

7.2 REACTOR PROTECTIVE SYSTEM

7.2.1 GENERAL

The RPS consists of sensors, amplifiers, logic, and other equipment necessary to monitor selected Nuclear Steam Supply System (NSSS) conditions and to effect reliable and rapid reactor shutdown if any one or a combination of conditions deviates from a preselected operating range. The system functions to protect the core and RCS pressure boundary.

7.2.2 DESIGN BASIS

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

- a. Instrumentation conforms to the provisions of the proposed IEEE, Criteria for Nuclear Power Plant Protection Systems (IEEE 279, August 1968).
- b. No single component failure can prevent safety action.
- c. Four independent measurement channels are provided for each parameter that can initiate safety action.
- d. Channel independence is assured by separate connection of the sensors to the process systems and of the channels to vital instrument busses.
- e. The four measurement channels provide trip signals to six independent logic matrices, arranged to effect a two-out-of-four coincidence logic having outputs to four independent trip paths.
- f. A trip signal from any two-out-of-four protective channels causes a reactor trip.
- g. When one of the four channels is taken out of service, the protective system logic can be changed to a two-out-of-three coincidence for a reactor trip by bypassing the removed channel.
- h. The protective system AC power is supplied from four separate vital instrument busses.
- i. Open circuiting, or loss of power supply for the channel logic, initiates an alarm and a channel trip.
- j. The trip logic matrices assume the nonconducting state to provide a tripping function.
- k. The RPS can be tested with the reactor in operation or shut down.
- l. The manual trip system is independent of the automatic trip system.
- m. Trip signals are preceded by pretrip alarms to alert the operator of undesirable operating conditions in cases where operator action can correct the abnormal condition and avoid a reactor trip.
- n. The RPS components are independent of the control system.
- o. All equipment, including panels, components and cables associated with the RPS, are marked with colored markers or nameplates in order to facilitate identification. The cabinets of the RPS are appropriately tagged A, B, C, and D, respectively, to distinguish between channels. Internal wiring in the RPS cabinets is not color coded. External to the RPS cabinets, the RPS uses color coded cable within the main control panels to ease identification of these channels. At termination points the incoming and outgoing cables of the RPS are appropriately tagged to identify the channel.
- p. Electrical circuit isolation is provided between the RPS and the annunciators and plant computer.
- q. The RPS is designed such that the de-energized state initiates a channel trip. This feature ensures that if channel continuity is lost, that channel will fail in a safe condition. The modules are not interlocked to prevent withdrawal but are designed such that withdrawal of one module causes a channel trip, associated channel trip annunciation and pretrip annunciation. Withdrawal of any other module of that

parameter will cause a full trip since the system is in the two-out-of-four trip mode. A unique key is available at the plant, allowing only one of the four channels of any one parameter to be bypassed at any time that the RPS is required to be operable. Strict administrative control ensures that this requirement is not violated. This bypass produces a two-out-of-three trip logic for the remaining three channels.

Generic Letter 83-28 requested response to certain generic concerns resulting from an incident at another plant in which the scram circuit breakers failed to open on receipt of an automatic reactor trip signal. There are four areas of concern:

Post-Trip Review

The Nuclear Regulatory Commission (NRC) asked for a description of the post-trip review to assure that the causes for unscheduled reactor shutdowns, as well as the response of safety-related equipment, are fully understood prior to plant restart.

We responded that administrative controls exist that require a post-trip review to be conducted to determine the acceptability of the restart. Another review is also conducted to provide an in-depth analysis of the events relative to long-term plant operations.

Equipment Classification and Vendor Interface

We were tasked to identify all safety-related components necessary to trip the reactor. This identification could be in documents, procedures or information handling systems used to control safety-related plant activities. In addition, a program was required to be established and maintained to ensure that vendor information for safety-related components is complete, current, controlled and referenced or incorporated in plant instructions and procedures.

We have a program to identify, classify and treat components required for performance of reactor trip as safety-related. Vendor information comes from Combustion Engineering, Inc. (CE) the NSSS vendor, and the RPS is a part of the CE interface.

Post-Maintenance Testing

The objective of this requirement was to assure that post-maintenance operability testing of safety-related components in the RPS is conducted. This testing should also prove that the equipment is capable of performing its safety function before being returned to service.

We have post-maintenance testing procedures which are required to be performed when maintenance is performed on these components. Vendor guidance is incorporated in these procedures.

Reactor Protective System Reliability Improvements

Vendor-recommended reactor trip breaker modifications and associated RPS changes were required to be completed, a comprehensive program of preventive maintenance and surveillance testing was required for the reactor trip breakers, and the shunt trip attachment must activate automatically.

Vendor Recommendations for modifications of reactor trip components were reviewed and implemented. Since that time, the trip breakers have been replaced with NLI/Square D Masterpact type breakers. Preventive maintenance is performed on these breakers in accordance with the manufacturer's recommendations. We verify the response time of the undervoltage and shunt trip circuits.

7.2.3 SYSTEM DESCRIPTION

As shown in Figures 7-1 and 7-2, the RPS consists of four trip paths operating through the coincidence logic matrices to maintain power to, or remove it from, the control element drive mechanisms (CEDMs). Four independent measurement channels normally monitor each plant parameter which can initiate a reactor trip. Individual channel trips occur when the measurement reaches a preselected value. The channel trips are combined in six two-out-of-two logic matrices. Each two-out-of-two logic matrix provides trip signals to four one-out-of-six logic units, each of which causes a trip of the breakers in the AC supply to the CEDM power supplies. Each CEDM power supply source is separated into two branches.

Reference Figure 4-1 for RCS process instrumentation.

As shown in Figure 7-2, a two-out-of-four logic operating on undervoltage relays on the CEDM power supply lines is used to provide an auxiliary signal coincident with reactor trip. This signal is utilized to trip the turbine.

Reactor trip is accomplished by deenergizing the CEDM coils allowing the control element assemblies (CEAs) to drop into the core by gravity. The reactor trip allowable limits and pretrip limits are listed in Table 7-1.

Figure 7-2A shows the RPS interface logic.

Reactor trip is initiated by the following conditions:

7.2.3.1 High Rate-of-Change of Power

The rate-of-change of power high trip is used to trip the reactor when excore logarithmic power measured by the wide range logarithmic neutron flux monitors indicates an excessive rate of change. This trip functionally minimizes transients for events such as a boron dilution event, continuous CEA withdrawal, or CEA ejection from subcritical conditions. Because of this function, such events are assured of having much less severe consequences than events initiated from critical conditions. The rate-of-change of power is monitored at start-up by four wide-range channels, as shown in Figure 7-4. The channels cover a range of greater than ten decades.

7.2.3.2 Variable Over Power Level

A reactor trip in power level (Q) (Section 7.2.3.7) is provided to trip the reactor in the event of a CEA ejection incident, and to help prevent violation of the CEA position vs. power level assumed in the Thermal Margin and Axial Flux Offset trips. The high power trip setpoint can be set no more than a predetermined amount above the indicated plant power. Operator action is required to increase the setpoint as plant power is increased. The setpoint is automatically decreased as power decreases.

The variable setpoint and Q are compared in a bistable trip unit in each of the four safety channels. The high power trip is initiated by two-out-of-four coincidence logic from the four safety channels.

Figure 7-20 shows the operation of the system. If Q decreases, the setpoint Q_{TR} follows it, remaining above Q by a fixed, adjustable bias Q_b . If Q now increases, the setpoint remains at the minimum value of $Q + Q_b$ last achieved until reset by the operator.

The system is capable of holding the setpoint Q_{TR} at the previous minimum of $Q + Q_b$ indefinitely. This capability is achieved by storing Q_{TR} as a digital word.

The reset circuit is designed to apply a momentary signal to the appropriate terminal of the digital storage device when a pushbutton is pressed. This causes Q_{TR} to achieve the current value of $Q + Q_b$. The reset circuit is buffered to permit locating one of the pushbuttons outside of the RPS, another pushbutton is located on the RPS channel panel.

The signal Q_{TR} is limited so that, regardless of the logic described above, it cannot go above or below limits set by potentiometers.

Other circuits generate a pretrip limit for the bistable trip unit, as well as a contact closure to alert the operator when power increases after reaching a minimum. The pretrip alarm provides audible and visual annunciation in addition to CEA withdrawal prohibit signals.

Power level and $Q - Q_{TR}$ are displayed on the main control board. Power Level is also taken to the Control Element Drive System (CEDDS) for use in the power dependent insertion limit (PDIL) calculation.

The pretrip alarm signals are initiated by bistable trip units from the same channels which provide the reactor trip signals. The pretrip alarms provide audible and visual annunciation in addition to CEA withdrawal prohibit signals.

7.2.3.3 Low Reactor Coolant Flow

This reactor trip is provided to protect the core against Departure from Nucleate Boiling (DNB) in the event of a coolant flow decrease. The setpoint for this trip is low enough to allow continued operation during abnormal frequency transients down to 57.5 Hz on the 500 kV system.

The flow measurement signals are provided by summing the output of the differential pressure (d/p) transmitters across each steam generator (SG) to provide an indication of the total coolant flow through the reactor. A reactor trip is initiated by two-out-of-four coincidence logic from the four independent measuring channels when the flow function falls below the preset value, as shown in Figure 7-5.

Pretrip alarms are initiated if the coolant flow function approaches the minimum required for reactor operation. The zero power mode bypass switch allows this trip to be bypassed for subcritical testing of CEDMs. The trip bypass is automatically removed above $10^{-4}\%$ power.

An indication of reactor flow rate is given by summing the d/p measurement across the SGs. This measurement is read out in the form of d/p in psi and not actual flow. The low-flow reactor trip is actuated directly by the summed d/p signal.

Both SG d/p signals are summed for all operating modes. The flow channels are also designated to monitor reverse flow.

The hot functional test program to determine low-flow trip setpoints consisted of two phases; first to demonstrate that the actual flow through the core was equal to or greater than the value stated in the Updated Final Safety Analysis Report (UFSAR); second, to establish the sum of the SG d/p at which the low-flow trip

would be set to meet the trip conditions listed in UFSAR, Chapter 14. These two phases are discussed in greater detail below.

PHASE I

The initial steady state reactor mass flow rates for four-pump, three-pump, two-pump same-loop and two-pump opposite-loop operation were determined during the power test program using the measured pump d/p and the pump characteristic curves. These flow rates, including the allowances made for measurement uncertainty, potential flow loss due to increased flow resistance with core life, and temperature effects were shown to be greater than or equal to the design flows used in the UFSAR Chapter 14 accident analysis.

The test instrumentation provided for Calvert Cliffs accurately measured the reverse flow which occurs with two-pump same-loop operation. The d/p across the pump was measured as the pump discharge pressure minus the pump suction pressure which is positive when the pump is operating. When a pump is not operating and reverse flow occurs through that pump, the pressure at the discharge side of the pump will still be higher than the pressure on the suction side, and a positive d/p occurs once again. The same pump d/p instrumentation which was calibrated to read the expected range of positive pump d/p was therefore used (along with the pump characteristic curves) to determine both forward and reverse flow. Accuracies on the d/p instrumentation were factored into the uncertainty assigned to the total reactor mass flow rate measurement.

The reactor mass flow rate was initially determined, as described above, by summing the measured mass flow rates through each primary coolant pump. In addition, a relationship was developed between the d/p across the SGs and the reactor mass flow rates for all pump combinations.

PHASE II

Having established the steady state adequacy of the flow for all allowable pump combinations, it was then necessary to develop protective system setpoints for all pump combinations which must be capable of tripping the reactor upon the loss of one or more pumps. The summed SG d/p values for a given pumping configuration are related to the reactor mass flow rate for any specified coastdown transient. The relationship was first calculated for each coastdown transient and then verified during the power test program. These relationships were used to generate low-flow trip calibration curves which in turn were used to determine the low-flow trip setpoints for the various pump configurations.

For the two-pump same-loop case in question, even though the SG d/p in the active loop is positive and the SG d/p in the inactive loop negative, the algebraic sum of the SG d/ps is related to the reactor mass flow rate during a pump coastdown transient by means of the two-pump same-loop low-flow trip calibration curve.

The SG d/p transmitters were calibrated such that the d/p for all pump combinations when the reactor is at operating temperature fell between the upper and lower 5% of their range.

7.2.3.4 Low Steam Generator Water Level

An abnormally low SG water level indicates a loss of SG secondary water inventory. If not corrected, this would result in a loss of capability for removal of heat from the RCS.

The low SG water level reactor trip protects against the loss of feedwater flow incident (Section 14.6). The trip allowable limit specified in Table 7-1 assures that sufficient water inventory will be in the SG at the time of trip to provide approximately 10 minutes before AFW is required for the removal of decay heat.

A reactor trip signal is initiated by two-out-of-four logic from four independent channels. Each channel actuates on the lower of two signals from two downcomer level d/p transmitters, one on each SG. Audible and visual pretrip alarms are actuated to provide for annunciation of approach to reactor trip conditions (Figure 7-17).

7.2.3.5 Low Steam Generator Pressure

An abnormally high steam flow from one of the SGs, e.g., that which would occur as the result of a steam line break, would be accompanied by a marked decrease in steam pressure. To protect against an excessive rate of heat extraction from the SGs and subsequent cooldown of the reactor coolant following a steam line break, a reactor trip is initiated by low SG pressure. The low SG pressure trip provides protection for larger feedwater line breaks.

A reactor trip signal is initiated by two-out-of-four logic from four independent channels. Each channel actuates on the lower of two signals from two pressure transmitters - one on each SG. Audible and visual pretrip alarms are actuated to provide for annunciation of approach to reactor trip conditions.

The reactor trip allowable limit specified in Table 7-1 is sufficiently below the full-load operating pressure so as not to interfere with normal operation, but still high enough to provide the required protection in the event of excessively high steam flow (Figures 7-17 and 7-18).

A bypass is provided for the low SG secondary pressure trip. Bypass is accomplished manually by means of a switch in each channel. The manual bypass is enabled only below a preset secondary pressure and is automatically removed above this setpoint.

The low SG pressure trip bypass is initiated manually by turning a switch to the BYPASS position. The bypass is removed, regardless of the manual switch position, if the actuated high of the SG pressures exceeds a predetermined setpoint. A latch feature ensures that the SG pressure will not remove the trip as it decreases. Figure 7-18 is a schematic of this circuit. Trip bypass is accomplished by energizing the "N" terminal of the trip unit with +15 Volts, through manually- and automatically-actuated contacts. Any open contact in this path will remove the bypass and allow trip. The automatic contact is actuated by relay K22, which is controlled through its own normally open (latch) contact by a bistable device set to operate at a predetermined pressure. To permit reset of K22, the latching contact is shunted when the manual switch is in the OFF position.

If the operator leaves the manual switch in the BYPASS position during plant heatup, the bistable contact will open when the highest SG pressure exceeds the setpoint. This will de-energize K22 and disconnect +15 Volts from the trip unit,

allowing trip. An annunciator is provided on the reactivity controls and protective system control board (1CO5) which indicates when the low SG channel trip is bypassed.

If the operator turns the manual switch to OFF, the path from +15 Volts to the trip unit will be interrupted by the manual contacts, and trip will be allowed.

For setting and testing the bistable device by use of the trip tester, a TEST SELECT switch is provided to disconnect the signal not being tested. This can only be done if the manual bypass switch is in the OFF position.

The contact testing system consists of two pushbuttons: one for auto bypass removal test and one for manual bypass removal test. The purpose of these tests is to check the status of the bypass circuit contacts. These tests do not alter or change the contacts from either an open or closed position.

Pressing the AUTO TEST pushbutton completes a path through the K22 contact to the light; therefore, an energized light indicates that bypass is allowed by the automatic removal circuit. Pressing the MAN TEST pushbutton similarly tests the manual contact. Pressing both pushbuttons energizes the light regardless of bypass status; this tests the light. The light is also energized for both the manual and automatic contacts closed, i.e., when the trip bypass is in effect.

7.2.3.6 High Pressurizer Pressure

A reactor trip for high pressurizer pressure with concurrent opening of the PORVs is provided to prevent excessive blowdown of the RCS by relief action through the pressurizer safety valves.

The trip signals are provided by four independent narrow-range pressure transducers measuring the pressurizer pressure.

A reactor trip is initiated by two-out-of-four coincidence logic from the four independent measuring channels if the pressurizer pressure exceeds 2400 psia. This signal also opens the power-operated relief valves (PORVs).

Pretrip alarms are initiated if the pressurizer pressure exceeds 2350 psia.

7.2.3.7 Thermal Margin/Low-Pressure Trip

A reactor trip is initiated whenever the RCS pressure signal drops below either a preset pressure or a computed value described below, whichever is higher. The computed value is derived using functions of the minimum permissible power to fuel design limit on Departure from Nucleate Boiling Ratio (DNBR) (P_{fdn}) and of the reactor inlet and outlet temperatures and nuclear instrument power. Output from the resistance temperature detectors (RTDs) in the hot and cold legs of each SG is used to generate a coolant differential temperature (ΔT) signal. This coolant ΔT signal is proportional to reactor power and is utilized as such. The ΔT power signal is compared to the nuclear instrument power signal (Figure 7-21) and the higher signal is modified by two functions which provide penalty factors based on the worst-case CEA position and the actual calculated Axial Shape Index. This signal feeds a setpoint calculator (Figure 7-6A).

In the setpoint calculator, a function generator produces a signal proportional to the minimum permissible P_{fdn} . The ratio of power and P_{fdn} is then combined with a

coolant temperature signal, a pressure signal representing an asymmetric SG loading (Figure 7-6B), and a reference signal (corresponding to the minimum pressure for trip) to define the pressure for reactor trip in order to assure that the minimum DNBR is not exceeded during anticipated operational occurrences.

The trip signal is initiated by a two-out-of-four coincidence logic from four independent safety channels, and audible and visual pretrip alarms are actuated to provide for annunciation on approach to reactor trip conditions. The pretrip action also initiates a CEA withdrawal prohibit. A block diagram of a thermal margin/low-pressure (TM/LP) trip channel is shown in Figure 7-6.

Figure 7-21 shows a block diagram of the thermal (ΔT) power calculation.

The calculation begins with the generation (by temperature transmitters) of currents representing the cold and hot leg temperatures in each loop. By forcing these currents through precision resistors and utilizing the resulting voltage drops, voltages representing cold leg temperatures (T_{c1} and T_{c2}) and hot leg temperature (T_h) are sent to the calculator. The latter signal is the average T_h for the two loops. The T_h temperature signal is also filtered by a lag module prior to the calculator to minimize the effect of momentary spikes and oscillations on the circuit.

In the calculator, the higher cold leg temperature signal is selected and subtracted from the hot leg temperature signal to determine the temperature rise. The calculator generates terms proportional to the first and second powers of the temperature rise and to the product of temperature rise and cold leg temperature. These three terms represent thermal power for four-pump operation and steady state conditions, accounting for coolant density, specific heat, and flow rate variations with temperature and power. To provide an adequate core power indication during mild transients, such as ramp load changes, a dynamic response term is added as shown. A bias term is added for calibration to adjust the output to zero at power. The sum of these terms represents the core power for four-pump operation under steady state or mild transient conditions.

The coefficient of the term proportional to the temperature rise (K_{α}) is set by the potentiometer labeled "Delta T Power Calibrate" on the Reactor Protective System Calibration and Indication Panel (RPSCIP) front panel. A plastic cover protects this potentiometer from accidental adjustment. This factor is adjusted to make the thermal power calculation agree with the plant calorimetric calculation.

The thermal power (B) is subtracted from the nuclear power (ϕ), generated by the NI Channel, and the difference is displayed on a meter with a range of -10% to +10% of full power. The meter has adjustable upper and lower setpoints. The contacts energize a local light when the deviation goes outside the range defined by the setpoints.

To make the nuclear power signal agree with the thermal power and/or the plant calorimetric calculation, a potentiometer labeled "Nuclear Power Calibrate" is provided on the RPSCIP front panel. This potentiometer adjusts the gain of the NI channel from 0.8 to 1.33. An auctioneering circuit selects the higher of nuclear power or thermal power for use in the remainder of the system. This auctioneered signal is called Q .

Regular checks are performed to ensure agreement between plant calorimetric and ΔT power; if required, adjustments are made at the "Delta T Power Calibrate" dial on the reactor protective calibration and indication panel.

The zero power mode bypass switch allows this trip to be bypassed for low power testing. The trip bypass is automatically removed above about $10^{-4}\%$ power. An additional feature of this zero power mode bypass is to remove the ΔT power component of the power signal Q. This prevents RCS temperature channel range limits from causing the generation of incorrect ΔT power signals which would cause false trips on high power during low power testing or plant heat-up and cooldown. This bypass applies to the low flow and TM/LP trips. This circuit is similar to the low SG pressure bypass, except that the bypass is automatically removed by a contact from a bistable device located in the wide-range nuclear instrument drawer, which actuates at a preset power level. No latching feature is required in this circuit. The contact status testing system is identical to the system for the low SG pressure bypass. An annunciator is provided on the reactivity controls and protective system control board (1C05) which indicates when the zero power mode channel is bypassed.

7.2.3.8 Loss of Load

The loss-of-load trip is an equipment protective trip and is not required for reactor protection. (Section 14.5)

A loss-of-load trip above a preset power level is initiated by actuation of the turbine trip system. This trip is anticipatory in nature as it precedes the high-pressure trip.

The plant annunciator indicates on control board CO5 when this trip is bypassed. This inhibit is automatically removed at a predetermined setpoint.

7.2.3.9 High Containment Pressure

A trip is provided on high containment pressure in order to assure that the reactor is tripped prior to, or at least concurrent with, safety injection actuation.

Four pressure transmitters actuate trip units which are connected in a two-out-of-four coincidence logic to initiate the protective action if the containment pressure exceeds a preselected value.

The containment pressure transmitter sensing lines are the only instrument lines to which Safety Guide 11 is applicable and are designed in accordance with this Safety Guide.

The containment pressure transmitters are located outside the Containment Structure in the electrical penetration room. They are located as close as practical to the containment and installed using short connections between the containment penetrations and the instruments. The transmitters are designed as pressure retaining devices, whereby rupture of the sensing device would not release radioactivity to the environment, but would contain the radioactivity within the housing of the instrument. Each sensing line is provided with a solenoid-operated isolation valve which is located as close as possible to the containment penetration. The isolation valves are controlled from the Control Room and are provided with position switches for remote indication in the Control Room. The isolation valves and instrument lines, up to and including the pressure retaining parts of the instruments, are Seismic Category I.

7.2.3.10 Manual Trip

A manual reactor trip is provided to permit the operator to trip the reactor. The actuation of two adjacent pushbutton switches on the control panel causes interruption of the AC power to the CEDM power supplies. Two sets of trip pushbutton switches are provided. The manual trip function is testable during reactor operation. The pressing of these two buttons is required to effect a reactor scram; however, they do not need to be depressed simultaneously.

7.2.3.11 Axial Flux Offset Trip

A reactor trip is initiated as determined by signals from the power range safety channels whenever the axial flux shape approaches a preset value. The axial flux offset trip signals are initiated by two-out-of-four coincidence logic from the four power range safety instrumentation channels, with audible and visual pre-trip alarms actuated to provide for annunciation on approach to reactor trip conditions.

The trip setpoint is selected to ensure that the axial flux distribution does not result in conditions exceeding fuel damage limits.

7.2.3.12 Asymmetric Steam Generator Load

A reactor trip is initiated via the TM/LP trip channel as determined by combining the SG pressure signals within the TM/LP Trip Calculator, such that, if these pressures differ by more than a fixed amount in either direction, the calculated primary pressure trip setpoint is raised by putting a signal into the maximum selector function that selects the highest of: the asymmetric factor signal, or the calculated pressure P_{var} , or P_{min} (Figures 7-6A and 7-6B).

This trip functions to add additional safety margins in the event of a slow closure of one of the MSIVs.

7.2.4 SIGNAL GENERATION

Four instrument channels are used to generate the signals necessary to initiate the automatic reactor trip action. The signal cable routing and readout drawer locations are separated and isolated to provide channel independence.

7.2.4.1 High Rate-of-Change of Power

The wide-range logarithmic channels obtain signals from four detector channels. Each channel consists of a two-ganged fission chamber assembly. These assemblies are located in wells on the reactor cavity wall around the reactor. The outputs are amplified at amplifier assemblies located outside containment and carried to the signal processing drawer in the Control Room. A signal proportional to the logarithm of neutron flux over the range of $10^{-8}\%$ to 200% of full power is obtained (Figure 7-7). This signal is then differentiated to obtain the rate-of-change of power.

7.2.4.2 High Power Level

The signal for each of the four power range safety channels is obtained from one of the four detector assemblies located on the reactor cavity wall around the reactor. Each assembly consists of two uncompensated ion chambers stacked vertically to monitor the full length of the core. The DC current signal from each ion chamber is fed directly to the Control Room drawer assembly. The ion chambers cover the range from 0.1% to 200% power (Figure 7-4).

7.2.4.3 Flow, Water Level, Pressure, and Thermal Margin

The flow, water level, pressure, and thermal margin trips are each actuated from signals generated by separate sets of transmitters. Flow is measured by monitoring the pressure difference between the hot leg piping and the SG outlet plenum. SG water level and pressure are monitored in each SG. The RCS pressure is measured in the pressurizer. Temperature measurements are taken from the reactor inlet and outlet piping in each loop and combined with coolant pressure to ensure adequate thermal margin.

Piping and connections for these transmitters are separated and isolated to provide independence. The output of each transmitter is an ungrounded current loop supplying signal receivers and bistable trip modules.

7.2.4.4 Axial Flux Offset

The signals for the axial flux offset trip are processed in the four power range safety channel drawer assemblies. Each channel receives signals from two vertically-stacked uncompensated ion chambers located in the reactor cavity. The two signals, representing flux in the upper half of the core and flux in the lower half of the core, are combined in each of the four drawer assemblies to generate four independent trip signals proportional to axial flux shape. The Axial Shape Index (Ye) from the excore detectors (power range and regulating channels) is the power level detected by the lower excore nuclear instrument detectors (L) less the power level detected by the upper excore nuclear instrument detectors (U) divided by the sum of these power levels. The Axial Shape Index (YI) used for the trip and pretrip signals in the Reactor Protection System is the above value (Ye) modified by an appropriate multiple (A) and a constant (B) to determine the true core axial power distribution for that channel. This value of Axial Shape Index (YI) represents the excore detector equivalent of the peripheral Axial Shape Index determined by the incore detector system for a given excore channel.

7.2.5 LOGIC OPERATION

Refer to Figure 7-2 for the following discussion.

Each measurement channel which can initiate protective action operates a channel trip unit; each trip unit includes three sealed, electromagnetically-actuated reed relays and associated contacts. Four trip units are actuated for each trip condition, e.g., high reactor coolant pressure. The relays in each of these four trip units provide a separate trip path; the trip paths are designated channels A, B, C, and D.

The relays in each trip unit are numbered one, two, and three. The normally open contacts from the No. 1 relay group of Channel A are connected into a two-out-of-two logic matrix with Channel B relay contacts. (The normally open contacts are used for the logic ladders so that the relays are energized and the contacts closed under operating conditions.)

The No. 2 and No. 3 relay contacts are similarly connected into two other two-out-of-two logic matrices with Channel C and Channel D relay contacts.

With the No. 2 and No. 3 relay contacts of Channels B, C, and D similarly arranged in BC, BD, and CD combinations of two-out-of-two logic matrices, there are a total of six two-out-of-two logic matrices, forming a two-out-of-four coincidence logic with respect to the input channels.

At the output of each logic matrix is a set of four sealed, electromagnetically-actuated relays. These sets are designated the AB, AC, AD, BC, BD, and CD logic trips. The contacts from one relay of the logic trip set from each logic matrix 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 trip breaker control relay whose contacts provide actuation of undervoltage and shunt trips on the trip circuit breakers, thus interrupting the AC power to the CEDM power supplies. Deenergizing of any one trip breaker control relay interrupts (opens) one trip path and trips the two breakers controlled by that trip path. Deenergizing any set of four logic trip relays causes an interruption of all trip paths and a full trip. Each of the six logic trip matrices energizes one set-of-four logic trip relays.

If one of the trip units is to be removed for maintenance, the logic matrices may be changed from a two-out-of-four trip to a two-out-of-three trip by the operation of the logic bypass switch (shown on the output of the trip module, Figure 7-3). One key-operated switch is provided for each trip unit. Only one key is provided for the trips for any one variable to ensure that only one of a group of four could be bypassed at one time. The operation of the key-operated switch to bypass the trip function of a single bistable trip unit is indicated by a light on its face. This light meets the requirements of paragraph 4.13 in IEEE 279 in that it provides continuous indication of the bypass in the Control Room.

Where the trip is to be allowed only in selected power ranges, a neutron flux signal is utilized to inhibit the action of the trip units. A manually-actuated inhibit action may, under administrative control, be applied to the low reactor coolant flow, thermal margin and low SG pressure trips for zero power testing. The inhibits on reactor coolant flow and thermal margin are automatically removed above a preset power. The inhibit on SG pressure is automatically removed above a preset pressure. The high power rate-of-change trip is automatically inhibited below about 10⁻⁴% power and above 15% power. Protective system criteria are met by this use of neutron flux signals to provide multiple independent inhibit or reset signals.

The CEDMs are separated into two groups. The CEDM power supplies in each group are supplied in parallel with three-phase AC power from the motor-generator sets. Two full capacity motor-generator sets are provided so that the loss of either set does not cause a release of the CEAs. Each power supply source is separated into two branches. Each side of each branch line passes through two trip circuit breakers (each actuated by a separate trip path) in series so that, although both sides of the branch lines must be deenergized to release the CEAs, there are two separate means of interrupting each side of the line. This arrangement provides means for the testing of the protective system.

7.2.6 TESTING

Since operation of the protective system will be infrequent, the system is periodically and routinely tested to verify its operability. A complete channel can be individually tested without initiating a reactor trip or violating the single failure criterion, and without inhibiting the operation of the RPS.

The RPS is capable of being checked from the trip unit input through the power supply circuit breakers of the CEDMs. The majority of the components in the protective system can be tested during reactor operation. The remainder of the components can be checked by comparison with similar channels or channels that involve related information. These components, which are not tested during reactor operation, will be tested during scheduled reactor shutdown to assure that they are capable of performing the necessary functions. Minimum frequencies for checks, calibration, and testing of the RPS

instrumentation are given in the Technical Specifications. Overlap in checking and testing is provided to assure that the entire channel is functional. The use of individual trip and ground detection lights, in conjunction with those provided at the supply bus, assure that possible grounds or shorts to another source of voltage can be detected.

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, initiating a test input and noting signal level required to effect trip action. 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 by a test signal generator which is connected to the trip module at the signal input terminals. With the test signal generator connected, the desired signal is selected and then inserted into the trip unit by depressing the manual test switch. The test circuit permits various rates of change of signal input to be used. 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 logic matrix are tested one at a time. The test circuits in the logic permit only one logic ladder to be opened and one set of relays to be held at a time; the application of hold power to one set denies the power source to the other sets. In testing a logic trip set (e.g., 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 pushbutton switch. Operation of the matrix trip test switch initiates a deenergizing current in the test coils of a parallel pair of trip unit relays. With the ladder logic relay contacts open, the logic trip relays may be deenergized one at a time (by rotating the matrix relay trip test switch) to open the associated trip breakers. Indicator lights on the trip status panel provide verification that coil operation and trip breaker actuation conditions have occurred.

Sensor responses were measured initially during factory acceptance tests. During plant startup testing, the response times from an input signal to the protection system trip units were verified through the opening of the trip circuit breakers.

The capability does not exist within the protection system to verify response times of trip parameters during normal plant operation; however, these tests can be performed during refueling periods.

The response times given in Table 7-2 provide one of the bases for operability determination of the RPS instrumentation referred to in the Technical Specifications.

Periodic testing can be carried out from the Control Room to ensure the continuity of the measurement loop. A supplementary signal is introduced into the measurement loop that is bypassed and the response to this signal is indicated on a meter in the protection system. This proves the continuity of the loop.

The overall loop response is designed to be less than those times used for safety analysis (Section 14.1).

7.2.7 SYSTEM EVALUATION

The RPS was manufactured under strict engineering and quality control specifications. These specifications require that the equipment be inspected for workmanship, proper materials, and channel separation as required by IEEE 279. Furthermore, all intra- and inter-connection wiring was tested for continuity and an insulation test was performed between each conductor and chassis ground, and between each individual pair of

connectors. An operational test was performed on the system during which time input signals were simulated to ensure that the protective system is capable of producing the proper trip signals. The system was packaged for shipment in accordance with specifications. The marking and packaging were inspected for compliance with the specification. All the above-mentioned tests were documented by the manufacturer. The quality assurance program described in Appendix 1A was applicable to the RPS during the construction phase.

The RPS is designed to limit reactor power and coolant conditions to levels within the design capability of the reactor core. Instrument performance characteristics, response time, and accuracy are selected for compatibility with, and adequacy for, the particular function. Trip setpoints are established by analysis of system parameters. Factors such as instrument inaccuracies, bistable trip times, CEA travel times, valve travel time, circuit breaker trip times, and pump starting times are considered in establishing the margin between the trip setpoints and the safety limits. The time response of the sensors and protective systems are evaluated for abnormal conditions. Since all uncertain factors are considered as cumulative for the derivation of these times, the actual response time may be more rapid. However, even at the maximum times which are added to the CEA drop time, the system provides conservative protection.

The wiring in the protective system is grouped so that no single fault or failure, including either an open or shorted circuit, will negate protective system operation. Signal conductors are protected and routed independently.

Loss of, or damage to, any one path will not prevent the protective action. Sensors are piped so that blockage or failure of any one connection does not prevent protective system action. The process transducers located in the Containment Structure are specified and rated for the intended service. Those components, which must operate in the loss-of-coolant accident (LOCA) environment, are rated for the LOCA temperature, pressure, and humidity conditions. Results of type test are used to verify these ratings. In the Control Room the nuclear instrumentation and protective system trip paths are located in four compartments. Mechanical and thermal barriers between these compartments reduce the possibility of common event failure. Outputs from the components in this area to the control boards are buffered so that shorting, grounding, or the application of the highest available local voltage does not cause channel malfunction. Where RPS signals feed annunciators, data loggers, or computers, buffering by isolation amplifiers (or equal) is used to ensure circuit isolation. In instances where the RPS is feeding the annunciators, isolation is ensured through the use of relay contacts. When redundant channels supply the computer, isolation amplifiers are used.

The protective system is designed and arranged to be able to perform its function with a single failure of any component. Some of the faults and their effects are described below.

In the analog portion of the system:

- a. A loss of signal in a measurement channel initiates channel trip action for all trips except high rate-of-change of power, high pressurizer pressure, high power level, and high containment pressure.
- b. Shorting of the signal leads to each other has the same effect as a loss of signal. Shorting a lead to a voltage source has no effect since the signal circuit is ungrounded. Periodic testing includes checks for possible grounds or applications of potential to the signal circuit.
- c. Open circuit of the signal leads has the same effect as a loss of signal.

- d. Single grounds of the signal circuit have no effect. Periodic checking of the system will assure that the circuit remains ungrounded.

In the logic portion of the circuit:

- a. Inadvertent operation of the relay contacts in the matrices will be identified by the indicating lights.
- b. Shorting of pairs of contacts in the matrices will prevent the trip relay set 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 logic matrix contact pairs.
- c. Shorting of the matrices to an external voltage has no effect since they are ungrounded. The testing process will indicate accidental application of potential to a matrix. Equipment is provided to detect grounds on the matrices.
- d. The logic matrices will each be supplied by two power sources. Loss of a single power source has no effect on operation. Loss of power to a logic matrix initiates a trip condition.
- e. Failure of a logic trip relay set to actuate has no effect since there are six sets in series in the trip action and any one set initiating trip action will cause the action to be completed.
- f. The failure of one trip breaker control relay in a trip breaker circuit has no effect since there are two trip breakers in series, either of which will provide the necessary action.
- g. Single grounds in the trip breaker control relay circuits have no effect since the circuit is ungrounded. Ground detectors on each 125 Volt DC bus also indicate an accidental ground.
- h. The AC circuit supplying power to the trip breaker control relay coil is fed from an isolation transformer. The circuit has a local ground detection system. Each of the four trip paths are fed from a separate 120 Volt AC vital instrument bus.
- i. The CEDM power supply circuits operate ungrounded so that single grounds have no effect. The CEDMs are supplied in two groups by separate pairs of power supplies to further reduce the possibility of a CEA being improperly held. The CEDM load requirements are such that the application of any other local available voltage would not prevent CEA release.

The locations of the sensors and the points at which the sensing lines are connected to the process loop have been selected to provide physical separation of the channels, thereby precluding a situation in which a single event could remove or negate a protective function. Process transmitters located inside the containment and required for short-term operation following a LOCA are qualified for the intended service in the LOCA environment. The routing of cables from these cabinets is arranged so that the cables are separated from each other and from power cabling to minimize the likelihood of common event failures. This includes separation at the containment penetration areas. 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 minimize the possibility of common event failure. Outputs from the components in this area to the control boards are buffered so that shorting, grounding, or the application of the highest available local voltages do not cause channel malfunction.

The RPS is designed as a Class I system. The specifications for the RPS components incorporate the applicable seismic requirements for each component, including spectrum response curves for the specific component location generated by the time-history method.

These components are qualified by either of the two following methods:

In most cases, the supplier is required to qualify his equipment by calculation or testing, or a combination of both. This qualification is formally documented and submitted for approval.

In other cases, tests or calculations are performed by independent consultants or laboratories who submit a formal report. Acceptance of the equipment from the supplier is contingent upon the proof of suitability as established by the results of those tests or calculations.

The choice of an analytical or experimental qualification procedure is determined by the size, shape, and structural or functional simplicity of the equipment in accordance with the criteria outlined in IEEE 344, "Guide for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations." Racks, panels, or other supporting structures are generally qualified by analysis, while bistable trip units and other modules are generally qualified through testing. Tests and calculations are performed following the guidelines of IEEE 344.

Type testing was used for RPS panels, racks, and equipment qualification in accordance with IEEE 323, "General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations." The results of type tests was submitted by Combustion Engineering, Inc. (CE) in the form of a topical report covering a series of plants. The submission date for this report was September 1972.

Radiation design criteria for RPS components located within normally radioactive areas are specified at a gamma level of 1 rad/hr for 40 years, except for the main coolant RTDs, which were specified at 10 rad/hr for 40 years. Protective system equipment not located in normally radioactive areas or located in areas of very low activity has been specified accordingly. Periodic tests and calibration will allow detection of gradual equipment deterioration and will assure capability of the system to operate as required by the original design basis since the interval between such tests will be short compared to the time required for significant deterioration.

All other material and equipment associated with safety-related systems have been specified to be suitable for the appropriate 40-year integrated dose.

There are no RPS instrumentation transmitters for which the trip setpoints are within 5% of the high or low end of the calibrated range, or within 5% of the overall instrument design range.

7.2.8 POWER SUPPLY

The power for the protective system is supplied from four separate and independent vital 120 Volt AC busses. Each vital bus is supplied from a separate battery system through a dual inverter. During normal operation, the battery chargers maintain a floating charge on each battery while at the same time, supplying power to the vital inverters. Upon loss of auxiliary AC power, the batteries provide the power for inverter operation. In the event of loss of one battery supply, only the protective channel associated with the battery goes into a trip condition. Each preferred bus also has provision for connection to an inverter backup bus to permit servicing of the inverters.

The distribution circuits from the preferred busses are provided with fuses properly coordinated with upstream fuses and circuit breaker protection to assure that individual circuit faults are isolated.

**TABLE 7-1
REACTOR TRIP ALLOWABLE LIMITS AND PRETRIP LIMITS**

<u>NO.</u>	<u>REACTOR TRIP</u>	<u>PRETRIP ALARM LIMIT</u>	<u>TRIP ALLOWABLE LIMIT</u>
1	High Power Level 4-Pump Operation	≤ 8% Above Measured Power Q ≤ 104.5%	≤ 10% Above Measured Power Q ≤ 107%
2	High Rate-of-Change of Power ^(a)	≤ 1.5 decades/min	≤ 2.6 decades/min
3	Low Reactor Coolant Flow ^(b) 4-Pump Operation	≥ 94%	≥ 92%
4	Low SG Water Level (Auctioneered low of SG #1, SG #2)	≥ 32" below normal water level	≥ 50" below normal water level
5	Low SG Pressure ^(c) (Auctioneered low of SG #1, SG #2)	≥ 735 psia	≥ 685 psia
6	High Pressurizer Pressure	≤ 2350 psia	≤ 2400 psia
7	Thermal Margin/Low-Pressure ^(b)	Variable, 50 psia above Trip Allowable Limit	Variable but not below 1875 psia
8	Loss of Load ^(d)	N.A.	N.A.
9	High Containment Pressure	≤ 3 psig	≤ 4 psig
10	Axial Flux Offset ^(d)	(e)	(e)
11	Manual Trip	N.A.	N.A.
12	Thermal Margin/SG Pressure Differential Hi	≤ 100 psid	≤ 135 psid

(a) Inhibited above 15% and below 10⁻⁴% power.

(b) Manual inhibit permitted below about 10⁻⁴% power: automatically removed above 10⁻⁴% power.

(c) Manual inhibit permitted below 785 psia: automatically removed above 785 psia.

(d) Inhibited below 15% power.

(e) Trip and pretrip setpoints are a function of power level.

TABLE 7-2
REACTOR PROTECTIVE INSTRUMENTATION RESPONSE TIMES
(BOTH UNITS)

<u>FUNCTIONAL UNIT</u>	<u>RESPONSE TIME</u>
1. Manual Reactor Trip	Not Applicable
2. Power Level – High	≤ 0.40 seconds ^{(a),(b)} and ≤ 12.0 seconds, cold leg ^(c) and ≥ 10.0 seconds and ≤ 60.0 seconds, hot leg ^{(c),(d)}
3. Reactor Coolant Flow – Low	≤ 0.50 seconds
4. Pressurizer Pressure – High	≤ 0.90 seconds
5. Containment Pressure – High	≤ 0.90 seconds
6. Steam Generator Pressure – Low	≤ 0.90 seconds
7. Steam Generator Water Level – Low	≤ 0.90 seconds
8. Axial Flux Offset	≤ 0.40 seconds ^{(a),(b)} and ≤ 12.0 seconds, cold leg ^(c) and ≥ 10.0 seconds and ≤ 60.0 seconds, hot leg ^{(c),(d)}
9. a. Thermal Margin/Low Pressure	≤ 0.90 seconds ^{(a),(b)} and ≤ 12.0 seconds, cold leg ^(c) and ≥ 10.0 seconds and ≤ 60.0 seconds, hot leg ^{(c),(d)}
b. Steam Generator Pressure Difference – High	≤ 0.90 seconds
10. Loss of Load	Not Applicable
11. Wide Range Logarithmic Neutron Flux Monitor	Not Applicable

NOTE: The response times given in this table provide one of the bases for operability determination of the RPS instrumentation referred to in the Technical Specifications.

- (a) Neutron detectors are exempt from Response Time testing. Response Time of the neutron flux signal portion of the channel shall be measured from detector output or input of first electronic component in channel.
- (b) Response Time does not include contribution of RTDs.
- (c) Calculator input response time only. This value is equivalent to the time interval required for the T-Cold RTDs and the T-Hot RTDs and T-Hot lag modules' outputs to achieve 63.2% of their total change when subjected to a step change in RTD temperature.
- (d) T-Hot response time of ≥ 10 seconds is input to UFSAR, Chapter 14, Safety Analyses. T-Hot response time of ≤ 60 seconds ensures that plant operation is not impacted by a delayed RTD response.