TABLE OF CONTENTS

11.2 LOW PRESSURE SAFETY INJECTION SYSTEM

LIST OF TABLES

LIST OF FIGURES

11.2 LOW PRESSURE SAFETY INJECTION SYSTEM

Learning Objectives:

1. State the purpose of the low pressure safety injection (LPSI) system.

2. Describe the LPSI flow paths including suction supplies, discharge points, and major components during the following operations:

   a. Power operations
   b. Shutdown cooling
   c. Injection phase
   d. Recirculation phase

3. State the purpose of the shutdown cooling heat exchangers, when the heat exchangers are used, and the cooling medium for the heat exchangers.

4. Explain why RCS pressure and temperature limits are placed on the initiation of shutdown cooling.

5. Explain how the LPSI system is protected against over pressurization while operating in the shutdown cooling mode of operation.

11.2.1 Introduction

The purposes of the LPSI system are:

1. To serve as the low pressure injection portion of the emergency core cooling system (ECCS) following a loss of coolant accident (LOCA),

2. To remove heat from the RCS during normal cool down and maintain proper coolant temperatures during maintenance and refueling, and

3. To transfer refueling water from the RWT to the refueling pool and to return the water to the tank following refueling activities.

The primary function of the LPSI system is to provide a low pressure, high volume safety injection to cool the core following a loss of coolant accident during the injection phase. The LPSI system is automatically secured in the recirculation phase of the LOCA; however, the system may be manually aligned to provide a heat sink for long term core cooling.

The secondary function of the LPSI system is to complete the cool down of the RCS and to maintain the proper RCS temperatures while shutdown. This mode of operation is called shutdown cooling. In the shutdown cooling mode of operation, the LPSI system will take a suction from one (1) of the two (2) RCS hot legs and will discharge the hot RCS fluid to the shutdown cooling heat exchangers which are normally connected to the containment spray pump discharge header. The shutdown cooling heat exchangers transfer the RCS decay heat to the component cooling water (CCW) system. From the outlet of the shutdown cooling heat exchangers, the water is returned to the RCS via the normal LPSI discharge piping.

The final function of the LPSI system is to transfer water to and from the RWT during refueling operations. During refueling, the refueling pool is flooded to allow safe fuel handling activities. Water is transferred from the RWT to the refueling pool via the LPSI pumps and piping. Once the refueling activities are completed, the water is returned to the RWT.

11.2.2 System Description

The LPSI system, as shown in Figure 11.2-1, consists of a suction supply from the RWT, two

(2) LPSI pumps, and four (4) RCS injection points. During power operations, the LPSI system is aligned for its accident mode of operation with the suction supply valves from the RWT open and the four (4) injection valves closed. If a LOCA occurs, the LPSI pumps will be started by a safety injection actuation signal (SIAS). The SIAS will also open the four (4) injection valves. The pumps will recirculate water back to the RWT until RCS pressure drops to below the shut-off head of the pumps (approximately 180 psia). Once the RCS has depressurized below this value, flow from the LPSI system starts to provide core cooling. The pumps will continue to provide flow to the RCS until a low RWT level is reached and a recirculation actuation signal (RAS) is generated. The RAS stops the LPSI pumps.

The LPSI shutdown cooling alignment is shown in Figure 11.2-2. After RCS temperature and pressure are reduced to < 300°F and 270 psia, the shutdown cooling heat exchangers are valved into the discharge of the LPSI pumps, and the suction supply from the RCS hot leg is established. Water is circulated from the RCS, through the shutdown cooling heat exchangers, and back to the LPSI discharge piping. The return flow to the RCS is controlled by two (2) valves, a flow control valve on the discharge of the LPSI pumps that is set to control a constant flow, and the other on the outlet of the shutdown cooling heat exchangers. The two (2) valves are used to control RCS temperature in the shutdown cooling mode of operation. For example, if the temperature of the RCS is to be decreased, the control valve on the outlet of the heat exchangers is opened to route additional flow through the heat exchangers. When the valve is opened, the total LPSI flow increases and the flow control valve will throttle down to maintain a constant flow. The final result is an increase in flow rate through the shutdown cooling heat exchangers and less flow bypassing the heat exchangers. Total LPSI flow remains constant.

The flow path described in the previous paragraph is also applicable in the refueling mode of operation. In addition, when the refueling pool is to be filled, one of the two LPSI pumps can be aligned to the RWT. Water will be pumped from the tank, through the injection valves, and into the RCS. Since the head is removed or detensioned, water will exit the vessel and fill the pool. When refueling is completed, the water is pumped back to the RWT by a connection just downstream of the shutdown cooling heat exchangers.

11.2.3 Component Description

11.2.3.1 Refueling Water Tank

The refueling water tank (RWT) performs the following functions:

1. Provides borated water to the HPSI, LPSI, and the containment spray pumps,

2. Provides makeup water to the spent fuel pool and

3. Stores refueling water.

The RWT (see Figure 11.2-3) is a flat-bottomed, cylindrical tank with a conical roof, and is fabricated from stainless steel. The tank has a total capacity of 420,000 gallons and must be filled to at least 400,000 gallons during power operations. The volume of 400,000 gallons will provide thirty-six minutes of safety injection during a LOCA with the HPSI, LPSI, and the containment spray pumps operating at design flow rates.

The RWT is borated to a concentration of 2300 to 2700 ppm, and the tank contents are

maintained at the proper concentration by the chemical and volume control system (CVCS). A recirculation pump and heat exchanger are used to maintain the RWT temperature >40°F. The heat exchanger is heated by the plant heating system.

The RWT has two outlet lines, one for each ECCS train, that supply water to the ECCS and containment spray pumps. The lines are physically separated to minimize the possibility of simultaneous plugging. Each outlet line has a protective screen with a mesh size such that any particle that passes through the screen will also pass through the ECCS and containment spray system components. Motor operated valves are installed in each line. The valves are normally open and are controlled from the control room. An annunciator is energized if the valves are shut.

Four (4) level transmitters are installed on the RWT to provide inputs to the RAS. In addition to the RAS level instrumentation, two (2) level indicators are installed to provide control room indication and annunciation. One of the transmitters is a narrow range indicator (444 to 468 inches) and is used to maintain the tank level within technical specification requirements. The other level indicator is wide range (0 to 39 feet) and is used when transferring the tank contents to the refueling pool. Temperature indication (0°F to 200°F) and alarm functions are also provided for the RWT.

11.2.3.2 LPSI Pumps

Two pumps are installed in the LPSI system. Table 11.2-1 contains the design data for the LPSI pumps. The pumps are horizontal, single-stage, centrifugal pumps. The pump shaft seal is a mechanical seal that is compatible with boric acid solutions. The seal is designed for operation at temperatures greater than 300°F, but to increase seal life, a portion of the LPSI pump inlet water is diverted by a pumping ring, cooled by the component cooling water system, and injected back into the seal. The water cools the seal and returns to the pumping ring, A throttle bushing is installed to back up the mechanical seal.

Table 11.2-1
LPSI Pump Data

Number Installed	2
Design Pressure	500 psig
Design Temperature	350°F
Design Flow	3000 gpm
Developed head	130 psig
Shut-off head	181 psig

Each LPSI pump is driven by a 400 hp, 4160 Vac electrical induction motor powered from the class 1E distribution system. The pump motor is capable of accelerating the pump to full speed in eight seconds with 75% of the nameplate voltage applied. The LPSI pumps are automatically started by a SIAS and automatically stopped by a RAS.

11.2.3.3 Shutdown Cooling Heat Exchangers

The shutdown cooling heat exchangers are used to remove core decay heat during plant shutdowns and in cold shutdown. The heat exchangers are designed to maintain the RCS at the refueling temperature (approximately 140°F) 27 1/2 hours after shutdown from an extended period of full power operations. The heat exchangers also cool the containment spray water during containment spray operations.

The heat exchangers are of the U-tube and shell design with component cooling water (CCW) flowing through the shell and RCS/RWT fluid flowing through the tubes. The tubes are

constructed of stainless steel and the shell is made of carbon steel. The shutdown cooling heat exchanger data is located in Table 11.2-2.

Each shutdown cooling heat exchanger is protected against tube side over pressurization by relief valves. The relief valves have a setpoint of 500 psig and are sized to accommodate the pressure developed by a sudden increase in temperature of the tube side fluid.

Table 11.2-2
Shutdown Cooling
Heat Exchanger Design Data

	Tube Side	Shell Side
Fluid	RCS/RWT	CCW
Temperature	450°F	250°F

11.2.3.4 LPSI Valves

Shutdown Cooling Suction Isolation Valves

The #12 RCS loop supplies shutdown cooling suction supply to the LPSI pumps via a 12-inch drop line that contains two series motor-operated valves (SI-652 and SI-651). These valves are interlocked with wide range pressurizer pressure and automatically close if pressurizer pressure exceeds 300 psia. The purpose of this interlock is to prevent over pressurization of the LPSI suction and discharge piping. The interlock setpoint is chosen to ensure that the pressure rating of the LPSI suction piping is not exceeded, and an assumption of operation at the setpoint plus the differential pressure developed by the LPSI pump (300 psia + 180 psid pump head = 480 psia) will not exceed the discharge piping pressure rating. A final assumption is that the shutdown cooling system temperature is less than the design temperature rating of the piping. The temperature requirement of 270°F is administratively maintained.

A relief valve is installed between the two (2) shutdown cooling isolation valves to protect the piping between the motor-operated valves from pressure developed due to sudden temperature increases in the containment. The setpoint of this relief valve is 2500 psia. This valve could function after the shutdown cooling system is removed from service and the section of piping between the closed suction isolation valves is hydraulically solid. An ambient temperature increase would increase pressure in the isolated section of piping and the relief valve prevents over pressurization.

A second relief valve is installed downstream of the second suction isolation valve (SI-651). This relief valve has a setpoint of 330 psia and is sized to protect the suction piping from over pressure assuming:

1. The pressurizer is solid,
2. All three charging pumps are started, and
3. The shutdown cooling pumps are operatting.

If the pressurizer is completely filled with water (solid), and the charging pumps are started, the increase in system mass could increase RCS pressure above the allowable value for shutdown cooling operations. The relief valve's capacity exceeds the capacity of the three charging pumps (132 gpm) and over pressurization is prevented.

Shutdown Cooling Flow Control and Bypass Valves

The shutdown cooling flow control valve (CV-306) is used to maintain the shutdown cooling system flow rate as measured by the flow

orifice in the common pump discharge line. Normal shutdown cooling flow is 3000 gpm with one pump and heat exchanger in service and 6000 gpm if both pumps and heat exchangers are used. Since this valve is in series with the four (4) LPSI injection motor-operated valves, it must be fully open to ensure that LPSI flow is available. The valve is locked open when the plant is operating at power.

The bypass valve (V-657) is used to determine the amount of shutdown cooling flow that is diverted through the shutdown cooling heat exchangers. As previously discussed, RCS temperature is controlled by positioning V-657 to the desired position and valve CV-306 throttles to maintain a constant shutdown cooling system flow. Since the valves are manually isolated when the shutdown cooling system is removed from service, no special provisions are required for normal LPSI or containment spray operations.

LPSI Injection Motor Operated Valves

Four (4) LPSI injection motor-operated valves are installed in parallel flow paths. Each flow path supplies safety injection flow to one (1) of the RCP discharge lines. Two (2) of the four (4) valves are powered from one (1) 480 Vac Class 1E electrical distribution train, and the other two (2) valves are powered from the opposite train. This power arrangement ensures LPSI flow in the event of a loss of one (1) Class 1E train. The valves are normally closed and are automatically opened by a SIAS. The capability to throttle LPSI flow exists by driving the valve to the desired position and overriding the SIAS signal with the valve control hand switch. An alarm is annunciated if a LPSI valve has been overridden.

Recirculation Isolation Valves

The minimum recirculation flow for the LPSI pumps is assured by flow orifices that pass 40 gpm flow through the pump recirculation lines to the RWT. Two series isolation valves (V-659 and V-660) are installed in this line and automatically close when a RAS is received. The valves are closed to prevent the transfer of radioactive containment sump water to the RWT during the recirculation phase of the loss of coolant accident.

11.2.4 System Operations

11.2.4.1 Plant Cool down

The initial phase of RCS cool down is accomplished by transferring heat from the steam generators to the condenser by using the turbine bypass valves to dump steam. The RCS is depressurized by using the pressurizer spray valve(s). When the RCS is cooled down to 300°F and depressurized to 270 psia, the shutdown cooling system is placed in service. The basic steps for placing the shutdown cooling system in service are:

1. Isolate the shutdown cooling heat exchangers from the containment spray system to prevent inadvertent containment spray. This is accomplished by disabling the spray pumps and manually closing the spray pump discharge isolation valves. In addition, the spray header isolation motor-operated valves are closed and power is removed from the valve motor,

2. Manually align the shutdown cooling heat exchangers to the discharge of the LPSI pumps,

3. Place the shutdown cooling flow and bypass control valves in service,

4. Ensure that cooling water is being supplied to the shutdown cooling heat exchangers,

5. Open the LPSI injection motor-operated valves and the shutdown cooling suction isolation valves,

6. Start the LPSI pumps.

The flow path for the shutdown cooling system is from the #12 hot leg to the suction of the LPSI pumps, a parallel flow path through the heat exchangers and the flow control valve, through the four (4) LPSI injection valves back to the RCP discharge lines, and into the core. The shutdown cooling system will be used in this alignment to reduce RCS temperatures to the desired value and at the desired cool down rate. Once the desired temperature is reached, the shutdown cooling system is used to maintain stable conditions.

11.2.4.2 Accident Operations

During power operations, the LPSI system is aligned as an emergency core cooling system with the RWT suction valves open and the four (4) LPSI injection valves closed. The flow control valve (V-306) is locked open. When a SIAS signal is received, the LPSI pumps start and the four (4) injection motor operated valves open. When system pressure drops below LPSI discharge pressure, LPSI flow starts. The system continues to operate in this mode until a RAS is generated by low RWT level. When the RAS is received, the LPSI pumps are automatically stopped, and the recirculation line motor operated valves are closed. The level of water in the containment building sump following a loss of coolant accident is not sufficient to ensure net positive suction head for the LPSI pumps during the recirculation phase; therefore, the pumps are stopped. Long term core cooling is provided by the HPSI system.

11.2.5 PRA Insights

The reactor safety study (WASH 1400) identified a potential core melt scenario that involves the LPSI system. The scenario assumes that there is a failure of the two (2) series check valves installed in the interface between the RCS and LPSI systems.

The failure pressurizes the LPSI piping, from the RCS injection point to the LPSI injection motor-operated valves, to RCS pressure. The LPSI injection valves are opened for testing and the high pressure RCS fluid over-pressurizes and ruptures the low pressure LPSI piping located in the auxiliary building. A loss of coolant accident has occurred with a significant difference, the coolant is not being collected in the sump. Since the sump is not available for the recirculation phase, and there is no way to recover the RWT and RCS water from the auxiliary building, a core melt will occur when the RWT empties. This scenario is identified in WASH 1400 as Event V and is also known as an inter-system LOCA. Generically, the inter-system LOCA is a major contributor to core melt frequency.

11.2.6 Summary

The LPSI system is an emergency core cooling system that provides a high volume of coolant at a low pressure. In addition, the LPSI pumps and piping are used in conjunction with the shutdown cooling heat exchanger to provide a method of reducing RCS temperatures to cold shutdown values.

In the emergency core cooling mode of operation, the LPSI pumps take a suction from the RWT and discharge to the four (4) RCP discharge lines. The LPSI pumps are stopped by an RAS signal.

In the shutdown cooling mode of operation, the LPSI pumps take a suction from the RCS hot leg and discharge to the RCP discharge lines via the shutdown cooling heat exchangers

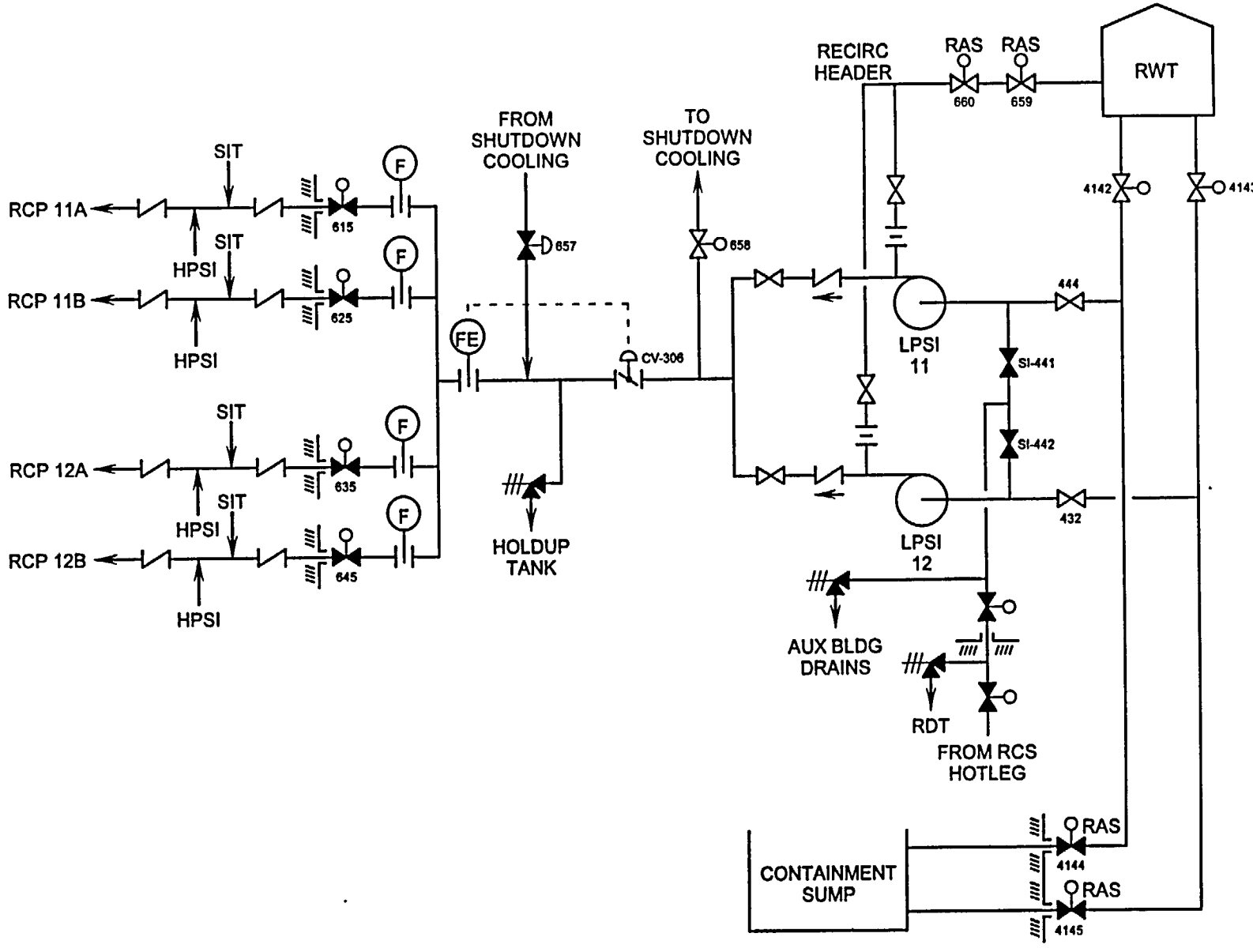


Figure 11.2-1 LPSI Flow Diagram

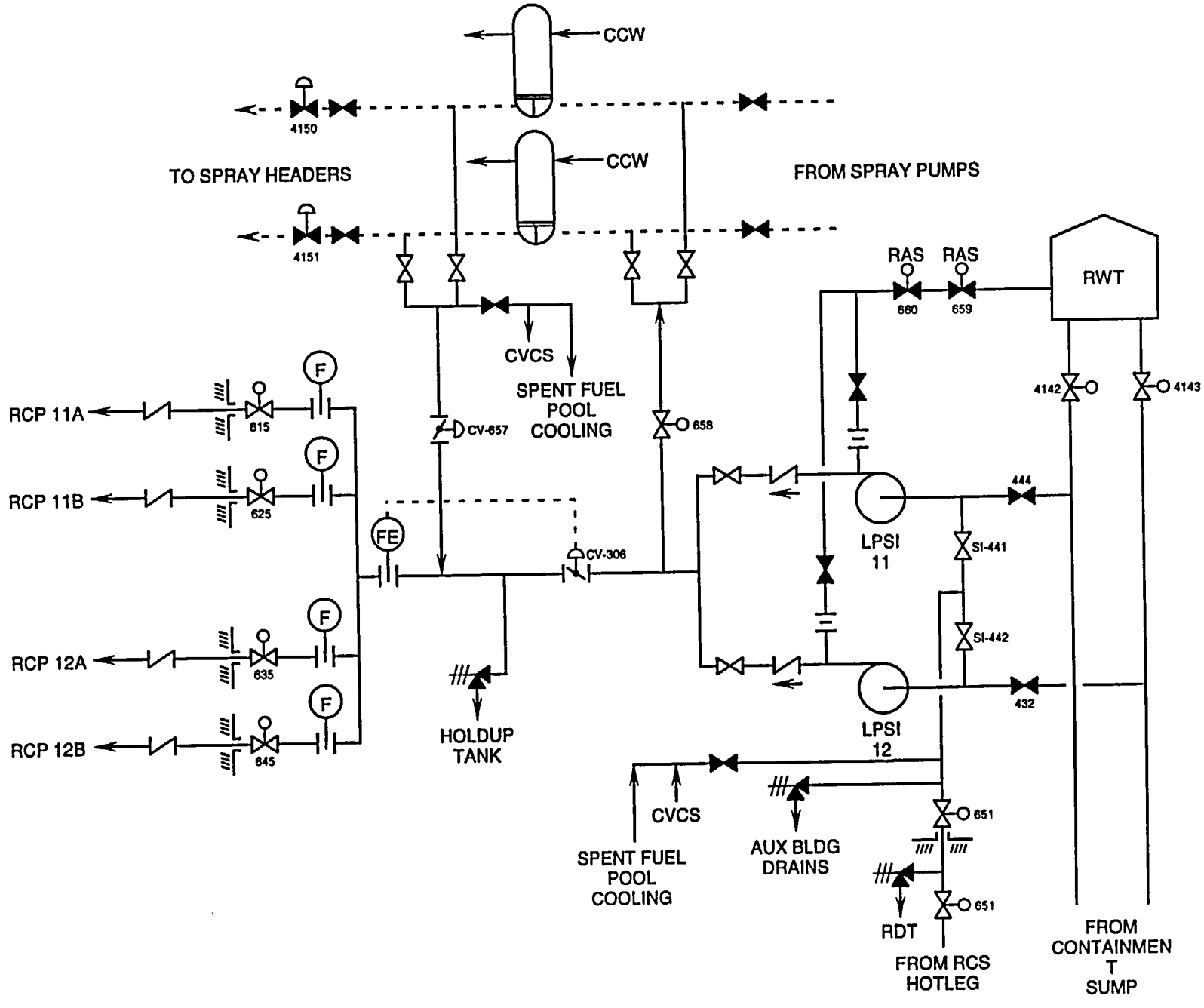


Figure 11.2-2 Shutdown Cooling Flow Diagram

1000-11

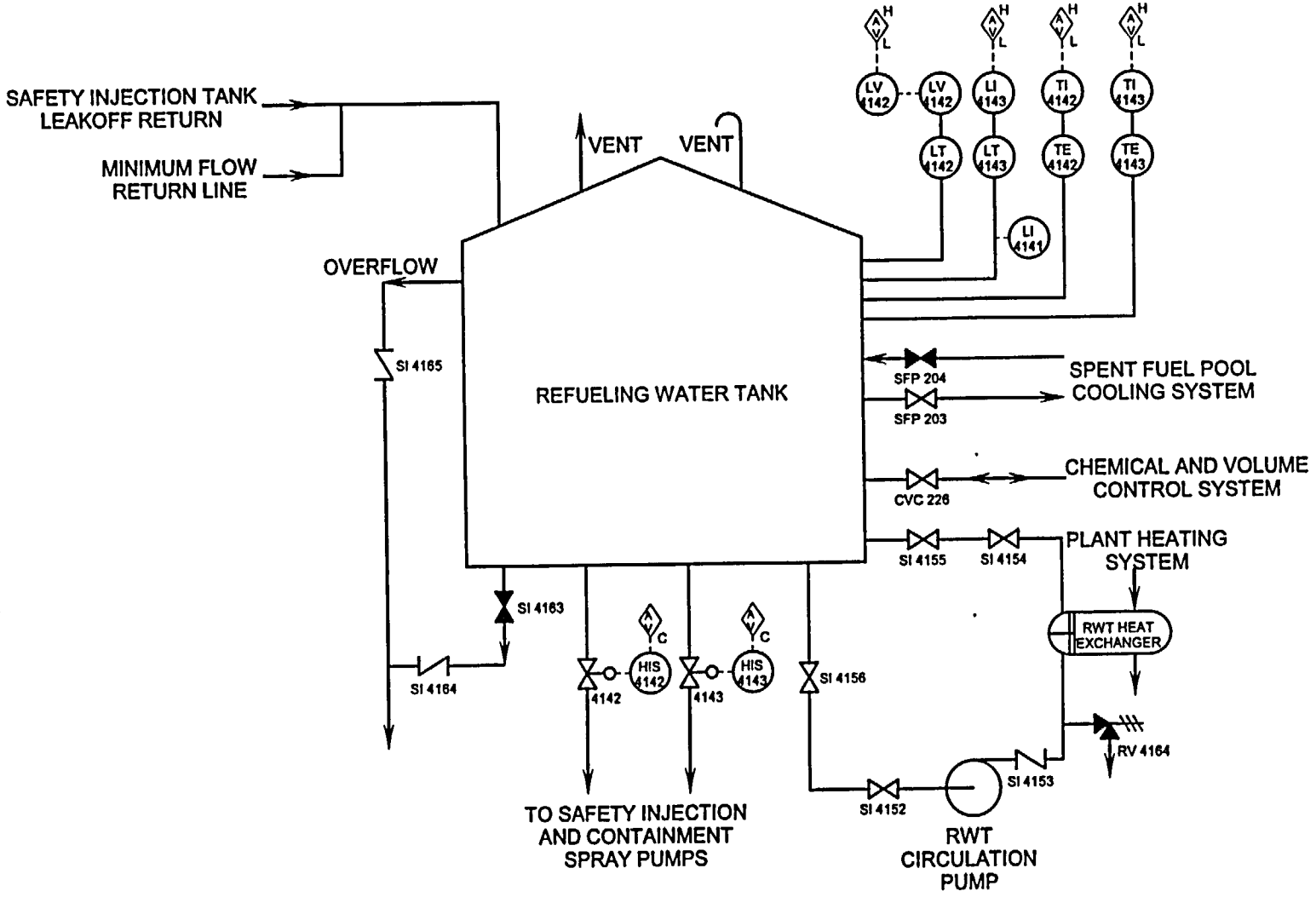


Figure 11.2-3 Refueling Water Tank

TABLE OF CONTENTS

11.3 INTEGRATED OPERATION OF THE EMERGENCY CORE COOLING SYSTEMS

LIST OF FIGURES

11.3 INTEGRATED OPERATION OF THE EMERGENCY CORE COOLING SYSTEMS

Learning Objectives:

1. Describe the operation of the emergency core cooling systems (ECCS) during the following operations:
   a. Injection phase
   b. Recirculation phase
2. State the purpose of the safety injection tanks (SIT).
3. List the order of ECCS injection during the following abnormal conditions:
   a. Inadvertent actuation at power
   b. Small break loss of coolant accident (slow depressurization)
   c. Large loss of coolant accident (LOCA)

11.3.1 Introduction

The purpose of the ECCS is to ensure that for any accident, up to and including the double ended rupture of the largest reactor coolant system pipe, the core will be re-flooded and cooled. These actions preclude fuel melting and minimizes the amount of cladding that will be damaged. This is accomplished by designing 100 percent capacity redundant components for the ECCS.

The following minimum number of components operating will protect the core:

1. One (1) high pressure safety injection (HPSI) pump,
2. One (1) low pressure safety injection (LPSI) pump,
3. One (1) emergency diesel generator and
4. Three (3) of the four (4) safety injection tanks (SITs).

11.3.2 System Description

The SITs as shown in Figure 11.3-1 are pressure vessels which contain borated water and are pressurized with nitrogen gas. The SITs are located inside the containment and are attached to the same injection piping used by the high pressure and the low pressure safety injection systems. The SITs are a passive system, meaning that it requires no automatic or operator action for this system to perform its intended function. Their function is to reflood and cover the core following a large LOCA.

11.3.3 Component Description

11.3.3.1 Safety Injection Tanks

There are four (4) SITs located inside the containment, each tank is constructed of carbon steel and internally clad with stainless steel to prevent corrosion. Each tank is typically 2000 cubic feet in size (16,000 gallons), and is approximately half filled with water. The water in these tanks is borated to 2500 ppm boron, and pressurized to 200 psig. The size of the SITs is based on the assumption that one (1) SIT dumps directly out the break leaving the remaining three (3) SITs to inject their contents into the cold legs and completely recover the core, until safety injection pumps can provide core cooling. The boron concentration is sufficient to maintain the core in a sub-critical condition following an accident.

Each SIT is supplied with a pressure relief valve which is set at 250 psig and discharges to the containment atmosphere to protect the SIT from over pressure. In addition, each SIT is

provided with the necessary valves and piping for filling, draining, venting, sampling, and adjusting the boron concentration. There are also redundant level and pressure instruments for each SIT in the control room to verify the technical specification limits on these tanks.

11.3.3.2 Safety Injection Tank Isolation Valves

Each SIT is connected to a reactor coolant system (RCS) loop cold leg through two (2) check valves in series. The check valves are normally held shut by the higher RCS pressure. When the RCS pressure drops below approximately 200 psig, the check valves open and the SITs discharge into the RCS. Each tank discharge line is equipped with a motor operated valve to isolate the tank from the RCS when the system is cooled down and depressurized. These valves are manually closed when the pressure in the RCS decreases to < 300 psig.

During a plant startup, the SIT discharge valves are manually opened when the pressure in the RCS reaches 250 psig; however, if these valves are inadvertently left closed, they will automatically open when the RCS pressure reaches 300 psig. After the valves are open, each valve is key locked to the open position on the control board and the supply breaker to its motor operator is opened. In addition, a safety injection actuation signal (SIAS) open command is provided to each valve during an accident.

11.3.4 System Operation

11.3.4.1 Integrated Operations

The operation of the ECCS (Figure 11.3-2) following a LOCA is divided into two (2) modes of operation, the injection phase and the recirculation phase. The injection phase is that time when the active components of the ECCS take a suction from the RWT and discharge into the RCS cold legs. This mode of operation will continue until the RWT reaches its low level setpoint.

When the refueling water tank reaches a low level condition a signal is sent to shift the active components from the injection phase to the recirculation phase, this signal is called the recirculation actuation signal (RAS). During the recirculation phase the mini flow recirculation valves receive a close signal and the LPSI pumps receive a stop signal. The HPSI pumps will continue to operate except that they now take a suction from the containment sump and return the fluid to the RCS and the core.

The sequence of events for a loss of coolant accident that results in a slow depressurization of the RCS is as follows:

1. As inventory is lost, letdown will be reduced to minimum and additional charging pumps will be placed in service by the pressurizer level control system,

2. Since the LOCA is larger than 132 gpm, pressurizer level will continue to decrease, and pressure will also drop,

3. More than likely, a reactor trip will be generated by the thermal margin low pressure (TMLP) reactor trip or possibly high containment building pressure,

4. A SIAS will be generated by low pressurizer pressure or high containment building pressure. The SIAS signal will start the charging pumps (if not already running), the HPSI pumps, and the LPSI pumps,

5. The SIAS signal is generated at 1740 psia. The shutoff head of the HPSI and LPSI pumps

is ~1300 and ~180 psia, respectively, ECCS flow is initially provided by the charging pumps,

6. As RCS pressure continues to decrease, flow from the HPSI pumps will begin when pressure is less than 1300 psia. When RCS pressure decreases to less than 200 psia, the SITs will begin to empty. Finally, the LPSI pumps will provide flow when RCS pressure decreases to less than 200 psia and

7. The charging pumps will be manually stopped when low level conditions are reached in the boric acid storage tanks. When a low level is reached in the RWT, a RAS will be generated. When the RAS is generated, the LPSI pumps will be tripped, and long term core cooling will be supplied by the HPSI pumps.

If a loss of offsite power occurs simultaneously with the LOCA, the sequence of events will be modified slightly. First, the charging pumps will not be powered (until the diesel-generator starts) and cannot respond to the decrease in pressurizer level. Next, the reactor trip will be caused by a loss of RCS flow because RCP power is lost. Finally, the diesel generator must start and its output breaker must close before charging and HPSI flows will be available. The timing of accident flows, with the exception of SIT flow, is dependent upon the sequencing of loads onto the vital 4160 Vac buses.

If a large break LOCA occurs, items 1 through 7 above happen in a much shorter time frame. If a large break LOCA and a loss of offsite power occur simultaneously, the SITs will probably empty before the diesel generators can start and energize the 4160 Vac buses.

11.3.4.2 Generic LOCA Considerations

The length of time that the ECCS is in the injection phase is dependent upon the size of the break and any operator action. The rate at which the volume of water is lost and the pressure reduction of the RCS is break size dependent and is analyzed in the FSAR. These analysis include various size small break LOCAs (SBLOCA) and the break of the largest piping in the RCS, normally called the large break LOCA (LBLOCA).

As documented in CEN-114, the designation of a particular break size, type , and location as the worst break must be accompanied by a list of assumptions. The assumptions may be on the specific plant design (SIT pressure), system performance (minimum HPSI flow), or system availability (number of HPSI pumps). Despite the fact that the worst break will change given a change in the assumptions, certain features of the break can be generalized and discussed independently of the individual assumptions.

With feedwater available (main feedwater until reactor trip and then auxiliary feedwater), the worst break falls within a narrow range of possibilities. For CE designed plants, the worst location has been the RCP discharge leg. This location results in the slowest depressurization and the least amount of liquid available for core cooling.

The small break spectrum from an Appendix K perspective, is bounded on the large end by the small/large break dividing point, typically taken to be 0.5 ft^2. For the larger break sizes in this range (0.1-0.5 ft^2), the core will uncover relatively early (the larger the break, the earlier the uncovery) but since the RCS depressurizes

quickly and completely, the SIT flow ensures a rapid recovering of the core. Due to the short uncovery duration, the fuel cladding has little time to heat up and consequently acceptable low clad temperatures result.

For intermediate break sizes (0.02 - 0.1 ft^2) the RCS does not depressurize to the SIT set point and if core uncovery occurs, recovery must be accomplished by the HPSI pumps alone. While these breaks uncover later than the larger breaks, the uncovery can be of a longer duration. As the break size decreases in this range, the core begins to uncover later, is of shallower depth, and may stay uncovered longer. For very small breaks (0.0 - 0.02 ft^2), the HPSI pumps are able to inject sufficient flow to prevent core uncovery, because the core heat generation rate has decayed to a point where the HPSI pumps are injecting at a rate exceeding core boil off before the core uncovers.

Since the very small breaks do not uncover the core, the clad temperature remains at a low value. As stated above, the larger breaks, due to rapid core uncovery also experience low clad temperatures. Therefore, the worst break size occurs in the intermediate range defined on the large end by SIT pressure and on the small end by core power (assumed decay heat generation rate) and HPSI pump performance. The worst break normally is the largest break in this range which relies on HPSI injection to terminate clad temperature rise). For plants with SIT pressure of 200 psi this break size is approximately 0.1ft^2 For plants with SIT pressure of 600 psi this break size is on the order of 0.05 ft^2. It is possible, given sufficient HPSI flow or low core power (best estimate) that these breaks may not experience any significant core uncovery. In this case, there would be no intermediate class of breaks and the worst break would have a significantly lower clad temperature and be one of the larger break sizes resulting in core uncovery.

There are two possible types of LOCAs associated with a loss of all feedwater (LOAF), those occurring concurrent with a LOAF, and those caused by the LOAF due to high RCS pressure. LOAF implies a loss of both main and auxiliary feedwater capability. For breaks > 0.02 ft^2 concurrent with a LOAF, the energy transferred to the secondary is insignificant and a loss of feedwater during the transient is of little consequence. These breaks result in similar system behavior with and without available feedwater.

As the break size decreases, (LOCA concurrent with LOAF) the availability of the steam generator as a heat sink becomes more important. For a range of break sizes, feedwater is beneficial but not necessary. Smaller breaks require feedwater to obtain acceptable results. For LOCAs caused by LOAF, feedwater is also a requirement. Therefore, to realistically define a worst break coupled with a LOAF, a criterion must be set to judge which is worst. The criterion chosen was the break which has a significant dependence on feedwater availability, and that requires initiation of auxiliary feedwater in the least amount of time to prevent core uncovery. An intermediate break size of 0.02 ft^2 is shown to have a significant dependence of feedwater availability and requires auxiliary feedwater flow be initiated at the earliest time after the break (< 1 hour).

11.3.4.3 Small Break Loss of Coolant Accident (SBLOCA)

The major concern with the SBLOCA is that it takes a long period of time for the pressure to decrease to a point where the ECCS will start to inject the cooling water to the core. The smaller the break, the longer it takes for the pressure to decay to the injection point. After the actuation signal is generated, all active components of the

ECCS will actuate assuming no failure of individual components. The HPSI pumps will start to inject and the LPSI pumps, which have started, will circulate water back to the RWT. As the pressure in the RCS slowly decays more and more flow from the HPSI will be injected into the RCS. However, water is continuing to flow out the break causing a net loss of reactor coolant. As pressure continues to drop the next component to inject will be the safety injection tanks at a pressure of less than 200 psig.

Since the break is not isolated, water inventory will continue to decrease and pressure will drop until the LPSI pumps start to inject. As described in this hypothetical accident it takes a certain amount of time for the different ECCS components to begin to inject their contents and replenish the loss of inventory from the RCS, which means a higher void fraction in the RCS

11.3.4.4 Large Break Loss of Coolant Accident (LBLOCA)

If a LBLOCA were to occur the first component to inject would be the SITs due to the fact that they are passive components and require no actuation signal or component to change position.

Assuming a concurrent loss of offsite power, the diesel generators would start and the high pressure safety injection and then the low pressure safety injection would be started. The injection phase will last for approximately 30 minutes when the recirculation actuation signal will actuate.

11.3.4.5 Abnormal Operations

If there was an inadvertent actuation of the SIAS when the plant was at power, the consequences would be minimal. All active components in the ECCS would actuate, but since the reactor coolant pressure is at or near 2200 psig, which is well above the discharge pressure of the HPSI or LPSI pumps, no water from the RWT will be injected into the RCS.

11.3.5 PRA Insights

Since the ECCS are required to mitigate the consequences of accidents, the failure of these systems during transients and accidents greatly increases the probability of core melt. In particular, the failure of the HPSI system in either the injection phase or the recirculation phase of operation is a major contributor to increases in core melt frequency. According to the Calvert Cliff's PRA, the HPSI system failure contribution to core melt frequency is 25%. Many of the failure sequences are caused by operator error.

The following sequences provide information on system failures and their consequences.

For certain small break sizes (< 1.9 inches in diameter), the proper operation of all ECCS components is very important. A scenario that increases core melt frequency is outlined below:

1. A LOCA occurs that results in the actuation of the ECCS,
2. All ECCS components function properly in the injection phase of the LOCA,
3. The RWT reaches a low level, but the switchover of the ECCS suctions to the containment sump is unsuccessful,
4. The failure of the sump suction lineup results in a loss of suction to the ECCS pumps, and no core cooling flow is available and
5. With no cooling flow, the core heats up and eventual melts.

The significant cut sets involve failure of pump seals or ECCS pump room cooling. For pump seal cooling, since only CCW heat exchanger #11 is normally in service, the most important recovery action is for the operator to manually open the discharge valve on CCW heat exchanger #12 in order to place it in operation. CCW seal cooling failure is assumed to fail the HPSI pumps as well as the LPSI and containment spray pumps. For pump room cooling, the operator can manually start the pump room coolers for local control faults. If the sump valves fail due to control faults, the operator can manually open the valves.

In a similar sequence, involving a SBLOCA, a failure of the HPSI system is considered such that no makeup is assumed in the injection phase of the accident.

This initiating event can be divided into two parts: RCP seal LOCAs ($2x10^{-2}$/yr) and other SBLOCAs ($1x10^{-3}$/yr). The other SBLOCA portion of the sequence is negligible when included with the failure probability of the HPSI system ($1.3x10^{-4}$) since the product result is less than $1x10^{-6}$. Work done by EG&G for the station blackout program indicates that for a leak of the maximum expected RCP seal LOCA (< 500 gpm), with secondary cooling available, approximately three (3) hours is available to isolate the leak or start primary makeup.

The dominant HPSI pump failure is attributed to the closure (fail close) of the valves in the common minimum flow recirculation line. This pump failure is due to the slow drop in primary pressure from 1600 to 1275 psi resulting in pump heat up and failure due to pumping against a shutoff head for a significant period of time (greater than 10 minutes). These minimum flow recirculation valves are common to all HPSI, LPSI and containment spray pumps.

Another sequence that illustrates the importance of the ECCS to risk is the intersystem or interfacing LOCA (also known as event V). In this sequence, a failure of both of the series check valves that separate the high pressure RCS from the low pressure systems is postulated. With the LPSI header motor-operated valves in an open position (operability test), the LPSI discharge piping is exposed to full RCS pressure. The discharge piping is over pressurized and fails. The largest risk achievement factors are associated with local faults for the minimum flow recirculation valves and the CCW valves. All had a risk achievement factor of 163. The risk reduction factors were negligible.

The failure results in a LOCA with some unique features. First, the LOCA is outside of the reactor building; therefore, the containment barrier is lost. Next, the assumed failure has the potential to also fail both trains of LPSI. Finally, the leakage from the RCS is not collected in the reactor building sump. When the refueling water tank empties, no cooling fluid is available for long term core cooling. With no cooling, the core overheats.

11.3.6 Summary

The purpose of the ECCS is to provide initial filling of the reactor vessel after a LOCA and to provide long term cooling of the core after the initial blow down of the RCS is over. The purpose of the SITs is to completely cover the core following a LBLOCA. The sizing and number of SITs is selected considering that one of the tanks spills its contents directly out the break, and the remaining three SITs inject into the cold legs and completely cover the core following a LBLOCA.

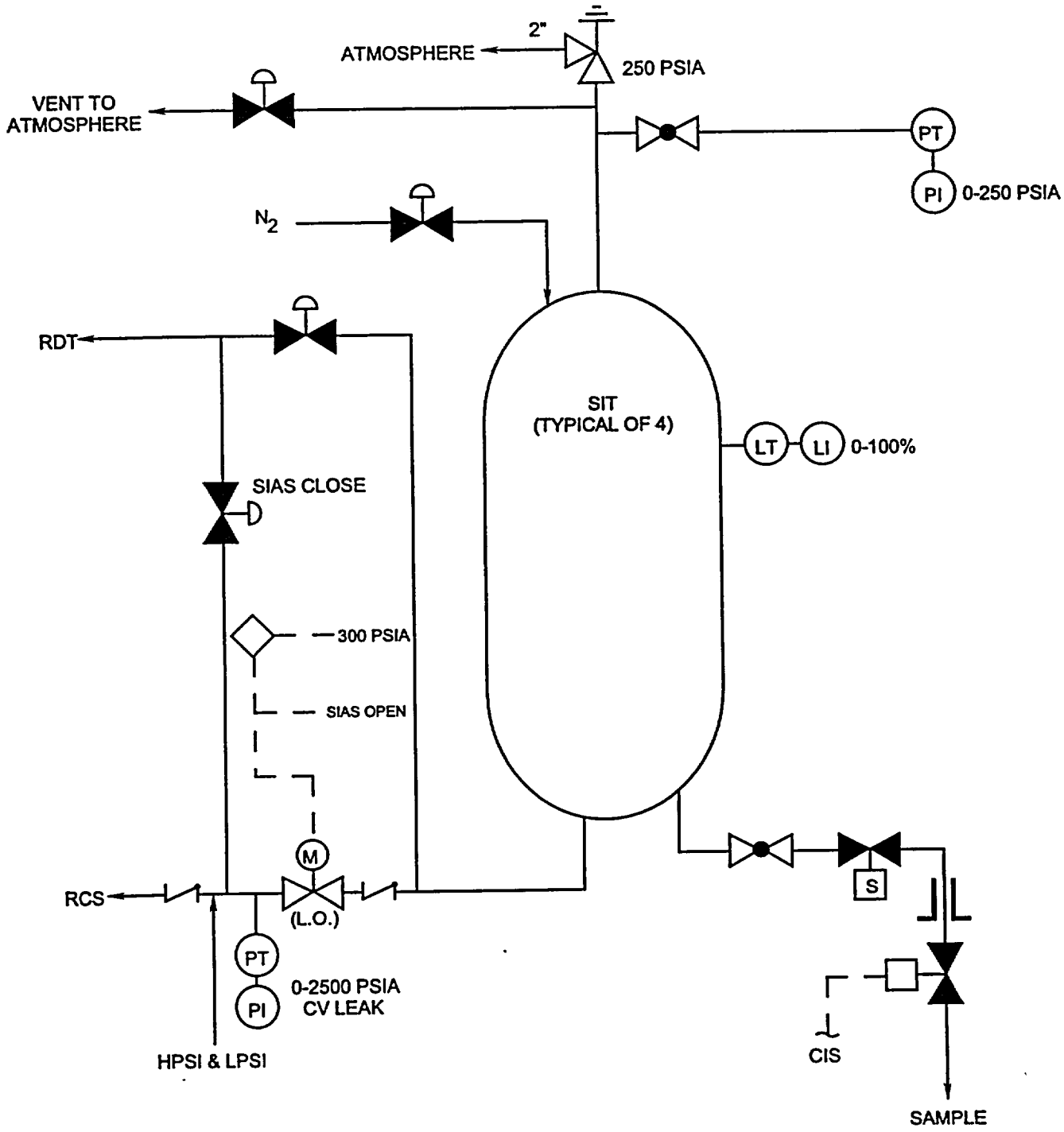


Figure 11.3-1 Safety Injection Tanks

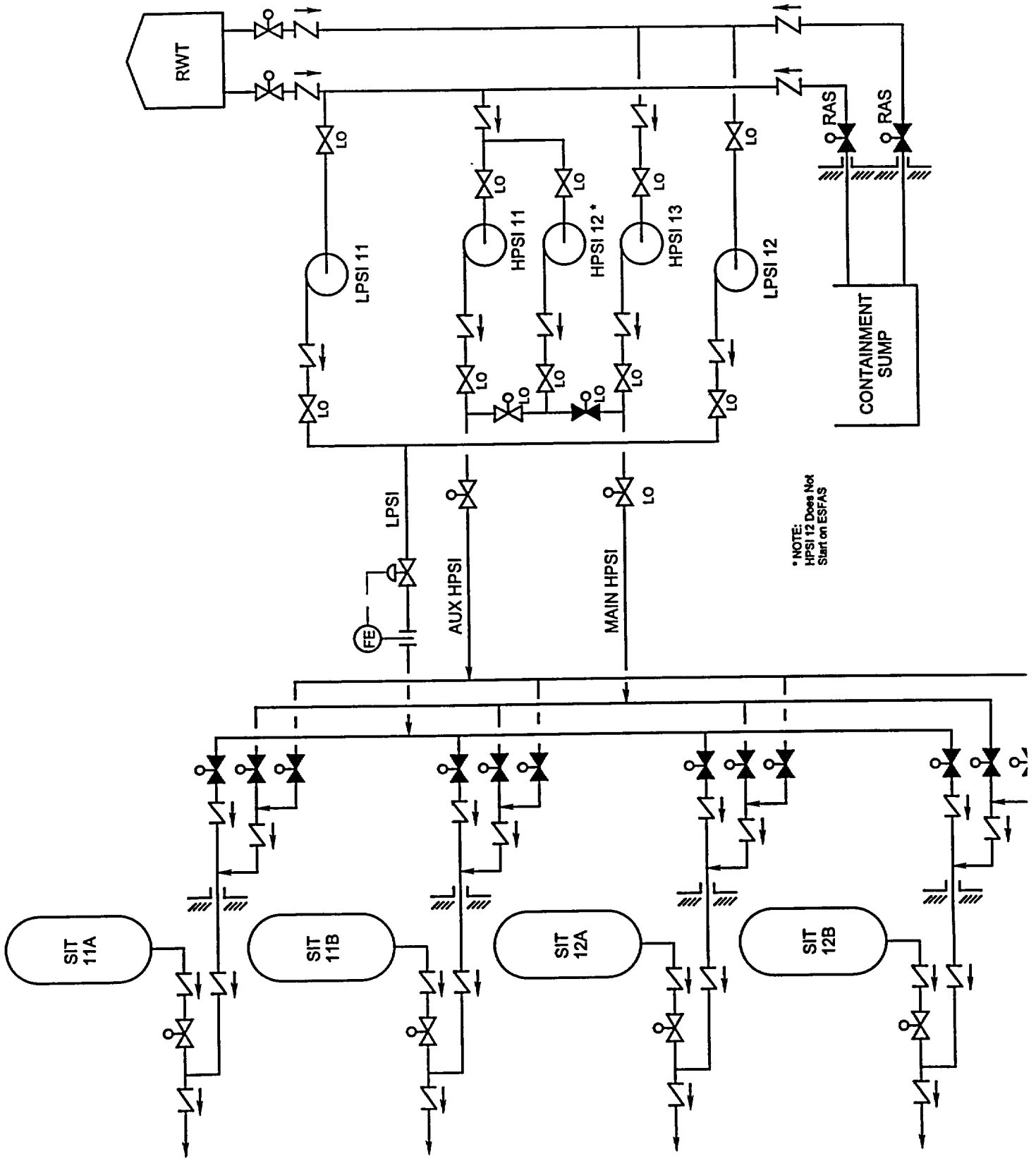


Figure 11.3-2 Emergency Core Cooling System

TABLE OF CONTENTS

11.4 CONTAINMENT SPRAY SYSTEM

LIST OF FIGURES

11.4 CONTAINMENT SPRAY SYSTEM

Learning Objectives:

1. State the purpose of the containment spray (CS) system.
2. List the sources of suction to the CS pumps.
3. Explain why trisodium phosphate (TSP) is added to the containment sump during a loss of coolant accident (LOCA).

11.4.1 Introduction

The CS system is an engineered safety features (ESF) system that maintains containment building integrity, helps to maintain containment sump pH neutrality, and cools the containment building recirculation sump water.

Containment integrity is assured by a reduction in building pressure. The reduction in containment building pressure is achieved by condensation of the steam released from the reactor coolant system (RCS) during a LOCA or from the steam generator during a main steam line break (MSLB) by the spray droplets from the containment spray nozzles.

Two safety benefits are realized by pressure reduction. The reduction in building pressure prevents the loss of the final barrier to the release of radioactive fission products to the public, and a pressure reduction also reduces the driving force for radioactive containment building leakage.

The addition of TSP to the containment sump following a LOCA maintains sump pH approximately equal to 7.0. This value aids in the prevention of stress corrosion cracking of metals during the operation of the safety injection systems.

Finally, the shutdown cooling heat exchangers are normally aligned to the CS pump discharges. During the recirculation phase of the LOCA, the hot sump water is discharged through the heat exchangers for cooling purposes.

11.4.2 System Description (Figure 11.4-1)

The CS system consists of two (2) redundant trains with each train containing a spray pump, shutdown cooling heat exchanger, spray nozzles and associated valves. A containment spray actuation system (CSAS) actuates the system when containment pressure exceeds the high-high set point of four and one-quarter (4.25) psig.

Two (2) suction sources are available to the CS pumps. The first suction source is the refueling water tank (RWT) that provides borated water to the pumps during the injection phase of an accident. When the RWT reaches a low level (30 in.), a recirculation actuation signal (RAS) is generated. This signal automatically transfers the suction of the spray pumps from the RWT to the containment sump. Regardless of the suction source, the CS pumps discharge to the containment spray headers via the shutdown cooling heat exchangers.

The shutdown cooling heat exchangers are installed on the discharge of the CS pumps to cool the hot recirculation water from the sump. The heat exchangers are cooled by the component cooling water system (CCW). The motor operated CCW supply valves are automatically opened when a safety injection actuation signal (SIAS) is actuated. Cool water from the heat exchangers then travels to the spray headers.

The flow of spray fluid to the spray headers is controlled by isolation valves that are automatically opened by a SIAS signal. When the valves open, spray water travels to the spray nozzles located in the containment building dome. The nozzles divide the spray fluid into small droplets which fall through the containment building atmosphere to the building sump. The CS system is redundant to the containment cooling system.

11.4.3 Component Description

11.4.3.1 Containment Spray Pumps

The CS pumps, manufactured by Byron Jackson, are single-stage, horizontal, centrifugal pumps. They have mechanical seals backed up with an auxiliary gland. Each pump is driven through a coupling by a 200 hp, 4160 Vac induction motor. CS pump 11 receives power from 4 kV unit bus 11, while CS pump 12 receives power from 4 kV unit bus 14. Both CS pumps start automatically when a CSAS is generated. Four (4) pressure detectors sense containment pressure separate from the pressure detectors used to generate a SIAS.

Each pump has a capacity of 1400 gpm in the injection mode of operation, and 1630 gpm in the recirculation mode. The minimum allowable flow for a CS pump is 50 gpm. In the injection mode of operation, the CS pumps must discharge against containment pressure, while in the recirculation mode the CS pumps take a suction from the containment building and thus do not have to pump against containment pressure. This reduced back pressure results in the higher spray pump capacity in the recirculation mode.

The pumps are provided with minimum flow recirculation lines which permit a flow of 50 gpm from each pump to recirculate back to the RWT during the injection mode of operation. The recirculation path is isolated upon the receipt of a RAS signal. The A pump is powered from the A emergency diesel bus while the B pump is powered from the redundant B emergency diesel bus.

11.4.3.2 Shutdown Cooling Heat Exchanger

There are two (2) shutdown cooling (SDC) heat exchangers in each unit. They are used to remove core decay heat and reactor coolant sensible heat during plant cooldowns and cold shutdown conditions. The heat exchangers also cool the containment spray water during containment spray system operations.

The SDC heat exchangers have a U-tube design with two (2) tube side passes and one (1) shell side pass. CCW passes through the shell side, while the tube side water is from the safety injection and, or, CS system. The tubes are stainless steel and the shell is carbon steel. The heat exchangers are located in the emergency core cooling system (ECCS) pump room of the same corresponding ECCS train's pump.

Each heat exchanger is protected against over pressurization on the tube side by a relief valve located on the recirculation line from the heat exchanger outlet back to the high pressure safety injection (HPSI) pump suction. Both relief valves have a set point of 500 psig, and are sized to accommodate the pressure developed due to a sudden temperature increase of the heat exchanger contents. The worst thermal transient considered is expected to occur at the beginning of containment spray recirculation with water temperature changing from 40°F to 276°F in 10 seconds.

Each heat exchanger is sized to maintain a refueling water temperature of 130°F or less, 27

1/2 hours after reactor shutdown, assuming the core has operated at its design power for an infinite duration. This feature also assumes the CCW supplied to the heat exchanger is at its maximum design temperature of 95°F. The heat removal capacity of the containment spray system is 240 million Btu per hour. The maximum system heat load, which occurs 70 seconds after the start of a LOCA, is 237 million Btu per hour.

11.4.3.3 Trisodium Phosphate Baskets

Three (3) baskets located on the containment floor contain the dry TSP. Containment spray water and, or, safety injection water on the containment floor dissolves the TSP and carries it through the containment spray and safety injection systems. The TSP, in solution, changes the pH of the water from approximately five (5.0, acidic) to seven (7.0, neutral). This neutralization of the water minimizes stress corrosion cracking of certain materials in the safety injection system.

The TSP baskets are located approximately six (6) inches above the containment floor, at approximately 120 degree intervals. Each basket is five (5) feet wide by five (5) feet long and 18 inches in height. The basket has a solid top and bottom, with stainless steel mesh screen sides. The safety injection and containment spray water dissolves the TSP as the water rises above the containment floor. Mixing of the TSP occurs as the solution is continuously recirculated. Technical specifications require a minimum of 100 cubic feet of TSP be contained within the three (3) TSP baskets.

11.4.3.4 Containment Spray Headers

Each containment spray header contains 90 nozzles, each of which is capable of a design flow of 15.2 gpm. The nozzles produce a mass equivalent drop size of approximately 700 microns at rated system conditions.

The spray headers are installed in the top of the containment building dome in concentric circles. Each of the circles is supplied from a separate CS train in an alternating fashion allowing complete coverage of the building in the event of a single CS pump failure.

The spray header isolation valves are normally shut, and open automatically when a SIAS is generated by the ESFAS. The spray header isolation valves open only on a SIAS to prevent an inadvertent actuation of the CS system in the event of an undesired actuation of the CSAS. The spray header isolation valves fail in the open position on loss of power or air. While the isolation valves are open, containment isolation is maintained by check valves in the spray header on either side of the containment building.

Each containment spray header has a connecting line which directs spray water to the containment iodine removal filter units. The spray water is used to douse the charcoal filter beds in the filter units, in the event decay heat causes the charcoal filter temperature to rise above 300°F. A solenoid operated isolation valve in the connecting line to the spray header is used to send spray water to the iodine removal filter units. These isolation valves are controlled by hand switches from the control room. Once the charcoal filter high temperature condition has cleared, the filter dousing is stopped.

11.4.4 Containment Spray System Design Basis

The Containment Spray System is designed to provide sufficient heat removal capability to maintain the containment pressure and temperature below their design values, in the

event of a Loss of Coolant Accident or Main Steam Line Break Accident.

The Containment Spray System is redundant with the Containment Air Cooling System. Any of the following combinations of the two system's equipment provides sufficient heat removal capability to maintain the post-accident containment pressure and temperature below their design values:

1) Two containment spray pumps provide 100% cooling capacity,

2) One containment spray pump and two (out of four) containment air cooling units provide greater than 100% cooling capacity, and

3) Three (out of four) containment air cooling units provide 100% cooling capacity.

The heat removal capacity of the Containment Spray System is sufficient to overcome the design maximum heat load occurring in the containment building seventy (70) seconds after the start of a Loss of Coolant Accident.

11.4.5 System Operations

Normally, the CS system is in a standby mode of operation with none of its equipment in service. Two different conditions can change the status of the spray system. The first condition is the receipt of a CSAS, a SIAS, and (later during the accident) a RAS signal. The second occurrence is a cooldown of the RCS which involves the use of the shutdown cooling heat exchangers.

11.4.5.1 Injection Mode

Following an accident which results in a CSAS being generated by the ESFAS, the two (2) containment spray pumps automatically start. This mode of system operation is called the injection mode. The CS pumps take a suction on the RWT through two outlet lines from the RWT. Each CS pump discharges borated water to one SDC heat exchanger where it is cooled by CCW. Each SDC heat exchanger sends the cooled water to a separate containment spray header whose isolation valves should have opened on a SIAS signal which would have occurred prior to the CSAS signal.

Each spray header terminates in a separate circular ring which sprays the borated water into the containment atmosphere. The cool spray drops absorb heat from the containment atmosphere, and thus reduce the containment pressure and temperature. The spray water falls to the containment floor where it collects in the containment sump.

11.4.5.2 Recirculation Mode

When the RWT level reaches a low level setpoint of 30 inches, the ESFAS generates a RAS, which initiates the recirculation mode of containment spray operation. Upon receipt of a RAS, the two (2) containment sump isolation valves open, and containment sump water is recirculated by the CS pumps through the SDC heat exchanger and back into containment as spray. Once initiated, recirculation continues until terminated or modified by operator action.

11.4.5.3 Shutdown Cooling Mode

During shutdown cooling operations, the discharge of the low pressure safety injection (LPSI) pumps is routed to the SDC heat exchangers. In order to prevent inadvertent containment building spray downs with

radioactive RCS water the following changes are made to the spray system:

1. The spray headers are isolated and

2. The CS pump stopcheck valves are closed and the pump breakers are racked down.

The CS and LPSI systems are returned to their normal alignment during the plant heatup.

11.4.6 PRA Insights

The CS system is used to remove heat from the containment following a high energy fluid break (steam, feed, or primary) into the containment. Many PRA studies consider the failure of the containment and subsequent release of fission products to the public. If the CS system fails, then the pressure reduction and scavenging functions are lost. If the fan coolers are also inoperable, containment pressure can exceed design pressure, and containment failure can occur.

Probable causes of a loss of CS systems include failure of the motor operated suction valves, closed manual valves in the suction lines, loss of ac power supplies, failure of the CS pumps to start and failure of the CS pumps to run after starting. It should be noted that the suction lines to the CS pumps are also utilized by the HPSI and LPSI systems. Therefore, a loss of suction to the spray pumps could also affect the ECCS pumps.

NUREG-1150 studies on importance measures have shown that the containment spray system is not a contributor to either risk achievement or risk reduction.

11.4.7 Summary

The CS system maintains the containment fission product barrier by reducing containment pressure following a LOCA or steam line break. In addition, the system cools the containment sump water during the recirculation phase of a LOCA. Trisodium phosphate is added to the containment sump to maintain sump pH within assumptions used to prevent stress corrosion cracking. The system is actuated by two (2) out of four (4) high-high containment building pressure signals.

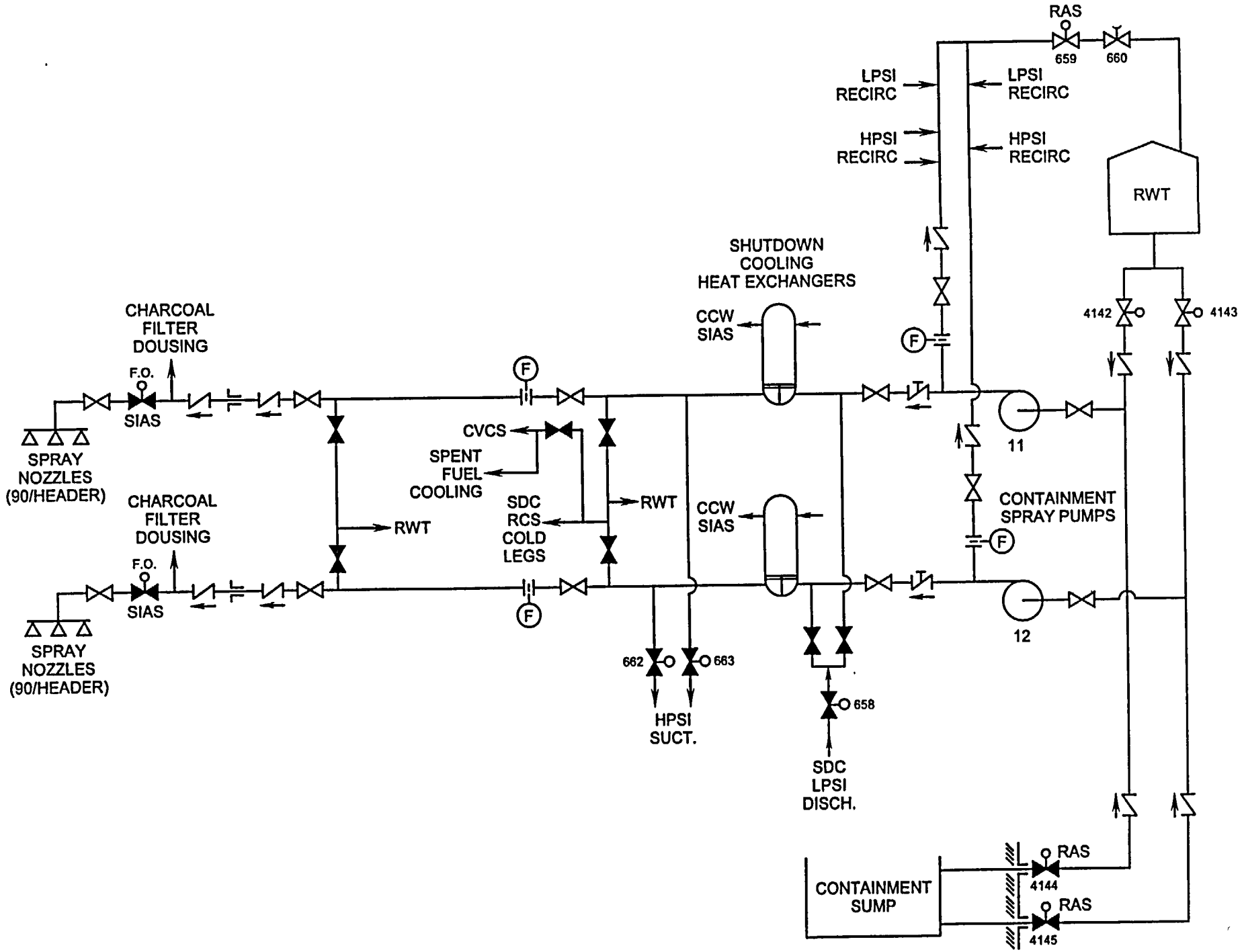


Figure 11.4-1 Containment Spray System

1201-11

TABLE OF CONTENTS

11.5 AUXILIARY FEEDWATER SYSTEM

LIST OF TABLES

LIST OF FIGURES

11.5 AUXILIARY FEEDWATER SYSTEM

Learning Objectives:

1. State the purposes of the auxiliary feedwater system (AFW) System.
2. List all suction sources for the AFW pumps and under what conditions each is used.
3. List the steam supplies to the AFW turbines.
4. State the purpose of the auxiliary feedwater actuation system (AFAS) block signal.
5. List the automatic start signal(s) for the AFW system.
6. Explain how decay heat is removed following a plant trip and loss of off-site power.
7. Explain the bases for a minimum volume of water in the condensate storage tank (CST).

11.5.1 Introduction

The AFW system is a safety-related system that maintains an inventory in the secondary side of the steam generators to ensure a heat sink for the removal of reactor decay heat. The AFW system provides feedwater to the steam generators during normal conditions, emergency conditions, and during cool down of the primary plant in the event that the main feedwater system is inoperative. Also, the AFW system is used to maintain steam generator levels during plant start-ups and shutdowns.

11.5.2 System Description (Figures 11.5-1, 11.5-2)

The major components of the AFW system are CST 12, two (2) turbine driven AFW pumps, one (1) motor driven AFW pump, eight (8) AFW blocking valves, four (4) AFW flow control valves, and associated piping. During normal plant operation, the AFW system is maintained in a standby mode with its components lined up for automatic actuation.

The AFW pumps take a suction on CST 12 and discharge to four (4) AFW lines. Two (2) AFW lines receive water from the turbine driven pumps, and two (2) AFW lines receive water from the motor driven pump. Each AFW line has two (2) blocking valves in series, followed by a flow control valve. The flow control valves are used to regulate the AFW flow to the steam generators.

After the flow control valves, each motor AFW line connects with a turbine AFW line to send auxiliary feedwater to one (1) steam generator. The AFW flowing into each steam generator maintains level in the steam generator and allows removal of decay heat and cool down of the reactor coolant system (RCS).

The purpose of the two (2) blocking valves in each AFW line is to isolate AFW flow to a steam generator when a rupture has occurred in the steam generator. The four (4) blocking valves for one steam generator shut automatically when an AFAS block signal is generated for that steam generator.

The AFW system can also be used to supply feedwater to the steam generators during a normal plant cool down. In this mode of operation, the AFW system is manually started and supplies feedwater to the steam generators for RCS cool down. The turbine driven AFW pumps are used during plant cool down. The motor driven pump is reserved for emergency use only.

Two (2) cross-connect lines are provided between the unit 1 and unit 2 motor driven AFW pumps discharge lines. The cross-connect lines allow the motor driven AFW pump in one unit to supply feedwater to the AFW system in the other unit, in the event of an AFW system failure. Each cross-connect line has a normally shut, remotely operated, isolation valve.

The two (2) AFW pump turbines are supplied by steam from either the main steam system or the auxiliary steam system. The turbines are normally driven by steam from the steam generators, but the auxiliary boilers can be used as an alternate steam supply. The AFW pump turbines are non-condensing, and exhaust directly to atmosphere. The turbine steam supply line from each steam generator has a steam supply valve which is normally shut. The two steam supply valves open automatically when an AFAS start signal is generated.

11.5.3 Component Description

11.5.3.1 AFAS

The function of the AFAS is to automatically start the AFW system upon low steam generator level, to identify a ruptured steam generator and block AFW flow to the ruptured steam generator.

The AFAS consists of four (4) sensor subsystems and two (2) actuation subsystems. The four (4) sensor subsystems monitor redundant and independent parameters in the steam generators. The subsystems trip when the parameters reach their set points. The two (2) actuation subsystems monitor the four (4) sensor subsystem outputs and, through coincidence logic, determine whether protective action is required.

The AFAS monitors four (4) channels of wide range level indication for each steam generator. When either steam generator has at least two (2) out of four (4) level indication channels at or below the low level setpoint (37%), an AFAS start signal is generated on both actuation channels. The AFAS start signal automatically initiates operation of the AFW system to maintain proper steam generator water inventory.

The AFAS also monitors four (4) channels of pressure indication for each steam generator. Each steam generator pressure channel is compared with its corresponding channel from the other steam generator. Four (4) differential pressure channels are thus produced for each steam generator. An AFAS block signal is generated for an individual steam generator when at least two (2) out of four (4) differential pressure channels indicates that the opposite steam generator pressure exceeds the given steam generator pressure by 115 psig.

The AFAS block signal prevents continued feedwater addition to a ruptured steam generator. Feedwater isolation is important for two reasons. First, the addition of feedwater continues the RCS cool down and its associated positive reactivity addition. Second, the feedwater flashes to steam and adds energy to the containment building. An unisolable steam break is terminated by boiling the affected steam generator dry. Only those valves on the affected steam generator are closed, while the unaffected generator is maintained at the proper level for decay heat removal by the AFW System.

11.5.3.2 Condensate Storage Tanks

The AFW pumps can receive a suction from either of three (3) CSTs. Normally both units are lined up to take suction on the number 12 CST.

The purpose of CST 12 is to provide a source of feedwater for unit 1 and unit 2 AFW systems.

The tank has a capacity of 350,000 gallons and is protected against tornadoes and tornado-generated missiles by a seismic class I concrete structure.

CSTs 11 and 21 are normally lined up to the condensate system in their respective units. If CST 12 is unable to supply water to the two AFW systems, then CSTs 11 and 21 can be lined up to supply the AFW system of their respective unit.

The CST supply is the preferred source of emergency feedwater to the steam generators because of its purity. Plant technical specifications require a minimum volume of 150,000 gallons of condensate quality water to be available for the AFW system. The minimum water volume ensures that a sufficient heat sink is available to maintain the RCS in a hot standby condition for six hours while dumping steam to the atmosphere through the safety valves or atmospheric dumps with a concurrent and total loss of offsite power.

In addition to its emergency function, the CST also supplies water to the AFW pumps during portions of a plant heat up. Water from the CST will be used as the suction source until plant power has been escalated to 5%. At this point, at least one main feedwater pump is operating and the AFW steam generator supply is not required. Above 5%, the AFW system is aligned to its emergency system lineup with CST 12 as its suction source.

An additional source of AFW can be supplied from the opposite unit through a cross-connect to the motor driven pump discharge lines. A last means of AFW supply can be taken from the plant fire main system to the suction of the motor driven pump. Of course, this low quality water should only be used as a last resort.

11.5.3.3 Electric Driven AFW Pump (Table 11.5-1)

The electric driven AFW pump is a multi-stage, horizontal centrifugal pump powered from the class 1E electrical distribution system. The pump has a design flow rate of 450 gpm. A minimum flow of 140 gpm through the pump is required for proper pump cooling. The recirculation path is controlled by an automatic recirculation valve to provide a flow of 140 gpm, a portion of which is returned to the suction of the pump; the remaining recirculation flow is returned through a common AFW recirculation line back to CST 12. The automatic recirculation valves also act as check valves to prevent reverse flow.

The electric motor is a 500 hp, 4000 Vac, induction motor powered from the 4.16 kVac unit bus 11.

11.5.3.4 Turbine Driven AFW Pump (Table 11.5-2)

The steam driven pump turbine is a single stage, solid wheel, non-condensing unit rated at 600 hp at 3990 rpm. The turbine, manufactured by the Terry Steam Turbine Company, is designed for variable speed operation and is equipped with an electro-hydraulic actuator for speed control, an over speed trip mechanism, and an integral trip throttle valve. The turbine is designed for rapid starting and will operate with steam pressures as low as 50 psig. The turbine is normally supplied from the main steam system but may also be supplied from the auxiliary steam system for start-up and shutdown operations.

The AFW pump turbine exhausts to the atmosphere via individual exhaust pipes to the top of the auxiliary building roof. All valves in the steam supplies to the turbine are powered from the instrument air system to ensure operability during

a complete loss of ac power. Turbine speed is manually controlled by a hand indicating controller (HIC) in the main control room.

The pumps that are driven by the AFW pump turbines are six stage, horizontal, centrifugal pumps manufactured by Byron Jackson. Each has a rated capacity of 700 gpm. A minimum flow of 80 gpm through each pump is required to ensure proper pump cooling. A recirculation line is provided for each pump to ensure that the minimum flow is met. A portion of the pump's discharge passes through the recirculation line back to CST 12. A flow orifice in each recirculation line is sized to pass the minimum allowable flow.

11.5.4 Small Break LOCA

The characteristics of a small break loss of coolant accident (SBLOCA) are different from a large break loss of coolant accident (LBLOCA).

In the LBLOCA, the RCS flashes to steam and depressurizes through the break very rapidly. The decrease in RCS pressure actuates the engineered safety features (ESF) equipment and allows the safety injection tanks (SITs) to reflood the core. After the core is reflooded, the flow from the high pressure safety injection (HPSI) pumps and the low pressure safety injection (LPSI) pumps removes the core's decay heat. The availability of the AFW system during a large break is not important. However, AFW is vital for core safety, if a SBLOCA occurs.

Consider the following SBLOCA scenario without the availability of AFW:

1. The SBLOCA causes a slow depressurization of the RCS,
2. The depressurization causes the formation of steam in the RCS,
3. The ESF equipment is actuated, but will not pump into the RCS until its pressure is below the shutoff head of the injection pumps. The SITs will not provide water to reflood the core,
4. When RCS pressure decreases to approximately 1400 psig, the HPSI pumps will start to pump into the core. However, the flow rate may be insufficient for decay heat removal,
5. A heat up of the core will begin. Since the RCS is in a saturated condition, its pressure will also increase and
6. When pressure exceeds the shutoff head of the HPSI pumps, core cooling stops and severe core damage can result.

If the AFW system is available, then the above scenario will not occur. With AFW, the steam generators are available for decay heat removal. This heat removal coupled with HPSI flow will prevent core damage.

11.5.5 PRA Insights

The proper operation of the AFW system is important for the prevention of core melt in pressurized water reactors. According to the Calvert Cliffs PRA, the system contribution to core melt frequency is 32%. The following sequences illustrate the importance of the AFW system.

The sequence starts with a transient that results in a loss of both of the main feedwater pumps or a similar event that causes a loss of

feedwater flow. If the AFW system fails, then decay heat removal is lost. The loss of decay heat removal will result in a heat up of the RCS. The RCS heat up causes a decrease in RCS density and a large insurge into the pressurizer. As pressurizer level increases, the RCS pressure will increase. When the set point for the power-operated relief valves (PORVs) is reached, the valves will open. If the PORVs fail to close (or cycle open and close), then a LOCA will result. All that is needed for core melt in this sequence is a failure of the HPSI system to deliver proper flow. Calculations performed by EG&G for station blackout indicate that approximately 86 minutes are available to start an AFW pump in order to prevent core uncovery.

In the Calvert Cliffs PRA, no credit was given for the possible use of primary feed and bleed. There are two questions about the feasibility of using this method. First, the thermal-hydraulic consideration that, due to the low shutoff head of the HPSI pumps, it may not be possible to reduce the pressure sufficiently by opening the PORVs within the short time available (~10 minutes) to initiate feed and bleed. Second, at the time of the PRA, Calvert Cliffs had no procedures for performing this action. The action requires the removal of two trip units from the RPS to de-energize bistables in order to keep the PORVs continuously open.

As a result of design changes in the AFW system, a motor-driven AFW pump has been added to each unit at Calvert Cliffs. These motor-driven pumps can each cross feed the other unit and supply sufficient water to cool down the plant. The actions required can be performed in the control room. The necessary actions require recovering AFW by either:

1. Starting, an assumed locked out, AFW pump 12,
2. Realign AFW pump 11 from test,
3. Recover offsite power (if lost) or
4. Cross feed from unit 2.

The risk reduction factors associated with the AFW system are relatively low, with the highest value (1.09) being a local fault (or maintenance) effecting the 11 turbine-driven AFW pump. The risk achievement factor, associated with a local fault of the condensate storage tank suction valve for the 12 AFW pump, was 601.

Failure to deliver auxiliary feedwater to the steam generators can be caused by many different failure modes. From the description of the system in this section, a common mode failure is required for total system inoperability. One such common mode failure could occur if the AFW isolation valves were incorrectly adjusted and could not open properly. A second common mode failure that has been observed at operating PWRs is the leakage of the check valves in the supply lines to the steam generators. Hot fluid from the steam generators leaks through the check valves and into the pump casings (assuming that the isolation valves are open and the pump discharge check valve also leaks). When the pump starts, it quickly becomes vapor bound and cavitates. Of course, when the pump cavitates, flow is not available from the pump.

11.5.6 Summary

The AFW system is a fully qualified safety system designed to provide feedwater to the steam generators to maintain decay heat removal capabilities. The design basis assumes that the main feedwater system and/or the condensate system is inoperative, due to a total loss of offsite power or other system failure. In addition, the AFW system is used to supply normal feedwater

to the steam generators during plant start-ups and shutdowns.

The AFW system is designed to maintain its functional capability in the event of a steam generator rupture and/or a single active failure in an AFW system component.

The minimum required flow to ensure adequate RCS decay heat removal can be supplied by any one (1) of the three (3) AFW pumps.The pumps normally receive water from CST 12 but can also receive water from CSTs 11 or 21.

Control of AFW flow is accomplished by control valves in the pump supply. The AFW valves and pumps are controlled by the AFAS.

TABLE 11.5-1

Motor Driven AFW Pump Design Parameters

Pump	
Quantity	1
Type	Eight-stage, horizontal, centrifugal, split case
Manufacturer	Ingersol - Rand
Capacity	450 gpm
Minimum flow	140 gpm
Head	2800 feet
Design pressure	1800 psig
Design temperature	110 °F
Motor	
Quantity	1
Type	Two pole, squirrel cage induction
Manufacturer	Westinghouse
Horsepower	500 hp
Speed	3560 rpm
Power	4.16 kVac, 3 phase, 60 Hz.

Table 11.5-2

Turbine Driven AFW Pump Design Characteristics

Pump

Quantity	2
Type	Six-stage, horizontal, centrifugal, split case
Manufacturer	Byron Jackson Division, Borg Warner Corporation
Capacity	700 gpm
Minimum flow	80 gpm
Head	2490 feet

Turbine

Quantity	2
Type	Single-stage, non-condensing
Manufacturer	Terry Steam Turbine Company
Overspeed trip	5250 rpm
Horsepower	80 hp - 600 hp
Speed	2000 rpm - 3990 rpm
Inlet steam pressure	64 psia - 1000 psia
Backpressure	17 psia - 25 psia
Inlet temperature	300 °F - 545 °F

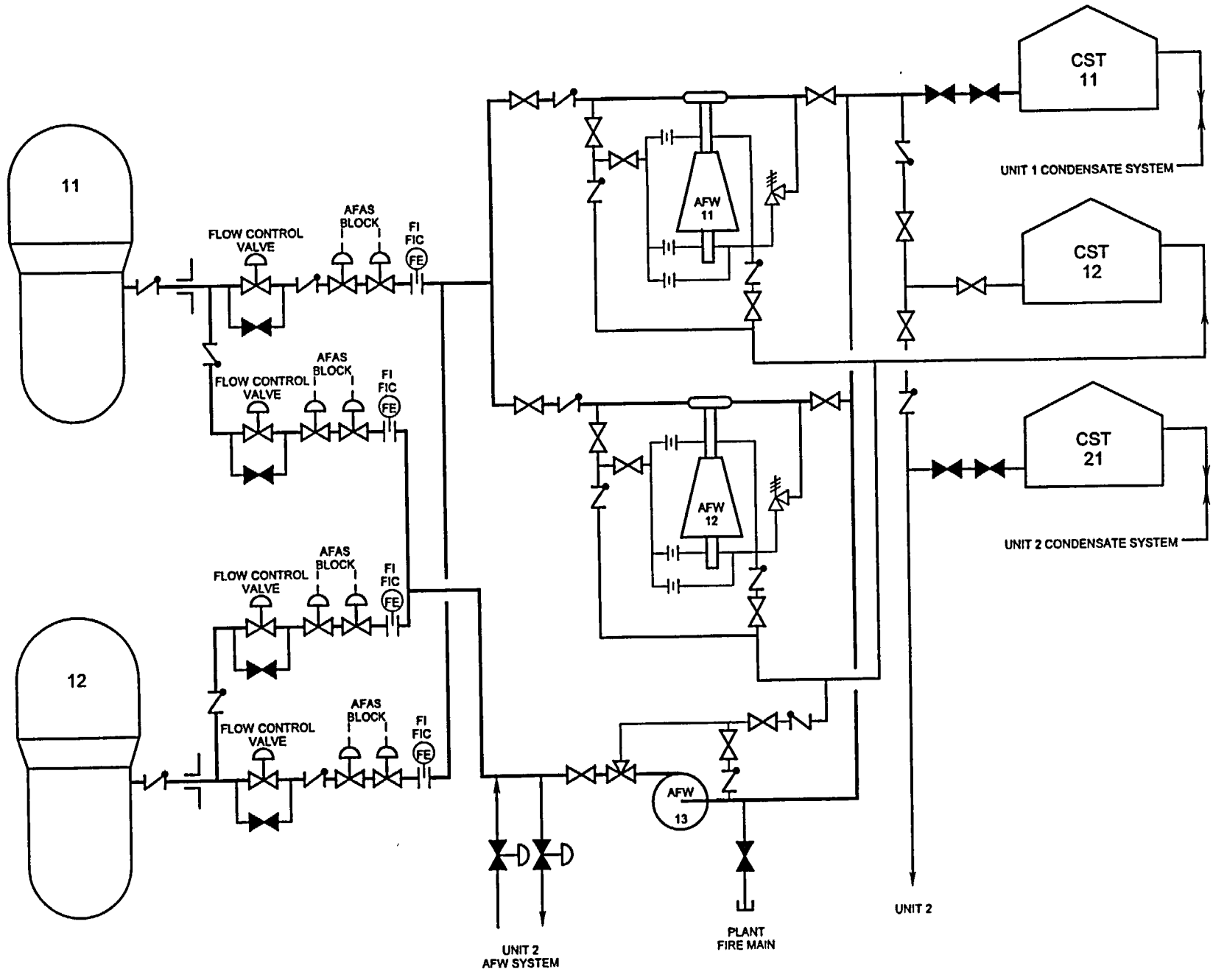


Figure 11.5-1 Auxiliary Feedwater System

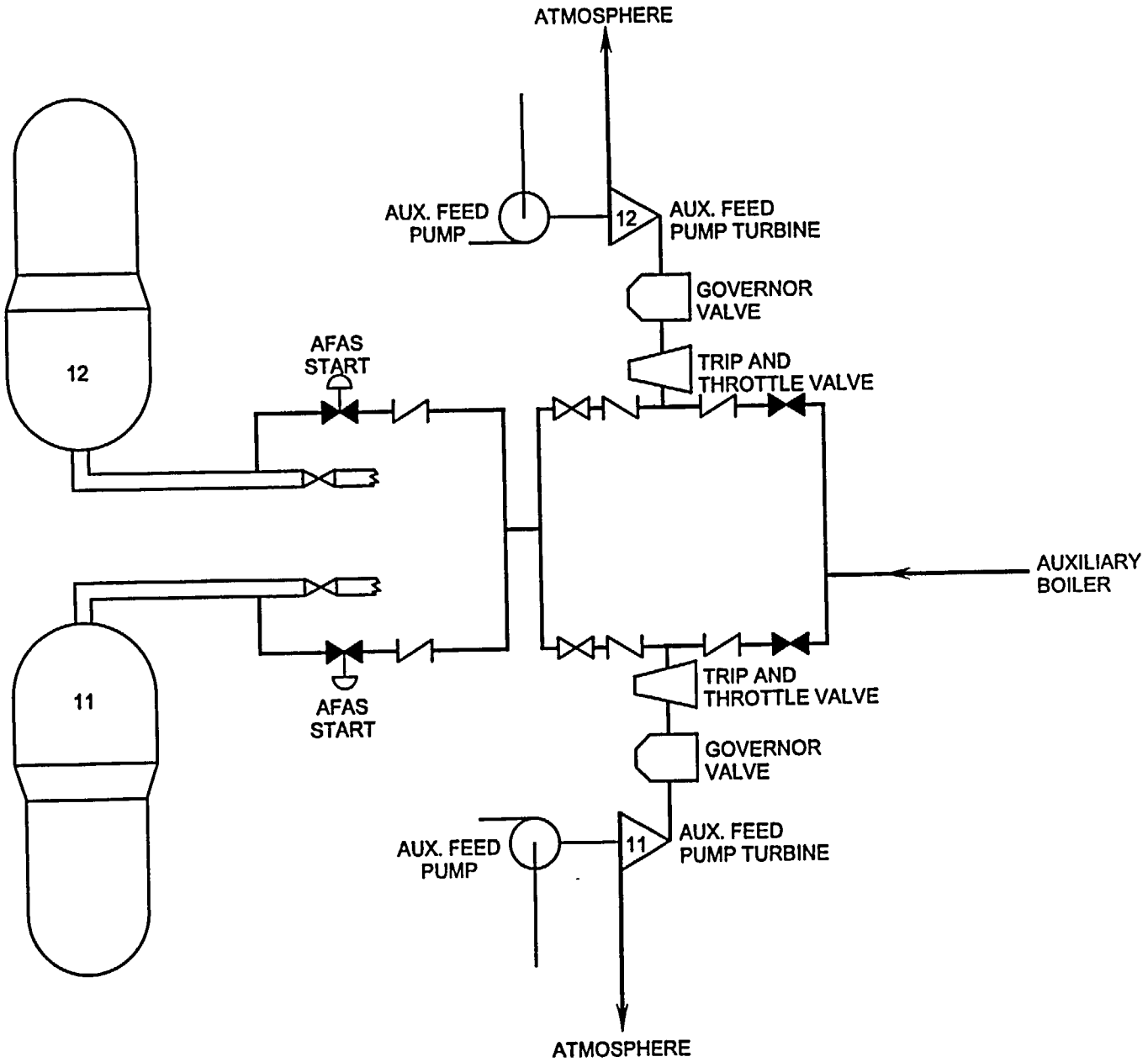


Figure 11.5-2 Auxiliary Feedwater Steam Supply

Combustion Engineering Technology
Cross Training Course Manual

Chapter 12

DIGITAL PROTECTION SYSTEMS

Section

TABLE OF CONTENTS

12.1 CORE PROTECTION CALCULATORS (CPC)

LIST OF TABLES

LIST OF FIGURES

12.1 CORE PROTECTION CALCULATORS (CPC)

Learning Objectives:

1. State the purpose of the core protection calculators (CPC).
2. Explain how the departure from nucleate boiling ratio (DNBR) and the local power density (LPD) limits are calculated by the CPCs.

12.1.1 Introduction

The purpose of the CPCs is to generate trip signals based upon LPD and DNBR which prevents these limits from being exceeded during anticipated operational occurrences (AOOs). The CPC is a digital computer that calculates a conservative value of plant LPD and DNBR. A CPC is installed in each of the four (4) reactor protection (RPS) channels and the trips that are generated by the calculators must satisfy the required two (2) out of four (4) RPS trip logic.

12.1.2 CPC Inputs

In order to provide protection for DNBR and LPD, the CPCs must be supplied with inputs that affect these limits. DNBR is a function of RCS pressure, RCS flow, RCS temperature, reactor power, and flux distribution. While LPD is a function of total power and power distribution.

12.1.2.1 Reactor Power

The reactor power input is supplied from two (2) sources. Those sources are loop temperatures and excore linear power. Hot leg (Th) temperature and cold leg (Tc) temperature are inputs into the calculation of ΔT power (ΔT = Th - Tc). ΔT power provides an accurate indication of true plant power when the unit is being operated at steady state. The highest of either ΔT power or excore linear power is supplied to the calculations of DNBR and LPD.

The output of the three (3) excore linear power detectors is supplied to the CPC, but because these detectors sense leakage neutrons several corrections are required before an accurate power signal is available. These corrections are discussed in Section 12.1.3.1.

12.1.2.2 Reactor Coolant Temperatures

Hot leg temperature and cold leg temperature is supplied to the CPCs for the calculation of ΔT power, correction of the excore detector signal, and as the temperature input into the DNBR calculation. Temperatures are sensed by well mounted resistance temperature detectors (RTDs).

12.1.2.3 Pressurizer Pressure

A pressurizer pressure transmitter supplies the DNBR calculation with the necessary pressure input.

12.1.2.4 Reactor Coolant System Flow

Reactor coolant system flow is not an input to the CPC, instead flow is calculated from the speed inputs of the four (4) reactor coolant pumps (RCPs). The flow of the RCS is verified during testing.

12.1.2.5 Control Element Assembly (CEA) Positions

CEA positions for the twenty CEAs located in the associated CPC core quadrant are used to correct the excore linear power input signals and

the power distribution calculations. These CEAs are called target CEAs. In addition to the target CEA positions, each control element assembly calculator (CEAC) modifies the power distribution calculations for CEA misalignments. Table 12.1-1 below summarizes the CPC inputs.

Each input is monitored for proper input range. Should an input be out of range, a sensor failure alarm will result.

Table 12.1-1
CPC Inputs

Input Signal	Range	Number Per CPC
RCP Speed	20-100% of Rated Speed	4 - 1/RCP
Cold Leg Temperature	465°F-615°F	2 - 1/Loop
Hot Leg Temperature	525°F-675°F	2 - 1/Loop
Pressurizer Pressure (psia)	1500 - 2500	1
Excore Linear Power	0 - 200%	3 - one from each detector

12.1.3 CPC Software (Figure 12.1-1)

12.1.3.1 Excore Linear Power Corrections

The first correction that is applied to the excore signal is called the shape annealing factor. Each excore linear channel consists of three (3) detectors located parallel to the axis of the core. The upper detector monitors leakage neutrons from the top one third (1/3) of the core, the middle detector senses neutrons from the center one third (1/3) of the core, and the bottom detector detects neutrons from the bottom one third (1/3) of the core. In theory, the use of three (3) detectors should yield an accurate indication of the core's axial power distribution. However, each of the detectors can sense neutrons from all parts of the core and the ability of the detectors to accurately reflect axial power distribution is impaired.

During power range testing, different axial power distributions are created by inducing an axial xenon transient. The incore instrumentation system is used to gather power distribution data which is compared with the excore detector output. Shape annealing factors result from the incore to excore correlation and are input into the CPC software as addressable constants. Addressable constants are program variables that can be changed. These shape annealing constants restore the accuracy of the excore detector flux distribution indication.

The second excore correction is called rod shadowing and corrects the output of the detectors for changes in power distribution due to CEA insertion. For example, deeply inserted CEAs in the center of the core forces power to the peripheral assemblies while rods inserted at the core periphery has the opposite effect. As illustrated in Figure 12.1-2, changes in individual detector outputs occur because of the different rod patterns. Target CEA positions are supplied to the rod shadowing calculation and compensates for excore detector output changes caused by rod position changes. After the excore signal is corrected for shape annealing and rod shadowing, it is supplied to the axial peaking calculation section of the CPC software.

The next excore correction is necessary because a change in water temperature in the

reactor vessel affects the leakage of neutrons from the core. Leakage is inversely proportional to temperature; therefore, as temperature decreases, detector output decreases. This could cause indicated power to be less than actual power. The effect is called temperature shadowing. The minimum Tc is used for this temperature shadowing correction because the vessel flow path places Tc water between the core and the detectors.

The final correction that is applied to the excore signal is the calibration addressable constant which is used to ensure that CPC power is in agreement with the power that is calculated by secondary heat balance (calorimetric power). Temperature shadowing and calibration corrections are applied to the total excore power signal before it is sent to the program section that high selects either excore or ΔT power for use in the calculation of LPD and DNBR.

12.1.3.2 ΔT Power

Core power based upon the difference in hot and cold leg temperatures is called ΔT power. The temperature inputs are combined with coolant mass flow rate to determine the core enthalpy rise. This energy rise is calibrated to secondary heat balance power by an addressable constant and is dynamically compensated by changes in average Th. The output of the ΔT power is sent to the high selection program section which is discussed above.

12.1.3.3 Power Distribution Calculations

Localized concentrations of heat flux are of prime importance in the calculation of LPD and DNBR. If the designer can assure that the worst case localized hot spots do not exceed these specified limits, then no local spot in the core will violate limits. Hot spots are characterized as areas of high heat generation and of low heat removal. The latter condition is caused by increased resistance to heat transfer and reductions in flow areas.

Examples are lack of mixing, enrichments of pellets at the maximum values, low gap conductivity, and flow reductions caused by fuel rod bow. The conditions change slowly and can be lumped together as an engineering penalty factor. A conservative engineering factor is assumed in the CPC algorithms.

Heat generation, is a dynamic factor and cannot be assigned a conservative value. Heat generation is a function of the flux in the localized area and for the CPC calculation is broken down into its radial and axial components. Radial flux distribution is a function of control rod position; therefore, radial peaking factors can be precalculated and programmed into a software table. Once these values have been established, the CPC needs only the input of control rod position to determine radial peaks. The input of control rod position comes from the twenty CEAs located in the core quadrant associated with a particular CPC. The CEAs are called target CEAs. From the target CEA inputs, the radial peaking program looks up the appropriate peaking factor in the preprogrammed table. From the table look up, the radial peaking factor is supplied to the hot pin calculation.

The axial component of flux distribution is derived from the corrected output of the three (3) excore linear power range detectors. The axial flux distribution is also supplied to the hot pin calculation.

In addition to the inputs of radial and axial flux distribution, the hot pin calculation receives an azimuthal tilt addressable constant and the

penalty factors from the CEACs. The azimuthal tilt constant is used to correct the hot pin calculation for steady state radial tilts.

The inputs from the CEACs correct the hot pin calculation for CEA misalignments between core quadrants. The hot pin selects the highest (worst case) penalty factor. The output of the hot pin program section is routed to the calculation of LPD and DNBR.

12.1.3.4 RCS Flow Calculations

The RCS flow rate is calculated by converting the pump speed input signals to a volumetric flow rate. The volumetric flow rate is corrected for system pressure losses and converted to a mass flow rate by considering fluid properties that are pressure and temperature dependent. Addressable calibration constants are used to insure that the calculated value of flow is in agreement with values measured during plant testing. Mass flow rate is sent to the calculation of ΔT Power, to the DNBR calculation, and a derivative of flow (negative values only) is used to update the DNBR calculation.

12.1.3.5 Reactor Coolant System Pressure

A pressurizer pressure transmitter supplies the pressure input to the DNBR and DNBR update calculations.

12.1.3.6 DNBR Calculation

The DNBR calculation is performed by manipulating the inputs of the following parameters:

1. Hot pin calculation,
2. Power (high selected ΔT or excore).
3. Maximum Tc
4. RCS flow and
5. Pressurizer pressure.

A value of DNBR is calculated. This value is called the static DNBR and is calculated every two (2) seconds. The output of the static DNBR calculation is supplied to the DNBR update calculation.

12.1.3.7 DNBR Update Calculation

The DNBR update calculation is performed every 100 milliseconds by considering the derivatives of the inputs to the static DNBR, and DNBR projections based on flow and coolant quality.

The derivatives are used to update the DNBR calculation based upon changes in these parameters that have occurred since the last calculation of DNBR. The factors (partial derivatives) that are used are a function of the values of a set of process variables. These variables are:

1. Cold leg temperature,
2. RCS pressure,
3. Axial shape index (ASI) and
4. The radial peaking factor.

As illustrated in Figure 12.1-3, these factors are combined into three separate regions with region 1 being defined as normal operation. Crossing from region 1 to region 2 results in the use of a larger value of derivatives that reduce DNBR. Likewise, moving from region 2 to region 3 results in even larger values being used. If the parameters exceed region 3, a DNBR trip results.

Because RCS flow has a drastic effect on DNBR, the effect of a negative rate of change of flow on DNBR is calculated every 50 milliseconds and supplied to the DNBR update calculation.

The final input into the DNBR update program is coolant quality. The coolant quality calculation accounts for changes in DNBR caused by unstable flow which results from boiling.

The updated value of DNBR is compared with the DNBR limit and a margin to trip is determined. This margin is displayed on a meter on the control board. If the margin reaches the pretrip set point a pretrip alarm results and if the margin decreases to zero a DNBR trip signal is generated.

12.1.3.8 LPD Calculation

The LPD calculation is used to generate a reactor trip signal before center line fuel melting limits are exceeded. This calculation receives inputs from the hot pin calculation and the highest of either excore power or ΔT power. The output of the LPD calculation is compared with the LPD limit. As in the DNBR trip routine, LPD margin is displayed, compared with the pretrip set point, and generates a LPD trip if the LPD margin drops to zero.

12.1.4 CPC Auxiliary Trips

The following will cause DNBR and LPD trips to be generated:

1. Internal computer processor faults,
2. Less than 4 RCPs running,
3. Operations in excess of region 3 parameters, or
4. ΔTc >17°F (asymmetric steam generators)

The auxiliary trip due to faults is installed to ensure that the CPC is functioning correctly and accurately calculating DNBR and LPD. Operations with less than four (4) reactor coolant pumps has not been analyzed and is prohibited.

Operation in region 3 represents the approach to the upper and lower sensor input ranges and values assumed in safety analysis. The final auxiliary trip provides protection against the large radial flux tilts that would result if one main steam isolation valve was closed. The program checks for deviations between loop A and B cold leg temperatures (ΔTc) and if the deviation exceeds 17°F, a reactor trip signal is generated.

12.1.5 Summary

The CPCs provide protection for LPD and DNBR during AOOs. The CPC is a digital microprocessor that receives LPD and DNBR sensitive inputs and accurately calculates the approach to these limits.

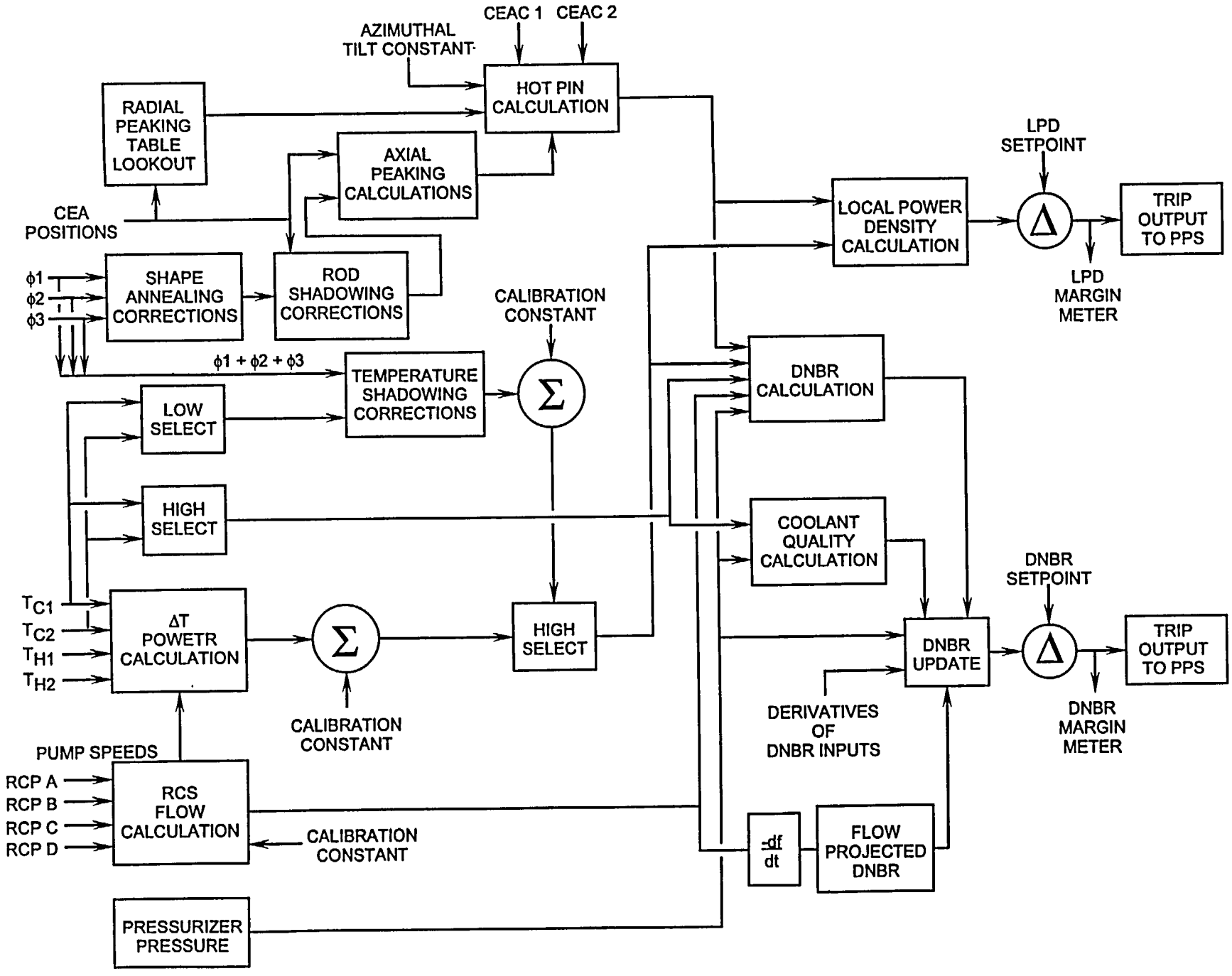


Figure 12.1-1 CPC Software Block Diagram

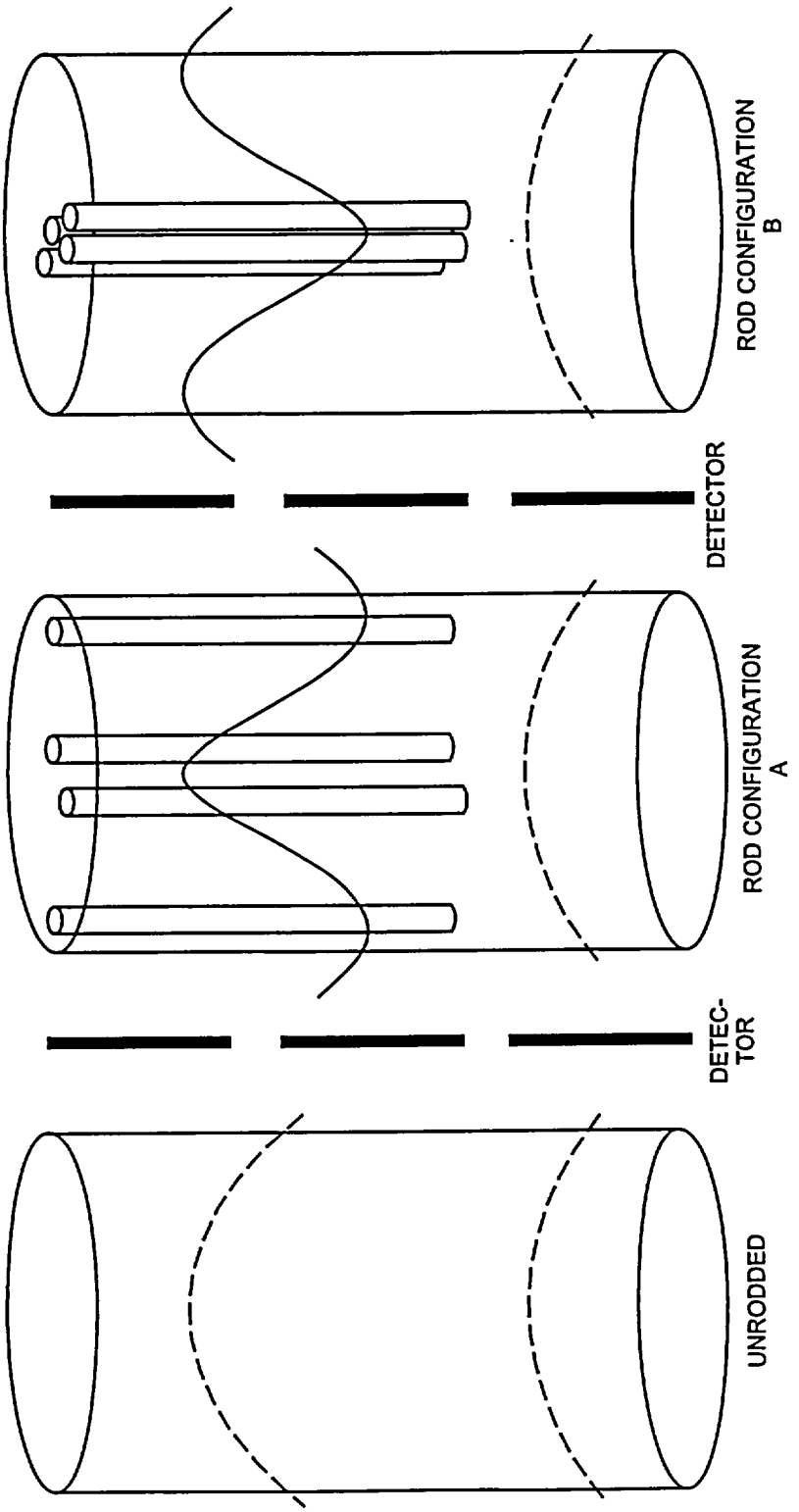


Figure 12.1-2 Rod Shadowing Examples

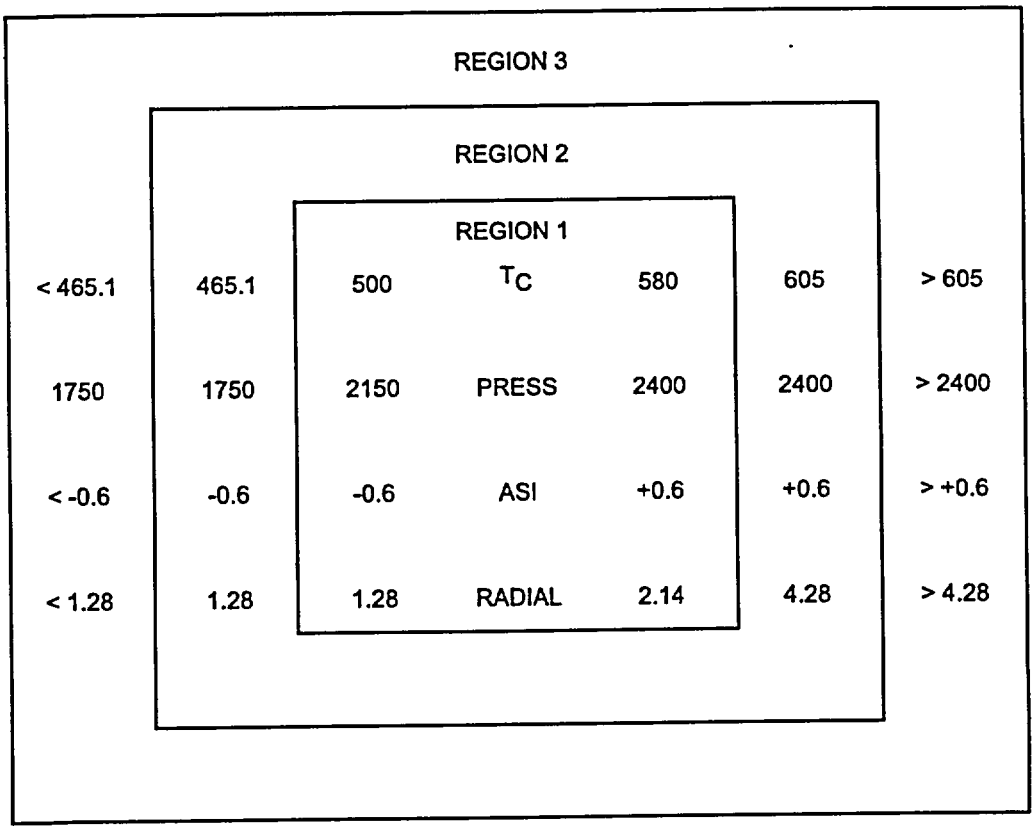


Figure 12.1-3 DNBR Update Program

TABLE OF CONTENTS

12.2 CONTROL ELEMENT ASSEMBLY CALCULATORS (CEACs)

LIST OF FIGURES

12.2 CONTROL ELEMENT ASSEMBLY CALCULATORS (CEACs)

Learning Objectives:

1. State the purpose of the control element assembly calculators (CEACs).

2. Explain why the CEACs are included in the reactor protection system (RPS) design.

12.2.1 Introduction

The CEACs sense the position of each of the control element assemblies (CEAs), determine CEA misalignment, and transmit misalignment information (in the form of penalty factors) to the core protection calculators (CPCs). The CEACs are required because each CPC receives CEA position from only one core quadrant and cannot sense misalignments that would affect local power density (LPD) and departure from nucleate boiling ratio (DNBR). In addition to supplying information to the CPCs, the CEACs provide CEA position indication.

12.2.2 CEAC Inputs (Figure 12.2-1)

Each CEA's position is sensed by redundant reed switch position transmitters (RSPTs). These RSPTs must supply target CEA positions for the CPC and supply position information to the CEACs.

The CEAC 1 inputs are as listed below:

1. 20 inputs from the CEAs that serve as target CEA inputs to CPC "B".

2. 20 inputs, via optical isolation, from the CEAs that serve as target CEA inputs to CPC "A".

3. 40 inputs from the redundant RSPT on the target CEAs for CPC "C" and CPC "D".

4. One direct input from the center CEA.

The inputs for CEAC 2 are as follows:

1. 20 inputs from the CEAs that serve as target CEAs for CPC "C".

2. 20 inputs, via optical isolation, from the CEAs that serve as target CEAs for CPC "D".

3. 40 inputs from the redundant RSPT on the target CEAs for CPC "A" and CPC "B".

4. One direct input from the center CEA.

12.2.3 Signal Processing (Figure 12.2-2)

The 5 to 10 volt analog input from the RSPT is converted to a digital signal corresponding to 0 to 100% withdrawn. A comparison is made to predetermined high and low limits. If a sensor fails high, the signal is set equal to the 100% withdrawn position, and conversely, if the signal fails low, the signal is set equal to the 0% withdrawn position. In either case, a sensor fail alarm is sent to the CPC/CEAC insert in the control room. Next, the calculator determines the reference position for each subgroup of CEAs by finding the lowest CEA in that subgroup. Each CEA position is compared with the reference position for its subgroup.

As an example, assume a four (4) CEA subgroup with one (1) CEA at 50% withdrawn and the remaining CEAs at 60% withdrawn. In this example, the CEAC would determine that three CEAs are misaligned. If the CEA exceeds a misalignment deadband (Figure 12.2-3) then a penalty factor is calculated.

Four (4) different case types each with different penalty factors, are calculated. The first case involves the deviation of one (1) CEA and provides protection for the uncontrolled withdrawal of a single or part length CEA. The second case provides protection for the misalignment of two (2) CEAs within a subgroup. The third case provides protection for the drop of a single CEA while the fourth and final case protects against the drop of a five (5) CEA subgroup. These four (4) cases represent the anticipated operational occurrences (AOOs) involving the CEAs.

12.2.4 CEAC Outputs (Figure 12.2-4)

The CEAC outputs two (2) types of signals. The first signal is position information and is sent to a CRT display via a selector switch. The selector switch allows either CEAC to display the position of all CEAs. Each CEAC also transmits a penalty factor via optical isolators to each CPC.

In the CPC, the highest penalty factor is selected and applied to the power distribution calculations. Should a single CEAC become inoperable, the CPCs will select the highest signal from either the operable CEAC or the last valid signal from the inoperable CEAC.

The inoperable CEAC may be bypassed by changing an addressable constant in the CPC software. When the CEAC is bypassed, the CPCs use the penalty factor from the operable CEAC. If both CEACs fail, plant operations may continue provided the CEACs are bypassed. Again, the bypass is accomplished by changing addressable constants in the CPCs. In this case, the CPCs use a predetermined conservative penalty factor.

12.2.5 Summary

The CEACs receive CEA position inputs, calculate penalty factors that are applied to the CPC power distribution calculations, and provide CEA position information to the control room display.

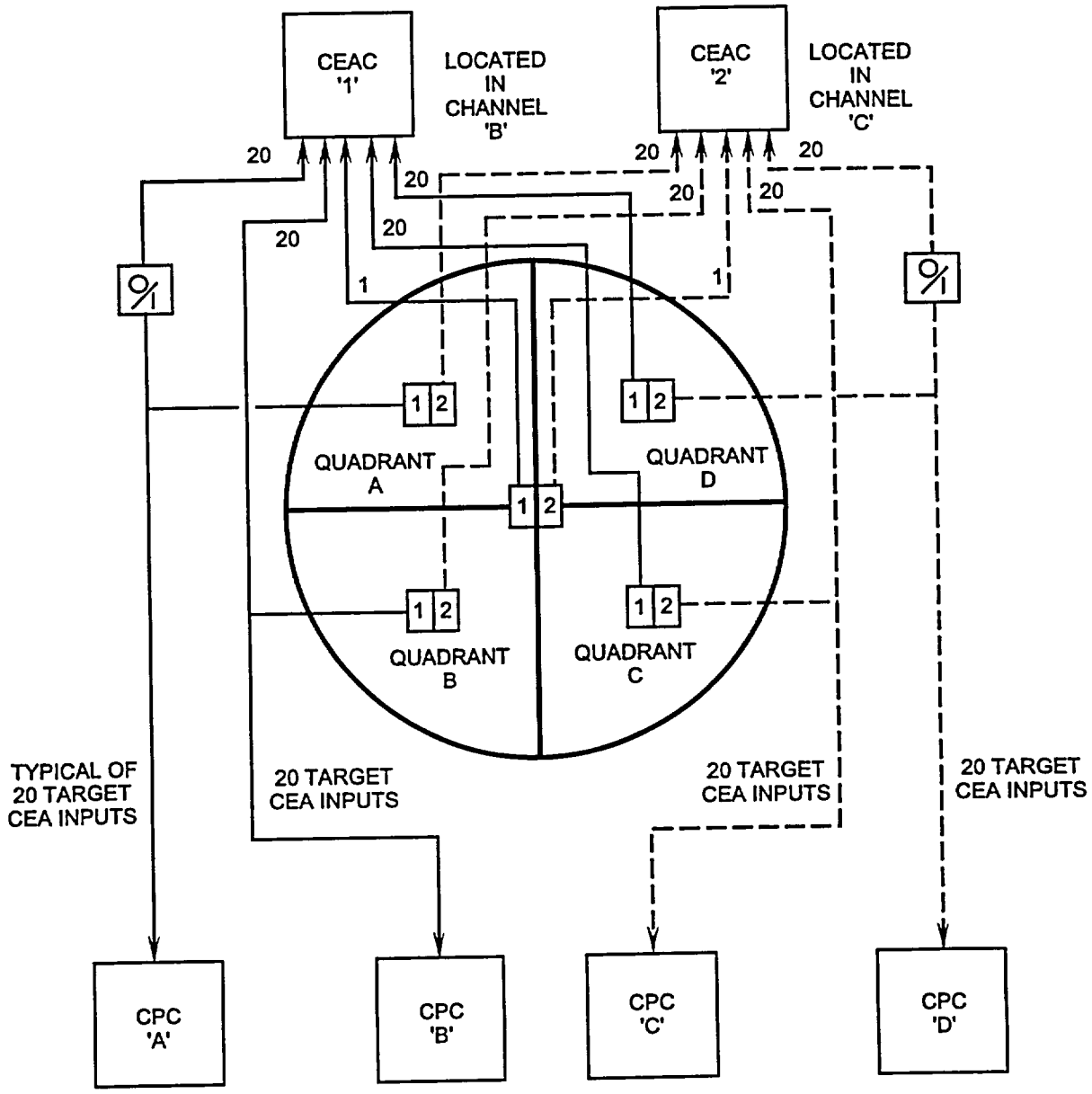


Figure 12.2-1 CEAC Inputs

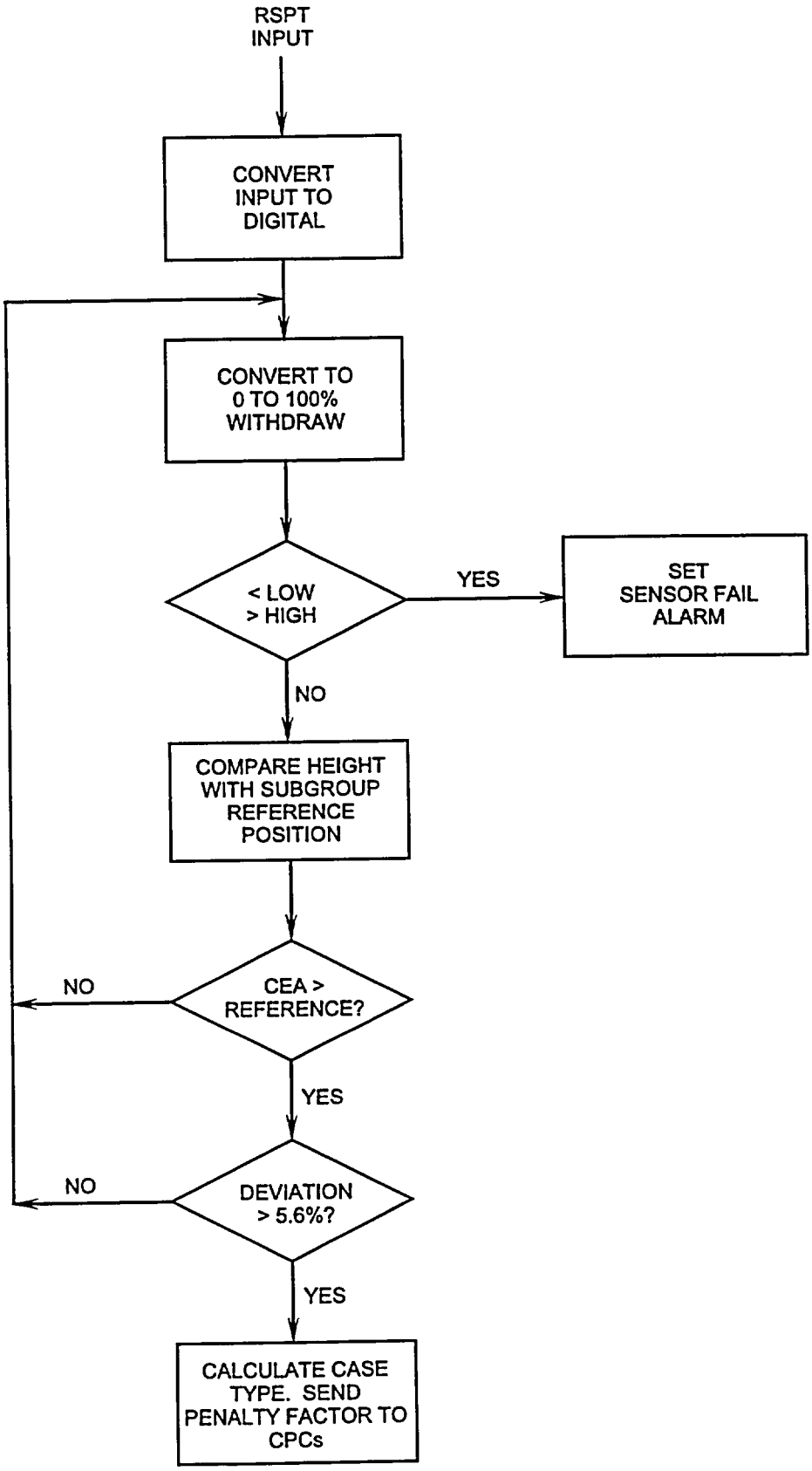


Figure 12.2-2 CEAC Software

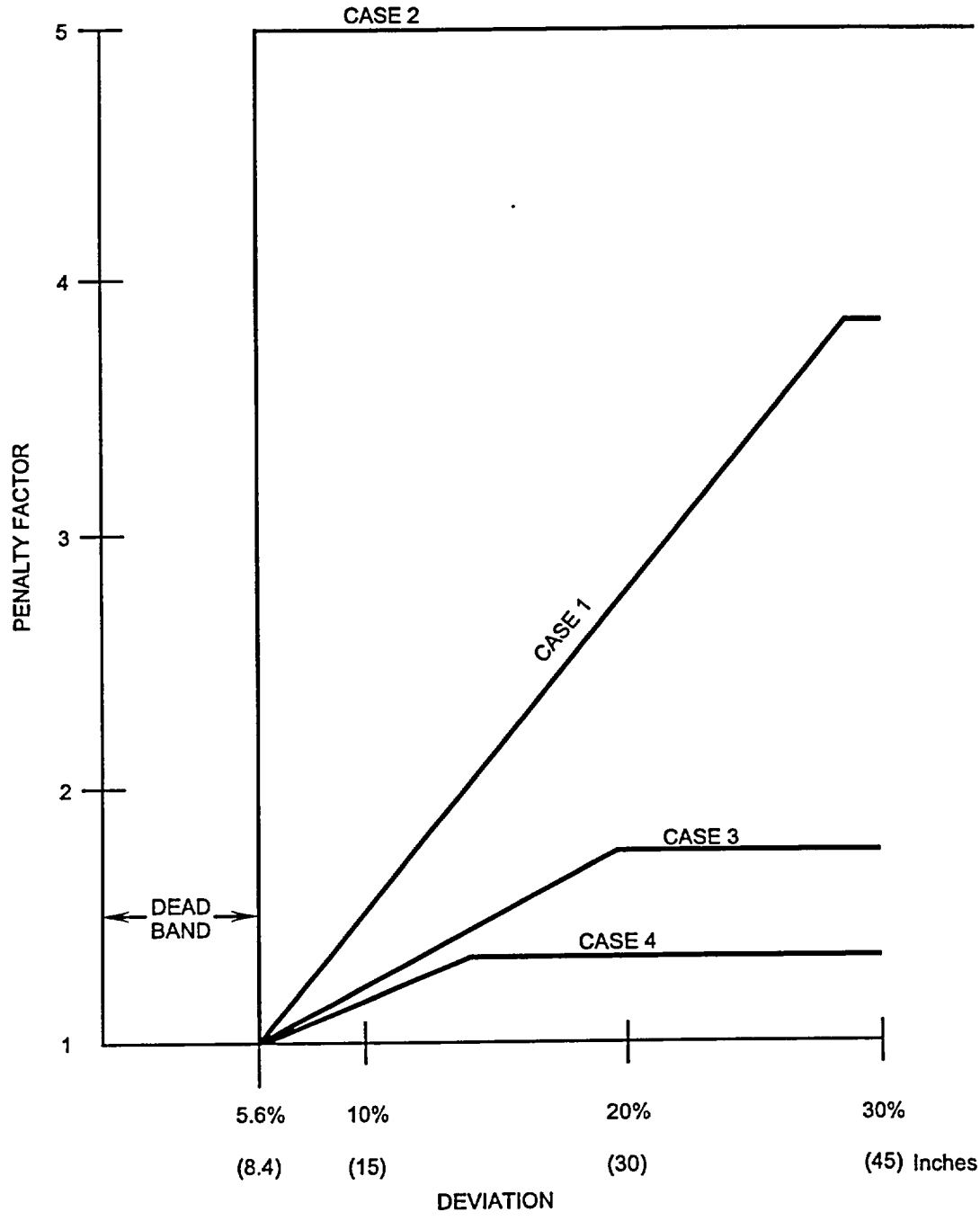
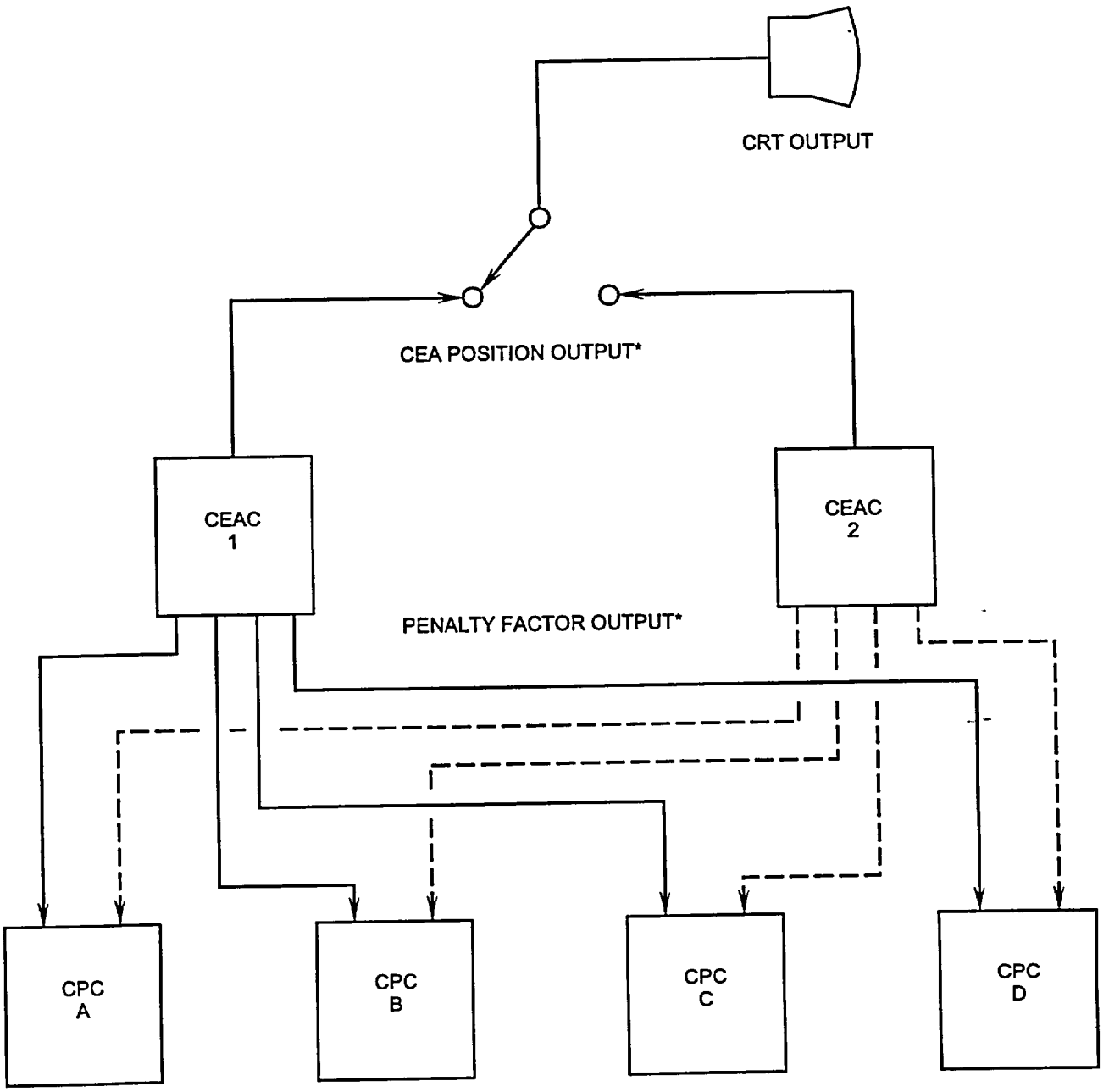


Figure 12.2-3 CEAC Penalty Factors



*OUTPUTS TRANSMITTED VIA OPTICAL ISOLATION

Figure 12.2-4 CEAC Outputs

TABLE OF CONTENTS

12.3 CORE OPERATING LIMIT SUPERVISORY SYSTEM (COLSS)

LIST OF FIGURES

12.3 CORE OPERATING LIMIT SUPERVISORY SYSTEM (COLSS)

Learning Objectives:

1. State the purpose of the core operating limit supervisory system (COLSS).

2. List the operating limits that are monitored by COLSS.

12.3.1 Introduction

The COLSS consists of process instrumentation and algorithms implemented by the plant computer to continually monitor the limiting conditions for operation on peak linear heat rate (LHR), margin to departure from nucleate boiling (DNB), total core power, azimuthal tilt and axial shape index (ASI).

The COLSS continually calculates DNB margin, peak LHR, ASI, total core power, and azimuthal tilt magnitude. COLSS then compares the calculated values to the limiting condition for operation on these parameters. If a limiting condition for operation is exceeded for any of these parameters, COLSS alarms are initiated by the plant computer and operator action is taken as required by technical specifications.

The selection of limiting safety system settings (LSSS), core power operating limits, and the azimuthal tilt operating limit are specified such that no safety limit will be exceeded as a result of an anticipated operational occurrence (AOO) and that the consequences of postulated accidents will be acceptable. The reactor protection system (RPS) functions to initiate a reactor trip at the specified LSSSs.

The COLSS is not required for plant safety since it does not initiate any direct safety-related function during AOOs or postulated accidents. The technical specifications define the limiting conditions for operation (LCO) required to ensure that reactor core conditions during operation are no more severe than the initial conditions assumed in the safety analyses and in the design of the low DNBR and high local power density trips. The COLSS serves to monitor reactor core conditions in an efficient manner and provides indication and alarm functions to aid the operator in maintenance of core conditions within the LCOs given in the technical specifications.

The COLSS algorithms are executed in the plant computer. The calculational speed and capacity of COLSS enables numerous separate plant operating parameters to be integrated into three more easily monitored parameters:

1. Margin to a limiting core power (based upon margins to DNBR, peak linear heat rate and licensed power limits),

2. Azimuthal tilt and

3. Axial shape index.

If COLSS were not provided, maintenance of reactor core parameters within the LCOs, as defined by the technical specifications, would be accomplished by monitoring and alarms on the separate non-safety related process parameters used in the COLSS calculations. Therefore, the essential difference in using COLSS in lieu of previous monitoring concepts is the integration of many separate process parameters into a few easily monitored parameters. The conciseness of the COLSS displays has distinct operational advantages, since the number of parameters that must be monitored by the operator is reduced.

The concept of COLSS was proposed in the core protection calculator (CPC) patent application. The CPCs and COLSS work together to assure that the CPCs are able to protect the specified acceptable fuel design limits (SAFDLs) such that DNBR will never drop below 1.2, nor will linear heat rate rise above 21 kW/ft in the event of AOOs.

Since it is the class 1E CPCs which actually provide the reactor trip, then one might expect that the CPCs could also be used to maintain the LCOs on DNBR and LHR, and the COLSS need not concern itself with these LCOs. The CPCs do in fact perform this function if COLSS is out of service. Technical specifications sections state that the appropriate LCOs on DNBR and LPD can be maintained by monitoring these parameters on the CPC remote modules. So why the desire to have a COLSS?

The answer is that the CPCs must be very fast and reliable to provide protection for the design basis AOOs and accidents, whereas COLSS can take the time to provide a more accurate calculation of core DNBR or LPD. COLSS can also use inputs which, although more accurate than those used by the CPCs, are less reliable. The result is that COLSS is more accurate than the CPCs. The CPC calculations must be biased to be conservative to offset their inaccuracy, so that the CPCs will normally calculate a value of DNBR that is lower, and a value of LPD that is higher than those calculated by COLSS.

It is therefore possible to operate with COLSS out of service; however the DNBR and ASI used are from the most restrictive CPC, thus it will likely be necessary to reduce power below 100% to be in compliance with the technical specifications. Stated another way, COLSS allows the core to be operated at a higher power density (higher power level) than would be possible with CPCs alone, and the CPCs and COLSS together allow much higher power densities than those which were possible with previous protection systems.

12.3.2 COLSS Design Requirements

COLSS is designed to assist the operator in implementing those sections of the technical specification requirements for monitoring of the following LCOs:

1.Thermal margin,

2.Linear heat rate,

3.Azimuthal tilt and

4.Axial shape index.

COLSS also assists the operator in maintaining core power equal to or below the steady state power level requirement imposed by the licensing letter issued by the Nuclear Regulatory Commission.

To implement these requirements, COLSS is required to perform the following functions:

1. Compute the thermal margin power operating limit LCO from process variable measurements,

2. Compute the peak linear heat rate power operating limit LCO from process variable measurements,

3. Compute the azimuthal tilt index and monitor it with respect to the LCO on azimuthal tilt,

4. Compute the axial shape index and monitor it with respect to the LCO on axial shape index,

5. Compute plant power from process variable measurements,

6. Compute the margin to the licensed power, peak linear heat rate, and thermal margin power operating limits and

7. Initiate appropriate alarm sequences and informative messages when any monitored margin or parameter exceeds its LCO.

The power operating limits are calculated such that no AOO will cause a SAFDL to be exceeded when initiated from inside the COLSS initial margin and proper plant protection system (PPS) action occurs and no postulated accident will have consequences more severe than those predicted in the safety analysis when initiated from inside the COLSS initial margin and proper PPS action occurs.

The LCOs are calculated using algorithms which have been designed with adequate time response for the following plant operating conditions:

1. Normal steady state operation at any power between 15 percent and 100 percent of licensed power,

2. Normal, controlled changes in unit load at any rate up to five percent per minute at any power between 15 percent and 100 percent of licensed power and

3. Step changes in unit load of up to 10 percent initiated at and ending at any power between 15 percent and 100 percent of licensed power.

12.3.3 COLSS LCOs

The design of the monitoring and protective systems are integrated with the plant technical specifications (in which operating limits and limiting conditions for operation are specified) to assure that all safety requirements are satisfied. The plant monitoring systems, protection systems, and technical specifications thus complement each other. Protection systems provide automatic action to place the plant in a safe condition should an abnormal event occur. The technical specifications set forth the allowable regions and modes of operation on plant systems, components, and parameters. The monitoring systems (meters, displays, and systems such as COLSS) assist the operating personnel in enforcing the technical specifications requirements. Making use of the monitoring systems, protection systems and technical specifications in the manner described above will assure that all anticipated operational occurrences or postulated accidents will have acceptable consequences if the following conditions are satisfied.

1. The operating personnel maintain all protective systems settings at or within allowable values,

2. The operating personnel maintain actual plant conditions within the appropriate limiting conditions for operation and

3. Equipment other than that causing an abnormal event or degraded by such an event operates as designed.

12.3.3.1 DNBR LCO

Note that item 2 above implies that the operator must maintain his LCOs in order for the protection system to properly function. The CPCs can provide timely protection for DNBR only if the operator maintains the steady state DNBR in accordance with technical specifications. This allows ample margin between steady state DNBR

and the trip setpoint so that DNBR protection is assured, even in the event of a rapid DNBR reduction.

Core parameters affecting the margin to DNB are continually monitored by COLSS, and a core power operating limit based on margin to DNB is computed. Operation of the reactor at or below this operating limit ensures that the most rapid DNB transient that can result from an AOO does not result in a DNB reduction to a value less than 1.20.

12.3.3.2 LPD LCO

The core power distribution is continually monitored by COLSS, and a core power operating limit based on peak linear heat rate is computed. Operation of the reactor at or below this operating limit assures that the peak linear heat rate is never more adverse than that postulated in the loss of coolant accident (LOCA) analyses. This will maintain the clad surface temperature below 2200°F in the event of a LOCA. Note that the LCO on linear heat rate is not based on protecting the 21 kW/ft LHR SAFDL in the event of AOOs. In this case, the concern of clad surface temperature in the event of a LOCA forces a lower kW/ft steady state operating limit than does the concern of exceeding 21 kW/ft in the event of AOOs. If the SAFDL requirement that the CPC LPD trip protects for LHR < 21 kW/ft during AOOs were the only concern, a higher steady state operating LPD could be permitted.

12.3.3.3 Licensed Power Level LCO

A core power operating limit based on licensed power level is also monitored by COLSS. Operation of the reactor at or below this operating limit ensures that the total core power is never greater than that assumed as an initial condition in the accident analyses.

12.3.3.4 Azimuthal Tilt LCO

The limitations on azimuthal tilt (Tq) are provided to assure that design safety margins are maintained. The azimuthal flux tilt is calculated in COLSS. The azimuthal flux tilt is not directly monitored by the plant protection system (PPS). This is because the CPCs each only monitor one (1) of the four (4) excore safety channels, making excore channel cross comparison impossible in the CPCs. The excores themselves can provide cross-comparison and that is used to determine azimuthal tilt if the incores are out of service.

Without the ability to cross compare excores, the CPCs are in essence blind to azimuthal tilt. For this reason, azimuthal tilt is an addressable constant in the CPCs. It is necessary for the operator to inform the CPCs of the correct value of azimuthal tilt by changing this addressable constant to reflect a Tq which is conservative with respect to the actual tilt.

COLSS normally calculates azimuthal tilt based on incore nuclear instrumentation, using symmetric sets of incores in the four (4) core quadrants to determine a valid tilt. This calculation is performed on line, as is the case with all COLSS calculations. If the azimuthal tilt, as calculated by COLSS, exceeds that in the CPCs, a CPC tilt limit exceeded alarm will result on the plant computer CRT. Provisions are also made for plant annunciation on this alarm.

Note that the CPCs and COLSS do not communicate with each other, since the CPCs are safety related, while the COLSS is not. It is therefore necessary for the operator to inform the COLSS as to the value of azimuthal tilt assumed in the CPCs. To accomplish this, plant computer prompting should be followed. Initially, the CPCs assume an azimuthal tilt of 2%, so this value should be entered in COLSS as the alarm setpoint.

If the tilt increases, and new values of azimuthal tilt are entered into the CPCs, these same values must be entered by the operator into the COLSS to be used for the alarm setpoint.

If the azimuthal tilt rises to 10%, a second alarm (technical specification tilt limit exceeded) will occur on the plant computer alarm CRT. There are also provisions for annunciation on this alarm. This alarm warns the operator that the azimuthal tilt has reached the maximum allowed for normal operation as defined in the technical specifications. An azimuthal tilt of 1.10 should normally not occur but if it does, power reduction is in order.

12.3.3.5 Axial Shape Index LCO

The LCO on ASI assures the actual value of ASI is maintained in the range assumed in the safety analysis.

12.3.4 System Description

12.3.4.1 COLSS Input/Outputs

Figure 12.3-1 shows all COLSS inputs and outputs. Since COLSS is in essence a program resident in the plant computer, there is no COLSS hardware to speak of with the exception of the process inputs and outputs. The inputs are the same inputs as those used for other programs and data logging.

12.3.4.2 Contact Outputs

All contact outputs are used to provide plant annunciation; however in addition to those alarms on the plant annunciator panels, alarm messages will also be displayed on the plant computer alarm CRT, for these and many other conditions affecting COLSS.

In addition to the four (4) contact outputs described below, COLSS will also print out a number of alarm messages for a variety of conditions affecting COLSS, including all sensor validity check failures, cross check failures, and the designation of any calculated block as bad.

12.3.4.3 COLSS Power Margin Alarm

This alarm is set (contacts open) if:

1. COLSS is not in scheduled mode (that is, COLSS has been turned off),

2. Licensed power is exceeded.This licensed power limit will normally be 100%, but can be any lower limit as imposed by the NRC licensing letter ,

3. Either power operating limit (POL) is exceeded. The two POLs are the DNBR POL and the LPD POL. These limits represent the maximum power the core could produce (based on current power distribution as sensed by process inputs) without violating the LCO on DNBR or LPD or

4. Plant power or a POL has a bad validity.

It is instructive to note that in COLSS actual power is not an input to the COLSS POL calculation. This contrasts with the CPCs where power is an input to the DNBR and LPD calculations. The reason for this is that the CPCs must calculate the actual DNBR and LPD for protection purposes, whereas COLSS calculates the hypothetical power the plant could safety produce without exceeding the LCOs on DNBR or LPD.

The COLSS margin alarm actually will alarm if the most restrictive of the licensed power,

DNBR POL, or LPD POL is exceeded by actual plant power.

COLSS has extensive self diagnostic capability, particularly with regard to input sensor out-of-range failures. Although COLSS also does have the ability to, in some cases, substitute backup sensors for failed sensors, if COLSS determines that there are inadequate inputs to give the desired output, it will declare the block of calculations affected by the input as bad. All outputs from the affected block will therefore also be bad, and any blocks downstream may be declared bad, unless there is an alternate input block which can be substituted. This latter case exists in the COLSS method of selecting plant power, in which three (3) different methods of power measurement are employed. Should one be declared bad, COLSS uses logic to eliminate the faulty calculation.

Opening contacts to the COLSS power margin alarm will also cause one or more of the following messages to be printed on the alarm CRT, as applicable:

DNBR POWER LIMIT EXCEEDED

KW/FT POWER LIMIT EXCEEDED

LICENSED POWER LIMIT EXCEEDED

INSTANTANEOUS DNBR POWER LIMIT EXCEEDED

INSTANTANEOUS KW/FT POWER LIMIT EXCEEDED

LPL ALARM DURATION EXCEEDED

DNBR ALARM DURATION EXCEEDED

KW/FT ALARM DURATION EXCEEDED

ANNUAL LPL VIOLATION

ANNUAL DNBR VIOLATION

ANNUAL KW/FT VIOLATION

The first three (3) alarm messages are derived directly from the COLSS power margin alarm.

12.3.4.4 CPC Azimuthal Tilt Exceeded Annunciator.

If the azimuthal tilt, as calculated by COLSS, exceeds that assumed by the CPCs alarm contacts will be opened. Several alarm messages associated with this alarm will also be printed on the alarm CRT, including:

CPC TILT LIMIT EXCEEDED

CPC TILT ALARM DURATION EXCEEDED

CPC TILT ALARM ANNUAL DURATION EXCEEDED.

The latter two (2) show the time since onset of the condition, and the total time, on an annual basis, that the alarm condition has been set.

12.3.4.5 Technical Specification Tilt Limit Exceeded Alarm

This alarm has a setpoint of 1.10, which is the maximum azimuthal tilt allowed for normal operation in accordance with technical specifications. Messages on the alarm CRT associated with this annunciator include:

TECHNICAL SPECIFICATION TILT LIMIT EXCEEDED

TECHNICAL SPECIFICATION TILT ALARM

DURATION EXCEEDED

TECHNICAL SPECIFICATION ALARM ANNUAL DURATION EXCEEDED.

12.3.4.6 ASI Alarm

This is not a contact output from the COLSS, therefore it does not warrant notice on Figure 12.3-1. However, COLSS does monitor ASI, and there are provisions for the following Alarm CRT Outputs:

ASI OUT OF LIMITS

ASI ALARM DURATION EXCEEDED

ASI ANNUAL DURATION EXCEEDED.

12.3.4.7 Analog (Indicator) Outputs

The following COLSS meters on the control board provide continuous (on line) information to the operators:

1. Core power operating limit based on peak linear heat rate (kW/ft POL; 0-125%),
2. Core power operating limit based on margin to DNB (DNBR POL; 0-125%),
3. Total core power (0-125%),
4. Margin between core power and nearest core power operating limit (Power Margin; -50 to +125%) and
5. Core average axial shape index (-.7 to +.7)

The power margin meter has a horizontal scale and is a digital display. It represents the difference between actual plant power, as calculated by COLSS, and the most restrictive (lowest) of DNBR POL, LPD POL and licensed power limit.

As long as COLSS is in service, and the surveillance requirements have been met, there is no reason to consult technical specifications or to worry about exceeding the limits, since the COLSS margin would go to zero and a COLSS power margin alarm would be set if the LCOs on these parameters were exceeded.

12.3.5 COLSS Functional Diagram

Figure 12.3-2 is a functional diagram of COLSS. COLSS sections pertaining to the calculation of plant power for use in the plant power indicator and the margin calculation have been highlighted, whereas those sections of COLSS involving power distribution and the generation of the POLs have not. The reason for this is that COLSS can, at least functionally, be thought of as being comprised of two (2) sections. One section performs the power calculation; and the other performs the POL calculation.

Strictly speaking, these are not totally independent, since plant power is an input to the in-core burnup calculation and the radial peaking factor lookup table, both of which are used in the power distribution algorithms used in the POL calculation. However, plant power in this application is a second order effect, that is, plant power should not be thought of as an input to the POL calculation since the power operating limit is accomplished by determining the current power distribution in the core and then assuming various increasing power levels until a hypothetical power is chosen which, based on the current power shape, violates the LCO on DNBR, or LPD.

Hypothetical power limits like this one are calculated independently for both DNBR and LPD

and the DNBR POL and LPD POL indicators are the result. Normally, with all CEAs withdrawn, and equilibrium xenon, both of these power limits should read well above 100% since to do otherwise would imply that the plant cannot reach 100% power without violating a LCO.

Plant power is, on the other hand, calculated independently, and the derived plant power is compared to the most restrictive of the DNBR POL, LPD POL, or licensed power, and the difference is read out on a power margin digital indicator. If the margin drops to zero, the power margin alarm will be present.

12.3.5.1 Plant Power Calculation

The inputs to the plant power calculation are shown in Figure 12.3-2. Prior to actually being used in any plant power calculations the inputs must be examined for validity. That is, COLSS will determine if the inputs are reading properly.

This is done in two ways:

Range Check -This check insures that the sensors are in range. If not, they are declared bad. If bad sensors are discovered, they will be alarmed, and they may be automatically replaced by COLSS with substitute sensors that are identical or similar. In some cases, no replacement sensors are provided, and COLSS alarms the condition to the operator on the alarm CRT and awaits operator response. Where no replacement is available the calculation based on the failed input is halted and the quality of the block is set to bad.

Cross Check - COLSS looks at two (2) sensors monitoring the same parameter and alarms if their difference exceeds a dead band value. No automatic replacement is done, since COLSS doesn't know which is faulty (they're both in range). It just alarms to the operator on the alarm CRT that the cross check has failed. It is then up to the operator (or I&C technician) to determine the reason for the failure.

In summary, three different power level measurement techniques are employed by COLSS. The reactor coolant ΔT power, the secondary calorimetric power, and turbine power (based on a correlation of core power with turbine first stage pressure).

The reactor coolant ΔT power is a less complex algorithm than secondary calorimetric power and is performed at a more frequent interval (every second for ΔT power, versus every 30 seconds for the more detailed and accurate secondary calorimetric power). The secondary calorimetric power is used as a standard to periodically adjust the gain coefficient on the calculation of reactor coolant ΔT power. This arrangement provides the benefits of the secondary calorimetric accuracy and the reactor coolant ΔT power speed of computation.

The reactor coolant ΔT power is calculated based on the reactor coolant volumetric flow rate (calculated from RCP speed and ΔP), the reactor coolant cold leg temperature, and the reactor coolant hot leg temperature. The reactor coolant ΔT power contains a dynamic term which provides a rapid indication of power changes during transients. The static form of the equation used is $Q = m C_p (Th - Tc)$.

The secondary calorimetric power is based on measurements of feedwater flow rate, feedwater temperature, steam flow, and steam pressure. A detailed energy balance is performed for each steam generator. The energy output of the two (2) steam generators is summed and allowances are made for reactor coolant pump heat, pressurizer heaters, and primary and secondary system energy losses. The secondary calorimetric power is very

accurate at steady state, but due to the system response characteristics is less accurate during transients.

The turbine power is calculated based on turbine first stage pressure. Turbine power provides a leading indicator of core power changes in response to load changes.

The best features of the ΔT power and turbine power measurements are obtained by calibrating them to secondary calorimetric power in a manner that, at steady state, the calibrated powers equal the more accurate secondary calorimetric power. During transients calibrated powers closely track their respective uncalibrated powers affording the dynamic tracking ability of the latter. This calibration is performed with a long time constant ranging from 15 minutes to 2 hours, depending on final data constants. The long calibration time constant assures that for quick transients the response of ΔT power and turbine power are retained, but that in steady state, the more accurate secondary calorimetric will dominate.

12.3.5.2 Power Calculations

Figure 12.3-3 shows the power selection logic used in the COLSS. The highlighted lines show the power calculations and power selection logic used when above 15% reactor power. A detailed description of each of these blocks follows.

Reactor ΔT Power Calculation

The primary calorimetric power (BDELT) is calculated based on the compensated hot and cold leg temperatures (Th and Tc), pressurizer pressure, and reactor coolant mass flow rate (TMFLOW). The determination of BDELT involves the use of a static power term which calculates the enthalpy rise across the core and a hot leg dynamic power term. Calculation of BDELT is performed every second with values transmitted to both the plant power select operation and the ΔT power calibration.

Turbine Power Calculation

The turbine power (BTFSP) is calculated using a correlation based on turbine first stage pressure (TFSP) acquired from the process inputs. The value of turbine power is sent to both the plant power selection and the turbine power calibration. BTFSP provides a relatively fast indication of core power change due to load changes. It is calculated every second.

Secondary Calorimetric Power Calculations

The purpose of the secondary calorimetric is to calculate the reactor power based on a secondary side energy balance and the system energy losses and credits.

The inputs to the power calculation include feedwater flow, feedwater temperature, secondary pressure and steam flow rate. The COLSS calculates the energy transferred to each steam generator by standard thermodynamic methods.

Energy losses of the system include losses from letdown flow, coolant pump seals, cooling water flow, all the primary coolant leaving the system, coolant piping and other losses from the nuclear steam supply system.

Energy credits are obtained from charging pump operation, reactor coolant pump operation, pressurizer heaters, and other sources of electrically generated heat.

The secondary calorimetric power (BSCAL) is finally calculated by summing the energy of the

steam generator and the energy losses and credits. The result of this 30 second calculation is used in the plant power selection (PPS) operation and the ΔT/Turbine power calibration.

It must be noted that the steam flow sensor is not used to derive steam flow in the secondary calorimetric. Steam flow is derived from:

Steam Flow = Feed Flow - Blow down Flow.

Feed Flow is a sensed variable, however, blow down flow is a constant fed into the plant computer by the operator. Failure of the operator to use the correct value for blow down flow will therefore result in an erroneous secondary calorimetric calculation. This secondary calorimetric is used to calibrate the ΔT and TFSP powers to the more accurate secondary calorimetric value. Furthermore, this same BSCAL is used as the plant power measurement during daily calibration of excores and CPCs to match plant power.

Therefore, if this power measurement is improper, all power measurements used in the safety system will be improper. This is obviously not desirable, and it is extremely important that the operator be certain of the accuracy of the secondary calorimetric calculation, and be wary of sudden or gradual changes in plant electrical output for a given thermal power

Errors similar to this have been made at plants prior to the advent of COLSS, where erroneous feed flow indication and subsequent errors in reading power resulted in plant operation above 100% power.

12.3.5.3 Δ T and Turbine Power Calibration

The purpose of this operation is to calibrate the ΔT power (BDELT) and the turbine power (BTFSP) to the secondary calorimetric power (BSCAL). This update is performed every second.

The calibrated ΔT power (CBDELT) is found by summing BDELT and a current calibration term, calculated in the COLSS program.

Similarly, the calibrated turbine power (BTFSP) is found by summing BTFSP and the current turbine calibration term.

The values of CBDELT and CBTFSP which are calculated every one second are then sent to the plant power select operation.

12.3.5.4 Plant Power Selection

The function of the plant power selector is to determine the larger of the calibrated primary power (CBDELT) or the calibrated turbine power (CBTFSP) for use as plant power level (PP). This section also calculates a margin bias and has alternate selection logic which is used when one or more of the inputs is determined to be of bad validity.

A second function of the plant power selection is the calculation of a biased plant power for use by the power dependent insertion limit CEA application program.

12.3.5.5 Alternate Power Selection Logic.

The choice of the larger of CBDELT or CBTFSP is only valid when above 15% power, when the secondary calorimetric is being performed (it is not performed below 15% power).

When below 15% power, CBDELT and CBTFSP will be bad because BSCAL is bad by virtue of its not being run. In this case, COLSS

selects the larger of the uncalibrated ΔT power (BDELT) or turbine first stage pressure power (BTFSP) for plant power, as shown in Figure 12.3-4. As power increases above 15%, as indicated by the highest of BDELT or BTFSP, per the plant power selection logic, a sudden step change in power may be observed on the COLSS power meter as plant power switches to the highest of CBDELT or CBTFSP.

If the secondary calorimetric is bad due to sensor failures, the COLSS uses the same alternate power selection logic, selecting the highest of uncalibrated BTFSP or BDELT.

Figure 12.3-5 shows a different situation. Here ΔT Power is bad. It is more unlikely for this to happen than for secondary calorimetric power to fail because BDELT and BTFSP inputs all have alternate sensor selection logic if one sensor goes out of range. That is, all sensors used in other than the secondary calorimetric calculations have a backup sensor which is automatically substituted by COLSS for the failed (out of range) sensor.

If ΔT power should fail, COLSS selects the highest of secondary calorimetric or calibrated turbine first stage power, as shown in Figure 12.3-5.

It is interesting that one plant with CPCs (ANO-2) runs normally in this configuration because the quality of BDELT is set to bad. This stems from the Th anomaly problem, in which primary calorimetric calculations when above 15% power are considered invalid due to incomplete coolant mixing in the hot legs.

In general, the following are true:

1. If a block is bad, the block fed from that block will also be bad. For example, if BSCAL is bad, CBDELT and CBTFSP are bad and not used in power selection.

2. If a block fails, plant power will choose the highest of the remaining two blocks.

For example, if BSCAL is bad, plant power is the highest of BDELT or BTFSP. If BDELT is bad, plant power is the highest of BSCAL or BTFSP.

3. If two power blocks are bad, then COLSS selects the remaining good power for plant power.

4. If all three power measurements are bad, plant power is bad, and COLSS is out of operation, setting the COLSS master alarm.

The only exception to this rule is on Failure of CBTFSP, in which case CBDELT is plant power.

Since plant power can be one of several different power measurements COLSS must take into account the accuracy of the different measurement techniques when using alternate plant power selection logic. This is accomplished by selecting different plant power biasing terms for each selection choice from a lookup table. The biasing term represents a conservative uncertainty factor added to the measured power.

12.3.6 Power Operating Limit Calculation

As stated previously, COLSS can be thought of as being made up of a power calculation, and a power operating limit calculation. Actual plant power is not a direct input into the POL calculation because the POL portion of COLSS is looking for the hypothetical power which the plant could be raised to without violating the

LCOs on DNBR or LPD, based on current power distribution. COLSS therefore must calculate a power profile based on process inputs to derive the proper axial, radial, and azimuthal power profiles.

The inputs available to COLSS are similar to those available to the CPCs, but in many cases are more accurate. For example, the CPCs must rely on three levels of excore neutron detectors to provide power information, the COLSS uses five levels of incore detectors, centered at 10%, 30%, 50%, 70%, and 90% of core height. Furthermore, there are 56 such strings of in-cores scattered throughout the core. Therefore the axial power distribution as calculated by COLSS will be more accurate than that calculated by the CPCs

It is interesting that COLSS does not use in-cores to derive radial power distribution, although they would seem to be well suited to that application. Incores are used to derive radial power profile off line, using such programs as INCA or CECOR. However, these are time consuming. COLSS uses the quicker method of radial peaking factor lookup tables, as do the CPCs. COLSS lookup tables are more involved, and the CEA position measurement for COLSS is more accurate since it uses computer pulse counting rather than the reed switches used by the CPCs.

The combination of more accurate sensors, more detailed algorithms, and more computational time mean COLSS is, at least in normal system operation, more accurate than the CPCs. This increased accuracy translates into a less conservative DNBR POL than would have been calculated if the CPCs had been used, hence higher operating powers. With COLSS out of service, maintaining the DNBR POL per technical specifications will likely require a power reduction of as much as 10%.

12.3.6.1 Detailed Power Distribution Calculations (Figure 12.3-6)

The algorithm uses an axial and radial synthesis to construct a core hot pin power distribution. Incore detector signals are used to construct a core average axial power distribution. The axial power distribution is then combined with pre-calculated planar radial peaking factors appropriate to the various axial regions defined by differing control rod configurations. By combining the axial power distribution with axially dependent radial peaking factors, a pseudo hot pin power profile is established. This power profile is then increased by the amount of azimuthal flux tilt calculated from the several symmetric incore detector sets available. The resulting three-dimensional power peak and power distribution are used to calculate the linear heat rate power operating limit.

The core is regarded as being divided into several radial regions in the horizontal plane, selected by taking into account the locations of the CEA groups and the locations of the various generations of reload fuel. As many as five (5) radial regions are allowed with the flexibility to use any lesser number provided through the appropriate selection of region wise constants. Axial power profiles in the hot pin are computed in each radial region for use in the margin computations. These power profiles are calculated using peaking factors which relate the power in the hot pin in each region to the core average power. Tables of these planar radial peaking factors are stored in COLSS as a function of CEA configuration resulting from normal sequential insertion of the CEAs. Thus, using the known CEA positions to define the axial profile of each unique CEA configuration, appropriate planar radial peaking factors are selected and combined with the core average axial shape to yield a hot pin axial power profile for each radial region.

The radial peaking factors stored in COLSS are predetermined from a set of rodded and unrodded power distributions, all of which assume the presence of an equilibrium xenon distribution corresponding to the full power, unrodded condition. However, radial redistribution of xenon following changes in CEA configuration can influence the planar radial peaking factors. This effect is neglected in the COLSS power distribution algorithms. The resultant small error is accommodated by inclusion in the overall COLSS uncertainty assessment.

Flux tilts are detected by comparison, at various levels in the core, of signals from symmetrically located sets of fixed incore detectors. The region wise power distribution data is corrected by application of the computed flux tilt before proceeding with the margin computations. Deviated single CEAs or out-of-sequence CEA groups, should these occur, are signaled to COLSS by the plant computer based pulse counting CEA position indicating system. Tables of conservatively large penalty factors are applied to the power distribution information.

These calculations are performed in six major blocks:

1. Detector signal to flux,
2. Flux to equivalent power,
3. Planar radial peaking factors,
4. Axial power distribution,
5. Azimuthal tilt calculation and
6. 3-D power distribution.

12.3.6.2 Incore Detector Signal Compensation

Dynamic compensation of the incore detector signals is performed to compensate the detector signal for the beta decay behavior of the rhodium detector element. COLSS utilizes a digital filter to compensate for the relatively slow incore detector dynamic response. This is necessary because the incores are self-powered. That is, they have no external voltage across them during operation. The detector output is a current which is in reality the sum of the electrons produced in the beta decay of the activated Rh^{104} to Pd^{104}. This decay follows two half lives, with the predominant one being 42 seconds. This is too slow, even for COLSS. COLSS dynamically compensates the incore output to, in effect, predict what the correct final detector current value will be based on a quick sample of the change in detector current produced during a power change.

12.3.6.3 Flux to Power Calculations

The incore detector compensated neutron flux is converted to relative power at each incore detector location. This process consists of three (3) modules. Module one performs the flux to power calculation at each location and is performed at ten second intervals. Module two integrates the relative power for calculation of fuel burn-up factors and is also performed at ten second intervals. The third module calculates fuel burn-up factors from the integrated relative power signals and is performed on a daily basis.

12.3.6.4 Planar Radial Peaking Factors

Planar radial peaking factors are generated based on CEA group positions, calculated in the CEA scan program, and plant power. The

calculations are performed as part of the 10 second group of calculations and are used in the determination of the 3-D power distribution.

12.3.6.5 Axial Power Distribution

The axial power distribution is calculated from the detector power signals using a numeric curve fit to an average detector string. That is, all incore detector readings on a given core level are averaged, and the average output at that core height is compared with the outputs from the other four (4) heights to produce an axial power distribution. A new axial power distribution for an average detector string and a new axial shape index are calculated as part of the ten second group of calculations. The axial power distribution and ASI are used in the determination of the kW/ft plant operating limit.

12.3.6.6 Azimuthal Tilt Calculation

Azimuthal tilt is calculated from a number of selected axial rings of four (4) incore detector strings at each axial level. At each level the detector ring tilts are averaged into a level average tilt. The level tilts are weighted and summed to construct a composite core average azimuthal tilt index. This calculation is part of the ten second block of calculations.

Two (2) alarms are associated with azimuthal tilt. The lowest of these has a set point corresponding to the azimuthal tilt value used by the CPCs. The highest of these is the technical specification azimuthal tilt limit.

12.3.6.7 Three Dimensional Power Distribution

The purpose of the 3-D power distribution calculation is to synthesize a three-dimensional power distribution for use in the linear heat rate power operating limit calculation. This power distribution is synthesized by applying the fuel densification augmentation correction and planar radial peaking factors to the core average axial power distribution. The 3-D power calculation is performed as part of the 10 second block of calculations.

12.3.6.8 Power Operating Limit Calculation

The POL calculations in COLSS are primarily concerned with generating two distinct power operating limits, they are:

1. Linear heat rate POL (kW/ft) and

2. Thermal margin POL (DNBR).

The kW/ft power limit is calculated using the azimuthal tilt magnitude (AZTILT), and the 3-D power peaking factor distribution (DPSEL). kW/ft calculations are performed for 40 axial node positions, this in turn generates data for a pseudo hot channel model which conservatively establishes a POL. The kW/ft power limit is calculated as part of the 10 second block of calculations.

The thermal margin power limits are calculated as part of the 30 second block of calculations, however the DNBR POL update is performed every second.

The function of this area is to evaluate the core power operating limit (POL) based on the limiting thermal margin determined from DNBR, quality at the node of minimum DNBR, or void fraction. The limiting DNBR, quality, and void fraction are calculated and compared to predetermined limits. The core thermal power is the independent variable in these calculations. Core power is adjusted and the calculations are repeated

until the DNBR, the quality at the node of minimum DNBR, and the void fraction meet specified convergence criteria. The calculation can be divided into four (4) sections.

1. Core average pressure drop,

2. Closed hot assembly mass velocity iteration,

3. Open hot channel mass velocity iteration and

4. Thermal margin calculation and core power operating limit iteration.

The core average pressure drop is based on a subcooled fluid single axial node representation of the reactor core. The hot assembly, hot channel and core power operating limit calculations are based on 20 axial nodes. The minimum DNBR in the hot channel is compared against a specified limiting minimum DNBR. The axial node with the smallest difference between nodal equilibrium void fraction and its mass velocity dependent void fraction limit is defined to be the limiting void fraction node for the current value of POL. Increase in the POL will generally cause DNBR to decrease and cause void fraction and quality to increase. In addition, increasing the POL may cause the node of minimum DNBR or the limiting void fraction node to shift.

It should be noted that COLSS does not calculate the present DNBR, it merely performs an iterative procedure that substitutes values of plant power and underflow fractions with present core operation parameters to project what power limit will cause the DNBR to approach, but not exceed, its limiting value. Underflow fraction is the fraction of normal flow during a four (4) pump loss of flow at which minimum DNBR occurs, once all system time delays are accounted for.

The zone update section reevaluates the axial shape index (ASI) and the maximum integral radial factor to determine if the initial radial zone chosen should still be the limiting one. Otherwise, one (1) of the other four (4) radial zones shall be used and the DNBR POL updated.

The plant operating limit update is performed at one (1) second intervals. The present values of flow, primary pressure, cold leg temperature and power distribution are compared to the previous values used in the 30 second thermal margin calculation. If a significant difference is found the DNBR POL is updated to reflect the change in parameters.

12.3.7 Core Power Operating Limit Filtering and Alarm Annunciation

The power operating limit filtering provides continuous monitoring of plant power with respect to the licensed power limit and the calculated core power operating limits. Two (2) separate checks are performed, an instantaneous check using unsmoothed power and unsmoothed POL, and a steady state check using smoothed power and smoothed POL. When unsmoothed plant power exceeds a power operating limit, an alarm sequence is started.

The alarm on the CRT will read instantaneous DNBR power limit exceeded or instantaneous kW/ft power limit exceeded as appropriate.

When smoothed plant power exceeds a smoothed POL, an alarm sequence is initiated. The alarm on the CRT will read DNBR POL exceeded, kW/ft POL exceeded, or licensed power limit exceeded, as appropriate.

The difference between smoothed and unsmoothed power is that the unsmoothed power

is the value calculated every second, and will fluctuate in value as each calculation is made. The main control board (MCB) indicators for plant power, the DNBR POL and kW/ft POL are all derived from the unsmoothed power, as are the alarms listed above.

The unsmoothed power based alarms are actually biased, so that if the instantaneous power rises to the POL on DNBR or LPD, an alarm will not occur. The biasing term corresponds to 2% power on these instantaneous alarms, so that power must rise 2% above the POLs for the instantaneous alarms to initiate. This prevents spurious alarms caused by normal calculation fluctuations.

The smoothed plant power and power operating limits on the other hand, are filtered or averaged values. These are averaged over time to eliminate spurious fluctuations, and if the smoothed plant power should exceed the most restrictive of the smoothed DNBR POL, smoothed LPD POL, or licensed power, an alarm sequence will initiate. There is no 2% bias here. On the smoothed limits, if the plant power reaches the most restrictive limit, one (1) of the three (3) alarms previously described will result, as well as the COLSS power limit annunciator contacts being opened. The difference between the smoothed plant power and the most restrictive POL (kW/ft, DNBR, or licensed power) will be indicated on the MCB digital margin meter.

The filtering of the power operating limits and the plant power consists of a smoothing process utilizing a two (2) stage averaging procedure. The first stage takes the average of the last 10 calculations, so that 10 seconds worth of data is averaged in a block. This block is then output to a second stage in which the 10 second block is averaged with the previous nine (9) 10 second blocks to produce a smoothed output. As new 10 second blocks are fed into the second stage, the oldest block is discarded, so that a 10 point running average results, with each of the 10 points representing in turn the average of ten individual one (1) second calculations.

Plant technical specification surveillance requirements require that corrective action be taken when the plant power operating limits are exceeded in the steady state. To meet these requirements the length of time over which the reactor was operated with a margin alarm set must be measured and monitored for each event. For example, technical specifications specify that if kW/ft or DNBR should exceed their limits, corrective actions should be taken within 15 minutes. For this reason there are LPD alarm duration exceeded and DNBR alarm duration exceeded alarms, set for 15 minutes. If an alarm condition exists for 15 minutes, this alarm will set. This alarm is cleared once the alarm condition clears.

There are also provisions for annual violation alarms on DNBR, LPD, and licensed power. COLSS has a timer which keeps track of the total amount of time an alarm condition has been exceeded. When the power limit alarm resets, the clock does not reset, but rather awaits the next alarm condition, then adds the time of the new violation to the total. If technical specifications should specify a maximum amount of time per year that the alarm condition can be in, similar to the present requirement on CEA insertion limits, the annual violations alarm will be set when this limit is exceeded. There is presently no such time limit applicable to COLSS, but the feature is there. The annual duration timer must be manually reset at the plant computer.

12.3.8 Summary

COLSS continually calculates DNB margin, peak LHR, ASI, total core power, and azimuthal tilt magnitude and compares the calculated values to the limiting condition for operation on these parameters.

COLSS, in conjunction with the CPCs, allow the core to be operated at higher power densities than previous designs.

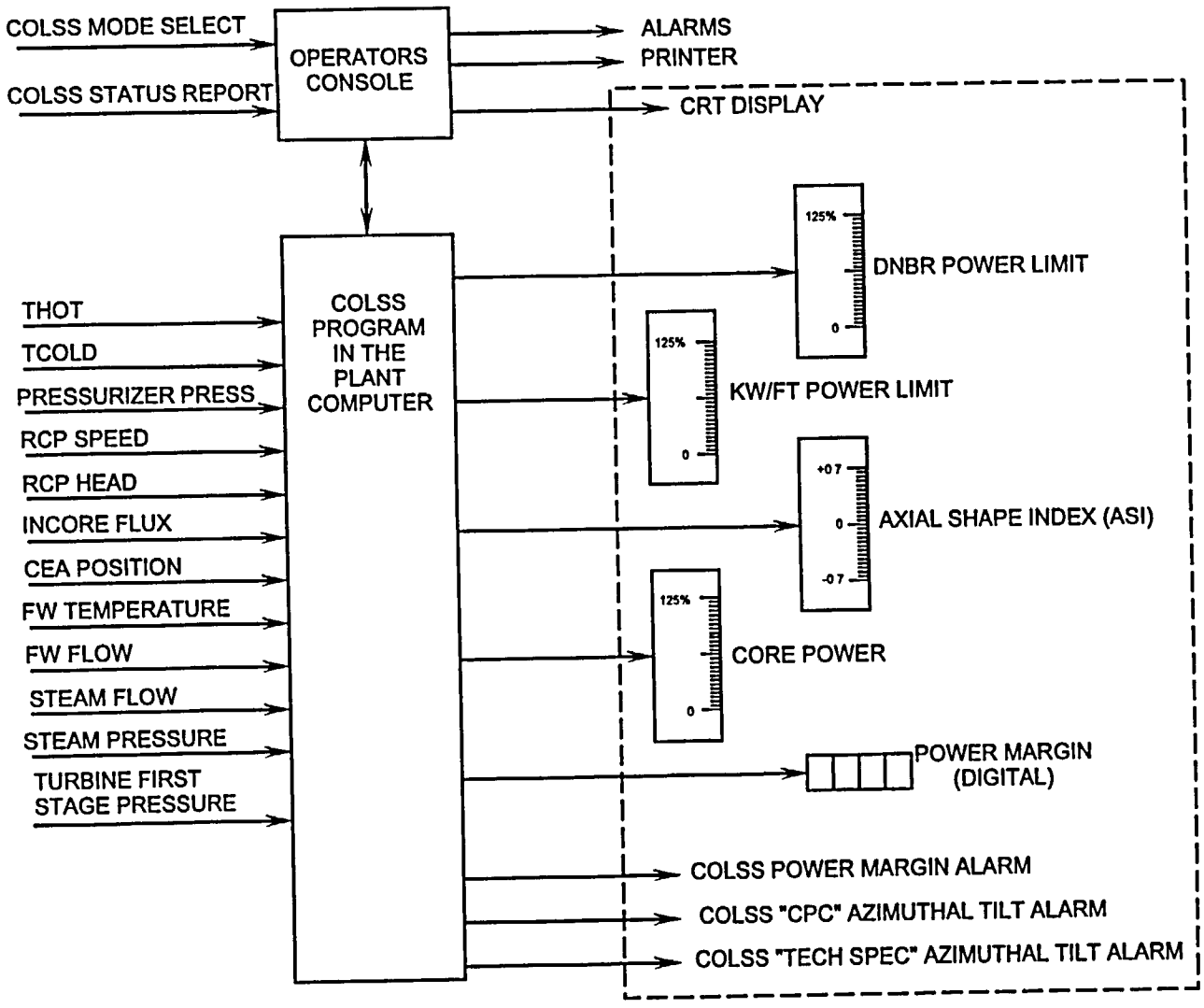


Figure 12.3-1 Core Operating Limit Supervisory Systems (COLSS)

1000-12

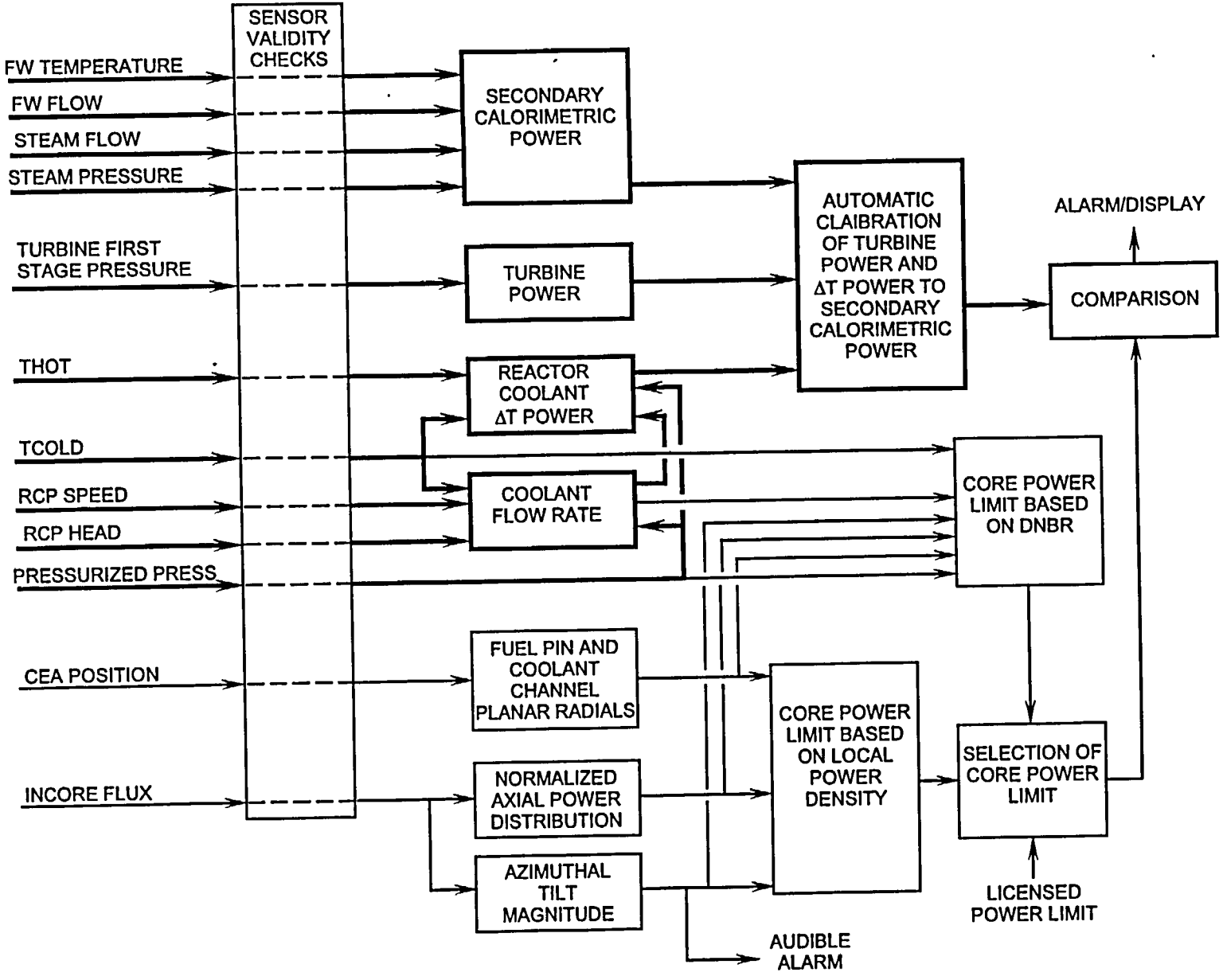


Figure 12.3-2 Functional Diagram of Core Operating Limit Supervisory Systems (COLSS)

1000-12

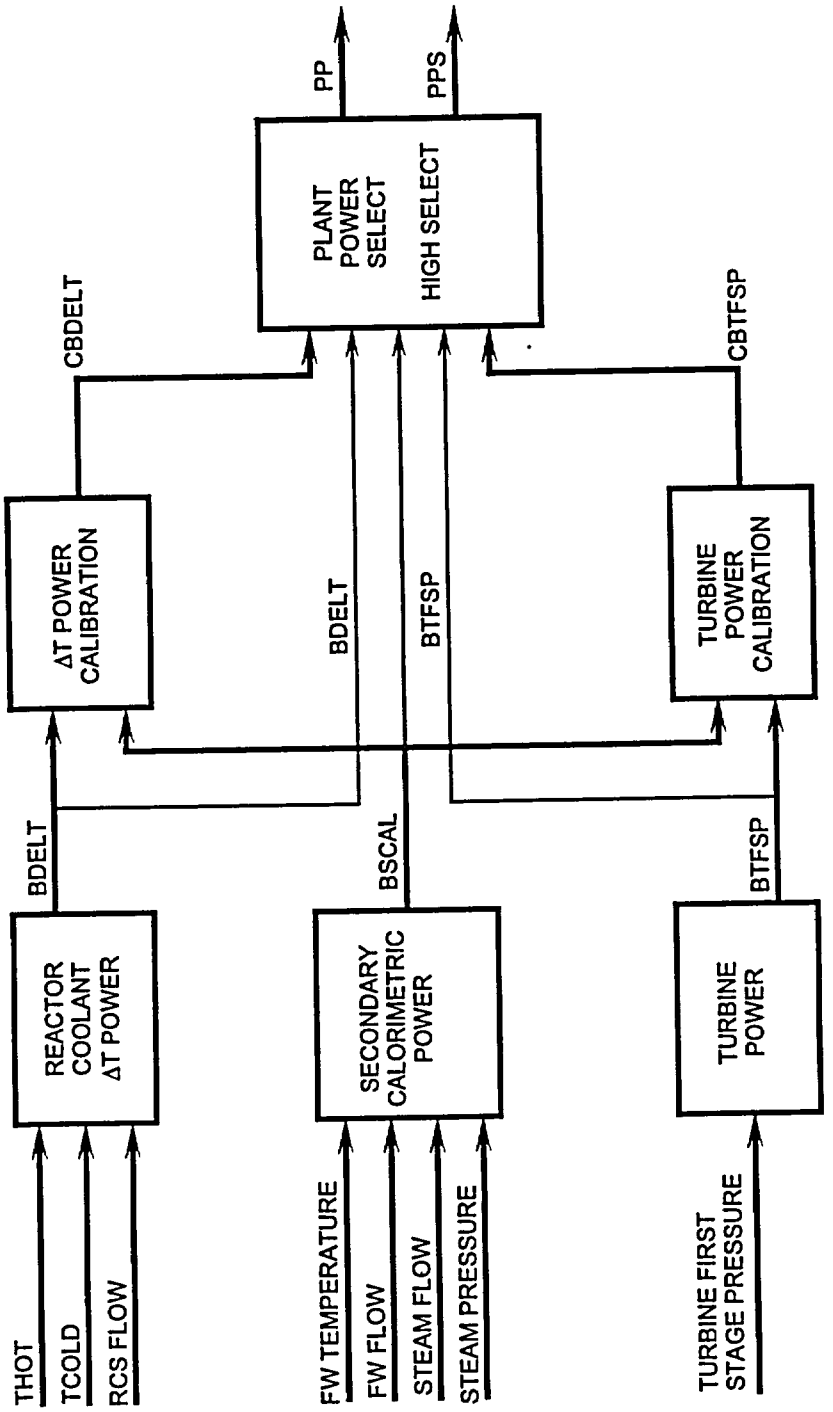


Figure 12.3-3 Power Calculations - Normal Power Operation Above 15%

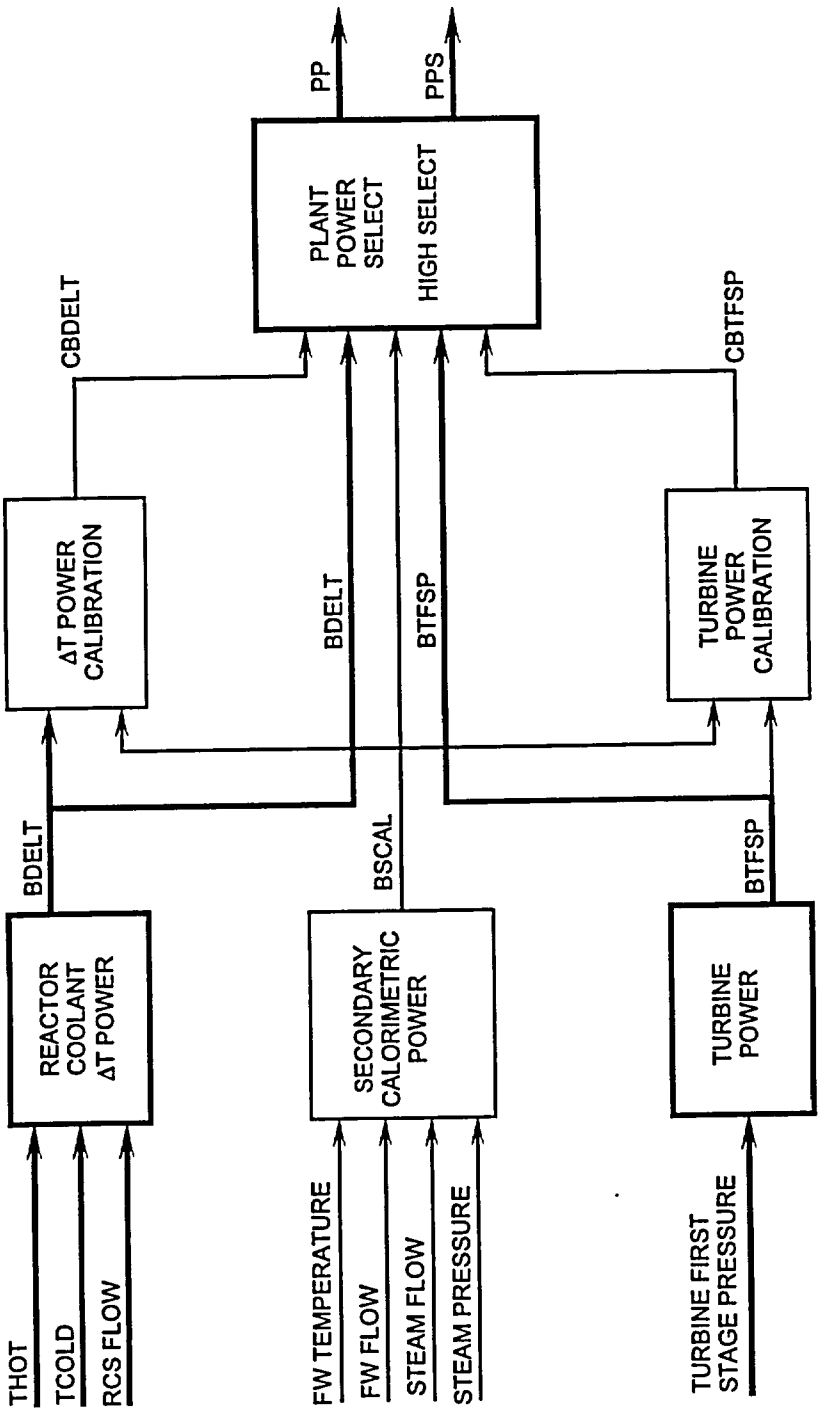


Figure 12.3-4 Power Calculations - Power Operation Below 15% or With BSCAL Bad

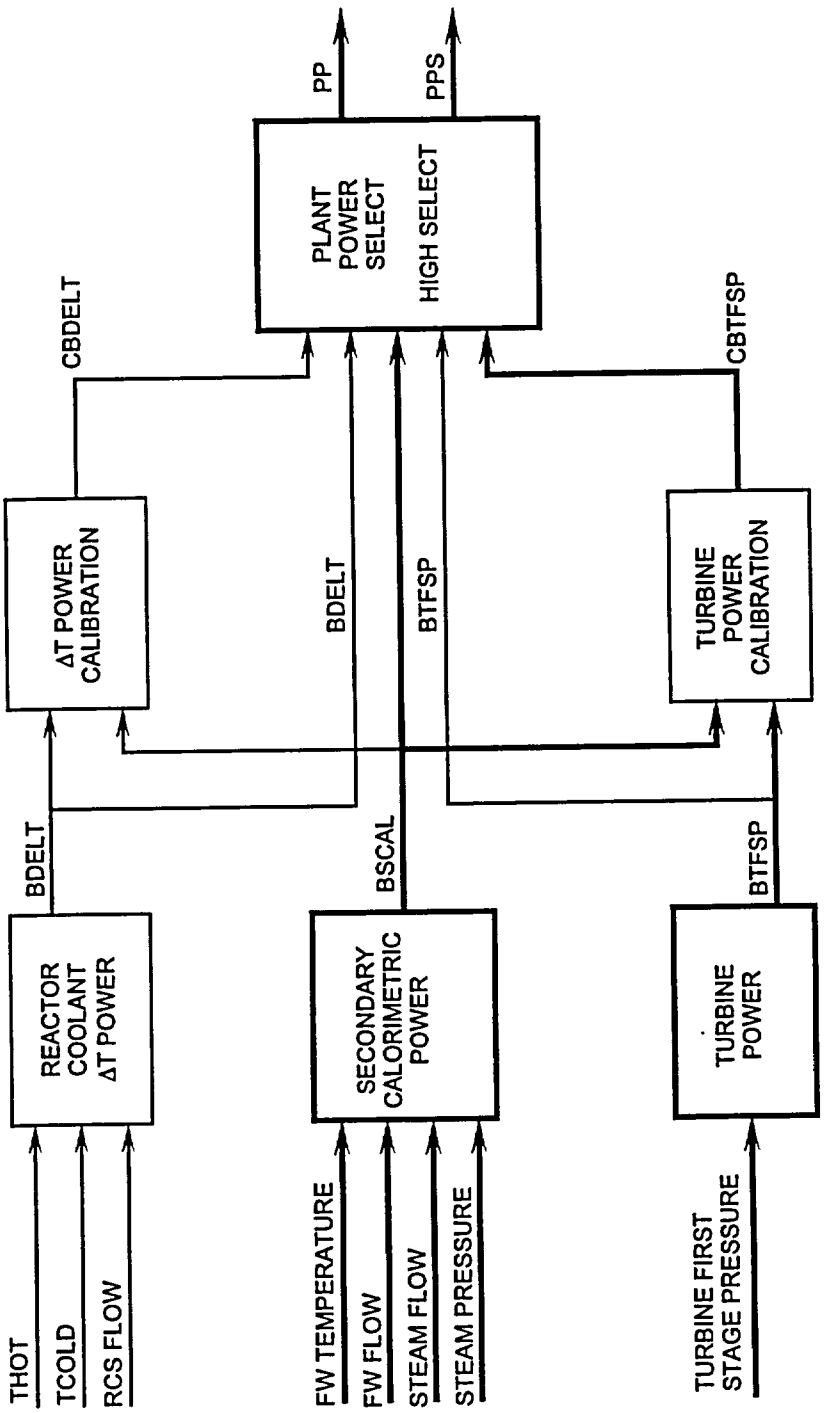


Figure 12.3-5 Power Calculations - Power Operation Above 15%, BDELT Bad

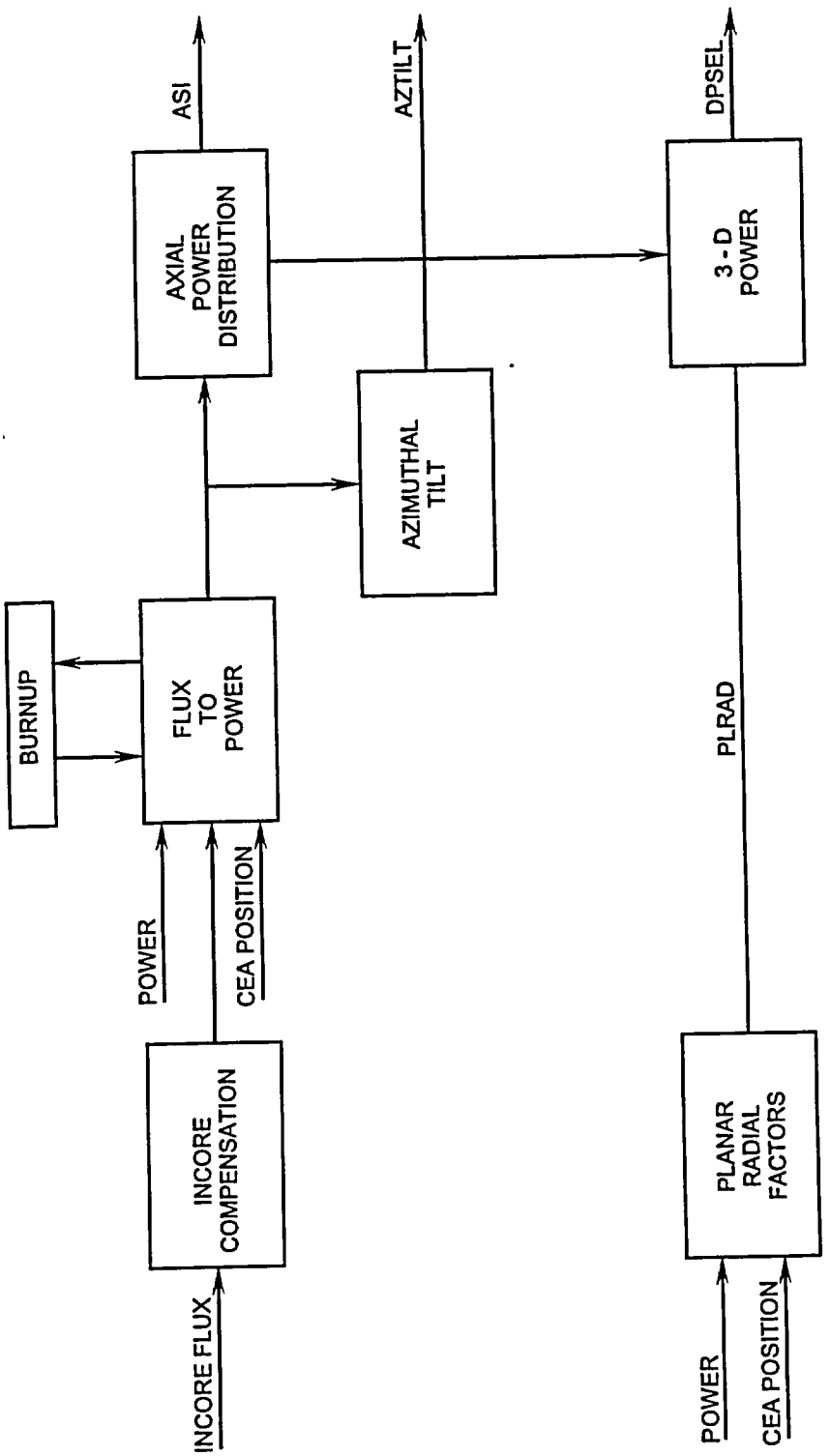


Figure 12.3-6 Power Distribution

TABLE OF CONTENTS

12.4 PLANT PROTECTION SYSTEM (PPS)

LIST OF FIGURES

LIST OF FIGURES (continued)

12.4 Plant Protection System

Learning Objectives:

1. State the purpose of the reactor protection system (RPS).
2. State the purpose of the engineered safety features actuation system (ESFAS).
3. Explain the purpose of each reactor trip.
4. Explain how the two (2) out of four (4) RPS trip logic is derived.
5. Explain the reactor trip circuit breaker trip logic.
6. List the operating bypasses incorporated into the Plant Protection System.
7. Explain the effect of placing an RPS trip in trip bypass.
8. Explain the operation of the low pressurizer pressure trip circuitry.
9. Explain the operation of the low Steam generator pressure trip circuitry.
10. Explain the ESFAS logic.
11. Explain the purposes of the ESFAS signals.

12.4.1 Introduction

(Figure 12.4-1)

The severity of a reactor accident depends on the extent of fuel damage, the extent of any release of radioactive fission products from the Reactor Coolant System (RCS) boundary, and the extent of any release of this radioactive material to the environment where it then threatens the health and safety of the general public. There are several ways to limit the severity of an accident in these terms. One way is to prevent or minimize fuel damage during an accident, another is to contain any radioactive release such that it never reaches the general environment.

The Plant Protection System (PPS) is designed to sense abnormal occurrences and/or accidents in the reactor plant and to initiate automatic actions to place the plant in a safe condition to maximize the capability of plant systems to maintain the integrity of the three fission product barriers. The PPS can be broken down into two subsystems; the Reactor Protection System (RPS) and the Engineering Safety Features Actuation System (ESFAS).

The PPS recognizes and protects the three boundaries between the radioactive fission products in the reactor core and the general public; the fuel cladding, the RCS system piping, and the Containment Building. Engineered Safety Feature (ESF) systems are specifically designed to protect the integrity of these boundaries, thereby ensuring that the health and safety of the public is protected. Specified Acceptable Fuel Design Limits (SAFDLS), Safety Limits, and Limiting Safety System Settings (LSSS) have been established for this purpose.

During an emergency, the RPS rapidly inserts the Control Element Assemblies (CEAs) to shutdown the nuclear chain reaction to reduce the heat generation rate. This action limits peak fuel centerline and cladding temperatures along with RCS temperatures and pressures. The ESFAS actuates valves, pumps, fans, and other plant equipment to enhance the ability of the plant to protect the three fission product barriers.

12.4.2 Reactor Protection System

The Reactor Protection System (RPS) monitors various plant parameters, such as reactor power, Reactor Coolant System (RCS) temperature, pressurizer pressure, steam generator water levels and pressures and trips the

reactor when a limit is approached. A reactor trip under these circumstances is intended to maintain the integrity of the fuel cladding and RCS boundaries during any Anticipated Operational Occurrence (AOO) and limit offsite radiation doses to within the limits of 10CFR100 during any design basis accident. In addition, the RPS aids the Engineered Safety Features (ESF) in the event of an accident by shutting down the reactor.

12.4.2.1 Design Basis

The RPS is designed to perform the following:

1. Prevent exceeding any SAFDLs during any AOO. SAFDLs are limits on monitored plant parameters which will assure the integrity of the fuel clading. Combustion Engineering has defined Linear Heat Rate (LHR) and Departure from Nucleate Boiling Ration (DNBR) as the two SAFDLs of interest.

2. Comply with 10CFR50, Appendix A, Criterion 21, which addresses protection system reliability, testability, redundancy, and independence. These features are designed into the PPS such that:

   a. No single failure will result in the loss of protective function, and
   b. Removal of any channel or component from service will not result in loss of the required minimum redundancy, and
   c, The PPS can be periodically tested at power without tripping the reactor or causing any protective actuation signals.
   d. To comply with the following provisions of IEEE-279 Criteria for Nuclear Power Plants:
      1.) Four independent measurement channels are provided
      2.) No single failure will prevent protective action.
      3.) System actuation on selected plant variables will be 2/4 coincidence.
      4.) When one channel is out of service, coincidence logic is reduced to 2/3.
      5.) Protective logic assumes the de-energized state to trip.
      6.) Manual reset is necessary once actuation is initiated.
      7.) Manual actuation is available and independent of automatic actuation.
      8.) System can be tested with the plant shutdown or operating.
      9.) System functions requiring operator attention or action during routine plant operations are displayed and/or controlled on the Main Control Board (MCB).
      10.) Selected plant variables may be manually blocked or bypassed during plant startup and shutdown evolutions.
      11.) All manually blocked or bypassed variables are automatically unblocked when permissive conditions no longer exist.
   e. To provide adequate protection during AOOs.
   f. To alert the operator when any monitored plant condition is approaching a condition that would initiate protective action.
   g. To ensure that protective action will not be initiated due to normal operation of the generating station.

12.4.2.2 Reactor Trips
(Figures 12.4-2 & 12.4-3)

High Linear Power

The High Linear Power Trip provides reactor core protection against rapid reactivity excursions which might result from an ejected CEA.

High Log Power Trip

The High Log Power Trip assures the integrity of the fuel cladding and RCS boundary due to an unplanned criticality from a shutdown condition, which could be caused either by CEA withdrawal or inadvertent dilution of the RCS.

Local Power Density (LPD)

The Local Power Density trip prevents the linear heat rate (Kw/ft) in the limiting fuel rod in the core from exceeding the fuel design limit in the event of any AOO. This trip setpoint is calculated in the Core Protection Calculators (CPCs) and is variable depending on plant parameter combinations at any given time.

Low Departure from Nucleate Boiling Ratio (DNBR)

The Low Departure from Nucleate Boiling Ratio trip prevents the DNBR in the limiting coolant channel in the core from exceeding the fuel design limit in the event of any AOO. This trip setpoint is calculated in the CPCs and is variable depending on plant parameter combinations at any given time.

High Pressurizer Pressure

The High Pressurizer Pressure Trip, in conjunction with the Pressurizer and Main Steam safety valves, provides RCS over pressure protection during a loss of load without reactor trip.

Low Pressurizer Pressure Trip (Figure 12.4-4)

The Low Pressurizer pressure Trip assists the ESF systems in the event of a Loss of Coolant Accident (LOCA) by tripping the reactor early in anticipation of reaching the ESF protective action setpoint. In addition to a LOCA, the Low pressure trip could be caused by an excessive cooldown or a Main Steamline Break (MSLB). During plant depressurizations and cooldown, this setpoint can be manually reset to a new setpoint 400 psia below existing pressurizer pressure to a minimum of 100 psia. Below 400 psia the trip may be bypassed.

Low Steam Generator Pressure Trip (Figure 12.4-5)

A Low Steam Generator Pressure Trip provides protection against an excessive heat removal from the Steam Generators and subsequent RCS cooldown. The resulting RCS cooldown represents an uncontrolled positive reactivity addition.

Low Steam Generator Level Trip

A Low Steam Generator Level Trip from each Steam Generator provides protection against events involving a mismatch between steam and feedwater flow. This trip ensures that a reactor trip will occur before the Steam Generator heat sink is lost. It also ensures that RCS design pressure will not be exceeded prior to the time that Emergency Feedwater can be supplied for decreased heat removal events.

High Steam Generator Water Level Trip

A High Steam Generator Water Level Trip protects the turbine from excessive moisture carryover.

High Containment Pressure Trip

The High Containment Pressure Trip provides assurance that a reactor trip is initiated concurrently with safety injection, containment isolation, and main steam isolation signals. This aids in preventing exceeding the containment internal design pressure during a design basis LOCA or MSLB.

Steam Generator Low Flow Trip

The Steam Generator Low Flow Trip provides protection against a Reactor Coolant Pump (RCP) sheared shaft event and a steam line break event concurrent with a loss of offsite power. It monitors RCS flow on the primary side of the Steam Generator to trip the reactor on loss of RCS flow. This trip is necessary because the Core Protection Calculator (CPC) generated DNBR protection uses RCP speed sensors for RCS flow indication and can't sense a loss of flow due to a sheared shaft incident.

Reactor Trip on Turbine Trip

Normally this trip is supplied to remove the heat source from service by reactor trip when the turbine is tripped in anticipation of a possible loss of heat sink. The setpoint and need for this trip is plant dependent. The need is determined by the existence of the Reactor Power Cutback (RXC) system and the capacity of the Steam Dump and Bypass Control system.
For plants that have the RXC system installed this trip is not required for plant safety and is normally disabled.

Manual Reactor Trip

Manual reactor trip is provided to permit the operator to trip the reactor manually from the Main Control Room per the design bases requirements.

12.4.2.3 Reactor Trip Methodology (Figures 12.4-6, 12.4-7. 12.4-8 & 12.4-9)

Process instrumentation sensors monitor selected plant parameters and send status to the RPS. This information is compared to bistable setpoints for each input parameter to determine if an unsafe plant condition is being approached, such as Pressurizer pressure decreasing or reactor power increasing above operating limits. The bistables convert the analog inputs into digital outputs for use by the RPS coincidence logic circuits to determine if a trip is necessary.

Coincidence logics are used to prevent a single instrument failure from causing an unnecessary reactor trip or preventing a needed one. This is done by using four independent and electrically separate sensor channels to compare critical plant parameters to trip setpoints and by basing protective action on at least two of the four sensors exceeding their trip setpoints. These channels, designated "A", "B","C", and "D" each have their own sensor with physically and electrically separated signal leads, power supplies, and bistables. A trip on one channel out of four will only cause an alarm, but two or more channels must trip to satisfy the 2/4 trip coincidence logic and establish a reactor trip path. Four input channels require six logic circuits to check for a two-out-of-four coincidence. These six coincidence circuits are called matrices. Each two-out-of-four coincidence matrix has four normally energized matrix output relays associated with it (6AB1, 6AB2, 6AB3, 6AB4 where the "6" prefix is the designation for the RPS portion of the PPS; the ESFAS portion has a different prefix). The four output relays for each matrix each operate one fail-open (energized closed) contact in each of four reactor trip paths (e.g., contacts 6AB1, 6AB2, 6AB3, 6AB4). A reactor trip path consists of six contacts in series, one for each associated matrix output relay. For example, trip path 1 has six normally closed contacts (6AB1, 6BC1, 6BD1, 6AC1, 6CD1, and 6AD1) wired in series. These contacts are fed from normally energized matrix output relays of the same designation.

There are 15 different reactor trip bistables in each of the four PPS channels. They can be readily identified by the three red RPS bistable relay indicating lamps immediately beneath them that correspond to each bistable's trip status in the

associated logic coincidence matrices. Assume that trip bistables for channels "A" and "B" monitor the same reactor trip parameter. When this parameter exceeds its trip setpoint, bistables "A" and "B" will trip, the "AB" matrix will detect a 2/4 coincidence and de-energize its four matrix output relays (6AB1, 6AB2, 6AB3, and 6AB4). Contacts 6AB1, 6AB2, 6AB3, and 6AB4 will fail open in the four trip paths and remove power to four solid state relays (SSRs) which drive normally energized relays K1, K2, K3, and K4. Note that just one coincidence logic matrix will trip all four reactor trip paths. The purpose of a trip path is to let the Reactor Trip Switchgear (RTSG) circuits know that at least one matrix has tripped, indicating a coincidence trip in at least 2/4 channels. Note that each relay operates two reactor trip circuit breakers (TCBs).

1. K1 operates TCB1 and TCB5
2. K2 operates TCB2 and TCB6
3. K3 operates TCB3 and TCB7
4. K4 operates TCB4 and TCB8

A reactor trip is accomplished by removing electrical power from the Control Element Drive Mechanism Control System (CEDMCS), which will cause the CEDMs to release the Control Element Assemblies (CEAs) and allow them to drop into the core by gravity. The CEDMs are powered from two 100% capacity CEDM Motor Generator sets (CEDM MGs), both of which are normally running in parallel. The power must pass through the eight TCBs, arranged in four parallel sets of two breakers in series. The function of the K relays is to trip the TCBs when required to remove power from the CEAs, tripping the reactor.

The breaker tripping arrangement is called a selective two-out-of-four scheme because not all possible 2/4 TCB pair combinations will cause a reactor trip. For example, if K1 and K2 trip TCBs 2,6,1,and 5, the reactor will not trip since the CEDMs will remain energized via TCBs 3, 7, 4, and 8. However, if K2 and K3 trip TCBs 2, 6, 3, and 7, then both power paths are interrupted and a reactor trip will occur. In other words, to trip the reactor, two of the four K relays must be de-energized as follows: (K1 or K2) AND (K3 or K4). De-energizing only the K1 and K2 relays will not trip the reactor, nor will de-energizing only relays K3 and K4 trip the reactor.

Note that the reactor trip function is de-energize to trip as required by the design bases. The bistable outputs de-energize, which de-energizes the matrix output relays, which de-energizes the K relays, which de-energizes the TCB undervoltage coils and energizes the shunt trip coils, which opens the TCBs and de-energizes the CEDM coils, tripping the reactor.

12.4.2.4 Logic Matrices (Figures 12.4-10, 12.4-11, 12.4-12 & 12.4-13)

Once a logic matrix has determined a 2/4 coincidence, it must actuate a reactor trip path. The six logic matrices are designated "AB", "AC", "AD", "BC", "BD", and "CD". The "AB" matrix monitors all trip signals from the RPS channel "A" and channel "B" trip bistables. For example, if a trip in channel "A" Hi Linear Power occurs coincident with a trip in channel "B" Hi Linear Power, the matrix will trip. The remaining matrices function in the same manner, comparing their respective channels bistable trip relays for a coincident trip condition.

Each matrix consists of bistable relay contacts connected in the form of a ladder. Auctioneered DC power supplies from each channel are connected in parallel to one end of the ladder. Four matrix output relays, 6AB1, 6AB2, 6AB3, and 6AB4, are connected in parallel at the other end. With this configuration, a failure of one of the power supplies will not result in a complete matrix trip; however, two relays will trip and cause two K relays to de-energize, tripping half the RTBs (this is not enough to trip the reactor). This situation can occur on loss of a single 120 VAC power supply failure. When a logic matrix

does trip, its four matrix output relays will de-energize. The matrix output relays open contacts in four trip paths and de-energize the four K relays to initiate a reactor trip.

In Figure 12.4-10, the "AB" matrix for reactor trip is shown with no trip signals present. Current flows down both legs of the ladder through the closed bistable relay contacts, energizing the four matrix output relays, 6AB1 through 6AB4, at the bottom of the ladder. All of the bistable relay indicating lamps are off. Note that the bistable relay lamps are red light emitting diodes (LEDs). These red LEDs turn on when the bistable trips. This differs from other RPS indicating lights which usually de-energize, or go off, on a trip.

Figure 12.4-11 shows the "AB" matrix with a Hi Linear Power Trip in channel "A". The channel "A" Hi Linear Power Trip bistable relay contacts at the top of the ladder have opened. The four matrix output relays remain energized through the right side of the logic matrix. The "AC" and "AD" matrices would be in the same configuration with a trip in channel "A" High Linear Power.

In Figure 12.4-12, the effect of adding a High Logarithmic Power Trip in channel "B" with a High Linear Power Trip in channel "A" is shown. The path across the matrix ladder allows the matrix output relays to stay energized, preventing a reactor trip in the case where tripped bistables are not for the same trip function. The three LED bistable relay indicating lamps will be illuminated under the HI LN PWR window in channel "A" and three under the HI LOG PWR window in channel "B".

See Figure 12.4-13 for a valid reactor trip condition in which both channels "A" and "B" have a High Linear Power trip condition (bistables A1 and B1 tripped). When the A1 and B1 bistables trip, they each de-energize three bistable relays. The contacts for bistable relay A1-1 are in the "AB" matrix. Those for A1-2 and A1-3 are in the "AC" and "AD" matrices, respectively. Similarly, the B1-1, B1-2, and B1-3 bistable relay contacts are in the "AB", "BC", and "BD" matrices, respectively.

As a result of the A1-1 and B1-1 contacts being opened, power is lost to the four matrix output relays, 6AB1, 6AB2, 6AB3, and 6AB4. The de-energized matrix output relays will open contacts in trip paths 1, 2, 3, and 4 (refer to figure 14), de-energizing the four K relays, which will trip open the RTSG TCBs.

It should be noted that if two or more different trips come in on a matrix ladder at the same time, only the highest (uppermost) bistable indicating lights will be illuminated due to the matrix contact arrangement. For example, if the reactor trips on Low Steam Generator Level, then initially the bistable relay indicating lights for Low Steam Generator Level will come on. If, as the reactor trips, the Hi LPD trip also comes in, then the final state will show the bistable relay indicating lamps on for only the Hi LPD trip but not for the low Steam Generator Level trip. This means that the RPS front panel indication related to the matrix output relay lamps cannot be used as a "first out" indication.

12.4.2.5 Operating Bypasses
(Figure 12.4-14 & 12.4-15)

Operating bypasses have the following characteristics:

1. Performed during normal plant operations to bypass certain trips to permit plant operation during startup, shutdown and low power testing conditions.
2. Affects 4/4 protection channels for a particular trip function.
3. Generally done via key switches in the Control Room. May also be done by pushbuttons or automatically.
4. Generally have individual alarms associated with the bypass.

Note: The periodic resetting of the Low Pressurizer pressure and Low Steam Generator pressure setpoints during a cooldown is not considered as an operating bypass since the trips are still in effect but at a different setpoint.

The following is a list of the PPS operating bypasses:

1. The CPC trips (DNBR and LPD) have an operating bypass to allow system tests at low power when pressurizer pressure may be low or the RCPs may be off. The bypasses are accomplished by key switches on each of the four CPC Remote Operators Modules. The trip will automatically reinstate,
2. The High Logarithmic Power Trip has an operating bypass to allow the reactor to be brought to the power range in a controlled manner during a reactor startup. The bypass is accomplished by depressing pushbuttons on each of the four PPS Remote Operators Modules. The trip will automatically reinstate.
3. The RPS/ESFAS Pressurizer Pressure Trip/Safety Injection Signal (SIAS) has an operating bypass to allow system testing at low pressure and to allow heatups and cooldowns with shutdown CEAs withdrawn and without actuating an unnecessary SIAS. The bypasses are accomplished by key switches on each of the four PPS Remote Operators Modules.
4. The Low Steam Generator Flow Trip is bypassed to allow CEDMCS maintenance with a low flow condition in the RCS. The bypass is accomplished by key switches on each of the four PPS Remote Operators Modules.
5. The High Steam Generator Water Level Trip is bypassed to accommodate Steam Generator level control swings during startup without causing a reactor trip. The bypass is accomplished by key switches on the PPS Remote Operators Module.
6. The Reactor Trip on Turbine Trip is bypassed if the Reactor Power Cutback System is available. The trip is bypassed in total from the reactivity control station. Individual channels may be bypassed by key switches on the PPS Remote Operators Module.

12.4.2.6 Trip Channel Bypasses (Figure 12.4-16)

Trip channel bypasses have the following characteristics:

1. May be done to only one channel at a time for a particular trip function for testing, maintenance, or removal from service due to inoperability.
2. Affects 1/4 protection channels for a particular trip function. Attempting to bypass two channels at the same time unbypasses both channels.
3. All trip channel bypasses annunciate a common alarm in the control room.

All trip bistables have Trip Channel Bypass capability to remove them from service for maintenance or testing. When one channel's bistable, for a particular trip function, is in Trip Channel Bypass, the trip logic is converted to 2/3 by relying on the three remaining channels. This bypass is both initiated and removed manually by toggle action pushbuttons (shown on Figure 12.4-8). There is an electrical interlock which allows only one channel for a given trip function to be bypassed at a time. Attempting to place two bistables in Trip Channel Bypass for a given trip function will result in both bistables defaulting to an unbypassed condition.

12.4.2.7 CEA Withdrawal Prohibits (Figure 12.4-17)

CEA Withdrawal Prohibit (CWP) signals are designed to increase plant availability by

prohibiting CEA withdrawal when certain pretrip conditions exist. No credit is taken for CWPs in the safety analysis. A CWP signal is sent to the Control Element Drive Mechanism Control System (CEDMCS) where it blocks CEA withdrawal in all mode except MANUAL INDIVIDUAL. CWPs are processed via the PPS and include a CWP generated by 2/4 Hi Pressurizer Pressure pretrips and several CWPs generated within the CPCs.

CPC-generated CWPs are:

1. 2/4 low DNBR or High LPD Pretrips.
2. Regulating subgroups deviation.
3. Regulating group out of sequence.
4. Excessive Part-Length CEA insertion.
5. Single CEA deviation (CEACs).

The CPC generated CWPs are automatically bypassed if power decreases below the range of 7.0E-5% and 10E-4% power to allow reactor startup operations since the CPCs cannot accurately calculate DNBR and LPD pretrips below that power level to actuate CWPs in a reliable manner. The Hi Pressurizer Pressure CWP is not bypassable.

12.4.2.8 PPS Testing

Power Trip Test Interlock

Since the Four Nuclear Instrumentation system safety channels input to the CPCs, an inoperable safety channel would render the affected trip circuits inoperable. To ensure conservatism, there is an interlock between the CPCs and the safety channels such that an inoperable safety channel will force the DNBR and LPD trip circuits to the tripped condition.

Safety channel trouble conditions that will actuate the Power Trip Test Interlock are:

1. Safety channel high voltage low.
2. Loss of safety channel drawer voltage.
3. Loose or removed circuit card in the safety channel drawer.
4. Calibrate or test safety channel drawer switches out of either the "OFF" or "OPERATE" positions.

In addition to the Power Trip Test interlock, there are other trip test interlocks associated with the safety channels. Since the safety channels input to the PPS for Hi Linear Power and Hi Log Power Trips, taking the LINEAR CALIBRATE switch out of "OFF" will cause a HI Linear Power trip in the affected channel and taking the LOG CALIBRATE switch out of "OFF" will cause a Hi Log Power trip in the affected channel.

CPC Test Enable

Before going into test mode, both the DNBR and LPD functions are placed in Trip Channel Bypass. This enables power to the CPC test circuitry and bypasses the DNBR and LPD channel trips to allow testing. A key switch allows access to the CPC for testing. A test teletype is connected to the CPC channel to facilitate the testing. The teletype may also be used to to dump a CPC trip buffer report following a reactor trip.

12.4.2.9 PPS Testing Design Features

The RPS has been designed to be functionally testable both at power and shutdown. The entire protective signal flow path is testable. The input sensors are continually checked during normal operation by comparing the outputs of similar channels and cross-checking them with related instruments. During extended shutdown and refueling periods, the sensors are checked and calibrated against known standards. This testing covers the sensor up to where it enters the RPS. RPS testing covers the entire RPS scope beginning with the sensor output where it enters the RPS, extending all the way through the protective system, and ending with the final actuation devices (TCBs). For convenience of

testing, the protection circuit (signal flow path) testing is done in an overlapping fashion by dividing the protection circuit testing into three segments: bistable testing, logic matrix testing, and trip path testing. Each segment overlaps adjacent segments such that performing all three segments individually ensures that the overall circuit path is tested and operable and that no part of the circuit is omitted

Bistable Testing

The bistable testing will verify that the bistable comparator cards actuate their respective trip relays at the proper setpoints. The bistable relays, the matrix relays and the ESFAS actuation relays are double-coil relays; that is they have both primary and secondary coils. The primary coil is fed by the normal actuation input signal. The secondary coil is a test coil that can generate a flux that is either the same polarity as the primary coil ("aiding") or the opposite polarity ("bucking"). For a bistable relay, the primary coil is fed from a process input sensor via a driver, while the test coil generates a bucking magnetic flux. Thus, energizing the test relay will cause the magnetic fluxes to "cancel out" and the relay will go to its de-energized, tripped position. Any bistable can then be "tripped" by energizing the test coil for that particular bistable trip function without affecting the primary coil or its input sensor signals.

Matrix Testing

Each matrix and each pair of ladder contacts within the matrix is individually tested by manipulation of switches and pushbuttons located on the six Matrix Test Modules (MTMs). The MTMs are separate and independent such that each MTM only tests one matrix. Additionally testing is limited to a single RPS trip function at a time due to the hardwiring of switches. Like the bistable trip relays, the matrix output relays are also double-coil relays. To allow testing, these test coils are wired as aiding coils (same polarity as the primary coils); that is, they will maintain the matrix output relay contacts in the energized state even if the primary coil is de-energized. The design intent of the test switches is to increase testing reliability and minimize the probability of a spurious reactor trip. The testing process checks that the bistable trips are capable of opening the necessary contacts in the matrix ladder to de-energize the matrix output relays. The test coils energizing ensure that the K relays stay energized and that the TCBs remain closed.

Trip Path Testing

The trip path testing will open one of the four trip paths (six series contacts) and actually trip one set of two series TCBs. However, the remaining three sets of TCBs will maintain power to CEDMCS and the reactor will not trip. The methodology uses matrix testing but allows the output aiding test coil for the matrix under test to be de-energized. The bistable relay bucking test coils then will be energized simulating a trip condition which then will de-energize the appropriate K relay and open one set of TCBs.

Manual Trip Test

The Manual Trip Test is accomplished by simply pushing one of the four manual REACTOR TRIP pushbuttons. Pushing only one pushbutton will open the two associated TCBs without causing a reactor trip. This function is done direct from the Control Board to the RTSG and does not pass through the PPS.

The four REACTOR TRIP pushbuttons are arranged in two sets of two, each set on a different control panel. Pressing both pushbuttons at either location will cause an actual reactor trip.

12.4.3 Engineered Safety Features Actuation System (Figure 12.4-19)

The Engineered Safety Features Actuation System (ESFAS) and associated Engineered Safety Features (ESF) systems are designed to ensure that accident consequences are kept within acceptable limits. The ESFAS generates actuation signals for the ESF and ESF support systems.

Like the RPS, the ESFAS receives sensor inputs to feed bistables, 2/4 coincidence logic matrices, and trip paths to actuate devices. However, the RPS and ESFAS differ in their trip actuation devices. While the RPS trip signals actuate the RTSG TCBs, the ESFAS trip signals actuate various ESF system components, such as valves, pumps, and fans. Additionally, some of the RPS trip bistables are shared between the RPS and the ESFAS. These can be readily identified by refering to the Bistable Control Panel (BCP) bistable relay matrix trip status lamp section of the BCP as shown in Figure 12.4-8. Note that the shared bistables have a total of six RPS and ESF matrix trip status lamps and include the LO PZR PRESS, LO SG-1 PRESS and LO SG-2 PRESS bistables. In addition, there are five trip bistables that are used exclusively by the ESFAS. These are indicated on the BCP by having only three ESF matrix trip status lamps and include HI CTN PRESS, HH CTN PRESS, LO RWT LEVEL, HI SG-1 DP, and HI SG-2 DP bistables.

Sensor inputs are sent to trip normally energized bistables. These bistables use the same type of bistable comparator cards and bistable relay cards that the RPS bistables use. However, while RPS bistables use two bistable relay cards, ESF bistables use three bistable relay cards due to the additional outputs required for the two selective 2/4 logic schemes. Like the RPS the ESFAS bistables de-energize to actuate ladder contacts in six different matrices with each matrix having four normally energized matrix output relays that open normally closed trip paths. Each trip path consists of six contacts in series, with each contact being fed from a 2/4 coincidence matrix. An open trip path actuates redundant SSRs (except SIAS and CIAS which use mechanical relays) which then send two independent trains of ESFAS signals to relays in each of the two Auxiliary Relay Cabinets. The Auxiliary Relay Cabinet relays then independently actuate their two trains of ESF system components. CIAS and SIAS use mechanical relays versus solid-state relays due to the larger current-carrying capacity of the mechanical relays which then support the larger number of plant loads operated by the CIAS and SIAS functions.

Unlike the RPS, all ESFAS signals (except Emergency Feedwater Actuation Signal), once actuated, de-energize a "lockout" relay that opens a contact in the trip path to maintain the ESFAS actuation relays de-energized even if the actuating bistables reset and the matrix relays later re-energize. This ensures that the ESF system remains in its safeguards lineup until deliberate manual action is taken to reset its lockout relay and restore the associated ESF lineup.

All ESFAS signals except RAS may be manually initiated from the Control Room from two physically separated portions of the Main Control Board via pushbuttons (Emergency Feedwater Actuation System has switches). These pushbuttons are normally closed contacts in the trip paths. Depressing either set of pushbuttons will initiate both trains of ESFAS. The two ESFAS pushbuttons for a given function need not be pushed simultaneously due to the action of the lockout relays. All ESFAS signals, including RAS, can be manually actuated at the Auxiliary Relay Cabinets. However, the two ESFAS MANUAL TRIP pushbuttons for a given function must be pushed simultaneously.

Note: Even though SIAS and CIAS share the same trip paths, they have separate

manual actuations, and manual SIAS does NOT cause CIAS.

12.4.3.1 Design Bases

Since both the RPS and the ESFAS are part of the PPS, they have the same design bases.

12.4.3.2 ESFAS Signals (Figure 12.4-18)

Safety Injection Actuation (SIAS)

The SIAS is generated by high containment pressure or by low pressurizer pressure. Low pressurizer pressure is interpreted as either an RCS Loss of Coolant Accident (LOCA) or a Main Steam Line Break (MSLB) induced RCS cooldown, which could be adding positive reactivity in an uncontrolled manner. High containment pressure is interpreted as either an RCS LOCA or a MSLB. In either case, SIAS will isolate RCS letdown, shift the charging pumps into emergency boration mode, start two high head safety injection pumps and two low head safety injection pumps to inject cool borated RWT water into the core to keep the core cooled, covered, and shutdown. In doing so, it will minimize the damage to the fuel cladding due to excessive decay heat relative to heat removal capabilities. It will also reduce reactor power and decay heat generation rates to very low levels, thereby limiting the peak pressure and temperature in the containment. This is done to maintain the integrity of the containment boundary and preclude releases of radioactivity to the environment.

Containent Isolation Actuation Signal (CIAS)

The CIAS is generated by high containment pressure or by low pressurizer pressure. The CIAS interprets the low pressurizer pressure event as either an RCS LOCAor a MSLB. High containment pressure is also interpreted as either an RCS LOCA or a MSLB. It automatically closes valves in non-essential piping lines penetrating the containment boundary to maintain containment integrity and preclude releases of radioactivity to the environment. It also precludes releases of radioactivity to the reactor auxiliary building and the control room, which would restrict operator accessibility and hamper post-accident recovery efforts.

Containment Spray Actuation System (CSAS)

The CSAS is generated by high-high containment pressure coincident with an automatic SIAS (a manual SIAS will not permit an automatic actuation of CSAS; however, an automatic SIAS should have actuated before the CSAS). This ensures that failure of both CSAS high-high containment pressure transmitters would not, by itself, cause a CSAS. Protection against this particular instrument failure scenario is necessary because the caustic spray solution can cause significant damage to components and electrical cabling inside containment and require significant amounts of time and money for cleanup and restoration purposes. Recall that the containment is the third and final fission product barrier protecting the health and safety of the general public. As long as its internal design pressure is not exceeded, the containment leakage rates under accident conditions will maintain offsite doses within acceptable ranges as assumed in the safety analyses. However, any large RCS LOCA or MSLB inside containment with its resulting steam release to the containment atmosphere could possibly over pressurize the containment and compromise its integrity. To protect against these DBAs, containment high-high pressure is interpreted as a large RCS LOCA or MSLB, and containment spray is initiated to condense atmospheric steam in the containment atmosphere, thereby reducing peak pressure and temperature for containment integrity purposes.

Main Steam Isolation Signal (MSIS)

The MSIS is generated by either high containment pressure or low steam pressure on either steam generator. Both of these conditions are interpreted as MSLBs; therefore, MSIS will close the main steamline isolation valves and the main feedwater isolation valves to isolate and terminate the steam release to the maximum extent possible. In addition, emergency feedwater isolation valves and flow control valves are closed in an attempt to stop feeding the break and to minimize the high energy mass release/blowdown to the containment.

Emergency Feedwater Actuation Signal (EFAS-1 and EFAS-2)

The EFAS is generated by a low steam generator level (in the narrow range) coincident with that steam generator's pressure being above the MSIS setpoint (variable) OR that steam generator being the highest pressure generator if an excessive steam generator pressure differential pressure exists. The level and pressure logic is designed to feed an intact steam generator and to prevent feeding a faulted steam generator. For preservation of heat sink, if an MSIS (closes emergency feedwater isolation valves) and a EFAS (opens emergency feedwater isolation valves) are present at the same time, the EFAS will override an MSIS in the higher pressure steam generator. The higher pressure steam generator is interpreted to be intact as long as its steam pressure exceeds the other steam generator by a set amount.

There are two separate actuation signals, one for steam generator number one and one for steam generator number two. Each EFAS has two trains. The actuation signals are interpreted as MSLBs and will start the emergency feedwater pumps, close the steam generator blowdown isolation valves, open the emergency feedwater isolation valves, and send a permissive open to the flow control valves, which will then cycle on steam generator level.

Since the EFAS systems must be capable of starting and stopping feed automatically based on steam generator level, the emergency feedwater flow control valves and isolation valves do not lock out (and do not need to be reset manually). To accommodate this design, the EFAS manual actuation pushbuttons are maintained contact switches rather than momentary contact pushbuttons like the other ESFAS signals.

Recirculation Actuation Signal (RAS)

The RAS is generated by RWT low water level and is interpreted to mean that a large LOCA is in progress since that is the most likely cause for a large drop in the RWT level. It is further assumed that this water has been transferred via safety injection into the ESF sump. In either case, any pumps taking suction from the RWT will soon lose net positive suction head and suffer cavitation damage. Therefore, this signal will trip the low pressure safety injection pumps, to prevent vortexing in the ESF sump due to their high capacity flow rate, and shift the suctions of the containment spray pumps and the high pressure safety injection pumps to the ESF sump to allow a long-term water source for the operating ESF system pumps. The RWT suction valves must be shut manually to isolate the emptying tank from the pump suctions.

12.4.3.3 Operating and Trip Channel Bypasses

There are only two bypasses associated with the ESFAS; an operating bypass on SIAS (low pressurizer pressure) and a trip channel bypass.

The low pressurizer pressure SIAS is operationally bypassable to allow controlled plant cooldowns (which would otherwise be interpreted

as accident-induced depressurizations) without invoking protective action that is not needed.

The trip bypass is identical to the reactor trip bypass for the corresponding low pressurizer pressure trip functions. In fact, the RPS and ESFAS bypasses on this function are integral. When the trip on low pressurizer pressure is operationally bypassed at the RPS the SIAS is also bypassed.

12.4.3.4 ESFAS Testing

Like RPS testing, ESFAS testing is performed in an overlapping manner such that the overall protection circuit is functionally tested. The final actuation devices in this case, however, are not the TCBs but the plant components actuated by the ESFAS signals.

Bistable Testing

ESFAS bistable testing is identical to RPS bistable testing.

Matrix Testing

ESFAS matrix testing is identical to RPS matrix testing except that the ESFAS positions of the test switches are used instead of the RPS positions.

Trip Path Testing

ESFAS trip path testing is identical to RPS trip path testing except that the ESFAS positions of the test switches are used instead of the RPS positions. With the exception of ESFAS, no components are actuated by trip path testing since only 1/4 trip paths are tripped at a time which does not satisfy the selective 2/4 logic scheme employed in the ESFAS.

ESFAS Actuation Relay Test

This test verifies proper operation of a single actuation relay at a time by de-energizing its coil. The actuation relay is de-energized and its components are actuated. Once the test circuits are removed the individual actuated components may be reset.

ESFAS Lockout Reset Test

This test verifies proper operation of the lockout relays and pushbuttons. The test enables both ESF actuated equipment and control room annunciation. Each Lockout relay and pushbutton is tested separately.

ESFAS Manual Actuation Test

This test is performed simply by depressing one manual ESFAS actuation switch and observing that the ESFAS function's local on indication goes out with appropriate control room annunciation due to the trip path being opened. No components should actuate since the 2/4 logic is not met.

12.4.4 Summary

The Plant Protection System is comprised of the Reactor Protection System and the Engineered Safety Features Actuation System.

The Reactor Protection System monitors various plant parameters and trips the reactor when a parameter limit is being approached. A reactor trip is intended to maintain the integrity of the fuel cladding and Reactor Coolant System boundaries during any Anticipated Operational Occurrence and limit offsite radiation doses to within 10CFR100 limits during any design basis accidents.

The Reactor Protection System aids the Engineered Safety Features Actuation System in the event of an accident by shutting down the reactor. This reduces the reactor heat generation and steam generation rates to ensure that the heat loads are maintained within the capabilities of the Engineered Safety Features Actuation Systems design requirements.

The Engineered Safety Features Actuation System and associated Engineered Safety Features systems are designed to keep the consequences of an accident within acceptable limits.

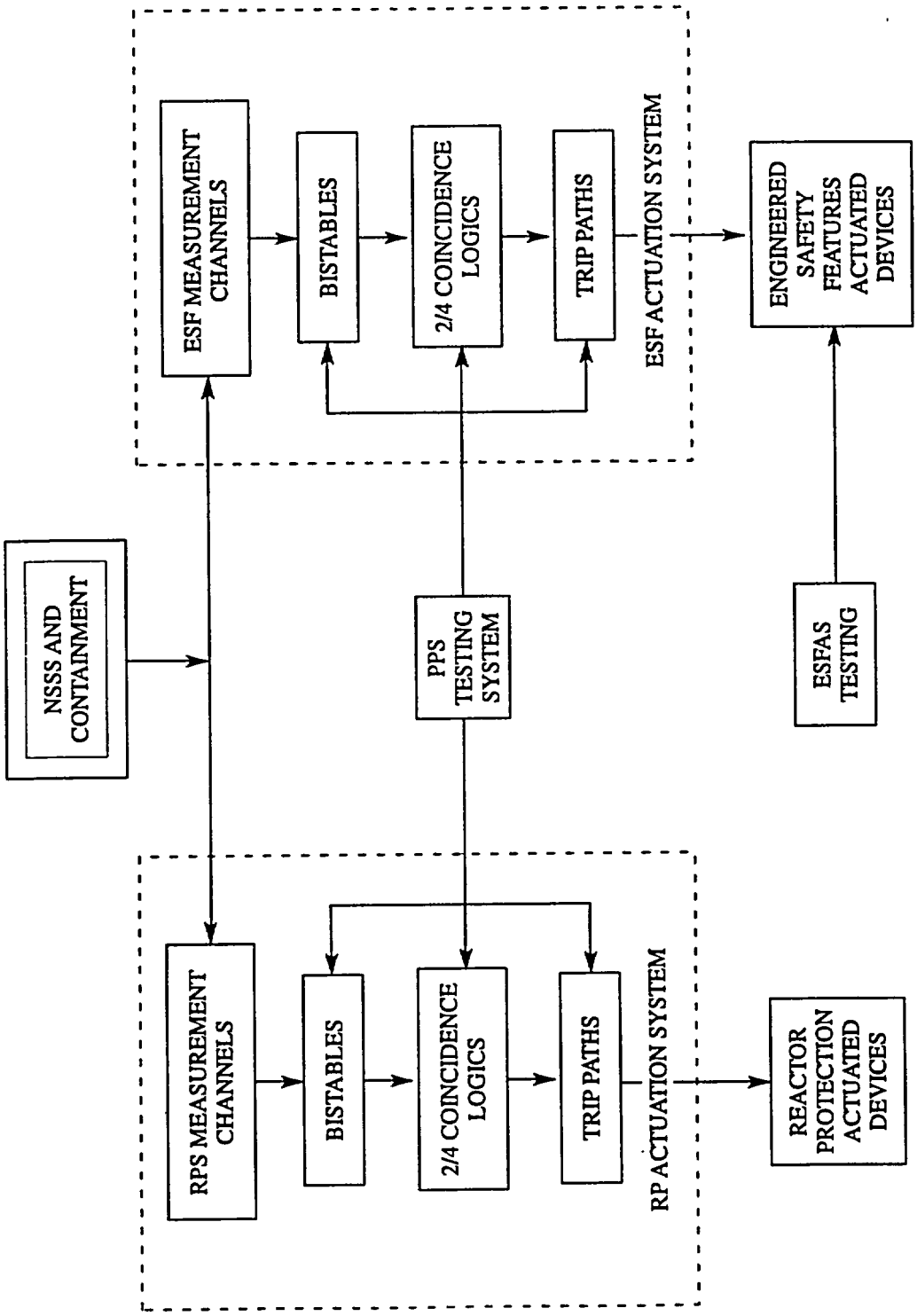


Figure 12.4-1 Plant Protection System Basic Block Diagram

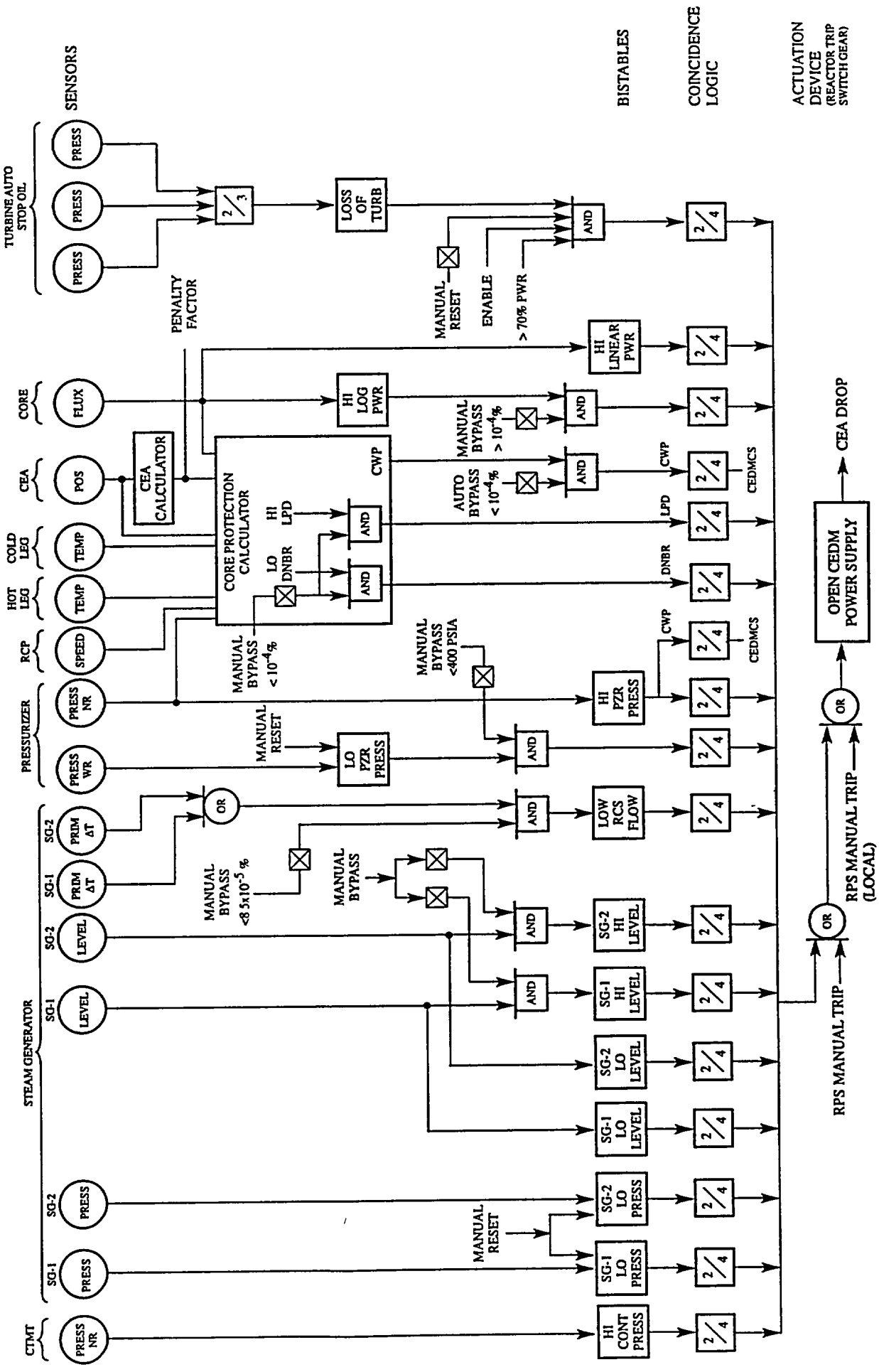


Figure 12.4-2 Reactor Trip Logic Diagram

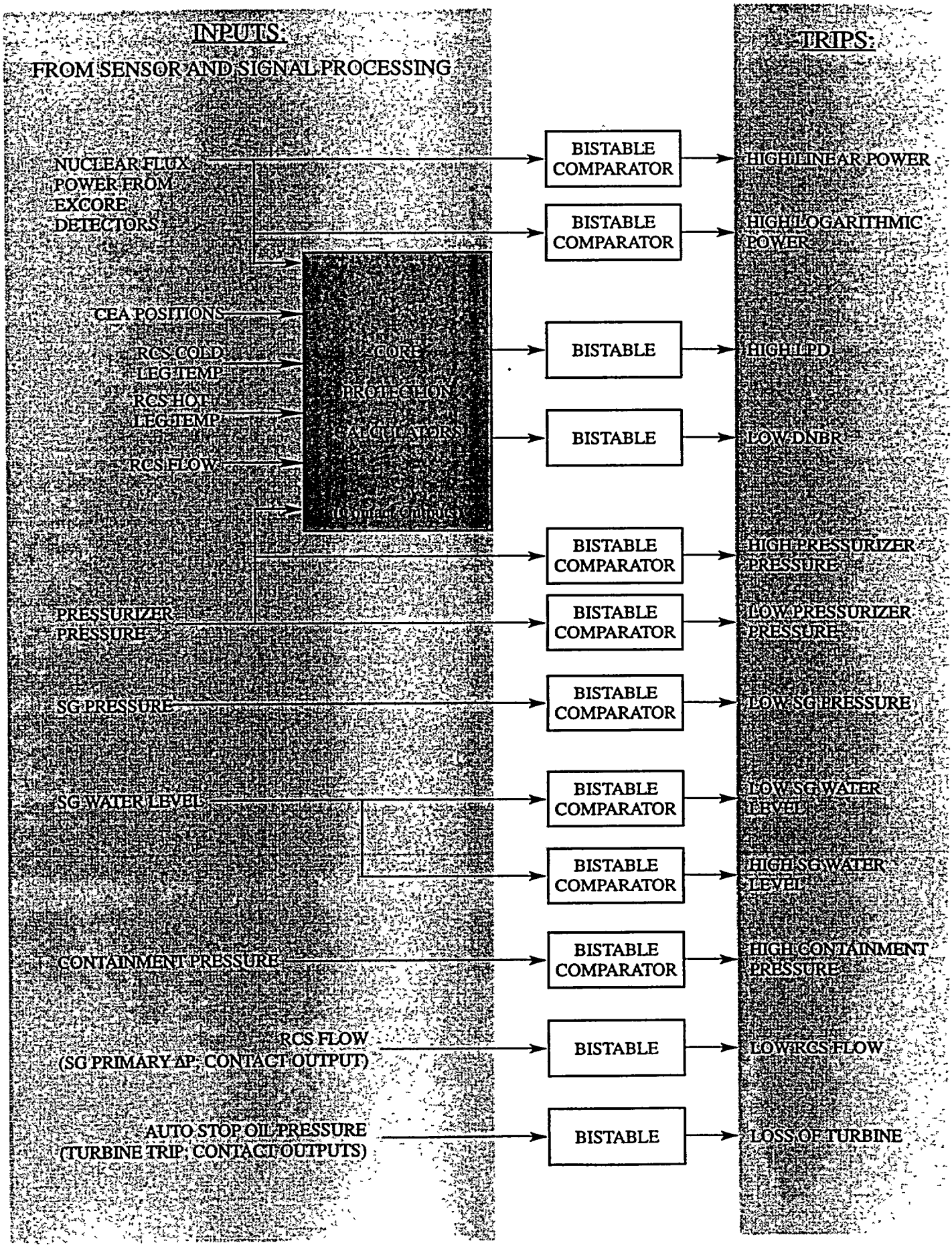


Figure 12.4-3 Bistable Comparator and CPC Process

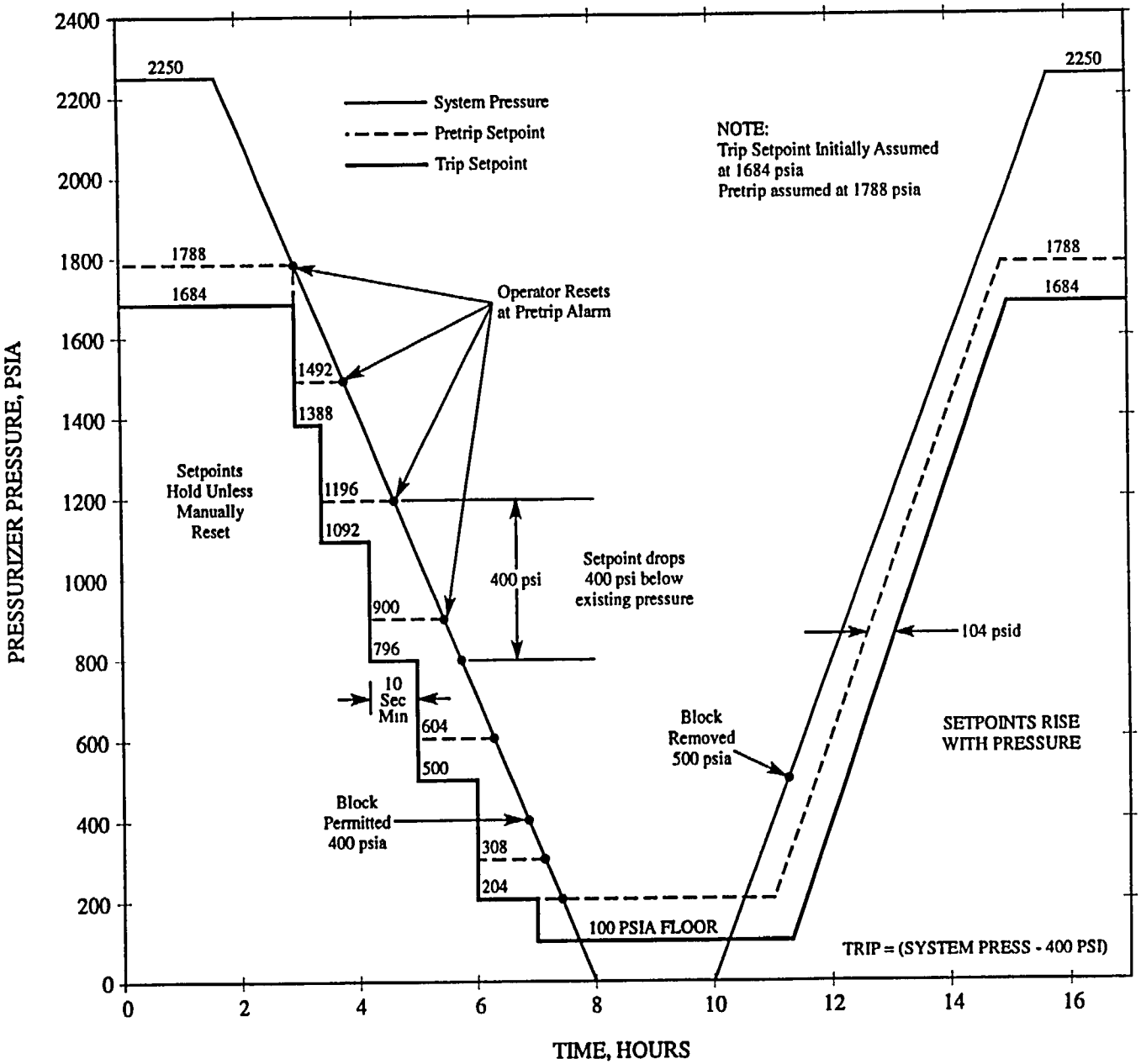


Figure 12.4-4 Low Pressurizer Pressure Variable Setpoint Operation

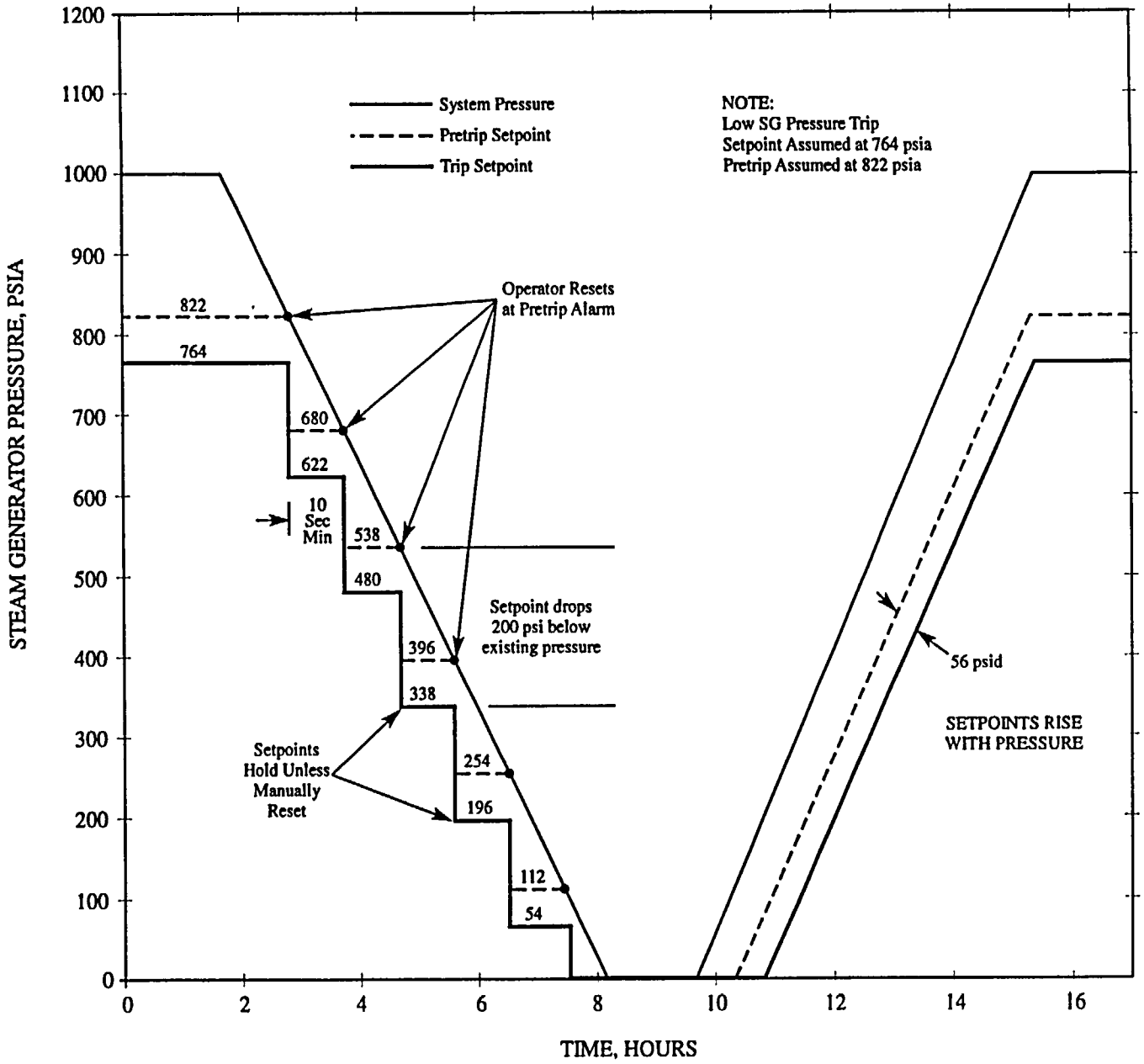
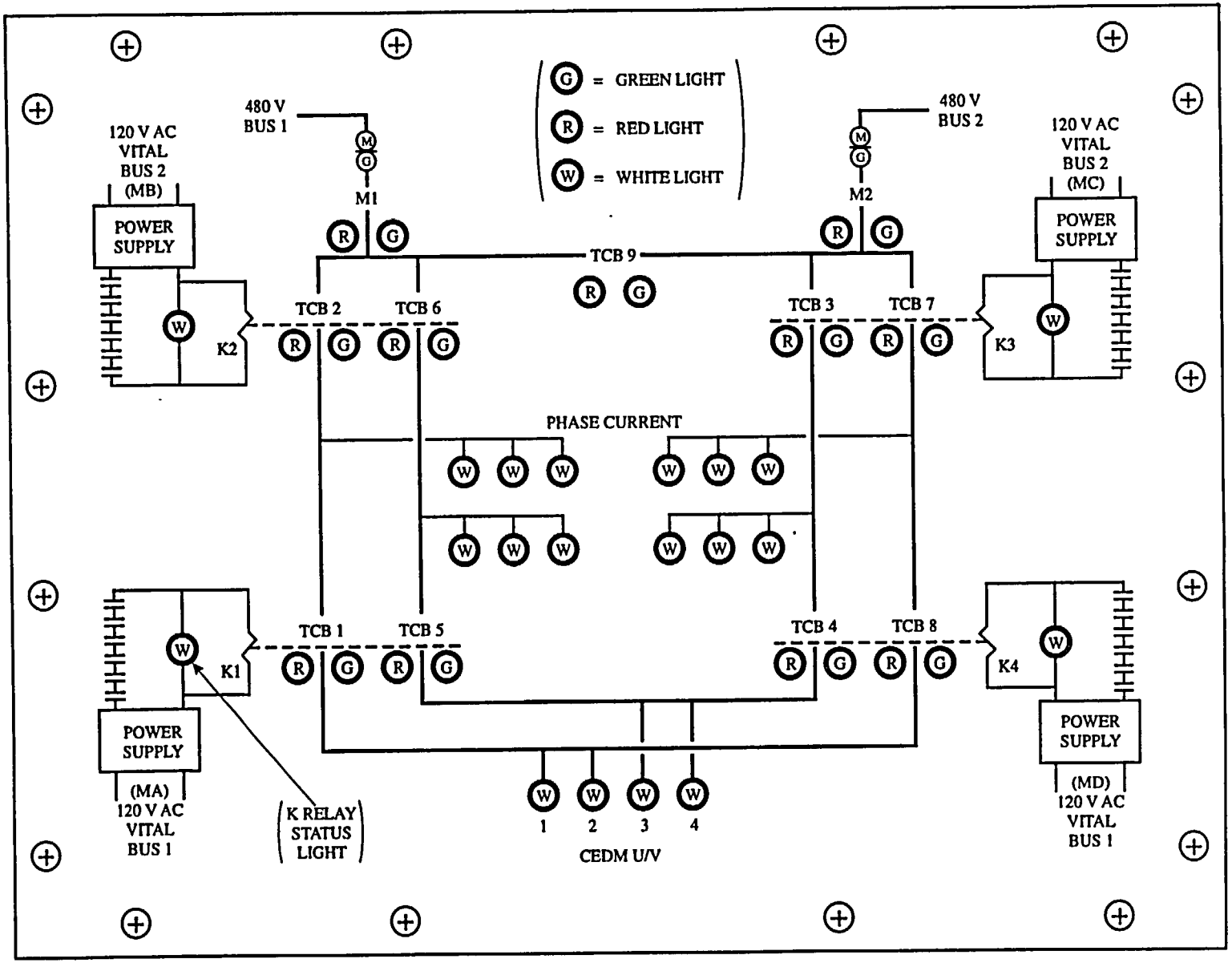


Figure 12.4-5 Low Steam Generator Pressure Variable Setpoint Operation



NOTES:

1. ALL WHITE AND RED LIGHTS NORMALLY ON FOR NON-TRIP CONDITION AT POWER CONDITION.
2. ITEMS IN PARENTHESIS SHOWN FOR INFORMATION BUT ARE NOT PHYSICALLY ON STATUS PANEL.

Figure 12.4-6 Reactor Trip Status Panel

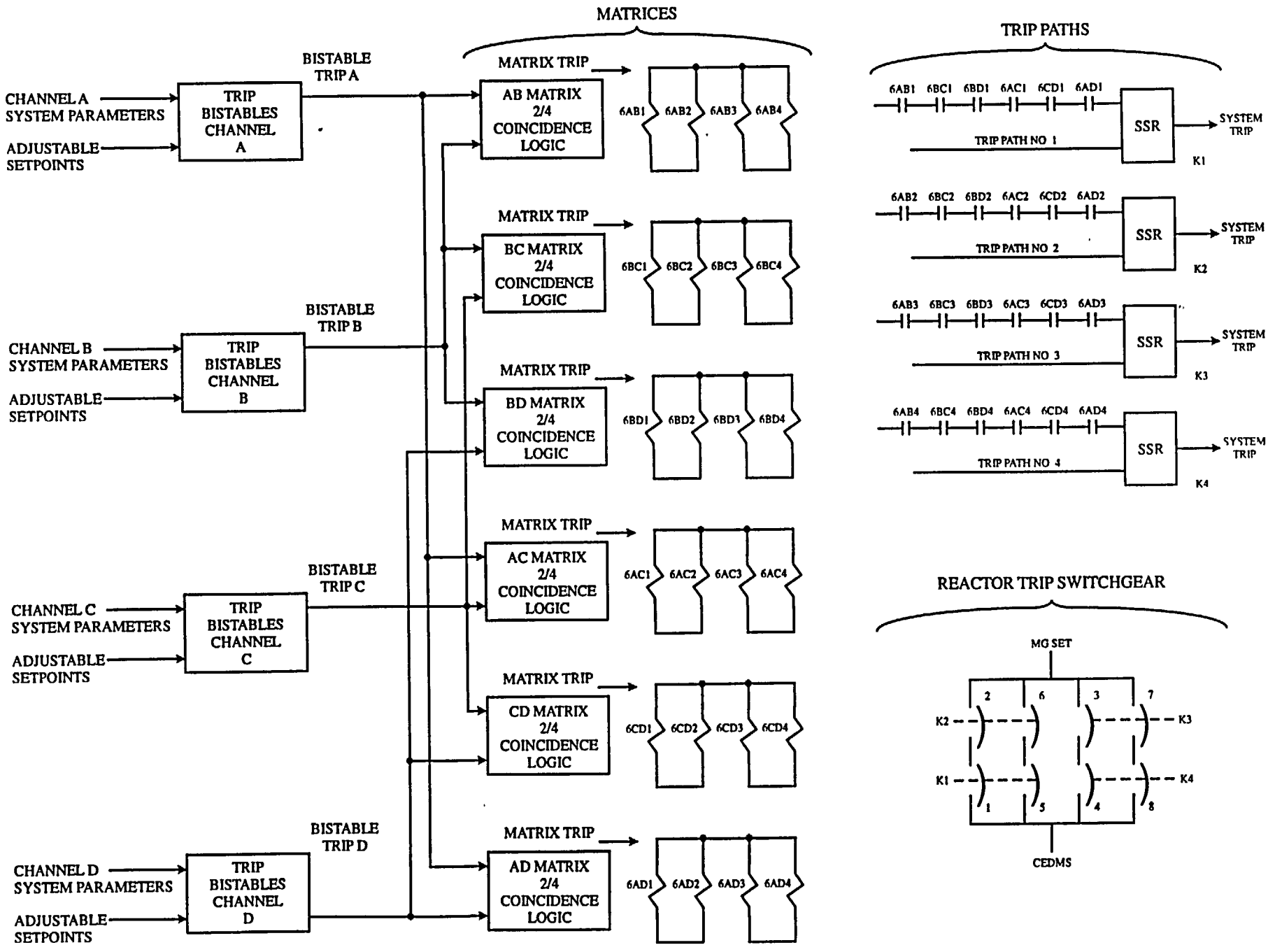


Figure 12.4-7 RPS Trip Signal Flowpath

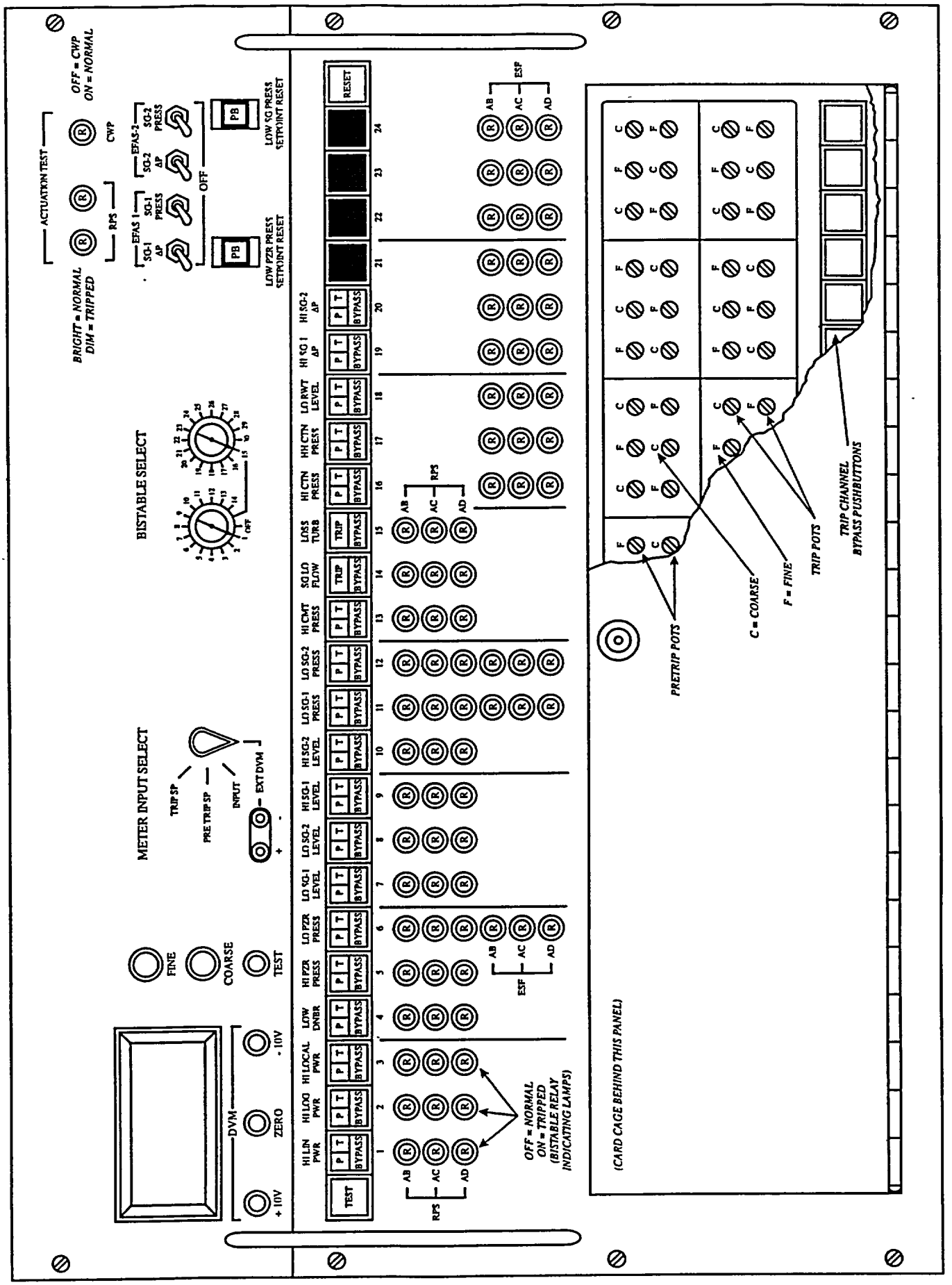


Figure 12.4-8 Bistable Control Panel Channel A

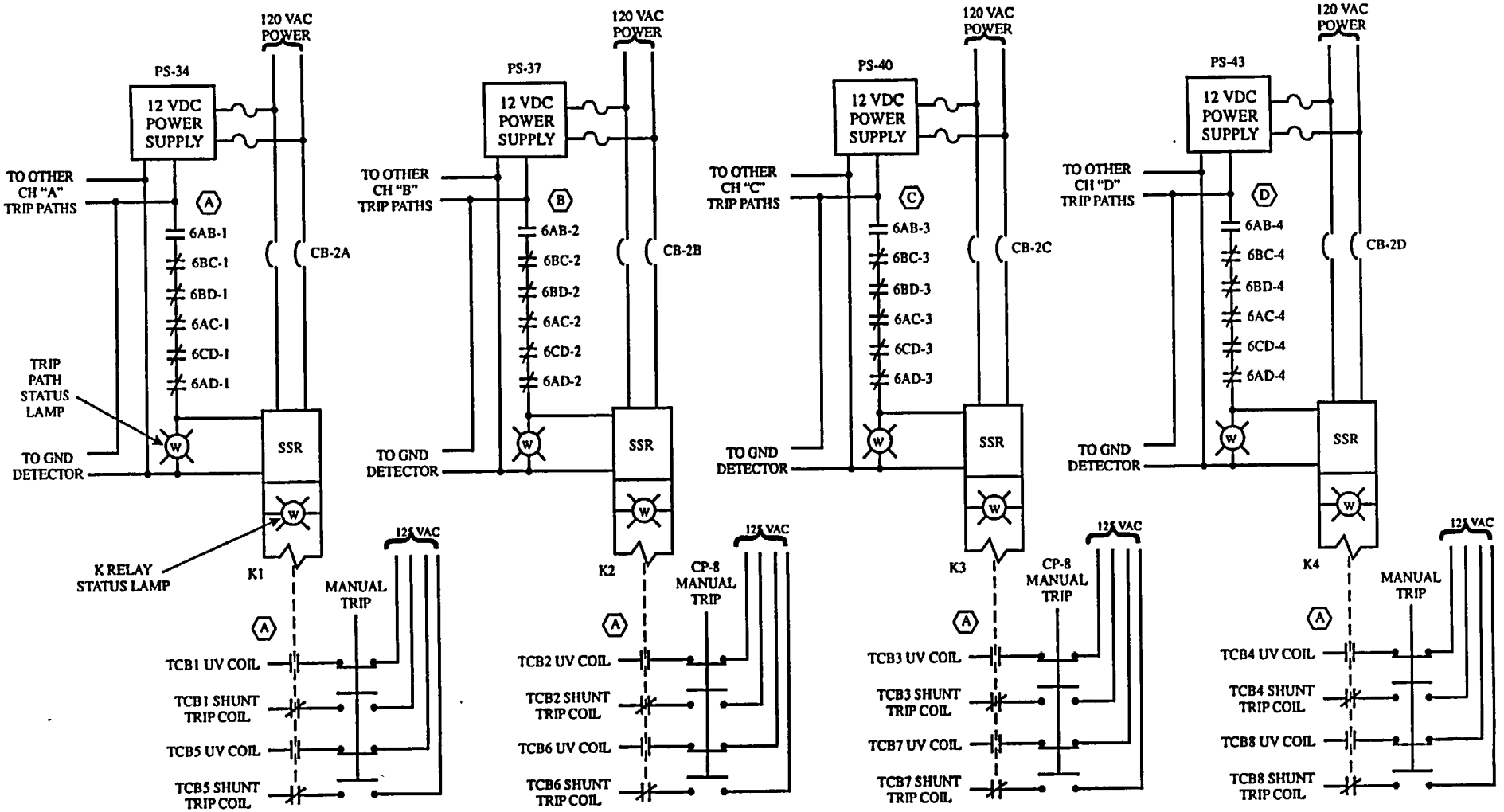


Figure 12.4-9 RPS Trip Path Status With Trip in the AB Matrix

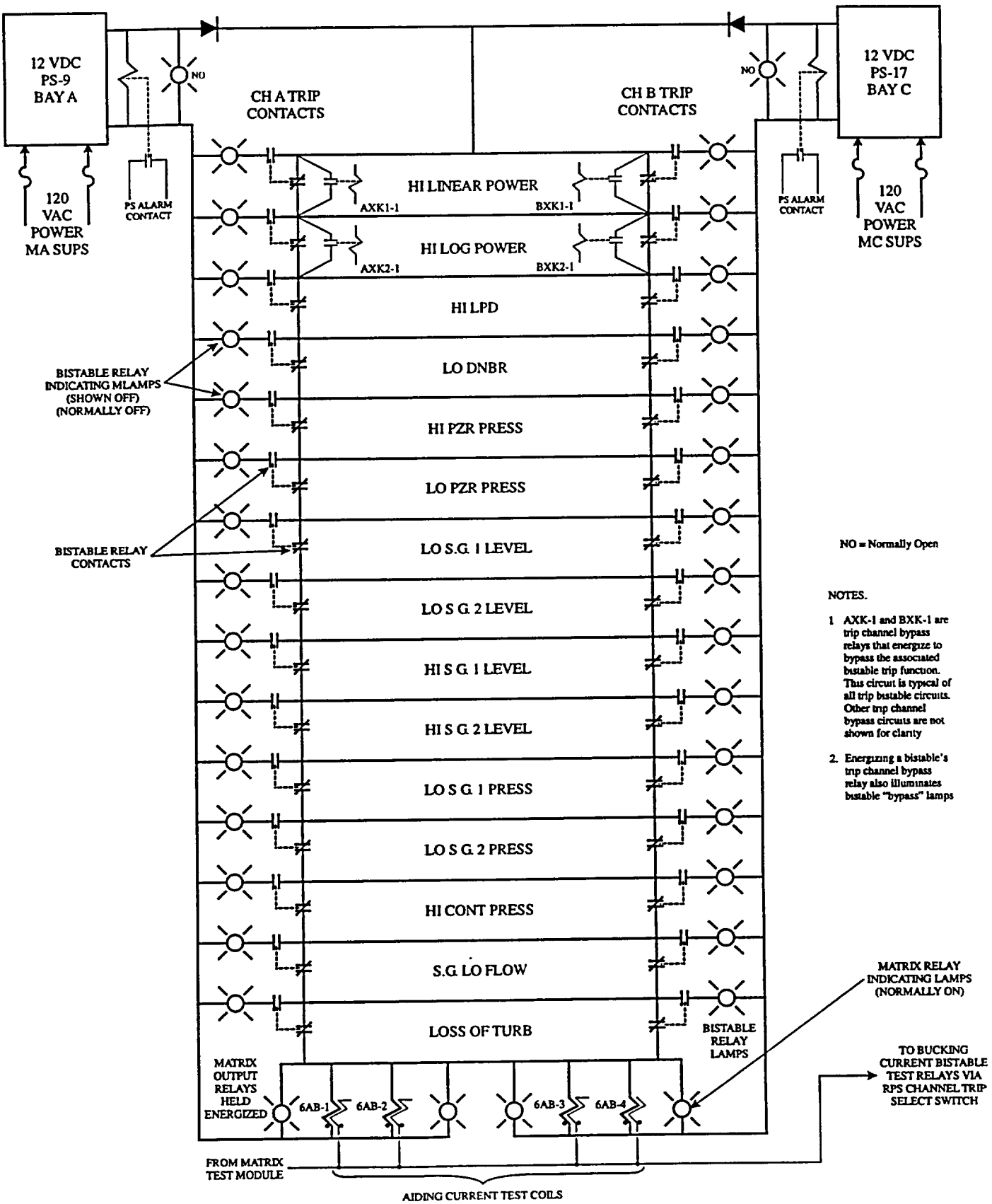


Figure 12.4-10 RPS AB Logic Matrix - Normal (untripped)

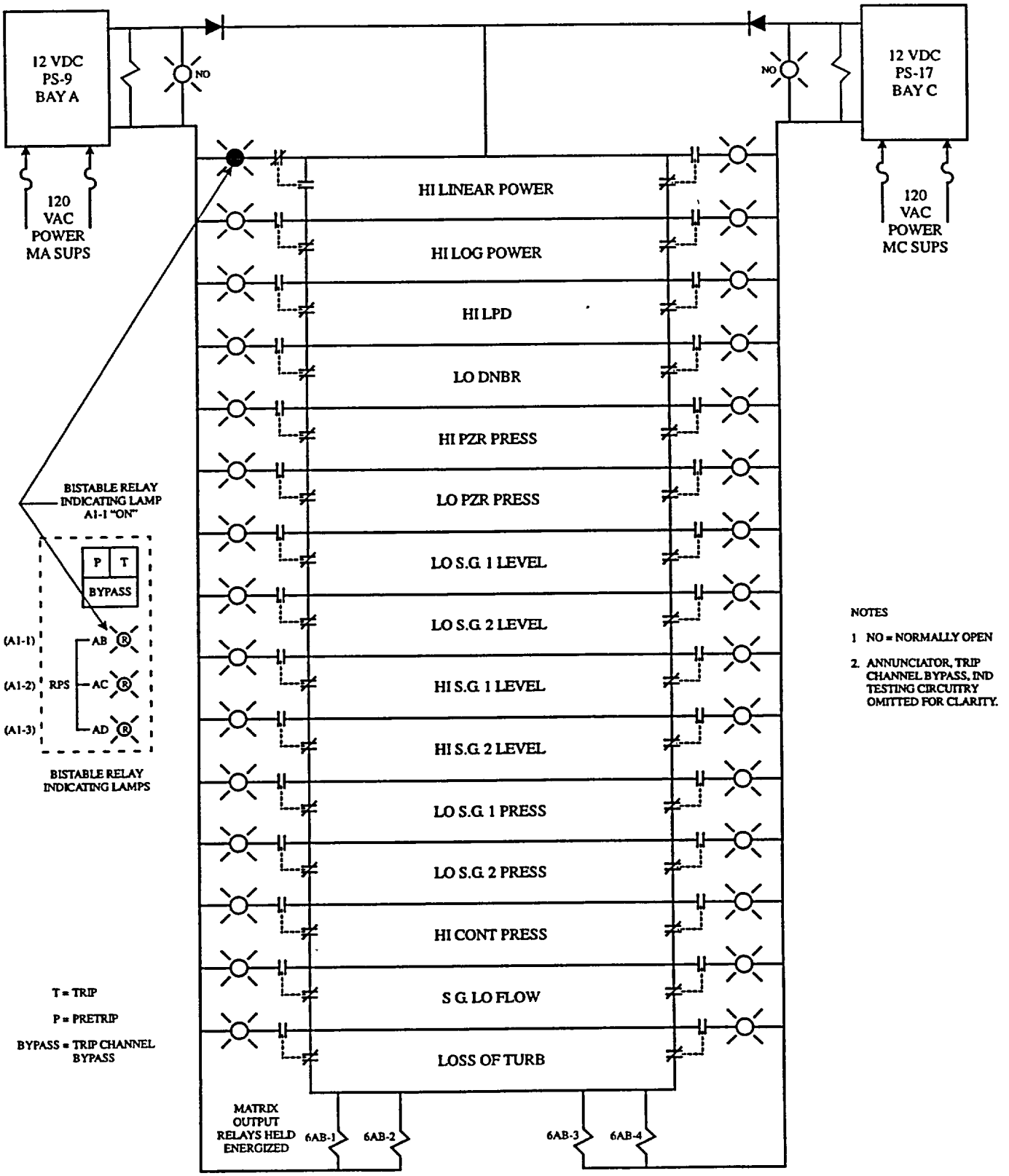


Figure 12.4-11 RPS Logic Matrix With High Linear Power Channel A Tripped

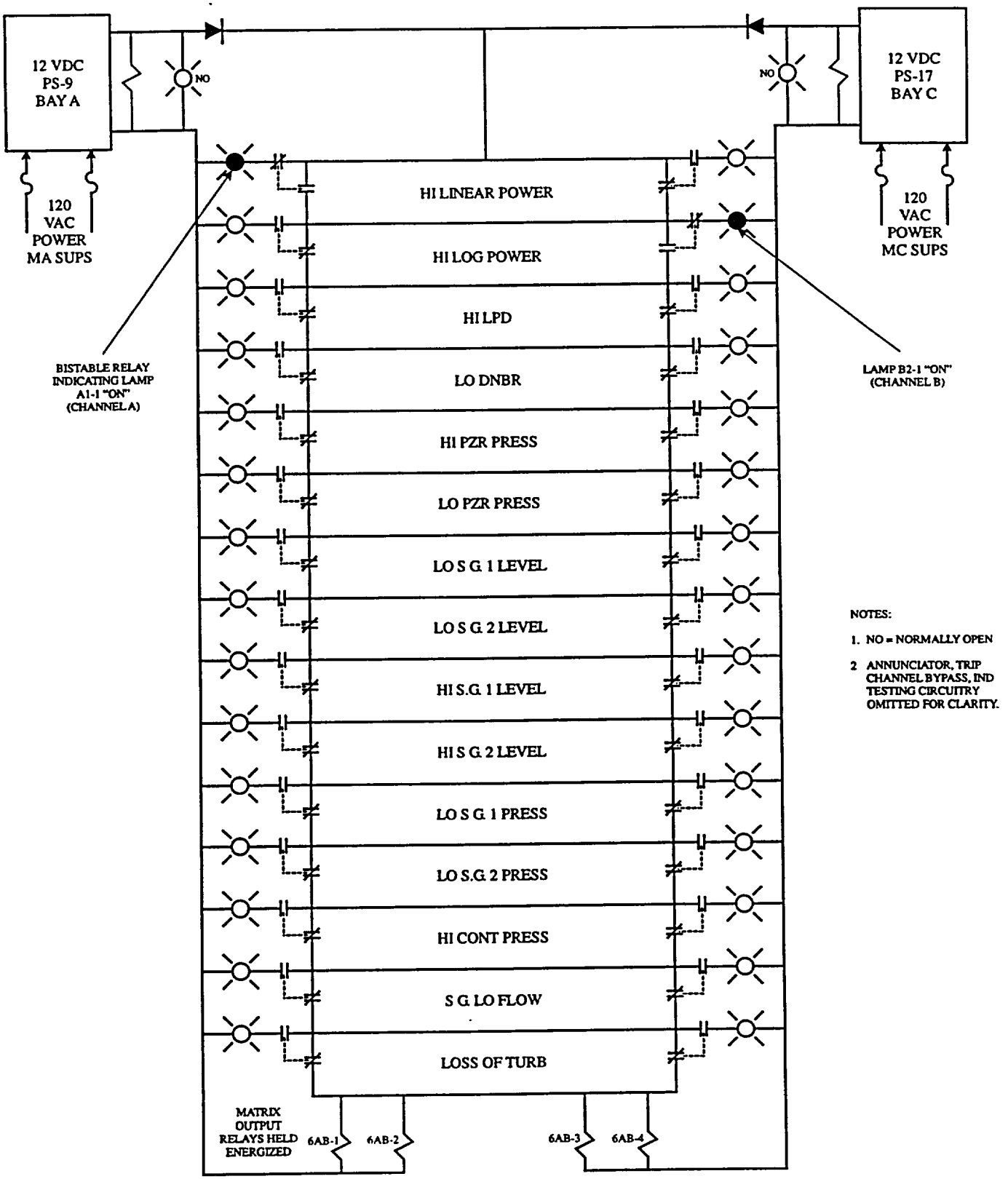


Figure 12.4-12 RPS Logic Matrix With Linear Power Channel A and High Log Power Channel B Tripped

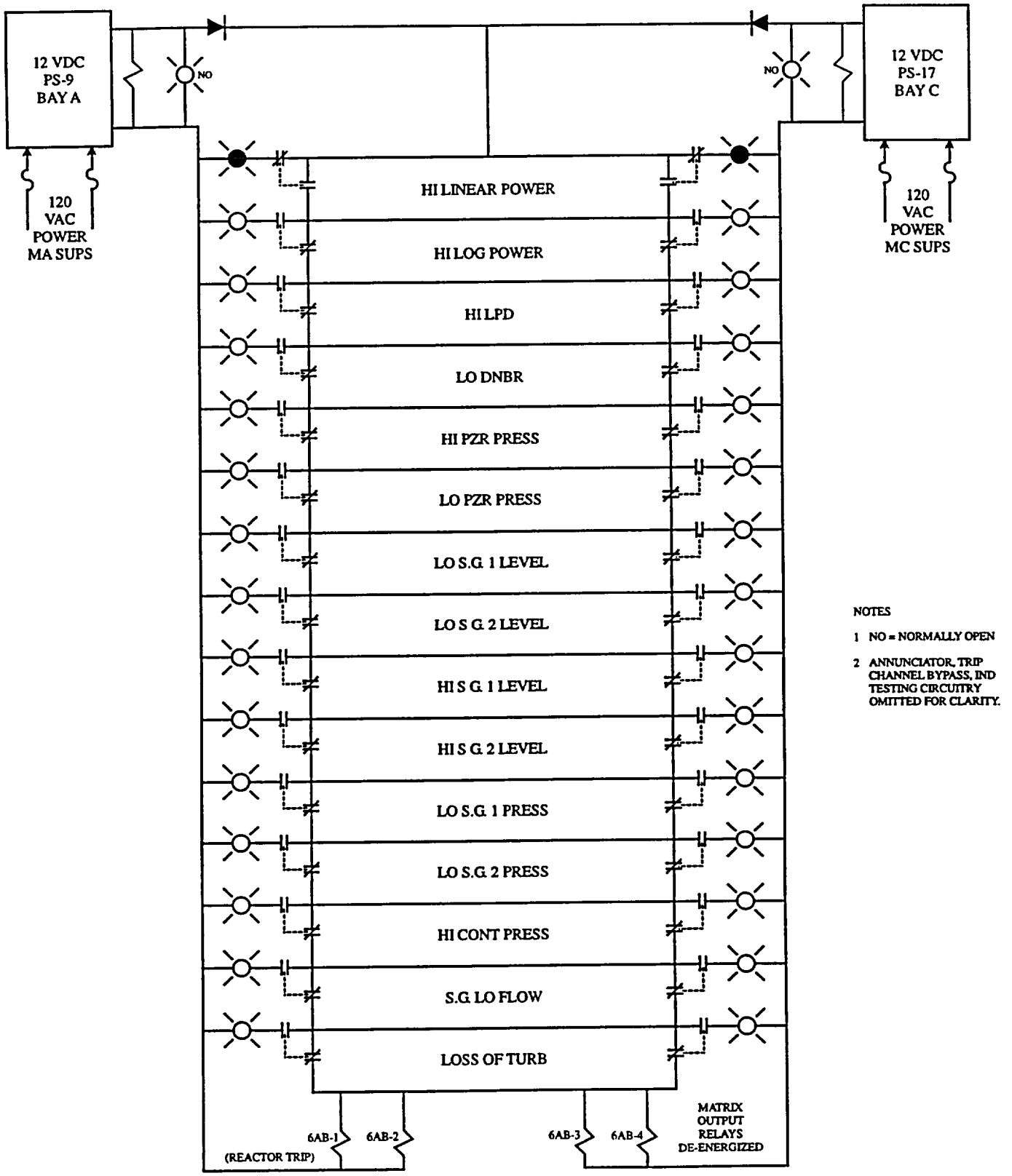


Figure 12.4-13 RPS AB Logic Matrix With High Linear Power Channel A and Channel B Tripped

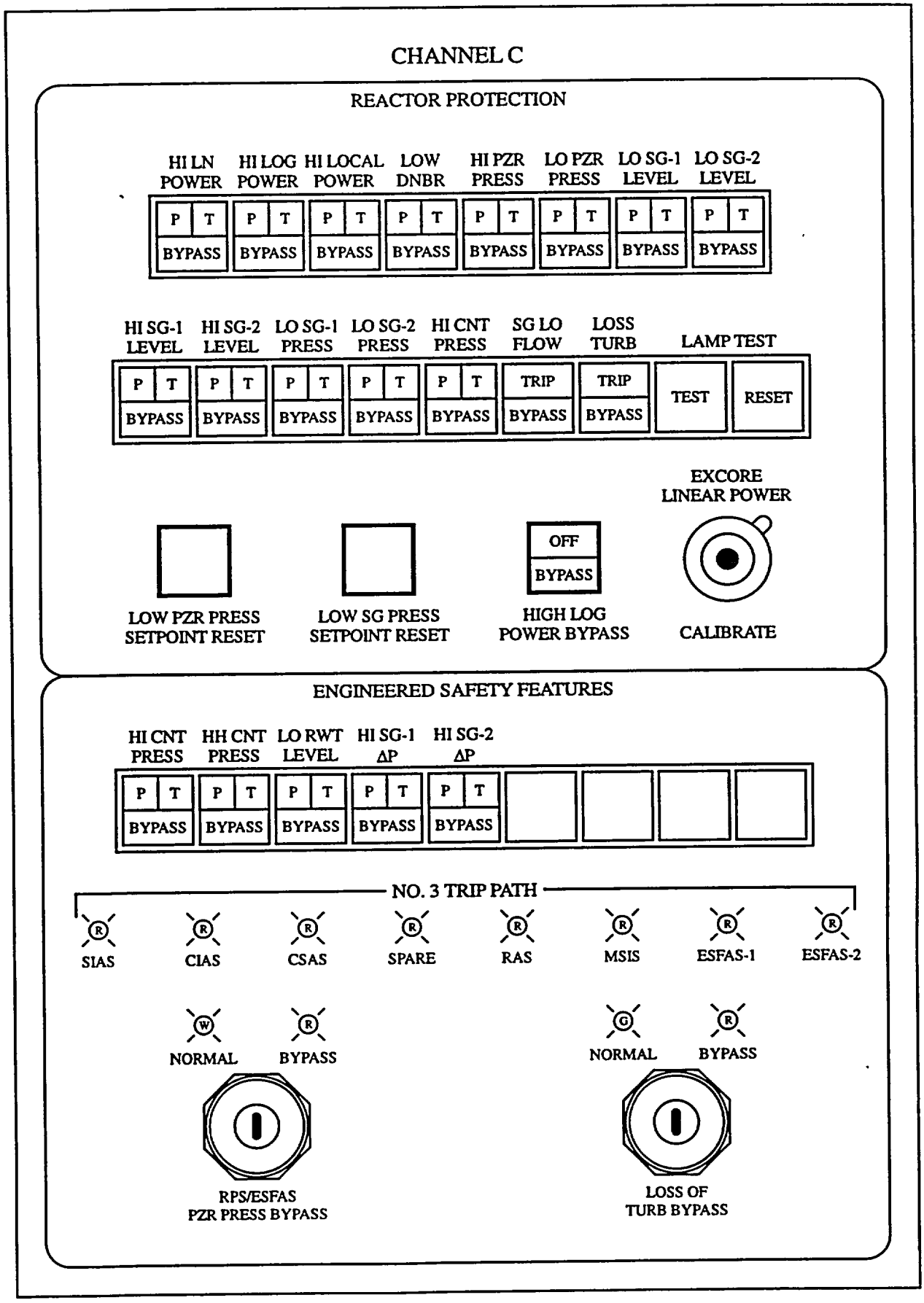


Figure 12.4-14 PPS Remote Operator's Module

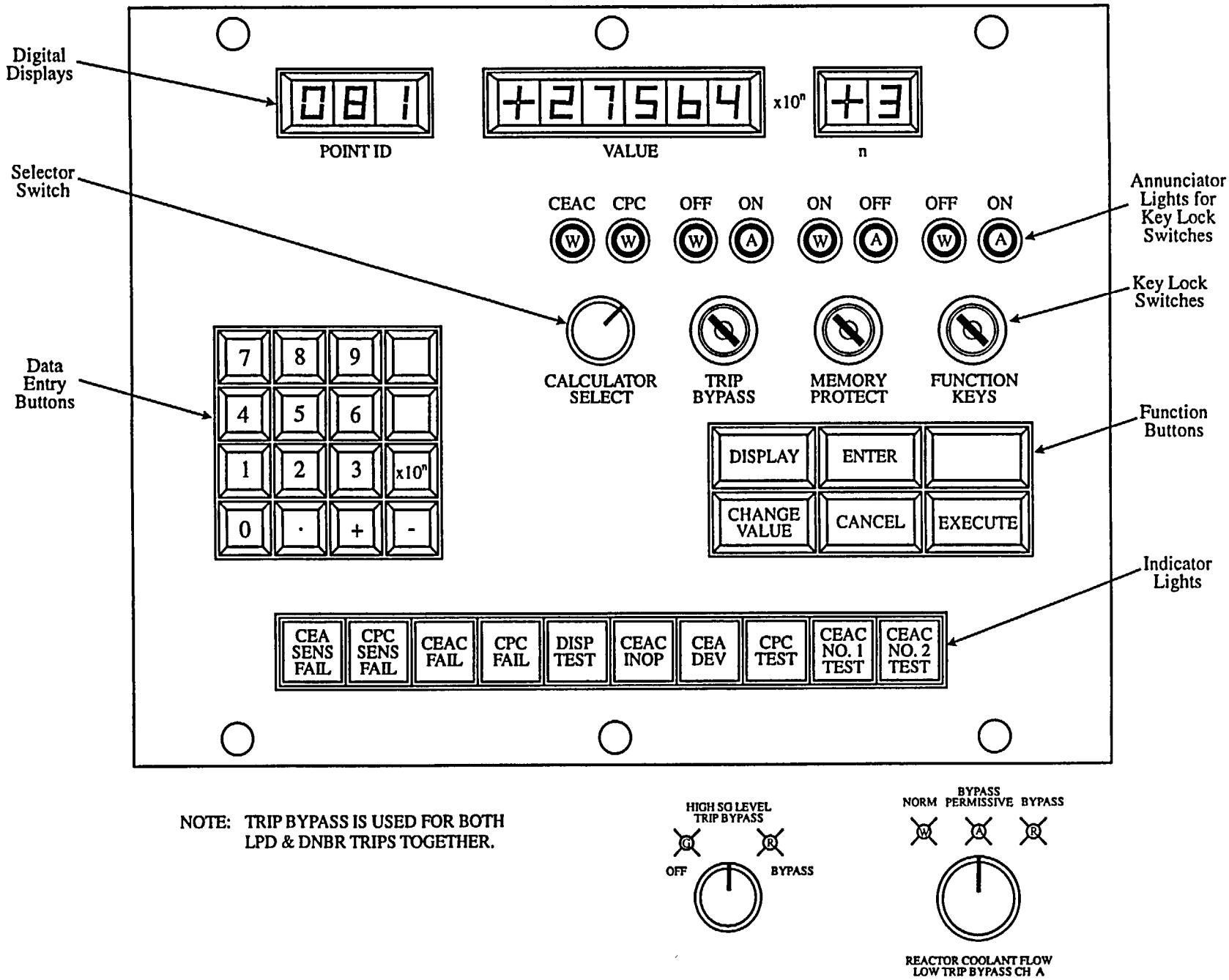
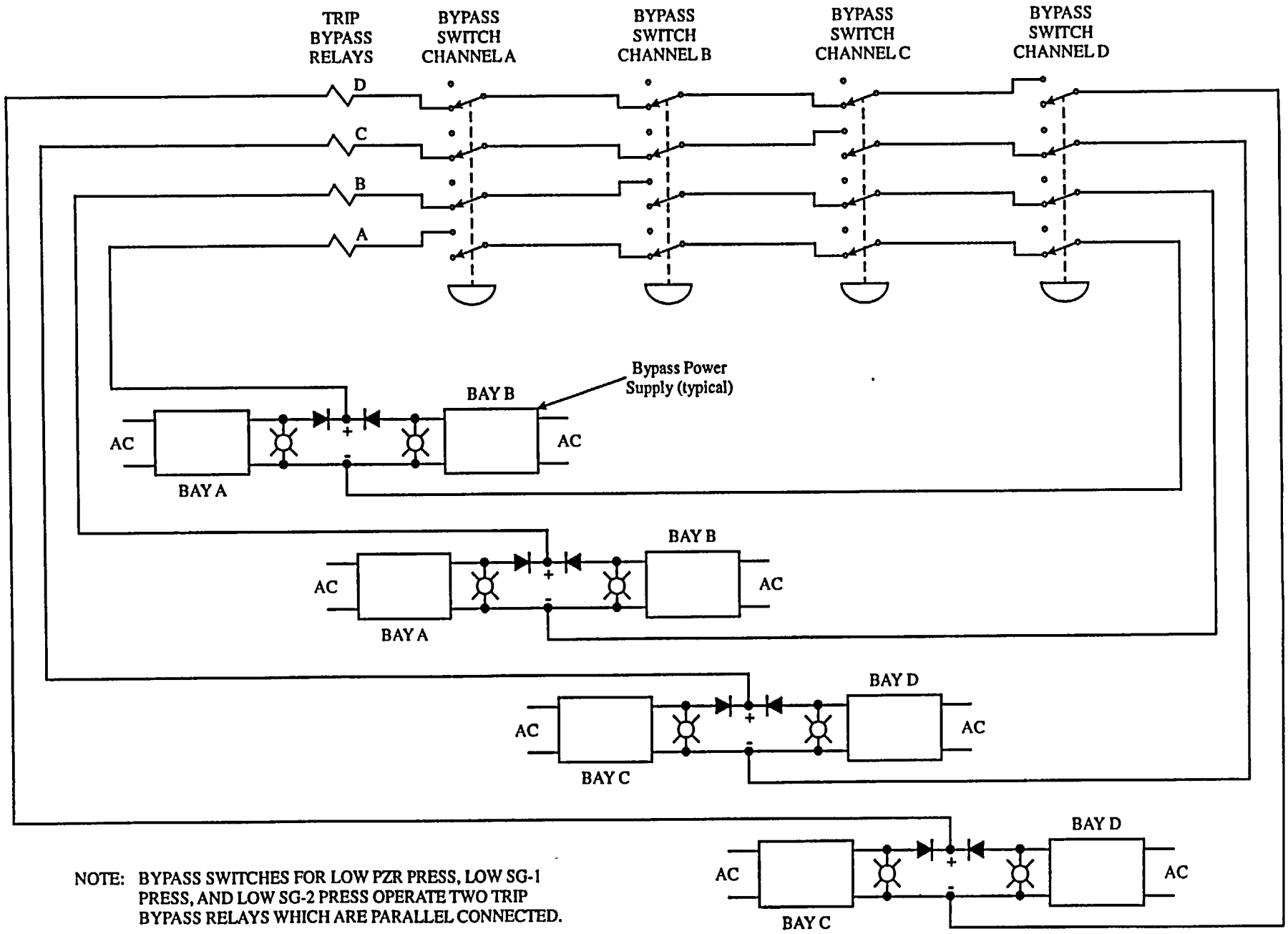


Figure 12.4-15 CPC Remote Operator's Module



NOTE: BYPASS SWITCHES FOR LOW PZR PRESS, LOW SG-1 PRESS, AND LOW SG-2 PRESS OPERATE TWO TRIP BYPASS RELAYS WHICH ARE PARALLEL CONNECTED.

Figure 12.4-16 Trip Channel Bypass Electrical Interlock

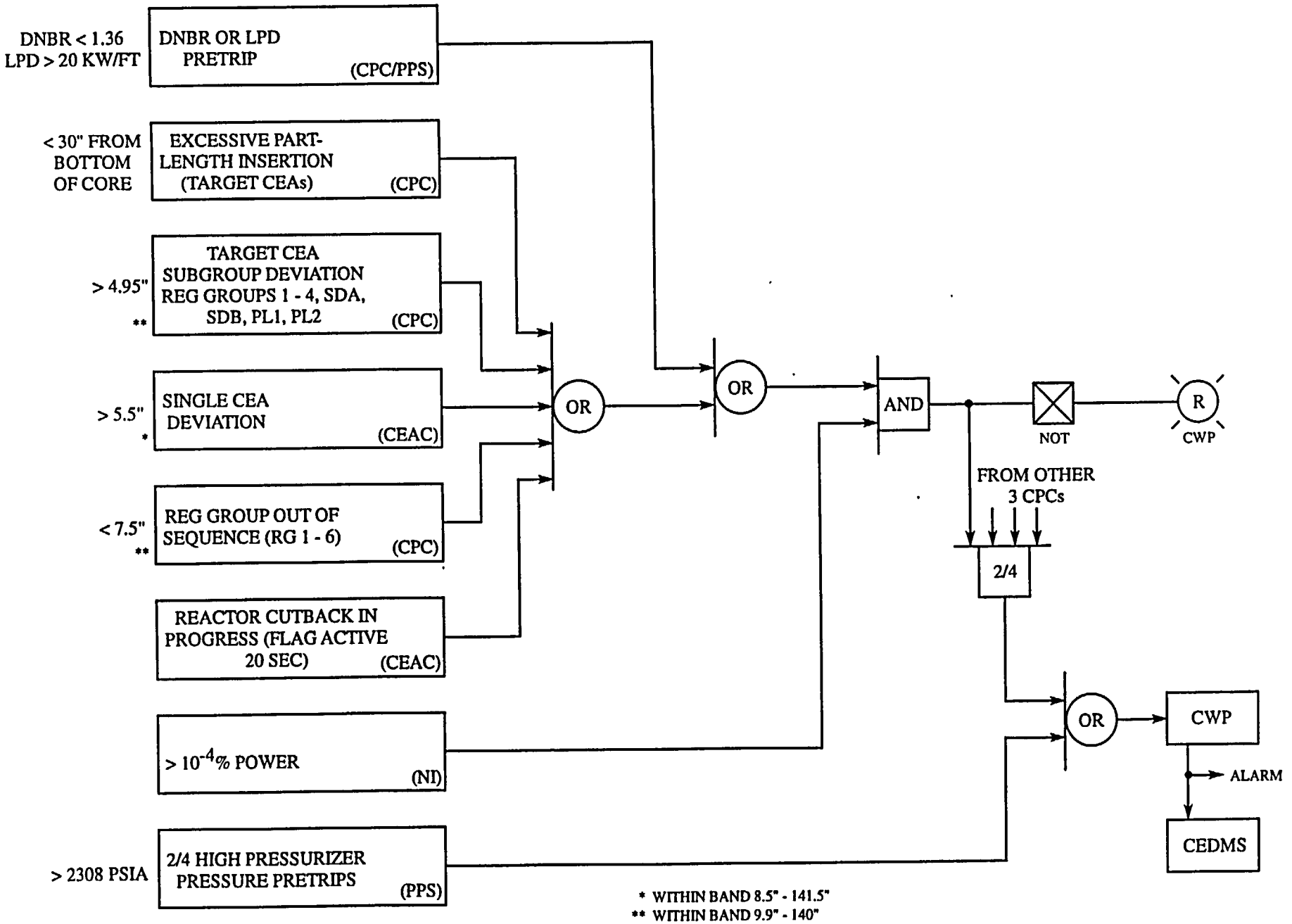


Figure 12.4-17 CEA Withdrawal Prohibit Logic Diagram

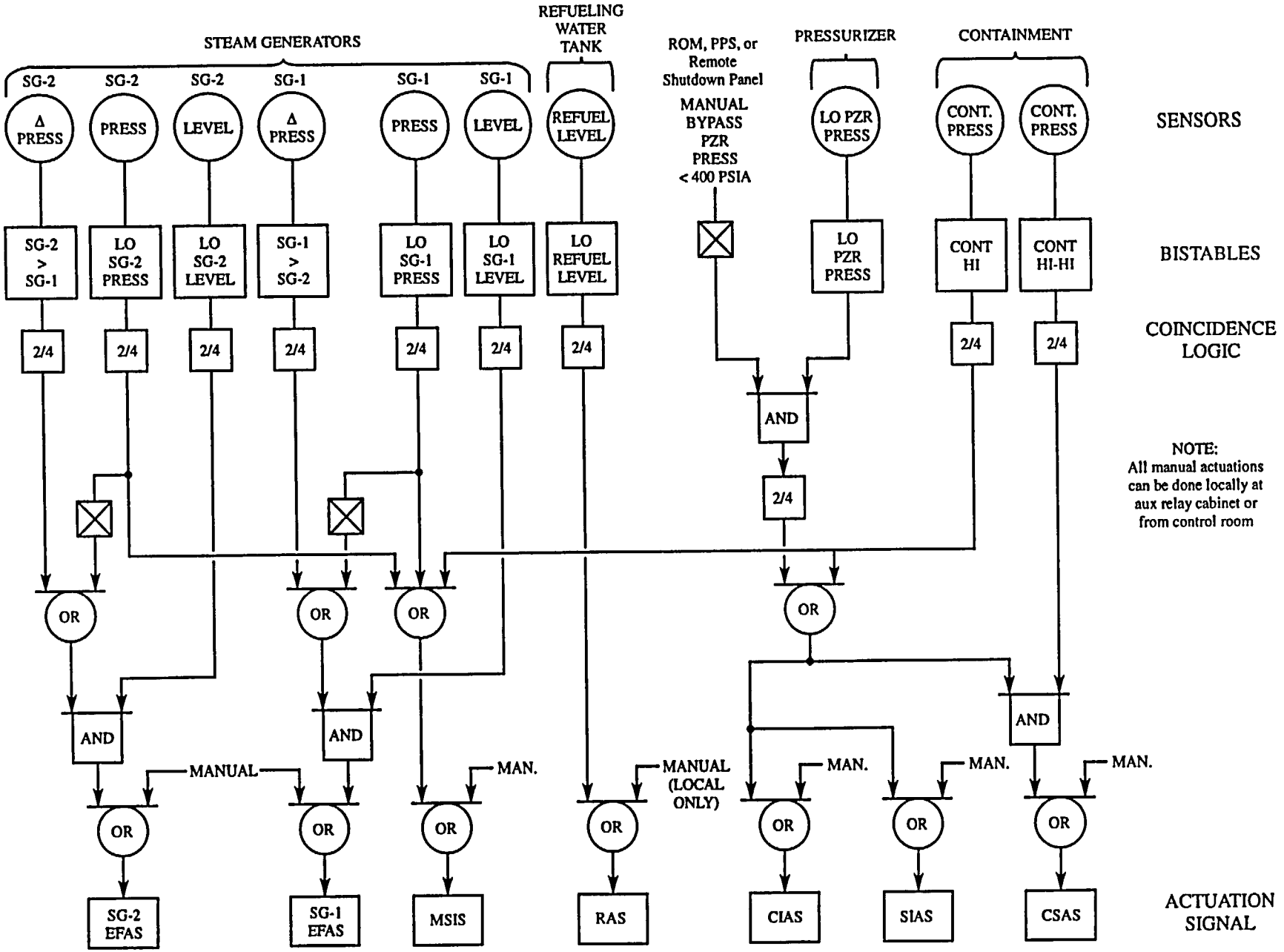


Figure 12.4-18 ESFAS Logic Diagram

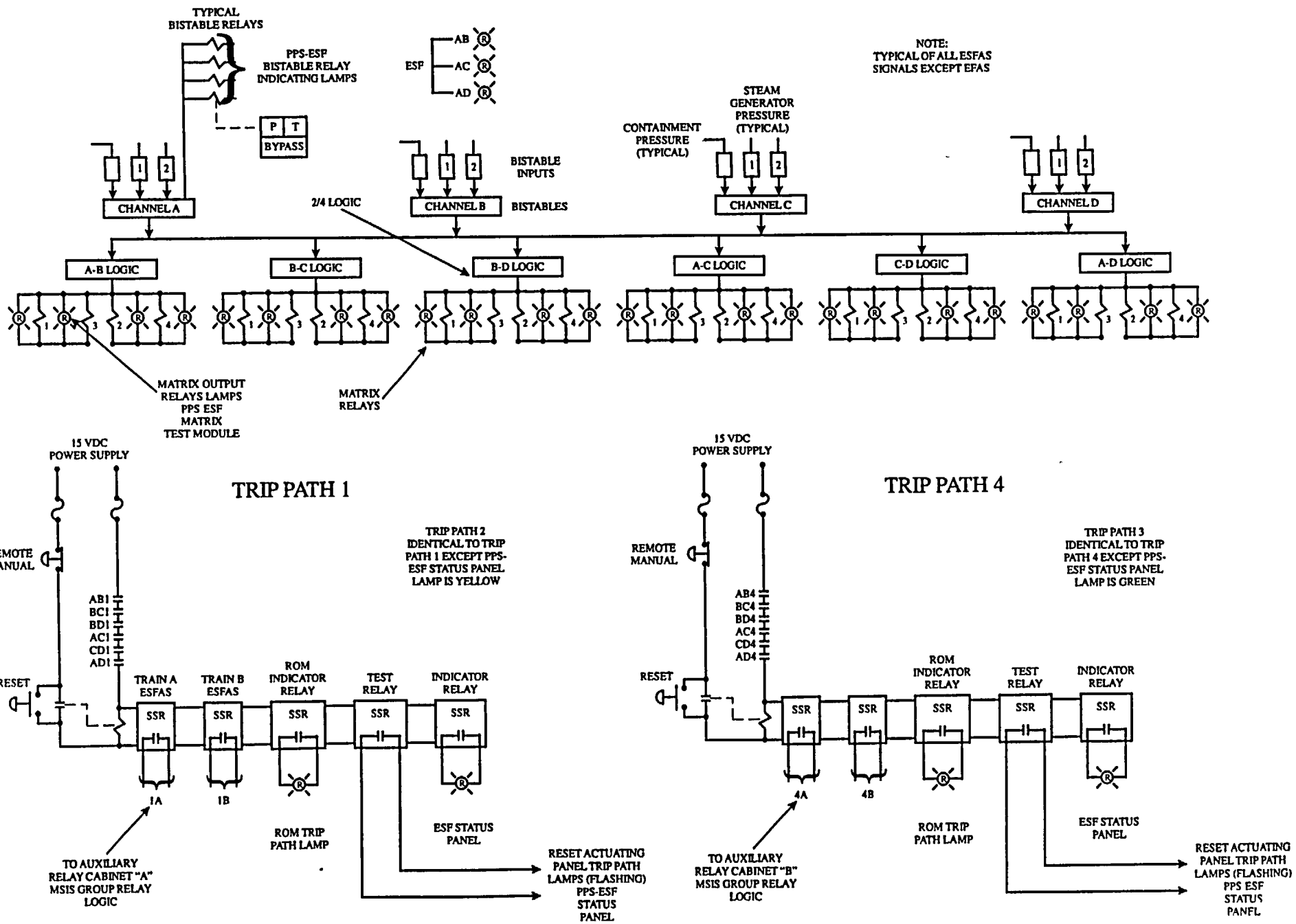


Figure 12.4-19 ESFAS Functional Diagram

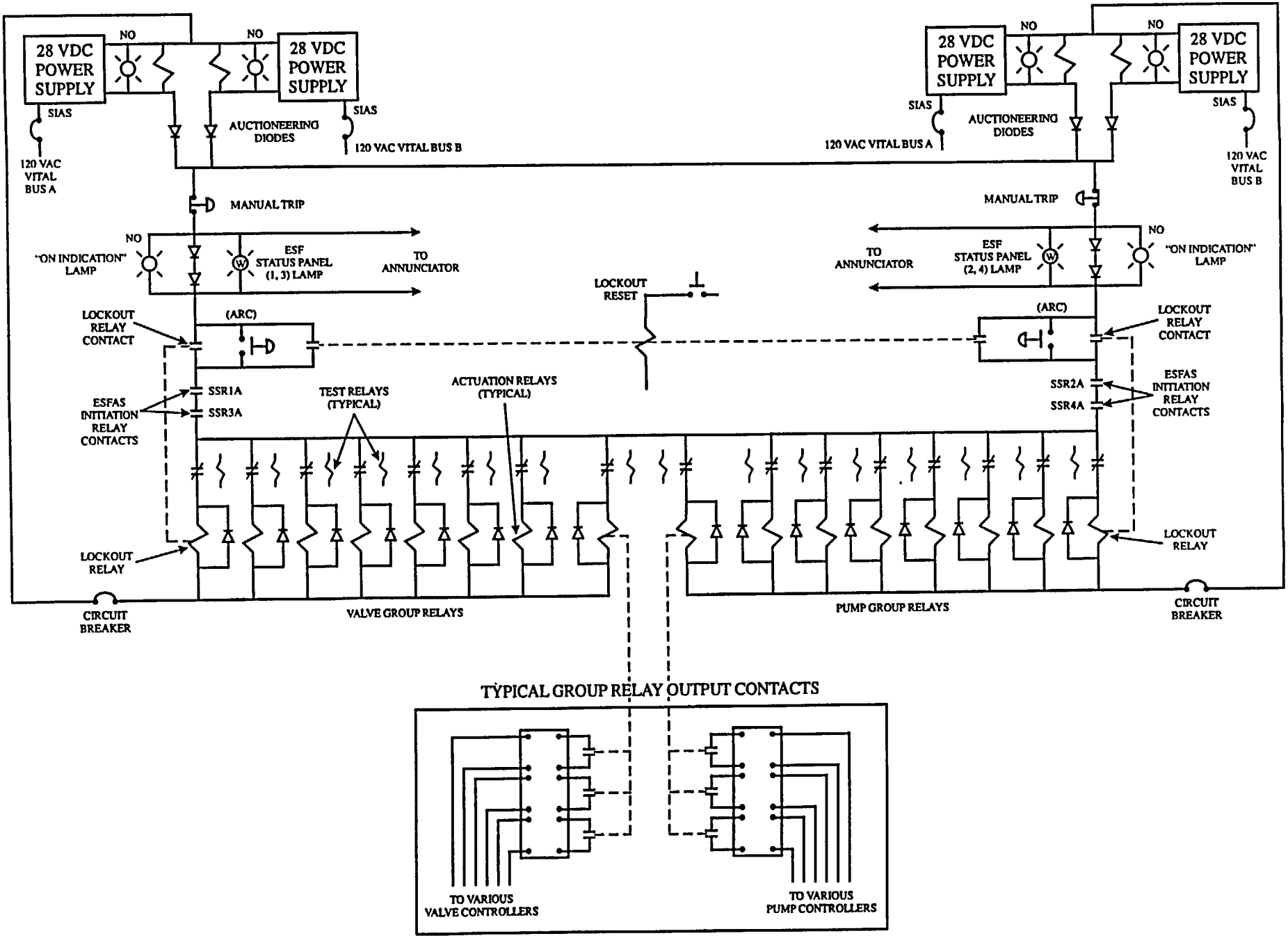


Figure 12.4-20 ESFAS Actuation Relay Cabinet Schematic - SIAS Circuit