CHAPTER 7

7.0 INSTRUMENTATION AND CONTROLS

CHAPTER 7
INSTRUMENTATION AND CONTROLS

TABLE OF CONTENTS

CHAPTER 7
INSTRUMENTATION AND CONTROLS

TABLE OF CONTENTS (continued)

CHAPTER 7
INSTRUMENTATION AND CONTROLS

TABLE OF CONTENTS (continued)

CHAPTER 7
INSTRUMENTATION AND CONTROLS

TABLE OF CONTENTS (continued)

CHAPTER 7
INSTRUMENTATION AND CONTROLS

TABLE OF CONTENTS (continued)

TABLE OF CONTENTS (continued)

TABLE OF CONTENTS (continued)

CHAPTER 7
INSTRUMENTATION AND CONTROLS

LIST OF TABLES

CHAPTER 7
INSTRUMENTATION AND CONTROL

LIST OF FIGURES

CHAPTER 7
INSTRUMENTATION AND CONTROLS

LIST OF FIGURES (continued)

7.0 INSTRUMENTATION AND CONTROLS

7.1 Introduction

The HBR 2 instrumentation and controls, including both safety-related and nonsafety-related systems, are described in this chapter. Systems described are the Reactor Protection System (RPS), systems which initiate engineered safeguards, instrumentation and controls required for safe shutdown, display instrumentation, and control systems not required for safety.

The RPS monitors all parameters related to safe operation of the reactor. The system is designed to trip the reactor so as to protect the core against fuel rod cladding damage caused by departure from nucleate boiling (DNB), and to protect the Reactor Coolant System (RCS) against damage caused by over-pressure. The Engineered Safety Features (ESF) Instrumentation System monitors parameters to detect failure of the RCS, and initiates containment isolation and ESF operation.

The RPS automatically trips the reactor to protect the reactor core when the following conditions exist:

1. The reactor power, as measured by neutron flux, reaches a preset limit

2. The temperature rise across the core as determined from loop ΔT reaches a limit, either from a fixed ΔT setpoint (function of T_{avg} and neutron flux distribution) or a variable ΔT setpoint (function of T_{avg}, pressurizer pressure, and neutron flux distribution)

3. The pressurizer pressure reaches a minimum limit, or

4. There is a loss of reactor coolant flow as sensed by low flow, loss of pump power or pump circuit breakers opening.

The RPS automatically trips the reactor to protect the RCS when the pressurizer pressure or level reaches a maximum limit. There are also trips on safety injection, turbine-generator trip, low-low steam generator level, source range neutron flux, and intermediate range neutron flux.

Interlocking functions of the RPS prevent control rod withdrawal when a specified parameter reaches a value less than the value at which reactor trip is initiated.

For anticipated abnormal conditions, protective systems in conjunction with inherent plant characteristics and ESF are designed to assure that limits for energy release to the containment and for radiation exposure are not exceeded.

The ESF actuation system automatically performs the following vital functions:

1. Starts operation of the Safety Injection System (SIS) upon low pressurizer pressure, or high containment pressure, or high differential pressure between any steam line and the steam line header, or on high steam flow in any two steam lines, coincident with low steam pressure or low reactor coolant average temperature

2. Operates the Phase A containment isolation valves upon automatic actuation of the SIS

3. Starts the Containment Spray System and operates the Phase B containment isolation valves upon detection of a high-high containment pressure signal

4. Starts operation of the Containment Air Recirculation System if not operating after operation of the required SIS is initiated

5. Closes all steam line isolation valves on occurrence of any of the following:

    1. High steam flow in any two steam lines coincident with low steam pressure or low reactor coolant average temperature

    2. High-High containment pressure signals

Any safety injection signal will isolate the main feedwater lines by closing all control valves (main and bypass valves), tripping the main feedwater pumps, and closing the pump discharge valves. Key switches are provided to bypass closure of main feedwater regulating bypass valves and allow starting of main feedwater pumps with the Feedwater Isolation Signal present. Key switches may be momentarily placed in Override/Reset to reset the Feedwater Isolation Signal to the main feedwater regulating bypass valves and main feedwater pumps when the actuating signal has been cleared. Operation of these switches is annunciated on the RTGB and the key cannot be removed in the override position. This change was made to allow the operators to respond to a loss of all AFW flow condition.

The instrumentation and control systems were designed in accordance with guidance available at the time. This included proposed General Design Criteria (discussed in Section 3.1) and IEEE-279 (proposed, 1968, discussed in Section 7.2).

7.2 REACTOR TRIP SYSTEM

7.2.1 DESCRIPTION

The Reactor Protection System (RPS) monitors all parameters related to safe operation of the reactor. The system is designed to trip the reactor to protect the core against fuel rod cladding damage caused by departure from nucleate boiling (DNB), and to protect the Reactor Coolant System (RCS) against damage caused by overpressure.

Rapid reactivity shutdown is provided by the insertion of full length rod cluster control assemblies (RCCA) by gravity fall. Duplicate series-connected circuit breakers supply all power to the full length control rod drive mechanisms (CRDM). The full length CRDM must be energized for the RCCA to remain withdrawn from the core; automatic reactor trip occurs upon the loss of power to the full length CRDM. The trip breakers are opened by the undervoltage coils and the automatic shunt trip on both breakers. The undervoltage coils and the auto shunt trip relays, which are normally energized, become de-energized by any one of the several trip signals. The de-energizing of the auto shunt trip relay causes a contact closure in the shunt trip circuit thereby causing a simultaneous shunt trip along with the undervoltge trip. The design of the devices providing signals to the circuit breaker undervoltage trip coils and auto shunt trip relays is such as to cause these coils and relays to trip the breaker on reactor trip signal or loss of power to the reactor protection system. Loss of power to the shunt trip attachment, however, will not trip the breaker.

During power operation, a sufficient amount of rapid shutdown capability in the form of control rods is administratively maintained by means of the control rod insertion limit monitors. Administrative control requires that all shutdown group rods be in the fully withdrawn position during power operation.

7.2.1.1 System Description

A list of reactor trips, means of actuation, and the coincident circuit requirements is given in Table 7.2.1-1. The permissive circuits referred to in Table 7.2.1-1 (e.g. P7) are listed in Table 7.2.1-2.

Certain reactor trip channels are automatically bypassed at low power where they are not required for safety. Nuclear source range and intermediate range trips are specifically provided for protection at low power or subcritical operation. For higher power operations they are bypassed by manual action.

A block diagram of the RPS showing various reactor trip functions and interlocks is shown in Figure 7.2.1-1.

Constraints which are selected for various core parameters so the departure from nucleate boiling ratio (DNBR) is not less than the safety limit are determined by a digital code which mathematically correlates the nuclear and thermal hydraulic properties of the primary system. Safety limits and maximum permissible trip settings for the overtemperature high ΔT trip at different pressures for three-loop operation, are given in the Technical Specification

(Appendix A to the operating license). The trip settings remain more restrictive than the core safety limits, and are used in the protection system to provide suitable margin for measurement and instrument errors.

Adequate margins exist between the maximum nominal steady state operating point (which includes allowance for temperature, calorimetric, and pressure errors) and required trip points to preclude a spurious plant trip during design transients.

7.2.1.1.1 Completion of Protective Action

Where operating requirements necessitate automatic or manual bypass of a protective function, the design is such that the bypass is removed automatically whenever permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protective function are part of the protective system and are designed in accordance with the criteria of this section.

7.2.1.1.2 Reactor Trips

The reactor trips are as follows:

1. <u>High Nuclear Flux (Source Range) Trip</u> - This circuit trips the reactor when one of the two source range channels reads above the trip setpoint. This trip, which provides protection during reactor startup, can be manually bypassed when one of two intermediate range channels reads above the P6 setpoint value and is automatically reinstated when both intermediate range channels decrease below this value (P6). This trip is also bypassed by two out of four high power range signals (P10). The trip can also be reinstated below P10 by an administrative action requiring coincident manual actuation. The trip point is set between the source range cutoff power level and the maximum source range power level.

2. <u>High Nuclear Flux (Intermediate Range) Trip</u> - This circuit trips the reactor when one out of the two intermediate range channels reads above the trip setpoint. This trip, which provides protection during reactor startup, can be manually bypassed if two out of four power range channels are above approximately 10 percent (P10): Three out of four channels below this value automatically reinstate the trip. The intermediate channels (including detectors) are separate from the power range channels.

3. <u>High Nuclear Flux (Power Range) Trip</u> - This circuit trips the reactor when two of the four power range channels read above the trip setpoint. There are two independent trip settings, a high and a low setting. The high trip setting provides protection during normal power operation. The low setting, which provides protection during startup, can be manually bypassed when two out of the four power range channels read above approximately 10 percent power (P10). Three out of the four channels below 10 percent automatically reinstate the trip. The high setting is always active.

4. Overtemperature ΔT Trip - The purpose of this trip is to protect the core against DNB. This circuit trips the reactor on coincidence of two out of the three signals, with one set of temperature measurements per loop. The setpoint for this reactor trip is continuously calculated for each loop by solving the following equation:

$$\Delta T_{setpoint} \leq \Delta T_0 \{K_1 - K_2 \frac{(1+\tau_1 S)}{(1+\tau_2 S)} (T - T') + K_3 (P - P') - f(\Delta I)\}$$

where: ΔT_O = indicated ΔT at rated thermal power;

T = average temperature, ºF;

P = pressurizer pressure, psig;

K_1 = set point bias (ºF)

K_2, K_3 = constants based on the effect of temperature and pressure on the DNB limits, (ºF/ºF), (ºF /psia)

$\frac{1+\tau_1 S}{1+\tau_2 S}2$ = the function generated by the lead-lag controller for T_{avg} dynamic compensation;

τ_1 & τ_2 = time constants utilized in the lead-lag controller for T_{avg}

T' = reference T_{avg} at rated thermal power;

P' = nominal RCS Operating Pressure;

S = Laplace transform operator, sec^{-1};

and $f(\Delta I)$ is a function of the indicated difference between top and bottom detectors of the power--range nuclear ion chambers; with gains to be selected based on measured instrument response during plant start-up tests.

Values for each of the parameters are given in the Technical Specification.

The hot and cold loop temperature signals required for input to the protection and control functions are obtained using thermowell mounted RTDs installed in each reactor coolant loop.

The hot leg temperature measurement in each loop is accomplished using three fast response narrow range RTDs mounted in thermowells. The hot leg thermowells are located within the three scoops previously used for the RTD bypass manifold except for the three RTDs in Loop A. The scoops that are used were modified by drilling a flow hole in the tip of the scoops. The other scoops were not used due to structural obstructions in the vicinity of the RTD locations in the hot leg. For these RTDs, new penetrations were made in the hot leg, maintaining the original spatial orientation.

The cold leg temperature measurements in each loop are accomplished by one fast response narrow range RTD. The existing cold leg RTD bypass penetration nozzle was modified to accept the thermowell and RTD. Temperature streaming in the cold leg is not a concern due to the mixing action of the reactor coolant pump.

Due to temperature streaming, the three fast response hot leg RTDs are electronically averaged to generate the hot leg temperature T_{Have}.

$T_{Have} = (T_{H1} + T_{H2} + T_{H3}) /3$

Where T_{H1}, T_{H2}, and T_{H3} are the three hot leg RTDs in a loop and T_{Have} is the hot leg average temperature in a loop.

The loop T_{avg} and ΔT signals are calculated using the average hot leg temperature and cold leg temperature as follows:

$T_{avg} = (T_{Have} + T_C) /2$

$\Delta T = T_{Have} - T_C$

where T_{avg} is the average loop temperature and ΔT is the difference between the loop average hot leg temperature and the cold leg temperature.

Failure of a hot leg RTD during power operation is detected by the $\Delta T/T_{avg}$ deviation alarms. Once a failed RTD is identified, the operator must remove its input from the three RTD hot leg average calculation. The operator then has two options. Option 1 allows for the summing amplifier in that loop to be rescaled and a manually calculated bias value corresponding to the failed RTD to be input. This procedure results in the two RTD-plus-bias average temperature being equivalent to the three RTD average temperature and is designed to enable 100 percent power operations with a two or three hot leg RTD operation. The second option is for the second element of the dual element RTDs installed at each location to be used in place of the failed RTD element. During normal operation with three hot leg RTDs available, the bias adjustment is set to zero.

The main requirement for reactor protection is that the net lead of the lead-lag filter on T_{avg}, $T_1 - T_2$, be greater than or equal to 17 seconds. All ΔT setpoints are in terms of the measured full power ΔT and, accurate absolute ΔT measurements are not required. Calculations are performed via secondary plant measurements to relate ΔT to power.

Three of the four long ion chamber pairs independently feed each separate overpower ΔT trip channel. Thus, a single failure neither defeats the function nor causes a spurious trip. Changes in F (q) can only lead to a decrease in trip setpoint.

A rod stop and turbine runback are initiated when;

$$\Delta T > \Delta T_{rod\ stop}$$

where: $\Delta T_{rod\ stop} = \Delta T_{setpoint} - B_p$

B_p = a setpoint bias

The turbine runback is continued until ΔT is equal to or less than $\Delta T_{rod\ stop}$. This function serves to maintain an essentially constant margin to trip.

The original FSAR allowed two loop operation and procedures were discussed which describe resetting the overtemperature ΔT trip and

overtemperature ΔT turbine runback (Original FSAR Section 7.2). Since the Emergency Core Cooling System sensitivity analysis was performed with three loop operation only, the plant cannot operate with one or more idle loops (Reference 7.2.1-1).

5. Overpower ΔT Trip - The purpose of this trip is to protect against power level (fuel rod rating protection). This circuit trips the reactor on coincidence of two out of the three signals, with one set of temperature measurements per loop.

The setpoint for this reactor trip is continuously calculated for each channel by solving equations of the form:

$$\Delta T_{setpoint} \leq \Delta T_0 \ \{K_4 - K_5 (\frac{\tau_3 S}{1+\tau_3 S}) T - K_6 (T - T') - f(\Delta I)\}$$

where:	ΔT_O	=	indicated Δ at rated thermal power, ºF;
	T	=	average temperature, ºF;
	T'	=	reference T_{avg} rated thermal power;
	K_4	=	a preset manually adjustable bias (ºF)
	K_5	=	a constant (ºF /ºF /sec)
	K_6	=	a constant (ºF /ºF)
	S	=	Laplace transform operator, sec^{-1};
	$\frac{\tau_3 S}{1+t_3 S}$	=	the function generated by the rate-lag controller for T_{avg} dynamic compensation;
	τ_3	=	time constant utilized in the rate-lag controller for T_{avg};
	f(ΔI)	=	as defined in d. above

Values are given in the Technical Specification.

A similar rod stop and turbine runback function is provided for overpower protection.

6. <u>Low Pressurizer Pressure Trip</u> - The purpose for this circuit is to protect against excessive core steam voids which could lead to DNB. A lead-lag filter is applied to the pressure signal to compensate for transient pressure overshoot. The circuit trips the reactor on coincidence of two out of the three low pressurizer pressure signals. This trip is blocked when either three of the four power range channels or one of two turbine first stage pressure channels read below approximately 10 percent power (P7).

7. <u>High Pressurizer Pressure Trip</u> - The purpose of this circuit is to limit the range of required protection from the overtemperature ΔT trip and to protect against RCS overpressure. The reactor is tripped on coincidence of two out of the three high pressurizer pressure signals.

8. <u>High Pressurizer Water Level Trip</u> - This trip is provided as a backup to the high pressurizer pressure trip. The coincidence of two out of the three high pressurizer water level signals trips the reactor. This trip is bypassed when either three of the four power range channels or one of two turbine first stage pressure channels read below approximately 10 percent power (P7).

9. <u>Low Reactor Coolant Flow Trip</u> - This trip protects the core from DNB following a low flow or loss of coolant flow accident. The means of sensing low flow and a loss of coolant flow accident are as follows:

a. Measured low flow or loss of coolant in the reactor coolant piping

   The low reactor flow signal is actuated by the coincidence of 2/3 signals for any reactor coolant loop. The loss of flow in any two loops causes a reactor trip in the power range above approximately 10 percent (P7). Above 40 percent power (P8), the loss of flow in any loop causes a reactor trip.

b. Monitored electrical supply to the RCP

   The power, voltage, and frequency to each RCP is monitored and the reactor is tripped on a loss of electrical power to the pump by undervoltage signal when (2/3) above approximately 10 percent power (P7). Underfrequency trips RCP breakers, consequently tripping the reactor.

10. <u>Safety Injection System (SIS) Actuation Trip</u> - A reactor trip occurs when the SIS is actuated. The means of actuating the SIS trips are discussed in Section 7.3.

11. <u>Turbine Generator Trip</u> - A turbine trip is sensed by two out of three signals from autostop oil pressure. A turbine trip causes a direct reactor trip above approximately 40 percent power (P-8) and a controlled short term release of steam to the condenser which removes sensible heat from the RCS and thereby avoids SG safety valve actuation.

The turbine control system automatically trips the turbine generator under any of the following conditions:

a. Turbine overspeed

b. Generator electrical faults

c. Low condenser vacuum

d. Thrust bearing failure

e. Low lube oil pressure

f. Low control oil pressure

g. Reactor trip

h. Manual trip

12. Steam/Feedwater Flow Mismatch Trip – Deleted. The steam and feedwater flow mismatch trip was deleted by License Amendment No. 234.

13. Low-Low Steam Generator Water Level Trip - The purpose of this trip is to preserve the steam generator heat sink for removal of long term residual heat. The trip is actuated on two out of the three low-low water level signals in any SG.

14. Manual Trip - The manual actuating devices are independent of the automatic trip circuitry, and are not subject to failures which make the automatic circuitry inoperable. Either of two manual trip devices located in the Control Room can initiate a reactor trip.

7.2.1.1.3 Reactor trip system interlocks

Interlocking functions of the RPS prevent control rod withdrawal when a specified parameter reaches a value less than the value at which reactor trip is initiated. These interlocks are:

1. Rod Stops - Rod stops are added to prevent a reactor trip or prevent an abnormal condition from increasing in magnitude.

   A list of rod stops is given in Table 7.2.1-3. Some of these have been previously noted under permissive circuits, but are listed again for completeness.

2. Rod Drop Protection - Two independent systems are provided to sense a dropped rod, a rod bottom position detection system, and a system which senses sudden reduction in out-of-core neutron flux.

   The primary protection for the dropped RCCA accident is the rod bottom signal derived for each rod from its individual position indication system. With the position indication system, initiation of protection is not dependent on location, reactivity worth, or power distribution changes.

   Backup protection is provided by use of the out-of-core power range nuclear detectors and is particularly effective for larger nuclear flux reductions occurring in the region of the core adjacent to the detectors. The rod drop detection circuit from nuclear flux consists basically of a comparison of each of the four ion chamber signals with the same signal taken through a first order lag network. Since a dropped RCCA will rapidly depress the local neutron flux, the decrease in flux will be detected by one or more of these circuits. Such a sudden decrease in ion chamber current will be seen as a difference signal. A negative signal output greater than a preset value (approximately 10 percent) from any one of the four power range channels will actuate the rod drop protection.

   The Nuclear Instrumentation System (NIS), including the dropped RCCA alarm, is described later in this chapter.

3. Automatic Turbine Load Cutback - Load cutback is initiated by an approach to an over power or over temperature condition This will prevent high power operation which might lead to minimum DNB ratio less than the safety limit specified in Section 4.4.

   Rod stop contacts are located in the rod control logic cabinet and in the rod speed control analog rack. The turbine runback acts by both of the following:

   Reduction of the load reference setpoint of the turbine E-H controller by a preset amount. This is accomplished by reducing the setpoint at a constant rate for a preset time.

   The function of the runback from the OTDT and OPDT trip circuitry is to preclude return to a power level that might result in a core damage because of adverse hot channel factors.

7.2.1.1.4 Reactor trip indication

Any of the following conditions will actuate an alarm:

1. Reactor trip (first-out annunciator)
2. Trip of any reactor trip channel
3. Actuation of any override
4. Significant deviation of any major control variable (pressure, T_{avg}, pressurizer water level, and SG water level)
5. Test initiation in any reactor trip channel (and control channel where feasible)

7.2.1.1.5 Analog Channels

The basic elements comprising an analog protection channel, shown in Figure 7.2.1-2, are a transmitter, power supply, bistable, bistable trip switch and proving lamp, test signal injection switch, test signal injection jack, and test point.

The RPS is designed to achieve isolation between redundant protection channels. The channel design is applied to the analog and the logic portions of the protection system, and is illustrated by Figure 7.2.1-3. Although shown for four channel redundancy, the design is applicable to two and three channel redundancy.

Isolation of redundant analog channels originates at the process sensors and continues along the field wiring and through containment penetrations to the analog protection racks. Isolation of field wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel. Analog equipment is isolated by locating redundant components in different protection racks. Each channel is energized from a separate AC power feed. Logic equipment separation is achieved by providing separate racks, each associated with individual trip breakers. Physical separation is provided between these racks.

Provisions are made to manually place the output of the bistable in a tripped condition for "at power" testing of all portions of each trip circuit including the reactor trip breakers. Administrative procedure requires that the final element in a trip channel (required during power operation) is placed in the trip mode before that channel is taken out of service for repair or testing so that the single failure criterion is met by the remaining channels.

Provision is made for the insertion of test signals in each analog loop. Verification of the test signal is made by plant instruments at test points specifically provided for this purpose. This enables testing and calibration of meters and bistables. Transmitters and sensors are checked against each other and against precision read-out equipment during normal power operation.

Each protection rack includes a test panel containing those switches, test jacks, and related equipment needed to test the channels contained in the rack. A hinged cover encloses the test panel. Opening the cover or placing the test-operate switch in the "TEST" position initiates an alarm. These alarms are arranged on a rack basis to preclude entry to more than one redundant protection rack (or channel) at any time. The test panel cover is designed such that it cannot be closed (and the alarm cleared) unless the test signal plugs (described below) are removed. Closing the test panel cover will mechanically return the test switches to the "OPERATE" position.

Administrative procedures require that the bistable in the channel under test be placed in the tripped mode prior to test. This places a proving lamp across the bistable output so that the bistable trip point can be checked during channel calibration. The bistable trip switches must be manually reset after completion of a test. Closing the test panel cover will not restore these switches to the untripped mode. However, the annunciator on the control board cannot be reset until these switches are returned to the untripped mode.

Channel calibration consists of inserting a test signal from an external calibration signal source into the test signal injection jack. Where applicable, the channel power supply serves as a power source for the calibration source and permits verifying the output load capacity of the power supply. Test points are located in the analog channel and provide an independent means of measuring the calibration signal level.

7.2.1.1.6 Logic Channels

The general design features of the logic system are described below. The trip logic channels for a typical two-out-of-three and a two-out-of-four trip function are shown in Figure 7.2.1-4. The analog portions of these channels are shown in Figure 7.2.1-5. Each bistable drives two relays ("A" and "B" for level and "C" and "D" for pressure). Contacts from the "A" and "C" relays are arranged in a 2/3 and 2/4 trip matrix for Trip Breaker 1. The above configuration is duplicated for Trip Breaker 2 using contacts from the "B" and "D" relays. A series configuration is used for the trip breakers. The logic system testing includes exercising the reactor trip breakers to demonstrate system integrity. Bypass breakers are provided for this purpose. During normal operation, these bypass breakers are open. Administrative controls are used to minimize the amount of time these breakers are closed and to prevent simultaneous closure of both bypass breakers. Indication of a closed condition of either bypass breaker is provided locally on the test panel and on the main control board (RTGB).

As shown in Figure 7.2.1-4, the trip signal from the logic network is simultaneously applied to the main trip breaker associated with the specific logic chain as well as the bypass breaker associated with the alternate trip breaker. Should a valid trip signal occur while AB-1 is bypassing TB-1, TB-2 will be opened through its associated logic train. The trip signal applied to TB-2 is simultaneously applied to AB-1 thereby opening the bypass around TB-1. TB-1 would either have been opened manually as part of the test or would be opened through its associated logic train which would be operational or tripped during a test.

An auxiliary relay is located in parallel with the undervoltage coils of the trip breakers. This relay is connected to a white test light which is used to indicate transmission of a trip signal through the logic network during testing. Lights are also provided to indicate the status of the individual logic relays.

The following procedure illustrates the method used for testing Trip Breaker Number 1 and its associated logic network:

a) With the bypass breaker (AB-1) racked-out, manually close and trip AB-1 to verify operation

b) Rack-in AB-1. Verify that the bypass breaker position is "tripped". Close AB-1. Verify that the bypass breaker position status lights indicates that the breaker is closed. Trip TB-1.

c) Sequentially de-energize the trip relays (A1, A2, A3) for each logic combination (1-2, 1-3, 2-3). Verify that the logic network de-energizes the undervoltage coil on TB-1 for each logic combination. Since the white test light monitors the signal applied to the undervoltage coil, operation of the undervoltage coil can be determined from the white test light.

d) Repeat c) above for every logic combination in each matrix

e) Reset TB-1

f) Trip TB-1 to validate prior test results as evidence by the white test light, and

g) Reset TB-1. Trip and rack-out AB-1.

In order to minimize the possibility of operational errors (such as tripping the reactor inadvertently or only partially checking all logic combinations), each logic network includes a logic channel test panel. This panel includes those switches, indicators, and white test lights needed to perform the logic system test. The arrangement is shown in Figure 7.2.1-6. The test switches used to de-energize the trip bistable relays operate through interposing relays as shown in Figures 7.2.1-2 and 7.2.1-5. This approach avoids violating the separation philosophy used in the analog channel design. Thus, although test switches for redundant channels are conveniently grouped on a single panel to facilitate testing, physical and electrical isolation of redundant protection channels is maintained by the inclusion of the interposing relay which is actuated by the logic test switches.

The reactor trip bistables are mounted in the analog protection racks and are the final operational component in an analog protection channel. Each bistable drives two logic relays ("C" and "D"). The contacts from the "C" relays are interconnected to form the required actuation logic for Trip Breaker Number 1. The transition from channel identity to logic identity is made at the logic relay coil/relay contact interface. As such, there is both electrical and physical separation between the analog and the logic portions of the protection system. The above logic network is duplicated for Trip Breaker Number 2 using the contacts from the "D" relays. Therefore, the two redundant reactor trip logic channels are physically separated and electrically isolated from one another. Overall, the RPS is comprised of identifiable channels which are physically, electrically, and functionally separated and isolated from one another.

7.2.1.1.7 Nuclear Instrumentation System

The NIS (Figure 7.2.1-7) consists of eight independent channels which provide inputs to the reactor protection system: two of these being the source range, two the intermediate range, and four the power range channels. In addition, there are three auxiliary channels, the visual-audio count rate channel, the comparator channel, and the startup rate channel. The various detectors associated with the eight primary channels are shown in relative position with respect to the core configuration on Figure 7.2.1-8. Figure 7.2.1-9 shows the typical range of operation of each channel.

Nuclear plant protection assurance is obtained from the three ranges of out-of-core nuclear instrumentation. Separation of redundant protective channels is maintained from the neutron sensor with its associated cables to the signal conditioning equipment in the Control Room with its associated output wiring, indicating or recording devices and protective devices. Where redundant protective channels are combined to provide nonprotective functions, the required signals are derived through isolation amplifiers. These devices are designed so that open or short circuit conditions as well as the

application of 120 V AC or ±150 V DC to the isolated side of the circuit will have no effect on the input or protection side of the circuit. As such, failures on the nonprotective side of the system will not affect the individual protection channels. Redundant channels are powered from independent power sources, each channel being provided with the necessary power supplies for its detectors, signal conditioning equipment, trip bistables, and associated trip relays. The nuclear instrumentation channels are mounted in four separate racks to provide the necessary physical separation between redundant channels.

The overpower protection provided by the out-of-core nuclear instrumentation consists of three discrete levels. Continuation of startup operation or power increase requires a permissive signal from the higher range instrumentation channels before the lower range level trips can be manually blocked by the operator.

A one-of-two intermediate range permissive signal (P6) is required prior to source range level trip blocking and detector high voltage cutoff. Source range level trips are automatically reactivated and high voltage restored when both intermediate range channels are below the permissive (P6) level. There are provisions for administratively reactivating the source range level trip and detector high voltage, if required. Source range level trip block and high voltage cutoff are automatically maintained by the same power range permissive (P10) which permits blocking of the intermediate range and low-range, power-range flux level trips.

The intermediate range level trip and low-range, power-range level trip can only be blocked after satisfactory operation and permissive information are obtained from two-of-four power range channels. Individual blocking switches are provided so that the low-range, power-range trip, and the intermediate range trip can be independently blocked. These trips are automatically reactivated when any three of the four power range channels are below the permissive (P10) level, thus ensuring automatic activation of more restrictive trip protection.

Blocking of any reactor trip function is indicated by the control board status lights. Channels which provide reactor plant protection through one-of-two or one-of-four logic matrices are equipped with positive detent type trip-bypass switches to enable channel testing. The trip-bypass condition for individual channels is indicated at the control board and at the nuclear instrumentation racks. The reactor plant protection afforded by the high-range, power-range trip is never blocked or bypassed.

The out-of-core NIS consists of various plug-in type modules which perform the functions indicated on Figure 7.2.1-7 for the source, intermediate, and power ranges. Components designed to military specifications are used, where possible, in conjunction with a conservative design stressing reliability, derating of components and circuits, and the use of field-proven circuits.

On-line testing and calibration features are provided for each channel. The test signals are superimposed on the normal sensor signal during plant operation. This permits valid trip conditions to over-ride the test signal since the sensing elements are never removed from the circuit.

7.2.1.1.7.1 Source Range Instrumentation - General Description

Two independent source range channels are provided. Each receives pulse-type signals from a proportional counter. The preamplified detector signal is received by the source range instrumentation conditioning equipment located in the Control Room racks. The detector signal, which is a random count rate proportional to leakage neutron flux, is conditioned for conversion to an analog signal proportional to the logarithm of the neutron flux count rate.

The isolated analog signals from each channel are sent to various recording and indicating devices to provide the operator with necessary startup information. Bistable units also located in the racks are used to generate alarms and reactor trip signals. Trip signals from the bistables are transmitted to relays in the protection relay racks where the necessary logic involved in generating reactor trip signals is performed.

An isolated count rate signal derived from either channel is connected to a scaler-timer. This same signal also feeds the audio count rate channel which provides an audible count rate signal, proportional to the neutron flux. Speakers are provided both in the containment and in the Control Room. Startup rate indication is also provided for each source range channel, and a startup rate meter is installed on the reactor and turbine-generator board to give the operator more accurate information on the core flux during startup. The startup rate signals are generated from the isolation amplifier output since there is no protection function involved.

7.2.1.1.7.2 Intermediate Range Instrumentation - General Description

Two independent compensated ionization chambers provide extended flux coverage from the upper end of the source range to approximately 100 percent power. The equipment for each channel, including the high voltage and compensating voltage power supplies, are located in separate drawers. To maintain separation between these redundant channels, the drawers are mounted in separate racks. The signal conditioning equipment furnishes an analog output voltage proportional to the logarithm of the neutron flux spectrum. Each channel covers approximately eight decades of leakage flux. Isolation amplifiers (for startup-rate circuits, remote recording, remote indication, etc.) and bistable amplifiers (for permissives, rod stop and reactor trip) use this analog voltage to indicate plant status and provide the necessary plant protection functions. All relays associated with plant control or protection are located in the logic or auxiliary relay racks.

7.2.1.1.7.3 Power Range Instrumentation - General Description

Four dual section, uncompensated ionization chambers are used for power range flux detection. Each chamber provides two current signal outputs (one from each section) to signal conditioning equipment in the Control Room racks. Each chamber has an independent high voltage power supply. The individual current signals obtained from each section of the detector are proportional to upper core and lower core neutron flux, respectively. These provide core flux status information at the instrument racks and, through isolation amplifiers, the same information at the control console. A separate output furnishes bias signals used in the overpower and overtemperature ΔT reactor trip functions. The individual current signals are combined to provide a total signal which is proportional to average core flux in the associated core quadrant. This

total signal is conditioned to provide an analog voltage signal for use in permissive control and protection bistable amplifiers.

Isolation amplifiers, which provide remote control signals and core power status information to the operator and computer, also utilize the average power analog signal. The four power range channels are operated from separate AC sources and are housed in separate racks so that a single failure will not cause loss of protection functions. Redundant relays for the protection functions are located in the logic portion of the protection system.

Isolated analog outputs from the power range channels are compared in a separate auxiliary channel drawer. This comparator provides the operator with annunciation of deviations in average power between the four power range channels. Switches are provided to defeat this comparison for a failed channel so that subsequent deviations or failures among the three remaining channels are annunciated.

7.2.1.1.7.4 Detectors

The NIS channels which provide inputs into the reactor protection system employ six detector radial locations containing a total of eight detectors (two proportional counters, two compensated ionization chambers and four dual section uncompensated ionization chamber assemblies) installed around the reactor in the primary shield. Windows in the primary shield minimize leakage flux attenuation and distortion.

BF_3 gas filled proportional counters having a nominal thermal neutron sensitivity of ten counts per neutron per square centimeter per second, provide pulse signals to the source range channels. These detectors are installed on opposite "flat" portions of the core containing the primary startup sources, at an elevation approximating the quarter core height.

Compensated ionization chambers serve as neutron sensors for the intermediate range channels and are located in the same instrument wells and detector assemblies as the source range detectors. These detectors have a nominal thermal neutron sensitivity of 7.6×10^{-14} amperes per neutron per square centimeter per second. Gamma sensitivity is less than 3×10^{11} amperes per Roentgen per hour when operated uncompensated, and is reduced to approximately 3×10^{-13} amperes/R/hr in compensated operation. The detectors are positioned at an elevation corresponding to the center of the quarter core height.

The detector assemblies containing one each of the above-mentioned detectors use aluminum enclosures. High density polyethylene, used as a moderator-insulator within the detector assemblies, will be confined at temperatures associated with a loss-of-coolant accident (LOCA). The detectors are connected to the junction box at the top of the detector well by special high temperature, radiation-resistant cables.

The remaining four detector assemblies contain the power range ionization chambers. Each provides two current signals corresponding to the neutron flux in the upper and lower sections of a core quadrant. These detectors have a total neutron-sensitive length of ten feet and a nominal thermal neutron sensitivity for each section of 3.1×10^{-13} amperes per neutron per square centimeter per second. Gamma sensitivity of each section is approximately 1.4×10^{-10} amperes per Roentgen per hour.

The detector assemblies for power range operation are installed vertically and located equidistant from the reactor vessel at all points, and, to minimize neutron flux pattern distortions, within one foot of the reactor vessel. Cabling from individual detector wells to the containment penetrations and to the instrument racks in the Control Room are routed in individual conduits, with physical separation between the penetrations and conduits associated with redundant protective channels.

7.2.1.1.7.5 Detailed description

The source range output information is tabulated in Table 7.2.1-4. The detector for each source range channel is a BF_3 gas filled proportional counter. The signal received from the counter has a range of 1 to 10^6 pulses per second randomly generated and is received through a low noise variable gain preamplifier located outside the containment. After the initial gain setting, the variable gain preamplifier is operated as a fixed gain preamplifier.

The preamp has internal provisions for generating self-test frequencies. These test oscillator circuits are energized by a switch located on the associated source range drawer. The source range channel power supplies furnish low voltage for preamp operation as well as low voltage for the drawer-mounted modules. The preamp is solid state in design with discrete components and includes an impedance matching network between the preamp output and the 75-ohm triaxial cable.

The preamp output is received at the post-amplifier located on the source range drawer. This module provides amplification and discrimination, both of which are adjustable. Discrimination is provided between neutron flux pulses and combined noise and gamma-generated pulses. The discriminator supplies two outputs: one output (isolated) to a scaler-timer unit on the visual-audio channel drawer (see source range auxiliary equipment); and the other to a pulse shaper (transistorized flip-flop circuit) which supplies a constant amplitude pulse to the log integrator module within the source range drawer.

Logarithmic integration of the pulse signal is performed in another modular unit to obtain an analog DC signal. The log signal is then amplified for local indication on the front panel of the source range drawer, and is also delivered through a parallel run to the source range level bistables and isolation amplifier. The analog output signal is proportional to the count rate being received from the sensor and is displayed by the front panel meter on a scale calibrated logarithmically from 10^0 to 10^6 cps. The solid state isolation amplifier provides five analog outputs, all of which are adjustable through attenuator controls. Three outputs are used as follows: as remote indication (0-1 ma DC); as remote recording (0-37.5 mv DC); and as an input to the computer (0-5 V DC). A 0-10 V DC output is used by the startup-rate amplifier to produce a startup-rate indication at the main control board. The remaining output (0-5 V DC) is a spare.

All bistables will employ a basic plug-in module with the external wiring determining the mode of operation (latching or non-latching and direction of output change with rising power). Bistables will have two adjustments: "Trip Adjust" and "Loop Adjust." The first adjustment determines the trip point of the bistable, while the second determines the "dead zone" difference between the trip and release points of the bistable. The bistable module card will include a relay driver circuit made up of an silicon control rectifier (SCR) and full-wave bridge configuration. The bistable output will control the SCR gate which, in turn, controls conduction of the full-wave bridge supplying the power to drive up to four 115 V AC WBF relays. All relays are located remote from the NIS racks.

Of the three bistables monitoring the source range level amplifier signal, one is a spare, one is used to monitor shutdown flux level only, and the third monitors source range operation during shutdown and startup operation and provides a reactor trip on high flux level. The reactivity of the core during shutdown is monitored by a bistable to ensure protection of plant personnel working in the containment. Bistable tripping will initiate local visual and audible annunciation and remote audible annunciation of any abnormal increase in core activity. Visual annunciation occurs at the NIS rack and on the main control board. Audible annunciation is handled by the annunciator located in the Control Room, and the evacuation horn located in the containment.

These annunciators ensure that plant personnel will be alerted to any potentially hazardous condition. This bistable action will be manually blocked by deliberate operator action during plant startup. Blocking is continuously annunciated at the control board during source range operation. The bistable trip point is approximately 3 times the flux level recorded during full shutdown.

The source range level bistable monitors the core activity during the full span of source range operation until such time as the intermediate range channels assume control of that portion of the reactor protection which is being supplied by nuclear instrumentation. At that time, when the intermediate range permissive P6 is available, the source range reactor trip bistable may be manually blocked and high voltage removed from the B10 detector by the operator actuating two momentary-contact switches located on the main control board.

A fourth bistable-relay driver unit is used as a high voltage failure monitor. Loss of this voltage actuates the bistable, the relay driver and then the associated relay. The relay provides control board annunciation through a one of two matrix formed with a similar relay controlled by the other source range. Failure of either source range high voltage actuates this common annunciator on the main control board. During normal operation the source range high voltage will be cut off (mentioned above) when manual block of the source range trips is initiated.

A test-calibrate module is also included in each source range drawer for self check of that particular channel. A multi-position switch on the source range front panel controls this module and also the operation of the built-in oscillator circuits in the preamp. The module is capable of injecting test signals of 60, 10^3, 10^5, and 10^6 cps at the input to the post-amplifier, or a variable DC voltage corresponding to 1 to 10^6 cps at the input to the log amplifier. An interlock between the trip bypass switch and the test-calibrate switch will prevent inadvertent actuation of the reactor trip circuits, (i.e., the channel cannot be put in the test mode unless the trip is defeated). Trip bypass will be annunciated on the source range drawer and on the main control board per the proposed IEEE 279 Standard, Section 4.13. Operation of the test-calibrate module will be annunciated on the control board as "NIS Channel Test." This common annunciator for all NIS channels will be alarmed when any channel is placed in the test position and will alert the operator that a test is being performed at the NIS racks.

a) Visual-Audio Count Rate - The visual-audio count rate receives a signal from each of the source range channels. This isolated signal originates at the discriminator output in each source range. A switch on the audio count rate drawer selects either source range channel for monitoring. The selected signal is fed to a scaler-timer unit which permits count accumulation in the preset time or preset count mode. A visual display to 6 digits is presented through counting strips located on the front of the audio count rate drawer.

   A "Scale Factor" switch permits division of the scaler output signal by 10, 100, 1000 or 10,000. This signal, derived from the printer output of the scaler, is conditioned and sent to two of the audio amplifiers which power two speakers: one speaker located in the Control Room, and the other in the containment. These speakers give plant personnel an audible indication of the count rate. Since the audio signal is taken from the coded scaler output, adjustment of the scale factor switch will alter only the audible count rate. This enables the operator to maintain the audible count rate at a distinguishable level.

b) Remote Count Rate Meter - The remote meter indication is an analog signal proportional to the count rate being received, and is obtained from the 0-1 ma DC isolation amplifier output.

   The meter is mounted on the main control board and calibrated logarithmically from 10^0 to 10^6 cps. This meter gives the same indication at the control board as is displayed by the local meter on the corresponding source range drawer.

c) Remote Recorder - This recorder is capable of continuously recording all NIS channels at any given time. In the case of the source ranges, a 0-37.5 mvDC signal, proportional to the count rate range of 10^0 to 10^6 cps, is supplied for recording during source range operation.

d) Startup-Rate Circuitry - The startup-rate drawer receives four input signals (0-10V DC) one from each of the source and intermediate range channels. Four rate amplifier modules condition these signals and output four rate signals to the respective Control Room startup-rate (SUR) meters. A test module is provided which can inject a test signal into any one of the rate circuits and can be monitored on a test meter mounted on the front panel of this drawer. Two power supplies are provided to assure rate indication from at least one Source and Intermediate Range channel pair.

7.2.1.1.7.6 Intermediate Range Detailed Description

Intermediate Range output information is tabulated in Table 7.2.1-5. Each intermediate range channel receives a direct current signal from a compensated ion chamber and supplies positive high voltage and compensating (negative) high voltage to its respective detector. The compensating high voltage is used to cancel the effects of gamma radiation on the signal current being delivered to the intermediate range channel. Both high voltage supplies will be adjustable through controls located inside the channel drawer. The detector signal is received by the intermediate range logarithmic amplifier. The modular unit, comprised of several operational amplifiers and associated discrete solid state components, produces an analog voltage output signal which is proportional to the logarithm of the input current. This signal is used for local indication and it is monitored by the isolation amplifier and the various bistable relay-driver modules within the intermediate range drawer. A 10^{-11} ampere signal is continuously inserted and serves as a reference during gamma compensation. Local indication is provided by a meter mounted on the front panel of the drawer which has a logarithmic scale calibration of 10^{-11} to 10^{-3} amperes. The isolation amplifier is the same solid state module that is used in the source range; it supplies the same five outputs and for the same usage. Six bistable relay-driver units are used in the intermediate range drawer to provide the following functions:

a) One monitors the positive high voltage

b) One monitors the compensating high voltage

c) One provides the permissive P6

d) One provides rod stop (blocks automatic and manual rod withdrawal)

e) One provides reactor trip

f) One serves as a spare

The intermediate range permissive P6 bistable drives two WBF relays (for redundancy) and the relays from each channel are combined in 1 of 2 matrices to provide the permissive function and control board annunciation of permissive availability. Permissive P6 permits simultaneous manual blocking of the source range trips and removal of the source range detector high voltage. Once source range blocking has been performed, the operator may, through administrative action, defeat permissive P6 and reactivate the source range high voltage and trip functions if required. This defeat is accomplished by the coincident operation of two control board mounted,

momentary-contact switches. This provision, however, is only operational below permissive P10 which is supplied by the power range channels. Above P10, the P6 permissive logic is bypassed and the P10 permissive maintains source range cutoff. The level bistable relay-driver unit which provides the intermediate range rod stop function also drives two WBF relays. Again, one-of-two matrices formed by the relays from the two intermediate range channels supplies the rod stop function and control board annunciation. Blocking of the outputs of these matrices is administratively performed when nuclear power is above permissive P10 and can only be accomplished by deliberate operator action on two control board mounted switches.

The intermediate range reactor trip function is provided by a similar circuit arrangement, the only difference being the trip point of the bistable units. The same control board switches which control blocking of the rod stop matrices also provide blocking action for the reactor trip matrices. These blocks are manually inserted when the power range of instrumentation indicates proper operation through activation of the P10 permissive function. On decreasing power, however, the more restrictive intermediate range trip functions are automatically reinserted in the protective system. While these trips are blocked, there will be continuous illumination on the main control board of "Intermediate Range Trip Blocked." The high voltage failure monitors provide both local and remote annunciation upon failure of the respective high voltage supplies. A common "Intermediate Range Loss of Detector Voltage" and separate "N-35 Loss of Comp Volt" and "N-36 Loss of Comp Volt" are provided as control board annunciators for the intermediate ranges.

Administrative testing of each intermediate range channel is provided by a built-in test-calibrate module which injects a test signal at the input to the log amplifier. The signal is controlled by a multi-position switch on the front of each intermediate range drawer. Fixed and variable test signals are available both of which are selectable in decade increments from 10^{-11} through 10^{3} amperes.

As in source range testing, the test switch on the intermediate range must be operated in coincidence with a trip bypass on the drawer. An interlock between these switches prevents injection of a test signal until the trip bypass is in operation. Removal of the trip bypass also removes the test signal.

1. Remote Meter - The remote meter indication is in the form of an analog signal (0-1 ma) proportional to the ion chamber current. The isolation amplifier in each channel supplies this output to a separate meter. Meter calibration is 10^{-11} to 10^{-3} amperes.

2. Remote Recorder - This is the same recorder described above for the source range. A 0-50 mv DC signal from the isolation amplifier is supplied to the recorder and is proportional to the ion chamber current range of 10^{-11} to 10^{-3} amperes. The signal from I.R. Number 1 is available in position 3 of the recorder selector switches, and I.R. Number 2 in position 4.

7.2.1.1.7.7 Power Range Detailed Description

The power range output information is tabulated in Table 7.2.1-6. The power range detector is a long uncompensated ion chamber assembly which is comprised of two separate neutron sensitive sections. Each section supplies a current signal to the associated power range. There is one high voltage power supply per channel and it supplies voltage to both sections of the associated detector. The two signals are received at the channel input and handled through separate ammeter-shunt assemblies. Four full-scale ranges can be selected for each ammeter through switches located on the front panel of the power range drawer, 100 ua, 500 ua, 1 ma, and 5 ma DC. The switch selects shunt resistors for the meter but never interrupts the ion chamber signal to the power range channel. The circuit is so designed that a failure of the meter or switch will not interrupt the signal to the average power circuitry.

The individual currents are displayed on the two front panel ion chamber current meters and are then sent to separate isolation amplifiers. There are two isolation amplifiers monitoring each of the two individual current signals. The unit feeding the ºT function is being used for its impedance matching characteristics rather than for isolation. All of the isolation amplifiers are capable of providing the same five output ranges as the isolation amplifiers previously described in relation to the source and intermediate ranges. Two of the isolation amplifiers (used as impedance matching networks), one monitoring each of the currents, supply signals to the ºT reset. The other two isolation amplifiers provide output for the remote, meter and computer. The individual current signals are then sent to a summing amplifier module which outputs a linear 0-10 V DC signal proportional to their total or sum. This linear amplifier has three controls: a "Zero" adjust located on the module itself, a "Fine Gain" adjust with a calibrated dial located on the drawer's front panel and a "Coarse Gain" adjust located inside the drawer. The output signal from this unit corresponds to 0 to 120 percent of full power and is displayed on a percent full power meter on the front panel of the power range drawer. This same signal is delivered directly to three isolation amplifiers, a dropped rod sensing assembly, and six bistable relay-driver modules. These isolation amplifiers are identical to those previously described and the outputs are the same in number and range but are used in different functions. (Specific outputs from the amplifiers are discussed in the auxiliary equipment section which follows.)

The dropped-rod sensor assembly is an operational amplifier unit which incorporates an adjustable lag network at one input and a non-delayed signal on the other. The unit compares the actual power signal with the delayed power signal received through the lag network and amplifies the difference. This amplified differential signal is delivered to a bistable relay-driver unit which trips when the level of this signal exceeds a preset amount.

Tripping of this unit indicates a power level change over the lag period which would be indicative of a dropped rod. This bistable unit is a latching type, ensuring that the necessary action will be initiated and carried to completion. Specifically, the unit controls dual WBF relays which, in one-of-four logic matrices, provide a rod stop and turbine load cut-back signal, a control board annunication signal, and a computer input signal. A reset switch on the associated power range drawer must be operated manually to remove the trip functions and reset the bistable.

The bistable units which sense the power level signal as derived by the linear amplifier are non-latching and perform the following functions:

a) Overpower rod stop (blocks automatic and manual rod withdrawal)

b) Permissive functions (provisions for three are incorporated in the design but only two, P8 and P10, are used)

c) Low-range reactor trip

d) High-range reactor trip

The overpower rod stop and permissive bistables are units which trip on high power level and control WBF relays in the remote relay racks. The rod stop relay matrices (one-of-four) provide a rod stop function to the rod control system and a main control board annunciation. Two-of-four logic, developed by relays controlled through the respective power range bistables, provide the signals required for the permissive functions. One set of relays provides permissive P10, as was previously discussed with regard to its use in the source range and intermediate range. A second set of relays are available to provide inputs to permissive P8, a third set of bistables are provided to contribute to the overall logic for permissive P9 but are not used.

Permissive P8 and P10 are supplied solely by nuclear instrumentation.

For this reason, the nuclear instrumentation design provides for main control board annunciation of P8 and P10 availability. Permissive P10 is used in all three ranges of nuclear instrumentation while P8 is provided by nuclear instrumentation for use in the RPS.

The low range trip bistable actuates two WBF relays in the logic system. The two relays provide redundancy within the logic portion of the protection system. Each relay is used in a separate matrix with the relays from the other power range channels to continue the redundancy. The logic circuitry formed by the contacts on these relays provide for one-of-four and two-of-four logic outputs. The low range trip relays provide the following functions:

a) Computer input (single channel)

b) Low range trip annunciation (two-of-four coincidence)

c) Reactor-trip signal to RPS (two-of-four coincidence)

d) Annunciation of "Single Channel Low Range Trip" (one-of-four)

e) Status Light (Single Channel)

Provisions for manually blocking these functions become available when 2 of 4 power ranges exceed the permissive P10 level. Operator action on two control board mounted momentary-contact switches then initiates the blocking action. A control board permissive status light, "Power Range Low Range Trip Blocked," will be illuminated continuously when the trip function is blocked. On decreasing power, three-of-four power ranges below the P10 power level will automatically reactivate the low range trip.

The high range reactor trip logic circuitry is developed identically to the low range reactor trip circuitry, but no provision for blocking is included.

The high range trip remains active at all times to prevent any continuation of an overpower condition.

An additional bistable unit monitors the high voltage power supply in the power range. Operation of this unit is identical to that for the source and intermediate ranges. The bistable provides relay actuation in the remote relay racks on failure of power range high voltage. While there is a separate relay for each power range, they control a common "Power Range Loss of Detector Voltage" annunciator on the main control board. Separate local indication of high voltage failure is provided on the power range drawers.

The test-calibrate module which is provided on each power range is capable of injecting test signals at several points in the channel. In all cases, the test signals are superimposed on the normal signal. A bypass of the dropped rod-rod stop circuit will be required during channel test. Since this circuit produces a load cutback through a one-of-four logic matrix for a sudden power change, it must be bypassed to prevent an inadvertent dropped rod indication. An interlock between the bypass switch and channel test switch is provided as was done in the source and intermediate ranges. The bypass switch from each power range will activate a common annunciator, "NIS Trip/Rod Drop Bypass," but individual bypass status lights will identify the particular channel. The remaining bistables which will be affected during channel test do not require bypasses since they operate in two-of-four logic. Test signals can be injected independently or simultaneously at the input of either ammeter-shunt assembly to appear as the individual ion chamber currents. Operation of the test-calibrate switch on any power range will cause the "Channel Test" annunciator to be alarmed on the main control board.

1. Comparator - The comparator receives an isolated signal from each of the four power ranges. These signals are conditioned in separate operational amplifier circuits and then compared with one another to determine if a preset deviation of power levels has occurred between the highest indicating and the lowest indicating power ranges. Should such a deviation occur, the comparator output will operate a remote relay to actuate the control board annunciator, "Power Range Channel Deviation." This alarm will alert the operator to either a power unbalance being monitored by the power ranges or to a channel failure. Through other indicators, the operator can then determine the deviating channel(s) and take corrective action. Should correction of the situation not be immediately possible (e.g., a channel failure, rather than reactor condition), provisions are available to eliminate the failed channel from the comparison function. The comparator can then continue to monitor the active channels.

b) Remote Meter - The remote meters receive the 0-1 ma DC isolated output that is available from each power range. This indication corresponds to that shown on the power range drawer. The signal is displayed on a meter scale calibrated from 0 to 120 percent of full power.

c) Overpower Recorder - A pair of recorders are used to monitor the individual average power indications from the four power ranges. Each recorder provides continuous monitoring of two power range channels and has a full-scale deflection time of 0.125 sec. The recorders are capable of displaying overpower excursions up to 200 percent of full power. A power range isolated output of 0-50 mv DC will correspond to the range of zero percent to 200 percent full power for these recorders.

d) Remote Meter (Delta Flux) - Four control board mounted meters display the flux difference between the upper and lower ion chambers directly for each of the power range detectors.

7.2.1.1.7.8 Miscellaneous Control and Indication Panel

Indicating lights (one per power range channel) are provided on this panel to be used during test of the dropped rod-rod stop function. Illumination of one of the lights indicates completion of the relay tripping function, concerned with turbine load cutback and rod stop, for the channel under test.

Switches are also provided on this panel to permit a failed power range channel's overpower-rod stop function to be bypassed. This will allow normal power operation to continue while the failed channel is repaired.

7.2.1.1.7.9 Output Information

Tables 7.2.1-4, 7.2.1-5, and 7.2.1-6 provide the NIS control and indication output information for the source, intermediate and power ranges, respectively.

7.2.1.1.7.10 Testing Nuclear Instrument Channels

In the source and intermediate ranges where the trip logic is one-out-of-two for each range, bypasses are provided for the testing procedure.

Administrative controls prevent the nuclear instrumentation source range and intermediate range protection channels from being disabled during periodic testing.

Nuclear instrument power range channels are tested by superimposing a test signal on the normal sensor signal so that the reactor trip protection is not bypassed. Based upon coincident logic (2/4) this will not trip the reactor; however, a trip will occur if a reactor trip is required. Power range overpower protection cannot be disabled since this function is not affected by the testing of circuits. In addition, the rod position system would provide indication and associated corrective actions for a dropped rod condition.

7.2.1.1.7.11 Energy Supply

A loss of power in the RPS causes the affected channel to trip. All bistables operate in a normally energized state and go to a de-energized state to initiate action.

Current to the mechanisms is interrupted by opening either of the reactor trip breakers. The 70 volt DC maintenance supply will also be interrupted since this supply receives its input power through the reactor trip breakers as described in Section 7.6 and Chapter 8.0.

7.2.1.1.8 Rod Drive Power

Power to the full length CRDM is supplied through duplicate series-connected circuit breakers. Upon proper coincidence of trip signals, as described above, the undervoltage coils and the auto shunt trip relays (part of these circuit breakers) are de-energized, opening both breakers and interrupting power to the full length CRDM. Rapid reactivity insertion is provided by the insertion of the RCCA by gravity fall on loss of power.

The solid state rod control system is operated from two parallel connected 400 kVa generators which provide 260 volt line-to-line, three phase, four wire power to the rod control circuit through two series connected reactor trip breakers. This AC power is distributed from the trip breakers to a line-up of identical solid state power cabinets using a single overhead run of enclosed bus duct which is bolted to, and therefore comprises, part of the power cabinet arrangement. Alternating current from the motor-generator sets is converted to a profiled direct current by the power cabinet and is then distributed to the mechanism coils (Figure 7.2.1-10). Each complete rod control system includes a single 70 volt DC power supply which is used for holding the mechanisms in position during maintenance of normal power supply.

This 70 volt supply, which receives its input from the AC power source downstream of the reactor trip breakers, is distributed to each power cabinet and permits holding mechanisms in groups of four by manually positioning switches located in the power cabinets. The 30 ampere output capacity limits the holding capability to five rods.

7.2.1.1.8.1 Reactor Trip

Current to the mechanisms is interrupted by opening either of the reactor trip breakers. The 70 volt DC maintenance supply will also be interrupted since this supply receives its input power through the reactor trip breakers.

7.2.1.1.8.2 Trip Breaker Arrangement

The trip breakers are arranged in the reactor trip switchgear in individual metal-enclosed compartments. The 1000 ampere bus work making up the connections between trip breakers will be separated by metal barriers to prevent the possibility that any conducting object could short circuit or bypass trip breaker contacts.

7.2.1.1.8.3 Maintenance Holding Supply

The 70 V DC holding supply and associated switches have been provided to avoid the need for bringing a separate DC power source to the rod control system during maintenance on the power cabinet circuits. This source is adequate for holding a maximum of five mechanisms and satisfies all maintenance holding requirements.

7.2.1.1.8.4 Control System Construction

The rod control system equipment is assembled in enclosed steel cabinets. Three phase power is distributed to the equipment through a steel enclosed bus duct, bolted to the cabinets. DC power connections to the individual mechanisms are routed to the reactor head area from the solid state cabinets through insulated cables, enclosed junction boxes, enclosed reactor containment penetrations, and sealed connectors. In view of this type of construction, any accidental connection of either an AC or DC power source, either internal or external to the cabinets, is not considered credible.

7.2.1.1.9 Primary Power Source

The primary power sources for the RPS are the instrument buses described in Chapter 8.0. The source of electrical power for the measuring elements and the actuation of circuits in the engineered safety features (ESF) instrumentation is also from these buses.

7.2.1.2 Design Basis Information

7.2.1.2.1 Reactor Protection System and DNB

The following is a description of how the RPS prevents DNB.

The plant variables affecting the DNB ratio are:

a) Thermal power

b) Coolant flow

c) Coolant temperature

d) Coolant pressure

e) Core power distribution (hot channel factors)

Figure 7.2.1-11 illustrates typical core limits for which DNBR for the hottest fuel rod is equal to the safety limit and shows the overpower and overtemperature ΔT reactor trips locus as a function of T_{avg} and pressure. This illustration is derived from the inlet temperature versus power relationships. Figure 7.2.1-12 shows analog symbols used in Figures 7.2.1-2, 3, 7, 13 through 16. Figure 7.2.1-13 indicates T_{avg} vs ΔT control and protection system logic and is typical for one reactor coolant loop.

Variations in both flow and power are monitored by the overpower and overtemperature ΔT trips since a decrease in flow would have the same effect on the measured loop ΔT signal as an increase in power. It is the nature of the DNB limits that a reduction in flow of 10 percent would require a reduction in power of only about 5 percent to maintain the same DNBR, all other variables remaining constant. Thus, the permissible ΔT increases somewhat at a reduced flow. The trip setpoints are therefore set for a maximum flow. A reduction in flow increases the margin between the trip point and the actual core limit. Periodic measurements using the in-core instrumentation system are used to verify that the actual core power distribution is within design limits.

Reactor trips for a fixed high pressurizer pressure and for a fixed low pressurizer pressure are provided to limit the pressure range over which core protection depends on the overpower and overtemperature ΔT trips.

Reactor trips on nuclear overpower and low reactor coolant flow are provided for direct, immediate protection against rapid changes in these parameters. However, for all cases in which the calculated DNBR approaches the safety limit, a reactor trip on overpower and/or overtemperature ΔT would also be actuated.

The RPS actuates a reactor trip for a set of conditions for which the calculated DNBR for the worst fuel rod approaches the safety limit. Because of the statistical nature of the DNB correlation and the statistical makeup of a portion of the hot channel factors, there exists a finite probability of a few rods being in DNB for a calculated ratio of equal to the safety limit for the worst fuel rod.

For the anticipated abnormal conditions, it is highly unlikely that the exact combination of conditions (reactor coolant pressure, temperature and core power, instrumentation inaccuracies, etc.) that cause a DNB of 1.17 will be approached before a reactor trip. In any event, the calculated DNBR at the worst fuel rod is near the safety limit for only a few seconds.

The hottest fuel rods are not adjacent to one another. They are located near the spare RCCA thimbles. Fuel rods located in the immediate vicinity of the hottest fuel rod have a DNBR higher than that rod.

The ΔT trip functions are based on the differences between measured hot leg and cold leg temperatures and have transient compensation terms based on T_{avg}.

The ΔT trip functions are provided with a nuclear flux feedback to reflect a measure of axial power distribution. This will assist in preventing an adverse axial distribution which could lead to exceeding the allowable core conditions.

Axial power distribution monitoring and control is discussed in Section 7.7.1.6.

In the event of a difference between the upper and lower ion chamber signals that exceeds the desired range, automatic feedback signals are provided to reduce the overpower-overtemperature trip setpoints, block rod withdrawal and reduce the load to maintain appropriate operating margins to these trip setpoints.

7.2.1.2.2 Principles of design

The following paragraphs summarize the principle of design as related to the proposed IEEE 279 "Standard, Nuclear Power Plant Protection Systems," August, 1968.

1. Redundancy and Independence - The protective systems are redundant and independent for all vital inputs and functions. Each channel is functionally independent of every other channel and receives power from two independent sources.

2. Manual Actuation - Means are provided for manual initiation of protective system action. Failures in the automatic system do not prevent the manual actuation of protective functions. Manual actuation is designed to require the operation of a minimum of equipment.

3. Channel Bypass or Removal from Operation - The system is designed to permit any one channel to be maintained, tested, or calibrated during power operation without system trip. During such operation the active parts of the system continue to meet the single failure criterion, since the channel under test is either tripped or makes use of superimposed test signals which do not negate the process signal.

   EXCEPTION: "One-out-of-two" systems are permitted to violate the single failure criterion during channel bypass provided that acceptable reliability of operation can be otherwise demonstrated.

4. Capability for Test and Calibration - The bistable portions of the protective system (e.g., relays, bistables, etc.) provide trip signals only after signals from analog portions of the system reach preset values. Capability is provided for calibrating and testing the performance of the bistable portion of protective channels and various combinations of the logic networks during reactor operation.

The analog portion of a protective channel (e.g., sensor and amplifier) provides an analog signal of the reactor or plant parameter. The following methods for checking the analog portion of a protective channel during reactor operation are provided:

1) Varying the monitored parameter

2) Introducing and varying a substitute transmitter signal

3) Cross checking between identical channels or between channels which bear a known relationship to each other and which have readouts available.

The design provides for administrative control for the purpose of manually bypassing channels for test and calibration purposes.

The design provides for administrative control of access to all trip settings, module calibration adjustments, test points, and signal injection points.

e) Information Readout and Indication of Bypass - The protective system provides the operator with complete information pertinent to system status and plant safety.

Indication is provided on the reactor and turbine-generator board if some part of the system has been administratively bypassed or taken out of service.

Trips are indicated and identified down to the channel level.

f) Vital Protective Functions and Functional Requirements - The RPS monitors all parameters related to safe operation of the reactor. The system is designed to trip the reactor so as to protect the core against fuel rod cladding damage causes by departure from DNB, and to protect the RCS against damage caused by overpressure. The ESF Instrumentation System monitors parameters to detect failure of the RCS, and initiates containment isolation and ESF operation.

g) Completion of Protective Action - Where operating requirements necessitate automatic or manual bypass of a protective function, the design is such that the bypass is removed automatically whenever permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protective function are part of the protective system and are designed in accordance with the criteria of this section.

   The protective systems are so designed that, once initiated, a protective action goes to completion. Return to normal operation requires administrative action by the operator.

h) Multiple Trip Settings - For monitoring nuclear flux, multiple trip settings are used. When it is necessary to change to a more restrictive trip setting to provide adequate protection for a particular mode of operation or set of operating conditions, the design provides positive means of assuring that the more restrictive trip setting is used. The devices used to prevent improper use of less restrictive trip settings are considered a part of the protective system and are designed in accordance with the other provisions of these criteria.

i) Interlocks and Administrative Procedures - Interlocks and administrative procedures required to limit the consequences of fault conditions other than those specified as limits for the protective function comply with the protective system criteria.

j) Protective Actions - The RPS automatically trips the reactor to protect the reactor core when the following conditions exist:

1) The reactor power, as measured by neutron flux, reaches a preset limit

2) The temperature rise across the core as determined from loop ΔT reaches a limit; both from a fixed ΔT setpoint (function of T_{avg} and neutron flux distribution) or a variable ΔT setpoint (function of T_{avg}, pressurizer pressure and neutron flux distribution).

3) The pressurizer pressure reaches a minimum limit

4) Loss of reactor coolant flow as sensed by low flow, loss of pump power or pump breakers opening

The RPS automatically trips the reactor to protect the RCS when the pressurizer pressure reaches a maximum limit.

Interlocking functions of the RPS prevent control rod withdrawal when a specified parameter reaches a value less than the value at which reactor trip is initiated.

For anticipated abnormal conditions, protective systems in conjunction with inherent plant characteristics and ESF are designed to assure that limits for energy release to the containment and for radiation exposure are not exceeded.

k) Indication - All transmitted signals (flow, pressure, temperature, etc.) which can lead to a reactor trip are either indicated or recorded for every channel.

All nuclear flux power range currents (top detector, bottom detector, and algebraic difference and sum of bottom and top detector currents) are indicated and/or recorded.

l) Alarms - Alarms are also used to alert the operator of deviation from normal operating conditions so that he may take corrective action to avoid a reactor trip. Further, actuation of any rod stop or trip of any reactor trip channel will actuate an alarm.

m) Operating Environment - The protective channels are designed to perform their function when subjected to the most adverse environmental conditions and to prevent loss of function resulting from the most adverse environmental conditions anticipated during their lifetime.

7.2.1.3 Instrumentation Cable Separation

The RPS is divided into four channels with each channel run in individual cable tray systems throughout the plant. Cables from different channels are never routed through the same penetration. These penetrations are separated by a minimum center to center distance of three feet. The majority of RPS logic is a two out of three scheme. At least one channel of each three channel logic scheme is routed in channel 1. Additional separation is provided by placing one complete channel (channel 1) consisting of penetration B-9 and C-9 on one side of a concrete wall separating the electrical penetrations into two groups.

The NIS is divided into a four channel system with each channel run in individual cable tray systems throughout the plant. Cables from different channels are never routed through the same penetration. These penetrations are separated by a minimum center to center distance of six feet. Additional physical separation is provided by placing one complete channel consisting of one penetration (A-4) on one side of a concrete wall separating the electrical penetrations into two groups.

The relays and associated circuitry for the Reactor Trip System are located in the lower relay room in the southwest corner of the Reactor Auxiliary Building. The initiating systems are divided in four channels physically arranged so that each channel is at the extremity of two rows of process racks. The two rows have a horizontal separation of three feet. Four redundant wireways, consisting of steel conduit and solid metal trays with a horizontal separation of 18 in. carry the input signals from the sensing devices of the process racks. Four channel separations are also maintained for the outputs from the process racks to the reactor protection and ESF relay racks. These relay racks are also arranged in two parallel rows, Train A and B, with a horizontal separation of three feet. The output from Train A relays and Train B relays are run in separate wireways with a horizontal separation of 18 in. In instances where physical conditions prohibit horizontal separation, horizontal fire barriers are provided. Fire barriers are also provided where wireways penetrate a wall. The inputs to the process racks and the outputs from the relay racks are run in separate wireways.

A rigid quality control procedure is followed in the field to ensure that redundant cables are run in the proper channels.

This combination of horizontal separation and a rigid quality control program ensures the independency of redundant channels so that a fire in one channel or train will not propagate to other wireways and thereby disable the complete system.

7.2.1.4 Final System Drawings

Figures 7.2.1-13 through 7.2.1-16 show block diagrams of individual trip channels.
Figure 7.2.1-12 shows abbreviations used for the drawings.

Figures 7.2.1-17 through 7.2.1-35 are logic diagrams of the protection systems.

TABLE 7.2.1-1

LIST OF REACTOR TRIPS & CAUSES OF ACTUATION OF: ENGINEERED SAFETY FEATURES, CONTAINMENT AND STEAM LINE ISOLATION & AUXILIARY FEEDWATER

REACTOR TRIP	COINCIDENCE CIRCUITRY AND INTERLOCKS	COMMENTS
1. Manual	1/2, no interlocks	High and low
settings; 2. High power range nuclear flux low	2/4, no interlocksmanual block and	automatic reset of setting by P-10, Table 7.2.1-2
3. Overtemperature ΔT	2/3, no interlocks	
4. Overpower ΔT	2/3, no interlocks	
5. Low pressurizer pressure (fixed set point)	2/3, blocked by P-7*	
6. High pressurizer pressure (fixed set point)	2/3, no interlocks	
7. High pressurizer water level	2/3, blocked by P-7	
8a. Low reactor coolant flow of	2/3, per loop blocked by P-7, and P-8	Low flow and loss power
8b. Monitored electrical supply to reactor coolant pumps	2/3, blocked by P-7, and P-8	

*Permissive circuit (P-7) listed in Table 7.2.1-2.

TABLE 7.2.1-1 (Cont'd)

REACTOR TRIP	COINCIDENCE CIRCUITRY AND INTERLOCKS	COMMENTS
9. Safety injection signal (actuation)	2/3 low pressurizer pressure, 2/3 high containment pressure; or 2/3 high differential pressure between any steam line header and steam line; or manual 1/2 or 2/3 high steam flow in coincidence with 2/3 low T_{avg} or 2/3 low steam line pressure	
10. Turbine-generator trip (low auto stop oil pressure signal)	2/3, blocked P-8	
11. Low-low steam generator water level	2/3, per loop	
12. High intermediate range nuclear flux	1/2, manual block permitted by P-10	Manual block and automatic reset
13. High source range nuclear flux	1/2, manual block permitted by P-6, blocked by P-10	Manual block and automatic reset

TABLE 7.2.1-2

PERMISSIVE CIRCUITS

NUMBER	FUNCTION	REQUIRED INPUT
1	Prevent rod withdrawal on overpower	1/4 high neutron flux (power range) or 1/2 high neutron flux (intermediate range) or 2/3 over-temperature ΔT or 2/3 overpower ΔT
2	Auto-rod withdrawal stop at low powers	Low Mwe (15% power) load signal (turbine pressure)
3	Auto-rod withdrawal stop on rod drop	1/4 rapid decrease of neutron flux (power range) or 1/1 rod bottom indication
4*		
5	Steam dump interlocks	Rapid decrease of Mwe load signal (turbine pressure)
6	Manual block of source range trip	1/2 high intermediate range flux allows manual block, 2/2 low intermediate range defeats block
7	Permissive power (block various trips). Required only at power	3/4 low-low neutron flux (power range) and 2/2 low Mwe load signal (turbine pressure)
8	Block single primary loop loss of flow trip and turbine trip	3/4 low neutron flux (power range)
9*		
10	Manual block of low power range trip (power range) intermediate range trip	2/4 high neutron flux allows manual block, 3/4 low neutron flux (power range) defeats manual block

*Not applicable to this plant.

TABLE 7.2.1-3

ROD STOPS

ROD DROP	ACTUATION SIGNAL	ROD MOTION TO BE BLOCKED
1. Rod Drop	1/4 rapid power range neutron flux decrease or any rod bottom signal	Automatic Withdrawal
2. Nuclear Overpower	1/4 high power range neutron flux or 1/2 high intermediate range neutron flux	Automatic and Manual Withdrawal
3. High ΔT	2/3 overpower ΔT or 2/3 over-temperature ΔT	Automatic and Manual Withdrawal
Actuation of High ΔT initiates a turbine load reduction		
4. Low Power	Low Mwe load signal (below 15%) for low turbine impulse pressure	Automatic Withdrawal

TABLE 7.2.1-4

SOURCE RANGE

SIGNAL AND SOURCE	DESTINATION AND/OR FUNCTION
1. Isolation Amplifier	
a. 0-10 V DC	Auxiliary Channel (SUR)
b. 0-5 V DC	Computer
c. 0-5 V DC	Spare
d. 0-1 ma DC	Remote Meter (cps)
e. 0-37.5 mv DC	Remote Recorder
2. Bistable Amplifiers	
a. 115 V AC	Misc. Proc. Relay Rack (Spare)
b. 115 V AC	Misc. Proc. Relay Rack (Hi Flux Level @ Shutdown)
c. 115 V AC	Reac. Prot. Relay Rack (Source Range Reactor Trip)
d. 115 V AC	Misc. Proc. Relay Rack (Annunciate "Source Range Loss of Detector Voltage")
3. Manual Block (115 V AC)	Misc. Proc. Relay Rack (Block Hi Flux Level @ Shutdown)
4. Trip Bypass (115 V AC)	Reac. Prot. Relay Rack (Block of S. R. Reactor Trip)
5. Test-Calibrate (115 V AC)	Misc. Proc. Relay Rack ("NIS Channel Test" - MCB)
6. Discriminator (1-10^6 cps)	Source Range Auxiliary Channel (Visual-Audio)

TABLE 7.2.1-5

INTERMEDIATE RANGE

SIGNAL AND SOURCE	DESTINATION AND/OR FUNCTION
1. Isolation Amplifier	
a. 0-10 V DC	Auxiliary Channel (S.U.R.)
b. 0-1 ma DC	Remote Meter (Ampere)
c. 0-50 mv DC	Remote Recorder
d. 0-5 V DC	Spare
e. 0-5 V DC	Computer
2. Bistable Amplifiers	
a. 115 V AC	Relay Rack (Spare)
b. 115 V AC	Reac. Prot. Relay Rack (Intermediate Range Permissive P-6)
c. 115 V AC	Misc. Proc. Relay Rack (Intermediate Range Rod-Stop)
d. 115 V AC	Reac. Prot. Relay Rack (Intermediate Range Reactor Trip)
e. 115 V AC	Misc. Proc. Relay Rack (Annunciate "I.R. Loss of Detector Voltage")
f. 115 V AC	Misc. Proc. Relay Rack (Annunciate "N-35 (N-36) Loss of Comp Voltage")
3. Trip Bypass (115 V AC)	Reac. Prot. Relay Rack (Block of Rod-Stop and Reactor Trip)
4. Test-Calibrate (115 V AC)	Misc. Proc. Relay Rack ("NIS Channel Test" - MCB)

TABLE 7.2.1-6
POWER RANGE

SIGNAL AND SOURCE	DESTINATION AND/OR FUNCTION
1. Isolation Amplifier (Ion Chamber A)	
a. 0-10 V DC	Upper Section Flux Deviation Circuitry
b. 0-5 V DC	Computer
c. 0-1 ma DC	Remote Meter (Delta Flux)
d. 0-5 V DC	Spare
e. 0-50 mv DC	Spare
2. Isolation Amplifier (Ion Chamber A)	
a. 0-10 V DC	ΔT Overpower-Overtemperature Compensation
3. Isolation Amplifier (Ion Chamber B)	
a. 0-10 V DC	Lower Section Flux Deviation Circuitry
b. 0-5 V DC	Computer
c. 0-1 ma DC	Remote Meter (Delta Flux)
d. 0-5 V DC	Spare
e. 0-50 mv DC	Spare
4. Isolation Amplifier (Ion Chamber B)	
a. 0-10 V DC	ΔT Overpower-Overtemperature Compensation
5. Isolation Amplifier (Average Power)	
a. 0-10 V DC	Spare
b. 0-5 V DC	Computer

TABLE 7.2.1-6 (Cont'd)

SIGNAL AND SOURCE	DESTINATION AND/OR FUNCTION
c. 0-1 ma DC	Remote Meter (Percent FP)
d. 0-50 mv DC	Remote Recorder
e. 0-5 V DC	Spare
6. Isolation Amplifier (Average Power)	
a. 0-10 V DC	Spare
b. 0-5 V DC	Spare
c. 0-1 ma DC	Spare
d. 0-50 mv DC	Spare
e. 0-5 V DC	Spare
7. Isolation Amplifier (Average Power)	
a. 0-10 V DC	Power Range Deviation Comparator
b. 0-5 V DC	Spare
c. 0-1 ma DC	Spare
d. 0-50 mv DC	Overpower Recorder
e. 0-5 V DC	Spare
8. Bistable Amplifiers	
a. 115 V AC	Reac. Prot. Relay Rack (Dropped Rod-Rod Stop)
b. 115 V AC	Misc. Proc. Relay Rack (Overpower Rod Stop)
c. 115 V AC	Reac. Prot. Relay Rack (Permissive P-8)
d. 115 V AC	Reac. Prot. Relay Rack (Permissive P-10)

TABLE 7.2.1-6 (Cont'd)

SIGNAL AND SOURCE	DESTINATION AND/OR FUNCTION
e. 115 V AC	Reac. Prot. Relay Rack (Spare Permissive)
f. 115 V AC	Reac. Prot. Relay Rack (Low Range Reactor Trip)
g. 115 V AC	Reac. Prot. Relay Rack (High Range Reactor Trip)
h. 115 V AC	Misc. Proc. Relay Rack (Annunciate "Power Range Loss of Detector Voltage")
9. Test-Calibrate (115 V AC)	Misc. Proc. Relay Rack (NIS Channel Test-MCB)
10. Rod Drop Bypass (115 V AC)	Reac. Prot. Relay Rack (Block of Rod-Drop Circuit)

7.2.2 ANALYSIS

7.2.2.1 General Design Criteria and IEEE 279

Information on how the design basis requirements of IEEE-279 are met is presented above. The applicable General Design Criteria are discussed in Section 3.1. Additional analysis are presented below.

7.2.2.2 Control and Protection Interaction

7.2.2.2.1 Nuclear Power

Four power-range nuclear flux channels are provided for overpower protection. If any channel fails in such a way as to produce a low output, that channel is incapable of proper overpower protection. In principle, the same failure may cause rod withdrawal and, hence, overpower; however, all automatic rod withdrawal signals have been defeated in the Rod Control System. Two-out-of-four overpower trip logic will ensure an overpower trip if needed even with an independent failure in another channel.

In addition, slow changes or drifts are compensated by the temperature control signals. Also, a rapid decrease of any nuclear flux signal will annunciate on the RTGB. Finally, an overpower signal from any nuclear channel will block automatic rod withdrawal; however, all automatic rod withdrawal signals have been defeated in the Rod Control System. The setpoint for this rod stop is below the reactor trip setpoint.

7.2.2.2.2 Coolant Temperature

The three T_{avg} channels (one per loop) are used in the overtemperature and overpower protection system logic. A reactor trip signal is generated if two out of the three signals exceed the calculated ΔT setpoint where overtemperature and overpower setpoint equations are given in Section 7.2.1.1.2.

The input signals to the Reactor Control System are obtained from electronically isolated protection T_{avg} and ΔT signals (one per loop). A Median Signal Selector (MSS) is implemented in the Reactor Control System, one for T_{avg} and one for ΔT. The MSS receives three channels as input and selects the median signal for input to the appropriate control systems. Any single failure (high or low) in a calculated temperature will not result in adverse control system behavior since the failed high or low temperature signal will be rejected by the MSS.

Hence, the implementation of a MSS in the Reactor Coolant System in conjunction with the two out of three protection logic satisfies the requirements of IEEE 279-1971, Section 4.7, "Control and Protection System Interaction."

The response time allocated for measuring RCS hot and cold leg temperature using thermowell mounted fast response RTDs is four seconds. This response time does not include the process electronics.

In addition, automatic rod withdrawal blocks will occur if any two of four nuclear channels indicates an overpower condition or if any two of three temperature channels indicates an overtemperature condition. Two-out-of-three trip logic is used to ensure that an overtemperature trip will occur if needed even with an independent failure in another channel. Finally, as shown in Chapter 15.0, the combination of trips on nuclear overpower, high pressurizer water level, and high pressurizer pressure also serve to limit an excursion for any rate of reactivity insertion.

7.2.2.2.3 Pressurizer Pressure

Three pressure channels are used for high and low pressure protection and as part of overpower-overtemperature protection. Two pressure channels are used for pressure control. These are discussed below:

1) Pressure Control: Spray, power-operated relief valves, and heaters, are controlled by isolated output signals from the pressure control channels.

2) Low Pressure - A spurious high pressure signal from one control channel can cause low pressure by spurious actuation of spray and/or a relief valve. Additional redundancy is provided in the protection system to ensure underpressure protection, i.e., two-out-of-three low pressure reactor trip logic and two-out-of-three logic for safety injection.

3) High Pressure - The pressurizer heaters are incapable of overpressurizing the reactor coolant system. Maximum steam generation rate with heaters is about 11,000 lb/hr, compared with a total capacity of 879,990 lb/hr for the three safety valves and a total capacity of 420,000 lb/hr for the two power-operated relief valves. Therefore, overpressure protection is not required for a pressure control failure. Two-out-of-three high pressure trip logic is therefore used.

   In addition, either of the two relief valves can easily maintain pressure below the high pressure trip point. The two relief valves are controlled by independent pressure control channels, one of which is independent of the pressure channel used for heater control. Finally, the rate of pressure rise achievable with heaters is slow, and ample time and pressure alarms are available for operator action.

7.2.2.2.4 Pressurizer Level

Three pressurizer level channels are used for reactor trip. Isolated output signals from these channels are used for volume control, increasing or decreasing water level. A level control failure could fill or empty the pressurizer at a slow rate (on the order of half an hour or more).

A reactor trip on pressurizer high level is provided to prevent rapid thermal expansions of reactor coolant fluid from filling the pressurizer: the rapid change from high rates of steam relief to water relief can be damaging to the safety valves and the relief piping and pressurizer relief tank. However, a level control failure cannot actuate the safety valves because the high pressure reactor trip is set below the safety valve set pressure. With the slow rate of charging available, overshoot in pressure before the trip is effective is much less than the difference between reactor trip and safety value set pressures. Therefore, a control failure does not require protection system action.

In addition, ample time and alarms are available for operator action.

7.2.2.2.5 Steam generator water level

Before describing control and protection interaction for these channels, it is beneficial to review the protection system basis for this instrumentation. (See Figure 7.2.1-16.)

The basic function of the reactor protection circuits associated with low steam generator water level is to preserve the steam generator heat sink for removal of long-term residual heat. Should a complete loss of feedwater occur with no protective action, the steam generators would boil dry and cause an overtemperature-overpressure excursion in the reactor coolant. Reactor trips on temperature, pressure, and pressurizer water level will trip the plant before there is any damage to the core or reactor coolant system. However, residual heat after trip would cause thermal expansion and discharge of the reactor coolant to containment through the pressurizer relief valves. Redundant emergency feedwater pumps are provided to prevent this. Reactor trips act before the steam generators are dry to reduce the required capacity and starting time requirements of these pumps and to minimize the thermal transient on the reactor coolant system and steam generators. Independent trip circuits are provided for each steam generator for the following reasons:

1. Should severe mechanical damage occur to the feedwater line to one steam generator, it is difficult to ensure the functional integrity of level and flow instrumentation for that unit. For instance, a major pipe break between the feedwater flow element and the steam generator would cause high flow through the flow element. The rapid depressurization of the steam generator would drastically affect the relation between downcomer water level and steam generator water inventory.

2. It is desirable to minimize the thermal transient on a steam generator for credible loss of feedwater accidents.

It should be noted that controller malfunctions caused by a protection system failure affect only one steam generator. Also, they do not impair the capability of the main feedwater system under either manual control or automatic control. Hence, these failures are far from being the worst cases with respect to decay heat removal with the steam generators.

a. Feedwater Flow - A spurious high signal from the feedwater flow channel being used for control would cause a reduction in feedwater flow. A reactor trip on low-low water level will ensure a reactor trip if needed.

   In addition, the three-element feedwater controller incorporates reset on level, such that with expected controller settings a rapid increase in the flow signal would cause only a 12 in. decrease in level before the controller re-opened the feedwater valve. A slow increase in the feedwater signal would have no effect at all.

b. Steam Flow - A spurious low steam flow signal would have the same effect as a high feedwater signal, discussed above.

c. Steam Generator Level – The steam generator water level transmitters for each channel are supplied, simultaneously, to both the Reactor Protection System (RPS) and as sensors inputs to the feedwater control system Median Signal Selector (MSS). The MSS selects the median level sensor input and supplies it to the three-element feedwater controller as one of the control elements.

   Should one of the steam generator water level transmitters have a spurious high or low signal, the feedwater control system would not be affected since the MSS signal selected would be a valid control signal and not the spurious high or low signal. This spurious action would have no impact on the steam generator level control, would not create a need for protection, and reactor trip on two-out-of-three low-level is acceptable.

   A slow drift in the level signal may not actuate a low feedwater signal. Since the level decrease is slow, the operator has time to respond to low level alarms. Since only one steam generator is affected, automatic protection is not mandatory and reactor trip on two-out-of-three low-level is acceptable.

7.2.2.2.6 Steam line pressure

Three pressure channels per steam line are used for steam break protection (two-out-of-three low pressure signals for any steam line actuates safety injection). An additional channel is used to control the power-operated relief valve on that steam line. These valves are typically rated at 10 percent of the safety valve capacity. A spurious high pressure signal from the channel used for control will open the relief valve and cause low pressure. This is a slow rate of steam release, classified as a credible steam (line) break in Chapter 15.0. In that the consequences of a more severe steam line break are acceptable, analysis for this event is not necessary. Therefore, control failure does not create a need for the protection, and two-out-of-three logic is acceptable.

7.2.2.3 <u>Nuclear Instrumentation</u>

During plant shutdown and operation, three discrete independent levels of nuclear protection are provided from the three ranges of out-of-core nuclear instrumentation. The basic protection philosophy is that the level protection is present in all three ranges to provide a reliable, rapid and restrictive protection system which is not dependent upon operation of higher range instrumentation.

Reliability is obtained by providing redundant channels which are physically and electrically separated. Fast trip response is an inherent advantage of using level trip protection in lieu of startup rate protection (with a long time constant) during plant startup. More restrictive operation is an inherent feature since an increase in plant power cannot be performed until satisfactory operation is obtained from higher range instrumentation which permits administrative bypass of the lower range instrumentation. On decreasing power level, protection is automatically made more restrictive. Startup accidents while in the source range are rapidly terminated without significant increases in nuclear flux and with essentially no power generation or reactor coolant temperature increase.

The indications and administrative actions required by this protection system are readily available to the operator and should result in a safe, uncomplicated increase of power.

7.2.2.3.1 Reactor trip protection

During reactor startup, the operator will be made aware of satisfactory operation of one or more intermediate range channels by annunciation of the P6 Permissive Bistable status light(s) at the control board. The source and intermediate range flux level information is also readily available on recorders and indicators at the control console. At this time, if both intermediate range channels are functioning properly, the operator would depress the two manual block switches associated with the source range logic circuitry, thus causing cutoff of source range detector voltages and blocking the trip logic outputs. The manual block should not be initiated, however, until at least one decade of satisfactory intermediate range operation is obtained. If one intermediate range channel is not functioning, normal power increase could be performed if desired. The permissive P6 annunciation is continuously displayed by the control board status lights.

Continuation of the startup procedure in the intermediate range would result in a normal power increase, and the receipt of a permissive signal from the power range channels when two-of-four channels exceed 10 percent of full power. The operator would be alerted to this condition by a control board permissive status light. Indicators (one per channel) and recorders also indicate plant status in terms of percent full power. If the operator does not block the intermediate range trip and continues the power increase, a rod stop will automatically occur from either of the intermediate range channels. The operator should then depress the momentary "Manual Block" pushbuttons associated with the intermediate range rod stop and reactor trip logic. This would transfer protection to the low-range trips for the four power range channels. The permissive P10 status light would be continuously displayed as was P6. The low-range manual block switches (two) must be depressed to initiate blocking prior to continuation of the power increase. The permissive functions associated with administrative trip blocking and automatic reactivation are provided with the same separation and redundancy as the trip functions.

When decreasing power operation to lower levels, more restrictive trip protection is automatically afforded when three-of-four power range channels are below P10 permissive and when two-of-two intermediate ranges are below the permissive P6.

7.2.2.3.2 Rod-Drop Protection

An additional protection function provided by the power range instrumentation is backup to the rod-drop protection of the rod bottom bistables on the Rod Position System. The nuclear instrumentation rod-drop protection is provided by comparison of the average nuclear power signal with the same signal which is conditioned by an adjustable lag network. This method provides a response to dynamic signal changes associated with a dropped rod condition, but does not respond to the slower signal changes associated with normal plant operation. Rod-stop actuation from at least one of the four power range channels will occur for any dropped rod condition.

Each rod-drop sensing circuit has associated with it a bistable amplifier driving two relays in separate logic relay racks. The logic relay matrices are connected in a one-of-four, "OR", configuration to block rod withdrawal and initiate a load cutback.

7.2.2.3.3 Control and Alarm Functions

Various control and alarm functions are obtained from the three ranges of out-of-core nuclear instrumentation during shutdown, startup and power operation. These functions are used to alert the operator of conditions which require administrative action and alert personnel of unsafe reactor conditions. They also provide signals to the rod control system for automatic blocking of rod withdrawal during plant operation to avoid unnecessary reactor trips.

a) Source Range - No control functions are obtained from the source range channels. Alarm functions are provided, however, to alert the operator of any inadvertent changes in shutdown reactivity. Visual annunciation of this condition is at the control board, with audible annunciation performed in the containment and Control Room. This alarm can either be blocked prior to startup or can serve as the startup alarm in conjunction with administrative procedures.

b) Intermediate Range - Both alarm and control functions are supplied by the intermediate range channels. Blocking of rod withdrawal is initiated by either intermediate range on high flux level. This condition is alarmed at the control board to alert the operator that rod-stop has been initiated. In addition, the intermediate ranges provide a status light indication when either channel exceeds the P6 permissive level. This alerts the operator to the fact that he must take administrative action to manually block the source range trips to prevent an inadvertent trip during normal power increase.

c) Power Range - The power ranges provide alarm and control functions similar to those in the intermediate ranges. An overpower rod-stop function from any of the four power range channels inhibits rod withdrawal and is alarmed at the control board. The power ranges also provide a status light indication when two-of-four channels exceed permissive P10 level. As in the case of P6 in the intermediate range, this alerts the operating personnel that administrative action (namely, blocking of intermediate and low range trips) is required before any further power increase may take place.

The power ranges also have provisions for two additional permissive functions. When P8 and P9 are used, the power ranges through two-of-four matrices provide P8 and contribute to the overall logic for permissive P9. A permissive status light is provided for P8, "Nuclear Power Below P8." The extinguishing of the P8 permissive status light alerts the operator that the flow trips and "pump breaker open" trips and turbine trips are now active. These trips are blocked while the status light is alarmed. Additional functions are provided in the power range of operation. A dropped control rod will be sensed by one or more of the power range channels, and this condition will initiate an RTGB alarm.

Another function is a power range channel deviation alarm. This alarm is furnished by the comparator channel through a comparison of the average power level signals being supplied by the power ranges. Actuation of this alarm alerts the operator to a power unbalance between the channels so that corrective action can be taken. Finally, two signals are supplied by three power range channels (N41, N42, and N43) to the reactor control and protection system; one signal from each ion chamber isolation amplifier.

7.2.2.3.4 Loss of Power

The nuclear instrumentation draws its primary power from the vital instrument buses whose reliability is discussed in Section 8. Redundant NIS channels are powered from separate buses. Loss of a single vital instrument bus would result in the initiation of all reactor trips associated with the channels deriving power from that source. During power operation, the loss of a single bus would not result in a reactor trip since the power range reactor trip function operates from a two-of-four logic. If the bus failure occurred during source or intermediate range operation (one-of-two logic), a reactor trip condition would result.

7.2.2.3.5 Safety Factors

The relation of the power range channels to the Reactor Protective System has been described. To maintain the desired accuracy in trip action, the total error from drift in the power range channels will be held to ±1.0 percent at full power. Routine tests and recalibration will ensure that this degree of deviation is not exceeded. Bistable trip set points of the power range channels will also be held to an accuracy of ±1.0 percent of full power.

7.2.2.4 Full Length Rod Drive Power Supply

The full length control rod drive power supply concept using a single scram bus system has been successfully employed on all Westinghouse plants. Potential fault conditions with a single scram bus system are discussed in this section. The unique characteristics of the latch type mechanisms with its relatively large power requirements make this system with the redundant series trip breakers particularly desirable.

7.2.2.4.1 AC Power Connections

The three-phase four-wire supply voltage required to energize the RCCA power cabinets is 260 V line to line, 58.3 Hz, 438 kVa capacity, zig-zag-connected. It is unlikely that any power supply, and in particular one as unusual as this four-wire power source, could be accidently connected in phase in the required configuration. Also it should be noted that this requires multiple connections, not single connections. The closest outside sources available in the plants are 480 V auxiliary power sources and 208 V lighting sources.

Connections of either a 480 or 208 V, 60 Hz source to the single AC bus supplying the rod control system cause currents to flow between the sources due to an out-of-phase condition. These currents flow until the generator accelerates to a speed synchronous with the 60 Hz outside source, a time sufficient to trip the generator breakers. The out-of-phase currents for an unlimited capacity outside source, an outside source with a capacity equivalent to the normal generator kVa, and for either one or two motor generator (MG) sets in service, are tabulated below:

Out of Phase Currents (Amperes)

		One MG Set in Service	Two MG Sets in Service
480V	Unlimited Capacity	25,000	50,000
	Unlimited Capacity	12,000	25,000
208V	Unlimited Capacity	16,000	32,000
	438 kVa Capacity	8,000	16,000

All of the foregoing currents are sufficiently high to trip out the generator breakers on either overcurrent or reverse current. This trip-out is detectable by annunciation in the Control Room. If the outside power source trips, the connection is of no concern.

Each solid state power cabinet is tied to the main AC bus through three fused disconnect switches; one for the stationary gripper coil circuits, one for the movable gripper coil circuits, and one for the lift coil circuits. Reference voltages to operate the control circuits for all three coil circuits must be in phase with the supply to all coil circuits for proper operation of the system. If the outside power source were brought into an individual cabinet, nine normal source connections would have to be disconnected and the outside source would have to be tied in phase to the proper nine points plus one neutral point to allow movement of the rods. This is not considered credible.

Connection of a single phase AC source (i.e. one line to neutral) is also considered improbable. This would again require a high capacity source which would have to be connected in-phase with the nonsynchronous MG set supply. Again, more than one connection is needed to achieve this condition. Each power cabinet contains three alarm circuits (stationary, movable, and lift) that would annunciate the condition to the operator. In addition, calculations show that a single phase source of 280 V, 260 V, or 480 V will not supply enough current to hold the rods. Therefore, a jumper across two trip circuit breaker contacts in series which results in a single phase remaining closed would not provide sufficient current to hold up the rods.

The normal source generators are connected in a zig-zag winding configuration to eliminate the effects of direct current saturation of the machines resulting from the direct currents that flow in the half wave bridge rectifier circuits. If this connection were not used, the generator core would saturate, and loss of generating action would occur. This condition would also occur in a transformer. An outside source not having the zig-zag configuration would have to have a large capacity (>400 kVa) to avoid the loss of transformer action from saturation.

Most of the components in the equipment are applied with a 100 percent safety factor. Therefore, the possibility exists that the system will operate at 480 V with a source of sufficient capacity. The system will definitely operate at 208 V with a source of sufficient capacity.

The connection of an outside source of AC power to one rod control system would first require a need for this source. No such need exists since two power sources (MG sets) are already provided to supply the system. If the source were connected in spite of the need, extreme measures would have to be taken by the intruder to complete the connection. The outside source would have to be a large capacity (400 kVa) one. The currents that flow would require the routing of large conductors or bus bars, not the usual clip leads. Then, the disassembly of switchgear or enclosed bus duct would be required to expose the single AC bus. Large bolted cable or bus bar terminations would have to be completed. A total of four conductors would have to be connected in phase with a nonsynchronous source. To expect that a connection could be completed with the equipment either energized or de-energized, in view of the obstacles which would prevent such a connection, is incredible. However, even if the connection were completed, the outside source connection would be detectable by the operator through the tripping of the generator breakers.

7.2.2.4.2 DC Power Connections

An external DC source could, if connected <u>inside</u> the power cabinet, hold the rods in position. This would require a minimum supply voltage of 50 V. Since the holding current for each mechanism coil is 4 amperes, the DC current capacity would have to be approximately 180 amperes to hold all rods. Achieving this situation would require several acts -- bringing a power source which is not required for any type of operation in the rod control system, preferentially connecting it into the system at the correct points, and actuating specific holding switches so as to interconnect all rods. Closure of twelve switches in four separate cabinets would be required to hold all rods. One switch could hold as many as four rods.

The application of a DC voltage to an individual rod external to the power cabinet would affect only a single rod -- connection with other rods in the group being prevented by the blocking diodes in the power circuits.

Should an external DC source be connected to the system, the system is provided with features to permit its detection.

Each solid state power cabinet contains circuitry which compares the actual currents in the stationary and movable gripper coils with the reference signals from the step sequencing unit (slave cycler). In taking a single step, the current to the stationary gripper coil will be profiled from the holding value to the maximum, to zero and return to holding level.

Correspondingly, the movable gripper coil must change from zero to maximum and return to zero. The presence of an external DC source on either the stationary or movable coil would prevent the related currents from returning to zero.

This situation would be instantaneously annunciated by way of the comparison circuit. Therefore, any rod motion would actuate an alarm indicating the presence of an external DC source. In addition, an external DC source would prevent rods from stepping. Thus, an external source could be detected by the rod position indication system indicating failure of the rod(s) to move.

Connection of an external DC power source to the output lines of the 70 V DC power supply can be detected by opening the three phase primary input of the supply and checking the output with a built-in voltmeter.

7.2.2.4.3 Evaluation Summary

In view of the preceding discussion, the postulated connection of an external power source (either AC or DC) or occurrence of short circuits that could prevent dropping of the rods is not considered credible. Specifically:

a) The need for an outside power source has been eliminated by incorporating built-in holding sources as part of the rod control system, and by providing two MG sets.

b) The equipment is contained within enclosed steel cabinets, precluding the possibility of an accidental connection of either AC or DC power in the cabinets.

c) AC power distribution is accomplished using steel-enclosed bus duct. The high capacity (400 kVa) AC power source is unique and not readily available. Multiple connections are required.

d) DC power is distributed to the individual mechanisms through insulated cables and enclosed electrical connections, precluding the accidental connection of an outside DC source external to the cabinets. The high capacity DC source required to hold rods is not readily available in the rod control system, would require multiple connections, and would require deliberate positioning of switches within the enclosed cabinets.

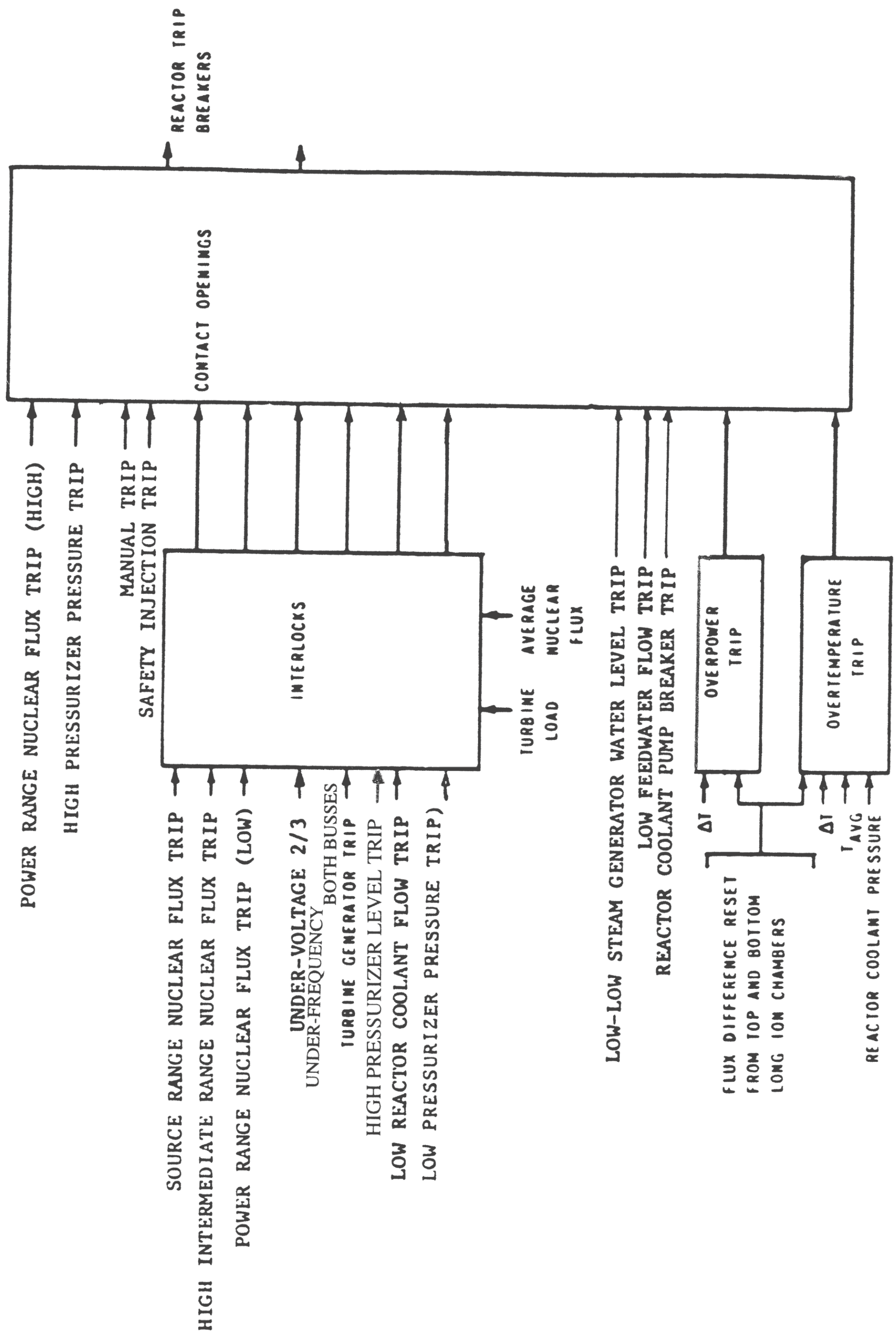
e) Provisions are made in the system to permit detection of an external DC source which could preclude a rod release.

The total capacity of the system including the overload capability of each motor generator set is such that a single set out of service does not cause limitations in rod motion during normal plant operation. In order to minimize reactor trip as a result of a unit malfunction, the power system is normally operated with both units in service.

Flywheels on the motor generator sets and high speed regulators on each unit enable the rods to ride through a complete loss of AC power for one second during electrical transients.

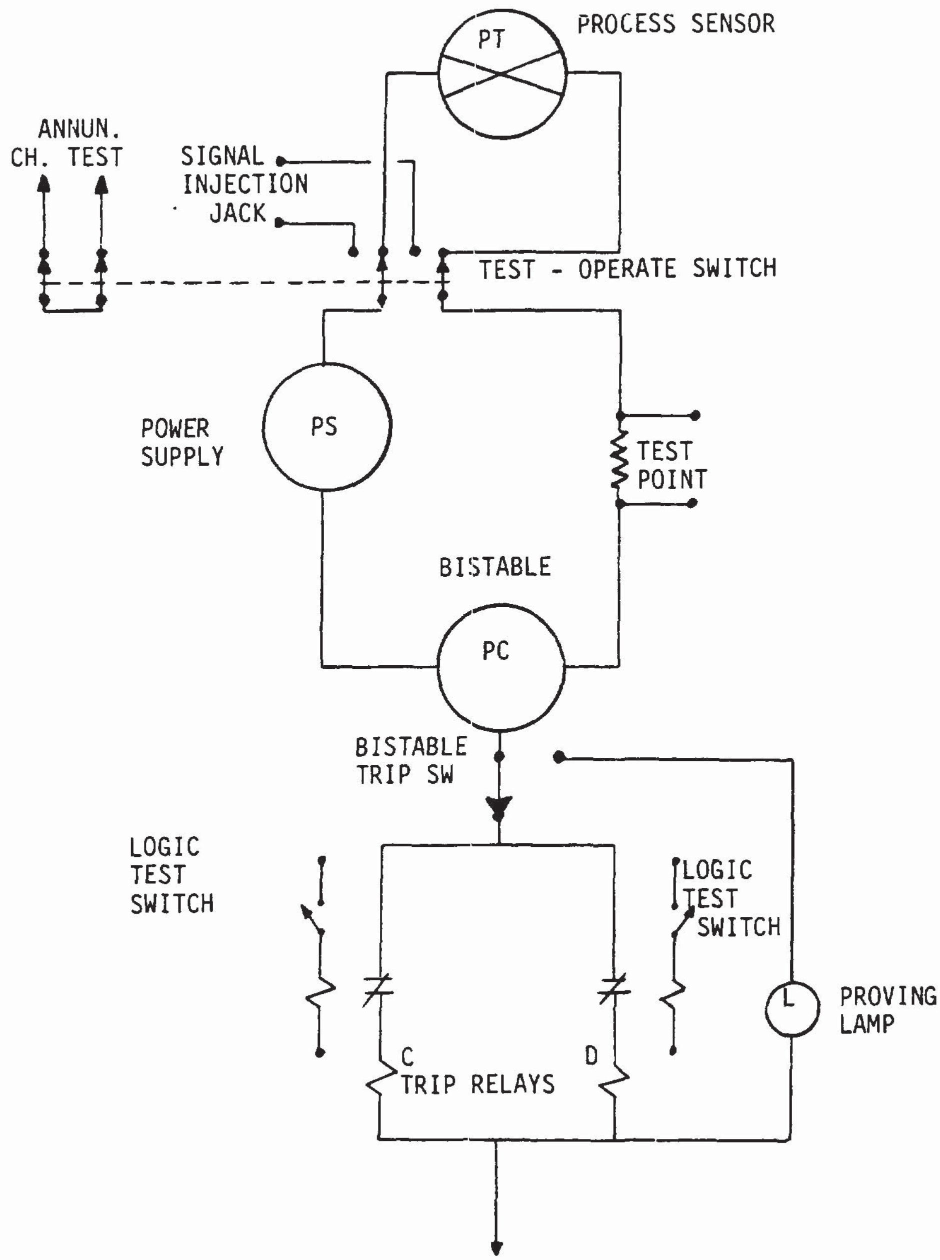
REFERENCES: SECTION 7.2

7.2.1-1 License Amendment No. 13, Change No. 38 to the Technical Specifications, Facility Operating License No. DPR-23, Docket No. 50-261.



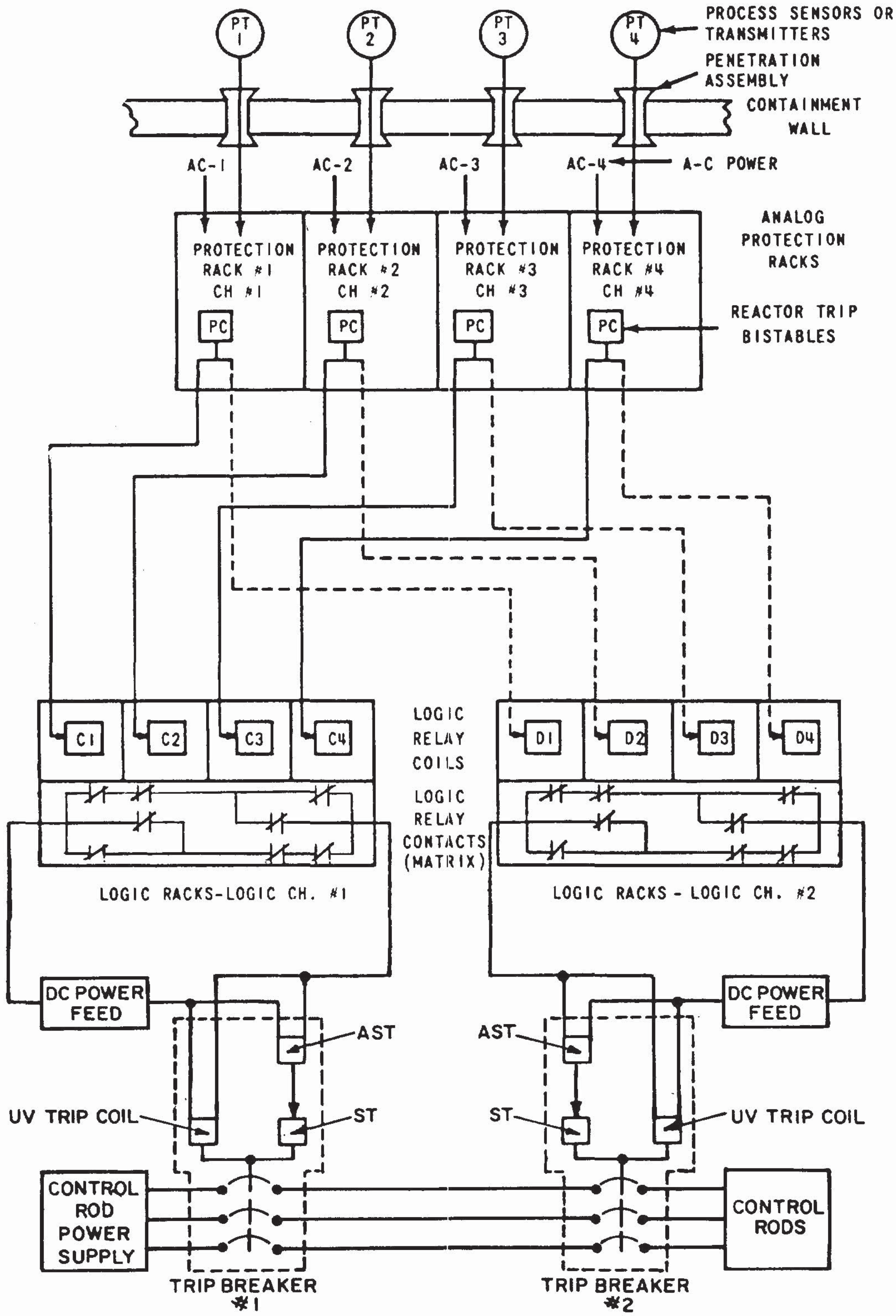
REVISION NO. 25

H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	REACTOR PROTECTION SYSTEMS	FIGURE 7.2.1-1



NOTE: SEE FIGURE 7.2.1-12 FOR DEFINITION OF SYMBOLS

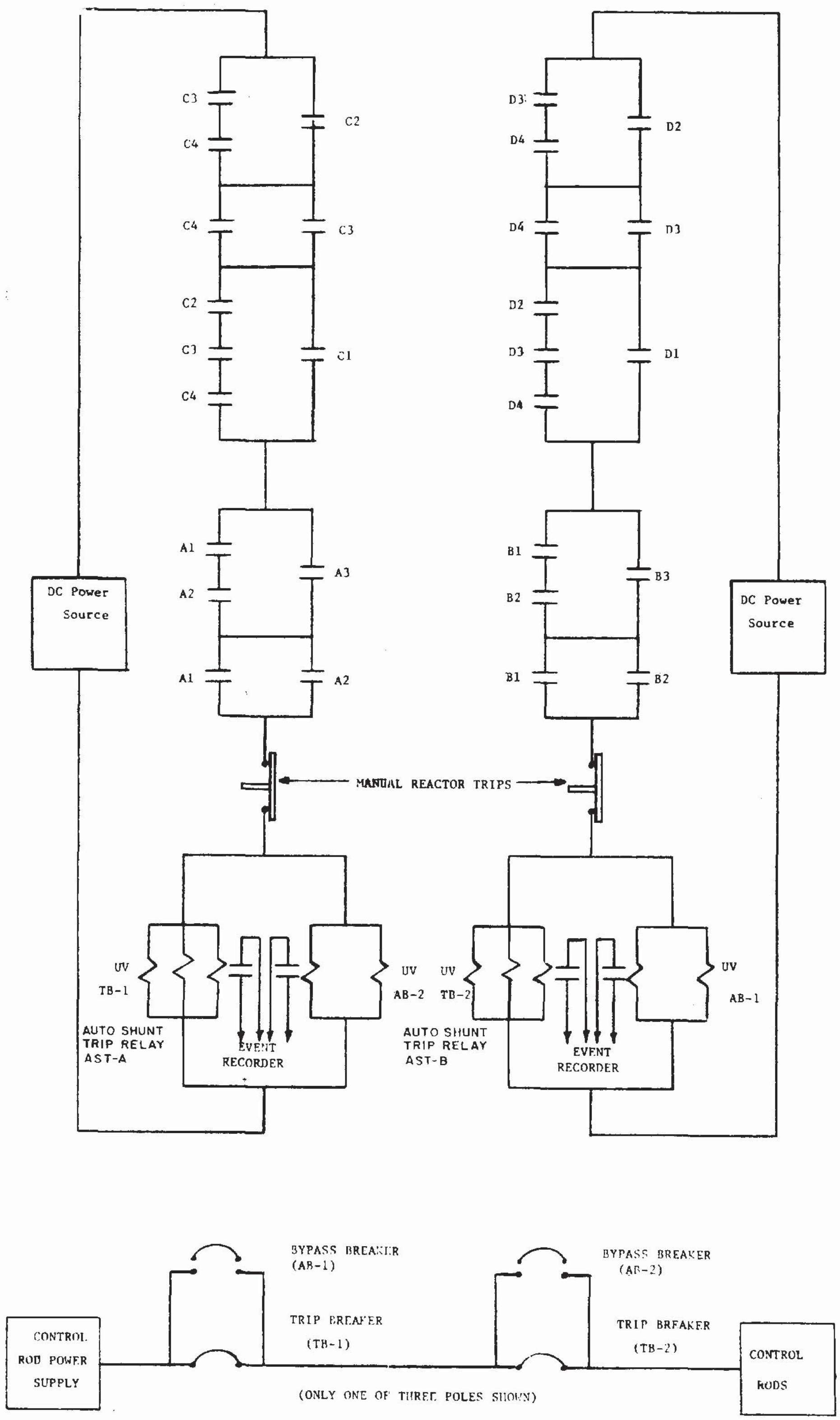
H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	TYPICAL ANALOG CHANNEL TESTING ARRANGEMENT	FIGURE 7.2.1 - 2



NOTE: SEE FIGURE 7.2.1-12 FOR DEFINITION OF SYMBOLS

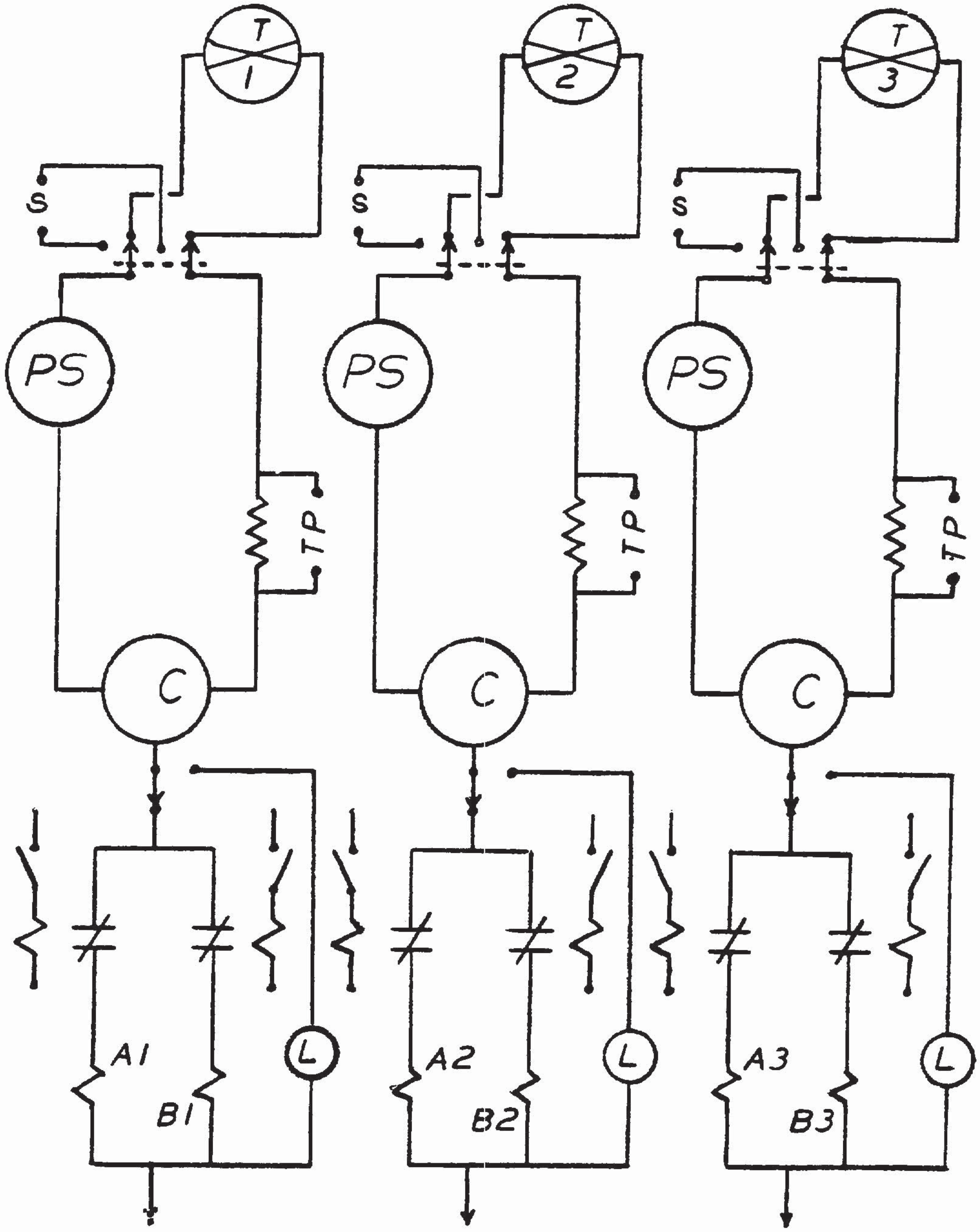
AMENDMENT 3

H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	DESIGN TO ACHIEVE ISOLATION BETWEEN CHANNELS	FIGURE 7.2.1 - 3



AMENDMENT 3

H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	TRIP LOGIC CHANNELS	FIGURE 7.2.1 - 4

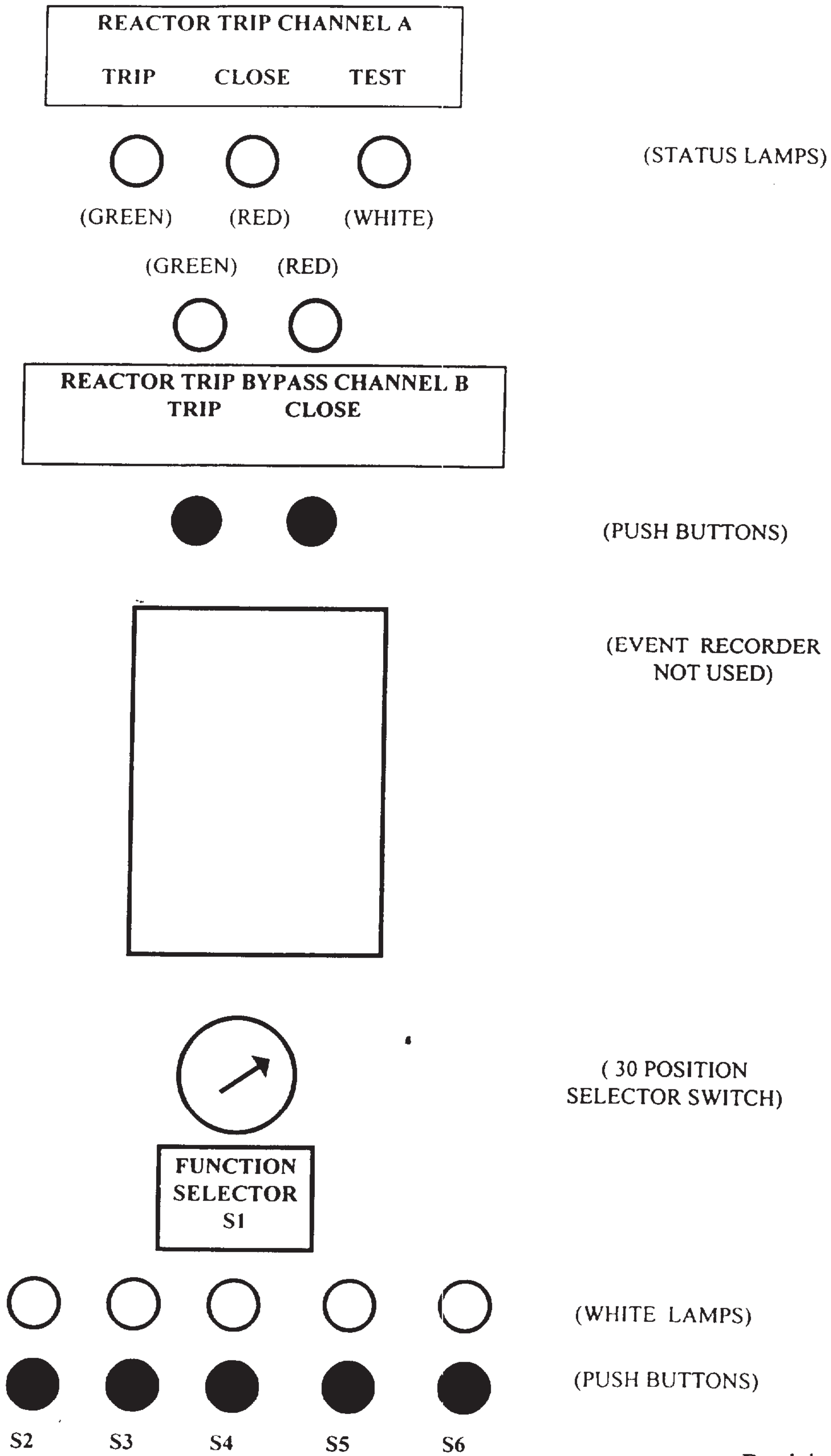


S - SIGNAL INJECTION

TP-TEST POINT

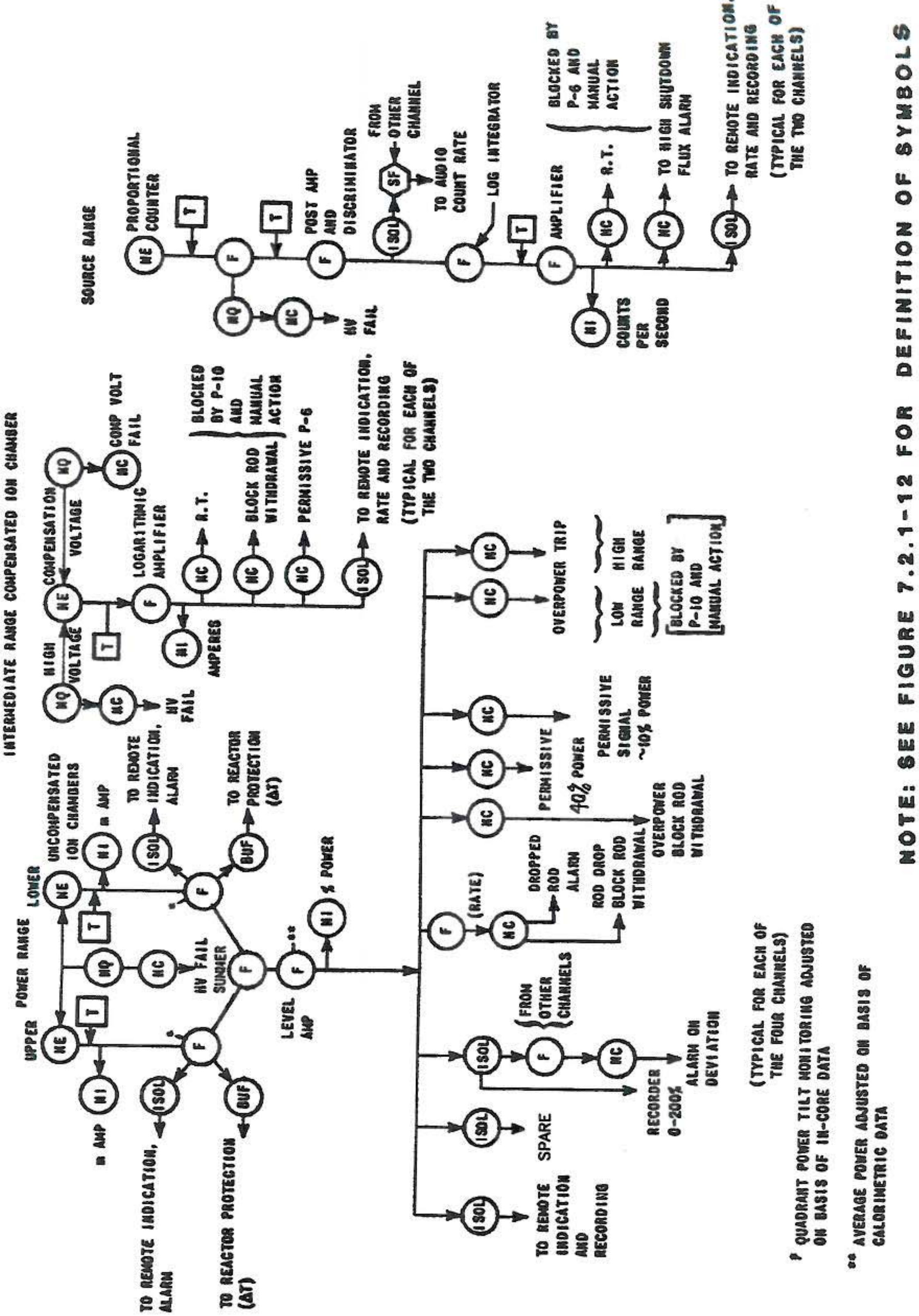
NOTE - REDUNDANT CHANNELS
ARE ISOLATED

H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	ANALOG CHANNELS	FIGURE 7.2.1 - 5



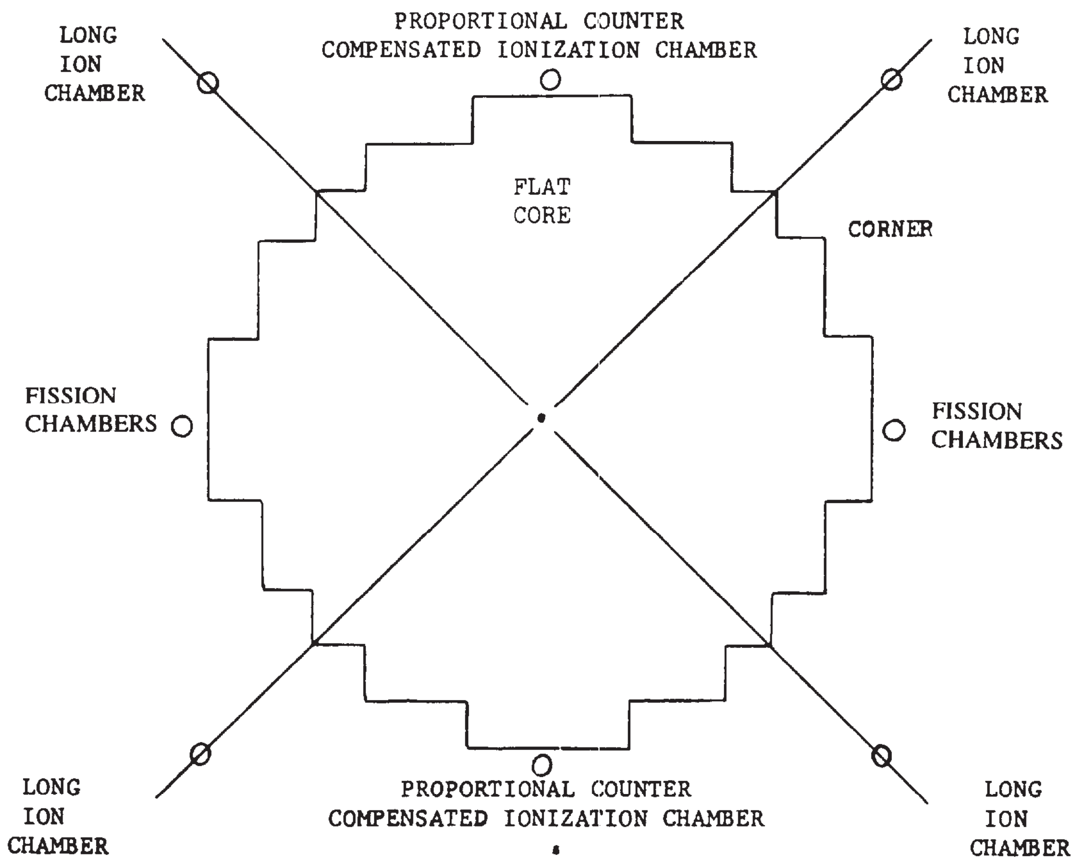
Revision No. 15

H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	LOGIC CHANNEL TEST PANELS	FIGURE 7.2.1 - 6



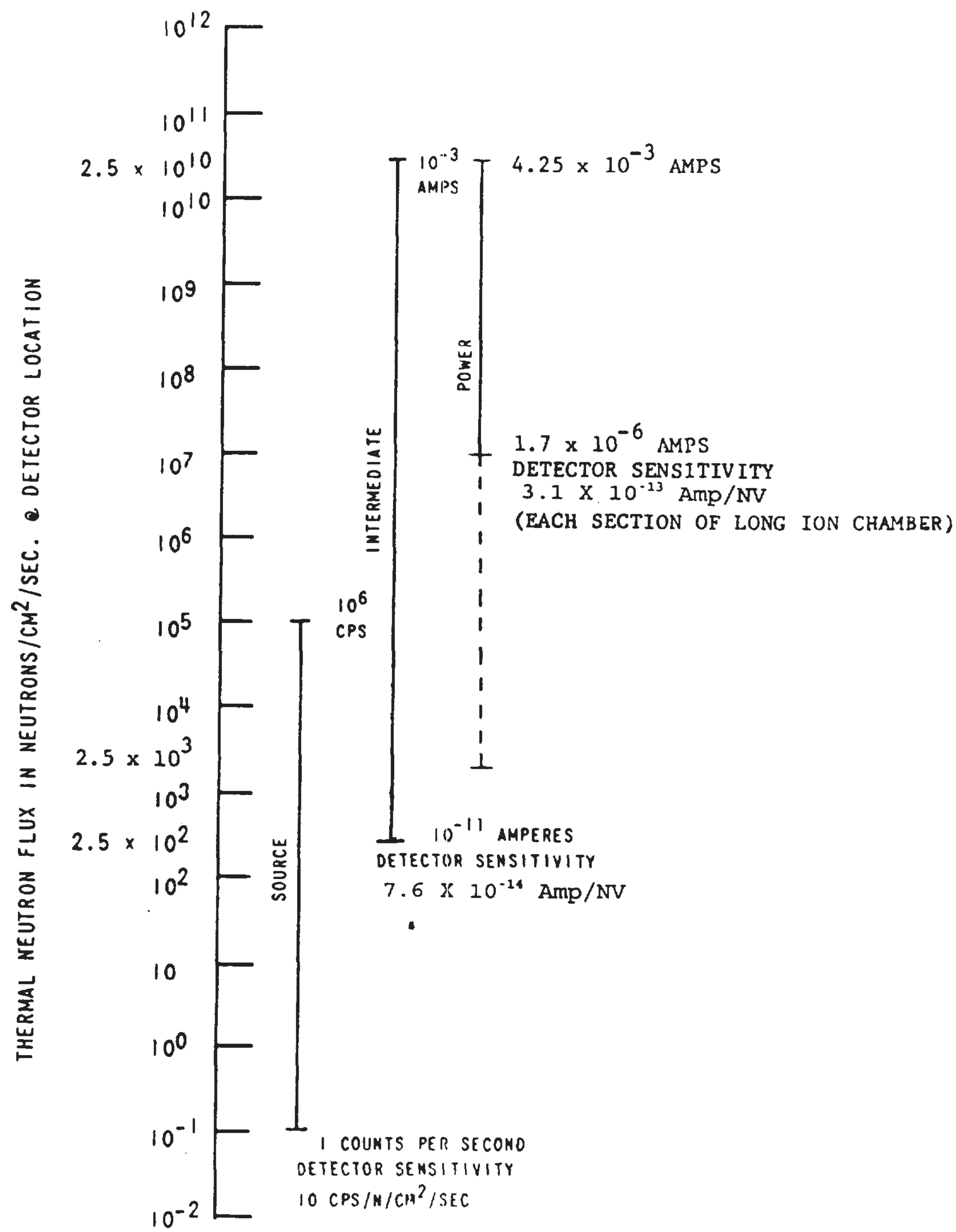
REVISION NO. 22

H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	NUCLEAR INSTRUMENTATION SYSTEM	FIGURE 7.2.1 - 7



Revision No. 15

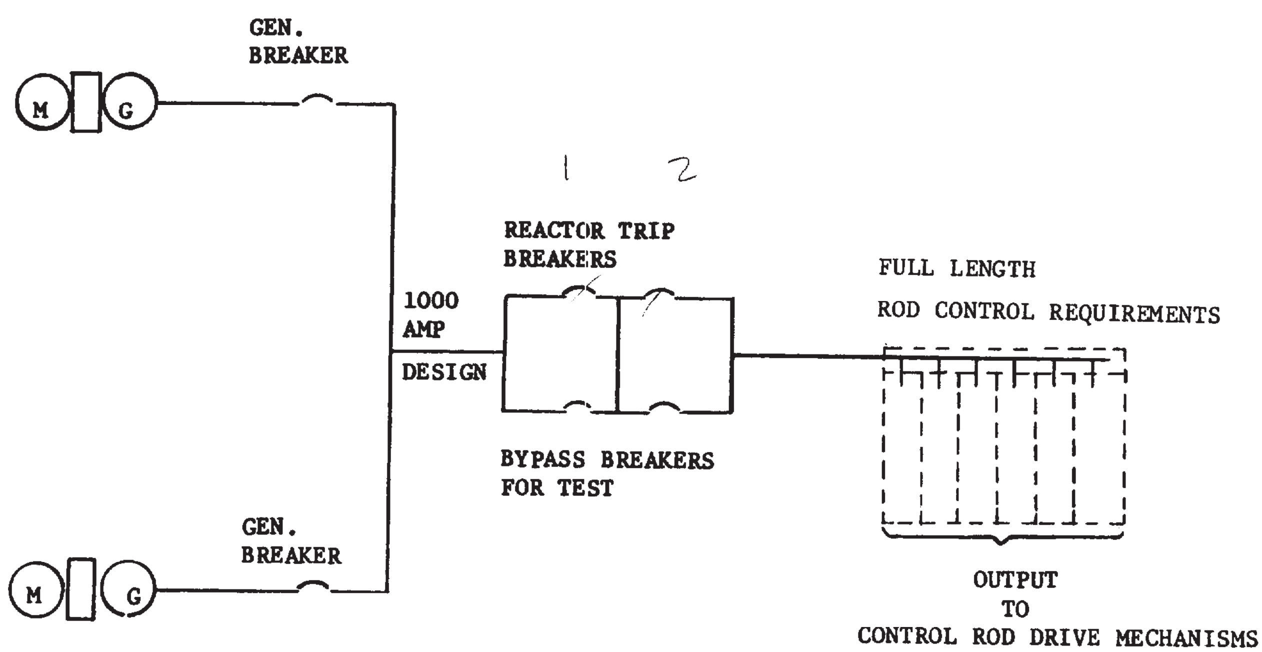
H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	PLAN VIEW INDICATING DETECTOR LOCATION RELATIVE TO CORE	FIGURE 7.2.1 - 8



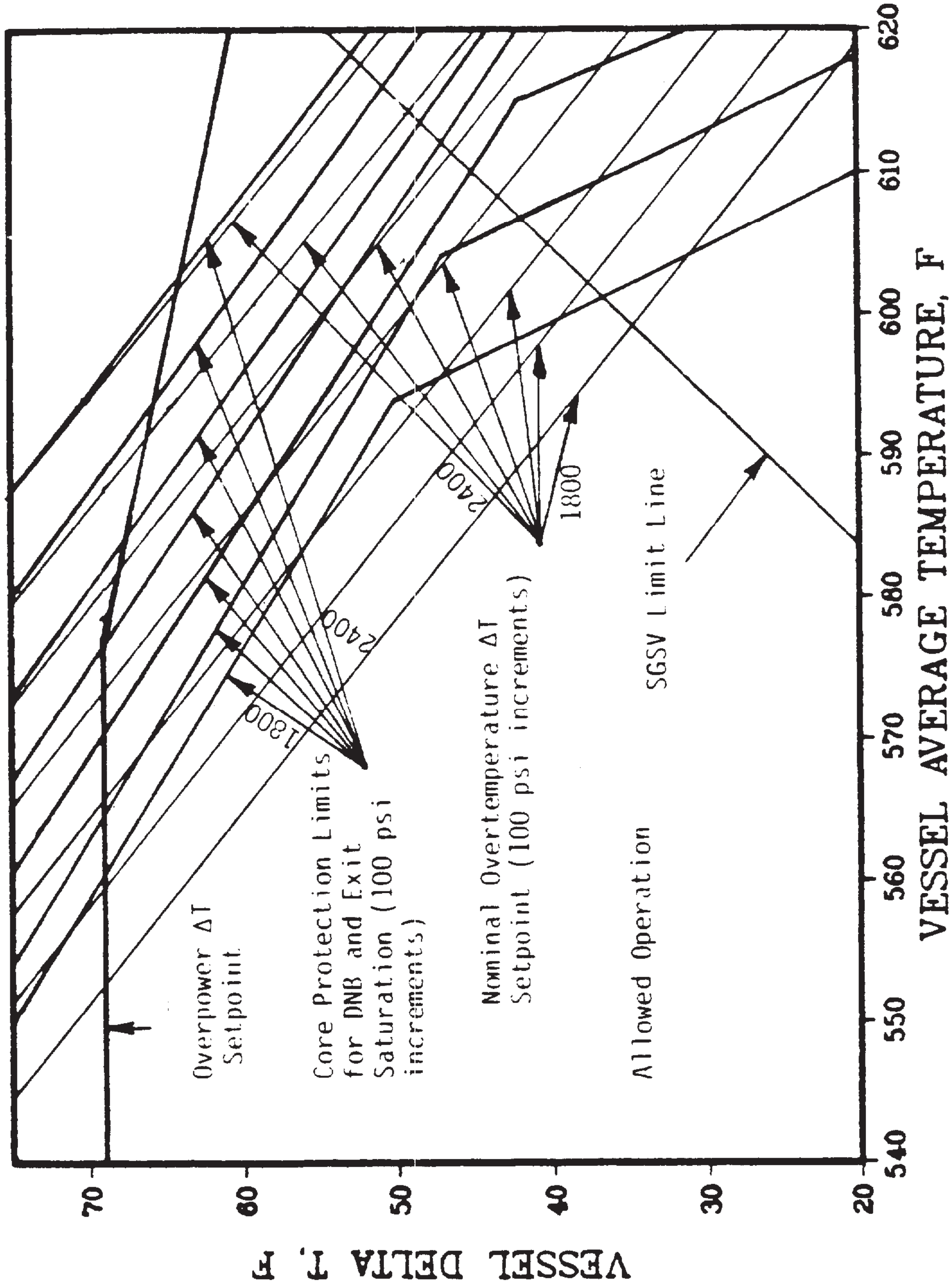
NOTE: This is typical indication of nuclear instrumentation overlap based on theoretical or specified neutron sensitivities. The actual overlap may be different.

Revision No. 15

H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	RANGE OF OPERATION OF NUCLEAR INSTRUMENT CHANNELS	FIGURE 7.2.1 - 9



H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	POWER SUPPLY TO ROD CONTROL EQUIPMENT AND CONTROL DRIVE MECHANISMS	FIGURE 7.2.1 - 10



AMENDMENT 3

H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	ILLUSTRATION OF OVERTEMPERATURE AND OVERPOWER ΔT PROTECTION	FIGURE 7.2.1 - 11

Al — Alarm

Buf — Buffer

d/dt — **derivative**

f — Special Function (such as a pressure compensation unit or lead lag compensation)

FC — Flow Controller (off-on unless output signal is shown)

FI — Flow Indicator

FT — Flow Transmitter

Hi L — **High Level**

Hi LRT — High Level Reactor Trip

Hi L Al — **High Level Alarm**

Hi PRT — High Pressure Reactor Trip

I/I — Isolation Current Repeater

ISOL — Isolation (other than I/I)

LC — Level Controller (off-on unless output signal is shown)

LI — Level Indicator

Lo Lo L — Low Low Level

Lo L — Low Level

Lo LRT — Low Level Reactor Trip

PRT — Low Pressure Reactor Trip

L/L — **Lead/Lag Amplifier**

L_{ref} — Programmed Reference Level

Lo L Al — **Low Level Alarm**

LT — Level Transmitter

MSS — Median Signal Selector

NC — Nuclear Flux Controller

NE — Nuclear Detector

NI — Nuclear Flux Indicator

NM **Function Generator**

NQ — Nuclear Power Supply

PC — Pressure Controller (off-on unless output signal is shown)

PI — Pressure Indicator

P_{ref} — Programmed Reference Pressure

PS — Power Supply

PT — Pressure Transmitter

REF — **Reference signal**

R/I — Resistance to Current Connector

R.T. — **Reactor Trip**

S — Control Channel Transfer Switch (used to maintain auto channel during test of the protection channel)

SF — **Switching Function**

SI — Safety Injection

S-1 — **Control Switch**

T — Built-in Test Point

TC — **Comparator, Temperature**

TE — Temperature Element

TI — **Temperature Indicator**

TJ — Test Signal Insertion Jack

TM — **Signal Isolator, Temperature**

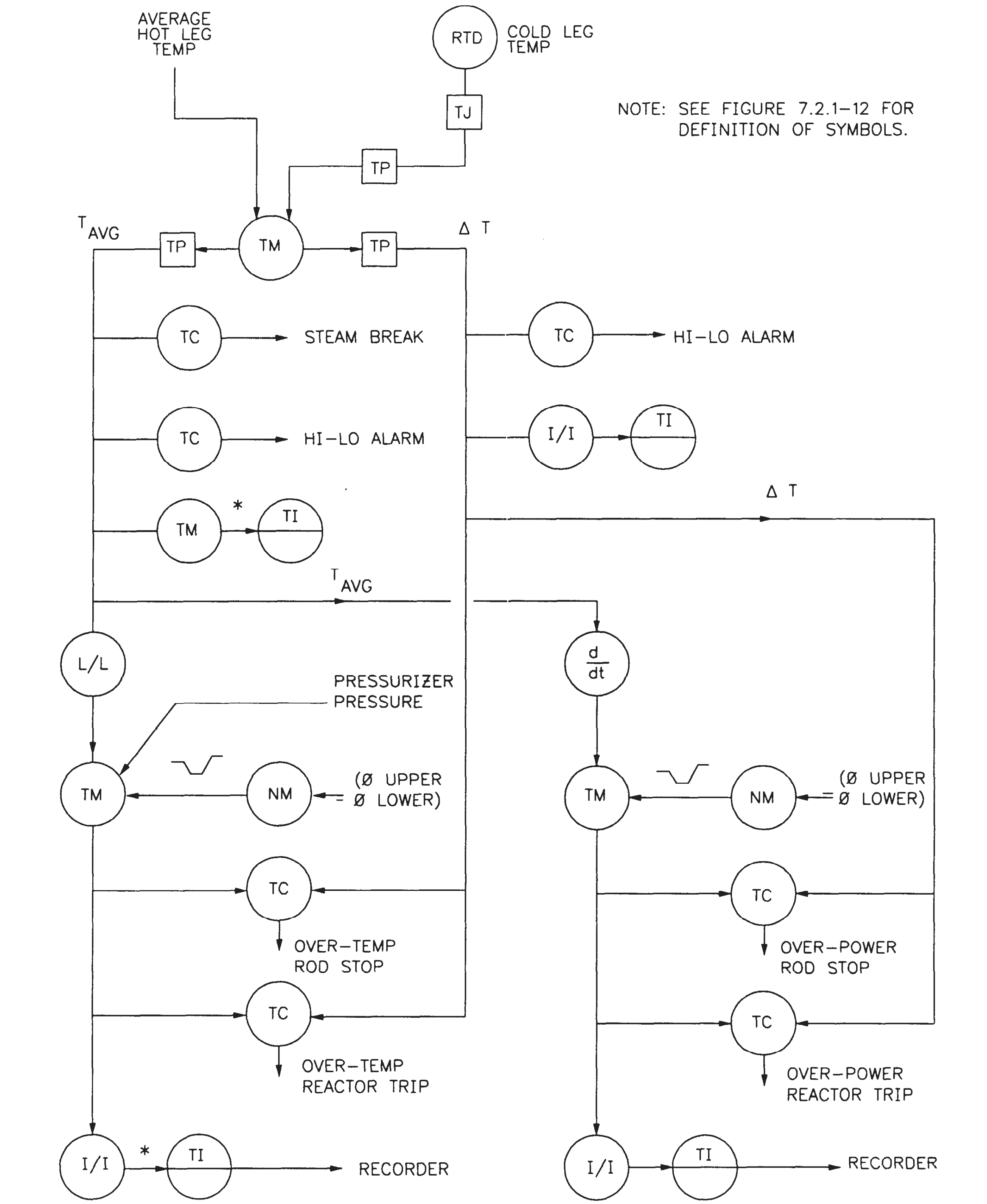
TP — Test Point

ϕU,L — Out of Core Upper or Lower Ion Chamber Flux Signals

H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

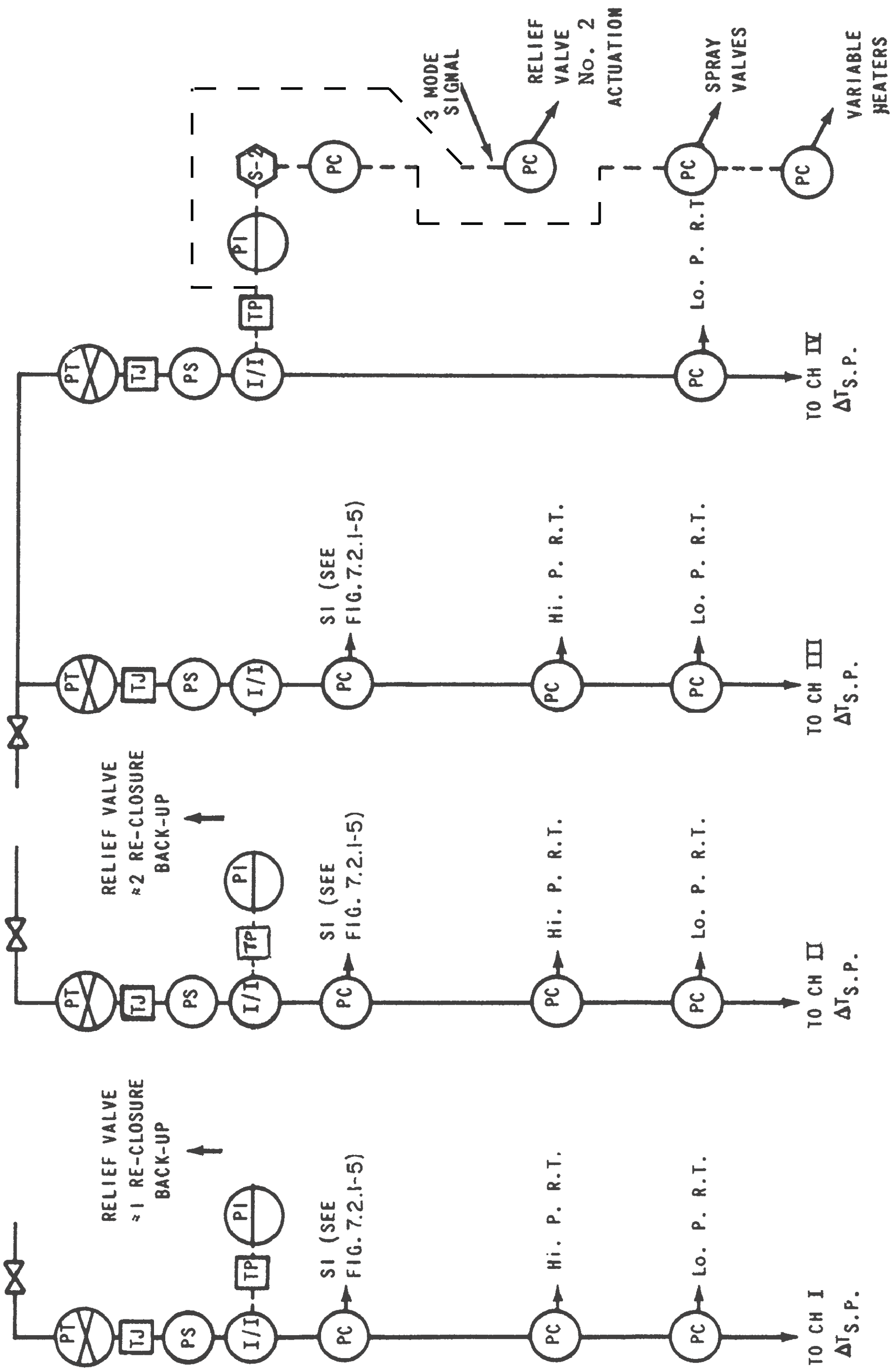
ANALOG SYSTEM SYMBOLS

FIGURE 7.2.1-12 REVISION NO. 24



REVISION NO. 15

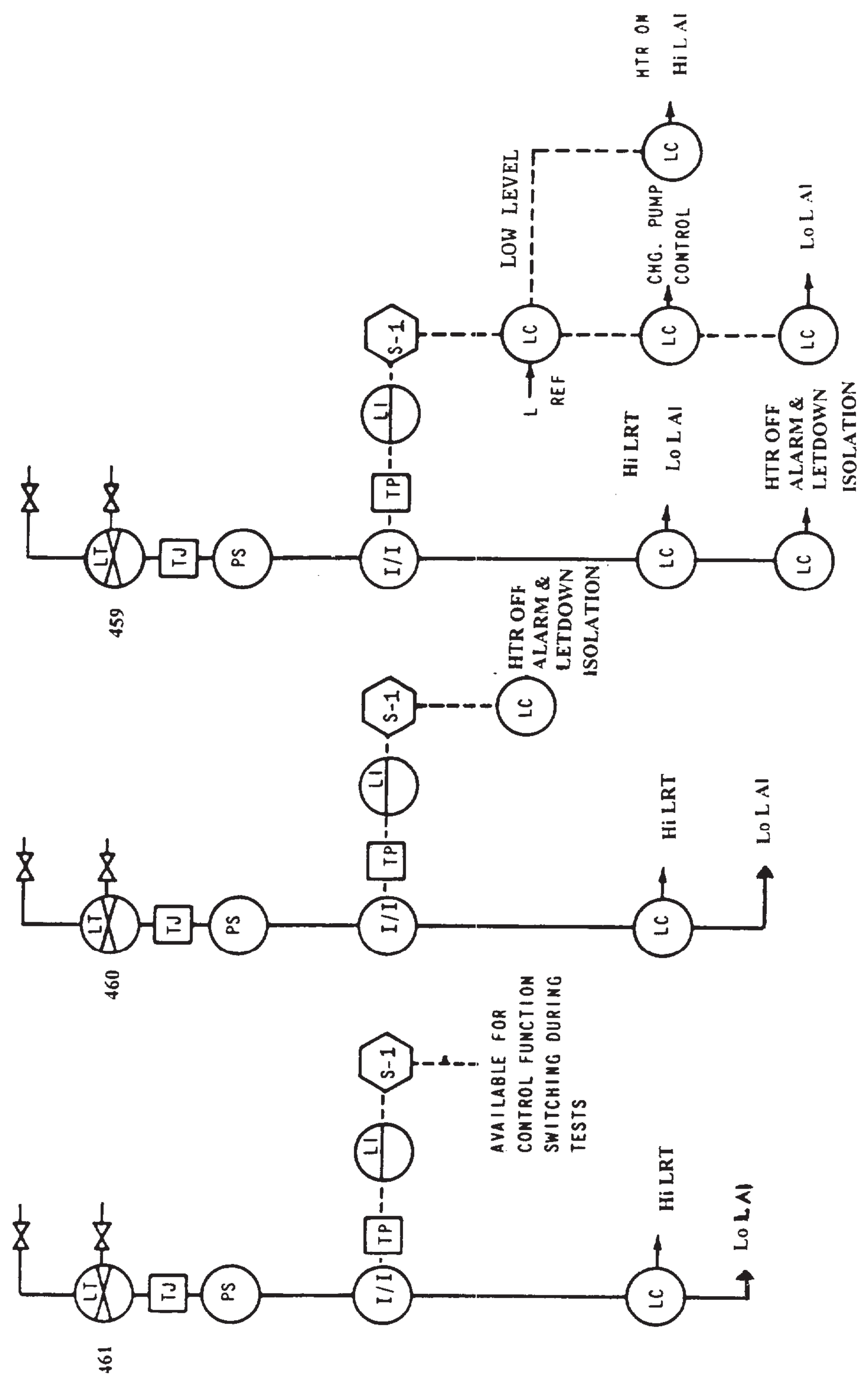
H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	T_{AVG} – ΔT PROTECTION SYSTEM	FIGURE 7.2.1-13



NOTE: SEE FIGURE 7.2.1-12 FOR DEFINITION OF SYMBOLS

REVISION NO. 25

H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	PRESSURIZER PRESSURE CONTROL AND PROTECTION SYSTEM	FIGURE 7.2.1 - 14

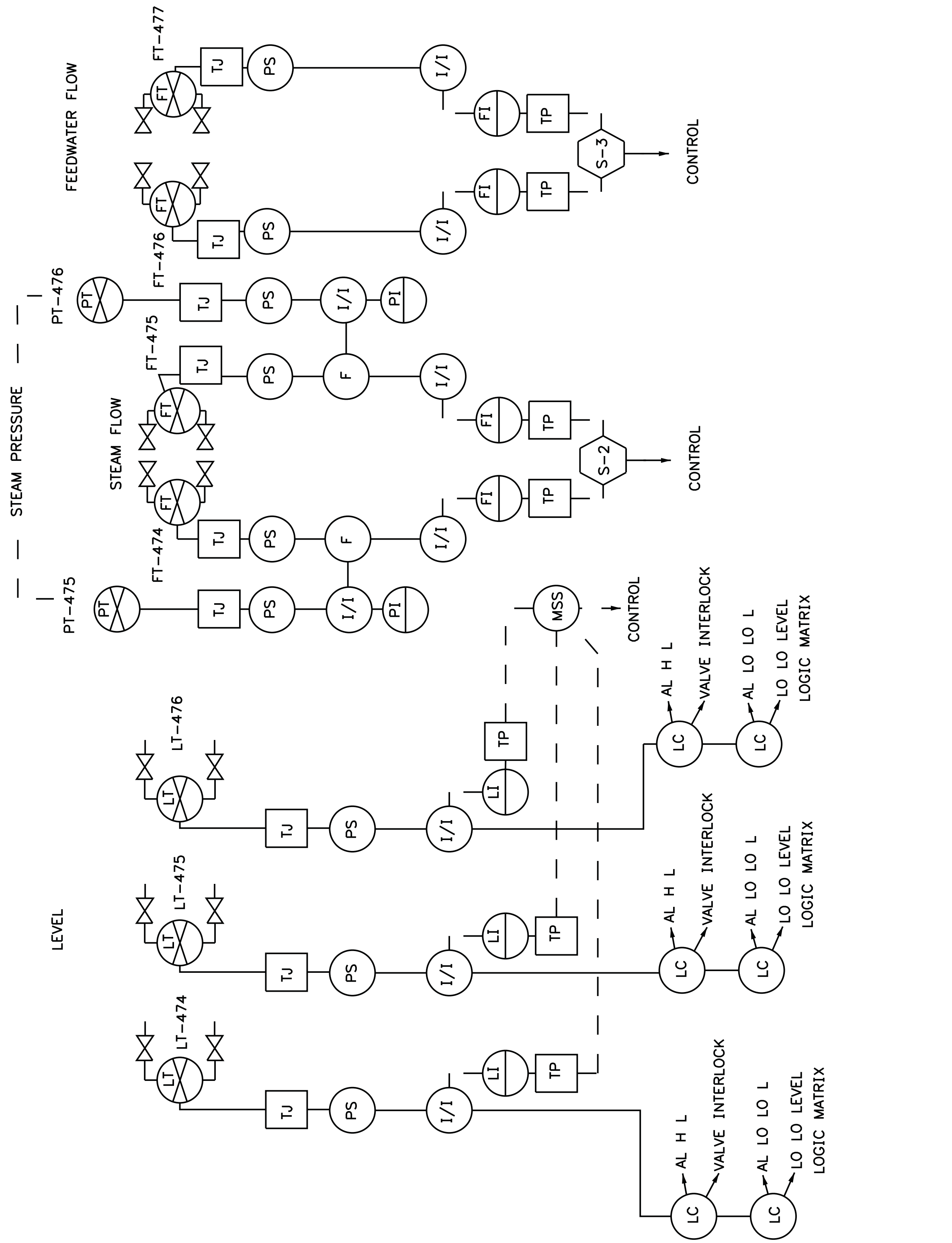


NOTE: SEE FIGURE 7.2.1-12 FOR DEFINITION OF SYMBOLS

FOR MORE INFORMATION REFERENCE STATION DRAWINGS 5379-3501, 5379-3530, & 5379-3482

Revision No. 15

H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	PRESSURIZER LEVEL CONTROL AND PROTECTION SYSTEM	FIGURE 7.2.1 - 15



NOTE: SEE FIGURE 7.2.1-12 FOR DEFINITION OF SYMBOLS.
FOR PLANT SPECIFIC SEE MASTER DRAWING 5379-3533 (5975DØØ).

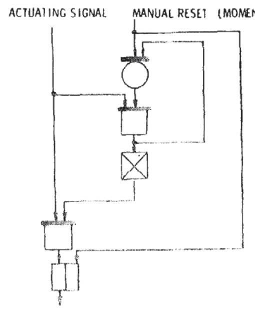
REVISION NO. 25

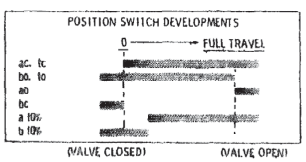
H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	STEAM GENERATOR LEVEL CONTROL AND PROTECTION SYSTEM	FIGURE 7.2.1-16

LOGIC SYMBOLS

(REF NEMA STANDARD ICI - 1959)

SYMBOL	LOGIC FUNCTION	
	AND	A DEVICE WHICH PRODUCES AN OUTPUT ONLY WHEN EVERY INPUT EXISTS
	NOT	A DEVICE WHICH PRODUCES AN OUTPUT ONLY WHEN THE INPUT DOES NOT EXIST
	OR	A DEVICE WHICH PRODUCES AN OUTPUT WHEN ONE INPUT (OR MORE) EXISTS
	OFF RETURN MEMORY	A DEVICE WHICH RETAINS THE CONDITION OF OUTPUT CORRESPONDING TO THE LAST ENERGIZED INPUT, EXCEPT UPON INTERRUPTION OF POWER IT RETURNS TO THE OFF CONDITION.
	RETENTIVE MEMORY	A DEVICE WHICH RETAINS THE CONDITION OF OUTPUT CORRESPONDING TO THE LAST ENERGIZED INPUT (ALSO UPON INTERRUPTION OF POWER)
	ADJUSTABLE TIME DELAY ENERGIZING	A DEVICE WHICH PRODUCES AN OUTPUT FOLLOWING DEFINITE INTENTIONAL TIME DELAY AFTER RECEIVING AN INPUT
	ADJUSTABLE TIME DELAY DE-ENERGIZING	A DEVICE WHICH CONTINUES TO PRODUCE AN OUTPUT FOR A DEFINITE INTENTIONAL PERIOD OF TIME AFTER THE INPUT HAS BEEN REMOVED
2/3	COINCIDENCE (2 OUT OF 3 SHOWN)	A DEVICE WHICH PRODUCES AN OUTPUT WHEN THE PRESCRIBED NUMBER OF INPUTS EXIST (EXAMPLE 2 INPUTS MUST EXIST FOR AN OUTPUT)
M.R. L R	RETENTIVE MEMORY WITH MANUAL RESET	A DEVICE HAVING THE LOGICAL FUNCTION AS INDICATED BY THE DIAGRAM BELOW





DETAIL "A"

ADDITIONAL SYMBOLS

- INSTRUMENT CHANNEL (SEE E-SPEC. G675164 FOR CODE LETTER EXPLANATION)
- INDICATES THAT THE DEVICE OR INSTRUMENT CHANNEL HAS A BISTABLE LOGIC OUTPUT WHEN,
  - ┌ -PARAMETER MEASURED IS GREATER THAN A PRESET VALUE
  - ┘ -PARAMETER MEASURED IS LESS THAN A PRESET VALUE
  - -PARAMETER MEASURED DEVIATES FROM A PRESET VALUE BY MORE THAN A PRESET AMOUNT.
- OR OR SAME AS ABOVE EXCEPT WITH AN AUTOMATICALLY SET VARIABLE VALUE
- ALARM ANNUNCIATOR (ALARMS ON THE SAME SHEET WITH THE SAME SUBSCRIPT SHARE A COMMON ANNUNCIATOR WINDOW)
- REACTOR TRIP "FIRST OUT" ANNUNCIATOR
- TURBINE TRIP "FIRST OUT" ANNUNCIATOR
- DEVICE FUNCTION NUMBER
- 52 / P17 CONTROL CIRCUIT, CHANNEL OR COMPONENT ITEM NUMBER
- LOGIC INFORMATION TRANSMISSION
- ACTION CALLED FOR BY LOGIC INPUT
- COMPONENT CONTROL CIRCUIT
- INDICATES THAT THE INSTRUMENT CHANNEL HAS AN OUTPUT AS FOLLOWS:
  - P - PROPORTIONAL TO THE MAGNITUDE OF THE PARAMETER MEASURED
  - R - PROPORTIONAL TO THE RATE OF CHANGE OF THE PARAMETER MEASURED
- BISTABLE DEVICE OR INDICATE SAME AS EXPLAINED ABOVE
- Ⓣ INDICATOR LAMP
  - T TRIP STATUS LIGHTS
  - P PERMISSIVE STATUS LIGHTS
  - B BYPASS STATUS LIGHTS
- - - - - - ANALOG INFORMATION TRANSMISSION
- ANALOG INPUT / CONTROL LOGIC INPUT / ANALOG GATE / ANALOG OUTPUT — A DEVICE WHICH PERMITS AN ANALOG SIGNAL TO PASS IN AN ISOLATED CIRCUIT IF THE CONTROL LOGIC INPUT EXISTS.
- (Σ) ANALOG SUMMER

NOTES:

1. ALL CIRCUITS ON SHEETS 1 THROUGH 15 ARE REDUNDANT EXCEPT WHERE INDICATED NOT REDUNDANT.
2. PROTECTION CHANNELS II & III ARE CONNECTED TO INVERTER-BUSSES.
3. FOR DUAL BISTABLES (I.E. BISTABLES WITH COMMON INPUT CIRCUITRY BUT WITH 2 SET POINTS, 2 OUTPUTS). THE OUTPUT/SETPOINT NUMBER (AS TAGGED PHYSICALLY ON THE BISTABLE) IS SHOWN CIRCLED BELOW THE BISTABLE SYMBOL.

E.G. TC 459A ① TC 459A ②

DEVICE FUNCTION NUMBERS AND LETTERS

(Ref. : AS A STANDARD 37.2 - 1956 AND NEMA STANDARD S G 5-1959)

1 - MASTER ELEMENT (CONTROL SWITCH)
20 - ELECTRIC OPERATED VALVE
33 - POSITION SWITCH
SUFFIX LETTER:
ac. ao. bc. bo - LIMIT SWITCH
to. tc - TORQUE SWITCH
SEE DETAIL "A" FOR OPERATION
43 - MANUAL SELECTOR SWITCH
52 - AC CIRCUIT BREAKER OR CONTACTOR
SUFFIX LETTER:
a - AUXILIARY CONTACT-OPEN WHEN MAIN CONTACTS ARE OPEN
b - AUXILIARY CONTACT-CLOSED WHEN MAIN CONTACTS ARE OPEN
(C) - REVERSING CONTACTOR OPERATING COIL-ENERGIZE TO CLOSE VALVE
(O) - REVERSING CONTACTOR OPERATING COIL-ENERGIZE TO OPEN VALVE
(CC) - BREAKER CLOSING COIL
(TC) - BREAKER TRIP COIL
(UV) - BREAKER UNDER VOLTAGE TRIP COIL
63 - LIQUID OR GAS PRESSURE, LEVEL OR FLOW RELAY
69 - PERMISSIVE SWITCH
72 - DC CIRCUIT BREAKER OR CONTACTOR
SUFFIX LETTER:
a' - AUXILIARY CONTACT-OPEN WHEN MAIN CONTACTS ARE OPEN
b - AUXILIARY CONTACT-CLOSED WHEN MAIN CONTACTS ARE OPEN
(C) - REVERSING CONTACTOR OPERATING COIL-ENERGIZE TO CLOSE VALVE
(O) - REVERSING CONTACTOR OPERATING COIL-ENERGIZE TO OPEN VALVE
(CC) - BREAKER CLOSING COIL
(TC) - BREAKER TRIP COIL
(UV) - BREAKER UNDER VOLTAGE TRIP COIL
86 - LOCK-OUT RELAY
SUFFIX LETTER:
P - PRIMARY
BU - BACK-UP

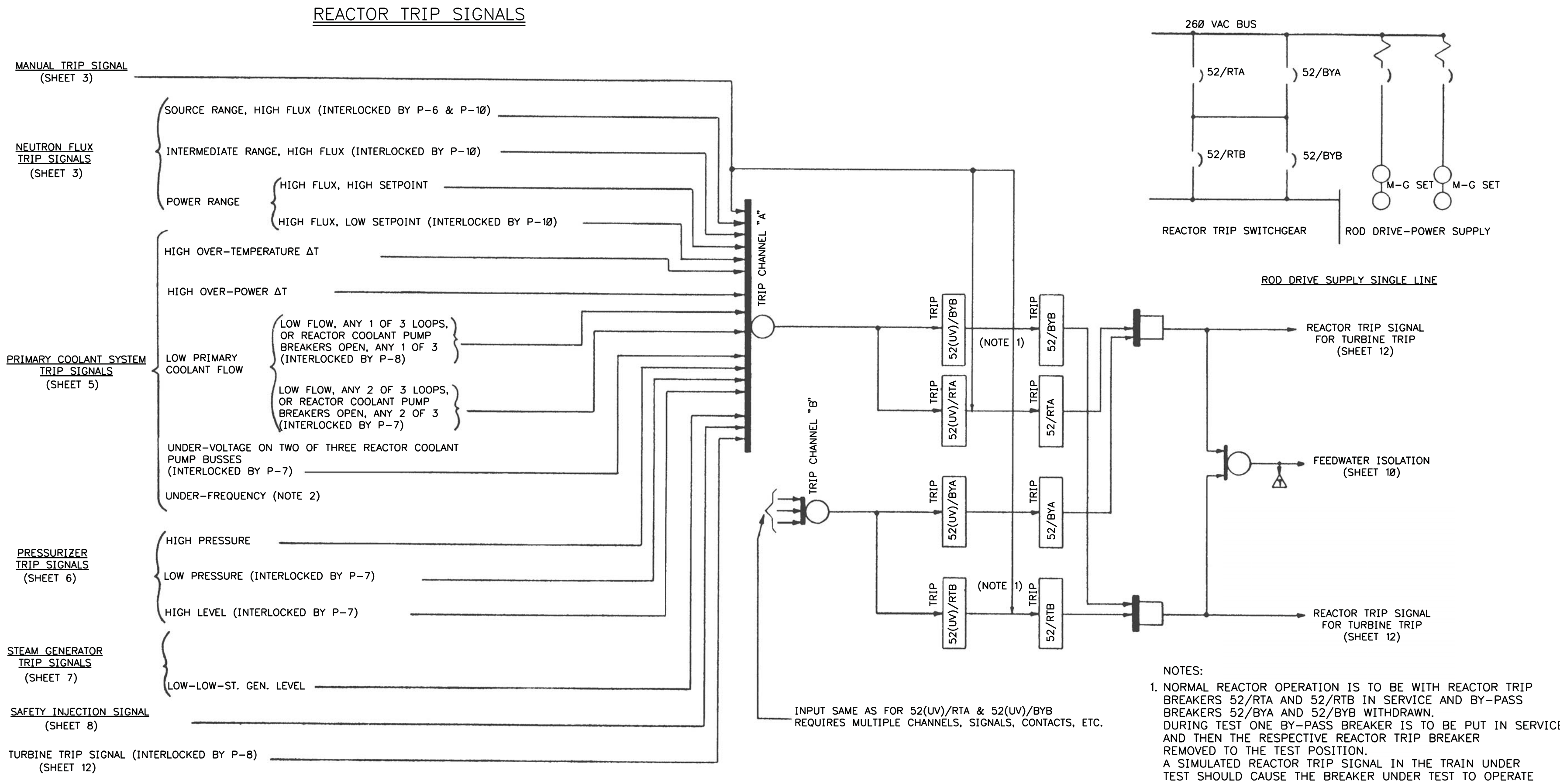
TITLE	VENDOR DRAWING 5648D69 SHEET NO.	CP&L DRAWING NUMBER
INDEX AND SYMBOLS	1	5379-02752
REACTOR TRIP SIGNALS	2	5379-02753
NUCLEAR INSTR. TRIP SIGNALS AND MANUAL TRIP	3	5379-02754
NUCLEAR INSTR. PERMISSIVES AND BLOCKS	4	5379-02755
PRIMARY COOLANT SYSTEM SIGNALS	5	5379-02756
PRESSURIZER TRIP SIGNALS	6	5379-02757
STEAM GENERATOR TRIP SIGNALS	7	5379-02758
SAFEGUARDS ACTUATION SIGNALS	8	5379-02759
ROD STOPS & TURBINE RUNBACKS	9	5379-02760
FEEDWATER ISOLATION	10	5379-02761
AUXILIARY FEEDWATER PUMPS-STARTUP	11	5379-02762
TURBINE TRIP SIGNALS	12	5379-03495
EMERGENCY GENERATOR STARTING & BUS CLEARING	13	5379-03368
SAFEGUARDS SEQUENCE	14	5379-03367
AUTO BUS TRANSFER	15	5379-04642
STEAM DUMP CONTROL	16	5379-03492
PRESSURIZER PRESSURE & LEVEL CONTROL	17	5379-03493
PRESSURIZER HEATER CONTROL	18	5379-03498

Revision No. 15 E2

H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS - SHEET 1
INDEX AND SYMBOLS

FIGURE 7.2.1 - 17



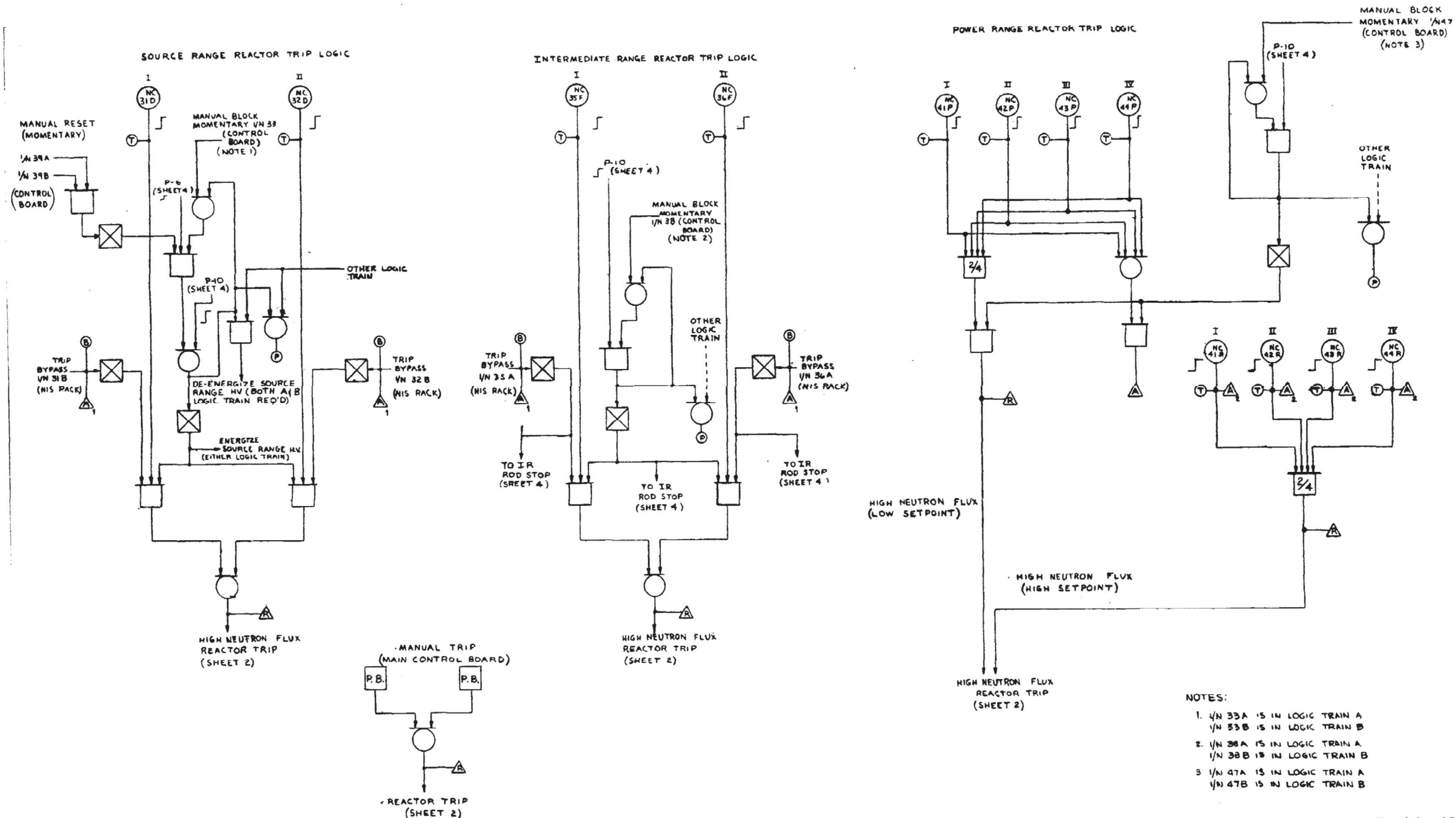
NOTES:

1. NORMAL REACTOR OPERATION IS TO BE WITH REACTOR TRIP BREAKERS 52/RTA AND 52/RTB IN SERVICE AND BY-PASS BREAKERS 52/BYA AND 52/BYB WITHDRAWN.
   DURING TEST ONE BY-PASS BREAKER IS TO BE PUT IN SERVICE AND THEN THE RESPECTIVE REACTOR TRIP BREAKER REMOVED TO THE TEST POSITION.
   A SIMULATED REACTOR TRIP SIGNAL IN THE TRAIN UNDER TEST SHOULD CAUSE THE BREAKER UNDER TEST TO OPERATE WITHOUT REACTOR TRIP.
   ONLY ONE REACTOR TRIP BREAKER IS TO BE TESTED AT A TIME.
2. UNDER-FREQUENCY ON TWO OF THREE REACTOR COOLANT PUMP BUSSES WILL TRIP ALL REACTOR COOLANT PUMPS AND CONSEQUENTLY CAUSE REACTOR TRIP.

H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS - SHEET 2
REACTOR TRIP SIGNALS

FIGURE 7.2.1-18 REVISION 25

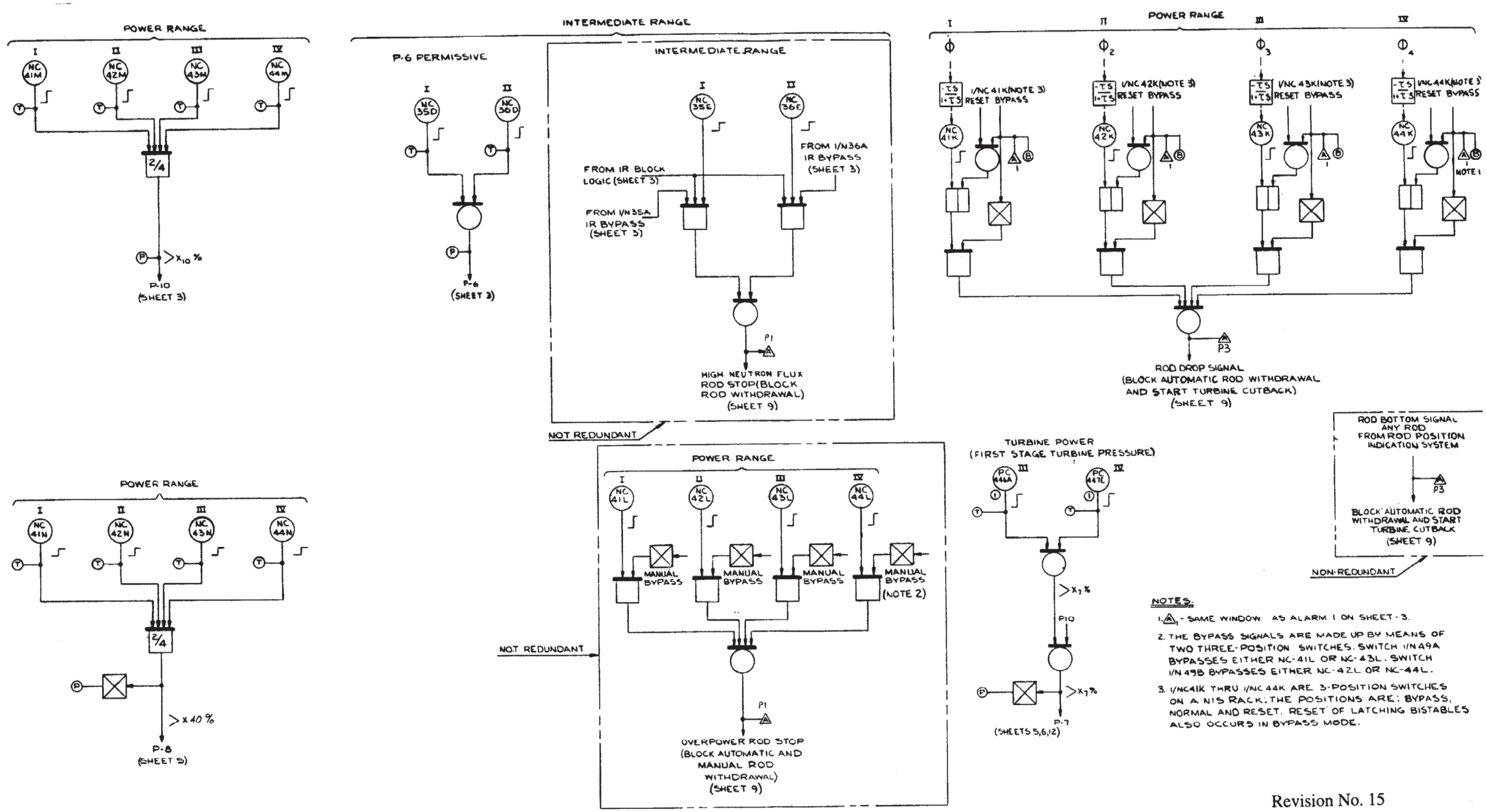


Revision No. 15

H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS - SHEET 3
NUCLEAR INSTRUMENTATION TRIP
SIGNALS AND MANUAL TRIP

FIGURE 7.2.1 - 19

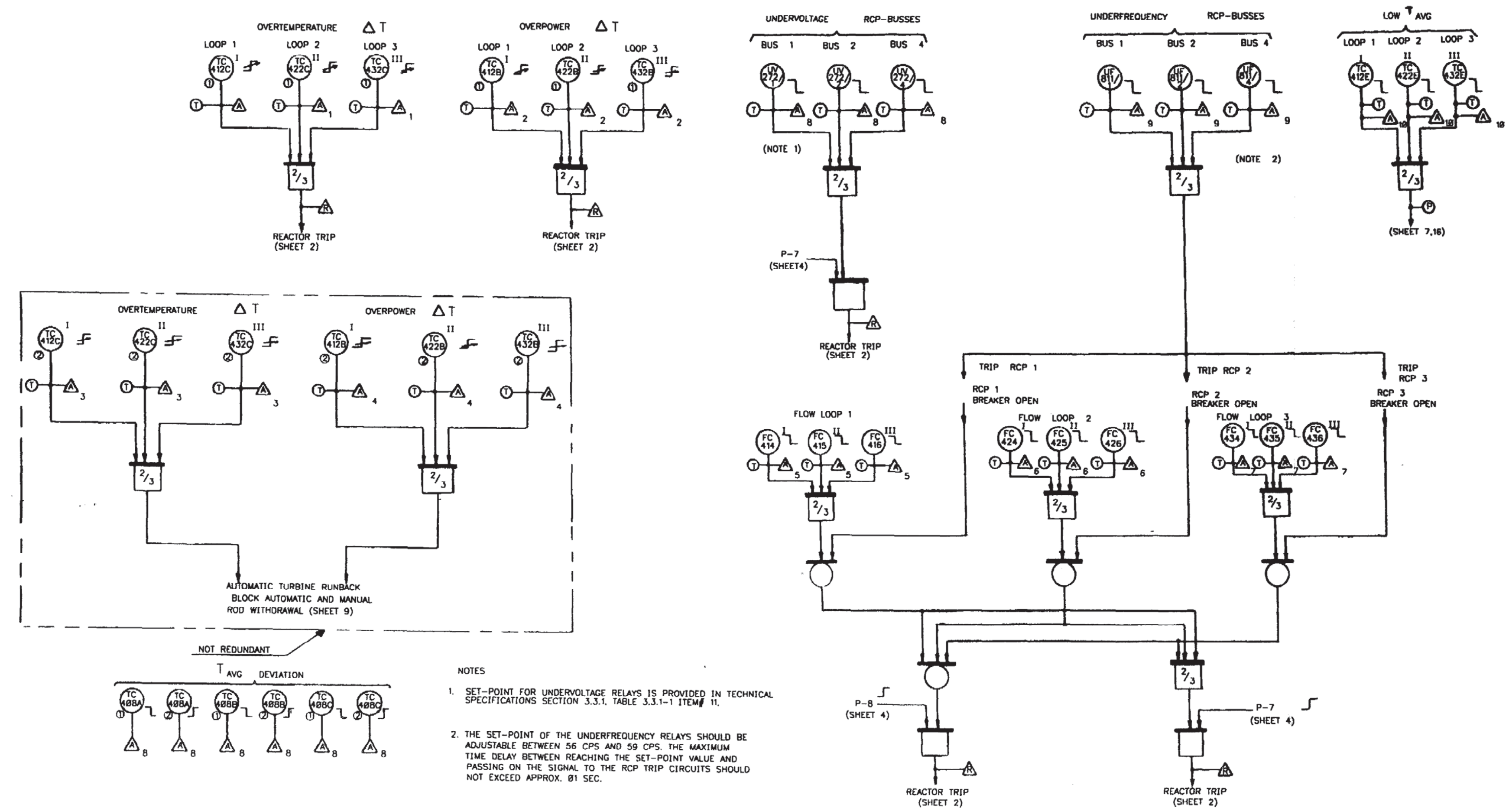


Revision No. 15

H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS - SHEET 4
NUCLEAR INSTRUMENTATION
PERMISSIVES AND BLOCKS

FIGURE 7.2.1 - 20



NOTES

1. SET-POINT FOR UNDERVOLTAGE RELAYS IS PROVIDED IN TECHNICAL SPECIFICATIONS SECTION 3.3.1, TABLE 3.3.1-1 ITEM# 11.

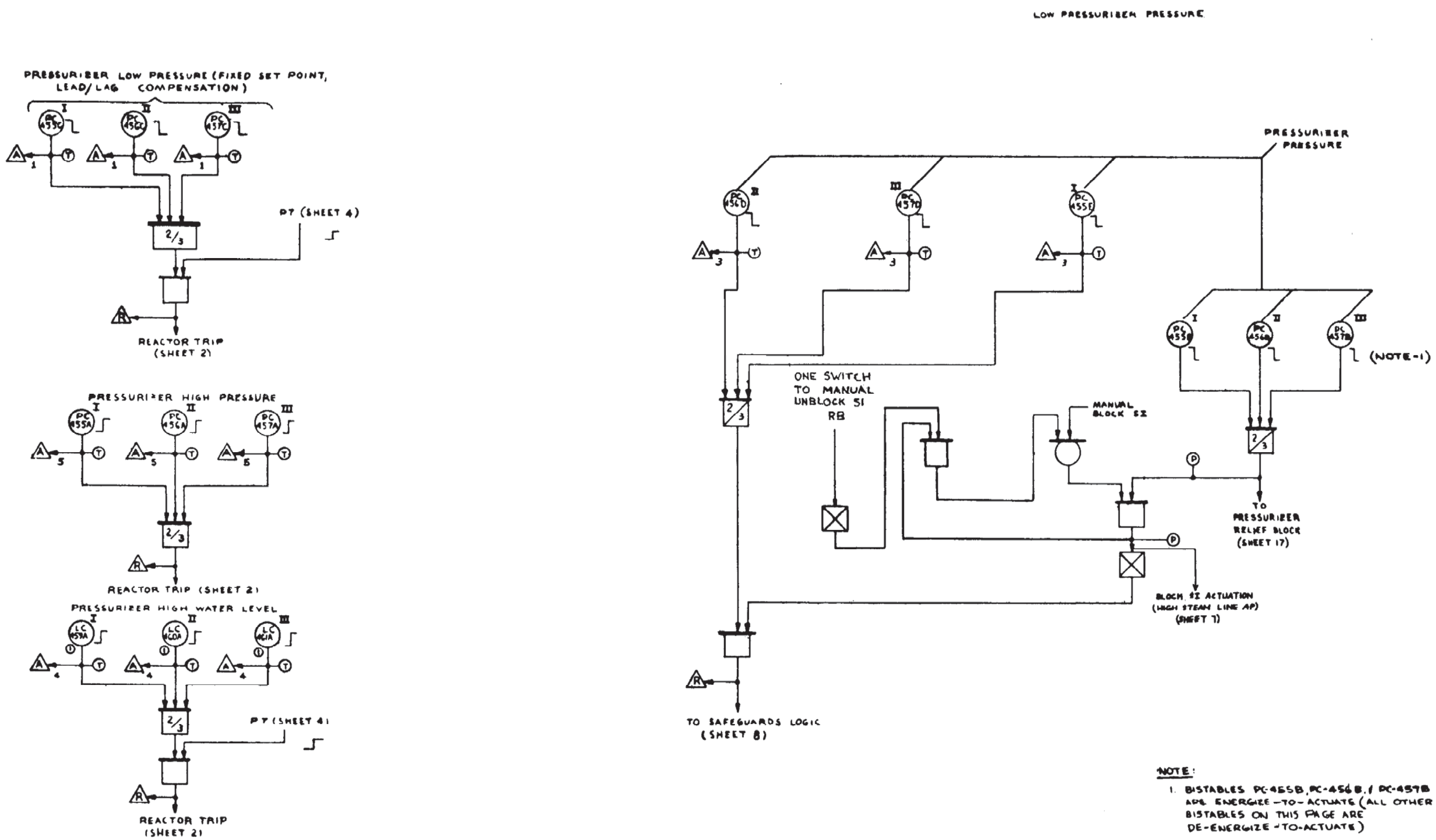
2. THE SET-POINT OF THE UNDERFREQUENCY RELAYS SHOULD BE ADJUSTABLE BETWEEN 56 CPS AND 59 CPS. THE MAXIMUM TIME DELAY BETWEEN REACHING THE SET-POINT VALUE AND PASSING ON THE SIGNAL TO THE RCP TRIP CIRCUITS SHOULD NOT EXCEED APPROX. Ø1 SEC.

REVISION NO. 15 E2

H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS - SHEET 5
PRIMARY COOLANT SYSTEM SIGNALS

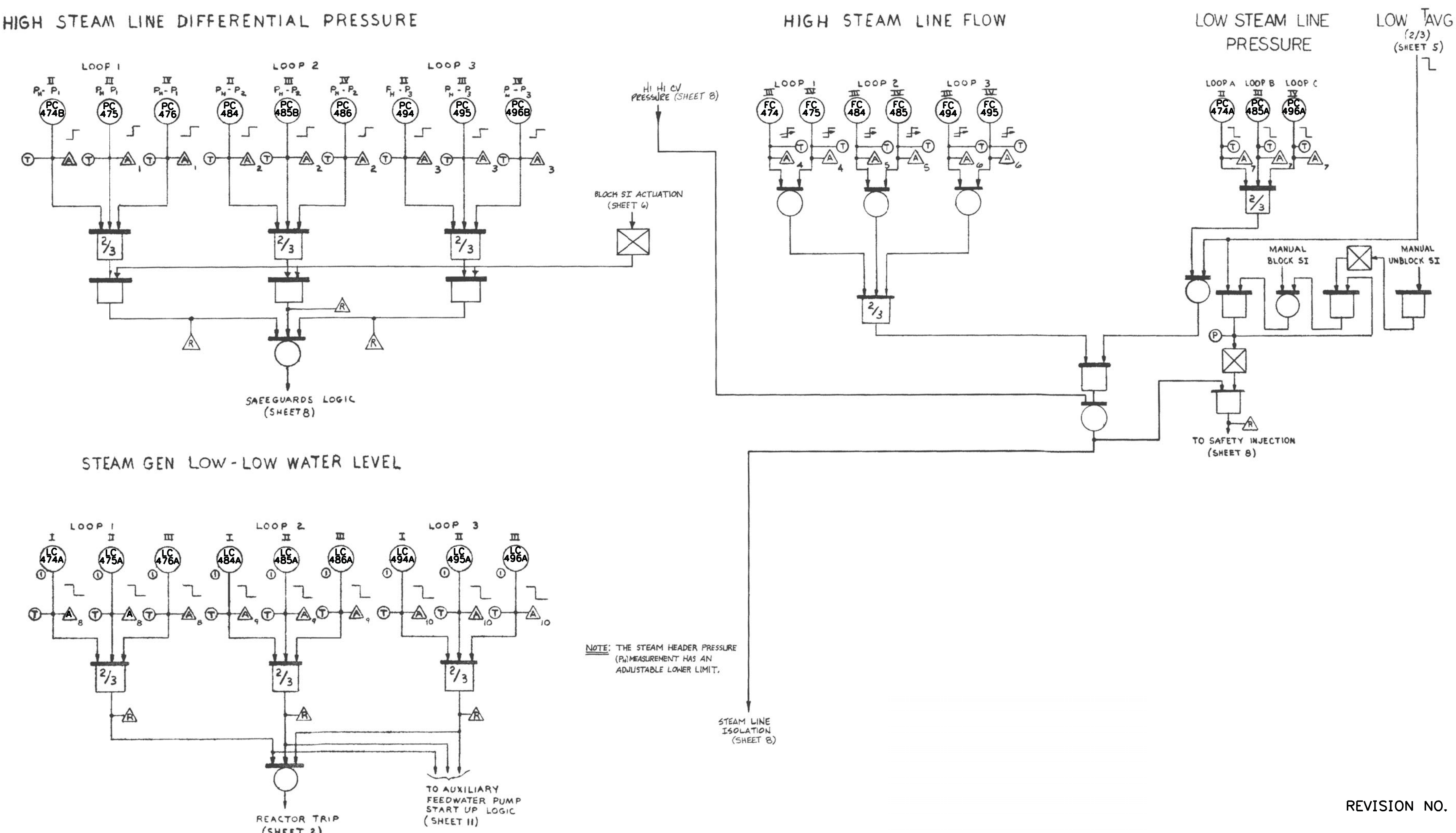
FIGURE 7.2.1 - 21



H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS - SHEET 6
PRESSURIZER TRIP SIGNALS

FIGURE 7.2.1 - 22

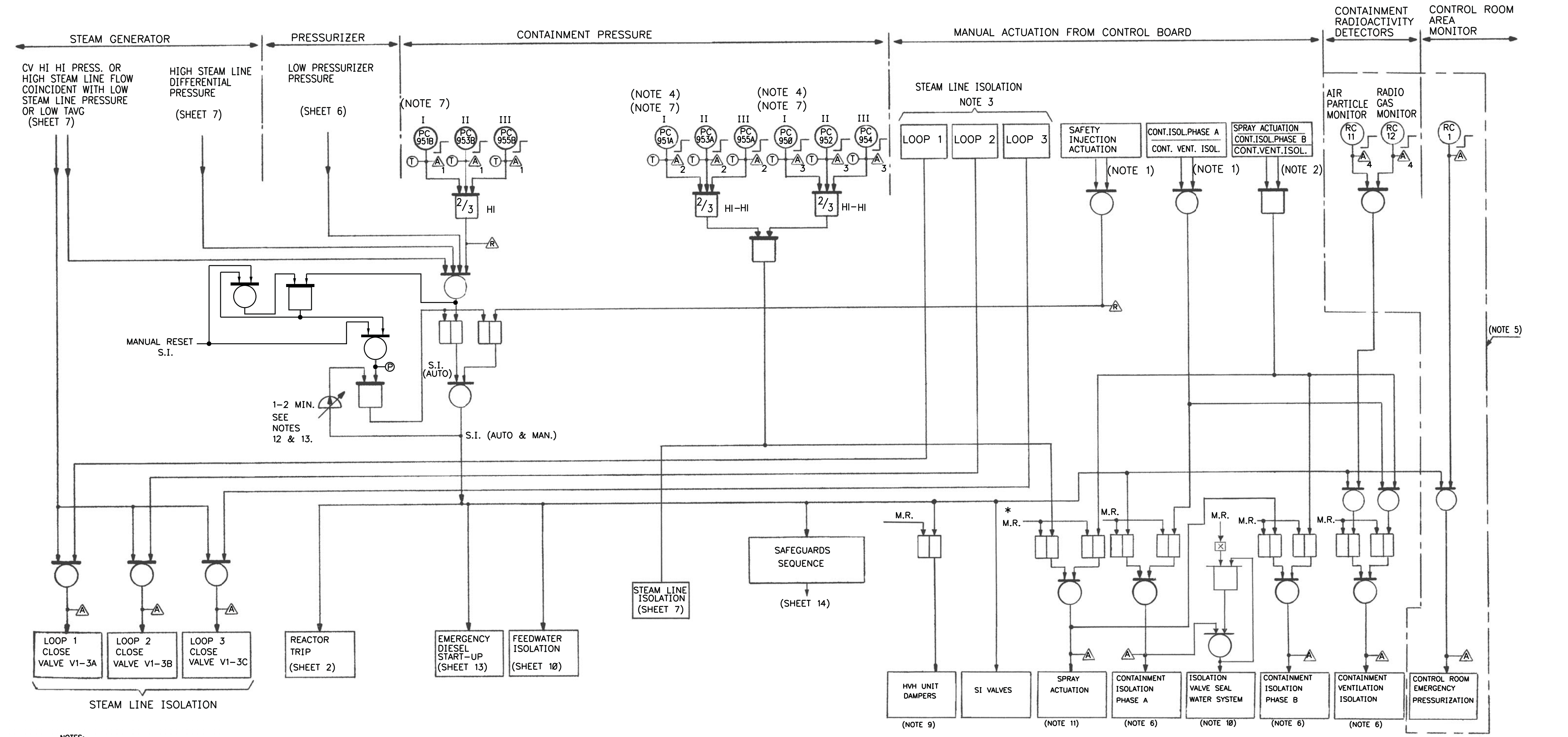


REVISION NO. 25

H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS - SHEET 7
STEAM GENERATOR TRIP SIGNALS

FIGURE 7.2.1 - 23



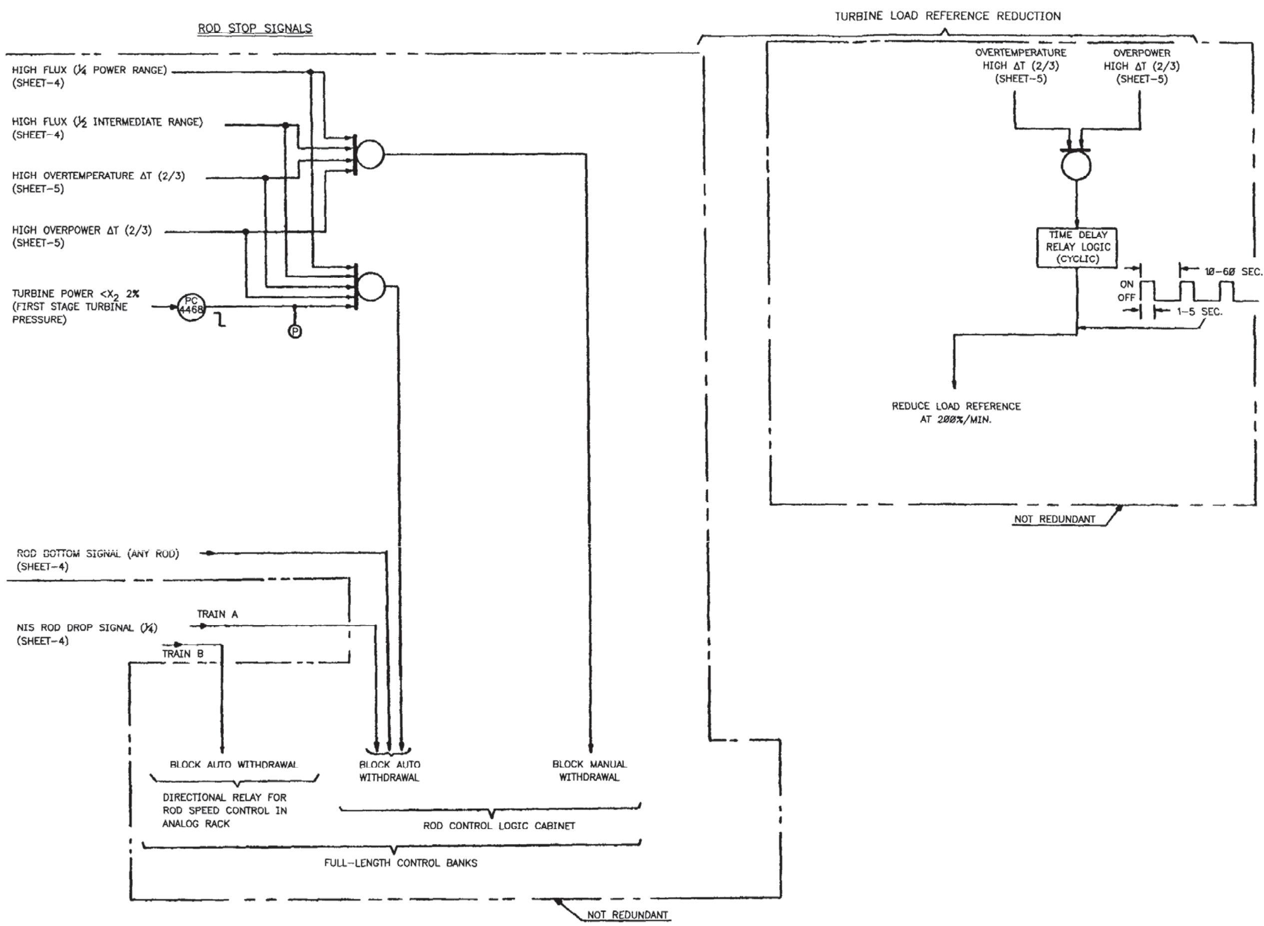
NOTES:

1. TWO MOMENTARY PUSH BUTTONS; PRESSING OF EITHER PUSH BUTTON WILL ACTUATE.
2. TWO MOMENTARY PUSH BUTTONS; ACTUATION IS EFFECTED ONLY IF BOTH PUSH BUTTONS ARE PRESSED SIMULTANEOUSLY.
3. ONE MOMENTARY PUSH BUTTON PER LOOP.
4. CONTAINMENT PRESSURE BISTABLES FOR SPRAY ACTUATION ARE ENERGIZE-TO-ACTUATE (OTHER BISTABLES ARE DE-ENERGIZE-TO-ACTUATE).
5. ENCLOSED CIRCUITRY IS NOT PART OF THE SAFEGUARDS SYSTEM AND IS NOT REDUNDANT.
6. COMPONENTS ACTUATED BY CONTAINMENT ISOLATION SIGNAL (PHASE A&B) AND COMPONENTS ACTUATED BY CONTAINMENT VENTILATION ISOLATION ARE ALL INDIVIDUALLY SEALED IN (LATCHED), SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE POSITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.
7. PC-950, PC-951A & PC-951B ARE FED BY THE DIESEL AUTOMATICALLY ON BLACKOUT.
8. UNDERVOLTAGE INCLUDES 480 VAC AND/OR 125 VDC CONTROL POWER.
9. COMPONENTS ACTUATED BY SI SIGNAL ARE INDIVIDUALLY SEALED IN (LATCHED) SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE POSITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.
10. COMPONENTS ACTUATED BY SI SIGNAL, CONT. VENT. ISOL. AND PHASE A ISOL. ARE INDIVIDUALLY ELECTRICALLY SEALED IN SO THE LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE POSITION PRIOR TO ACTUATION SIGNAL.
11. ITEM MARKED WITH * MAY BE MAINTAINED BY KEY LOCK SWITCH.
12. IF THE SI RESET PUSHBUTTON IS DEPRESSED PRIOR TO WAITING 2 MINUTES AFTER A MANUAL SAFETY INJECTION IS INITIATED, THE SIGNAL WILL NOT RESET AFTER THE 2 MINUTES HAS ELAPSED.
13. IF THE SI RESET PUSHBUTTON IS DEPRESSED PRIOR TO WAITING 2 MINUTES AFTER AN AUTOMATIC SAFETY INJECTION IS INITIATED, THE SIGNAL WILL RESET AFTER THE 2 MINUTES HAS ELAPSED. IF AUTO SI SIGNAL STILL EXISTS.

H. B. ROBINSON
UNIT 2
DUKE ENERGY
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS – SHEET 8
SAFEGUARD ACTUATION SIGNALS

FIGURE 7.2.1-24 REVISION 27

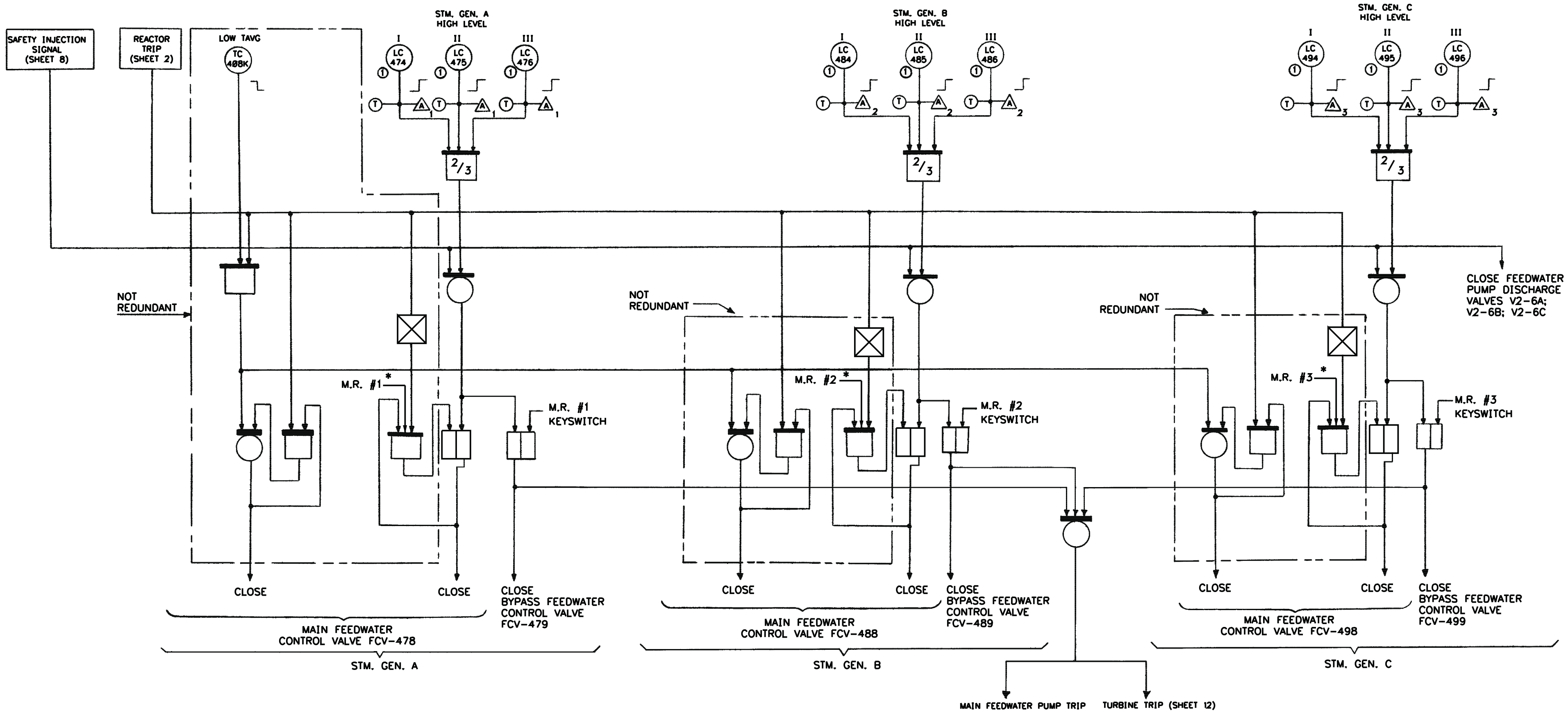


H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS – SHEET 9
ROD STOP AND TURBINE LOAD CUTBACK

FIGURE 7.2.1-25

REVISION 17

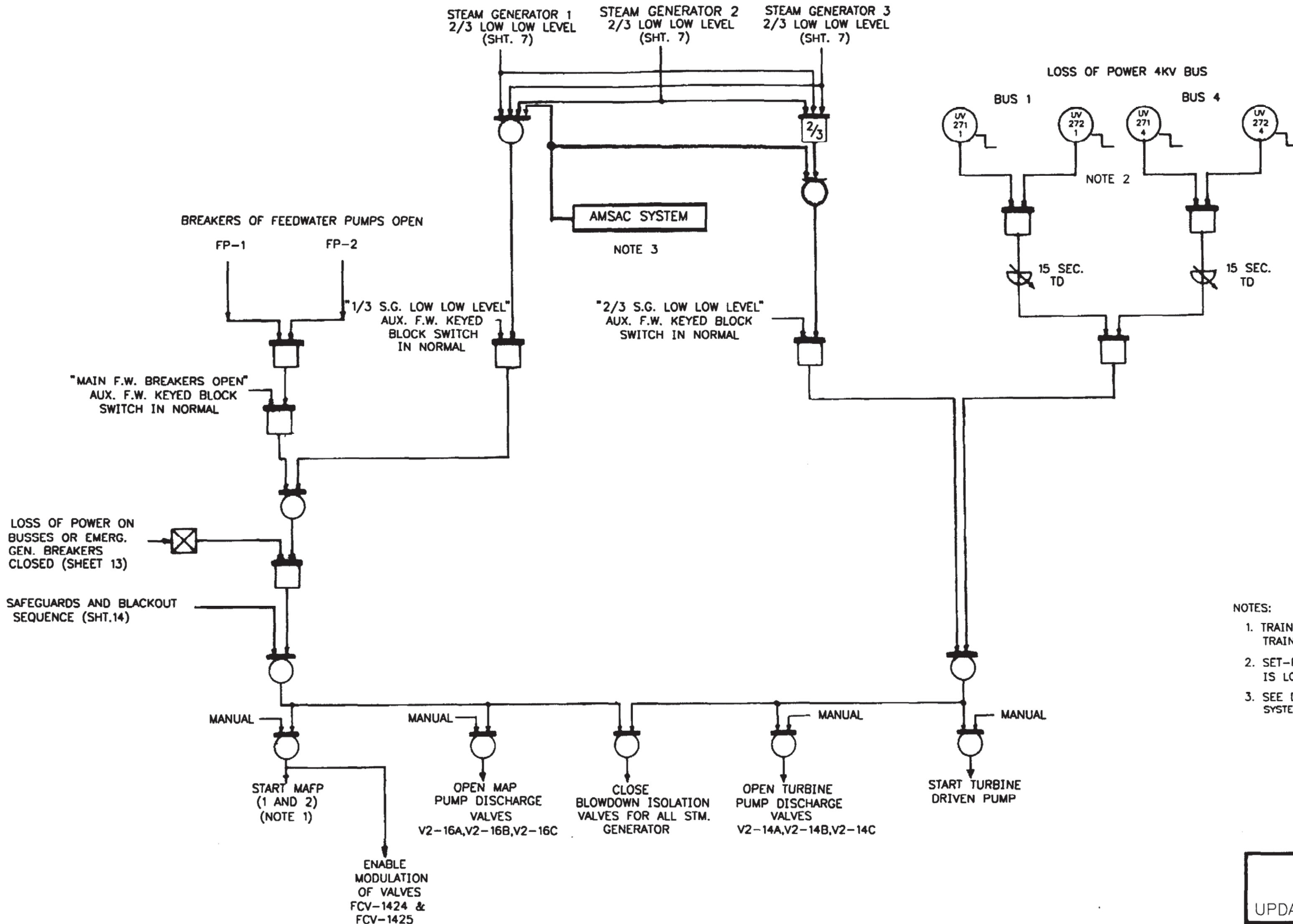


* ACTUATED BY RESET OF BYPASS FEEDWATER CONTROL

H. B. ROBINSON
UNIT 2
CAROLINA POWER & LIGHT COMPANY
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS – SHEET 10
FEEDWATER ISOLATION

FIGURE 7.2.1-26 REVISION 24



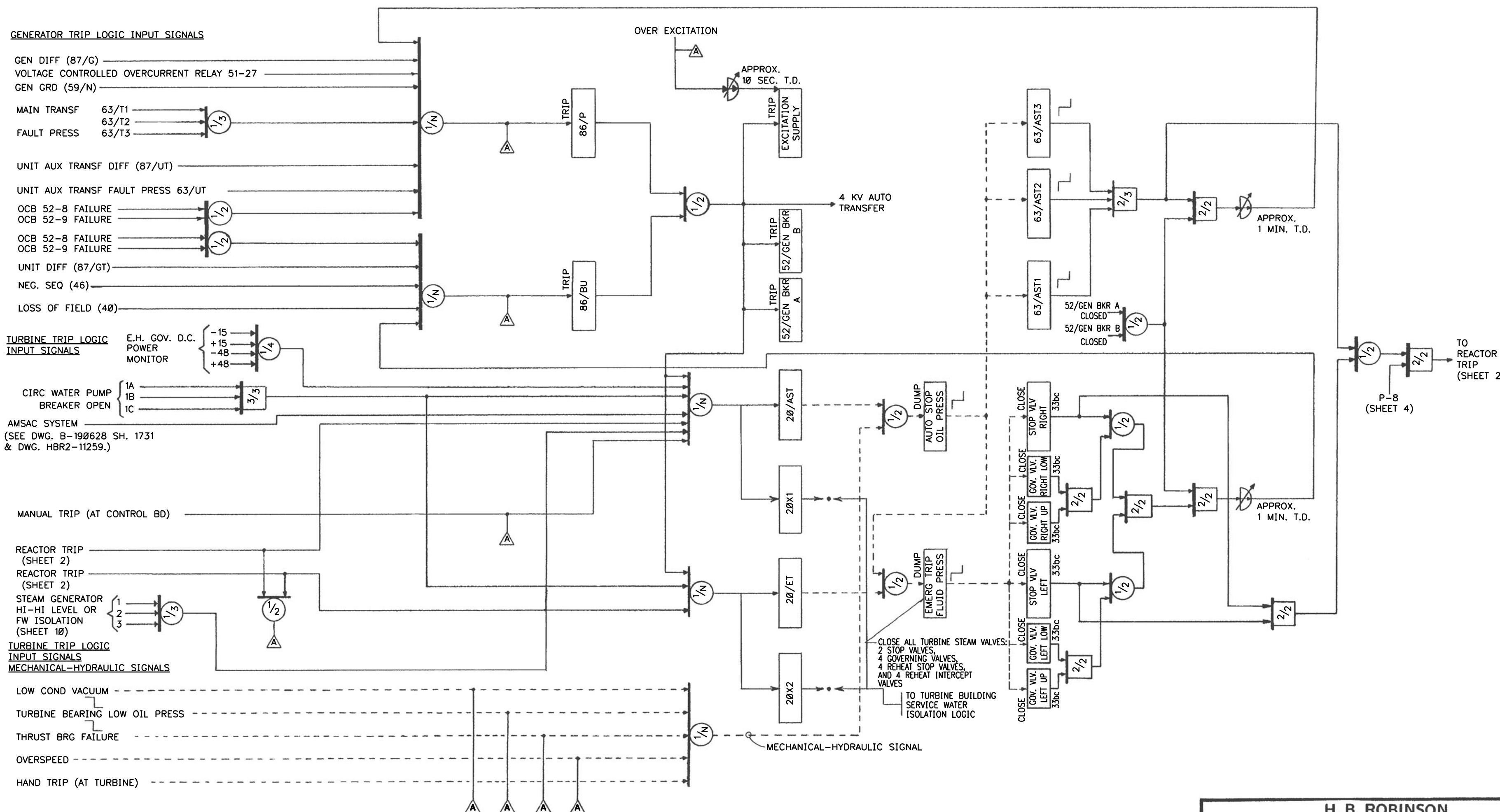
NOTES:

1. TRAIN "A" CONTROLS MAFP 1, BREAKER 52/20A
   TRAIN "B" CONTROLS MAFP 2, BREAKER 52/24C
2. SET-POINT FOR UNDER-VOLTAGE RELAYS IS LOCATED IN TECHNICAL SPECIFICATION SECTION 3.3.1.
3. SEE DWG. B-190628 SH.1731 AND HBR2-11259 FOR AMSAC SYSTEM.

REVISION NO. 15

H.B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

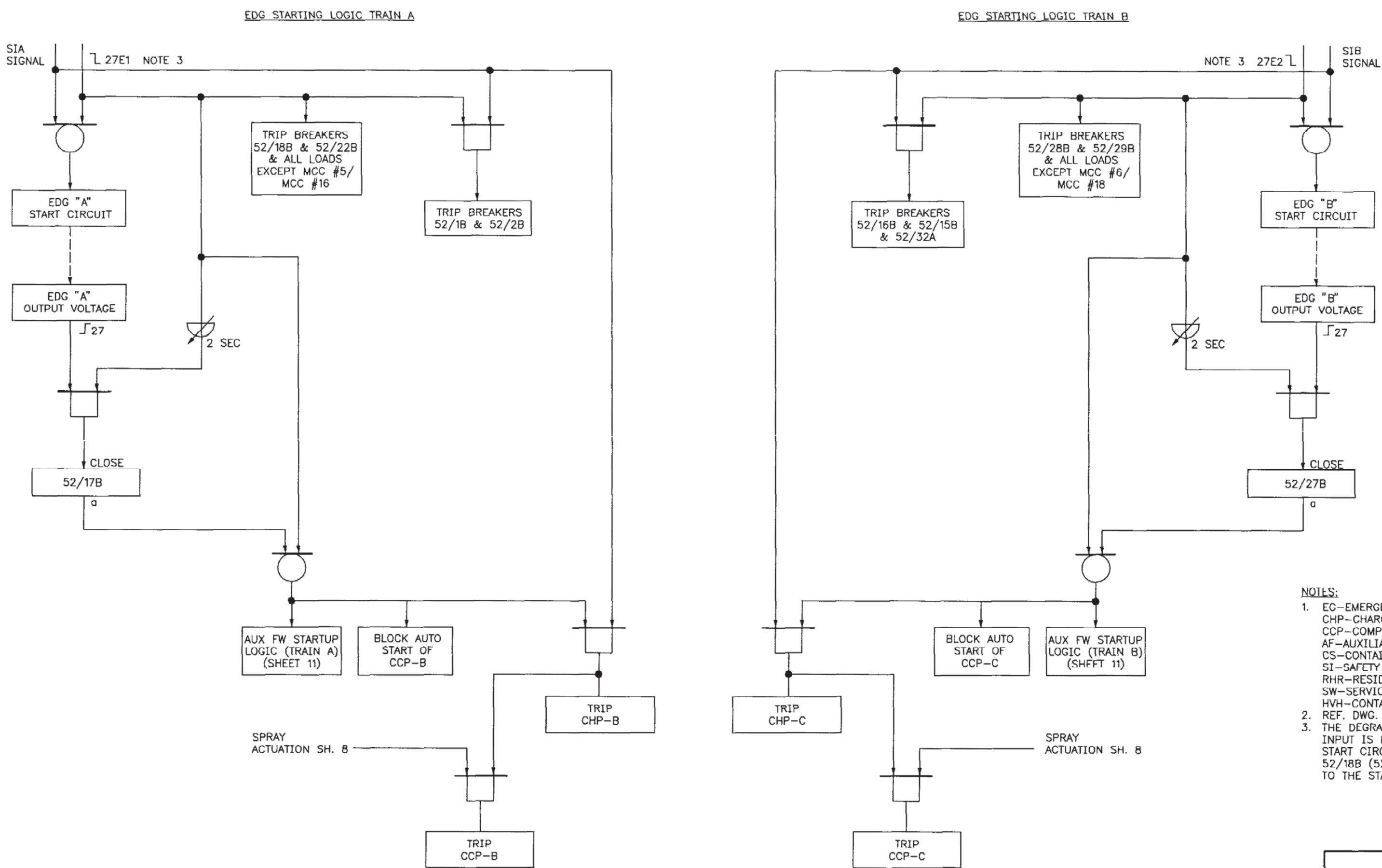
LOGIC DIAGRAMS - SHEET 11
AUXILIARY FEEDWATER PUMP START-UP
FIGURE 7.2.1 - 27



H. B. ROBINSON
UNIT 2
DUKE ENERGY
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS - SHEET 12
TURBINE TRIP SIGNAL

FIGURE 7.2.1-28 REVISION NO. 27



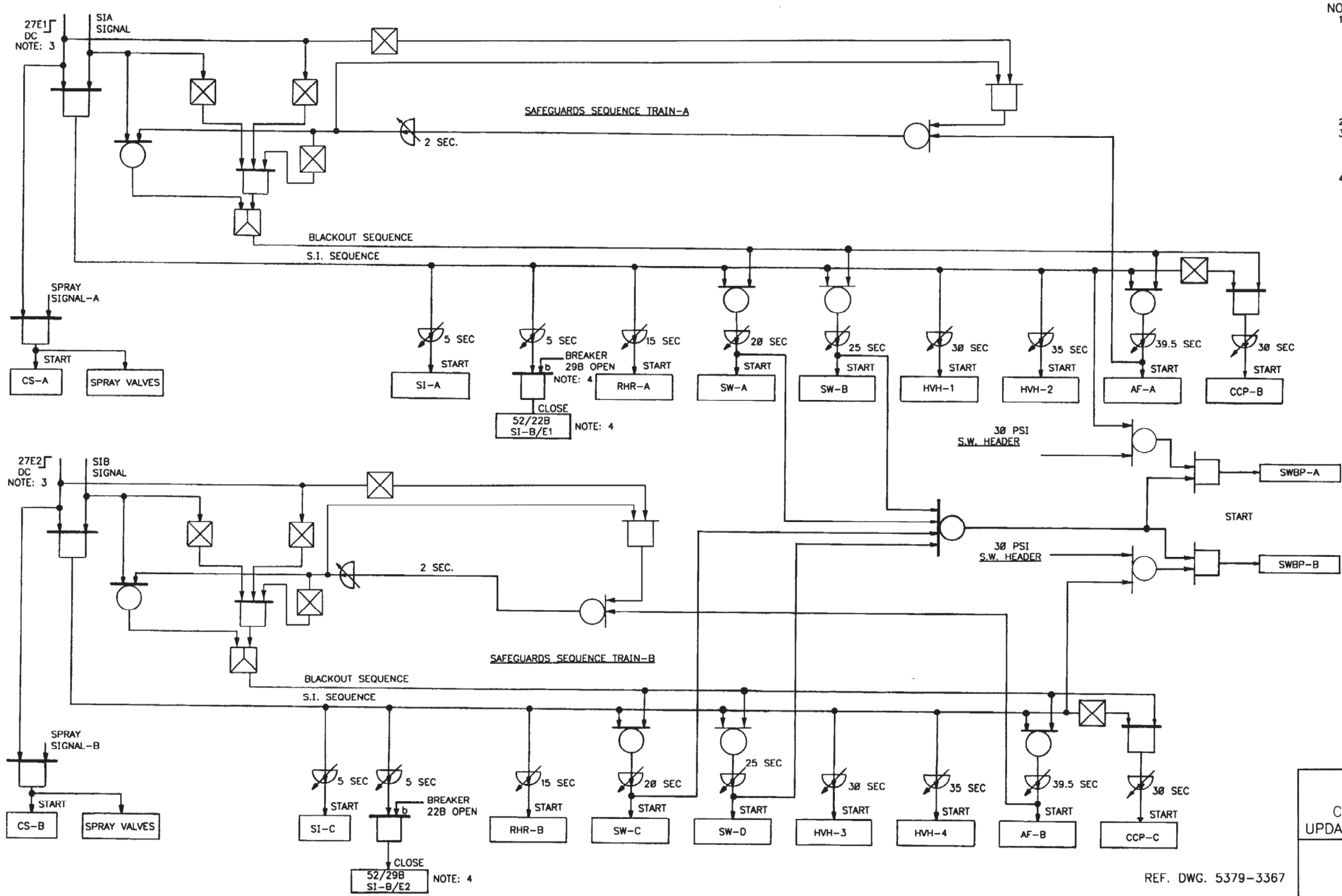
NOTES:

1. EG-EMERGENCY GENERATOR
   CHP-CHARGING PUMP
   CCP-COMPONENT COOLING PUMP
   AF-AUXILIARY FEEDWATER PUMP
   CS-CONTAINMENT SPRAY PUMP
   SI-SAFETY INJECTION PUMP
   RHR-RESIDUAL HEAT REMOVAL PUMP
   SW-SERVICE WATER PUMP
   HVH-CONTAINMENT FAN
2. REF. DWG. 541F214.
3. THE DEGRADED GRID VOLTAGE (GREATER THAN 10 SECONDS) INPUT IS PROVIDED TO THE EMERGENCY DIESEL GENERATOR START CIRCUIT BY TRIPPING THE NORMAL INPUT BREAKER 52/18B (52/28B) WHICH PROVIDES THE 27E1 (27E2) SIGNAL TO THE START CIRCUITRY.

H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS-SHEET 13
EMERGENCY GENERATOR AND
BUS CLEARING

REVISION 18E — FIGURE 7.2.1-29



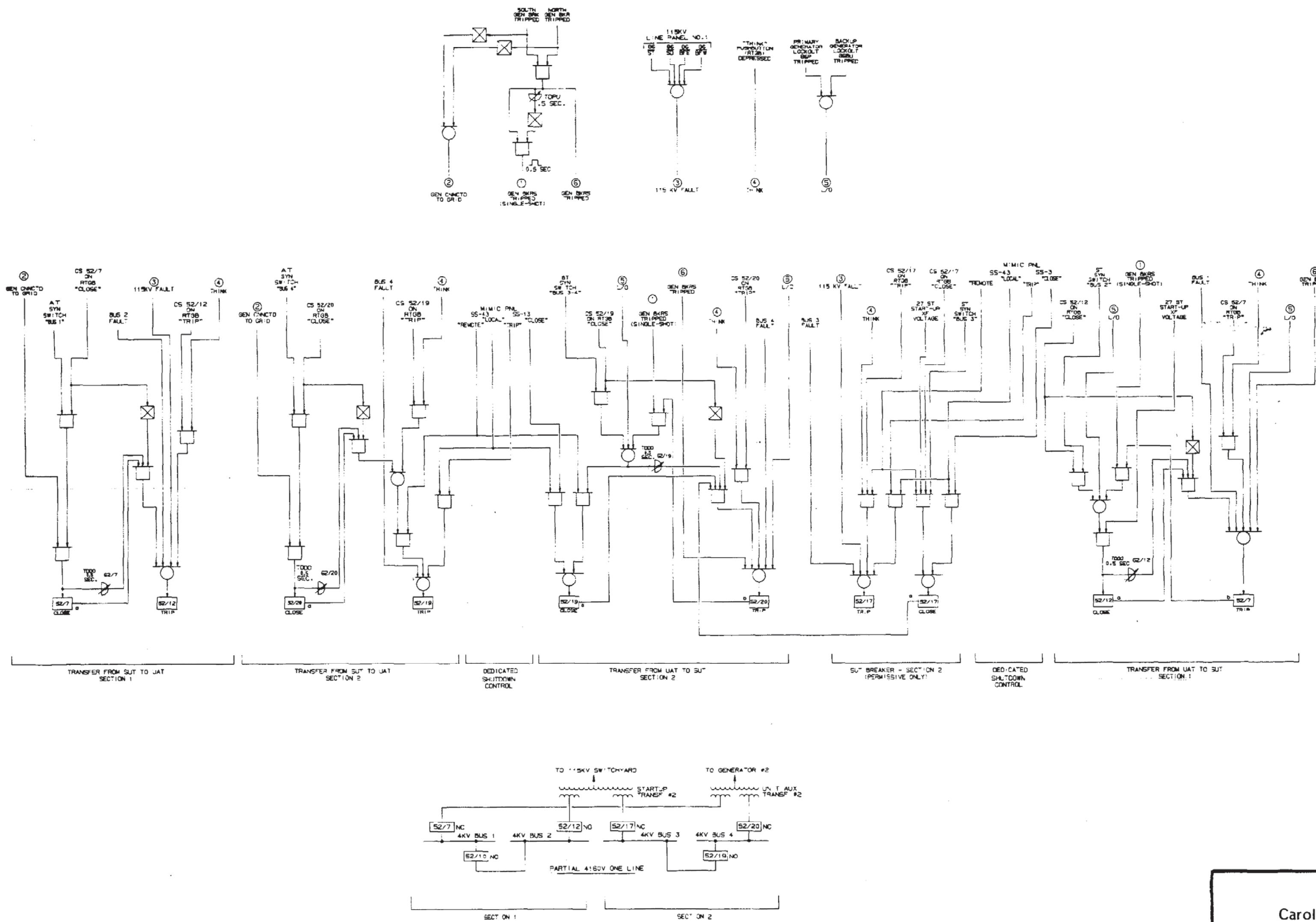
NOTES:
1. EG - EMERGENCY GENERATOR
   CHP - CHARGING PUMP
   CCP - COMPONENT COOLING PUMP
   AF - AUXILIARY FEEDWATER PUMP
   CS - CONTAINMENT SPRAY PUMP
   SI - SAFETY INJECTION PUMP
   RHR - RESIDUAL HEAT REMOVAL PUMP
   SW - SERVICE WATER PUMP
   HVH - CONTAINMENT FAN
2. REF. DWG. 541F214
3. BOTH 480 VAC AND 125 VDC FOR THE BUS MUST BE AVAILABLE BEFORE THE SEQUENCE WILL START. MOD-947.
4. BREAKERS 52/22B AND 52/29B WILL NORMALLY BE RACKED OUT UNLESS "B" SI PUMP IS BEING USED TO REPLACE "A" OR "C" SI PUMP. BREAKER 52/29C WILL BE NORMALLY CLOSED.

REF. DWG. 5379-3367

REVISION 16

H.B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS - SHEET 14
SAFEGUARD SEQUENCE
FIGURE 7.2.1-30

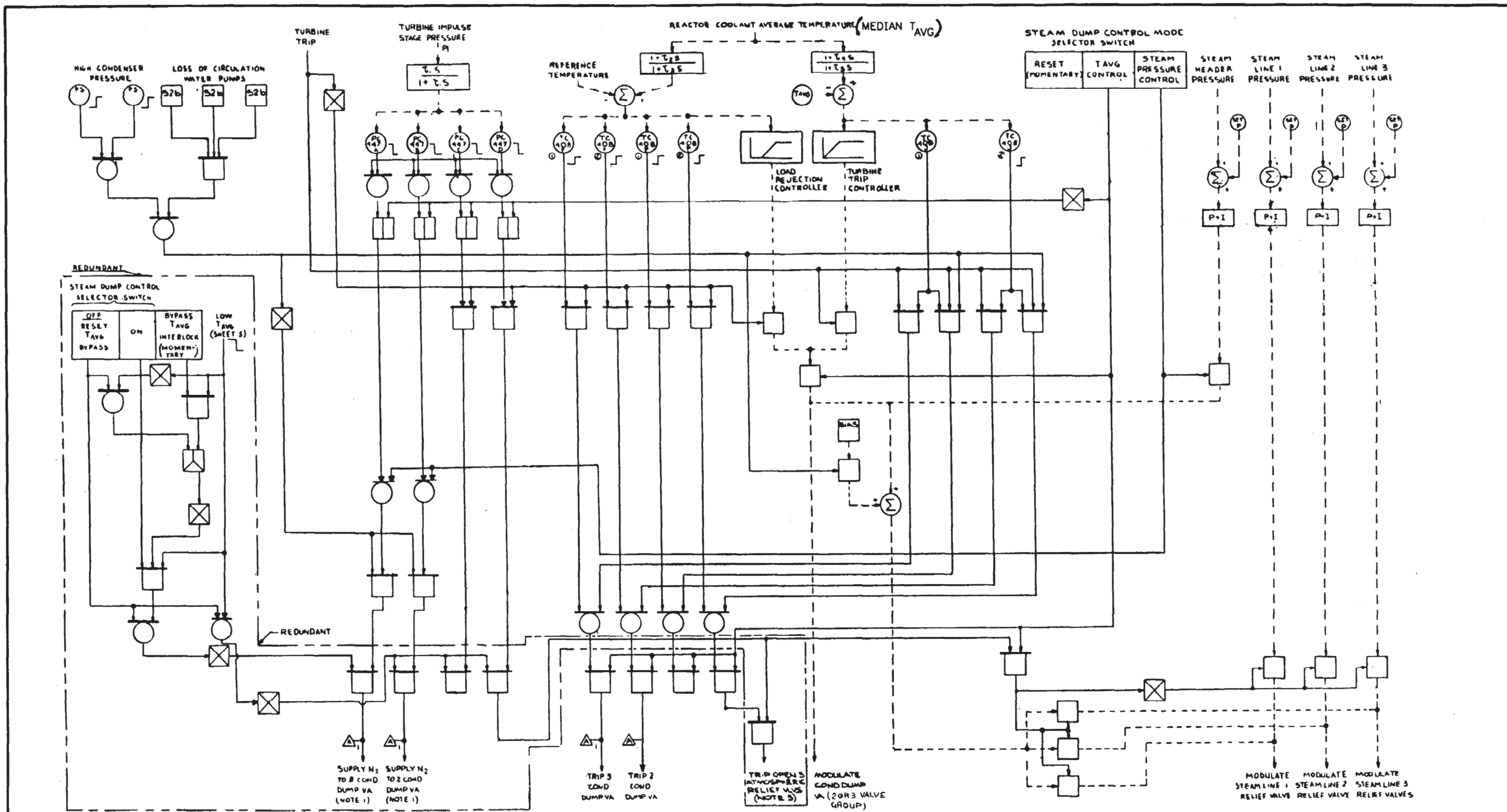


Revision No. 15

H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS - SHEET 15
4160 V AUTO BUS TRANSFER

FIGURE 7.2.1 - 31



REVISION NO.15

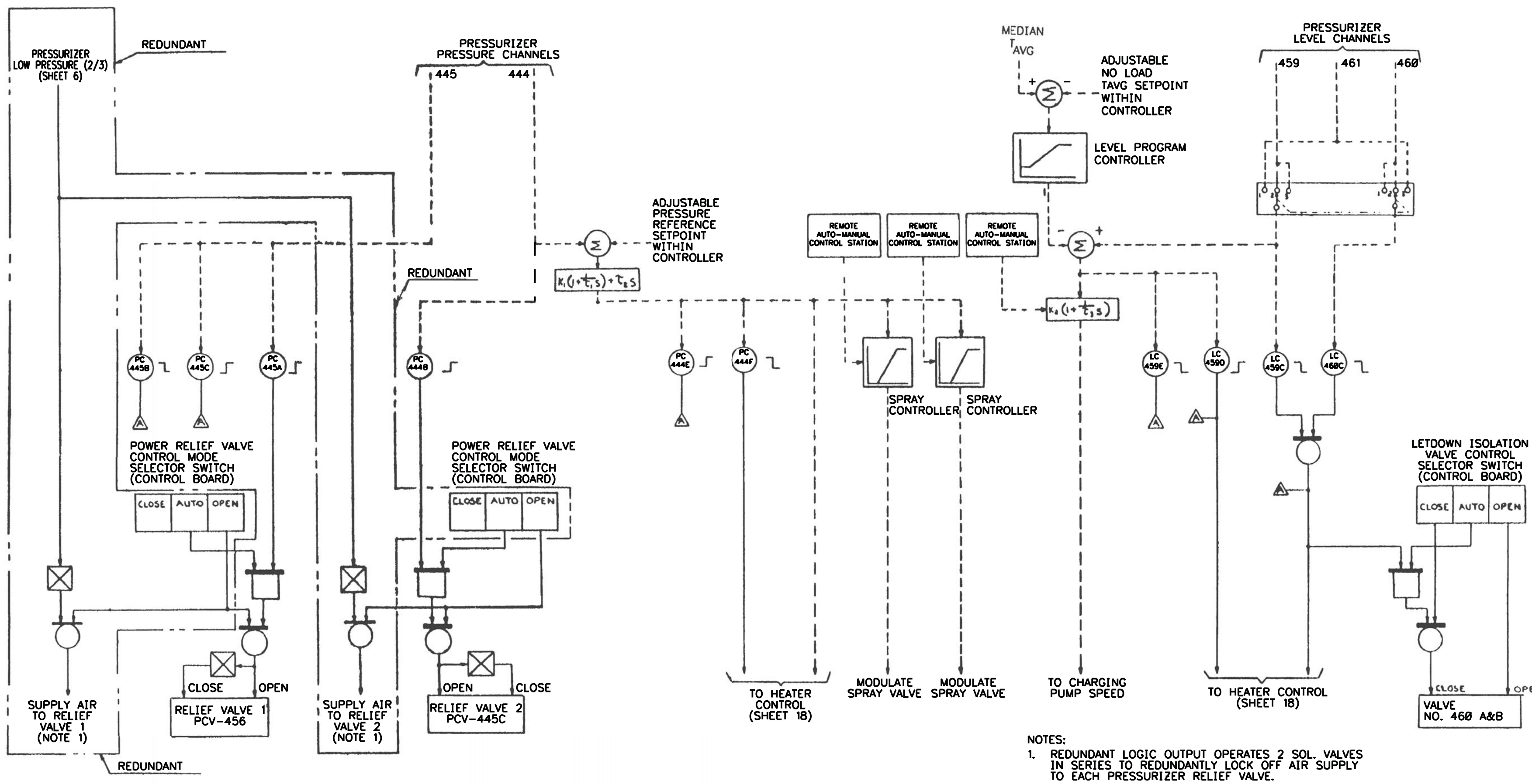
NOTES

1. REDUNDANT LOGIC OUTPUT OPERATES 2 SOLENOID VALVES IN SERIES TO REDUNDANTLY LOCK OFF N2 SUPPLY TO THE STEAM DUMP VALVES.
2. ALL CIRCUITS ON THIS SHEET ARE NOT REDUNDANT EXCEPT WHERE INDICATED "REDUNDANT".
3. THE REDUNDANT LOCK OUTPUT OPERATES 2 SOLENOID VALVES IN SERIES IN THE AIR LINE BETWEEN THE MAIN AIR SUPPLY AND EACH RELIEF VALVE DIAPHRAGM THE SOLENOID VALVE ARE DE-ENERGIZED TO CLOSE WHICH REDUNDANTLY STOPS THE TRIP OPEN FUNCTION.

H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS - SHEET 16
STEAM DUMP CONTROL

FIGURE 7.2.1 - 32



NOTES:

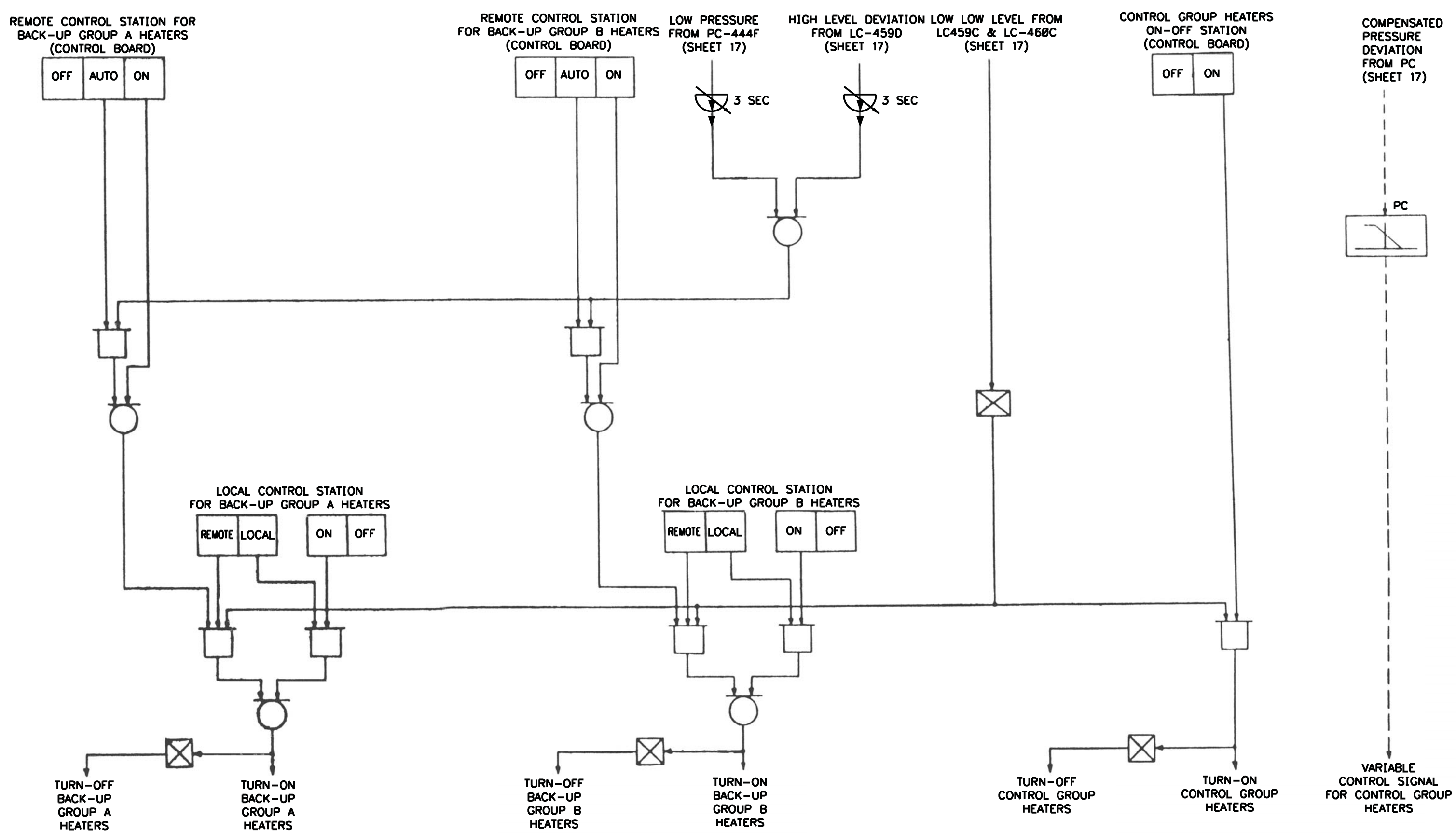
1. REDUNDANT LOGIC OUTPUT OPERATES 2 SOL. VALVES IN SERIES TO REDUNDANTLY LOCK OFF AIR SUPPLY TO EACH PRESSURIZER RELIEF VALVE.
2. ALL CIRCUITS ON THIS SHEET ARE NOT REDUNDANT, EXCEPT WHERE INDICATED "REDUNDANT."

REVISION NO. 25

H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS - SHEET 17
PRESSURIZER PRESSURE AND
LEVEL CONTROL

FIGURE 7.2.1 - 33



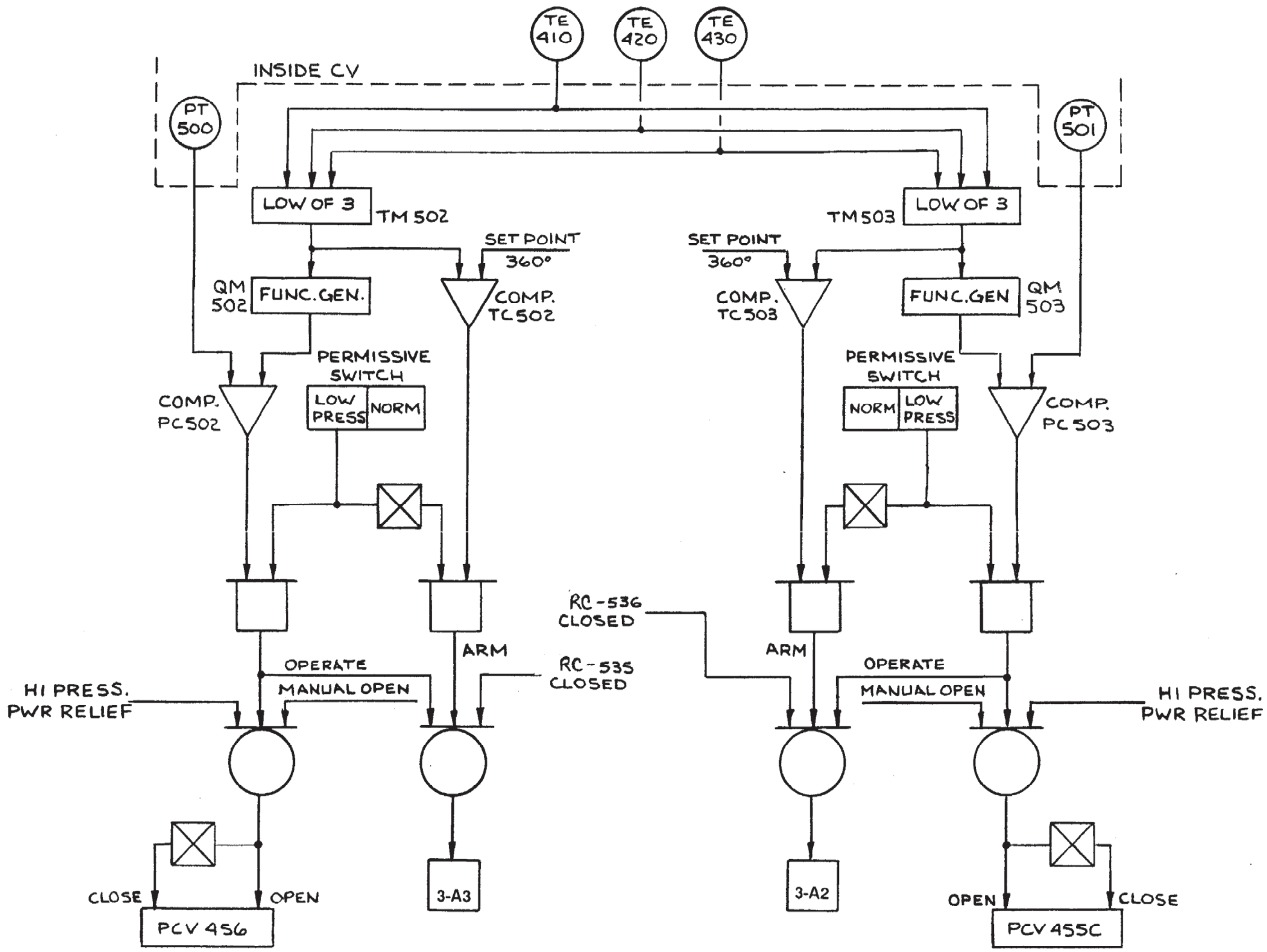
NOTES:
1. ALL CIRCUITS ON THIS SHEET ARE NOT REDUNDANT.

REVISION NO. 25

H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAMS - SHEET 18
PRESSURIZER HEATER CONTROL

FIGURE 7.2.1 - 34



REVISION 18

H. B. ROBINSON
UNIT 2
Carolina Power & Light Company
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAM
HIGH PRESSURE - LOW TEMPERATURE
PROTECTION SYSTEM
FIGURE 7.2.1-35

7.3 ENGINEERED SAFETY FEATURE SYSTEMS

The Engineered Safety Feature (ESF) Instrumentation measures temperatures, pressures, flows, and levels in the Reactor Coolant System (RCS), Reactor Containment, and Auxiliary Systems, activates the ESF, Containment Isolation, Steam Line Isolation, and Emergency Feedwater, and monitors their operation.

7.3.1 DESCRIPTION

7.3.1.1 System Description

The ESF actuation instrumentation performs the functions shown in Table 7.3.1-1. These functions are summarized below.

a) Operation of the Safety Injection System (SIS) is initiated upon occurrence of any of the following events: low pressurizer pressure; high containment pressure; high differential pressure between any steam line and the steam line header; or high steam flow in any 2 steam lines, coincident with low steam pressure or low reactor coolant average temperature.

b) Operation of the containment isolation valves in nonessential process lines (phase A) is initiated upon automatic actuation of safety injection.

c) Operation of the Containment Spray System and remaining containment isolation valves (phase B) is initiated upon detection of a high-high containment pressure signal.

d) Operation of the Containment Air Recirculation Cooling System is started after initiation of the SIS.

e) The following signals will close all steam isolation valves:

   1) High steam flow coincident with low reactor coolant average temperature or low steam pressure

   2) High-high containment pressure signals

   Steam line isolation is required to prevent the blowdown of more than one steam generator (SG) in the unlikely event of a steam line fracture.

f) Any safety injection signal will isolate the main feedwater lines by closing all control valves (main and bypass valves), tripping the main feedwater pumps and closing the pump discharge valves. Key switches on the RTGB will allow the operator to override/block the Feedwater Isolation signal to the Feedwater Control Bypass valves and to the Main Feedwater pumps. The isolation signal to the Main Feedwater Control valves may be reset by these switches in conjunction with closing the Reactor Trip breakers. Placing of these key switches in the override/reset position will give an alarm on the RTGB and the keys cannot be removed when the switches are in the override/reset position. The auxiliary feedwater system is actuated by the safety injection signal.

g) Although the emergency feedwater system is not considered to be an engineered safeguard, its actuation is described below.

7.3.1.1.1 Auxiliary feedwater system initiation

The controls used to automatically start the auxiliary feedwater pumps are designed to meet the single failure criterion, with the exception of the opening of both feedwater pump circuit breakers and AMSAC. The following pump starting logic is used:

1. The two motor driven auxiliary feedwater pumps are started automatically on:

a. 2/3 low low level in any SG

b. Opening of both feedwater pump circuit breakers (one contact per pump breaker is used)

c. Any Safety Injection Signal

d. Loss of offsite power (i.e., the blackout sequence)

e. Manually

f. AMSAC trip (two of three SG below low-low setpoint at 35% power)

2. The turbine-driven auxiliary feedwater pump is started automatically on:

a. 2/3 low low level in any two SG

b. Loss of voltage on 4 kV buses 1 and 4. Two sensors are provided for each bus with 2/2 logic to indicate a loss of voltage on any one bus.

c. Manually

d. AMSAC trip (two of three SG below low-low setpoint at 35% power)

In the Loss of Normal Feedwater analysis, in Section 15.2.7, it has been assumed that the auxiliary feedwater pumps are started on the low low steam generator level signals. The analysis has been performed assuming only one motor-driven auxiliary feedwater pump is started at approximately one minute (see section 15.2.7) after reaching the low low level setpoint in all three SG.

The relay logic for starting the auxiliary feedwater pumps is separated into train A and train B logic, as is done for the relay logic used to actuate ESF. Logic train A will start one motor driven pump and logic train B will start the second motor-driven pump. Either logic train will open appropriate steam system valves to start the turbine-driven pump. The circuits used to start the auxiliary feedwater pumps will also open the appropriate valves to ensure delivery of flow to the SG.

To prevent the start of the auxiliary feedwater pumps under shutdown conditions, key switches have been installed as discussed in Section 7.3.2.2.2.

7.3.1.1.2 ESF Instrumentation

7.3.1.1.2.1 Design Basis

The ESF instrumentation measures temperatures, pressures, flows, and levels in the RCS, Steam System, Reactor Containment and Auxiliary Systems, actuates the ESF, and monitors their operation. Process variables required on a continuous basis for the startup, operation, and shutdown of the unit are indicated, recorded, and controlled from the Control Room. The quantity and types of process instrumentation provided ensure safe and orderly operation of all systems and processes over the full operating range of the plant.

Certain controls and indicators which require a minimum of operator attention, or are only in use intermittently, are located on local control panels near the equipment to be controlled. Monitoring of the alarms of such control systems are provided.

The same channel isolation and separation criteria as described for the reactor protection circuits (Section 7.2) are applied to the ESF actuation circuits.

The DC control supply associated with the ESF is designed to meet the single failure criterion such that one failure will not prevent actuation of sufficient ESF to meet the core and containment cooling criteria.

7.3.1.1.2.2 Design Features

The ESF instrumentation system is designed to use analog channels and initiation logic similar to that of the Reactor Protection System described in Section 7.2.

The initiating systems for the Containment Ventilation System, the Feedwater Isolation System, and the Containment Isolation System are designed so that actuation cannot be over-ridden, and an open or failed reset switch will not impede manual operation. Key switches on the RTGB will allow the operator to override/block the Feedwater Isolation signal to the Feedwater Control Bypass valves and to the Main Feedwater pumps. The isolation signal to the Main Feedwater Control valves may be reset by these switches in conjunction with closing the Reactor Trip breakers. Placing of these key switches in the override/reset position will give an alarm on the RTGB and the keys cannot be removed when the switches are in the override/reset position. The Safety Injection Actuation System and the Containment Spray Actuation System are designed so that an open or failed reset switch will not impede manual operation. Until the start of Cycle 21 operation, the Containment Spray Actuation Signal may be manually blocked by manipulation of test switches in the auxiliary relay room. Subsequent to Refueling Outage 20, the signal may be blocked from the RTGB.

7.3.1.1.2.3 ESF instrumentation equipment

The following instrumentation ensures monitoring of the effective operation of the ESF.

1. Containment Pressure

   Eight channels, monitoring containment pressure, and derived from three pressure taps monitor the effectiveness of the containment cooling systems and other ESF. High pressure indicates high temperatures and reduced pressure indicates reduced temperatures. Indicators and alarms are provided in the Control Room to inform the operator of system status and to guide actions taken during recovery operations. Containment pressure indication will be used to distinguish between various incidents.

   Redundant containment pressure signals are provided to isolate the containment. Each of the three pairs of differential pressure transmitters external to the containment in the Auxiliary Building have their own connection to the containment. Remote indicating facilities and alarm and control signals are provided from each transmitter.

   Remote indicating facilities are provided which afford the operator the opportunity to read containment pressure.

2. Refueling Water Storage Tank Level

   Level instrumentation on the refueling water storage tank consists of three channels. One channel provides a local indication. The second channel provides remote indication (on the control board) a low level alarm, a low low level alarm, and a high level alarm. The third channel provides remote indication on the control board.

3. Emergency Core Cooling System Pumps Discharge Pressure

   These channels clearly show that the emergency core cooling system pumps are operating. The transmitters are outside the containment.

4. Pump Energization

   All pump motor power feed breakers indicate that they have closed by energizing indicating lights on the control board.

5. Radioactivity

   Means are provided to measure the radioactivity in the containment atmosphere after the incident, since this information will be required for any subsequent entry into the containment following a loss-of-coolant accident (LOCA). In the event of a major LOCA, radioactivity levels would be such that area monitors located outside the containment would respond to the activity levels inside the

containment. The containment system particulate and gaseous monitoring equipment would also provide information useful in post-accident recovery operations at pressures below 5 psig, and with favorable containment temperature and radiation conditions.

6. Valve Position

All ESF remote-operated valves have position indication on the control board to show proper positioning of the valves. Air-operated and solenoid-operated valves are selected to move in a preferred direction with the loss of air or power. SI-856A and B fail to the preferred position during normal operation but fail to the unpreferred position with a manual handwheel as backup during the recirculation mode of operation. After a loss of power to the motors, motor-operated valves remain in the same position as they were prior to the loss of power.

7. Air Coolers

The cooling water discharge flow of each of the coolers is alarmed in the Control Room if the flow is low. The transmitters are outside the reactor containment. In addition, the exit flow is monitored for radiation and alarmed in the Control Room if high radiation should occur. This is a common monitor and the faulty cooler can be located locally by manually valving each one out in turn.

8. Sump Instrumentation

The containment sump instrumentation consists of four level switches with gasketed junction boxes designed to operate in a post-accident environment. The transmitter housings are located above any possible flooding level. The indicators and alarm system are located in the Control Room.

Indicated on the reactor and turbine-generator board (RTGB) are two status lights which light when the water level in the reactor vessel cavity sump rises above 0.5 ft. The containment sump level is indicated on the RTGB from 0 to 7 ft above the containment floor in 0.5 ft increments. Two extended range (analog channels) level indicators are displayed on the core cooling and containment panel which indicate the water level from 3.5 in. above the reactor vessel cavity floor to 423.5 in.

9. Local Instrumentation

In addition to the above, the following local instrumentation is available.

a. Residual heat removal pumps discharge pressure

b. Residual heat exchanger exit temperatures

c. Containment spray test lines total flow

d. Safety injection test line pressure and flow

10. Alarms

    Visual and audible alarms are provided to call attention to abnormal conditions. The alarms are of the individual acknowledgement type; that is, the operator must recognize and silence the audible alarm for each alarm point.

11. Indication

    All transmitted signals (flow, pressure, temperature, etc.) which can cause actuation of the ESF features are either indicated or recorded for every channel.

12. RHR Pit Level Indication and Alarms

    Level indication has been provided on the RTGB to monitor water level in the RHR pits. This indication in conjunction with corresponding HI and HI-HI RHR Pit A&B Level Annunciation on APP-001 will provide operators with sufficient time to isolate any water sources to the particular RHR pump pit to preclude a common mode RHR pump failure.

7.3.1.1.2.4 Interlocks to prevent diesel generator overload during safety injection and loss of offsite power.

1. To limit the load on the diesel generators, the following circuits will trip or inhibit the start of the following loads:

a. Trip the Charging Pumps upon coincident safety injection and loss of offsite power.

b. Trip the Component Cooling Pumps upon coincident safety injection and loss of offsite power plus CV spray signal.

c. Inhibit the start of the Component Cooling Pumps upon loss of offsite power plus low CCW header pressure.

d. Inhibit the start of the Auxiliary FW pumps upon loss of offsite power plus low S/G level, loss of FW pumps, or AMSAC.

2. Pressurizer Heaters

    The 150 kW group of pressurizer heaters used to assure natural circulation at hot standby conditions are fed from redundant diesel generator buses during loss of off-site power. However, upon initiation of a safety injection signal, the pressurizer heater load will be shed to prevent overloading its DG.

3. Safety Injection Block

    During shutdown, the SG differential pressure safety injection signal is blocked during normal shutdown operation to prevent spurious safety injection due to large deviations in the SG pressure which normally occurs during plant shutdown.

7.3.1.2 Design Basis Information

The information presented in 7.2.1.2.2 is applicable. Additional design basis information is presented in 7.3.1.1, above.

7.3.1.3 Instrumentation Cable Separation

The Engineered Safety Features (ESF) System is divided into two channels with each channel run in individual cable tray systems throughout the plant. Cables from different channels are never routed through the same penetrations. These penetrations are grouped into two groups for channel 1 consisting of penetration C3, D2, C2, F1, D3, and D4 and channel 2 consisting of penetration B8, C9, C10, D8, and D9. The penetration in these two groups are separated by a horizontal distance of approximately 14 ft. Additional physical separation is provided by placing one complete channel consisting of penetration C3, D2, C2, F1, D3, and D4 on one side of a concrete wall separating this channel from channel 2 consisting of penetration B8, C9, C10, D8, and D9.

The relays and associated circuitry for the ESF are located in the upper relay room in the southwest corner of the Reactor Auxiliary Building. The initiating systems are divided into four channels physically arranged so that each channel is at the extremity of two rows of process racks.

The rack arrangements and separation criteria are the same as that provided for the Reactor Trip System cable described in Section 7.2.1.3.

7.3.1.4 Final System Drawings

Figures 7.2.1-2, 7.2.1-3, 7.2.1-5, 7.2.1-6, 7.2.1-14, and 7.2.1-17 through 7.2.1-34 are applicable.

TABLE 7.3.1-1

ACTUATION OF ENGINEERED SAFETY FEATURES
CONTAINMENT AND STEAM LINE ISOLATION
AND AUXILIARY FEEDWATER

CONTAINMENT ISOLATION ACTUATION	COINCIDENCE CIRCUITRY AND INTERLOCKS	COMMENTS
1. Phase A (Safety Injection Signal)	2/3 low pressurizer pressure, or 2/3 high containment pressure; or 2/3 high differential pressure between any steam line and steam line header; or 2/3 high steam flow in coincidence with 2/3 low T_{avg} or 2/3 low steam line pressure; or manual	Actuates all non-essential service containment isolation trip valves and actuates Isolation Valve Seal Water System
2. Phase B Containment Pressure	Coincidence of two 2/3 containment pressure (Hi-Hi pressure, same signal which actuates containment spray), or manual 2/2	Actuates all essential service containment isolation trip valves
3. High Containment Activity	High activity signal, from air particulate detector or radiogas detector. (1/2)	This additional signal closes containment purge supply, exhaust ducts and pressure relief ducts only.
ENGINEERED SAFETY FEATURES ACTUATION		
4. Safety Injection Signal (s)	See Item 1.	

TABLE 7.3.1-1 (Cont'd)

ENGINEERED SAFETY FEATURES ACTUATION	COINCIDENCE CIRCUITRY AND INTERLOCKS	COMMENTS
5. Containment Spray	Coincidence of two 2/3 containment pressure (Hi-Hi pressure); or manual 2/2	
6. Spray Additive Valves	Open on "P" signal, manual	
7. Containment Air Recirculation Cooling	Safety injection signal initiates starting of all fans in accordance with the Safety Injection starting sequence, 2/3 high containment pressure or manual 1/2	
8. Isolation Valve Seal Water	See Item 1.	
STEAM LINE ISOLATION		
9. Steam Flow	Coincidence of high steam flow in 2/3 lines and 2/3 low T_{avg} or 2/3 low steam line pressure	
10. Containment Pressure	Coincidence of two 2/3 high-high containment pressure	

TABLE 7.3.1-1 (Cont'd)

AUXILIARY FEEDWATER ACTUATION	COINCIDENCE CIRCUITRY AND INTERLOCKS	COMMENTS
11. Manual	1/1 per steam line	
12. Turbine Driven Pump	Coincidence of 2/3 low level in two steam generators; or loss of voltage on 2/2 4kV volt buses; or manual 1/2	Key switches are provided to bypass 2/3 low level in 2 steam generators.
13. Motor Driven Pumps	2/3 low level in any one SG; or trip of 2/2 main feedwater pumps; or safety injection signal; or manual 1/2	Key switches are provided to bypass 2/3 low level in any one SG.
MAIN FEEDWATER ISOLATION		
14. Close Main Feedwater Control Valves, Trip Main Feedwater Pumps, Main Feedwater Control Bypass Valves, and turbine trip.	See Item 1.	Key switch provided to bypass start of motor driven auxiliary feedwater pump when both main feedwater breakers are opened. Key switches are provided to bypass closure of main feedwater regulating bypass valves and allow starting of main feedwater pumps with Feedwater Isolation Signal present. Key switches may be momentarily placed in Override/Reset to reset the Feedwater Isolation Signal to the main feedwater regulating bypass valves and main feedwater pumps when the actuating signal has been cleared.

7.3.2 ANALYSIS

7.3.2.1 Instrumentation Used During Loss-Of-Coolant Accident

Instruments provided and designed to function following the major loss-of-coolant accident (LOCA) are those which initiate or otherwise govern the operation of ESF. Pressurizer pressure and SG flow and level sensors are located outside the missile barrier but inside the containment because an equivalent signal cannot be obtained from a sensor location more isolated from the reactor. SG pressure signals are located outside the containment.

It should be emphasized, however, that for the large LOCA, the initial suppression of the transient is independent of any detection or actuation signal. That is, the water level will be restored to the core by the passive accumulator system.

All pumps used for safety injection and initial containment spray are located outside the containment. The operation of the equipment can be verified by instrumentation that reads in the Control Room. This instrumentation will not be affected by the accident.

Depending upon the magnitude of the LOCA, information relative to the pressure of the RCS will be required to determine which pumps will be used for recirculation. The information relative to the pressure of the RCS will be required to decide if the charging pumps are required for make-up water, such as for a relatively small LOCA. Discharge pressure of the charging pumps, as read on instrumentation outside the containment, will be sufficient. In conjunction with the available accumulator instrumentation, a full range of system pressure can be determined.

The back-up for the instrumentation is the refueling water storage tank level instrumentation. Core recirculation and containment spray recirculation (if necessary) will be manually initiated, when the refueling water storage tank is empty.

Considerations have been given to all the instrumentation and information that will be necessary for the recovery time following a LOCA. Instrumentation external to the reactor containment such as radioactivity monitoring equipment will not be affected by this postulated incident, and will be available to the operator.

7.3.2.2 System Evaluation

Redundant instrumentation has been provided for all inputs to the protective systems and vital control circuits.

Where wide process variable ranges and precise control are required, both wide range and narrow range instrumentation is provided.

Instrumentation components were selected from standard commercially available products with proven operating reliability.

All electrical and electronic instrumentation required for safe and reliable operation is supplied from the vital instrumentation buses.

7.3.2.2.1 Pressurizer Pressure

Any accident condition requiring emergency core cooling would involve low pressurizer pressure. The present design for emergency core cooling is accomplished by the SIS actuation from primary system variables. Actuation is initiated by low pressurizer pressure with 2/3 logic. This coincidence arrangement will prevent false actuation of the SIS in the event of a spurious pressure signal. A safety injection block switch is provided to permit the primary system to be depressurized and its water level lowered for maintenance and refueling operation without actuation of the SIS.

This manual block switch is interlocked with pressurizer pressure in such a way that the blocking action is automatically removed above a preset pressure as operating pressure is approached. If two-out-of-three pressure signals are above this preset pressure, blocking action cannot be initiated. The block condition is annunciated in the Control Room.

7.3.2.2.2 SG Level Control During Plant Cooldown

The successful operation of the ESF involves only actuation control functions, with one exception. This exception is the SG level control function associated with plant cooldown using the auxiliary feedwater pumps. This level control system involves remote manual positioning of feedwater flow control valves in order to maintain proper SG water level. SG water level indication and controls are located in the Control Room and at a local control station.

Three sets of keylock switches (a set of switches is one each for train A and train B) are installed in the auxiliary feedwater controls for the purpose of preventing the start of the pumps and the closing of SG blowdown valves during shutdown conditions. The first set of switches block the automatic start of the motor-driven auxiliary feedwater pumps due to the SG feedwater pumps being stopped. The second set blocks the automatic start of the motor-driven auxiliary feedwater pumps due to low low level in one SG and prevents the automatic closing of the SG blowdown lines. The automatic start of the steam driven auxiliary feedwater pump due to low low level in two steam generators and the automatic closing of the SG blowdown lines is prevented by the third set of switches.

A status light for each train of the auxiliary feedwater controls is located near the auxiliary feedwater pump start switches and is illuminated when any of the bypass keyed switches addressed above are placed in the bypass position.

7.3.2.2.3 Motor and Valve Control

For starting pump and fan motors, the control relays, when deenergized, cause the closing coil on the motor starter or circuit breaker to be energized through redundant sets of contacts. When motor starters are used, the starter operating coil is supplied by power from the same source as the subject motor. When circuit breakers are used for motor control, the circuit breaker close and trip coils are supplied by power from a 125 V DC battery bus as outlined in Section 8.3.

For valve motor control, the control relay causes the coil on the main contactor for the closing circuit to be energized. The closing circuit is deenergized by either the torque switch or the position limit switch on the valve operator, thereby ensuring that the valves have closed to a leak-tight position. Air actuated containment isolation valves are spring-loaded to close upon loss of air pressure.

7.3.2.3 Function Initiation Period

The ESF instrumentation equipment inside the containment is designed to operate under the accident environment of a steam-air mixture and radiation. Environmental design is discussed in Section 3.11.

7.3.2.4 Testing and Reset Prevention

The ESF are designed so that once actuated they remain in the emergency mode upon reset or removal of the ESF actuation signal. The safety injection signal can be over-ridden after a two minute programmed delay. This override condition is indicated by status lights and annunciation in the Control Room. Until the start of Cycle 21 operation, the Containment Spray Actuation Signal may be manually blocked by manipulation of test switches in the safeguards cabinet. Subsequent to Refueling Outage 20, the signal may be blocked from the RTGB. Containment isolation valves RC-519A and RC-519B will not close in response to a Phase A containment isolation signal if the post accident sampling containment isolation override switch, located on the RTGB, is in the override position.

7.4 Systems Required For Safe Shutdown

7.4.1 Description

The Control Room Building, its equipment, and furnishings have been designed so that the likelihood of fire or other conditions which could render the Control Room inaccessible even for a short time is extremely small.

As a further measure to assure safety, provisions have been made so that plant operators can shut down and maintain the plant in a safe condition by means of controls located outside the Control Room. During such a period of Control Room inaccessibility, the reactor will be tripped and the plant maintained in the hot shutdown condition. If the period extends for a long time, the Reactor Coolant System (RCS) can be borated to maintain shutdown as Xenon decays, via the refueling water storage supply. The capability to achieve and maintain cold shutdown conditions from outside the Control Room, in the event of a fire, is also provided.

Local controls are located so that the stations to be manned and the times when attention is needed are within the capability of the plant operating crew.

Several methods of communications are available for use during execution of safe shutdown manual actions and subsequent system monitoring. If offsite power is available, the PA may be used. If offsite power is not available, then portable radios or cellular phones are credited (Note: the Cellular Phone System has a dedicated power supply). Operators will be directed to obtain an Appendix R radio during execution of some procedures.

For a description of the systems required for safe shutdown in the event of a fire, refer to Appendix 9.5.1C. For a description of the functions and systems required for safe shutdown in the event of a Station Blackout (10CFR50.63) event, refer to the Station Blackout Coping Analysis, Document Number 8S19-P-101.

The functions for which local control provisions have been made are listed below along with the type of control and its location in the plant. Transfer to these local controls is annunciated in the Control Room.

7.4.1.1 Equipment Control Outside Control Room

7.4.1.1.1 Reactor shutdown

If the Control Room should be evacuated suddenly without any action by the operators, the reactor can be tripped by either of the following:

1. Open rod control breakers at the reactor trip switchgear
2. Actuate the manual turbine trip

7.4.1.1.2 Decay heat removal

Removal of heat from the RCS during hot shutdown and cooldown to cold shutdown is accomplished using the steam generators. For the continued use of the steam generators for decay heat removal, it is necessary to provide a source of water, a means of delivering that water and, finally, instrumentation for pressure and level indication.

Feedwater may be supplied to the steam generators by the motor driven auxiliary feed pumps or by the steam-driven auxiliary feed pump. In addition to the normal feed circuit the plant may fall back on:

1. The condensate storage tanks
2. Service water
3. Onsite deep well water

7.4.1.1.3 Pressurizer pressure and level control

Following a reactor trip the primary temperature will automatically reduce to the no-load temperature condition as dictated by the steam generator temperature conditions. This reduction in the primary water temperature reduces the primary water volume and if continued pressure control is to be maintained primary water makeup is required.

The pressurizer level is controlled in normal circumstances by the Chemical and Volume Control System (CVCS). This requirement implies operation of a charging pump. In the event that all charging pumps are inoperable (as the result of a fire that causes damage to cables serving all three pumps), RCS inventory can be maintained by depressurizing the RCS and utilizing the safety injection pumps.

7.4.1.1.4 Indication and controls provided outside the control room

The specific indication and controls provided outside the Control Room for the above capability are summarized as follows:

1. Indication
   a. Level Indication for the Individual Steam Generators
      1. Motor Driven Auxiliary feed pumps room
      2. Main feed bypass control valves
      3. Turbine Building mezzanine dedicated shutdown (DS) panel
      4. Charging pump room DS panel

   b. Pressure Indication For the Individual Steam Generators
      1. Turbine Building mezzanine DS panel

c. Pressurizer Level and Pressure Indicators

1. Motor Driven Auxiliary feed pumps room (level only)
2. Turbine Building mezzanine DS panel
3. Charging pump room DS panel

d. Wide range RCS Loop "A" T_H and T_C Instrumentation

1. Turbine Building mezzanine DS panel
2. Charging pump room DS panel

e. Nuclear Instrumentation

1. Charging pump room DS panel (meter only)

2. Controls

Local stop/start motor controls are provided at each of the following motors:

a. Motor-Driven Auxiliary Feedwater Pumps

b. Charging Pumps

c. Boric Acid Transfer Pumps (The Boric Acid Transfer Pumps controls function may be satisfied by the Charging Pumps controls and Refueling Water Storage Tank level functions as identified in Table 9.5.1C-2)

d. Component Cooling Water (CCW) Pump A for the DS system (at the charging pump room DS panel)

e. Service Water Pump D for the DS system (at the charging pump room DS panel)

The selector switch will transfer control of the switchgear from the Control Room to local at the motor, or remote panel. Placing the local selector switch in the local operating position will give an annunciator alarm on the Control Room panel.

Remote stop/start motor controls are provided for each of the following motors:

a. Service Water Pumps

b. Containment Air Recirculation Fans

These controls are grouped at two points. Service Water Pumps A and B and Containment Air Recirculation Fans HVH-1 and 2 in the emergency switchgear room convenient for operation. Service Water Pumps C and D and Containment Air Recirculation Fans HVH-3 and 4 in the Rod Drive Room convenient for operation. The selector switch will transfer control of the switchgear from the Control Room to the remote point. Placing the selector switch to local operation will give an annunciator alarm in the Control Room and will turn out the motor control position lights on the Control Room panel.

Alternate motor control points are not required for the following:

a. Component Cooling Water Pumps B and C. (Automatically restarted on a loss of offsite power once the diesel generators are operating.)

b. Instrument Air Compressors and Cooling Pumps. (These will start automatically on low pressures in the air and water services, once the diesel automatically energizes the bus, and the motor control centers are manually energized. Instrument Air Compressors must be reset and restarted upon reenergizing motor control centers. The control point is local to the compressors.)

3. Speed Control

Speed control is provided locally for:

a. The Steam-Driven Auxiliary Feed Pump

b. The Charging Pumps

4. Valve Control

Valve control is provided locally for:

a. Main Feed Regulators

b. Main Feed Bypass Regulators

c. Auxiliary Feed Control Valves. (These valves are located local to the auxiliary feed pumps and turbine building mezzanine DS panel)

d. Steam generator power operated relief valves

e. All other valves requiring operation during hot shutdown can be locally operated at the valve

f. Letdown orifice isolation valves (local to the charging pumps); local control and selector switches and position indicating lamps are provided

5. Pressurizer Heater Control

Stop and start buttons with selector switch and position lamp are located in the Rod Drive Room adjacent to containment for two backup heater groups. For heater group capacity, refer to UFSAR Section 5.4.6.

6. Lighting

Emergency lighting is provided in operating areas described above (as required to support post-fire shutdown operation), as well as in access and egress paths to those areas.

7.4.1.2 Safe Shutdown System Improvement Modifications

Major modifications were made to improve the alternative shutdown system ability to withstand common mode failures and particularly fires, as described below.

In the original plant configuration, fires occurring in some areas could impair the use of any or all of this equipment, primarily through destruction of power and control cables. Consequently, provisions have been made for the transfer of power and/or the control of select components to alternate sources to mitigate the consequences of a severe fire in these critical plant areas (e.g., Control Room, cable spreading room, emergency switchgear room, or battery room or Auxiliary Building Hallway first floor).

Plant modifications have been implemented to provide alternative and dedicated shutdown features as required to support the post-fire shutdown modes described in Section 7.4.1.3.

7.4.1.2.1 Steam-Driven Feedwater Pump Shutoff Valves

A transfer switch panel located in the Auxiliary Building enables the transfer of control for the steam-driven feedwater pump shutoff valves V1-8A and V2-14A from the existing remote control signals to local control at the turbine building mezzanine DS panel. The modification does not change the existing control voltage or power source alignment with the valves. The transfer to local control is annunciated in the Control Room.

7.4.1.2.2 Steam Generator Power-Operated Relief Valves

The turbine deck control panel also provides for disabling the existing remote control of steam generator power-operated relief valves RV1-1, RV1-2, and RV1-3. When transferred to local control, the valves can be operated by using the valve controllers in the turbine building mezzanine DS panel. The transfer to local control is annunciated in the Control Room.

7.4.1.2.3 Component Cooling Pump A Control Transfer

A transfer switch is provided on the charging pump room control panel to disable the existing remote control of component cooling pump A and to transfer control of the pump to a local switch on the panel. The transfer to local control is annunciated in the main Control Room. The pump power and control source is normally from 480V Bus DS.

7.4.1.2.4 Alternate Power Source for Service Water Pump D

The normal supply for service water pump (SWP) "D" is 480V Bus E2, with control from the plant Control Room. To provide a power supply and controls independent of the critical fire areas, an alternate supply has been installed via the DS Bus. When properly aligned, these breakers provide an alternate power supply and control station for SWP "D". The breakers are provided with a key interlock to prevent the simultaneous closure of both breakers.

Service water header isolation valve V6-12D, isolates SWP "D" from its associated service water header, and is powered via an administratively controlled breaker and a local switch. The valve is normally powered from MCC-6 but administrative controls allow alternative operation from MCC-5. Power train isolation is maintained by administrative control of the MCC breakers, and valve operation is available from the dedicated shutdown bus.

7.4.1.2.5 Charging Pump A

Alternate controls, independent of the critical fire areas, have been provided for charging pump A. The normal power supply for this pump (480V bus DS) is outside the emergency switchgear room.

The alternate controls for charging pump A, consisting of a control transfer switch and control switch, are located on the charging pump room control panel.

7.4.1.2.6 Alternate Power Supply for MCC-5

The normal power supply for MCC-5 is 480V Bus El. To provide a power supply independent of the emergency switchgear room, key-interlocked manual circuit breakers 3 and 4 have been installed; by manually realigning these circuit breakers, MCC-5 is supplied from 480V Bus DS, which is independent of the emergency switchgear, control, cable spreading, and battery rooms.

7.4.1.2.7 Dedicated Shutdown (DS) Instrumentation

The DS instrumentation provides the following local displays at the charging pump room DS panel:

a) Wide range RCS Loop 'A' hot and cold leg temperatures
b) Nuclear instrumentation
c) Steam generator 1 wide range level
d) Steam generator 2 wide range level
e) Steam generator 3 wide range level
f) Pressurizer level
g) Pressurizer pressure

With the exception of the nuclear instrumentation, duplicate shutdown instrumentation displays are provided at the turbine building mezzanine DS panel. In addition, the condensate storage tank level is displayed at the turbine building mezzanine DS panel.

7.4.1.2.8 Separation of Power and Control Cables

All new components that provide alternate power or control capabilities for the DS system have been located so that alternate power sources or control stations will not be affected by any fire that could damage the normal shutdown systems. In addition, all conduits and cable for the DS systems have been routed through areas that will not be affected by fires that could damage systems normally required for shutdown.

All new dedicated shutdown cable has been installed in rigid steel conduit routed through areas remote from cables presently used for the normal shutdown systems. Where this level of separation was not achievable, selective installation of rated fire-protective cable wraps and related protective measures (e.g., fire suppression systems) have been implemented.

7.4.1.3 Alternative and Dedicated Shutdown Capability

Duke Energy Progress, LLC has performed and documented a comprehensive analysis of the separation between redundant safe-shutdown components and cables in the context of post-fire shutdown system separation requirements defined by 10CFR50, Appendix R, Section III.G (Reference 7.4.1-1). The analysis considered the effects of fire on plant equipment and identified methods of achieving a stable cold shutdown condition from normal plant power operation.

Refer to Appendix 9.5.1C for a description of this analysis and the basis for establishment of alternative and dedicated post-fire shutdown capabilities.

Procedures have been established for achieving safe shutdown by using a combination of alternative equipment, depending upon the fire location.

7.4.2 Analysis

7.4.2.1 Compliance With Applicable Codes and Standards

The engineered safety feature systems were designed in accordance with the applicable General Design Criteria (GDC) effective in 1968. The reactor protection system was also designed in accordance with applicable GDC and IEEE 279, "Proposed Criteria for Nuclear Power Plant Protection Systems," August, 1968. No regulatory guides were available for incorporation into the original design criteria for the engineered safety features.

The alternative/dedicated shutdown system modifications do not impact the physical integrity of the auxiliary shutdown system components. The only penetrations into the existing system pressure boundary were for the installation of new impulse lines for new DS system instrumentation. The modification did not impact the system process and the auxiliary shutdown system will continue to meet all of the original mechanical and operational design criteria.

The post-fire safe-shutdown modifications provide for:

1. Separation of Redundant Circuits. Where safety-related circuits have been modified, new wiring and components have been installed so that, as a minimum, the design is in compliance with the intent of the separation criteria defined by Regulatory Guide 1.75. The basis for the modifications (fire hazards analysis) dictated that power and control wiring for selected components (e.g., one charging pump, one service water pump or CCW pump) be rerouted so that cables serving redundant pumps would either not pass through common fire areas or would be run in dedicated conduit or be fire-wrapped.

2. Fault Isolation for Safety-Related Circuits and Power Supplies. Electrical isolation, consistent with those of the existing plant designs and with the requirements of IEEE-279 and IEEE-384-1977, is provided to ensure that external faults (fire-induced) will not degrade existing or new safety-related electrical systems.

3. Separation of Safety and Non-Safety Related Circuits. Isolation devices and/or physical separation are provided to ensure that failures in non-safety related circuits will not jeopardize adjacent safety-related circuits.

4. Annunciation in Main Control Room for Bypass or Assumption of Local Control of major components. For those components provided with a "control transfer" features, auxiliary contacts on each control transfer switch are used to provide annunciation (in the Control Room) when the component is switched out of its "remote control" mode.

   This annunciation feature has been implemented for all auxiliary shutdown components having remote/local control capabilities.

5. Interlocks and Administrative Controls to Limit the Consequence of Faulted Conditions. Features such as key interlocks or racking out of selected circuit breakers prevent the inadvertent cross-connection or simultaneous faulting of redundant power supplies.

6. Seismic Installation in Safety-Related Areas or Safety-Related Cabinets. Interfaces with existing safety-related cabinets and new safety-related cabinets (e.g., charging pump room panel, transfer switch panels) and their included components have been designed to remain functional through a safe shutdown earthquake (SSE).

7. Single-Failure Criterion. All new safety-related components and safety-related interfaces are designed so that a single failure cannot cause the loss of redundant safety systems. The modifications generally affect only one of redundant equipment trains. The failure of one of these equipment trains will not initiate the failure of the redundant train; electrical and physical separation of the redundant trains have not been degraded as a result of the modification.

7.4.2.2 Control and Power Circuit Separation

In conducting the fire hazard analysis, it was determined that several plant fire areas were critical in that cables for redundant shutdown-related components were routed through these areas. As a result, a severe fire in one of these areas could incapacitate redundant equipment trains by destroying power and control cables, or by destroying power supplies.

In order to mitigate the consequences of a fire in any one of the plant fire areas, power and control cables for selected shutdown-related components were rerouted to avoid these areas or routed in conduit or fire-wrapped. The alternate power sources and local control panels and the device itself are independent of the areas of concern or a means of manual or remote operation has been provided.

7.4.2.3 Operating Requirements

7.4.2.3.1 Operators

Sufficient qualified operators will be available to conduct shutdown activities, whether from the control room or following a control room evacuation. Operator staffing is adequate for implementation of post-fire shutdown procedures in the event of a fire in any plant fire area.

7.4.2.3.2 Equipment adequacy

The functions required for post-fire shutdown are equivalent to those functions that must be maintained, as a minimum, in a safe-shutdown scenario that does not involve accident mitigation functions. The specific equipment credited to perform these functions, and the adequacy of the equipment to fulfill the necessary operational objectives are discussed in Appendix 9.5.1C.

7.4.2.4 Analyses Affecting Equipment Controlled Outside the Control Room.

7.4.2.4.1 Reactor Shutdown

When the reactor is held at hot shutdown conditions, boration of the Plant is not required immediately after shutdown. The Xenon transient does not decay to the equilibrium level until some 10 to 15 hours after shutdown, and a further period would elapse before the 1 percent reactivity shutdown margin provided by the full length control rods had been canceled. This delay would provide time for useful emergency measures.

7.4.2.4.2 Decay Heat Removal.

Failure to maintain water supply to the steam generators following a normal plant shutdown would result in steam generator dry out after some 400 seconds and loss of the secondary system for decay heat removal. Independently controlled relief valves on each steam generator maintain the steam pressure. These relief valves are further backed up by coded safety valves on each steam generator. Numerous calculations, verified by startup tests on the Connecticut-Yankee and San Onofre Power Plants, have shown that with the steam generator safety valves operating alone, the RCS maintains itself close to the nominal no-load condition. The steam relief facility is adequately protected by redundancy and local protection.

7.4.2.4.3 Service Water.

For operation of only one Service Water Pump, SWP "D", fed from the DS system, hydraulic analyses have shown that SWP "D" will provide adequate service water for cooling without experiencing run out.

7.4.2.4.4 Auxiliary Feedwater Flow.

For operation of a single Auxiliary Feedwater (AFW) pump, analyses have shown that an AFW flow as low as 240 gpm will support cooling the RCS. This flow rate is within the capability of a single AFW pump.

INTENTIONALLY LEFT BLANK

REFERENCES: SECTION 7.4

7.4.1-1 Safe Shutdown Component/Cable Separation Analysis [10CFR50, Appendix R, Section III.G] for H. B. Robinson Unit 2.

7.4.1-2 "Station Blackout Coping Analysis Report," H. B. Robinson, Unit 2, Document No. 8S19-P-101.

7.4.1-3 Letter NO-81-1524, dated September 16, 1981, CP&L to NRC, "Emergency Procedures and Training for Station Blackout Events."

7.4.1-4 Letter NLS-89-045, dated March 3, 1989, CP&L to NRC, "Response to Station Blackout Rule (TAC 68595)."

7.4.1-5 Letter NLS-90-071, dated March 30, 1990, CP&L to NRC, "Supplemental Response to Station Blackout Rule."

7.4.1-6 Letter NLS-91-273, dated October 21, 1991, CP&L to NRC, "Response to NRC Supplemental Safety Evaluation of the Response to the Station Blackout Rule (NRC TAC No. 68595)."

7.4.1-7 Letter NLS-91-069, dated March 13, 1991, CP&L to NRC, "Response to NRC Station Blackout Safety Evaluation (NRC TAC No. 68595)."

INTENTIONALLY LEFT BLANK

7.5 SAFETY-RELATED DISPLAY INSTRUMENTATION

7.5.1 DESCRIPTION

The design of a centralized Reactor-Turbine Generator Control Board (RTGB) incorporates the arrangement of controls and information instrumentation for the safe operation of both the Nuclear Steam System and conventional plant equipment in such a manner as to effectively reduce the amount of board area that the control operator needs to keep under his surveillance, and to provide quick access to controls. Control stations on the board are packaged in a modular concept and are grouped according to function to minimize the possibility of operator error due to juxtaposition of unrelated control functions. Control stations with both automatic and manual positions are provided with "bumpless" transfer of function.

Instrumentation, trend recorders, and annunciator panels are incorporated in the vertical section of the RTGB to keep the operator informed on process flows, pressure, temperatures, etc., as well as alarms for out-of-limit points requiring operator action. The console section contains control devices (switches and control stations) and related indicating lights.

The general layout of the Control Room and the RTGB is shown in Figure 9.5.1-3. Section "A" contains control and instrumentation for Nuclear Steam Supply Systems. The left portion contains components less frequently used (e.g., for startup, shutdown, or less frequent surveillance).

The center portion contains control and instrumentation for Engineered Safety Features Systems. Redundant indicators are provided where required for high reliability. Monitoring lights provide a means of quickly evaluating the status of components in these systems should they be actuated. Controls and indicators for backup or redundant components are located on separate modules.

The right portion of Section "A" (adjacent to Section "B") contains those components more frequently used during normal plant operation. This includes pressurizer level control and reactor makeup control, as well as related indicators and recorders.

Section "B" contains rod control system and nuclear instrumentation system control and instrumentation. This includes a position indicator and rod bottom limit light manually controlled at the console. All nuclear instrumentation information required to operate the reactor is displayed here. Some of the reactor makeup system control devices are also included on the left portion of this section.

Sections "C" and "D" contain instrumentation and controls for secondary plant functions including feedwater and condensate systems, heater vent and drain systems, electrical systems, heating, ventilating, and air conditioning systems (except containment air recirculation system which appears in engineered safeguards portion of Section "A").

7.5.1.1 Pressurizer Power Operated Relief Valve Position Indication

A visual indication of the position of the pressurizer power operated relief valve and an audible alarm are provided in the Control Room to alert the operator should the valve open. The position indication system is a direct position indication system which employs limit switches actuated by the valve stem as a sensor for valve position. This system is part of the original design of the H. B. Robinson Plant and does not qualify as "safety grade" in the strictest sense of current standards; however, it does satisfy the short-term lessons learned requirements in that it is a reliable, single channel, direct indication powered from a vital instrument bus. In addition, this system is backed up by indirect means of determining valve position such as temperature and pressure downstream of the valves.

An acoustic system, which senses flow through the pressurizer Safety Relief Valves, has been installed. This newly installed position indication system provides the capability to continuously and automatically detect acoustic signals generated by flow through the valves. These signals are transmitted to an instrument panel mounted in the Cable Spreading Room where the system compares the current noise level to a quiescent level determined during calibration. When the quiescent level is exceeded by a predetermined amount, visual indication and an audible alarm informs the operator that the valve is open.

7.5.1.1.1 Control Stations Layout, Information Display, and Recording

The principal criterion of control station design and layout is that all controls, instrumentation displays and alarms required for the safe operation and shutdown of the plant are readily available to the operators in the Control Room.

The Control Room (Figure 9.5.1-3) is located as an integral part of the HBR-2.
The Control Room is approximately 40 ft x 40 ft.

7.5.1.1.2 Computer System

This section deleted. This equipment has been replaced by the ERFIS system, which is described in Section 7.7.1.8.

7.5.1.1.3 Local Control Panels

Local control panels are provided for certain systems and components which do not require full time operator attendance or are not used on a continuous basis. Such systems are the Waste Disposal System, Sampling System, Boron Recycle System, and the Turbine-Generator Hydrogen Cooling System. In these cases, however, appropriate alarms are located in the Control Room and are activated to alert the operators of equipment malfunction or approach to unsafe conditions.

The waste disposal control board is located in the Reactor Auxiliary Building, in the vicinity of the boric acid and waste evaporators. This board permits the auxiliary operator to control and monitor the processing of wastes from a central location in the general area where equipment is located. Alarm signals from waste disposal components annunciate on this board. Actuation of any alarm on this panel actuates a general "Waste Disposal" alarm on the RTGB. In this manner, the control operator can maintain general surveillance over the system from the Control Room, and can dispatch an operator to the waste disposal board, if necessary.

Although the waste disposal control board provides the instrumentation required to control the release of wastes, instrumentation provided to monitor activity release is indicated and/or alarmed in the Control Room. The auxiliary operator has complete knowledge of permissible discharge rates and quantities before any scheduled release is made, and the waste disposal board permits him to control those parameters. By monitoring activity release from the Control Room, the control operator maintains surveillance.

7.5.1.1.3.1 Technical Support Center (TSC)

The TSC provides a location to house individuals who are knowledgeable of and responsible for engineering and management support or reactor operations following an event. The plant operators and operating staff are responsible for the safe operation of the plant, and for the initial action to minimize the consequences of the event. The TSC supports the operating staff with access to up-to-date plant records of the plant configuration. Plant design/operation information are available in the form of drawings, FSAR, Technical Specifications and visual display of parameters. In addition, direct communications with the Control Room is provided which allows the TSC personnel to assess the status of the plant and stay abreast of the plant parameters. With this information, the TSC staff can provide short and long term technical advice and support during and after an event.

7.5.2 ANALYSIS

7.5.2.1 Control Room Environment

The safety-related electrical equipment is designed to operate and perform its design function within specified safe limits without degradation of performance (accuracy, repeatability, time response) under the expected normal and abnormal ambient conditions associated with its location. The normal ambient design temperature is 75°F (plus or minus 10°F) for Control Room located equipment. The abnormal ambient condition associated with the design of Control Room located safety equipment is 120°F for short term operation associated with a loss of air conditioning. Safety-related electrical equipment in other than the Control Room, such as the cable spread room, electrical equipment room and the cable vault is designed to operate under the worst case environment for which it is required to perform its function.

Provision for air conditioning has been made by supplying the two redundant Control Room air conditioners from separate emergency diesel power supplies. Thus, interrupted stay time or equipment malfunction due to loss of air conditioning is considered to be highly unlikely.

7.5.2.2 Instrumentation Power Supplies

The instrumentation is designed into four channels and each channel is powered by its respective instrument bus. Table 8.3.1-2 gives information about these power supplies. The instruments feed into the two trains of Reactor Protection and Engineered Safeguards which are powered by DC from the "A" and "B" Station Batteries to the respective trains. The loss of one of the instrument buses should not result in a reactor trip. In the event of a loss of an instrument bus, there remains adequate indication and protection in service from the remaining channels such that the safety of the plant is not jeopardized. From instrument status lights panels on the RTGB, the operator would be aware of which bus was lost and could have it manually switched to its back-up supply.

The four instrument channel status lights are in horizontal rows, with each row indicating in a different color corresponding to a different bus. The instrument status lights each indicate the existence of a specific alarm condition for an instrument on the bus. The loss of an instrument bus would result in illumination of the status lights for those bistables that are "de-energize to actuate" and that receive control power from the de-energized Instrument Bus.

Power to the status light modules is supplied by two instrument buses to preclude the loss of all lights due to a loss of power. The module on the Section "A" (Safeguards) portion of the RTGB is powered by Instrument Bus 3 and the modules on the Section "B" (Reactor Protection) portion of the RTGB are powered by Instrument Bus 1.

7.6 All Other Instrumentation Required For Safety

7.6.1 Reactor Overpressure Protection

As discussed in Section 5.2.2, the pressurizer power operated relief valves (PORV) are utilized to protect against exceeding safe pressure limits under low temperature conditions. The logic diagram for the instrumentation which controls the PORV opening is shown in Figure 7.2.1-35, and the PORV nitrogen supply is shown in Figure 7.6.1-2. Each PORV is opened by nitrogen, with a nitrogen accumulator and instrument air as backups. A separate nitrogen accumulator is provided for each PORV, capable of achieving 100 valve operating cycles.

The instrumentation system uses temperature and pressure inputs. Wide range temperature signals from all three loops provide inputs to a low-auctioneer device. The low-auctioneer selects the lowest temperature to ensure using the most conservative measure for the Appendix G curve. The lowest loop temperature is then utilized as input to a function generator. The function generator shapes the linear input signal into an output signal conforming to the slope of the plant's Appendix G curve. The specially shaped output from the signal generator is utilized for comparison with a plant wide-range pressure signal via a signal comparator. One wide-range pressure transmitter is provided for each control channel.

When the setpoint of the comparator is exceeded, the comparator's output activates a relay whose contacts activate the primary PORV solenoid and an annunciator in the Control Room to signal the condition.

A manual permissive switch is utilized to arm the overpressure protection channel when the plant is below 350ºF and capable of a solid water condition (no steam bubble in the pressurizer). A non-redundant temperature comparator will provide an annunciator signal when the loop temperature drops below 350ºF.

During normal plant operation, the permissive switch is not armed and the PORV are not operable in the low temperature/overpressure mode. With the system not armed, a reduction in temperature below 350ºF (normal cooldown procedures or abnormal conditions) would cause the annunciator to energize signaling the operator to arm the overpressure protection system via the permissive switch. Redundancy for the arming function is provided by the plant operating procedures which will require arming the system before the temperature drops below 350ºF. When armed, the PORV become operable. Exceeding the setpoint with the system armed causes the PORV to open. The annunciator will not light under normal conditions if the system was armed prior to the temperature dropping below 350ºF. With the system armed below 350ºF, the next energizing of the annunciator indicates the setpoint has been exceeded and the PORV will open.

Additional information on the system is presented in References 7.6.1-1 through 7.6.1-5.

7.6.2 CONTAINMENT AIR RECIRCULATION SYSTEM

The containment air recirculation system is used to cool the following equipment: control rod drive mechanism (CRDM), reactor vessel supports, out-of-core nuclear instrumentation, and any other safety related equipment cooled by this system.

Loss of cooling air can result from loss of fan, malfunctioning of dampers, or loss of cooled air supply from fan coolers.

The following instrumentation is provided for the systems to provide annunciation and remedial action in case of "loss of fan" or "malfunctioning of dampers":

a) CRDM Cooling System: On/off switch with indicating lights on Reactor Turbine Generator Board for each fan, and one air flow switch in the discharge duct of each fan (HVH-5A and HVH-5B).

b) Reactor Vessel Support Cooling System: On/off switch with indicating lights on Reactor Turbine Generator Board for each fan, and one air flow switch in the suction duct of each fan (HVE-6A and HVE-6B).

c) Concrete Shield Cooling System: On/off switch with indicating lights on Reactor Turbine Generator Board for each fan, and one air flow switch in the discharge duct of each fan (HVH-9A and HVH-9B).

The air flow switches in these systems shall start standby fan operation, annunciate "Low Flow" and sound alarm on the Reactor Turbine Generator Board in the Control Room.

Loss of cooling air from any one of the four reactor containment fan coolers is annunciated on the Reactor Turbine Generator Board as well. This annunciation is actuated by air flow switches in the discharge duct of each reactor containment fan cooler unit.

The CRDM require cooling to keep the coils in these mechanisms from gradually degrading. Above 400ºF, the insulation life is shortened. A short in the coil may develop in 10-12 hr. This causes a full length rod to insert by gravity. This failure mode is acceptable.

The Nuclear Instrumentation System (NIS) operation at elevated temperatures is limited by the field cables to the detectors. The detectors themselves can operate at temperatures in the range of 300ºF. The field cable is susceptible to insulation softening above about 175ºF; however, this is a gradual process and not a catastrophic event. To provide adequate margin, the temperature specified for the continuous operation of the NIS is 135ºF. The detector assemblies can operate at 175ºF for eight hours after loss of cooling. Degradation of cable insulation would be apparent by abnormal channel operation and would be verified by insulation resistance (megger) tests.

In the unlikely event that cooling is lost to the reactor vessel supports, the maximum rate of temperature rise is expected to be 15ºF/hr which provides the operator with ample time to reestablish cooling.

REFERENCES: SECTION 7.6

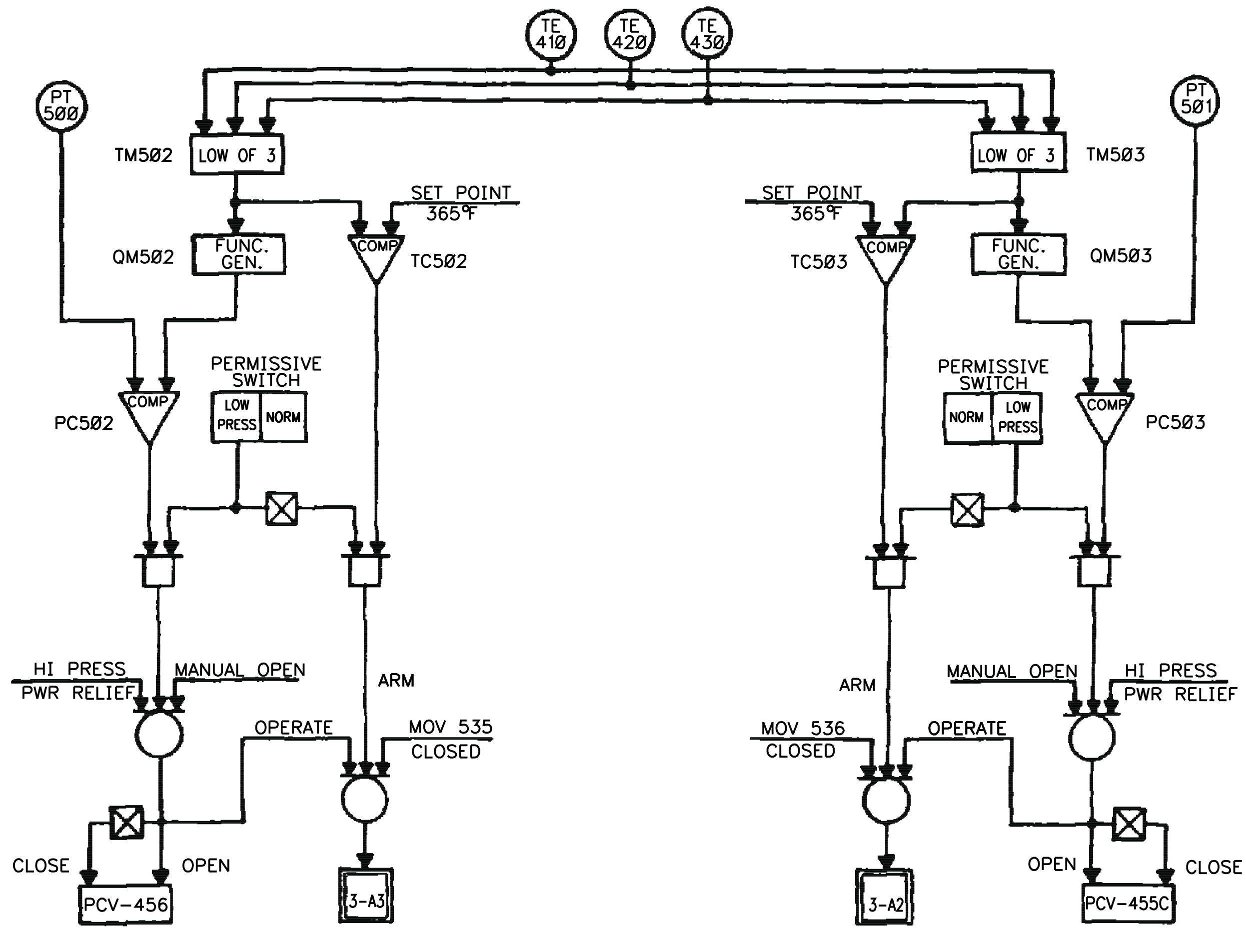
7.6.1-1 Letter, Ser. No. NG-77-1215, dated October 31, 1977, from CP&L (Furr) to NRC (Reid), subj: H. B. Robinson Steam Electric Plant, Unit 2, Lic. No. DPR-23, Reactor Vessel Overpressurization Protection (w/encls: Paper, "Functional Description of Overpressure Protection System Electrical Components" (2 pp.), with Drawings on Logic Diagram (2 pp.) and Paper, "Reactor Coolant System Overpressure Mechanical Modification Description" (2 pp.), with Drawing on H. B. Robinson Unit 2 Overpressure Protection Nitrogen Supply. (1 p.)

7.6.1-2 Letter, File No. RC/A-2, No Ser. No., dated December 22, 1977, from CP&L (Utley) to NRC (Reid), subj: H. B. Robinson Steam Electric Plant, Unit 2, Docket Lic. No. DPR-23, Overpressure Protection Wiring Diagram.

7.6.1-3 Letter, Ser. No. GD-78-231, dated January 25, 1978, from CP&L (Utley) to NRC (Reid), subj: H. B. Robinson Steam Electric Plant, Unit 2, Docket No. 50-261, Lic. No. DPR-23, Reactor Vessel Overpressure Protection Request for License Amendment, w/encl: Drawing on Logic Diagram for Overpressure Protection. (Rev. 1-3-78, 3 pp.)

7.6.1-4 Letter, Ser. No. GD-78-586, dated February 28, 1978, from CP&L (Utley) to NRC (Schwencer), subj: H. B. Robinson Steam Electric Plant, Unit 2, Docket No. 50-261, Lic. No. DPR-23, Overpressure Protection System, w/encl: Drawing on Logic Diagram for Overpressure Protection. (Rev. 2-15-78, 1 p.)

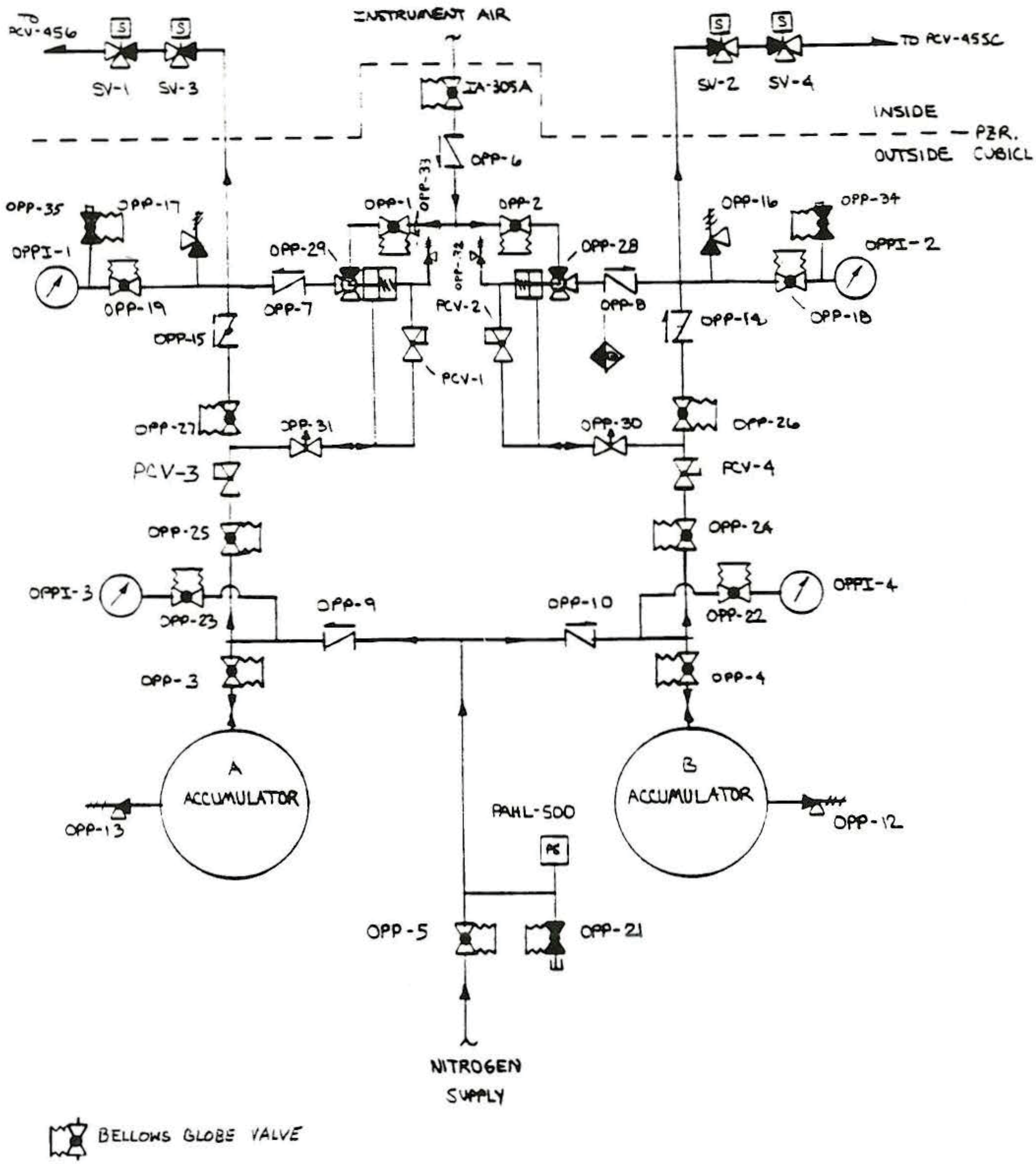
7.6.1-5 Letter, Ser. No. GD-78-1374, dated May 10, 1978, from CP&L (Utley) to NRC (Schwencer), re H. B. Robinson Steam Electric Plant, Unit 2, Docket No. 50-261, Lic. No. DPR-23, Response to Overpressure Protection Questions, w/encls: Paper, Request for Additional Information, dated April 3, 1978, and attachments, Drawings 418-3 (Rev. 1, 1 p.); 418-5 (Rev. 1, 2 pp); 418-9 (Rev. 1, 1 p.), all dated 2-15-78.



H. B. ROBINSON
UNIT 2
CAROLINA POWER & LIGHT COMPANY
UPDATED FINAL SAFETY ANALYSIS REPORT

LOGIC DIAGRAM
FOR OVERPRESSURE PROTECTION

FIGURE 7.6.1-1 REVISION No. 25



Amendment No. 7

H.B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	**NITROGEN SUPPLY FOR PORV**	FIGURE 7.6.1 - 2

7.7 CONTROL SYSTEMS NOT REQUIRED FOR SAFETY

7.7.1 DESCRIPTION

The systems discussed below include the control systems which control the rod cluster control assemblies (RCCA), pressurizer level and pressure, steam dump, and the feedwater to the steam generators. Also, the incore instrumentation, core power distribution control, and core subcooled monitor are described.

The reactor automatic control systems are designed to constrain nuclear plant transients for the designed load perturbations, so that reactor trips will not occur for these load changes.

The Reactor Control System is designed to enable the reactor to follow load reductions automatically when the plant output is above 15 percent of nominal power. Control rod positioning may be performed automatically (Rod insertion only) when plant output is above this value, and manually at any time.

The automatic rod control system is designed to restore programmed average temperature following a step reduction in load of 10 percent or a ramp reduction of 5 percent per minute within the range of 15 to 100 percent power. However, under nominal operating conditions, the control system allows the plant to accept step load reductions of 19 percent and ramp load reductions of 14 percent per minute over the load range of 15 to 95 percent power. The turbine bypass system, in combination with the reactor coolant system, permits the plant to accept approximately a 60 percent loss of electrical load without reactor or turbine trip.

The control system is capable of restoring coolant average temperature to within the programmed temperature deadband following a scheduled or transient change in load.

The pressurizer water level is programmed to be a function of the average coolant temperature. This is to minimize the requirements on the Chemical and Volume Control and Waste Disposal System resulting from coolant density changes during loading and unloading from full power to zero power.

Following a reactor and turbine trip, sensible heat stored in the reactor coolant is removed without actuating the steam generator safety valves by means of controlled steam bypass to the condenser and by injection of feedwater to the steam generators. Reactor coolant system (RCS) temperature is reduced to the no load condition. This no load coolant temperature is maintained by steam bypass to the condensers, which removes residual heat.

The control system is designed to operate as a stable system over the full range of automatic control throughout core life without requiring operator adjustment of setpoints other than the normal calibration procedures.

7.7.1.1 Rod Control System

The Rod Control System includes the following:

a) Rod Drive Programmer

b) Rod Position Indication

1) Individual

2) Group

7.7.1.1.1 Rod Control

There are 45 full length RCCA which are divided into a shutdown group comprising two shutdown banks of 8 rod clusters each, and a control group comprising 4 control banks containing 8, 8, 8, and 5 rod clusters. Figure 4.3.2-5 shows the location of the rods in the core. The four banks of the control group are the only rods that can be manipulated under automatic control. The banks are divided into subgroups to obtain smaller incremental reactivity changes. All RCCA in a subgroup are electrically paralleled to step simultaneously. Position indication for each RCCA type is the same.

7.7.1.1.1.1 Control Group Rod Control

The automatic rod control system maintains the average coolant temperature by adjusting the RCCA positions. The Reactor Control System is capable of restoring programmed average temperature following a load reduction. The coolant average temperature increases linearly from zero power to full power.

The control system will also initially compensate for reactivity changes caused by fuel depletion and/or xenon transients. Final compensation for these two effects is made by adjusting the boron concentration. The control system then readjusts the control group rod in response to changes in coolant average temperature resulting from changes in boron concentration.

The function of the Reactor Control System is to provide automatic control of the RCCA during power operation of the reactor. The system uses input signals of coolant temperature and plant turbine load. The Chemical and Volume Control System (CVCS) supplements the reactor control system by the addition and removal of varying amounts of boric acid solution.

A block diagram of the Reactor Control System is shown in Figure 7.7.1-1. Figure 7.7.1-2 shows in more detail the T_{avg} Control System. As it shows, the coolant temperatures are measured by the hot leg and the cold leg Resistance Temperature Detectors. There is one average temperature per loop. The median of three measured average temperatures is the main control signal. This signal is sent to the control group rod programmer through a lead/lag compensation unit. The control group rod programmer commands the direction and speed of control group rod motion.

The RCCA are divided into several main banks, and each bank into several subgroups, to follow load changes over the full range of power operation. Each subgroup in a bank is driven by the same variable speed rod drive control unit which moves the subgroups sequentially one step at a time. The sequence of motion is reversible; that is, a withdrawal sequence is the reverse of the insertion sequence. The variable speed sequential rod control affords the ability to insert a small amount of reactivity at low speed to accomplish fine control of reactor coolant average temperature about a small temperature deadband.

Manual control is provided to move a control bank in or out at a preselected fixed speed.

Proper sequencing of the RCCA is assured by fixed programming equipment in the Rod Control System, and through administrative control of the reactor plant operator. Startup of the plant is accomplished by first manually withdrawing the shutdown rods to the full out position. This action requires that the operator select the SHUTDOWN BANK position on a control board mounted selector switch and then position the IN-HOLD-OUT lever (which is spring return to the HOLD position) to the OUT position.

Additional RCCA are then withdrawn under manual control of the operator by first selecting the MANUAL position on the control board mounted selector switch and then positioning the IN-HOLD-OUT level to the OUT position. In the MANUAL selector switch position, the rods are withdrawn (or inserted) in a predetermined programmed sequence by the automatic programming equipment.

When the reactor power reaches approximately 15 percent, the operator may select the AUTOMATIC position, where the IN-HOLD-OUT lever is out of service, and rod motion is controlled by the Reactor Control and Protection Systems. A permissive interlock limits automatic control to reactor power levels above 15 percent. In the AUTOMATIC position, the rods are again withdrawn (or inserted) in a predetermined programmed sequence by the automatic programming equipment.

Programming is set so that as the first bank out (control bank C-2) reaches a preset position near the top of the core, the second bank out (control bank C-3) begins to move out simultaneously with the first bank. When control bank C-2 reaches the top of the core, it stops, and control bank C-3 continues until it reaches a preset position near the top of the core where the control bank C-4 motion begins. This withdrawal sequence continues until the plant reaches the desired power level. The programmed insertion sequence is the opposite of the withdrawal sequence, i.e., the last control bank out is the first control bank in.

With the simplicity of the rod program, the minimal amount of operator selection, and two separate direct position indications available to the operator, there is very little possibility that rearrangement of the control rod sequencing could be made.

7.7.1.1.1.2 Shutdown Groups Control

The shutdown groups of control rods together with the control groups are capable of shutting the reactor down. They are used in conjunction with the adjustment of chemical shim and the control groups to provide shutdown margin of at least one percent following reactor trip with the most reactive control rod in the fully withdrawn position for all normal operating conditions.

The shutdown groups are manually controlled during normal operation and are moved at a constant speed. Any reactor trip signal causes them to fall into the core. They are fully withdrawn during power operation and are withdrawn first during startup. Criticality is always approached with the control groups after withdrawal of the shutdown groups.

7.7.1.1.2 Reactivity Control

7.7.1.1.2.1 General

Overall reactivity control is achieved by the combination of chemical shim and RCCA. Long-term regulation of core reactivity is accomplished by adjusting the concentration of boric acid in the reactor coolant. Short-term reactivity control for power changes or reactor trip is accomplished by moving RCCA.

There is no provision for a direct continuous visual display of primary coolant boron concentration. When the reactor is critical, the best indication of reactivity status in the core is the position of the control group in relation to plant power and average coolant temperature. There is a direct relationship between control rod position and power and it is this relationship which establishes the lower insertion limit calculated by the rod insertion limit monitor. There are two alarm setpoints to alert the operator to take corrective action in the event a control group approaches or reaches its lower limit.

Any unexpected change in the position of the control group under automatic control or a change in coolant temperature under manual control provides a direct and immediate indication of a change in the reactivity status of the reactor. In addition, periodic samples of coolant boron concentration are taken. The variation in concentration during core life provides a further check on the reactivity status of the reactor including core depletion.

7.7.1.1.2.2 Control Group Rod Insertion Monitor

Control Rod Groups A and B use preset rod insertion limits. Control Rod Groups C and D use the following formula to calculate the rod insertion limits. The C and D control group rod insertion limits, Z_{LL}, are calculated as a linear function of power as represented by reactor coolant median differential temperature. The equation is:

$$Z_{LL} = A \text{ median } \Delta T + C$$

where A is a preset manually adjustable gain and C is a preset manually adjustable bias. The median ΔT is the median of the individual temperature differences from the reactor coolant hot leg and the cold leg.

An insertion limit monitor with two alarm setpoints is provided for each control bank. The "Low" alarm alerts the operator of an approach to a reduced shutdown reactivity situation requiring boron addition by following procedures with the CVCS. If the actuation of the "Low-Low" alarm occurs, the operator will take action to restore the rods to above the alarm setpoint within one hour or within the time specified by the axial power distribution methodology, whichever is sooner.

7.7.1.1.3 Interlocks.

The rod control group used for automatic control is interlocked with measurements of turbine-generator load to prevent automatic control rod withdrawal below 15 percent of nominal power. The manual and automatic controls are further interlocked with measurements of nuclear flux, ΔT, and rod drop indication to prevent approach to an overpower condition.

The operator is able to select any single bank of rods for manual operation. This is accomplished with a multiposition switch so that he may not select more than one bank. He may also select automatic or manual reactor control, in either case, however, the control banks can be moved only in their normal sequence with some overlap as one bank reaches its full withdrawal position and the next bank begins to withdraw. Relay interlocks, designed to meet the single failure criterion, are provided to preclude simultaneous withdrawal of more than one group of control and shutdown rods except in overlap regions.

7.7.1.1.4 Rod Drive Performance.

The control group is driven by a sequencing, variable speed rod drive programmer. In the control group of RCCA, control subgroups (each containing a small number of RCCA) are moved sequentially in a cycle such that all subgroups are maintained within one step of each other.

The sequence of motion is reversible, that is, the withdrawal sequence is the reverse of the insertion sequence. The sequencing speed is proportional to the control signal from the Reactor Control System. This provides control group speed control proportional to the demand signal from the control system.

A rod drive mechanism control center is provided to receive sequenced signals from the programmer and to actuate contactors in series with the coils of the rod drive mechanisms. Two reactor trip breakers are placed in series with the supply for these coils. To permit on-line testing, a bypass breaker is provided across each of the two trip breakers.

7.7.1.1.5 Full Length Rod Cluster Control Assemblies Position Indication.

Two separate systems are provided to sense the display control rod position. The digital and analog systems are the two separate systems; each serves as backup for the other. Operating procedures require the reactor operator to compare the digital and analog readings upon recognition of any apparent malfunction. Therefore, a single failure in rod position indication does not in itself lead the operator to take erroneous action in the operation of the reactor.

7.7.1.1.5.1 Analog System.

An analog signal is produced for each RCCA by a linear position transmitter.

An electrical coil stack is placed above the stepping mechanisms of the control rod magnetic jacks external to the pressure housing. When the associated control rod is at the bottom of the core, the magnetic coupling between a primary and secondary is small and there is a small voltage induced in the secondary. As the control rod is raised by the magnetic jacks, the relatively high permeability of the lift rod causes an increase in magnetic coupling. Thus, an analog signal proportional to within 3 percent of rod position is derived.

Direct, continuous readout of every RCCA position is presented to the operator by individual meter indications, without need for operator selection or switching to determine rod position. In addition, the individual rod position signals may be fed to the plant computer for readout. A deviation monitor alarm is actuated if an individual rod deviates from its group position by a preselected distance.

Lights are provided for rod bottom positions for each rod. The lights are operated by bistable devices in the analog system.

7.7.1.1.5.2 Digital System.

The digital system counts pulses generated in the rod drive control system. One counter is associated with each group (or subgroups) of RCCA. Readout of the digital system is in the form of electronic add-subtract counters reading the number of steps of rod withdrawal with one display for each group or subgroup. These readouts are mounted on the control panel.

7.7.1.1.5.3 Full Length Rod Drive Power Supply.

The full length control rod drive power supply concept using a single scram bus system has been successfully employed on all Westinghouse pressurized water reactor plants. Potential fault conditions with a single scram bus system are discussed in Section 7.2. The unique characteristics of the latch type mechanisms with its relatively large power requirements make this system with the redundant series trip breakers particularly desirable.

The solid state rod control system is operated from two parallel connected 400 kVa generators which provide 260 volt line to line, three phase, four wire power to the rod control circuits through two series connected reactor trip breakers. This AC power is distributed from the trip breakers to a line-up of identical solid state power cabinets using a single overhead run of enclosed bus duct which is bolted to and therefore comprises part of the power cabinet arrangement. Alternating current from the motor-generator sets is converted to a profiled direct current by the power cabinet and is then distributed to the mechanism coils (see Figure 7.2.1-10). Each complete rod control system includes a single 70 volt DC power supply which is used for holding the mechanisms in position during maintenance of normal power supply.

This 70 volt supply, which receives its input from the AC power source downstream of the reactor trip breakers, is distributed to each power cabinet and permits holding mechanisms in groups of four by manually positioning switches located in the power cabinets. The 30 ampere output capacity limits the holding capability to eight rods.

7.7.1.2 Turbine By-Pass

Turbine by-pass is provided by the steam dump system. It accommodates a reactor trip with turbine trip, or a 60 percent loss of load without reactor and turbine trip. The steam dump system removes steam to reduce the transient imposed upon the RCS. The control rod system can then reduce the reactor power to a new equilibrium value without causing overtemperature and/or overpressure conditions.

The steam dump system is actuated when the compensated average coolant temperature exceeds the programmed value by a given amount and electrical load decrease is greater than a given value. All the steam dump system valves stroke to full open immediately upon receiving the maximum by-pass signal. After they are full open, the valves are modulated by the compensated coolant average temperature signal. The steam dump system reduces proportionally as the control rods act to reduce the average coolant temperature. The artificial load is therefore removed as the coolant average temperature is restored to its programmed equilibrium value.

The steam dump system capacity is 50 percent of full load steam flow at full load steam pressure. The reactor coolant system will accommodate approximately 10 percent loss of load.

7.7.1.3 Feedwater Control

Each steam generator is equipped with a three-element feedwater controller (see Figure 7.7.1-3) which maintains a programmed water level as a function of load on the secondary side of the steam generator. The three-element feedwater controller regulates the feedwater valve by continuously comparing the feedwater flow signal, the water level signal, and the steam flow signal which is compensated by a steam pressure signal. The steam generators are operated in parallel, both on the feedwater and on the steam side.

Continued delivery of feedwater to the steam generators is required as a sink for the heat stored and generated in the reactor coolant following a reactor trip and turbine trip. An override signal closes the feedwater valves when the average coolant temperature is below a given temperature or when the respective steam generator level rises to a given value. Manual override of the feedwater control systems is also provided.

7.7.1.4 Pressure Control

The RCS pressure is maintained at constant value by using either the heaters (in the water region) or the spray (in the steam region of the pressurizer). The electrical immersion heaters are located near the bottom of the pressurizer. A portion of the heater groups are proportional heaters which are used to control small pressure variations. These variations are due to heat losses, including heat losses due to a small continuous spray. The

remaining (backup) heaters are turned on either when the pressurizer pressure controller signal is below a given value or when pressurizer level is above a given level.

The spray nozzles are located at the top of the pressurizer. Spray is initiated when the pressure controller signal is above a given setpoint. The spray rate increases proportionally with increasing pressure until it reaches a maximum value. Steam condensed by the spray reduces the pressurizer pressure. A small continuous spray is normally maintained to reduce thermal stresses and thermal shock and to help maintain uniform water chemistry and temperature in the pressurizer.

Two power relief valves limit system pressure to 2350 psia for large load reduction transients.

Three spring-loaded safety valves limit system pressure to 2750 psia following a complete loss of load without direct reactor trip or turbine by-pass.

7.7.1.5 Incore Instrumentation

7.7.1.5.1 Design Basis

The incore instrumentation is designed to yield information on the neutron flux distribution and fuel assembly outlet temperatures at selected core locations. Using the information obtained from the incore instrumentation system, it is possible to confirm the reactor core design parameters and calculated hot channel factors. The system provides means for acquiring data and performs no operational plant control.

7.7.1.5.2 System Design

The incore instrumentation system consists of environmentally and seismically qualified, bottom-mounted thermocouples, positioned to measure fuel assembly coolant outlet temperature at preselected locations, and flux thimbles, which run the length of selected fuel assemblies to measure the neutron flux distribution within the reactor core.

The measured data obtained from the incore temperature and flux distribution instrumentation system, in conjunction with previously determined analytical information, can be used to determine the fission power distribution in the core at any time throughout core life. This method is more accurate than using calculational techniques alone. Once the fission power distribution has been established, the maximum power output is primarily determined by thermal power distribution and the thermal and hydraulic limitations determine the maximum core capability.

The incore instrumentation provides information which may be used to calculate the coolant enthalpy distribution, the fuel burnup distribution, and an estimate of the coolant flow distribution.

The information provided by the incore instrumentation system is available through the system's Indication System which consists of two plasma display panels (one per instrumentation channel) installed in the main control room. Both instrumentation channels comply with R.G. 1.97 requirements.

Both radial and azimuthal symmetry of power may be evaluated by combining the detector and thermocouple information from the one quadrant with similar data obtained from the other three quadrants.

7.7.1.5.2.1 Thermocouples

Chromel-alumel, bottom-mounted thermocouples are inserted into the neutron flux thimble guide tubes that enter the reactor vessel through the seal table, and terminate at the end of the thimbles. For every thermocouple that is electrically connected to the system there is one spare thermocouple installed in the same guide tube and electrically connected through the seal table and thimble fittings to the corresponding intermediate junction box in the seal table area to allow easy replacement if necessary. Thermocouple outputs are recorded in the Control Room.

7.7.1.5.2.2 Movable Miniature Neutron Flux Detectors

Five fission chamber detectors (employing U_3O_8 which is enriched to more than 90 percent U_{235}) can be remotely positioned in retractable guide thimbles to provide flux mapping of the core. Approximate chamber dimensions are 0.188 in. in diameter and 2.10 in. in length. The stainless steel detector shell is welded to the leading end of the helical-wrap drive cable and the stainless steel or Inconel sheathed coaxial cable. Each detector is designed to have a minimum thermal neutron sensitivity of 1.0×10^{-17} ampere/nv and a maximum gamma sensitivity of 3×10^{-14} ampere/R/hr. Other types of miniature detectors, such as gamma ionization chambers and boron-lined neutron detectors, can also be used in the system. Retractable thimbles into which the miniature detectors are driven are pushed into the reactor core through conduits which extend from the bottom of the reactor vessel down through the concrete shield area and then up to a thimble seal table.

The thimbles, which are dry inside, are closed at the leading (reactor) ends, and serve as the pressure barrier between the reactor water pressure and the atmosphere. Mechanical seals between the retractable thimbles and the conduits are provided at the seal table.

During reactor operation, the retractable thimbles are stationary. They are extracted downward from the core during refueling to avoid interference within the core. A space above the seal table is provided for the retraction operation.

The drive system for the insertion of the miniature detectors consists basically of five drive units, ten limit switch assemblies, five 5-path rotary transfer devices, five 10-path rotary transfer devices, and forty-nine isolation valves. The drive system pushes hollow helical-wrap drive cables into the core with the miniature detectors attached to the leading ends of the cables and small diameter sheathed coaxial cables threaded through the hollow centers back to the trailing ends of the drive cables. Each drive assembly generally consists of a gear motor which pushes a helical-wrap drive cable and detector through a selective thimble path by means of a special drive box and includes a storage device that accommodates the total drive cable length.

7.7.1.5.2.3 Control and Readout Description

The control and readout system provides means for inserting the miniature neutron detectors into the reactor core and withdrawing the detectors at a selected speed while plotting a level of induced radioactivity versus detector position. Each detector can be driven in or out at speeds of 72 ft/min or 12 ft/min. In normal operation, the detectors would move at a speed of 72 ft/min outside the reactor core and 12 ft/min when scanning or recording the neutron flux. The average path length external to the core is 120 ft.

During normal operation, five separate fuel assemblies can be scanned simultaneously. A full core map can normally be recorded in about one hour. The control system consists of two sections, one physically mounted with the drive units, and the other contained in the Control Room. Limit switches in each drive conduit provide means for pre-recording detector and cable positioning in preparation for a flux mapping operation. Each gear box drives an encoder for positional data plotting. One 5-path group selector is provided for each drive unit to route the detector into one of the flux thimble groups. A 10-path rotary transfer device is used to route a detector into any one of up to ten selectable paths. Ten manually operated isolation valves allow free passage of the detector and drive wire when open, and prevent leakage of coolant in case of a thimble rupture, when closed. A path common to each group of flux thimbles is provided to permit cross calibration of the detectors.

The Control Room contains the necessary equipment for control, position indication, and flux recording. Panels are provided to indicate the core position of the detectors, and for plotting the flux level versus the detector position. Additional panels are provided for such features as drive motor controls, core path selector switches, plotting and gain controls. A "flux-mapping" consists, briefly, of selecting (by panel switches) flux thimbles in given fuel assemblies at various core quadrant locations. The detectors are driven or inserted to the top of the core and stopped automatically. An x-y plot (position vs. flux level) is initiated with the slow withdrawal of the detectors through the core from top to a point below the bottom. In a similar manner, other core locations are selected and plotted.

Each detector provides axial flux distribution data along the center of a fuel assembly. Various radial positions of detectors are then compared to obtain a flux map for a region of the core.

7.7.1.5.3 Evaluation

The thimbles are distributed nearly uniformly over the core with about the same number of thimbles in each quadrant. The number and location of thimbles permit measurement of enthalpy rise and heat flux hot channel factors to an accuracy of 4 and 5 percent (95 percent probability/95 percent confidence), respectively. Measured nuclear peaking factors are increased by these uncertainties to allow for possible instrument error and analytic processing error. The heat flux hot channel factor is also increased by 3 percent to allow for engineering tolerances in fuel fabrication and by functions of core height specified in the Core Operating Limits Report. If the measured nuclear peaking factors are not within the limits specified in the Core Operating Limits Report, then required actions shall be taken to reduce thermal power as specified in Technical Specifications.

7.7.1.6 Deleted

This section deleted in Revision 18

7.7.1.7 Core Subcooling Monitor

The purpose of the subcooling monitor is to provide a continuous indication of margin to saturated conditions. The monitor uses inputs from core outlet thermocouples, RCS hot leg resistance temperature detectors and RCS system pressure to drive a microprocessor which calculates saturation temperature and determines the margin to saturation based on the inputs. The individual inputs as well as the margin to saturation can be displayed on the monitor's plasma display panels (there is one plasma display panel for each of the two instrumentation channels).

7.7.1.8 Emergency Response Facility Information System (ERFIS)

ERFIS is an integrated signal data gathering, signal processing and information display system that acquires analog and digital inputs from field sensors and input from other plant systems. This data is processed by the ERFIS system to produce meaningful displays, logs, alarms and plots of current or historical plant performance with the intent of improving the decision making process in the event of an emergency, as well as improving routine plant operation. The ERFIS can display its information in the Unit 2 Control Room, Technical Support Center (TSC), Emergency Operations Facility (EOF) and other emergency facilities such as the Operations Support Center (OSC) and the Joint Information Center (JIC). The Safety Parameters Display System (SPDS) is a subsystem of the ERFIS system that provides the Control Room and the emergency stations with the overall status of the Critical Safety Functions Status display. High ERFIS system availability is achieved by the use of alternate power sources one of which is a diesel generator (building backup power supply), an Uninterruptible Power Supply (UPS), multiple input units, redundant data paths, redundant data acquisition units, redundant host computers, multiple display stations and multiple hard copy output devices.

7.7.1.8.1 System description.

The ERFIS system consists of the following major hardware subsystems:

1. Distributed Data Acquisition System hardware
    a. Central controllers (2)
    b. Time Stamp Synchronizers (2)
    c. Remote multiplexers (up to 16)

2. Computer System hardware
    a. ERFIS Local Host computers (2)
    b. Display computers (as required)

3. Power Supply
    a. Uninterruptible Power Supply (UPS)
    b. Batteries
    c. Diesel generator (building backup power supply)

The ERFIS system major software subsystems are as follows:

1. Operating System
2. System Failover software
3. Data acquisition software
4. Database management software
5. Human Machine Interface (HMI) software
6. Log Generation and Reporting software
7. Data Archive and Retrieval software
8. SPDS software
9. Nuclear Steam Supply System (NSSS) software
10. Emergency Preparedness (EP) functions software
11. Meteorological (MET) Data link software
12. Alarm Display software
13. Miscellaneous special software links to other systems

7.7.1.8.1.1 System hardware.

The data acquisition system consists of distributed process input/output hardware that includes microprocessor based remote multiplexers (up to 16), redundant microprocessor based central controllers and redundant host computers.

The remote multiplexers consist of field device terminations including isolation devices for the analog and digital field inputs/outputs, electronics for signal conditioning/scanning and digitizing of the input signals and redundant communications and control back to the central controllers.

The redundant central controllers and redundant ERFIS local host computers receive, processes, buffers and stores the input data from the remote multiplexers. The central controllers communicate with each other and the remote controllers via redundant high-speed fiber optic links. The system is configured to support automatic failover for critical hardware failures in order to provide a high level of availability and reliability.

The ERFIS local host computers have network connections to display computers in the Control Room, TSC, EOF, and OSC. The Control Room also has a network connected computer display dedicated as an SPDS display. Additional computer displays are located in other areas of the plant as required. The Control Room, TSC, EOF, OSC and the JIC have printers for text and graphics printing as needed. To accommodate security concerns with data transmission off-site to the JIC, that link uses additional application software and cyber security protection. The ERFIS local host computers also connect to utility server computers that serve as serial communications links to serial devices providing data to or from the ERFIS system. The serial links include such systems as the MET data system and plant systems data such as Inadequate Core Cooling Monitor (ICCM).

7.7.1.8.1.2 System Software

The ERFIS system software consists of a real time operating system that includes the necessary functional software such as system initialization and startup, task maintenance, network communications, output to graphics and text printers, data storage to hard disk drives and tape drives and source code generation and maintenance. The various ERFIS functions are written in modular software units according to the function needs or requirements. The modular software design allows new functions to be added to the system as needed. The software modules are identified by the primary function performed by the software. The major software subsystems are listed above in this section.

The real time operating system combined with the unique software modules of the ERFIS system perform all of the required functions the ERFIS system must perform.

7.7.1.8.1.2.1 Safety Parameter Display System

The Safety Parameter Display Subsystem is based upon the Westinghouse Owners' Group critical safety function definitions and status trees.

SPDS is a combination of displays arranged in a three-level hierarchy: SPDS level one or primary displays, SPDS level two or secondary displays, and the SPDS level three displays.

The SPDS level one display is dedicated to overall plant safety. It consists of a series of six color-coded boxes horizontally arranged and always present on the screen of the CRT once any of the SPDS displays have been brought up on a display console. Each box is dedicated to a specific critical safety function (CSF), whose performance is important in maintaining the plant in a safe condition. For HBR-2, the set of CSFs in decreasing order of importance is:

- Subcriticality
- Core Cooling
- Heat Sink
- RCS Integrity
- Containment Integrity
- RCS Inventory

The subcriticality box appears at the bottom left and remaining CSFs in descending hierarchy to the right, with the RCS inventory CSF appearing on the right-most box. Each box can be lit with one of the five colors.

The following five-color status hierarchy is used to identify the priority status of operator action for current plant conditions:

- Green - the CSF is satisfied; no operator action is called for
- Yellow - the CSF is not fully satisfied; operator action may eventually be needed
- Orange - the CSF is under severe challenge; prompt operator action is necessary
- Red - the CSF is in jeopardy; immediate operator action is required
- White - the status of the CSF cannot be determined

The color priority status hierarchy takes precedence over the function hierarchy. For example, a red RCS integrity condition must be responded to before an orange heat sink condition. The highest priority box will blink and will remain locked until the operator manually acknowledges through the keyboard that he has taken the proper corrective action.

The SPDS level two or secondary displays are more detailed status tree representations of the conditions defining a critical safety function based on the Westinghouse Owners' Group status trees. These trees show success or degrees of failure of the CSF, the proper operator action(s), and the priority of operator response.

The subcriticality critical safety function status tree gauges the reactivity state of the reactor core and is satisfied if either the neutron flux is in the source range with a zero or negative startup rate (SUR), or if power is below 5% with a startup rate of less than -0.2 decades per minute (dpm). The status tree is arranged in a logical downward progression through the ranges of neutron flux instrumentation, starting with power range and proceeding down through intermediate range to source range.

If the current state of the system is in a status branch where the CSF is not satisfied, then the operator is directed to the appropriate function restoration procedure (FRP). Both red and orange paths direct the operator to the function restoration procedure FRP-S.1. The required actions are the same, but the degree of urgency is different and indicated by the color.

The SPDS level three displays consist mostly of trend plots and x-y plot of key plant parameters related to specific critical safety functions. The six CSF boxes of the SPDS level one display will appear on all SPDS level two and level three displays.

The SPDS portion of the HBR-2 ERFIS provides timely plant information to aid Main Control Room personnel in determining the safety status of the plant during abnormal or emergency conditions. The graphic displays will be based on the Emergency Response Guidelines (ERGs) (Reference 2) and will be formatted to give assistance in following the HBR-2 Emergency Operating Procedures (EOPs) (Reference 3). The ERFIS can easily be changed to accommodate revisions in the ERGs. Human factor engineering has also been taken into account during development of the HBR-2 SPDS to maximize the ability to Control Room personnel to readily determine plant status and to minimize their errors during its use.

The HBR-2 SPDS was added as an aid to plant personnel. It is not intended as a substitute for other safety-related equipment or instrumentation but rather as an adjunct to such equipment.

7.7.2 ANALYSIS

The Rod Control System is designed to limit the amplitude and the frequency of continuous oscillation of coolant average temperature about the control system setpoint within acceptable values. Continuous oscillation can be induced by the introduction of a feedback control loop with an effective loop gain which is either too large or too small with respect to the process transient response, i.e., instability induced by the control system itself. Because stability is more difficult to maintain at low power under automatic control, no provision is made to provide automatic control below 15 percent of full power.

The control system is designed to operate as a stable system over the full range of automatic control throughout core life.

7.7.2.1 Step Load Changes Without Turbine By-Pass

A typical power control requirement is to restore equilibrium conditions, without a plant trip, following a plus or minus 10 percent change in load demand, over the 15 to 100 percent power range for automatic control. The design must necessarily be based on conservative conditions and a greater transient capability is expected for actual operating conditions. A load demand greater than full power is prohibited by the turbine control load limit devices.

The function of the control system is to minimize the reactor average coolant temperature deviation during the transient within a given value and to restore average temperature to the programmed setpoint within a given time. Excessive pressurizer pressure variations are prevented by using spray and heaters in the pressurizer.

The margin between over-temperature ΔT setpoint and the measured ΔT is of primary concern for the step load changes. This margin is influenced by nuclear flux, pressurizer pressure, average reactor coolant temperature, and temperature rise across the core.

7.7.2.2 Loading and Unloading

Ramp loading and unloading is provided over the 15 to 100 percent power range under automatic control. The function of the control system is to maintain the average coolant temperature and pressure as functions of turbine-generator load. The minimum control rod speed provides a sufficient reactivity rate to compensate the reactivity changes resulting from the moderator and fuel temperature changes.

The average coolant temperature increases during loading and causes a continuous insurge to the pressurizer as a result of coolant expansion. The sprays limit the resulting pressure increase. Conversely, as the coolant average temperature is decreasing during unloading, there is a continuous outsurge from the pressurizer resulting from coolant contraction. The heaters limit the resulting system pressure decrease. The pressurizer level is programmed such that the water level is above the setpoint at which the heaters cut out during the loading and unloading transients.

The primary concern for the loading is to limit the overshoot in average coolant temperature so that a margin is provided for the over-temperature ΔT setpoint.

The automatic load controls are designed to safely adjust the unit generation to match load requirements within the limits of the unit capability and licensed rating.

7.7.2.3 Loss of Load With Turbine By-Pass

The reactor control system is designed to accept a 60 percent loss of electrical load. No reactor trip or turbine trip should be actuated. The automatic turbine by-pass system is able to accommodate this abnormal load rejection and to reduce the effects of the transient imposed upon the reactor coolant system. The reactor power is reduced at a rate consistent with the capability of the rod control system. Reduction of the reactor power is automatic down to 15 percent of full power. Manual control must be used when the power is below this value. The by-pass flow reduction is as fast as RCCA are capable of inserting negative reactivity.

The pressurizer relief valves might be actuated for the most adverse conditions, e.g., the most negative Power coefficient, and the minimum incremental rod worth. The relief capacity of the power-operated relief valves is sized large enough to limit the system pressure to prevent actuation of high pressure reactor trip for the above conditions.

7.7.2.4 Turbine-Generator Trip With Reactor Trip

Whenever the turbine-generator unit trips at an operating level above 40 percent power, the reactor also trips. The plant is operated with a programmed average temperature as a function of load, with the full load average temperature significantly greater than the saturation temperature corresponding to the steam generator pressure at the safety valve setpoint. The thermal capacity of the reactor coolant system is greater than that of the secondary system, and because the full load average temperature is greater than the no load steam temperature, a heat sink is required to remove heat stored in the reactor coolant to prevent actuation of steam generator safety valves for this trip from full power. This heat sink is provided by the combination of controlled release of steam to the condenser and by makeup of cold feedwater to the steam generators.

The turbine by-pass system is controlled from the reactor average coolant temperature signal whose setpoint values are reset upon trip to the no load value. Actuation of the turbine by-pass must be rapid to prevent actuation of the steam generator safety valve. With the by-pass valves open, the average coolant temperature starts to reduce quickly to the no load setpoint. A direct feedback of temperature acts to proportionally close the valves to minimize the total amount of steam which is by-passed.

Following the turbine trip, the steam voids in the steam generators will collapse and the fully opened feedwater valves will provide sufficient feedwater flow to restore water level in the downcomer. The feedwater flow is cut off when the average coolant temperature decreases below a given temperature value or when the steam generator water level reaches a given high level.

Additional feedwater makeup is then controlled manually to restore and maintain steam generator level while assuring that the reactor coolant temperature is at the desired value. Residual heat removal (RHR) is maintained by the steam generator pressure controller (manually selected) which controls the amount of steam flow to the condensers. This controller operates the same bypass valves to the condensers which are used during the initial transient following turbine and reactor trip.

The pressurizer pressure and level fall rapidly during the transient because of coolant contraction. If heaters become uncovered following the trip, the CVCS will provide full charging flow to restore water level in the pressurizer. Heaters are then turned on to restore pressurizer pressure to normal.

The turbine by-pass and feedwater control systems are designed to prevent the average coolant temperature falling below the programmed no load temperature following the trip to ensure adequate reactivity shutdown margin.

References: Section 7.7

7.7.1-1 U.S. Nuclear Regulatory Commission, "Requirements for Emergency Response Capability," Supplement No. 1 to USNRC Report NUREG-0737, December 1982

7.7.1-2 Westinghouse Owners' Group Emergency Response Guidelines (ERG)

7.7.1-3 Nuclear Operations Department, H. B. Robinson Unit 2 Steam Electric Plant (HBR-2) Emergency Operating Procedures

7.7.1-4 "Safety Evaluation Report on the Emergency Response Guidelines," Generic Letter 83-22, D. G. Eisenhut, NRC, to all licensees, June 3, 1983

7.7.1-5 Deleted

7.7.1-6 Standard Review Plan (SRP) 18.2, "Safety Parameter Display System," Revision 0, 84/12, with Appendix A, Revision 0, December 1984

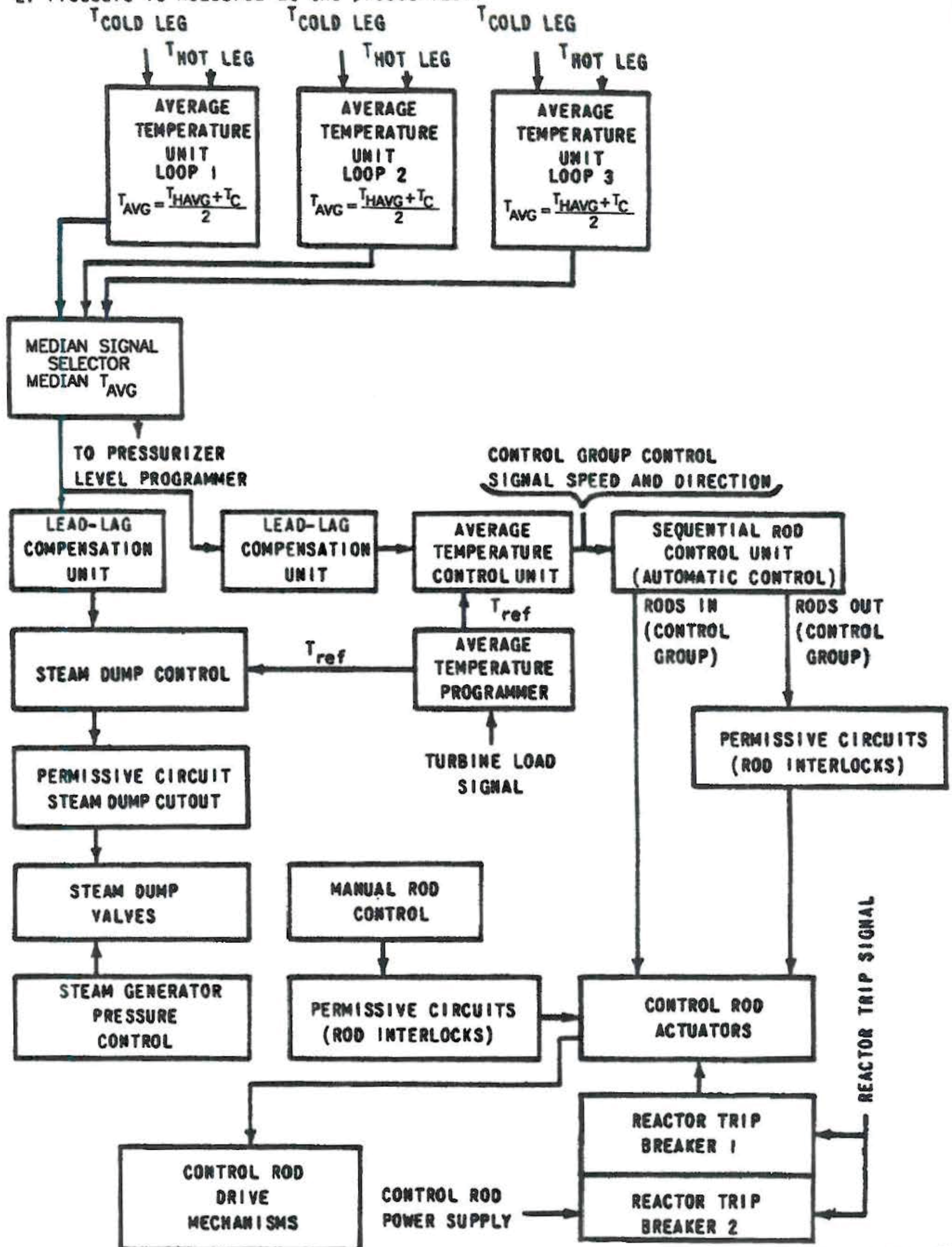
7.7.1-7 Deleted

7.7.1-8 WCAP-7308-L-P-A, "Evaluation of Nuclear Hot Channel Factor Uncertainties," June 1988.

7.7.1-9 EMF-93-164(P)(A) w/Correspondence, "Power Distribution Measurement Uncertainty for INPAX-W in Westinghouse Plants," Siemens Power Corporation, February 1995.

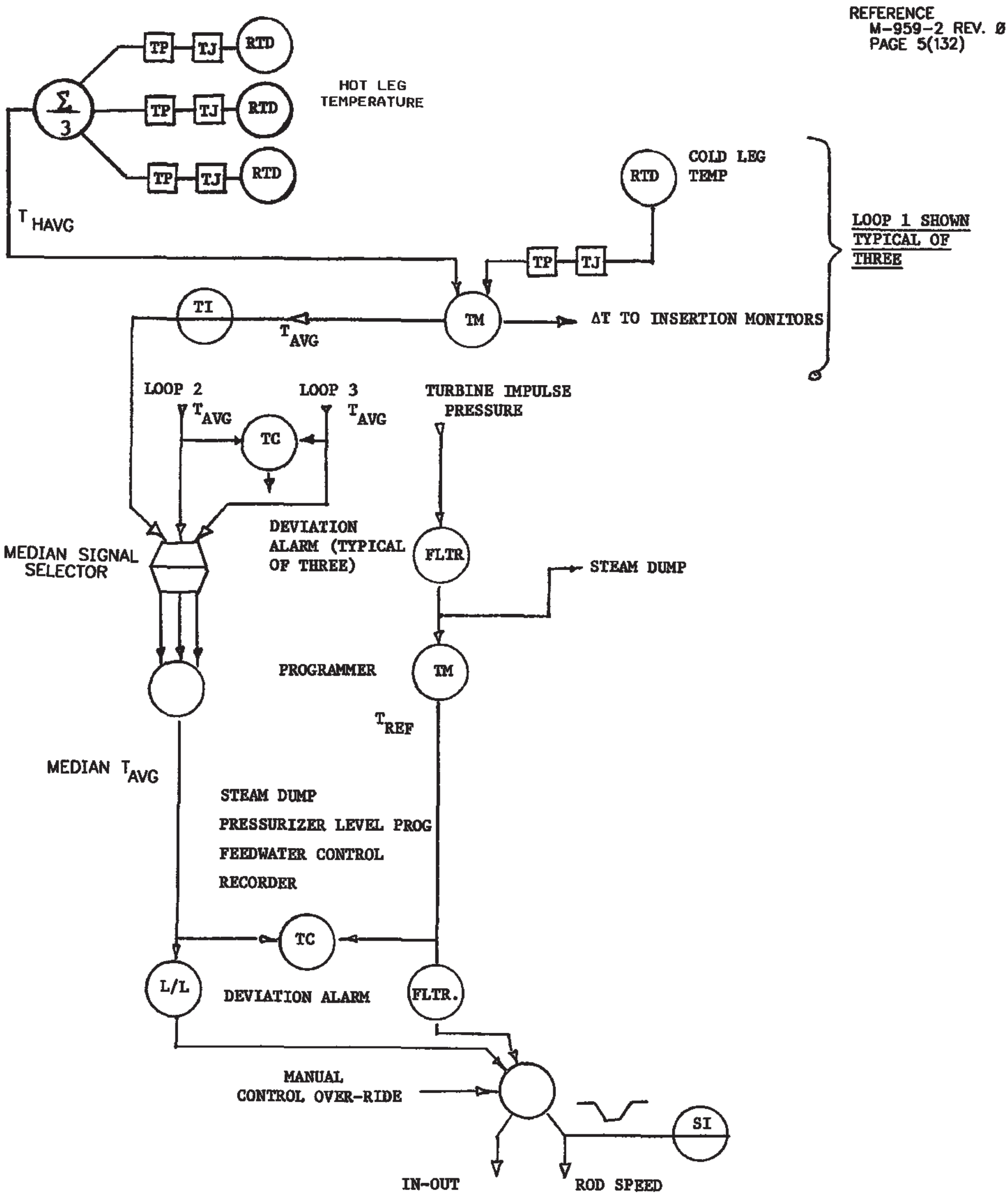
7.7.1-10 Westinghouse Letter SCS-LTR-06-22, “H. B. Robinson Unit 2 Turbine Trip without Reactor Trip Transient from the P-8 Setpoint Analysis”

NOTES:
1. Temperatures are measured at steam generator's inlet and outlet.
2. Pressure is measured at the pressurizer.



REVISION NO. 22

H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	SIMPLIFIED BLOCK DIAGRAM OF REACTOR CONTROL SYSTEMS	FIGURE 7.7.1–1

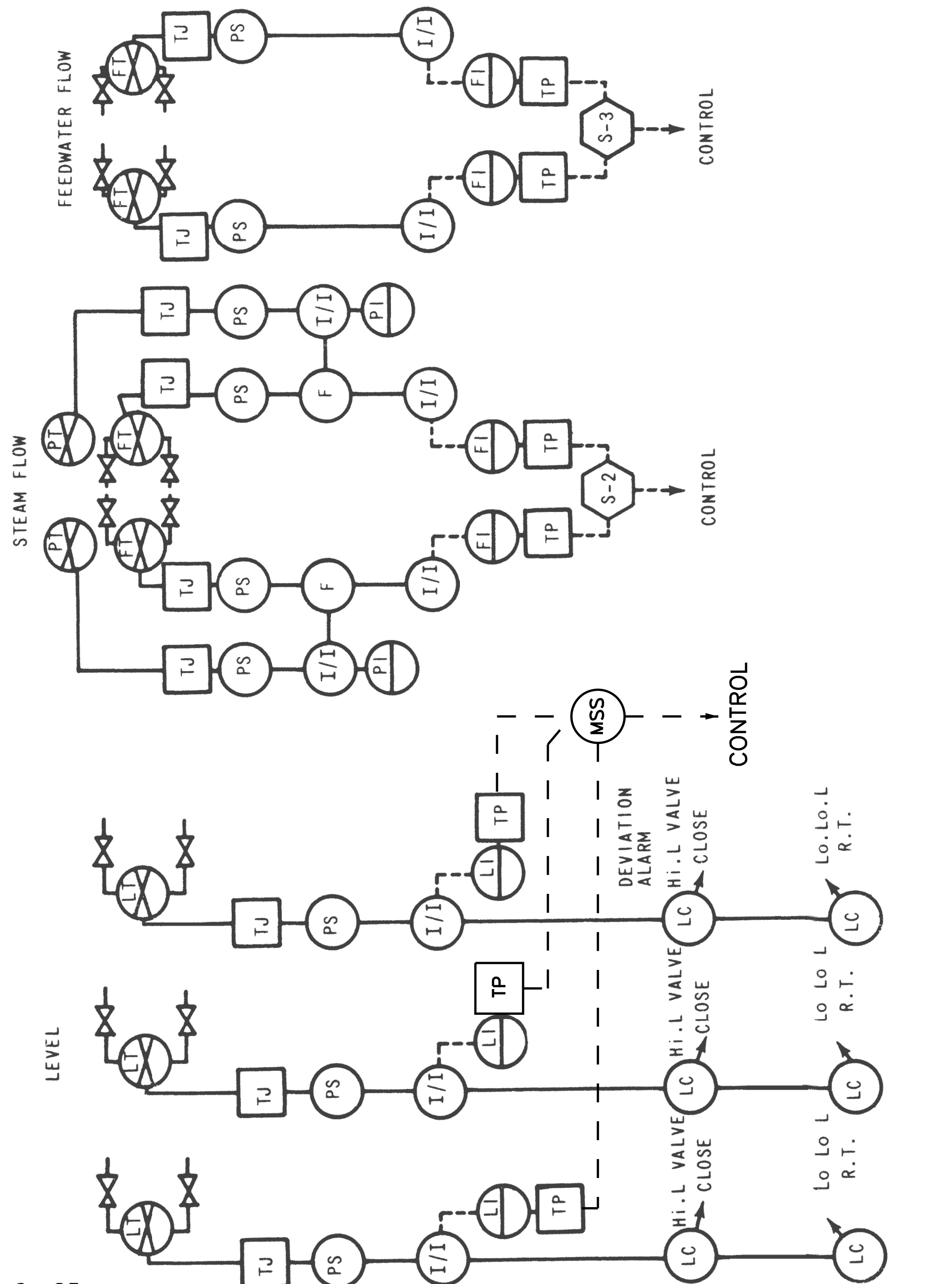


NOTE: SEE FIGURE 7.2.1-12 FOR DEFINITION OF SYMBOLS

REVISION NO. 24

H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	T_{AVG} CONTROL SYSTEM	FIGURE 7.7.1 - 2

NOTE: SEE FIGURE 7.2.1-12 FOR DEFINITION OF SYMBOLS



REVISION NO. 25

H. B. ROBINSON UNIT 2 Carolina Power & Light Company UPDATED FINAL SAFETY ANALYSIS REPORT	STEAM GENERATOR LEVEL CONTROL AND PROTECTION SYSTEM	FIGURE 7.7.1-3