is supplied from four separate buses.

h. Open circuitry or loss of power supply of one of the instrument channels initiates an alarm and a channel activation.

i. Loss of 125 volt dc power from one dc power source disables only one AFW pump auto start channel and this loss of power is alarmed.

Operation of the non-safety related, diesel-driven AFW pump P-8D is not affected by a site loss of power, and the pump has sufficient capacity to provide cooling to both steam generators.

7.4.3.2 Auxiliary Feedwater Flow Controls and Isolation

1. Design Bases

Reliable AFW flow and steam generator level instrumentation are necessary in order to adequately determine and control, from the control room or alternate shutdown stations, the performance of the safety-related portion of the Auxiliary Feedwater System since the operation of this system is considered as an anticipated operational occurrence by 10 CFR 50, Appendix A, GDC 13. NUREG-0578 and 0737 have identified the criteria to be met by this instrumentation and are outlined below.

In the event of a main steam line break inside containment, the AFW flow toward the affected steam generator must be terminated. This function must be performed using isolation valves in each steam generator's AFW supply line. The valves are isolated manually based on a low water level in one steam generator and excessive pressure differential between steam generators. The operator is instructed on manual steam generator isolation in the Emergency Operating Procedures.

Redundant Class 1E environmentally and seismically qualified, instrumentation channels' components have to be provided. The redundancy must meet IEEE 279-1971 criteria. The component qualification must meet IEEE 323-1974 and IEEE 344-1975 criteria. Power supplies must come from emergency sources.

The manual controls for operation of the nonsafety-related AFW pump P-8D are located in the atmospheric dump valve missile shield room, in close proximity of the main control room for enhanced communications

during a postulated fire scenario. The controls are battery-operated, and instruments are provided to monitor pump discharge flow, discharge pressure, and suction pressure.

2. Design Description

For the safety-related portion of the AFW system, four Class 1E AFW flow control channels are provided, fed from separate preferred ac sources, two for each steam generator (Figures 7-43 and 7-44). Two flow control channels relate to motor-driven AFW Pump A and turbine-driven Pump B, while the other channels relate to motor-driven Pump C. In each flow control channel, a flow indicating controller maintains constant flow rates to the applicable steam generator and provides flow indication in the main control room. The four channels are physically and electrically isolated including fire barriers according to IEEE 384-1977. The channels' components are qualified to IEEE 323-1974 and IEEE 344-1975.

The AFW flow control valves activated by these channels are CP Co Design Class 1. The flow control valves corresponding to operation with the turbine-driven AFW pump have a 8-hour motive nitrogen supply.

For FIC-0727 and FIC-0749, the flow controllers keep the control valves shut until one of the AFW pumps is started (Figures 7-46 and 7-47). This is accomplished using two flow set points on the controllers, one for shutdown (valve closed) and one for operation (valve opened for predetermined flow). Set point switching is provided by the motor-driven pumps' circuit breaker auxiliary contacts and the turbine-driven pump steam admission valve controls auxiliary contacts on an OR logic basis. This design allows timely and smooth opening of the AFW flow control valves without operator intervention.

For FIC-0736A and FIC-0737A, the flow controllers keep the control valves shut until an AFAS signal is received. This is accomplished by the program in the controller. The program looks for a pump start signal and an AFAS signal before automatically opening the valves. This design allows timely and smooth opening of the AFW flow control valves without operator intervention.

A separate Class 1E AFW flow indication channel for each AFW flow path (Figure 7-45) and a wide-range steam generator level indication channel for each steam generator are also provided allowing indication of flow independent from the control channel and monitoring of steam generator water level to cover all anticipated transients. These indication channels are qualified in the same way as the control channels and are also fed from preferred ac sources.

A "feed-only-good-generator" (FOGG) logic circuit (Figure 7-48) monitors the pressure differential between the steam generators using four independent and redundant Class 1E pressure sensors on each steam generator. These pressure sensors are also used by the Reactor Protective System and main steam isolation circuits (refer to Subsection 7.2.3.8). Concurrent excessive differential pressure between steam generators and low level in the depressurized steam generator initiates isolation of the depressurized steam generator by closing corresponding motor-operated isolation valves in the AFW supply lines (Figures 7-49 and 7-50). Two-out-of-four (2/4) differential pressure logic is used in coincidence with the output of the steam generator low-level logic described in Subsection 7.4.3.1. The isolation signal is generated through electronic bistable modules. Due to nuclear safety considerations, the automatic isolation feature of the FOGG system has been disabled and the operator is instructed by Plant Emergency Operating Procedures to isolate the affected steam generator using the flow control valves (see Section 9.7.2). The FOGG MOVs are de-energized and locked open.

The normally de-energized motor-operated automatic isolation valves are supplied from Class 1E 480 volt motor control centers. One isolation valve from each of the four discharge headers to the steam generators is supplied from the left channel of power and the other from the right channel to meet the single failure criterion.

Operation - Auxiliary feedwater flow indication, controls and isolation are normally from the main control room. In the event the control room must be evacuated, indication and controls can be taken over from either the Engineered Safeguards Auxiliary Panel C-33 or from the Auxiliary Hot Shutdown Control Panel C-150, depending on the nature of the emergency (see Subsections 7.4.1, 7.7.3 and 7.7.4). The controls at the alternate locations are manual. The locked open, de-energized motor-operated isolation valves are controlled locally at the valve by the operator.

If the pressure differential between the steam generators reaches the set point for actuation of FOGG circuit and the water level is low in one of the steam generators, the redundant FOGG signals close the motor-operated isolation valves to the depressurized steam generator. Due to nuclear safety considerations, the automatic isolation feature of the FOGG system has been disabled and the operator is instructed by Plant Emergency Operating Procedures to isolate the affected steam generator using the flow control valves (see Section 9.7.2). Isolation valve status can potentially be monitored in the control room. However, since the FOGG MOVs are de-energized and locked open, the control room position indication is currently de-energized. The FOGG circuit status is annunciated on the main control board (Figures 7-51 and 7-52).

Testing - Testing of the flow control instrumentation is provided by actual system functional testing since the Auxiliary Feedwater System is used during normal Plant evolutions.

The FOGG logic circuit including bistable isolation modules is provided with test push buttons for test of the coincidence logic and isolation modules for on-line testing.

For the nonsafety-related AFW pump P-8D, a digital controller is installed in the P-8D pump shed for operating the pump diesel driver and displaying system parameters.

3. Design Evaluation

The performance of the safety-related portion of the AFW system can be assessed by the AFW flow indicators, two for each steam generator located in the control room and alternate stations outside the control room and a wide-range water level indicator for each steam generator. All components of the indication system are Class 1E, seismically and environmentally qualified, and as such exceed the requirements of NUREG-0578/0737.

The AFW flow control and isolation systems meet IEEE 279-1971 in the same fashion as the AFW initiation circuitry. Their adequacy is demonstrated by their components qualification as well as their redundancy features both with a dedicated channel activating a given AFW control or isolation valve and in location (control room versus alternate stations).

The automatic AFW flow control system limits the AFW flow to a predetermined amount. Testing has demonstrated that with flow well above the set point of the instruments, no water hammer will occur.

7.4.4 CONTAINMENT HYDROGEN CONTROLS

7.4.4.1 Design Basis

A change to 10 CFR 50.44 for combustible gas control (Reference 19) eliminated the hydrogen release associated with a design base LOCA and the associated requirements for the hydrogen recombiners. The hydrogen recombiners were subsequently removed from containment.

Hydrogen monitoring in containment is described in Section 9.9. This equipment has been qualified in accordance with Regulatory Guide 1.97, Category 1 requirements for post-accident monitoring service.

The change to 10 CFR 50.44 also changed the classification of the containment hydrogen monitoring system to non-safety related, Regulatory Guide 1.97 Category 3.

7.4.5 VENTILATION AND EFFLUENT RELEASES CONTROLS

Safety related automatic isolation controls of ventilation and effluent releases are summarized in this subsection. Details of the applicable control systems are given in Section 9.8 and Chapter 11.

7.4.5.1 Control Room

Control room ventilation is provided with an automatic isolation upon containment high-pressure or high-radiation signal (see Subsection 7.3.3) to protect the operating personnel from any radioactivity release during an accident. The control room ventilation controls are Class 1E and are fed from the preferred ac power sources. In the event of isolation, all the makeup air for the control room is drawn through a charcoal filter to provide equal to or greater than 0.125 inch of water positive pressure design in the air recycle to ensure no in-leakage of radioactivity.

7.4.5.2 Engineered Safeguards Pump Rooms

One radiation monitor is installed for each engineered safeguards pump room to provide a room isolation signal upon high radioactivity levels in the applicable room. The automatic isolation reduces dose levels at the site boundaries. This system contributes to the leak detection capability described in Chapter 6.

7.4.5.3 Radwaste Area

One radiation monitor provides a ventilation shutdown signal for the area in the event of spillage. The area is maintained under negative pressure to prevent radioactive leakage out of the building with the supply fan and damper shut off while one of the exhaust fans is not shut off. Alarms in the control room warn the operator that one or more radwaste area ventilation fans have tripped off.

7.4.5.4 Fuel Handling Areas

The fuel handling areas are provided with radiation monitors to protect against radioactivity releases in the event of a fuel handling accident. Half of the ventilation is automatically shut off. The fuel handling building is then maintained under negative pressure to prevent leakage out of the building with a fan which is not shut off. Upon receiving an alarm from this monitor, the operator can manually trip the ventilation of the area.

7.4.5.5 Waste Gas Decay Tank

A high-radiation monitoring signal is provided to automatically close the waste gas decay tank discharge valve when the release rate exceeds the limits in the Offsite Dose Calculation Manual.

7.4.6 OTHER SAFETY RELATED DISPLAY SYSTEMS

Systems covered by this subsection are required to monitor Plant transients as identified in NUREG-0578/0737 and Regulatory Guide 1.97 and not discussed elsewhere. Appendix 7C provides a listing and an evaluation of all instrumentation contributing toward meeting Regulatory Guide 1.97.

7.4.6.1 Subcooled Margin Monitor

1. Design Basis

   Instrumentation detecting, displaying and annunciating physical parameters indicative of inadequate reactor core cooling is provided in the main control room as required by Regulatory Guide 1.97. Since this instrumentation involves the integrity of the core, it is classified as Class 1E, Seismic Category I and environmentally qualified. Through this system the operator is relieved from the time-consuming task of using steam tables along with primary coolant pressure and temperature observations during a transient when these parameters may be varying rapidly, thus eliminating the potential for corresponding operator errors.

2. Design Description

   The subcooled margin monitor is made out of two redundant and separate channels designed in accordance with IEEE 279-1971. Each channel includes Class 1E primary coolant process signal inputs, a digital recorder and an annunciator. Both display and annunciator are located on the main control board in the main control room.

   The system provides a continuous indication of the °F of primary coolant margin from saturation conditions. One channel monitors Coolant Loop 1 and the other Coolant Loop 2. The two channels are powered from separate preferred ac sources for assured continuity of monitoring.

   Each channel receives a pressure signal from a Primary Coolant System wide-range pressure transmitter and four wide-range temperature signals from given primary coolant hot and cold legs. The temperature ranges of the instruments are 50°F to 700°F and the pressure input is 0-3,000 psia. The process signals are input to a digital recorder capable of calculating values for saturation conditions. By comparing these values with the actual primary coolant values, a margin for saturation is calculated. Either the temperature or the pressure margin can be displayed.

IEEE 279-1971 separation requirements are met by the inclusion of isolation devices in accordance with IEEE 384-1977 between the temperature inputs and the applicable margin monitor channel circuit as well as interfaces with the primary coolant wide-range pressure channels.

Testing - Capability is provided for testing and calibrating the channels by observing proper system output for various input signals. The subcooled margin monitor testing requirements are included in the Technical Specifications.

3. Design Evaluation

The criteria of IEEE 279-1971 and Regulatory Guide 1.97 are met via separation, redundancy and testing features in the design. Interfaces, where inputs to the system mix more than one redundant channel, are provided with suitable isolators in accordance with IEEE 384-1977. Finally, the system and its inputs have been qualified per IEEE 323-1974 and IEEE 344-1975.

7.4.6.2 Wide-Range Containment Pressure, Temperature and Water Level

1. Design Basis

Operator performance during transient and accident conditions must include recognition and response to containment atmosphere pressure conditions and potential inadequate core cooling. Highly reliable instruments covering wide-range pressure and water level are considered as essential aids to accident diagnosis and control by NUREG-0578/0737 and Regulatory Guide 1.97. Additional instrumentation for monitoring containment atmosphere temperature throughout the accident range is also required for proper diagnosis in conjunction with pressure and water level.

2. Design Description

Containment Pressure - Two redundant Class 1E continuous wide-range pressure transmitters fed from separate preferred ac power sources are installed and transmit signals to two recorders located in the control room with state-of-the-art accuracy and response time characteristics. The monitors have a range of 0 psia to 200 psia enveloping the range of -5 psig to at least three times the design pressure of the containment building (Chapter 5).

Containment Water Level - Two redundant Class 1E instrument channels (magnetic float devices) provide containment floor water level indication up to the 597-foot elevation. A diverse system provides two other redundant Class 1E instrument channels for containment sump water level indication and recording via level transmitters in the containment sump drain line to the dirty waste drain header. The combined range of these overlapping channels covers the maximum level theoretically obtainable during a Loss of Coolant Accident. Each of the measurement channels is fed from a separate preferred ac power source. These instruments have also state-of-the-art accuracy.

Containment Temperature - Four instruments are provided for monitoring the containment atmosphere temperature throughout the predicted accident range. Reactor cavity, steam generator space and containment dome temperature are indicated on the main control board up to 400°F. The system provides continuous display even though this is not a requirement. Sensors are resistance temperature detectors placed in appropriate locations in the containment. Indicators are mounted in a control panel containing Class 1E instruments within the main control room. Instrument power is provided by preferred ac Panel Y30 which receives its power from the Plant emergency power sources.

3. Design Evaluation

Both pressure and water level instrument channels meet IEEE 323-1974 and 344-1975. The process connections and the sensors, as well as all components of these channels, are Seismic Category I per Regulatory Guide 1.29 and meet Regulatory Guide 1.97 as required by NUREG-0578/0737.

7.4.6.3 Reactor Vessel Level Monitoring System

1. Design Basis

In accordance with the requirements of Generic Letter 82-28, a Reactor Vessel Level Monitoring System (RVLMS) is installed to provide indication for detection of Inadequate Core Cooling (ICC) conditions. The system provides indication of level in the Primary Coolant System covering a range from near the top of the reactor vessel head to just above the reactor core. The RVLMS instrumentation system assists the operator in avoidance of ICC when voids in the Primary Coolant System and saturation conditions result from overcooling events, steam generator tube ruptures or small-break loss of coolant events.

2. Design Description

The RVLMS consists of two independent, physically separated, redundant and identical channels. Each channel includes one Radcal® Level Instrument (RLI) which extends from the incore instrument nozzle closure flange down through the guide tube attached to the control rod shroud, ending just above the fuel assemblies. The RLIs are inserted into existing incore instrument guide tubes. Each RLI terminates above the reactor vessel head in a multi-pin, 1E qualified electrical connector. Two 1E qualified in-containment cable assemblies, connected in series, are provided for each channel from the RLI connector to the containment penetration. Outside of containment, 1E qualified cable is provided for each channel to transmit signals and supply power between the containment penetration and the level and temperature recording indicator (LTRI) located in the main control room.

Each RVLMS channel is composed of a manometer tube and an RLI containing eight sensors. The manometer is created by cutting ports in the existing incore instrument guide tube and is divided into regions with hydraulic isolators which are part of the RLI. Two separate regions, the head region and the Upper Guide Structure (UGS) region, are monitored by four sensors each. The head region extends from the reactor head instrument nozzle flange down approximately 5.5 feet to the first hydraulic isolator. The UGS region extends from the first hydraulic isolator to the second hydraulic isolator located approximately at the top of the fuel alignment plate. The porting patterns cut in the incore instrument guide tube were determined by tests performed to establish proper manometer performance.

The RLI is a stainless steel rod containing sensors which consist of differentially connected thermocouple pairs. One thermocouple junction is electrically heated and the other is not. In water the heat transfer from the junctions is high so that the differential temperature indication is low. In steam the heat transfer rate is reduced and the heated junction gets hotter, increasing the differential temperature indication. High differential temperature is the indication of water uncovery of the sensor.

Indication for the RVLMS is provided by two identical units (LTRIs), one for each channel, located in the control room. The level indication consists of two strings of vertical Light-Emitting Diodes (LEDs). A green LED indicates covered and a red LED indicates uncovered for each sensor in the RLI. The sensors are numbered and their distance above the fuel is indicated. Level information is also displayed on adjacent strip chart recorders, one for the head region and one for the UGS region. The recorders display differential temperature information from the RLI sensors which can be used to diagnose potential degradation or failure of the sensors and aid in interpretation of level information. Two additional recorders in the same panel display the outputs of eight CETs (16 total in the two channels) to provide the required CET backup displays. The CET and RLI signals are isolated and transmitted to the Plant Computer CFMS Multiplexor for the primary displays.

3. Design Evaluation

The RVLMS conforms to the design and qualification criteria for Category 1 instrumentation of Regulatory Guide 1.97. An evaluation of the RVLMS against Regulatory Guide 1.97 criteria is provided in Appendix 7C. RVLMS meets NUREG-0737 requirements for inadequate core cooling instrumentation as described in Reference 8. RVLMS instruments have had operability and testing requirements incorporated into Technical Specifications with Amendment 129 (see Reference 13). The NRC has accepted the RVLMS as Palisades' Inadequate Core Cooling Instrumentation (ICCI) in a letter dated January 12, 1987 (Reference 8). The stated basis for approval was that the RVLMS meets the requirements of Item II.F.2 of NUREG-0737.

7.4.6.4 Core Exit Thermocouple (CET) System

See FSAR Section 7.6.1.4 and Appendix 7C, Item C01, for a discussion of this system.

7.5 NONSAFETY-RELATED REGULATING CONTROLS

7.5.1 DESIGN BASES

7.5.1.1 Reactor Regulating

Reactivity is controlled by a combination of chemical shim and CRDM motion. Variation of the chemical shim (boric acid) concentration provides long-term regulation and control. The Chemical and Volume Control System is used to increase or decrease boron concentration with concentration being measured by chemical analysis.

Control rod motion is used for short-term regulation. Sequential insertion or withdrawal of the control rods in the regulating groups is used for normal power regulation until the rods are in the All Rods Out (ARO) configuration. When the control rods are in the ARO configuration, boron chemical shim is used to control power level. Reactivity control is a manual operation whether using control rods or boron chemical shim.

Either of two independent channels may be selected to provide reactor average coolant temperature and a reference temperature value corresponding to turbine power. The reactor average coolant temperature and reference temperature values are displayed to operators who manually adjust primary coolant temperatures by either moving the control rods or by use of the boron chemical shim.

The primary coolant average temperature is adjusted according to a preselected program. This program provides an average temperature which is linearly increasing with power.

Inputs to the temperature computing stations are primary coolant cold leg temperature, primary coolant hot leg temperature, and turbine first stage pressure. The temperature computing stations are two separate stations with each having separate inputs as listed above. Rod position instrumentation is covered later in this section and details of the CRDM are covered in Chapter 3.

Control rods are grouped into shutdown, regulating and part-length groups. The shutdown groups are the first to be withdrawn on start-up and they remain withdrawn throughout power operation to provide a definite shutdown margin at all times. The regulating groups are manually positioned. The part-length control rods are manually positioned individually or by group and cannot be tripped. Alarms exist in the control rod position instrumentation to annunciate deviation of control rods within any group except the part-length group. Any individual control rod may be positioned manually if required.

The part-length control rods are completely withdrawn from the core during power operation except for control rod exercises and physics tests. The insertion of part-length rods into the core while critical, except for rod exercises or physics tests, is not permitted since it has been demonstrated on other CE plants that design power distribution envelopes can, under some circumstances, be violated by using part-length rods.

The regulating and shutdown control rods are inserted by gravity action (backed up by control rod rundown) on the receipt of a reactor trip signal.

Control rod withdrawal is prohibited in certain situations where reactor limits are being approached. These prohibitions are detailed in Subsection 7.5.2.1.

7.5.1.2 Primary Pressure Regulating

The primary pressure controls maintain primary system pressure within preset limits by the use of pressurizer heaters and spray valves.

Pressurizer pressure and level sensors provide inputs to the controls. When system pressure is low, heaters are energized on a proportional or group basis to raise pressure. Before the level is low enough to uncover the heaters, level sensors cause the power to be interrupted to the heaters. When system pressure is high, pressurizer spray valves are opened on a proportional basis to reduce pressure.

Two channels of control are provided and the controlling channel is selected by a switch. Manual control of heaters and spray may be selected at any time.

7.5.1.3 Feedwater Regulating

The feedwater controls maintain steam generator downcomer level within acceptable limits by positioning the feedwater regulating valves supplying each steam generator (see Subsection 10.2.3.3). The speed of the turbine-driven main feedwater pumps is also controlled by the feedwater controls.

Automatic control of feedwater is provided when the plant is at power. Steam flow, feedwater flow and downcomer level are used in a three-element controller on each steam generator to maintain preset level during steady-state and transient operation above 25%. At low power levels (5% to 25%), feedwater flow is regulated automatically by a single-element controller acting on the feedwater regulating bypass valves according to steam generator downcomer level requirements.

Manual control of feedwater flow may be assumed by the operator at any time. In the event of a reactor or turbine trip and if the feedwater pump turbine drivers are in the automatic control mode, the speeds of the feed pumps are automatically ramped down to a lower value. Following or during the ramp-down, operators can manually control main feedwater flow or initiate auxiliary feedwater flow as necessary to restore and maintain desired steam generator levels.

In the event of low steam generator pressure < 500 psia or containment high pressure (CHP), the main feedwater regulating and regulating bypass valves are closed to prevent excessive flow into the steam generators. This ensures containment pressure is not exceeded during a main steam line break inside containment (refer to Subsections 7.2.3.8 and 7.3.3.3). The valve closing on CHP was added by FC-906 in 1990 when analysis disclosed that for a small steam line break, low steam generator pressure would not occur fast enough to prevent exceeding containment design pressure. Control of the bypass of the steam generator pressure signal to close the main steam isolation valves, the main feedwater regulating and regulating bypass valves is facilitated by using push buttons on the panel to override the signal to allow manual take-over of the controls. In addition to the push buttons, manual take-over of the feedwater regulating bypass valves can be accomplished by using key-operated switches.

7.5.1.4 Pressurizer Level Regulating

Pressurizer level is maintained within an operating band by means of the Chemical and Volume Control System. Water is continuously drained and charged automatically to and from the pressurizer with control inputs from pressurizer level sensors. The level set point is programmed as a function of T_{avg} (average of hot and cold leg temperatures). There are two completely independent automatic control channels with channel selection by means of a manual control switch. Automatic control is normally used during operation but manual control may be utilized at any time.

This control system is one of the defenses against high pressurizer level or water solid conditions. The Reactor Protective System provides the other defenses through the high pressurizer pressure reactor trip protective function (refer to Subsection 7.2.3.4).

7.5.1.5 Steam Dump and Bypass

The steam dump system provides a means of dissipating excess NSSS stored energy and sensible heat following a turbine trip, without lifting the safety valves. See Subsection 10.2.1.3 for details. Steam is discharged from the main steam lines to the atmosphere via steam dump valves and to the condenser via a steam bypass valve. The steam dump and bypass valves are sized to prevent opening of the steam generator safety valves following a turbine trip at full load. The steam flow is regulated by the dump and bypass valves in response to T_{avg} and secondary pressure signals.

Inputs to the controls are T_{avg}, turbine trip signal and steam header pressure.

The steam dump and turbine bypass controls need to be operable to control steam generator pressure such that P-8C is able to provide sufficient flow to maintain heat removal capacity.

The controls for the turbine bypass and atmospheric dump valve controls were designed and installed to provide reliable service in normal plant ambient conditions. Under accident conditions (with the exception of a main steam line break) the solenoid valves, switches, transducers, etc. will be in essentially a normal environment. If a main steam line break occurs that can't be isolated (to restore normal conditions), the steam generator will blow down. The dumps or bypass are not required, but may be used if available.

7.5.1.6 Turbine Runback

The original design included a turbine runback upon detection of a dropped rod. Later analysis showed that at the beginning of reactor core cycle, turbine runback could have unacceptable effects on reactor performance. Thus, the turbine runback feature has been disabled.

Turbine runback upon detection of a dropped rod doesn't exist in the Digital Electrohydraulic (DEH) control system. However, there is an operator selectable runback to 5% or 50% which, when selected, will runback to 5% or 50% at the rate that the DEH system was originally running.

7.5.1.7 Turbine Generator Controls

The turbine generator controls are the means by which the turbine generator is made to meet the electrical load demand placed upon it. The turbine impulse chamber pressure, turbine speed, and electrical load are used as the control indices.

7.5.2 SYSTEM DESIGN

7.5.2.1 Reactor Regulating

A block diagram of the primary loop temperature instrumentation is shown in Figure 7-54. The instrumentation consists of:

1. Four high level isolated transmitters.

2. Two temperature computing stations.

3. Two primary coolant loop hot leg temperature alarm/indicators.

4. One six-input loop T_{AVE}, T_{REF} and differential temperature recorder.

5. One two position switch to select either of the two channels to provide the T_{AVE} signal to the steam dump controller and pressurizer level controllers.

6. One digital indicator to display T_{AVE} as selected by the switch.

7. Two voltage to current converters.

Inputs to the temperature computing stations are:

1. Loop 1 Temperature computing station.
    1. Primary coolant loop 1 cold leg temperature.
    2. Primary coolant loop 1 hot leg temperature.
    3. Turbine first stage pressure.
    4. Primary coolant loop 2 T_{AVE}.

2. Loop 2 Temperature computing station.
    1. Primary coolant loop 2 cold leg temperature.
    2. Primary coolant loop 2 hot leg temperature.
    3. Turbine first stage pressure.

All inputs are isolated from protective system instrumentation.

Outputs of the temperature computing stations are:

1. Loop 1 temperature computing station.
    1. Primary coolant loop 1 T_{AVE}.
    2. Primary coolant loop 1 differential temperature.
    3. T_{REF} (for primary coolant loops T_{AVE}).
    4. Deviation alarm; (T_{AVE1}/T_{AVE2})
    5. Deviation Alarm; (T_{AVE}/T_{REF})

2. Loop 2 temperature computing station.
    1. Primary coolant loop 2 T_{AVE}.
    2. Primary coolant loop 2 differential temperature.
    3. T_{REF} (for primary coolant loop T_{AVE}).
    4. Deviation alarm; (T_{AVE}/T_{REF})

Two separate T_{AVE} channels are provided for pressurizer level control and steam dump control. Either channel may be selected. In each channel a temperature computing station establishes primary coolant temperature (T_{REF}) based on a power reference signal from first stage turbine pressure. T_{REF} varies linearly with power from a nominal temperature of 532°F at hot standby to an adjustable limit of 550°F to 580°F at 100% power. T_{REF} is compared with the actual loop T_{AVE}, and provides a deviation alarm at a prescribed value.

Control rods are divided into the following groups:

1. Shutdown: Two groups

2. Regulating: Four groups

3. Part-Length: One group

The circuitry utilized for sequential control rod group movement during manual operation is indicated on the Rod Drive Control System Schematic Diagram, Figure 7-55.

Each control rod remains stationary except when a raise or lower signal is present. When such a signal is received, the control rod will move at a fixed speed of approximately 46 inches per minute.

The shutdown control rods may be moved in the manual control mode only with either individual control rod or individual group movement. A selector switch prevents withdrawal of more than one shutdown group at any time. The shutdown groups must be withdrawn above the regulating rod withdrawal permissive height (122") before regulating group withdrawal is possible. The upper 10 inches of shutdown group control rod travel is designated as the exercise band and is provided so the shutdown control rods may be exercised while the reactor is at power. An interlock from the primary control rod position indication system synchro limit switches described in Subsection 7.6.2.3 prevents the shutdown groups from being driven down more than 10 inches unless the regulating control rods are fully inserted. Refer to Figure 7-56. This interlock is bypassed for a control rod rundown following a reactor trip. The reactor trip initiates rundown of the shutdown and regulating control rods through relays connected in parallel with the CRDM clutches (see Subsection 7.2.5.1).

Regulating control rods may be moved in manual control with sequential group movement. Automatic sequential control utilizes outputs from the primary control rod position indication system data processor described in Subsection 7.6.2.3. Individual and groups of control rods may be moved in manual control. Sequential group movement provides that when the moving group reaches a programmed low (high) position, the next group begins lowering (raising); the initial group stops upon reaching its lower (upper) limit. This procedure, applied successively to all regulating groups, allows a smooth and continuous rate-of-change of reactivity.

When the regulating groups reach the "prepower dependent insertion limit" alarm point, this condition will be annunciated. If insertion is continued, a "power dependent insertion" alarm point is reached and a continuous alarm is initiated. This second, continuous alarm can only be silenced by removing the condition (withdrawing control rods or lowering power). These two programmed limits may be adjusted during the life of the Plant and are provided by the primary rod position and secondary rod position indication systems data processors to assure adequate shutdown margin according to Technical Specifications requirements (see Subsection 7.6.2.3).

All control rods will be prevented from being withdrawn if either a high power or high power rate-of-change pretrip condition exists.

Interlocks to prohibit regulating group withdrawal are provided to prevent the reactor from reaching undesirable conditions. These interlocks are summarized in Table 7-2.

The part-length control rods may be moved manually either individually or as a group. A selector switch prevents simultaneous manual movement of the part-length and any other control rods. The part-length control rods have upper and lower limits of travel.

The part-length control rods are completely withdrawn from the core during power operation except for physics tests. The insertion of part-length rods into the core, except for physics tests, is not permitted since it has been demonstrated on other CE plants that design power distribution envelopes can, under some circumstances, be violated by using part-length rods.

7.5.2.2 Primary Pressure Regulating

Two independent pressure channels provide suppressed range (1,500 to 2,500 psia) signals for control of the pressurizer heaters and spray valves. The output of either controller may be manually selected to perform the control function. During normal operation the backup heaters are on. The spray valves are modulated to maintain system pressure. A continuous flow is maintained through the spray lines at all times to keep the pipes warm and to assure that the pressurizer maintains the proper boron concentration.

The two pressure control channels are recorded in the control room and provide independent high and low alarms.

Two independent level channels provide pressurizer level signals for two specific functions:

1. A low-level signal from either channel will de-energize all heaters.

2. A high-level signal from either channel will energize the backup heaters.

Control and alarm pressure set points are shown on Figure 7-57.

7.5.2.3 Feedwater Regulating

The steam generators are operated in parallel on the feedwater and on the steam sides. Each generator has a three-element controller with inputs of feedwater flow, steam flow (corrected for pressure) and downcomer level. Output of each controller when in automatic control is used to provide pneumatic signals to position the respective feedwater regulating control valve. The higher of the two signals provides a speed control signal to the main feedwater, turbine-driven pumps. This signal controls pump speed if the turbine speed control is in automatic. When Plant power is between 5% and 25%, feedwater is automatically controlled by a single-element controller monitoring steam generator downcomer level and positioning the feedwater regulating bypass valves. Four overrides are provided:

1. When contacts in the steam dump permissive switch are actuated on a main turbine trip, feedwater regulating control valves are maintained in the position which existed prior to the switch activation. The feedwater pumps, if in automatic speed control, ramp down to a fixed speed which corresponds to approximately 5% of full flow. Due to the slow rampdown, operators may manually control main feedwater flow or initiate auxiliary feedwater flow as necessary to restore and maintain steam generator levels.

2. When an abnormally high-steam generator level is sensed by an independent downcomer level sensor, a signal is sent to close the associated feedwater regulating control valve and a control room alarm is annunciated.

3. During low-steam generator pressure < 500 psia, the main feedwater control valves and the bypass valves are closed automatically. The operator can manually take control of the bypass valves by isolating the low steam generator pressure signal using a key switch on the control panel.

4. During high containment pressure, the main feedwater regulating valves and their bypass valves are closed automatically (FC-906, 1990).

Manual control of the feedwater flow may be assumed at any time to circumvent malfunction of components within the system except for control of the feedwater regulating valve when the steam generator high level override, steam generator low pressure override, or Containment High Pressure override is present. Each of these override signals blocks the valve control signal between the level controller and the feedwater regulating valve, causing the valve to be driven closed. Otherwise, when in manual control, the operator in the control room can:

1. Position manually each feedwater regulating control valve

2. Control speed of the two main feedwater pumps

3. Open or close each feedwater stop valve

4. Position manually each feedwater bypass regulating valve

Operation of the Auxiliary Feedwater System is always available to supplement the above options (refer to Subsection 7.4.3).

7.5.2.4 Pressurizer Level Regulating

The operating level of the pressurizer is a programmed function of the primary coolant loop T_{AVE}. It is programmed to accommodate plant load changes and transients while keeping the primary coolant system volume changes to a minimum.

Programmed level is established by the pressurizer level controllers, which receive a T_{AVE} input from the primary loop temperature instrumentation. The pressurizer level controller establishes a set point directly proportional to T_{AVE}. Refer to Figure 4-10. The controllers also receive pressurizer level information from two level sensors. Controller output is sent to control charging pumps and letdown orifice valves. The outputs of either of two automatic control channels may be selected by the operator for level control in addition to manual control.

Controller action and program level are described in Section 9.10, Chemical and Volume Control System.

7.5.2.5 Steam Dump and Bypass

A block diagram of the steam dump and bypass controls is shown in Figure 7-58. The system consists of:

1. One steam dump controller located in the Control Room

2. Two steam dump controllers (performs tracking in auto mode) at engineered safeguards panel

3. Four atmospheric steam dump valves

4. One turbine bypass pressure controller located in the Control Room

5. One signal auctioneering unit

6. One turbine bypass valve

Inputs to the controls are:

1. T_{AVE}

2. Steam header pressure

3. Turbine trip (contacts in steam dump permissive switch)

4. Loss-of-condenser vacuum (contacts)

Outputs of the controls are:

1. Atmospheric steam dump valve position signal

2. Turbine bypass valve position signal

The steam dump controller generates a suppressed range signal proportional to (T_{avg} – 532°F). Upon receipt of a turbine trip, this signal is supplied to open the atmospheric steam dump valves, and is an input to the turbine bypass auctioneering unit to simultaneously open the bypass valve. The position of the atmospheric steam dump and bypass valves is proportional to the signals supplied to them, thus providing a controlled relieving of excess pressure.

After a turbine trip, the steam dump controller's quick opening signal will cause quick opening for the dump and bypass valves.

The atmospheric steam dump valves will close proportionately as T_{avg} reduces and will close completely at 535°F. They will remain closed unless T_{avg} increases again to more than 540°F.

The turbine bypass valve receives the higher of the steam dump controller or steam bypass pressure controller signals through an auctioneering unit. This controller generates a suppressed range signal proportional to secondary pressure over the range 895 psia to 905 psia. Loss-of-condenser vacuum will prevent the opening of the bypass valve.

By manually changing the set point on the steam bypass pressure controller, the operator may control primary coolant temperature during Plant cooldown by use of the bypass valve. Once the turbine trips, the operator may manually control the atmospheric dump valves and still control the turbine bypass valve.

7.5.2.6 Turbine Generator Controls

The turbine generator controls (or electrohydraulic control system) controls steam flow to the turbine. The controls consist of the following five parts:

1. Operators Interface Panel

2. Digital Controller & Engineers Console

3. Steam valve servo actuator assemblies

4. High-pressure fluid supply

5. Emergency trip

The electronic controller performs basic digital computations on reference signals and turbine feed-back signals and generates an output to the actuators.

The operator's panel contains push buttons and switches which are used to change the reference input to the controller to vary the speed or load. Indicators provide continuous monitoring of steam admission valve position, load limit setting and control signal.

The servo valves position the governing valves by directing the flow of E-H oil to the actuators.

The high-pressure fluid controls operate the stop, governor, reheat stop and interceptor valves. The fluid is stored in a stainless steel reservoir and is furnished with a duplicate system of oil pumps, filters and heat exchangers. The fluid pressure is controlled by constant pressure, variable displacement pumps.

The emergency trip uses bearing lubricating oil as its control medium. The trip device is a diaphragm valve which is sensitive to the dump valve servo actuator position and releases the emergency trip oil to drain. This action is caused by the turbine over-speed trip, the local manual trip and the operation of trips loaded in the protective device unit. The trips located in the protective device unit are low condenser vacuum, low bearing oil pressure, and the 20 AST solenoid trip. Several trips feed through the 20 AST solenoid trip including generator/breaker trips, turbine no load trip, reactor trip, main steam isolation valve not full open trip, turbine DEH loss of power trip and the control room manual turbine trip pushbutton. The main steam isolation valve not full open trip also feeds the 20 ET solenoid trip, as does the thrust bearing trip and the ATWS trip. The emergency trip 20 ET solenoid directly releases EHC fluid to drain.

A reactor trip results from a turbine generator trip only when the reactor is above 15% full power level. A turbine generator trip on closure of the main steam isolation valves (MSIVs) is provided to protect the MSIVs from experiencing the full differential pressure of a steam generator.

The turbine generator unit is controlled from the operator's interface panel. The panel shows which devices are controlling the turbine generator. The controller computes signals to position the governor valves. As the speed reference is changed during start-up, the speed transducer signal is compared to the reference speed setting. During load control, the controller also computes signals to position the governor valves. As the load reference is changed by the control operator, the controller compares the load reference to the feed back from the megawatt transducer, the first stage steam pressure transducer, and from valve curves contained within the computers memory. The difference or load error then sets the position of the governor valves servo actuators. The governor valve servo actuators change the steam flow to the turbine. The result is a change in turbine load which is detected by the transducers and is compared to the reference load setting.

The turbine generator controls are composed of the digital computer controller and the valve servo driver cards. The Valve Servo Driver accepts serial input from the local auto controller, plus LVDT inputs. It outputs to Moog Valve Coils and the Valve Position meter. Manual inputs and Manual functions, plus valve contingencies are also built-in capabilities.

The reheat stop and interceptor valves can be tested while the turbine is loaded. A signal can be introduced to the Valve Servo Driver cards to cause the servo valves to exercise the stop and governor valves.

7.5.3 SYSTEM EVALUATION

7.5.3.1 Rod Drive Control System

Control rods are segregated into three groups: shutdown, regulating and part-length. The shutdown and part-length control rods remain raised throughout power operation to provide a shutdown margin at all times. When the reactor is tripped, all control rods except the part-length are inserted by gravity and backed up by control rod rundown.

Sequential insertion and withdrawal of regulating group control rods are employed for normal power regulation. The manual demand signal controls the application of power to the regulating group(s) selected for movement by the action of the group sequencing relays. The group sequencing relays are programmed by permissive actions initiated by the data processor, utilizing information from the primary rod position system.

The circuitry used for sequential control rod group movement is shown on the Rod Drive Control System Schematic Diagram, Figure 7-55. The insertion of the shutdown rods before the regulating rods is prevented by the contacts from the shutdown rod insertion permissive relays R/RS1 through R/RS4 or the exercise band limit switches and contacts from the shutdown group relay R/AD1. A single failure could cause the shutdown rods to be inserted beyond the exercise limit prior to the insertion of the regulating rods, only in conjunction with the operator selecting the shutdown group for insertion. Simultaneous insertion of the regulating and shutdown rods could occur only by energizing the rod run-down relay. Failure of a single CRDM clutch power supply "K" relay (Subsection 7.2.5.3) will not cause rod rundown. De-energization of the clutch power supply bus will run down all control rods.

The simultaneous withdrawal of more than two groups of control rods could occur upon certain single failures in the control system. This could occur during the overlap period when two groups of rods are being withdrawn, so that the failure of the sequential permissive contact in the sequence relay circuit of a third group would permit three groups to be moving at once. Indication of the group(s) selected for rod motion and indication of the direction of rod motion for the group(s) selected is provided at the main control room console (refer to Figure 7-55). An out-of-sequence alarm initiated from the rod position is provided to alert the operator of an out-of-sequence condition.

It is possible for a rod group to be withdrawn out of proper sequence if certain single failures occur in coincidence with specific operational situations. This could occur during the overlap period when two groups of rods are being withdrawn so that any failure, such as the de-energization of the group relay which stops the movement of the leading group, will interrupt the planned sequence. The out-of-sequence alarm will be actuated in such an event. Again, the nonsequential withdrawal is not a continuous withdrawal.

7.5.3.2 Primary Pressure Regulating

Two independent channels are available for automatically regulating the pressurizer heaters and spray valves. Either channel may be used to control the pressure in the system, and the output from both channels is recorded in the control room. Independent high and low alarms are provided.

7.5.3.3 Feedwater Regulating

For power above 25% full power, conventional three-element, feedwater control is used with fail-as-is, feedwater control valves. Manual override of the automatic control is always available. Manual bypass valves and feedwater stop valves provide backup for feedwater valve failure. For power below 25% full power, and to facilitate start-ups, a single-element feedwater bypass valve controller is used. Manual override of this automatic control is also available.

Feedwater pump speed control is by automatic or manual means.

Feedwater flow from the condensate pumps will be shut off via closure of the feedwater regulating and bypass valves on low steam generator pressure (< 500 psia). 500 psia is above the maximum condensate pump delivery head such that the maximum of feedwater delivered to the steam generator will be no greater than that assumed in the safety analysis.

Accurate measurements of reactor power output use the feedwater flow instruments as a base for calorimetric calculations (see Subsection 7.2.3.2 for reactor power level measurement versus reactor trip function). These flow instruments' calibration is thus regulated by the Operating Requirements Manual.

A long term operational affect on the feedwater flow instrumentation (by methods such as venturi fouling) causes them to indicate conservatively (indicated feedwater flow is greater than actual feedwater flow). In order to determine the actual feedwater flow, an ultrasonic flowmeter has been used. By comparing the feedwater flows from both the feedwater flow instrumentation and the ultrasonic flowmeter, a correction factor (the ratio of ultrasonic flowmeter flow to feedwater instrumentation flow) can be calculated. This correction factor can be multiplied by the feedwater flow instrumentation indicated flow and then inputted into the calorimetric calculation as the actual feedwater flow. This will result in the most accurate available measurement of reactor power.

7.5.3.4 Pressurizer Level Regulating

Two separate level control channels are provided with redundant level transmitters and controllers. Only one channel is used during operation. The controllers are located in the control room. Control can be accomplished by either automatic or manual operation. Three charging pumps and three letdown orifice valves provide redundant means of increasing or decreasing primary coolant water inventory. The variable pressurizer level control program minimizes primary coolant discharge and addition required during Plant load changes.

The pressurizer level control system is sufficient to protect the Primary Coolant System fluid boundaries without a reactor trip on high pressurizer level to protect against a water solid condition. If a malfunction is suspected in the operating channel, operation can be switched to the other channel. If a failure of the controller output is postulated, a large "program minus actual level" difference will result. This will cause two orifice stop valves to close and will start all three charging pumps. When the pressurizer level increases 4.6% above the programmed level, two charging pumps will be secured and the two orifices' stop valves reopened. This failure will not result in a filled pressurizer.

If a failure in the level transmitter is postulated, a low-low level signal is initiated causing all orifice stop valves to close and all three charging pumps to operate. In order to fill the pressurizer, this condition would have to exist unchecked by operation action for a period of about 30 minutes (time required to fill the 700-ft^3 steam space in the pressurizer). During this period, an alarm would sound alerting the operator to the mismatch between charging and letdown flow. Also, a low-level alarm from the volume control tank would sound. (There are about 3,600 gallons stored in the volume control tank, and over 5,000 gallons are required to fill the 700-ft^3 steam space.) Continuous operation of the charging pumps is indicated by lights in the control room. The operator can switch to pressurizer level control Channel B (assuming Channel A is in service at the time) to determine if the reason for the extended charging operation is caused by a malfunction of the level transmitter. The operator can manually secure the charging pumps when the problem has been diagnosed, or allow the backup channel to assume control.

Assuming that no operator action was taken, and the pressurizer continued filling with water, and pressure continued to rise, the pressurizer pressure control system will maintain pressure at about 2,180 psia. At 1,700 seconds after the transient is initiated, the spray nozzle, which extends about 2 feet from the top of the pressurizer, becomes submerged by the rising water and is no longer effective (the effectiveness of the spray is reduced even before submergence of the spray nozzle, owing to the shape of the spray extending from the nozzle). At the level of nozzle submergence, a 40-ft^3 steam space remains at the top of the pressurizer. A simplifying and conservative assumption invoked for this analysis is that pressurizer pressure is maintained at 2,180 psia until it is completely filled, thereby neglecting the mitigating effect of the 40-ft^3 steam space in minimizing pressure during the incident.

After the pressurizer fills, it is assumed that all three charging pumps continue to deliver water into the Primary Coolant System at the maximum rate of 120 gpm and that all letdown orifices remain closed. The time required to increase system pressure from 2,180 psia to reactor trip pressure of 2,255 psia is approximately 2 minutes (owing to the compressibility of one-half million pounds of water at 578°F, more than 1,000 pounds of additional water is required to raise system pressure 220 psi).

Following the high pressurizer pressure reactor trip signal, the control rods are inserted 90% of travel within 2.7 seconds. The turbine admission valves are closed at 0.3 second, and all rods are fully inserted. Although the steam dump and bypass valves will open following turbine trip (and thereby reduce the pressure increase in the steam generator and subsequently reduce the increase in primary system temperature), credit is not taken for such action in this analysis. The maximum increase in the average temperature of the primary system following trip of the reactor and turbine is less than 0.5°F. This energy increase in the Primary Coolant System results in a Primary Coolant System pressure transient as shown on Figure 7-59. The maximum pressure increase is 26 psi and occurs approximately 4 seconds following trip. Since reactor outlet temperature is decreasing during the entire transient following trip, the primary system temperature increase is due entirely to the increase in steam generator pressure, causing an increase in primary coolant temperature exiting from the steam generators.

At four seconds following reactor trip, core heat flux is decreasing at a faster rate than primary coolant temperature exiting from the steam generators is increasing; and therefore, the Primary Coolant System pressure begins decreasing as shown in Figure 7-59.

If it is postulated that the pressurizer fills solid with water, owing to a malfunction in the pressurizer level control system concurrent with the assumption of no operator response to the various alarms and indications available, the maximum Primary Coolant System pressure during the transient is well below the hydrostatic test pressure of 3,125 psia. Because of the rapid response of the reactor protection system in causing a reactor trip at 2,255 psia, and because of the large heat sink supplied by the 241,000 pounds of liquid stored in the steam generators, the maximum pressure during the transient is 2,426 psia; and operation of the pressurizer safety valves is not required.

7.5.3.5 Steam Dump and Bypass

The steam dump valves can be operated from either the control room or from the engineered safeguards local panel. Automatic or manual control is provided at the control room station.

Inadvertent opening of the atmospheric dump valves is prevented by requiring that the turbine stop valves be closed before the dump valves can be opened. Excessive primary system cooldown by the dump valves when in automatic control is prevented by a narrow-range T_{avg} temperature signal which has a minimum output corresponding to 515°F.

Turbine bypass is available whether the turbine valves are open or closed and will limit the maximum steam pressure to 900 psia during hot standby.

7.5.3.6 Turbine Generator Controls

The electrohydraulic control used, is a conventional control system with many unit-years of operating experience. This type control has been refined and has proved to be very reliable and superior to earlier controls.

With the redundancy and safety features designed into the turbine control and protection system as described below, the probability of turbine overspeed occurring is very remote.

The steam required to produce turbine overspeed has to come from either the main steam system or flashing from feedwater heaters and moisture separators after a turbine trip. All feedwater heaters with sufficient energy to overspeed the turbine have extraction nonreturn valves and the moisture separator outlets have intercept valves to limit steam flow following a turbine trip. To have an uncontrolled source of steam from the main steam line, all of the following turbine control devices would have to fail:

1. Main governor and governing valves.

2. Overspeed protection controller. This is an acceleration response device which closes the turbine main governing valves and moisture separator intercept valves.

3. Mechanical overspeed trip. This is a centrifugally actuated device which trips the turbine main stop, control, reheat stop and intercept valves (16 valves total).

The main governor and overspeed protection controller both control high-pressure fluid system which provides the motive force to operate the turbine steam valves. The high-pressure fluid system consists of duplicate oil pumps, filters and heat exchangers. The fluid reservoir is stainless steel to minimize the possibility of contamination.

The mechanical overspeed trip actuates the auto stop oil system which uses turbine oil as the control medium and is separate from the high-pressure fluid control system used for the main and auxiliary governing systems.

The turbine main stop and governing valves, and moisture separator intercept and reheat stop valves are all spring-loaded to fail closed.

The turbine overspeed event has been analyzed in Section 5.5.

7.6 NUCLEAR STEAM SUPPLY SYSTEM INSTRUMENTATION

This section primarily describes nonsafety-related instrumentation relevant to the systems discussed in Sections 7.2, 7.3 and 7.5. Safety-related instrumentation for these sections and Section 7.4 are mentioned only for clarity of text.

7.6.1 DESIGN BASES

7.6.1.1 Process Instrumentation

The nuclear steam supply system (NSSS) nonnuclear process instrumentation measures temperatures, pressures, flows and levels in the Primary Coolant System, secondary system, NSSS auxiliary systems and measures containment parameters such as pressure, sump level, hydrogen content, and gamma radiation. Process variables required on a continuous basis for start-up, operation and shutdown of the Plant are indicated, recorded and controlled from the control room. Other instrumentation which is used less frequently or which requires a minimum of operator action is located near the equipment with remote alarms annunciated in the control room. Alternate indicators and controls are located at other locations than the control room to allow reactor shutdown and cooldown should the control room have to be evacuated as described in Section 7.4.

Four independent measurement channels are provided to monitor each process parameter required for the Reactor Protective System (refer to Section 7.2). Redundant channels are provided for engineered safeguards action to meet the single failure criterion (refer to Section 7.3). The four independent channels provide sufficient redundancy to ensure system action and to allow each channel to be tested during Plant operation. Class 1E instruments listed in Table 5.7-7 are designed to withstand seismic loads described in Section 5.7 and have been environmentally qualified when applicable as described in Chapter 8, Subsection 8.1.3.

Two independent channels are provided to monitor parameters required for critical control functions (refer to Section 7.5).

7.6.1.2 Nuclear Instrumentation

Eight channels of instrumentation are provided to monitor the neutron flux. The system consists of four power range safety channels, and two source range channels combined with two wide range channels. The source/wide range channels share high sensitivity fission chambers, enclosure, and power supply; while the power range channels are completely independent with each channel complete with separate detectors and power supplies. Each power range safety channel is also provided with a rod drop detection circuit and provides calibrated flux, upper and lower signals to its channelized thermal margin monitor and non-channelized critical function multiplexor. The operating range of the eight monitoring channels is greater than ten decades of neutron flux with channel overlap adequate to monitor the reactor power from shutdown through start-up to 200% of full power(10^{-8}% to 200% of full power). See Figures 7-8 and 7-9 for channel range and overlap.

The neutron flux detectors are located in instrument thimbles in the biological shield around the reactor vessel. Each start-up and wide-range detector is placed approximately 180° apart. The power range safety channel detectors are placed in thimbles approximately every 90° around the core.

7.6.1.3 Control Rod Position Instrumentation

The Palisades Plant Computer is a distributed computer system composed of a host computer and several nodes. Two of these nodes are the PIP node and the SPI node. The SPI system, composed of the SPI node plus the host computer, is redundant to the PIP node in the tasks of control rod measurement, control rod monitoring, and limits processing.

The PIP Node ("PIP") uses the output of a synchro to provide the rod position. Each of the 45 control rods has a synchro. Control rod position is visually displayed on a control room panel. This information is also passed to the host Computer and to the control room workstation. Position information is also used to initiate alarms under certain limiting conditions, to provide contact closures for control rod sequencing and control, and to monitor for excessive control rod position deviation between individual rods within a group. The PIP is capable of measuring and recording the time for a control rod to reach bottom after the control rod clutch is released during a control rod drop test.

The SPI system ("SPI") consists of the SPI node plus the host computer. The SPI node functions as an input module and all processing of information is done in the Host Computer. The SPI node gathers information on the control rod positions from the reed stack switches. Each of the 45 control rods has a reed switch stack. The host computer monitors the various limits associated with the control rods. These limits include the PDILs and rod sequencing. If a limit is exceeded, an alarm is annunciated on the control room workstation. It does this monitoring using the rod positions from the synchro transducers. If a synchro input card on the PIP were to fail, the host computer would use the rod position from the SPI input module in the monitoring of rod limits. The host computer also compares the position of the rod position from the synchro transducer and the rod position from the reed stack switches. If there is deviation in the positions greater than a preset limit, an alarm is annunciated on the control room workstation.

7.6.1.4 Incore Instrumentation

The primary function of the incore instrumentation is to provide measured data which may be used in evaluating the neutron flux distribution in the reactor core. This data may be used to evaluate thermal margins and to estimate local fuel burnup.

The bases for the design of the incore monitors are as follows:

1. Detector assemblies are installed in the reactor core at selected locations to obtain core neutron flux and coolant temperature information during reactor operation in the power range.

2. Flux detectors of the self-powered type, with proven capabilities for incore service, are used.

3. The information obtained from the detector assemblies may be used for fuel management purposes and to assess the core performance. It is not used directly for automatic protective or control functions, however it is used for ex-core instrument calibration.

4. The output signal of the flux detectors will be calibrated or adjusted for changes in sensitivity due to emitter material burnup.

5. The detector assemblies are comprised of local neutron flux detectors (stacked vertically for axial monitoring) and a thermocouple.

Axial spacing of the detectors in each assembly and radial spacing of the assemblies permit representative neutron flux mapping of the core and monitoring of the fuel assembly coolant outlet temperatures.

The incore instrumentation is required to measure radial peaking factors for Technical Specifications limits monitoring. This assures that the assumptions used in the analysis for establishing DNB margin, linear heat rate and the TM/LP and high-power Reactor Protective System trip set points remain valid during operation.

The incore instrumentation must also provide a diverse monitoring of reactor core quadrant power tilt and linear heat rate, both parameters being monitored also by the excore nuclear instrumentation (Subsection 7.6.1.2). This diversity of monitoring assures that, in the event of an LOCA, the peak fuel cladding temperature will be acceptable and the minimum DNB will be maintained above acceptable levels (fuel damage will not exceed acceptable limits) during anticipated transients. Quadrant power tilt and linear heat rate are limited by Technical Specifications. Linear heat rate is monitored in the control room normally via the incore alarm system. When required, the quadrant power tilt is determined from calculations involving incore detector readings.

Sixteen of the incore detectors are provided with electrical connectors and cabling inside containment which has been environmentally qualified to the requirements of IEEE 323-1974. This provides assurance that the sixteen core exit thermocouples (4/core quadrant) will be available to provide indication of the approach to inadequate core cooling conditions following postulated accident conditions. Design of these core exit thermocouple instrument loops meets the intent of NUREG-0737 and Regulatory Guide 1.97.

7.6.1.5 Palisades Plant Computer (PPC)

This monitoring system is provided to display, print, and store plant process information. Functions provided include Sequence of Events (SOE) monitoring, Safety Parameter Display System (SPDS) and Emergency Response Data-link System (ERDS). It is part of and provides services to the PIP/SPI control rod monitoring system described elsewhere. It provides a link between the Incore neutron inputs and Incore analysis software.

Sequences of events for safety- and non-safety-related Plant parameters of the following systems are monitored, displayed, and recorded.

1. Reactor Protective System
2. Engineered Safeguards Controls
3. Reactor Shutdown Controls
4. Fluid Systems Protection
5. Regulating Controls
6. Primary Plant Process Instruments
7. Secondary Plant Process Instruments
8. Electrical Power Distribution

The PPC is a non-class 1E monitoring system.

The PPC includes and conforms to Critical Functions Monitoring System (CFMS) design. This design provides concise display of important parameters to control room operators. The PPC is designed to provide the same information to the Technical Support Center (TSC) and Emergency Operations Facility (EOF) to aid in emergency response management. The CFMS is a Safety Parameter Display System as described in Supplement 1 to NUREG-0737. In a letter dated April 19, 1990 the NRC found the Palisades' SPDS to be acceptable on the basis that it meets NUREG-0737 Supplement 1 requirements (References 11 and 12).

The PPC typically interfaces with Class 1E systems through electronic isolation devices, 100K ohm isolation resistors, relay contacts and the CFMS input termination/ multiplexer cabinets located in the control room. The CFMS input control cabinets are designed to be seismically qualified to the criteria of IEEE 344-1975. The CFMS input cabinets also provide for separation and isolation of Class 1E and Nonclass 1E equipment in accordance with the requirements of IEEE 384-1977.

The SOE node, Cooling Tower Control System (CTCS) node, PIP node, SPI node and the D204 Battery backed power system include components located in the CP Co Design Class I portion of the auxiliary building and, as such, are required to be housed in cabinets qualified as Seismic Category I per Regulatory Guide 1.29 to prevent damage to other equipment through structural failure. This system has been classified as functional Nonclass 1E, as such interfaces of Class 1E components with the system must meet IEEE 384-1977 and be in accordance with 10 CFR 50, Appendix A, GDC24.

7.6.2 SYSTEM DESCRIPTION

7.6.2.1 Process Instrumentation

The following process instruments are associated with the reactor protective, reactor control or primary Plant controls. They are safety related or nonsafety related as indicated.

Temperature - Temperature measurements are made with precision resistance temperature detectors (RTDs) which provide a signal to the remote temperature indicating control and safety devices. Class 1E temperature channels in each primary reactor coolant leg are provided power from separate preferred ac buses.

The following is a brief description of each of the temperature measurement channels:

1. Hot Leg Temperatures - Class 1E

   Each of the two Primary Coolant System hot legs contains four safety grade temperature measurement channels. Each of these channels provides a narrow-range (515°F-615°F) temperature signal to the thermal margin monitors which input to the reactor protection system. Two of these channels on each hot leg also provide wide-range (50°F-700°F) temperature signals to the subcooled margin monitors discussed in Subsection 7.4.6.1.

   One of these channels from each loop provides narrow range input through an isolation device to the temperature computing station and an indicator as discussed in section 7.5.2.1. Both the narrow-range and wide-range signals are obtained from the same RTD through use of a dual-range RTD transmitter.

   Indications for each of the narrow-range temperature channels are provided in the control room. Indication of one of the wide-range temperature channels on each hot leg is provided in the control room and at the auxiliary hot shutdown control panel (C-150). Two of the wide-range hot leg temperature channels are also available in the Critical Function Monitoring System (CFMS) computer.

2. Hot Leg Temperature - Nonclass

   A hot leg control grade signal is obtained from a safety channel through an isolation device for each hot leg. These channels provide a narrow range signal (515°F – 615°F) to the temperature computing station. Indication of the control grade temperature measurements for each hot leg is provided in the control room. A high temperature alarm is provided by these channels to alert the operator to a high temperature condition.

3. Cold Leg Temperature - Class 1E

   Each of the four Primary Coolant System cold legs contains two safety grade temperature measurement channels. Each of these channels provides a narrow range (515°F-615°F) temperature signal to the thermal margin monitors which input to the reactor protection system. A T_C alarm is initiated by the thermal margin monitors if the maximum monitors T_C (Class 1E) exceeds a T_C max or T_C min operator adjustable set point. One of these channels on each cold leg provides wide-range (50°F-700°F) temperature signals to the subcooled margin monitors discussed in Subsection 7.4.6.1. One of these channels from each loop provides narrow range input through an isolation device to the temperature computing station and an indicator as discussed in Section 7.5.2.1. One of these channels from each loop provides wide range input through an isolation device to LTOP. Both the narrow-range and wide-range signals are obtained from the same RTD through use of a dual-range RTD transmitter.

   Indications for each of the narrow-range temperature channels are provided in the control room. Indication of one of the wide-range temperature channels from each Primary Coolant System loop is also provided in the control room and at the auxiliary hot shutdown control panel (C-150). One wide-range channel from each of the four cold legs is available in the CFMS computer.

4. Cold Leg Temperature - Nonclass

   A cold leg control grade signal is obtained from a safety channel through an isolation device for each cold leg. These channels provide a narrow range signal (515°F – 615°F) to the temperature computing station.

5. Loop Average Temperature

   Loop average temperature is computed through the computing station in each loop. The computing station receives inputs from the control channel hot and cold leg temperatures. It outputs to a control room recorder.

   A single recorder provides indications of the temperature outputs of both loop computing stations. The recorder provides indication of loop average temperature (T_{AVE}), programmed reference temperature (T_{REF}) and loop differential temperatures for each loop.

6. Loop Differential Temperature

   The loop differential temperature (Nonclass 1E) is computed from the control channel hot leg and cold leg temperature detector signal. Each loop differential temperature is recorded in the control room.

Pressure - Pressure is measured by electronic pressure transmitters. The transmitter produces a dc current output that is proportional to the pressure sensed by the instrument. The dc current outputs are used to provide signals to the remote pressure indicating control and safety devices.

The following is a brief description of each of the pressure measurement channels:

1. Pressurizer Pressure (Protective Action) - Class 1E

   Four pressurizer pressure transmitters provide independent suppressed range pressure signals for initiation of Reactor Protective System trips on high-pressure and low thermal margin. In addition to the above trips, signals are provided for initiation of safety injection.

   These four independent pressure channels provide the signals for the Reactor Protective System high-pressure trip and the variable thermal margin/low-pressure trip. These channels also provide the low-low-pressure signal to the safety injection units. All four pressure channels are indicated in the control room and high, low, and low-low alarms are annunciated. Each channel is provided power from a separate preferred ac bus.

2. Pressurizer Pressure (Control and Indication) - Class 1E

   Redundant narrow-range pressure channels are provided for overpressure interlocks on the suction line valves for shutdown cooling. These interlocks provide additional assurance that the high-low pressure interface between the Primary Coolant System and the Shutdown Cooling System is not breeched when the Primary Coolant System is pressurized above the design pressure of the Shutdown Cooling System. These narrow-range pressure channels also initiate opening of the PORVs (less than 600 psia) when required for overpressure protection of the Primary Coolant System at low temperatures (see Subsection 7.4.2.1). Indication and recording of these narrow-range pressure channels is provided in the control room. Power to the pressure channels is provided from separate preferred ac buses.

Redundant wide-range pressure channels initiate opening of the PORVs (greater than or equal to 600 psia) when required for overpressure protection of PCS at low temperatures and provide for indication of Primary Coolant System pressures as recommended by Regulatory Guide 1.97. Components of these channels located in a harsh environment are qualified to the requirements of IEEE 323-1974 to provide assurance that the indicating loops will continue to function during post-accident conditions. These pressure channels also provide input to the subcooled margin monitors described in Subsection 7.4.6.1.

3. Pressurizer Pressure (Control and Indication) Nonclass

   Two independent pressure channels provide suppressed range signals for control of the pressurizer heaters and spray valves during normal operations. The output of either pressure control loop may be selected for primary pressure control by a selector switch located in the control room. These pressure channels are indicated and recorded in the control room and are powered from independent preferred ac buses.

   Level - Level is sensed by level transmitters which measure the pressure difference between a reference column of water and the pressurizer water level. This pressure difference is converted to a dc current signal proportional to the level of water in the pressurizer. The dc current outputs of the level transmitters provide signals to the remote level indicating, control and safety devices.

The following is a brief description of each of the level measurement channels:

1. Pressurizer Level

   Two Nonclass 1E independent pressurizer level transmitters provide signals for use by the chemical and volume control charging and letdown system. In addition, signals are provided for pressurizer heater override control. These level transmitters are calibrated for steam and water densities existing at normal pressurizer operating conditions.

   The two pressurizer level control channels each provide a signal for recorders in the control room. One pen records actual level as sensed by the level control channel and the other pen records the programmed level set point signal as calculated by the level controller. The recorder also records pressurizer pressure channels as discussed above.

One Class 1E pressurizer level transmitter provides a signal to a control room indicator. Indication is provided also on the Auxiliary Hot Shutdown Control Panel C-150. The level transmitter receives power from a preferred ac bus. The level transmitter is calibrated for cold conditions in the Primary Coolant System.

Pressurizer level is also measured by a second Class 1E level transmitter which indicates in the control room and on the Engineered Safeguards Auxiliary Panel C-33. This level transmitter is calibrated for cold conditions in the Primary Coolant System.

2. Steam Generator Level

Each steam generator has four Class 1E narrow-range level transmitters for Reactor Protective System channels and two Nonclass 1E transmitters for control function. Each protection channel is provided with physically separated sensing taps. Each channel has level indication in the control room. One of the four indications is also located on the Auxiliary Hot Shutdown Control Panel C-150. In addition, two Class 1E wide-range level channels per steam generator are available to ensure proper monitoring of steam generator level during operation with auxiliary feedwater (see Subsection 7.4.3.2). Indication from these last channels is located in the control room.

Flow - An indication of primary flow is obtained from measurements of pressure drops across each steam generator. These pressure drops are sensed by differential pressure transmitters which convert the pressure difference to dc currents. The dc currents provide a signal to the remote flow indicating and safety devices.

The following is a brief description of the flow measurement channels:

1. Primary Coolant Loop Flow Rates

Four independent Class 1E differential pressure transmitters are provided in each loop branch to measure the pressure drop across the steam generators. The outputs of one of these from each loop branch are summed to provide a signal of flow rate through the reactor core, which is indicated and supplied to the Reactor Protective System for loss-of-flow determination. The differential pressure sensed by each transmitter is indicated in the control room. The arrangement of the flow transmitters is shown on Figure 7-6.

7.6.2.2 Nuclear Instrumentation

Introduction - The Nuclear Instrumentation System consists of eight channels.

The combined source/wide range channels and power range safety channels are located in the Reactor Protective System cabinet in the control room. Four cabinets designated as A, B, C and D each house one channel of the protective system. Cabinets A and B each contain one power range channel. Cabinets C and D each contain one source/wide range channel and one power range safety channel. Mechanical and thermal barriers between the cabinets reduce the possibility of common event failure. The source and wide-range detector cables of a channel originate from the same preamp and are routed in the same cable tray. Each redundant source/wide range channel is separated and fed through different penetrations. The power range safety channel detector cables are routed separately from each other including penetration areas. The nuclear detector locations are shown in Figure 7-60.

The source range indications are derived from dual independent high sensitivity fission counters. The detector output signals from this dual fission chamber arrangement are amplified, discriminated and summed at a remotely mounted preamplifier. This conditioned signal is input to the source level source rate circuitry located in the control room. Audible count rate signals are available in the control room and in the containment building.

The wide range indications receive signals from one of the dual high sensitivity fission counters used also for source range detection. The detector signal is preamplified before input to the count rate and Campbell circuits in the source/wide range drawer.

Four channels are designated as power range safety channels and are connected to the Reactor Protective System. These channels operate from 0% through 125% of full power. Instantaneous nuclear power signals are input to the Thermal Margin Monitor (TMM) for use in variable high-power trip, thermal margin/ low-pressure set point calculation and axial shape index alarm. Each of these four channels contains detectors consisting of dual-section ion chambers which monitor the axial length of the reactor core at four circumferential positions. They can detect axial flux imbalance conditions as calculated by the TMM axial shape index alarm. Comparison between the channels allows detection of radial flux imbalance. The gain of each power range channel is adjustable to provide a means for calibrating its output against a Plant heat balance.

The system is generally designed in accordance with the following criteria:

1. The nuclear instrumentation sensors are located so as to detect representative core flux conditions.

2. Multiple channels are used in all flux ranges.

3. The channel ranges overlap sufficiently to assure that the flux is continually monitored from source range to 200% of full power.

4. The power range safety channels are classified as 1E and are an integral part of the Reactor Protective System input channels.

5. Each of the power range safety channels is physically separated from the others. Left and right channels of each source/wide range channel are separated from each other.

6. Uninterrupted power is supplied to the system from four separate ac buses. Loss of a channel bus will disable one power range, and in the case of channels C and D, one source/wide range channel.

7. All channel outputs are buffered so that accidental connection to 120 volts ac, or to channel supply voltage, or shorting individual outputs does not have any effect on any of the other outputs.

Source Range Indication - The source range nuclear instrumentation portion uses a pulse signal from a pair of high sensitivity fission chambers. The use of two detector elements within the detector assembly permits high neutron visibility while operating in gamma fluxes up to 200 rem/h. System reliability is improved through the use of integral coaxial detector cables housed in a high-pressure moisture barrier. The output of each detector is amplified and summed in a remotely mounted preamplifier. The pulse signals are also discriminated against gamma pulses and again amplified to drive 300 feet of cable between the amplifier and signal processing drawer in the control room. Here, the pulse input is converted to a signal proportional to the logarithm of count rate. This signal drives a front panel meter, a remote recorder, and a remote meter (all 0.1 cps to 10^5 cps). An audio signal proportional to the count rate is connected to control room and containment loudspeaker. The channel also provides a shaped pulse output for attachment of a scaler.

The source range signal is differentiated to provide rate-of-change of power information (-1 to +7 decades/minute). This rate signal feeds a front panel meter, and a remote meter.

Internally generated pulse signals are available for testing count rate circuitry at predetermined cardinal points. A fixed ramp test signal is available for testing the rate-of-change circuitry.

No automatic protective function is assigned to the source range instrumentation portion.

Wide Range Indication - The wide range nuclear instrumentation portion uses Campbelling techniques and conventional pulse counting techniques to permit the single channel to monitor over 10 decades of flux from 10^{-8}% full power to 200% full power. A single high-sensitivity fission chamber is used as the detecting element. Pulses from the detector pass to a remotely mounted amplifier where they are amplified for transmission to the signal processing drawers.

The amplifier drives approximately 300 feet of cable between the detector and the signal processing drawer in the control room. At the signal processing drawer, the pulse signal is simultaneously applied to two separate detection and amplification circuits. One circuit consists of a pulse counting circuit. The other circuit uses the ac component of the chamber signal rather than the dc component of the signal.

Using Campbell's Theorem, it can be shown that the output of square law detection of the ac portion of a random pulse signal is proportional to the pulse rate (see Reference 3). Because square law detection is used, the smaller gamma pulses produce a very small contribution to the overall signal. Within the mean square portion of the channel, the pulse signal is fed to a band-pass amplifier, a rectifier and filter and a dc log amplifier. The band-pass amplifier and rectifier provide effective square law detection. The output of the pulse counting type circuit is effective over the first five decades. The mean square circuit is effective over the remaining five decades.

By using the two techniques in one channel, a dc signal proportional to the logarithm of neutron flux over approximately ten decades is obtained. This signal drives a front panel meter (10^{-8}% full power to 200% full power), a remote meter, a remote recorder and trip units.

The log level signal is differentiated to provide rate-of-change of power information from -1 to +7 decades/minute. The rate signal feeds a front panel meter, a remote meter and trip units.

Detector high voltage is also monitored by a trip unit which initiates an alarm on decrease of detector voltage or channel trouble.

Channel test and calibration are accomplished by internally generated test signals. Pulse rates controlled by a crystal oscillator, check the count rate portion of the circuitry, and the mean square portion of the circuitry.

A ramp signal is available for check of the rate-of-change circuitry.

Each source/wide range channel contains eight trip units. Operation of the trip units is according to Table 7-3.

The contact output of each trip unit is fed to a single channel of the Reactor Protective System. Thus, with two source/wide range channel portions, a separate rate trip signal is fed to Channels A, B, C and D of the Reactor Protective System. The < 10^{-4}% of full power rate-of-change bypass is initiated by the wide-range channel level signal. The level signal is fed to two trip units set to trip above 10^{-4}%. Contacts from each trip unit open above 10^{-4}% to remove the rate trip bypass and enable ΔT power block in TMM via Relay K26 and to remove the zero power manually actuated bypass associated with a single channel (see Subsection 7.2.5.2).

The > 15% full power rate-of-change trip bypass and LPD alarm enable for a particular channel are initiated by a trip unit in the power range safety channel via Relay K25. Above 15% full power, the trip unit resets closing a contact of Relay K25 in parallel with the rate trip contact associated with that channel (A, B, C or D). This method of rate trip bypass permits maximum independence of rate trip channels.

The rate-of-change of power pretrip alarm utilizes a single trip unit (containing two sets of relay contacts) in each wide-range logarithmic channel. Each set of contacts feeds an auxiliary trip unit in one of the channels of the Reactor Protective System. The auxiliary trip unit in turn initiates the control rod withdrawal prohibit signal and pretrip alarm. The signal to the auxiliary trip unit is bypassed below 10^{-4}% and above 15% of full power to avoid spurious alarms and control rod withdrawal prohibits.

Power Range Safety Channels - The four power range channels measure flux linearly over the range of 0% to 125% of full power. The detector assembly consists of two uncompensated ion chambers for each channel. One detector extends axially along the lower half of the core while the other, which is located directly above it, monitors flux from the upper half of the core. The upper and lower sections have a total active length of 12 feet. The dc current signal from each of the ion chambers is fed directly to the control room drawer assembly without preamplification. Integral shielded cable is used within the region of high neutron and gamma flux.

The signal from each chamber (lower and upper detectors, Subchannels L and U, respectively) is fed to independent linear amplifiers (Figure 7-9). The output of each amplifier is indicated, compared and summed. The outputs of the L and U subchannels are sent to the thermal margin monitor for calculation of the ASI function. Internal to the drawers, the subchannel signals are summed. Signals are sent to the comparator averager, rod drop detection circuit, remote power level recorder/indicators, critical function multiplexor, and thermal margin monitor for VHPT, TM/LP and LPD function calculations.

The output from the comparator averager (grand average) is returned to each channel drawer and compared to each channel via two deviation comparators. Variable deviation set points are calculated from the grand average core power in the comparator averager using deviation set point potentiometers. The set point signals are entered in the deviation comparators for alarm setting at two levels. The two levels of deviation are alarmed at the channel drawer and also by remote alarms as percent average core power radial (quadrant) flux tilt, Level l, or Level 2, for operator action to ensure the Technical Specifications limits on radial peaking factors are observed.

The 0%-125% full-scale output of the power range safety channels is fed to the comparator averager which computes the grand average power level of all four channels, and to the trip unit which disables the logarithmic channel rate trip above 16.5% full power which also enables the ΔT power in the TMM. The summing circuit also has an X2 gain selector switch which disconnects the input of one ion chamber and doubles the gain for the other ion chamber to allow full-scale power indication should one ion chamber fail.

Channel calibration and test is accomplished by an internal current source which checks amplifier gain and linearity. A check of the level trip set point is provided by a current signal which is added to the normal detector output.

Each power range channel contains a single bistable trip unit set at 15% power. Operation of the trip units is according to Table 7-4.

Power Monitoring - In addition to panel meters for decades per minute (DPM) and percent power (logarithmic scale) from, respectively, the start-up and wide-range channels, wide-range linear percent power meters are provided fed from the wide-range channels. All the external metering equipment is considered as nonsafety related because it is for operator control information only and is isolated from safety-related equipment in accordance with IEEE 384-1977.

7.6.2.3 Control Rod Position Instrumentation

PIP Node - The PIP node measures control rod positions by use of synchros. Outputs are provided for visual display on the main control board and for control rod control.

The major components are:

1. Forty-five control rod position synchros (one per control rod)

2. One node (PIP) containing a VAX computer and an input multiplexer

3. Seven visual displays with seven switches to select control rods within a group

The synchro for each control rod is geared to the control rod drive shaft below the control rod clutch. Full control rod travel corresponds to 264° of synchro rotation. Synchro output is transmitted to the PIP node which scans and converts synchro outputs into inches of control rod withdrawal. The resolution of this system is approximately ± 0.5 inch.

The PIP, located in the main control room area, performs the following functions:

1. Converts the signal from the synchros to control rod positions and checks these positions against limiting positions

2. Initiates alarms and interlocks under certain limiting control rod positions as detailed in Subsection 7.5.2.1 (control rods at upper and lower control rod stops, regulating control rods at prepower and power dependent insertion limits, 4 inch and 8 inch deviations within a group, and control rod groups out-of-sequence.)

3. Provides contact outputs under other control rod positions as detailed in Subsection 7.5.2.1 (these outputs are used as permissive conditions in the regulating control rod sequencing controls)

4. Provides visual displays of the control rod positions on the main control board

5. Calculates the control rod drop times

The operator normally has two means of displaying control rod positions from the PIP node:

1. Seven visual displays are mounted above the control rod drive controls on the main control console. There is one display for each control rod group; a selector switch at each display will allow position of any control rod in that group to be indicated.

2. The control room workstation. Selected screens on this workstation will display the synchro rod positions.

SPI System - The SPI system ("SPI") consists of the SPI node plus the Host Computer. The SPI node functions as an input multiplexer and all processing of information is done in the Host Computer. The SPI node measures control rod positions by use of control rod-actuated magnetic reed switches. The reed switch stack contains a number of series resistors to form a voltage divider network with reed switches connected at each junction. This stack is attached to the control rod extension housing. A magnet on top of the control rod extension will actuate the reed switches as the control rod moves. The output signal depends on the particular reed switch that is closed. The signal is directly proportional to control rod position. The resolution of the signal is ± 1.5 inches.

The outputs from all reed stacks are sent to the host computer. The host computer performs the following functions related to the control rods:

1. Initiates alarms under certain limiting control rod positions as detailed in Subsection 7.5.2.1 (control rods at upper and lower control rod stops, regulating control rods at prepower and power dependent insertion limits, 4 inch and 8 inch deviations within a group, and control rod groups out-of-sequence.)

The SPI system is completely independent of the PIP node as far as rod monitoring is concerned. If the PIP node were to fail, the SPI system would use the reed stacks in monitoring and processing of rod positions and limits.

Interlocks and Limit Signals - Limit switches independent of either the PIP node or SPI system are provided within the control rod drive mechanism. These switches, which are controlled by cams on the control rod synchro shaft, provide shutdown control rod insertion limit signals (interlock function discussed in Subsection 7.5.2.1) and control rod upper and lower electrical limit signals.

Additional Control Rod Position Indication - Located on a vertical panel immediately behind the main control console, is a group of 45 light displays arranged in a shape corresponding to the control rod distribution. Each display, which represents one control rod, contains four different colored lights. These lights give individual control rod information as indicated in Table 7-5.

7.6.2.4 Incore Instrumentation

The incore instrumentation consists of a maximum of 43 fixed incore detector assemblies inserted into selected fuel assemblies. Only 43 incore locations out of 45 are available; two locations are reserved for use by the reactor vessel level monitoring system. Each incore detector assembly runs the length of the active core and contains a thermocouple and neutron detectors. Outputs are fed to the SPI node (see Subsection 7.6.2.3) in the control room.

The thermocouples are of Inconel sheathed, Chromel-Alumel construction and are located at the top end of each incore detector assembly so that the primary coolant outlet temperatures may be measured. The neutron detectors in the assemblies are short rhodium detectors equally spaced. These units with their cabling are contained inside a 0.311-inch nominal diameter stainless steel sheath. Sixteen of the detectors are provided with environmentally qualified electrical connectors and cabling inside containment to provide increased reliability of the thermocouple readout for monitoring the potential approach to inadequate core cooling conditions. The readout from these thermocouples goes through the Cutler-Hammer (CFMS) multiplexer and not the SPI node. Assemblies are inserted into the core through eight instrumentation ports in the reactor vessel head. Each assembly is guided into position in an empty fuel tube in the center of the fuel assembly via a fixed stainless steel guide tube. The seal plug forms a pressure boundary for each assembly at the reactor vessel head. The neutron detectors produce a current proportional to neutron flux by a neutron-beta reaction in the detector wire. The emitter, which is the central conductor in the coaxial detector, is made of rhodium and has a high thermal neutron capture cross section. The rhodium detectors are 40 cm long and are provided to measure flux at several axial locations in fuel assemblies. Useful life of the rhodium detectors is expected to be about three years at full power, after which the detector assemblies will be replaced by new units.

The information received by the SPI node is forwarded to the Host Computer. The host computer is where the processing of the incore information occurs. The host:

1. Corrects the raw incore values for detector burnup.
   (A detector background correction is made in the SPI node.)

2. Compares these corrected values to preset alarm limits. This comparison facilitates the monitoring of reactor core radial peaking factors, quadrant power tilt, and linear heat rate.

3. Initiates an alarm if the limits are exceeded.

Verification of incore channel readings and identification of inoperable detectors are done by correlation between readings and with computed power shapes using a computer program. The incore alarm system operability can be monitored through the SPI trouble alarm on the main control room panels and an alarm on the workstations.

Quadrant power tilt and linear heat rate can be determined from the excore nuclear instrumentation (Subsection 7.6.2.2), provided they are calibrated against the incore readings as required by the Technical Specifications. Quadrant power tilt calibrations of the excore readings are performed based on measured quadrant power tilt calculated using the incore monitoring system which determines tilts based on symmetric incore detectors or integral power in each quadrant of the core (Subsection 3.3.2.5). Linear heat rate calibration of the excore readings involves two intermediary parameters, axial offset and allowable power level, which can be determined by the incore readings. The Technical Specifications give limits on these parameters above a certain reactor power level to ensure that the core linear heat rate limits are maintained while using the excore instruments.

7.6.2.5 Palisades Plant Computer

System Layout - The plant computer consists of four intelligent input nodes, one direct connected multiplexor, multiple display workstations, printers and interconnecting hardware. The plant computer is a distributed system which communicates via Ethernet. There are separate Ethernet cabling systems for the Input nodes and for the Man Machine Interfaces.

The Man-Machine-Interfaces are Computer Workstations. At the very least, there are workstations in the Control Room, TSC, and EOF. The host computer in the CFMS trailer distributes all data to the workstations. Page printers are located in the Control Room (CR), TSC, and EOF for prints of the workstation screens and reports from the host computer.

Four input nodes, PIP, SPI, SOE, and CTCS, are combinations of an input multiplexor and a computer. These nodes perform input processing including Analog to Digital Conversion, Sequence of Events time-stamping, and engineering units conversion. This processed data is assembled and passed to the Host computer. The host computer in turn performs alarm processing, event logging, historical recording and database distribution functions based on this data. Two nodes, the PIP and CTCS nodes, perform additional software tasks such that control rod monitoring and Cooling Tower Fans can be operated independent of host computer operability. The host computer runs several custom software modules such as CFMS processing, Incore monitoring, Rod monitoring, Meteorological data interface, and calculated point processing.

Identification of the PPC components and general location is shown in Figure 7-61. The host computer interfaces, Meteorological, EOF, and the backup alarm printer, are located in the CFMS trailer on the turbine deck. The communications hubs and the SOE node are located in the Cable spreading room below the control room. The control room has at least one permanently located workstation. A page printer is located here. The PIP, SPI, and CTCS nodes are located in the control room also. The Cutler-Hammer input multiplexor is also located in the control room and communicates back to the CFMS trailer directly.

The power supply for the PPC host computer and SOE node includes a 125 volt dc subsystem (one battery, two chargers and one distribution panel) and a dc-to-ac conversion subsystem (two inverters, two static switches) with bypass transformers. Power is taken from the 480-volt MCCs 3 and 4. Only those components required to maintain minimal PPC functionality to the Control room, TSC, and EOF are powered from this system. Extra workstations and non-essential devices are powered from lighting panel power. The CTCS node is powered from the Instrument AC panel Y-01, while the PIP and SPI nodes are powered from the Preferred AC panels Y-20 and Y-40, respectively.

Interfaces - The Reactor Protective System is monitored by the SOE node. The interfaces are both analog and digital. Refer to Subsection 7.2.9.2 for details. Interfaces with the engineered safeguards controls and the Class 1E electrical distribution system are exclusively digital. They are provided via relay contact inputs from these controls, thus ensuring adequate electrical isolation as required by IEEE 384-1977 and 10 CFR 50, Appendix A, GDC24. Interfaces with the reactor shutdown control, and auxiliary feedwater controls are also exclusively digital via relay contacts. Interface with the fluid systems protection is via relay contact to the SOE Node for PRV-1043B and by direct connection from the valve indicating light to the SOE Node for PRV-1042B.

Interfaces with non-safety-related systems (regulating controls, primary and secondary plant process and Nonclass 1E electrical distribution) are both digital and analog. They do not require any special isolation means.

The PPC is comprised of reliable electronic gear fed from an uninterruptible type of power supply. Being a Nonclass 1E system, all safety systems interfaces have isolation means in accordance with IEEE 384-1977 and GDC24 either via relay coil-contact isolation or qualified electronic isolators. As described in Section 5.2, components located in the CP Co Design Class 1 portion of the auxiliary building (the PPC cabinets in the cable spreading room, and certain power supply subsystem components in switchgear room 1D), have been qualified as Seismic Category I (Section 5.7). The system battery enclosure in switchgear room 1D is equipped with a hydrogen evacuation system, V-928, designed to provide a scavenging rate which precludes the formation of an explosive concentration.

The CFMS method or design was carried over from the stand alone CFMS replaced in 1995 into the User interface of the new PPC. The principal software function of the CFMS is to provide concise displays of Plant data, provide for trending of input data and to provide for historical data storage and retrieval. This information is available to system users at each of the various workstations. The CFMS software design provides a hierarchy of displays showing the status of the Plant's critical safety functions. The hierarchy starts with a top-level display showing individual boxes that give an indication of the status of each critical safety function. Lower-level displays give system overviews with current values of important process variables and more detailed mimic diagrams showing system line-up and indicating variables that are in alarm state by use of color of component symbols or variable values. Displays such as the Critical Function Matrix, event and alarm log, trends and others can be accessed with dedicated function keys on the keyboard. A small representation of the Critical Functions Matrix is visible from every display and indicate the overall status of each critical function.

The PPC provides historical storage and retrieval of Process data in order to assist plant personnel in process trending and post-trip or transient recreations. Historical data can viewed in the form of real-time trends, X-Y plots, and statistical reports. Historical data can be archived to disk or tape for later viewing. Sequence of events logs are also archived.

Additional information on the PPC/CFMS is provided in References 6 and 7.

For Cyber Security requirements, the PPC network is logically isolated from the Palisades site business LAN. All PPC data is sent through a deterministic one-way "Data Diode" to computers on the Business LAN. Computer monitoring tools, on the Business LAN, provide the EOF with monitoring capabilities equivalent to Control Room and TSC. Data sent from the Meteorological Monitoring System to the PPC is isolated through an analog to digital circuit.

The PPC via the "Data Diode", provides data to the NRC's Emergency Response Data-link System (ERDS). This data link is capable of sending a preselected group of PPC input variables to the NRC.

7.7 OPERATING CONTROL STATIONS

7.7.1 GENERAL LAYOUT

The operating control stations consist of the control room for centralized control during start-up, normal, shutdown and emergency operations; and auxiliary stations for emergency operation of the engineered safeguards and shutdown systems, normal operation of the radwaste system and normal operation of miscellaneous noncritical systems.

Radiation and shielding design of the spaces in which operating personnel occupancy is required, including adequate access to the vital areas for control of the Plant during and after an accident, has been provided. Refer to Chapter 11 for details of radiation zones.

An onsite Technical Support Center (TSC) is located just outside the control room in an extension to the auxiliary building, provided with dedicated communications with the control room and other centers identified in the Palisades Emergency Plan, including a dedicated display terminal from the Plant Process Computer (Subsection 7.6.2.5). The intent of this TSC is to meet NUREG-0696.

7.7.2 CONTROL ROOM

The control room is accessible from the auxiliary and turbine buildings and houses the control console, vertical duplex boards, cooling tower boards, and switchyard supervisory boards for operation and monitoring of all critical systems. The control console consists of three sections arranged as follows:

1. Center Section - Control devices, indicators and recorders, reactivity regulation, primary coolant components, shutdown cooling and Chemical and Volume Control System.

2. Left Section - Control devices, indicators and controllers for the Engineered Safeguards Systems, Service Water System, Component Cooling System and Containment Air Cooling Systems.

3. Right Section - Control devices, indicators, recorders and controllers for the main turbine and generator and feedwater control systems.

The vertical board is a totally enclosed walk-in panel. One part of the vertical board is arranged in three connected sections with equipment layout and physical separation similar to the control console. The equipment on the front of the vertical panel is located directly behind the console section having devices for that same system. Other control and monitoring equipment for other systems is located on the back of this board and on separate vertical duplex boards. The annunciators for the entire Plant are located across the top of the vertical panels providing visual and audible indication of off-normal conditions requiring operator action.

A program to review the human factors of the control room was initiated in late 1980 in response to NUREG-0660 and NUREG-0737, Supplement 1, and consistent with the guidance provided by NUREG-0700. The objective, as stated in NUREG-0660 was to improve the ability of control room operators to prevent accidents or to cope with them, should they occur, by improving the information provided to them.

Short-term improvements were completed during the 1983 refueling outage while long-term improvements were scheduled for subsequent outages. On September 14, 1989 the NRC issued a final SER on the program. Based on review of the CP Co Summary Report submitted on August 29, 1986 and onsite inspections, the SER concluded that the Palisades Plant meets all the requirements of Supplement 1 to NUREG-0737 for the Detailed Control Room Design Review.

Control console and panel sections listed in Table 5.7-7 and containing Class 1E devices are designed to withstand seismic loads described in Section 5.7. All other panels and equipment in the control room have been anchored to stay in place during a seismic event (see Section 5.10).

The control room is located in the CP Co Design Class 1 portion of the auxiliary building. Sufficient concrete shielding is provided to ensure safe occupancy of the control room during all normal and abnormal Plant conditions. The control room atmosphere is air-conditioned for personnel comfort and equipment cooling using redundant HVAC with Class 1E controls (see Section 9.8). The ventilation system is arranged for outside makeup air to be drawn through absolute and charcoal filters in the event of a DBA. The control room area is provided with an area radiation monitor. Temperature monitors are provided to warn of high temperature conditions in the vicinity of the Reactor Protective System and Engineered Safeguards System panels. These monitors alarm at 110°F since these systems are designed for 120°F ambient.

The present Thermal Margin Monitors (TMM) were originally qualified to 131°F. However, the location in the panel requires fan cooling. Analysis shows that (with forced-air cooling) 131°F is reached by the TMM when the control room ambient temperature is 106°F. Because the TMM portion of the RPS is no longer capable of operating at 120°F, an administrative limit of 90°F was imposed (Reference 9).

The only time that control room temperature is postulated to exceed 90°F would be during a station blackout when temperatures may approach 120°F (Reference 10). Under these conditions, the RPS would not be required to be operable. See Chapter 1 for additional information on station blackout.

All materials of construction used in the control room are noncombustible. Electrical wiring is flame-retardant as proven by applicable vertical flame tests.

Control Room Protection Against Fire

Cables related to safety-related control cabinets and consoles including all the systems required for Plant shutdown penetrate the floor directly into control panels and consoles.

The combustibles in the area consist mainly of electrical wiring insulation contained within the cabinets and a small amount of ordinary combustibles such as paper. An unmitigated fire in one of the control panels would probably be limited to one panel involving only one division of safe shutdown equipment due to the low combustible loading and the physical separation and barriers provided. In the event a larger fire should occur, capability to achieve a safe shutdown includes required instrumentation and centralized controls (Panel C-150) independent of the control room and not affected by a fire in the control room.

In addition, smoke detectors are installed in the walk-in cabinet enclosures and throughout the ceiling of the control room and adjacent offices. Smoke detectors are not installed in the main control consoles since they are designed with outlet ventilation openings at the top which will allow the control room operators to observe any smoke present from a fire.

Other fire protection features are described in the Fire Safety Analyses (Section 9.6.3) for this area.

The control room ventilation system can be controlled manually by the control room operator and will allow shutoff of the fans if smoke was observed entering the control room. Manual operation of the ventilation system for venting the control room is also available.

All cable penetrations into the control room have been sealed with flame-retardant material.

There are no concealed floor or ceiling spaces that contain cables in the control room (area over panels, only).

The control room is not used as a cable right of way.

7.7.3 ENGINEERED SAFEGUARDS AUXILIARY PANEL (C-33)

The engineered safeguards auxiliary panel is located in the auxiliary building. This panel provides a second point of control, outside the control room, for reactor shutdown and contains devices to permit the following emergency operations in the event the control room must be evacuated:

1. Operation of auxiliary feedwater control valves.

2. Monitoring steam generator level.

3. Monitoring pressurizer pressure and level.

4. Operation of boric acid tank.

5. Operation of atmospheric steam dump valves.

6. Initiation of shutdown cooling by control of corresponding valves.

7. Control of component cooling water and service water.

8. Control of the motor-operated valve in the line from the SIRW tank to the suction of the charging pumps. This provides a large backup supply of shutdown concentrated borated water to the Primary Coolant System.

Engineered Safeguards Auxiliary Panel Area Protection Against Fire

The engineered safeguards auxiliary panel is not functional if all cable spreading room or control room equipment is inoperable due to fire. Panel C-150 is provided for such an emergency. The control function available from Panel C-33 is limited to that of positioning of valves. Starting and stopping of motors could be accomplished at the switchgear for each motor. The panel control devices are wired in parallel with the control room devices and thus the effects of control circuit damage would be common to either location. However, a fire damaging the circuitry of one channel would not prevent the ability to control equipment from the other channel from either control location.

Other fire protection features are described in the Fire Safety Analyses (Section 9.6.3) for this area.

7.7.4 AUXILIARY HOT SHUTDOWN CONTROL PANELS (C-150/C-150A)

In order to ensure use of sufficient components of the Auxiliary Feedwater System and sufficient process information to permit reactor hot shutdown control in the event a fire damages equipment and circuitry of the main feedwater system or the Auxiliary Feedwater System in the control room, cable spreading room, Engineered Safeguards Auxiliary Panel C-33 room, or the corridor between Switchgear Room 1-C and the charging pump rooms, Auxiliary Hot Shutdown Control Panels (C-150/C-150A) have been provided and located in the southwest electrical penetration room. These panels are comprised of two enclosures, the main enclosure C-150 and an auxiliary one called C-150A. The description below combines these two enclosures into one entity called "Panel C-150."

From this panel, control of the auxiliary feedwater valves is enabled by transfer (see Figure 7-53 for this transfer system) and control of auxiliary feedwater turbine steam supply Valve B. Indication of auxiliary feedwater flow to both steam generators, water level of both steam generators and pressurizer level are enabled by transfer. In addition, primary coolant pressure (pressurizer pressure) is displayed by a primary sensor dedicated to this use. Transfer of the above-mentioned systems is annunciated in the control room.

Equipment controls provided at control panel (C-150) required by the alternative dedicated method of achieving and maintaining hot shutdown are as follows:

1. Auxiliary feedwater valves

2. Auxiliary feedwater pump turbine-driven steam Valve B

Instrumentation systems displayed on the Auxiliary Hot Shutdown Control Panel are:

1. Source range flux monitor

2. Auxiliary feedwater flow

3. Pressurizer pressure

4. Pressurizer level

5. Steam generator level and pressure

6. Primary coolant temperatures (hot and cold legs)

7. Turbine-driven auxiliary feedwater pump low-suction pressure warning light

8. SIRW tank level

Equipment and equipment housings procured for and utilized to take the Plant to safe shutdown have been specified to be qualified in accordance with IEEE 344-1975 and IEEE 323-1974 when placed within or interfacing with safety systems.

Switches, which transfer control or instrument functions from the control room to the auxiliary shutdown control panel, alarm in the control room when the devices in the Auxiliary Hot Shutdown Control Panel are enabled.

The transfer switches of the Auxiliary Hot Shutdown Control Panel provide access to the Auxiliary Feedwater System for hot shutdown only. No other means of achieving hot shutdown exists if a fire damages the control room or the cable spreading room.

Wiring, including power sources for the control circuit and equipment operation for the alternate shutdown method, is independent of equipment wiring in the postulated fire areas.

Alternate shutdown power sources, including all breakers, have isolation devices on control circuits that are routed through the postulated fire areas, even if the breaker is to be operated manually.

Procedures are provided for taking the Plant to hot shutdown via the Auxiliary Hot Shutdown Control Panel in the event a fire prevents use of the control room.

Spare fuses are available for control circuits where fuses may be required in supplying power to control circuits used for the alternate shutdown method and may be blown by the effects of a cable spreading room fire. The spare

fuses are located convenient to the existing fuses. The shutdown procedure informs the operator to check these fuses.

Testing - Periodic testing of the auxiliary shutdown system will be in accordance with Regulatory Guide 1.22 and IEEE 338.

7.7.5 RADWASTE SYSTEM LOCAL CONTROL PANEL

The Radwaste System control panels are located in the auxiliary building and are accessible through the Access Control. These panels contain all the control and monitoring devices to initiate, control and monitor the Radwaste System components.

7.7.6 MISCELLANEOUS LOCAL CONTROL STATIONS

Miscellaneous noncritical systems are controlled from local stations throughout the Plant.

Off-normal conditions in all systems are alarmed on the respective local panel and on the main control panel annunciators.

7.7.7 FEATURES WHICH ENHANCE SAFE OPERATION

Steel fire barriers are incorporated in the main control console, main control panel, and engineered safeguards auxiliary panel. The barriers are arranged to separate control circuits similar to the separation of equipment power supplies.

All panels and consoles are totally enclosed and constructed from steel plate welded to steel frames. Fire retardance and rigidity for mounted equipment and cabling is provided by this construction.

7.7.8 IN-PLANT COMMUNICATION SYSTEM

The in-plant communication system is comprised of five subsystems: a telephone system, a public address system, an intercommunications system, a sound-powered phone system and an onsite/offsite radio system.

Paging over a Plant-wide public address system is initiated by dialing a preselected number from any of the telephone stations. Plant-wide paging can also be accomplished by a microphone in the control room. Paging from the control room station overrides paging from any other station.

An intercommunications system permits common talking between the control room, the fuel pool area and inside containment as an aid in the fuel handling operation. A closed circuit television system with a screen in the control room aids in monitoring fuel handling.

The sound-powered phone system is intended for equipment test and calibration which require vocal communication between the equipment and control room. It can be used also by personnel in the Technical Support Center during an emergency.

The onsite/offsite radio system includes a base station in the turbine building, a remote base station in the control room for onsite communication with portable transceivers. A repeater unit is located onsite for use by security personnel.

Communications between operators performing manual actions and those providing feedback are not a requirement but rather an enhancement to aid in bringing the plant to either hot or cold shutdown conditions.

7.7.9 OUT-OF-PLANT COMMUNICATION SYSTEM

The telephone system provides normal external communications for the Plant.

Additional offsite communications are provided by the onsite/offsite radio system. This system has offsite communications with the Emergency Operations Center and with a repeater in the site emergency vehicle.

Direct communications with the Michigan State Police are by means of a base station located in the secondary security alarm station. A second remote station is located in the central security alarm station.

All emergency communications are addressed in the Emergency Plan.

7.8 QUALITY CONTROL

For a discussion of the Quality Assurance Program, see Chapter 15.

7.8.1 SPECIFICATIONS

The following tests and inspections were performed as a minimum by the Reactor Protective System supplier:

1. Surface examination
2. Isolation requirements
3. Point-to-point continuity test
4. Insulation test

Upon completion of the above production tests, the following operation tests were performed:

1. Bistable trip unit operating tests
2. Bistable trip unit environmental tests
3. Auxiliary trip unit operating tests
4. Auxiliary trip unit environmental tests
5. Reactor protection system operating tests

The following standards were incorporated in whole or in part in the specifications:

National Bureau of Standards TID-20298 - Standard Nuclear Instrument Modules

IPCEA S-61-402 (NEMA WC-5-1961)

NEMA IC1-2.42

EIA RS-310, Racks, Panels and Associated Equipment

7.8.2 SUPPLIER'S QUALITY CONTROL

The quality control procedures as required by the applicable engineering specification of all vendors to Combustion Engineering Nuclear Power Department (CENPD) were reviewed by the Combustion Engineering (CE) quality assurance organization. The functions and organization of CE quality assurance organization were as given in Chapter 15.

All major components of the Reactor Protective System fabricated by outside vendors were treated in the manner described in the above reference. As such, and as detailed in the above reference, the quality control procedures of the various RPS vendors mentioned above were the responsibility of the manager of quality control of the manufacturing services department.

7.8.3 REACTOR PROTECTIVE SYSTEM SHOP TEST

The complete RPS was tested at the vendor's plant prior to shipment to the jobsite. This test was witnessed and approved as satisfactory by members of the design group of the CENPD. The test was also witnessed by Consumers Power personnel.

The purpose of the test was as follows:

1. To assure that the RPS functions as designed throughout all modes of operation prior to shipment

2. To assure that the nuclear instrumentation system operates properly and is properly interfaced with the RPS

Summary of Tests:

1. Trip Logic Test
2. Test Capability Check
3. Trip Inhibit Test
4. Nuclear Instrumentation Operability Test
5. Nuclear Instrumentation Interface Test
6. Zero Power Mode Test
7. Low Flow Protection Test
8. Miscellaneous Features Test
9. Bus Failure Test
10. Ground Fault Detection Test
11. System Response Time Test
12. Power Demand and Design Data Test
13. Temperature Rise Test

The above tests were performed in accordance with test procedures approved by CE.

7.8.4 SHIPPING AND STORAGE

The cabinet assembly was skid mounted (suitable for sling hoisting) for shipping and was packaged such that it would withstand:

1. Normal handling and weather during shipping without suffering damage

2. Unforeseen prolonged storage conditions in nonair-conditioned warehouse

7.8.5 RELIABILITY

The CE reliability group performed an independent review and analysis of the Reactor Protective System (RPS) during the design phase of the program. A mathematical model of the system was generated and a reliability review followed using the model as a basis for numerical predictions. This consisted of identifying the major reliability components of the design, calculating the electrical operating stresses of each critical item at the environment specified, and calculating the reliability prediction of the bistable trip unit and RPS.

Failure mode effects and sensitivity analysis were performed on each major item to assess the design approach used by the designer and to reveal all areas of potential reliability jeopardy and safety hazards. The results of this analysis highlighted those areas earmarked as critical and effected closer examination of the design by the responsible design engineer into those areas.

Parts and stress application analysis was performed on the electronic components to ascertain proper selection of intended parts, to review their usage in the design, and to assure that each item is properly derated in its application for reliability purposes. A separate review of each applicable detailed drawing and specification for the trip unit BTU and RPS was conducted. Particular emphasis was placed on details for design interfaces and adequacy of controls to assure proper compliance to detail requirements.

7.8.6 RECORDS AND CERTIFICATION

The following records were kept:

1. Trip unit operating and environmental test results

2. Supplier's inspection and test reports

3. Records of all operational tests performed on the system

In addition, complete records were kept on the extensive testing performed on the prototype trip unit developed in the CE laboratories which is identical to the trip units used in the Reactor Protective System.

The following certifications of satisfactory fabrication and test performance were made:

1. Certification that the reactor protection system has been fabricated in accordance with the applicable engineering specifications and references

2. Certification of satisfactory completion of all tests and inspections

7.8.7 FIELD QUALITY CONTROL

Upon receipt of equipment in the field, inspection was made for conformance to specifications, codes and drawings. Checks were made for completeness of shop inspection and material certification if required by specification and/or damage in transit. A record of this inspection was made on a special form. If deficiencies were present, they were noted on the forms and sent to the Job Engineer for correction. Copies of the forms were filed with the Quality Assurance Engineer and the Project Engineer. If the item was not immediately set in its final position, a notation was made on the form regarding the storage of the item and the protection provided. Field storage was determined by standard construction practices supplemented by any special requirements specified by the manufacturer. Periodic site inspections were made of equipment to ensure that proper storage procedures were being maintained.

The Consumers Power construction personnel made an independent check of equipment as it arrived onsite and observed proper handling and storage until it was placed. After installation, continual checks were made to ensure that it was properly protected until ready for initial operation.

When the item was set or installed, inspection was employed to confirm that electrical and instrumentation items were properly set and connected. A record of this inspection was made on a special form. Any deficiencies were noted on the form for correction in a similar manner as when the equipment was received. A visual checkout of wiring was made by System Protection and Laboratory Services Department personnel to assure that it was wired in accordance with the connection diagrams.

During the construction phase of installing cable and wiring, routine checks were made by both Bechtel and Consumers Power to assure that proper cableway routing and separations were being maintained as required for the protective and engineered safeguards systems. This included verification of separate penetration areas for these systems which enter the containment building.

Prior to preoperational testing, function tests of all electrical controls and instrumentation were performed by System Protection and Laboratory Services Department personnel and the Plant Instrumentation Group. This functional testing verified that with the equipment energized, it functioned as it should with an overall checkout being made from sensor through control and output device. In addition, instruments were calibrated during the functional test including most sensors although in some cases, sensors were calibrated prior to installation and this was considered adequate. These calibrations and system tests were recorded on special forms.

During the preoperational testing program, the correct functioning and calibration of all control systems was given a final verification by performance of a preoperational test on all Plant systems. The test procedures for each of these systems defined all instrumentation and control functions in the respective systems and the observed response was noted on the test forms. Any deviations from design specifications were noted on the forms and these were corrected prior to considering the test complete.