TABLE OF CONTENTS

LIST OF FIGURES

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 out of four 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

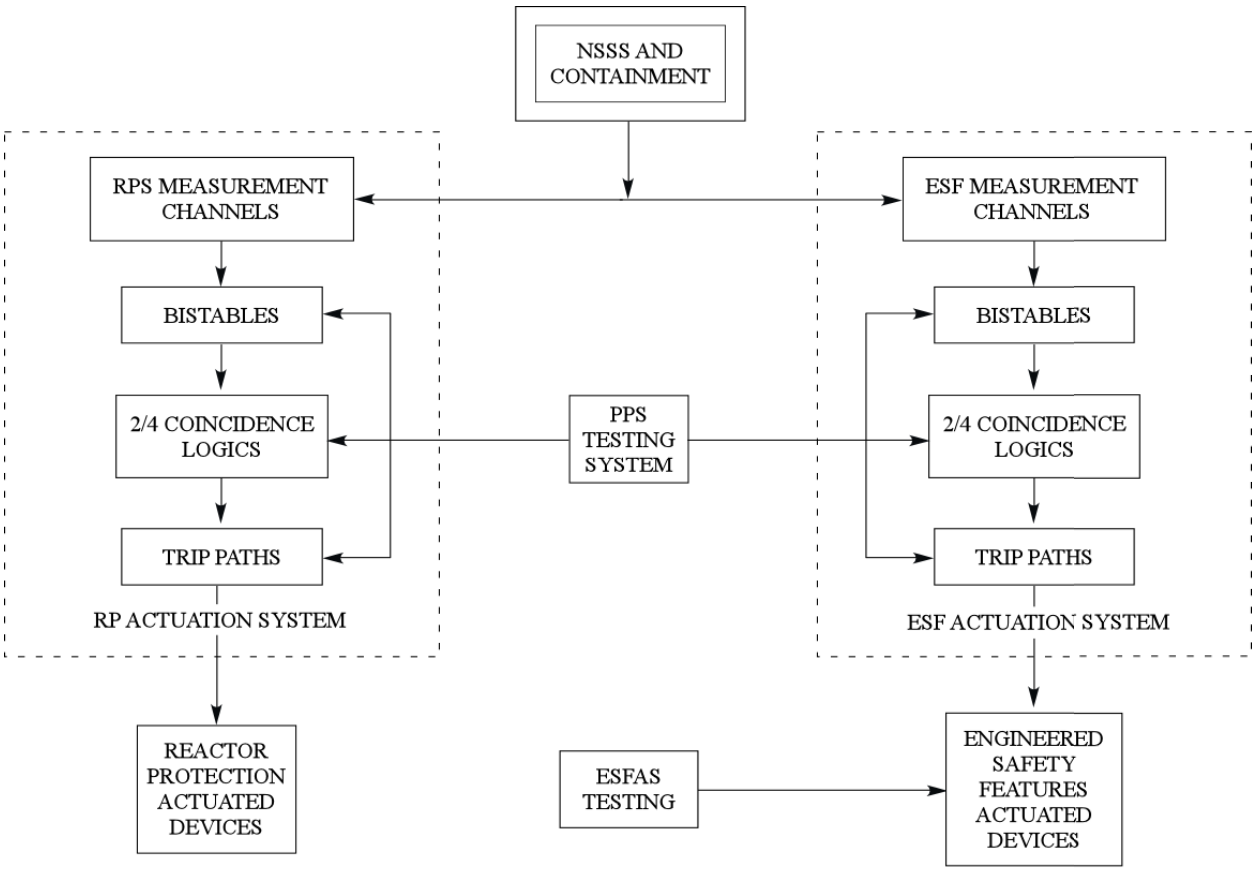


Figure 12.4-1 Plant Protection System Basic Block Diagram

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.

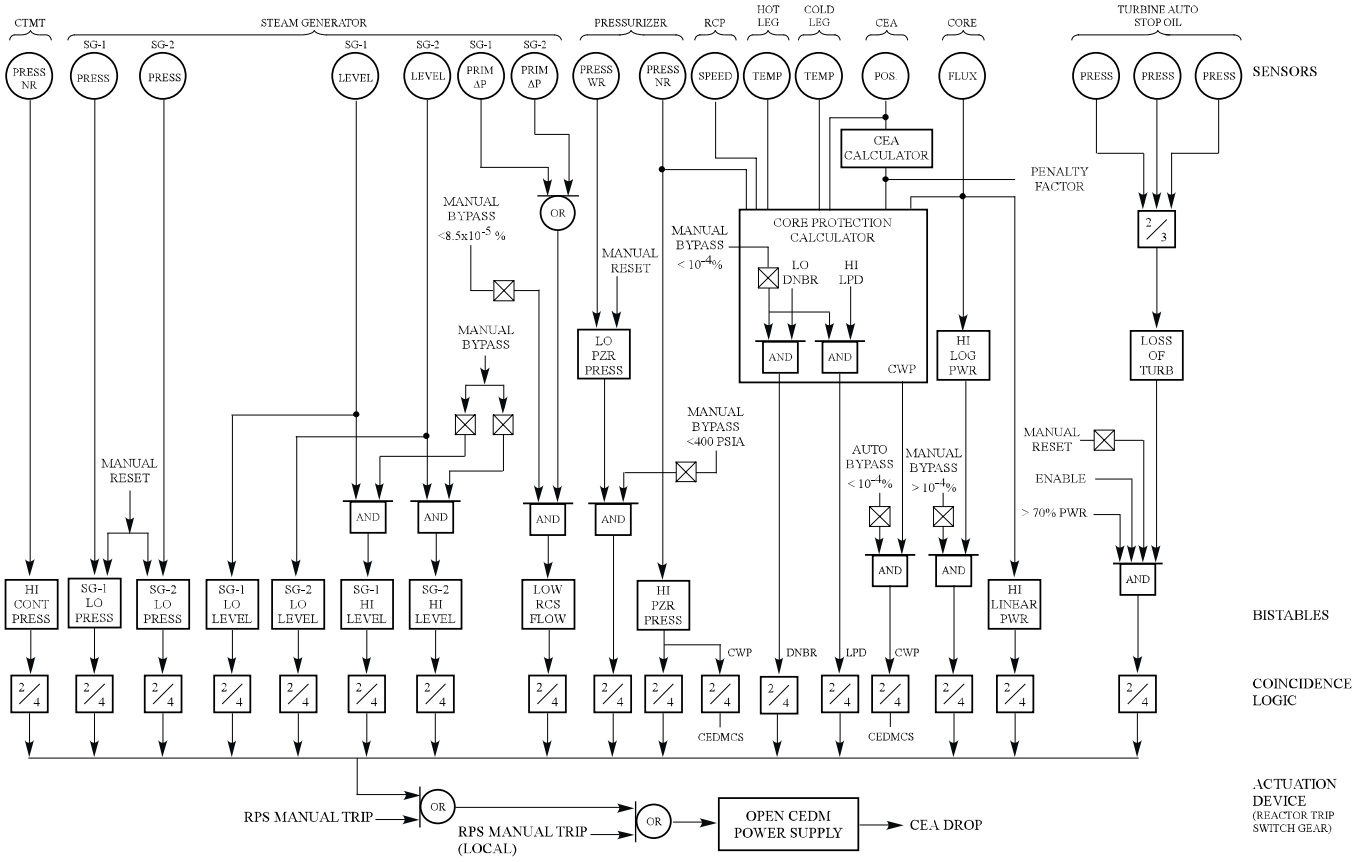
11.) All manually blocked or bypassed variables are automatically unblocked when permissive conditions no longer exist.

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



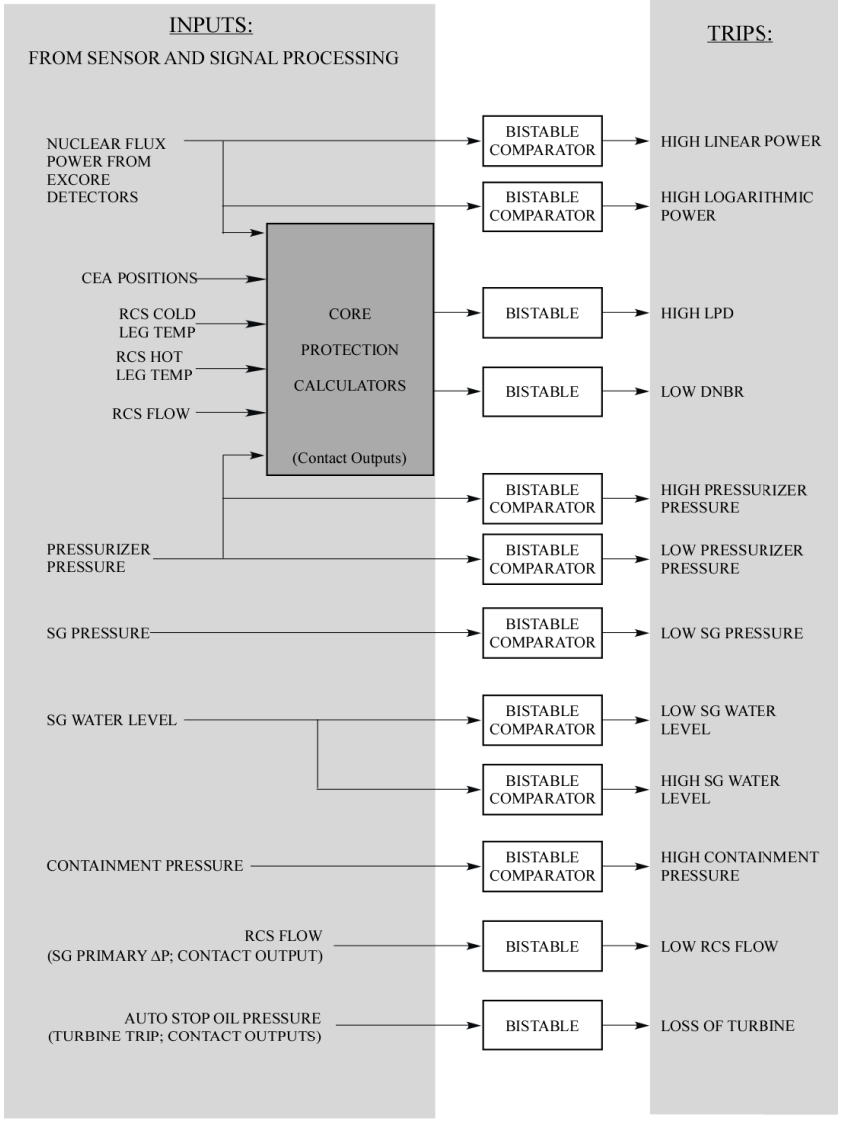


Figure 12.4-3 Bistable Comparator and CPC Process

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

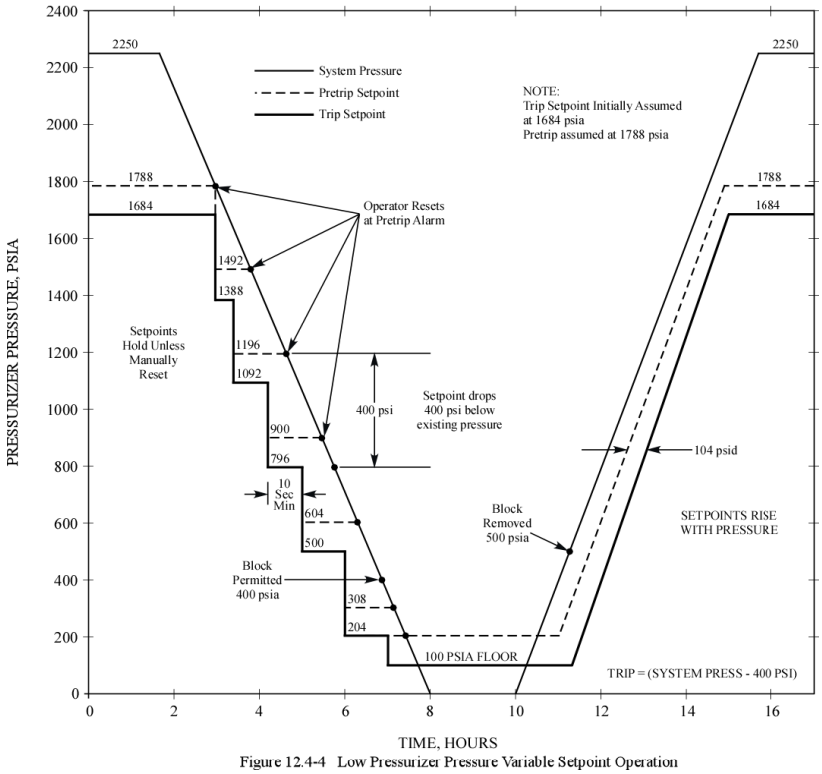


Figure 12.4-4 Low Pressurizer Pressure Variable Setpoint Operation

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

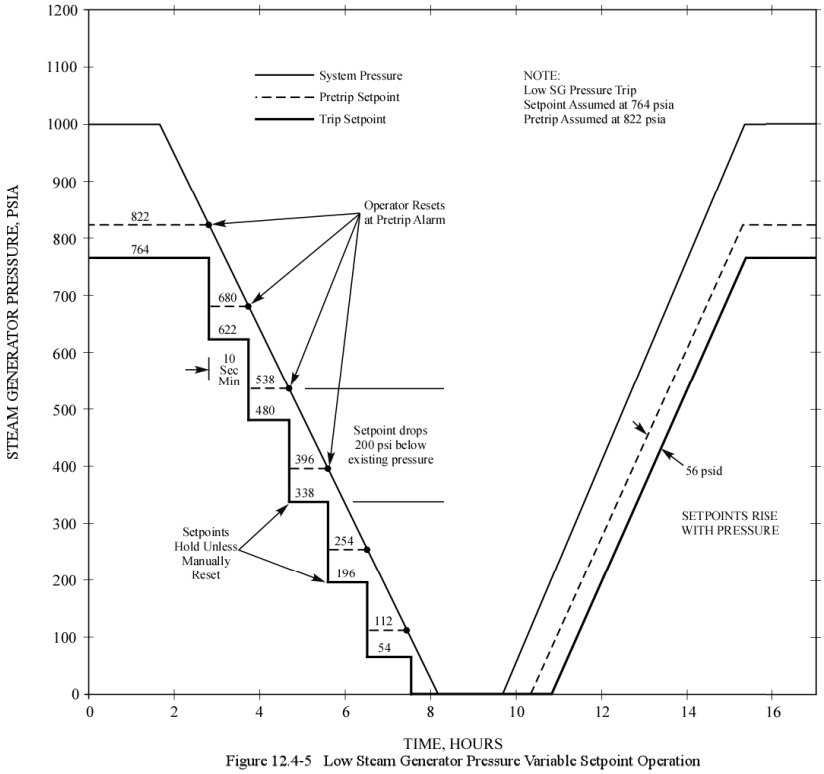


Figure 12.4-5 Low Steam Generator Pressure Variable Setpoint Operation

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

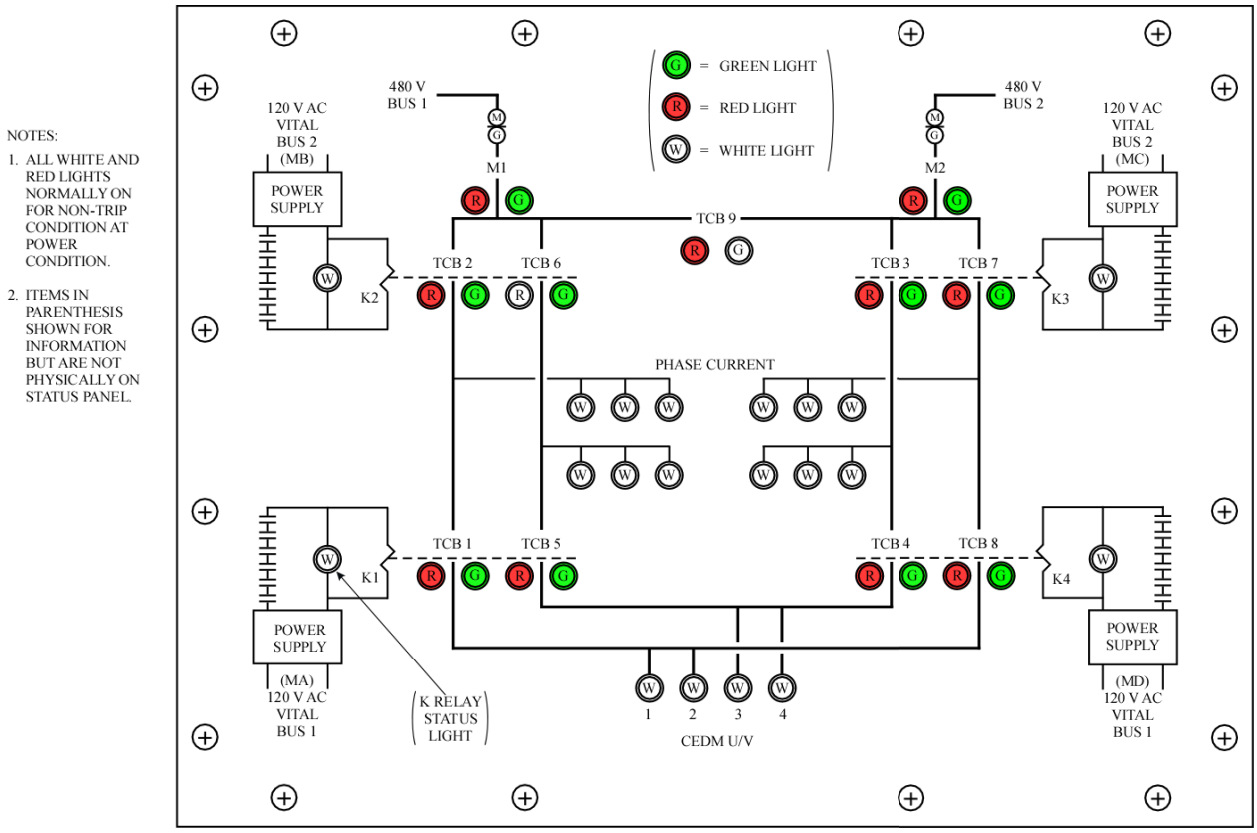


Figure 12.4-6 Reactor Trip Status Panel

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.

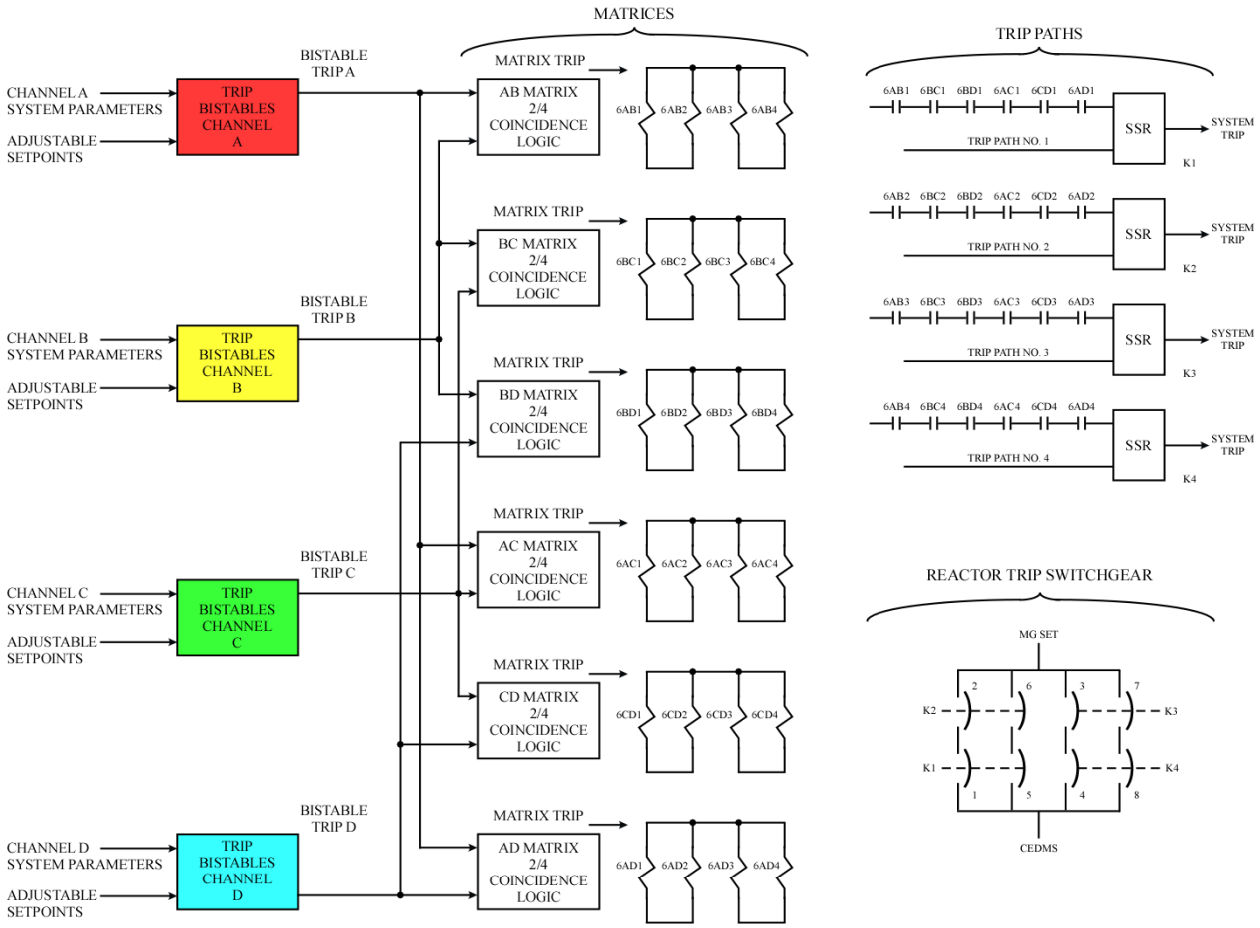


Figure 12.4-7 RPS Trip Signal Flowpath

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).

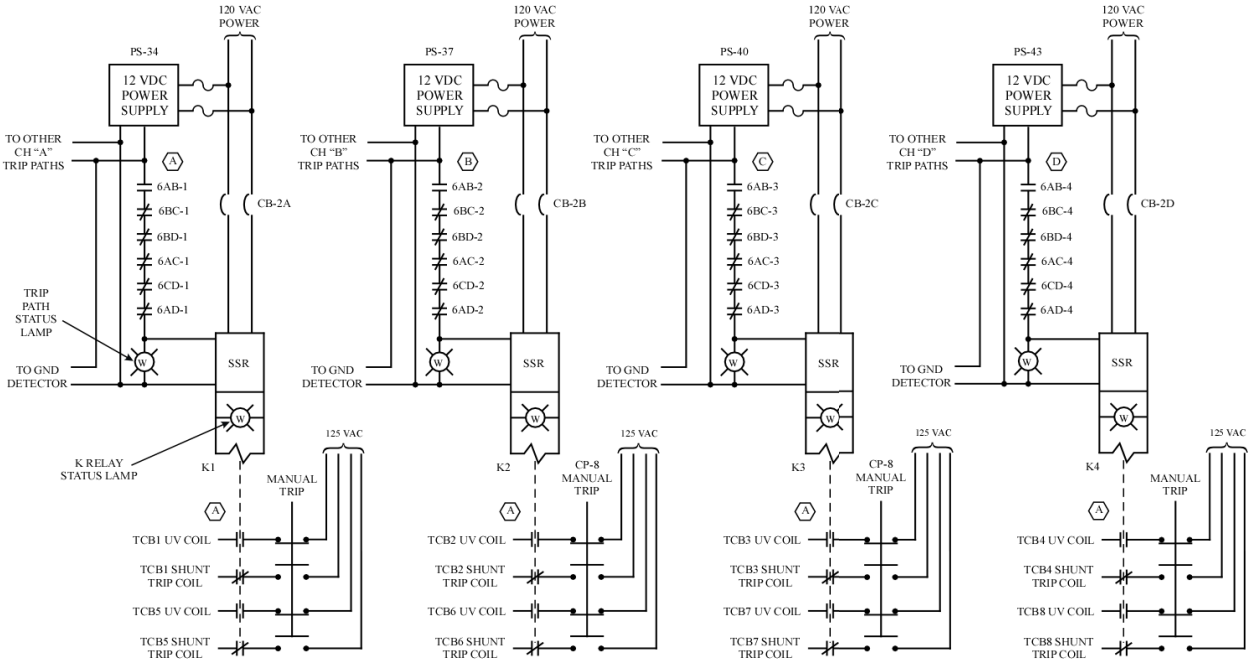


Figure 12.4-9 RPS Trip Path Status With Trip in the AB Matrix

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.

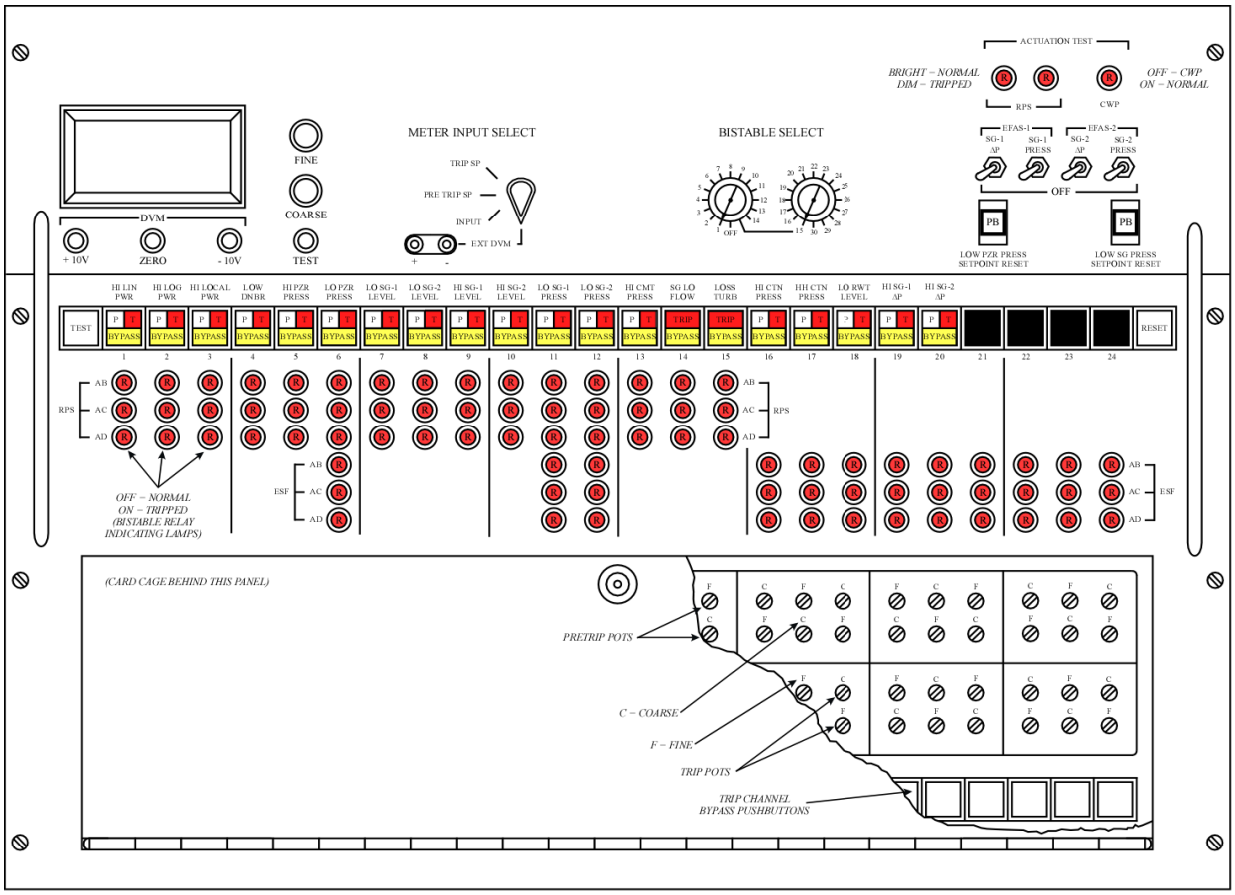


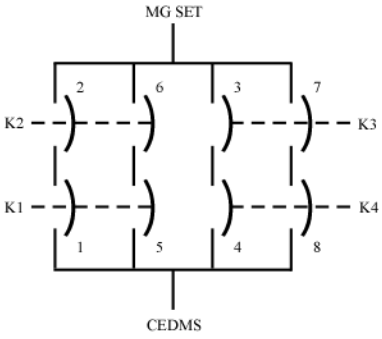
Figure 12.4-8 Bistable Control Panel Channel A

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

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.

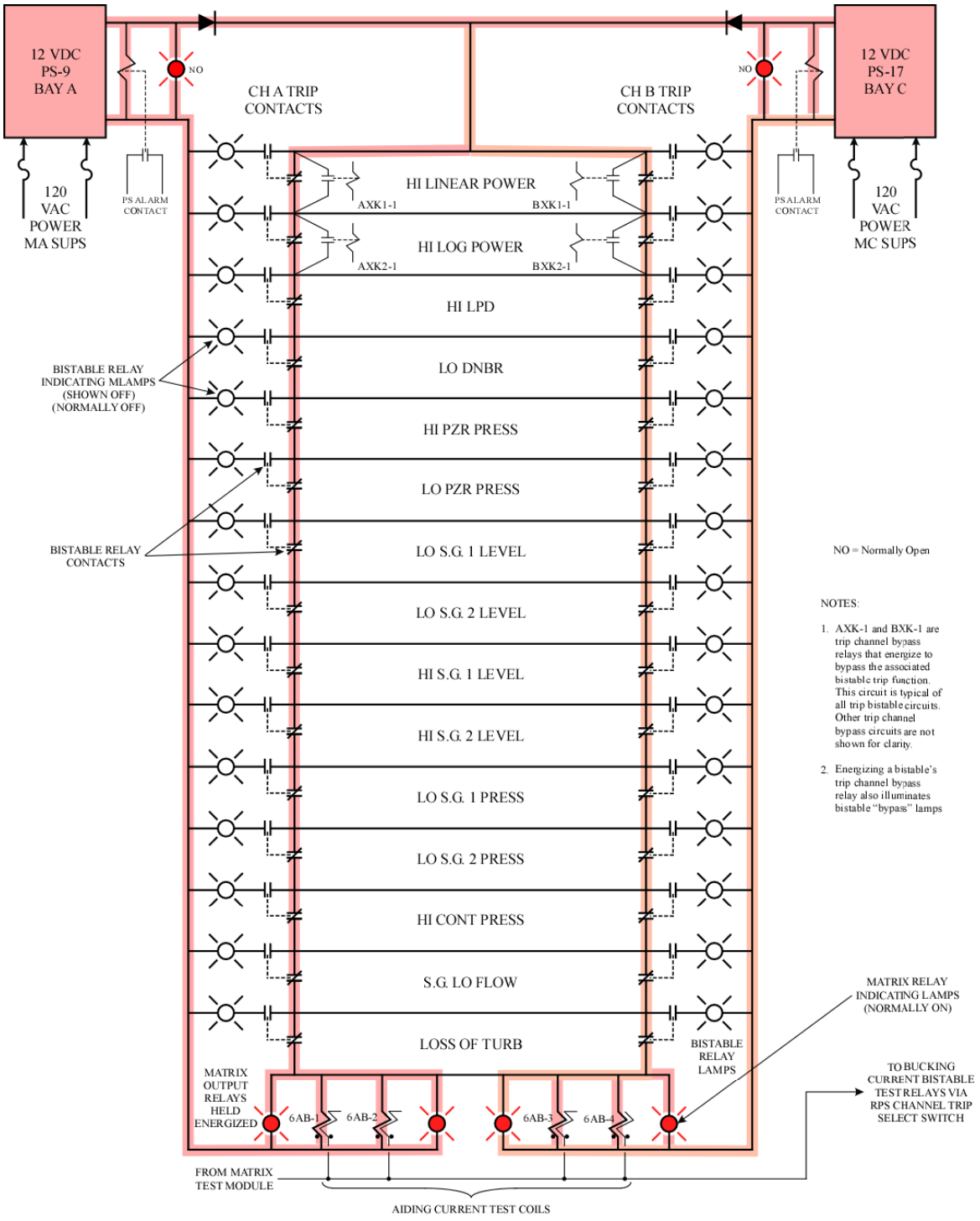


Figure 12.4-10 RPS AB Logic Matrix - Normal (untripped)

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.

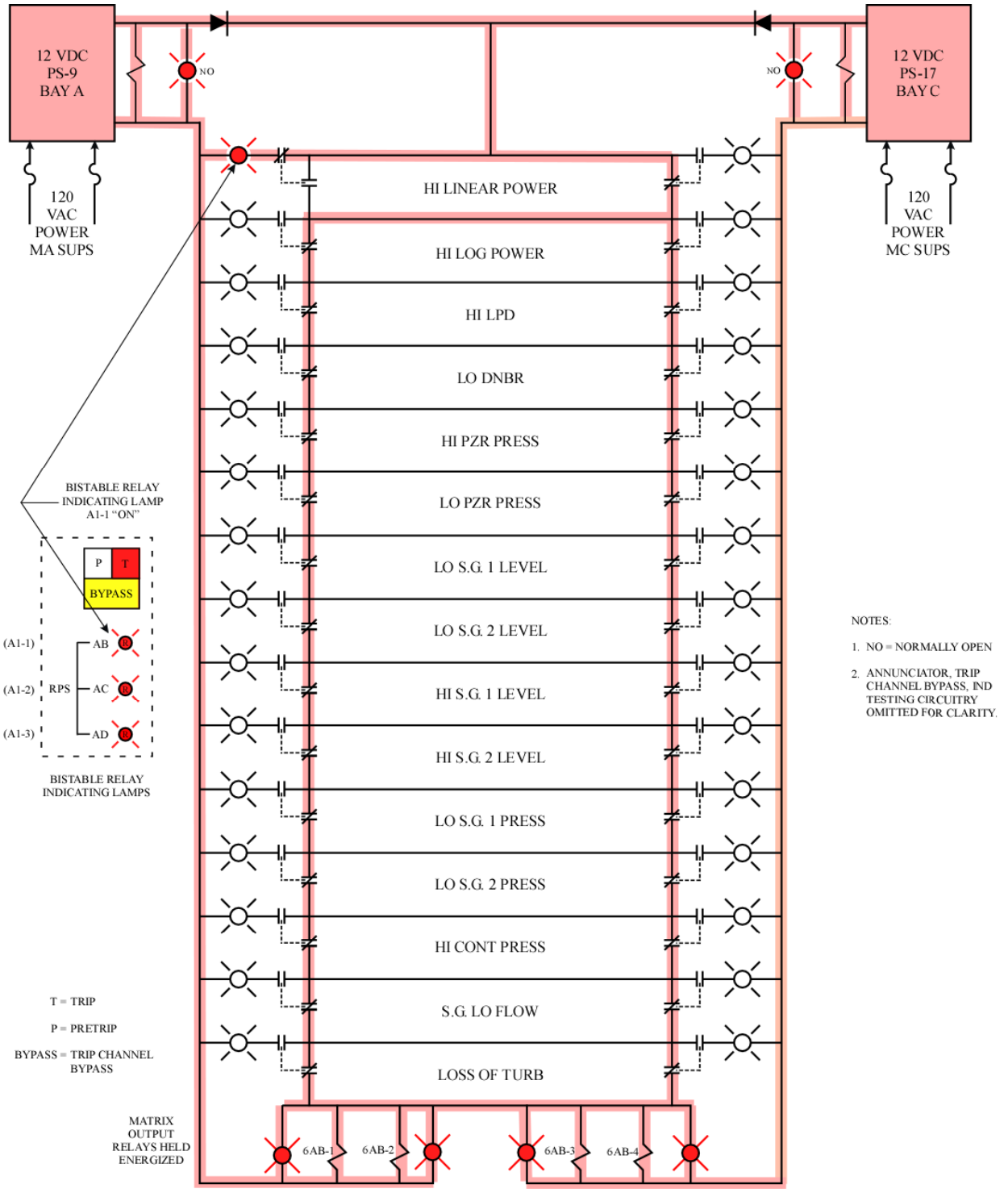


Figure 12.4-11 RPS Logic Matrix With High Linear Power Channel A Tripped

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.

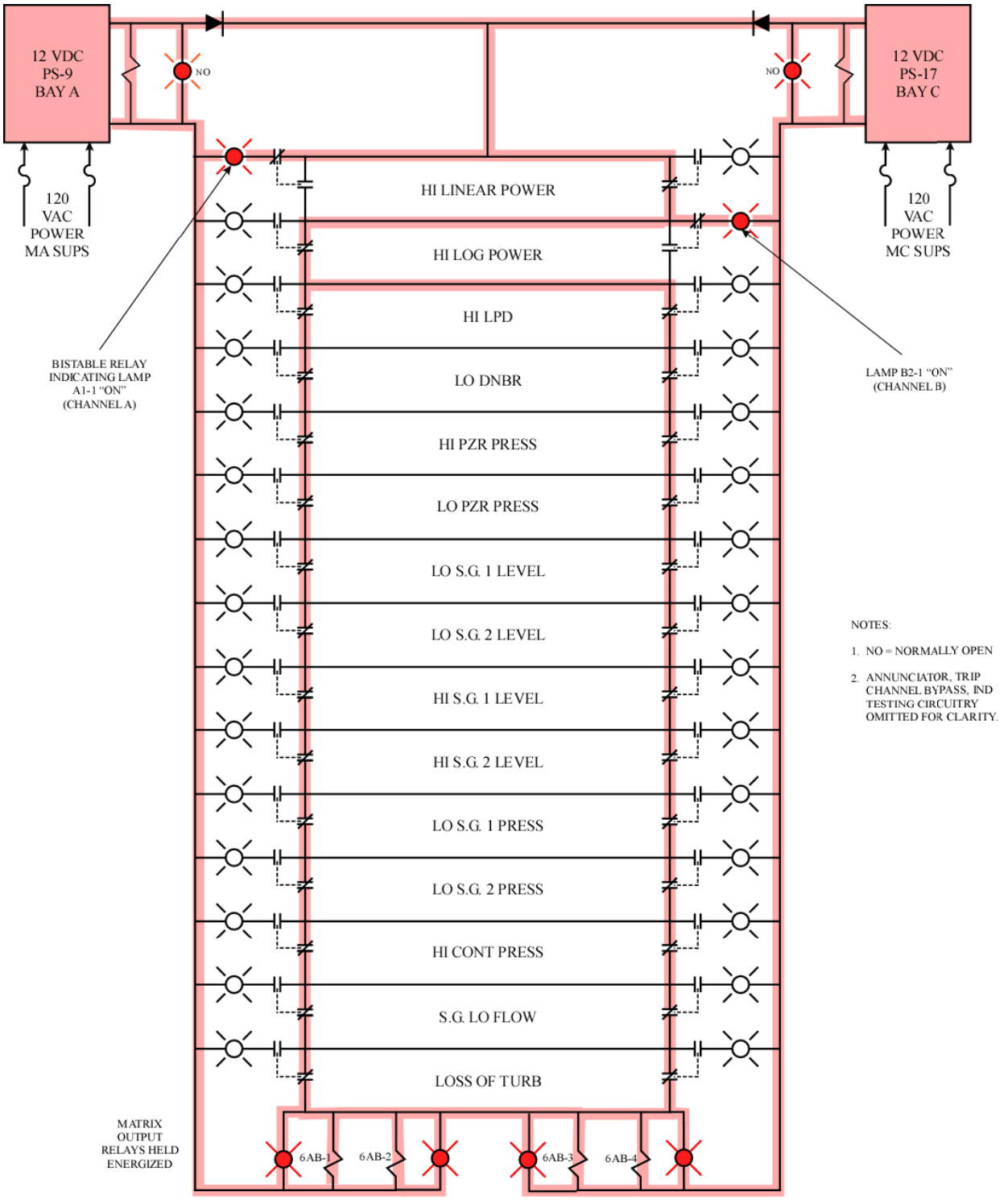


Figure 12.4-12 RPS Logic Matrix With Linear Power Channel A and High Log Power Channel B Tripped

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".

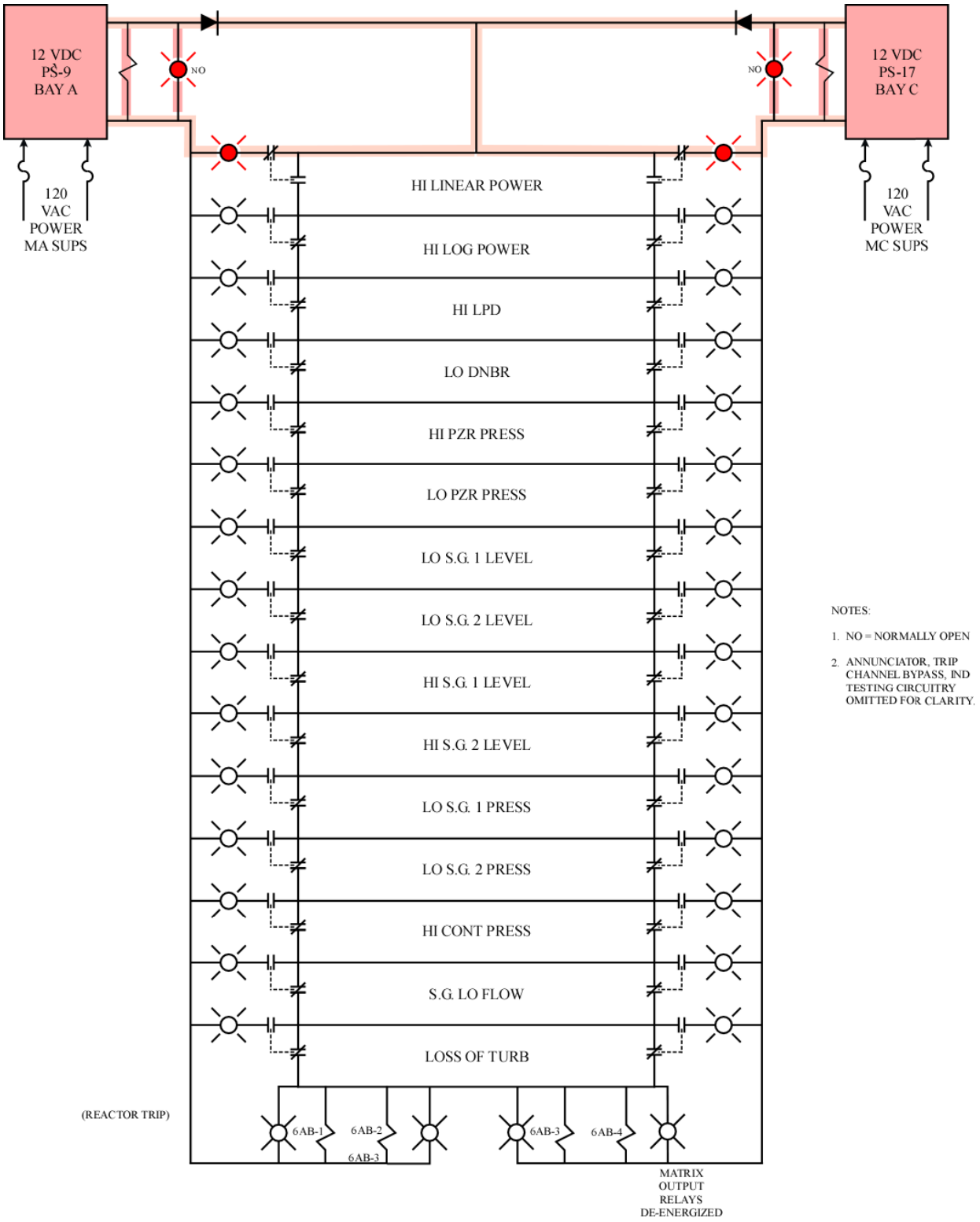


Figure 12.4-13 RPS AB Logic Matrix With High Linear Power Channel A and Channel B Tripped

Figure 12.4-13 depicts 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

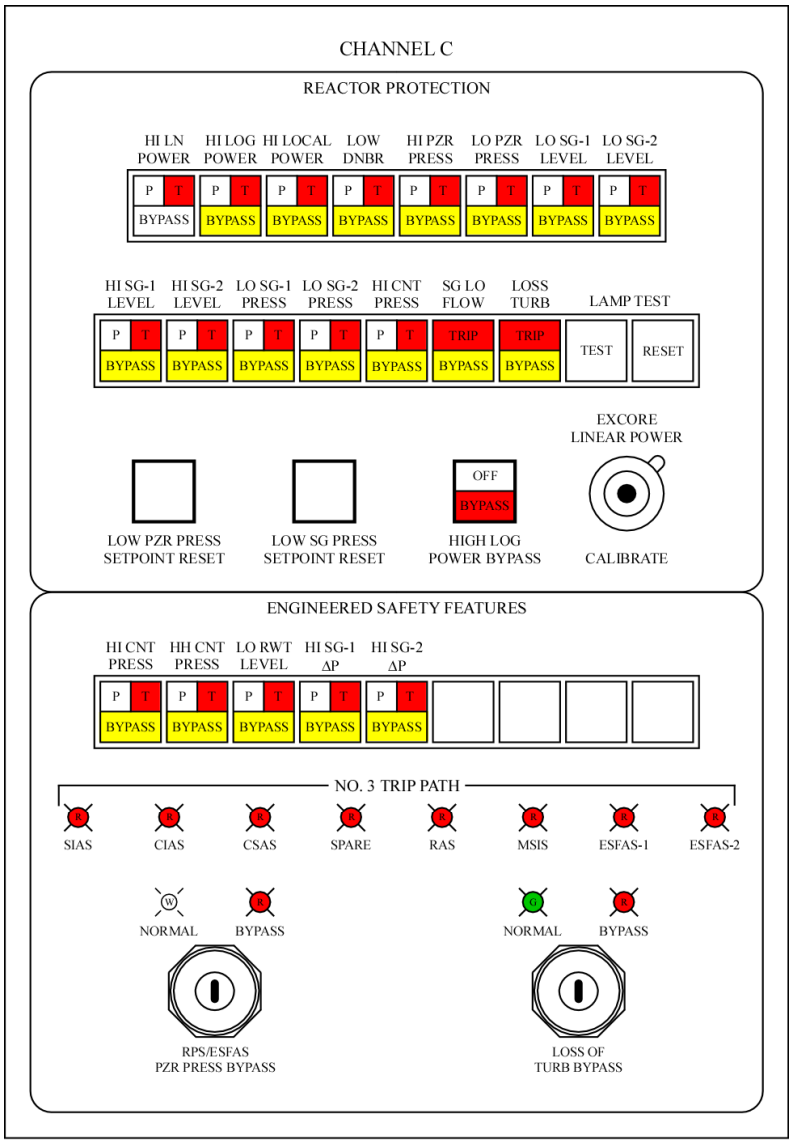


Figure 12.4-14 PPS Remote Operator's Module

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 an operating bypass since the trips are still in effect but at a different setpoint.

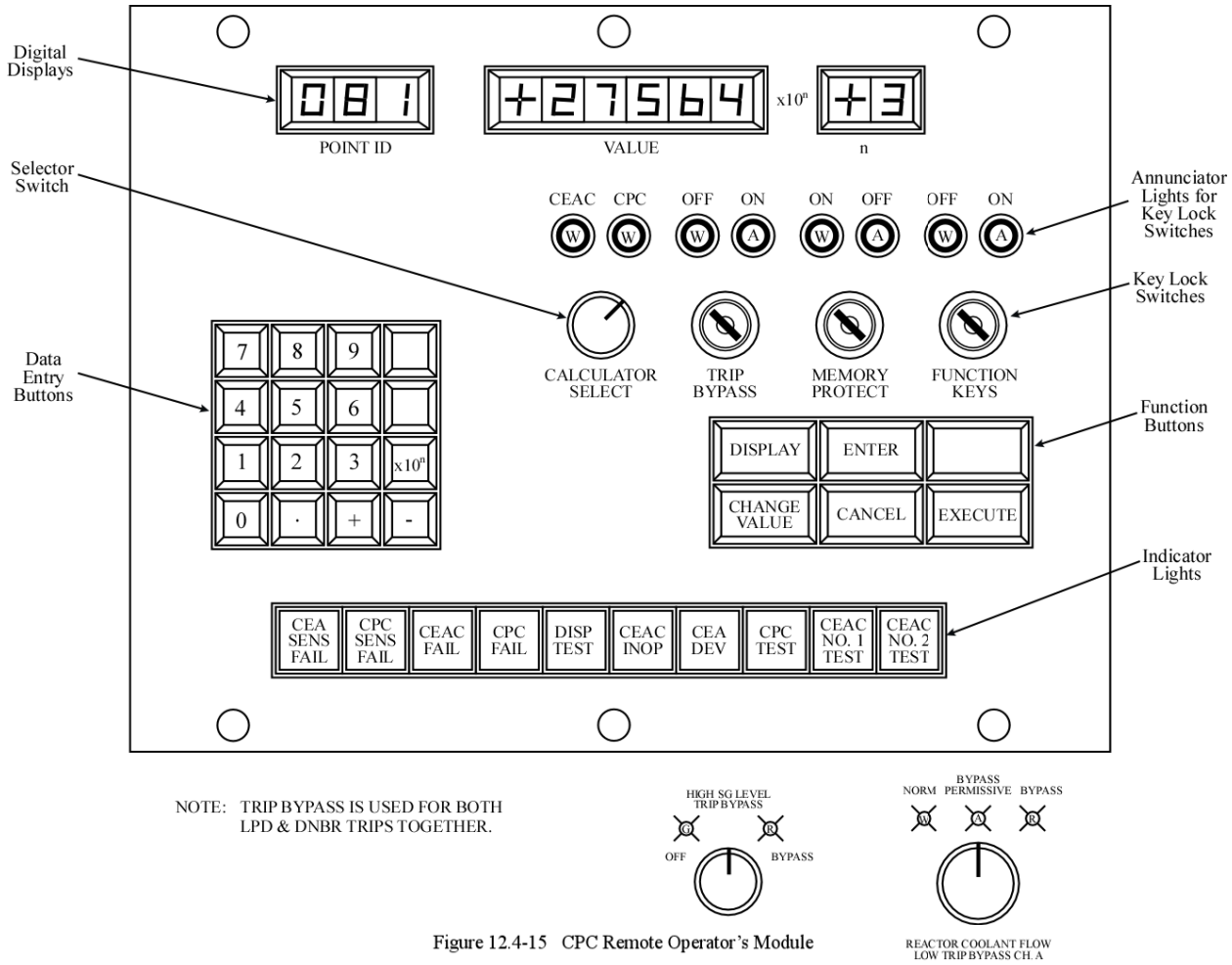


Figure 12.4-15 CPC Remote Operator's Module

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 Bypass

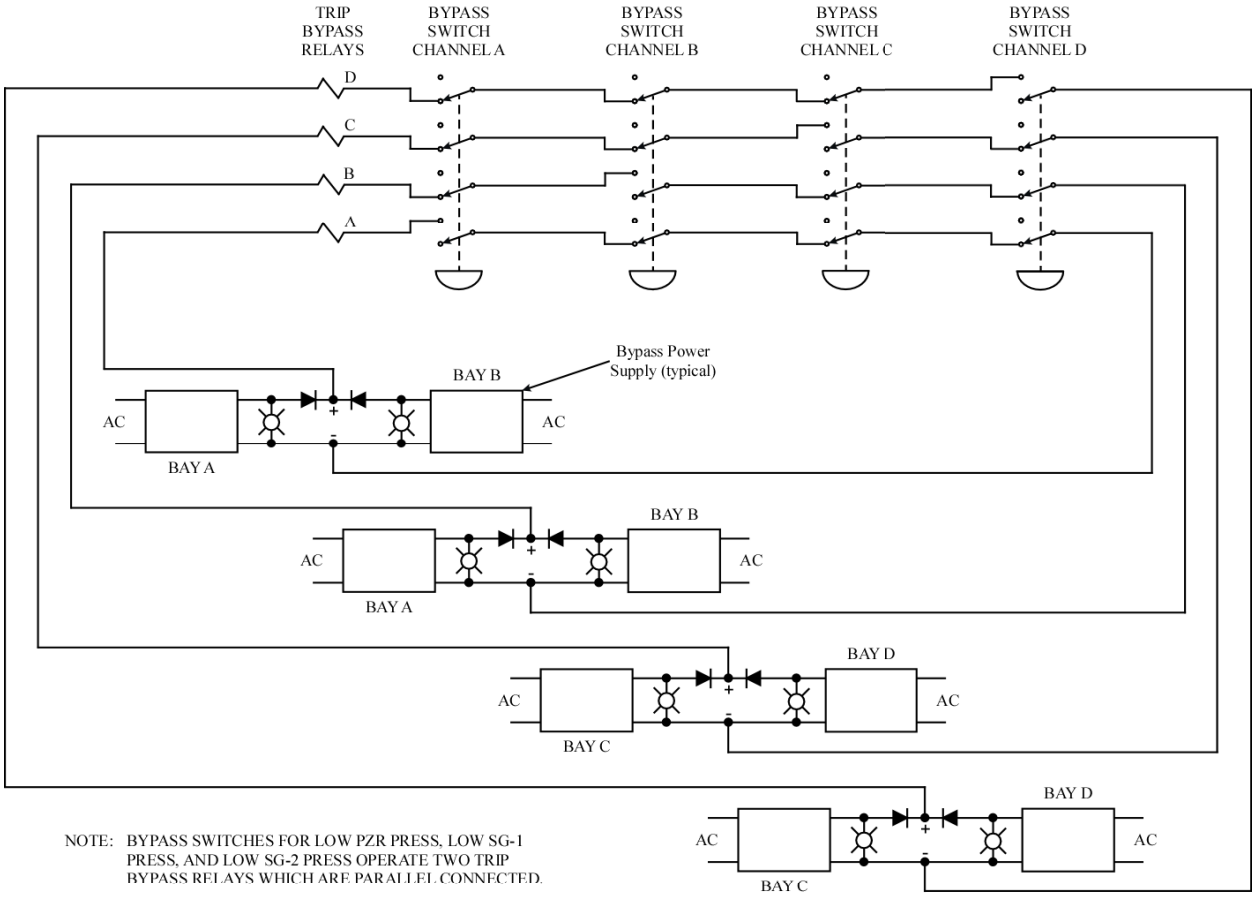


Figure 12.4-16 Trip Channel Bypass Electrical Interlock

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

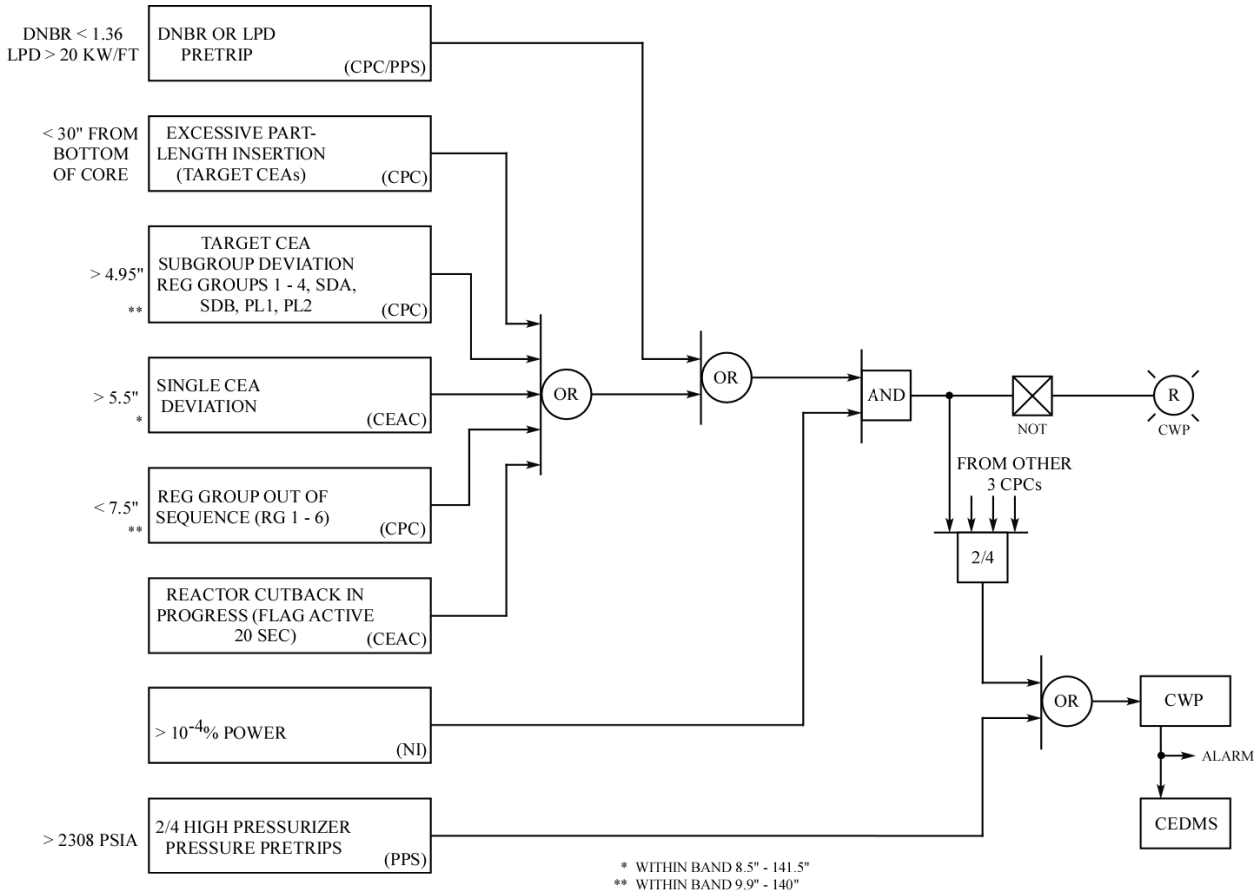


Figure 12.4-17 CEA Withdrawal Prohibit Logic Diagram

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 7.0×10^{-5}% and 10×10^{-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

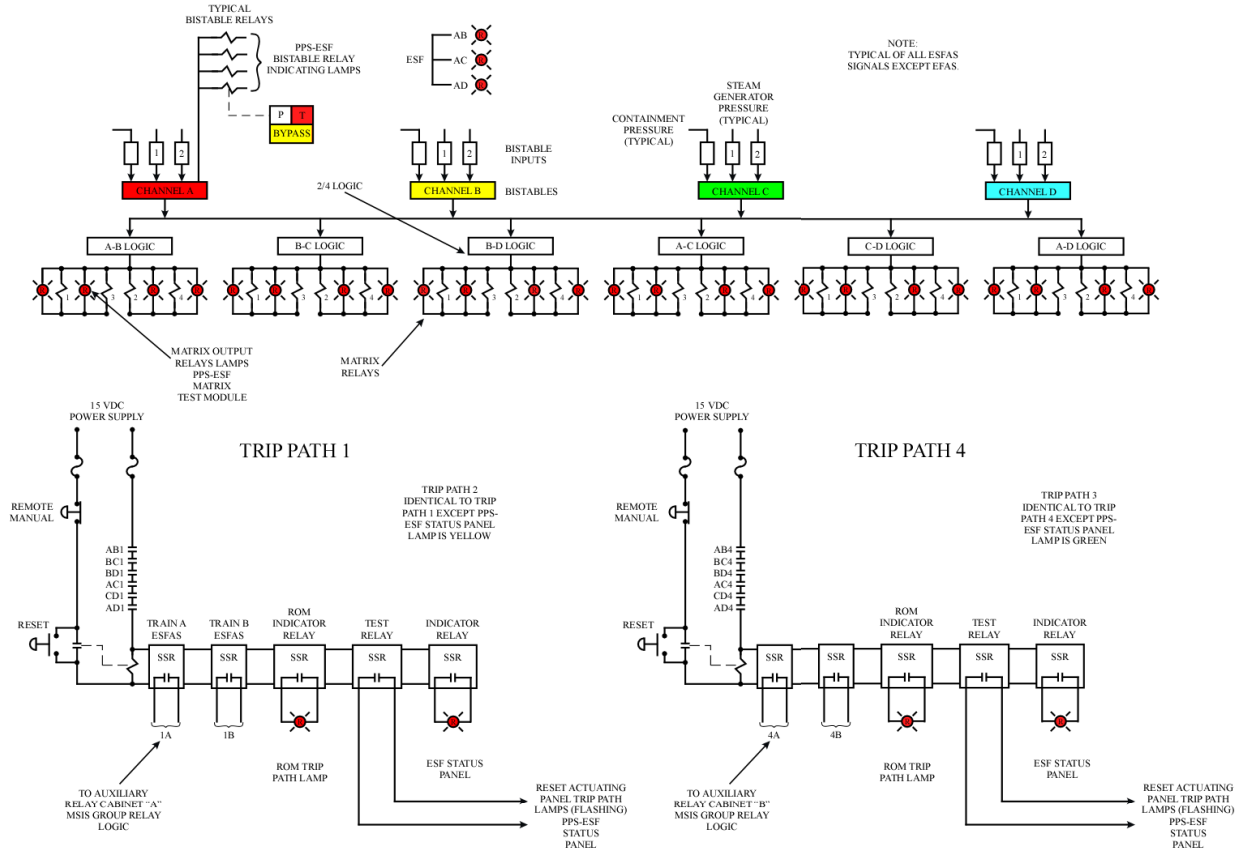


Figure 12.4-19 ESFAS Functional Diagram

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.

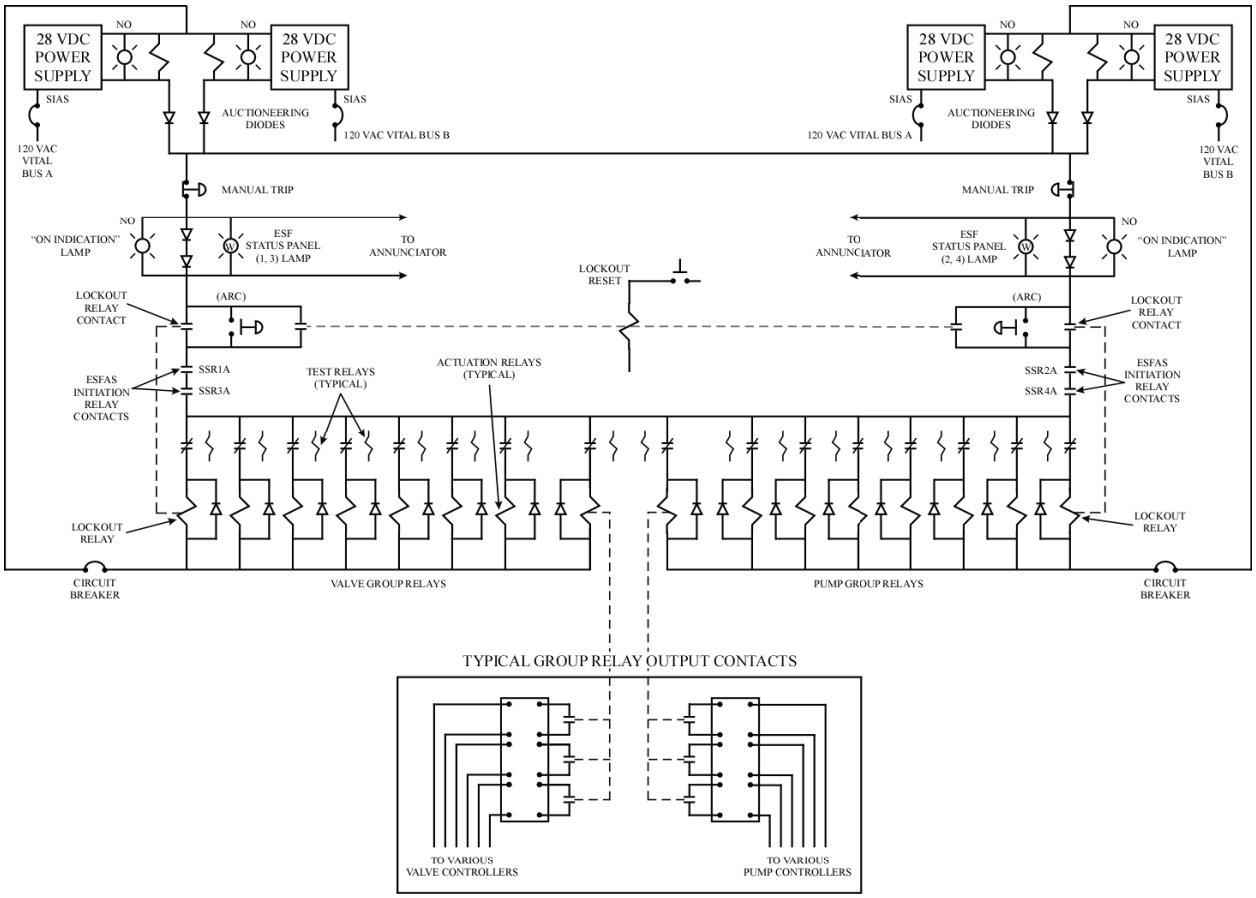


Figure 12.4-20 ESFAS Actuation Relay Cabinet Schematic - SIAS Circuit

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

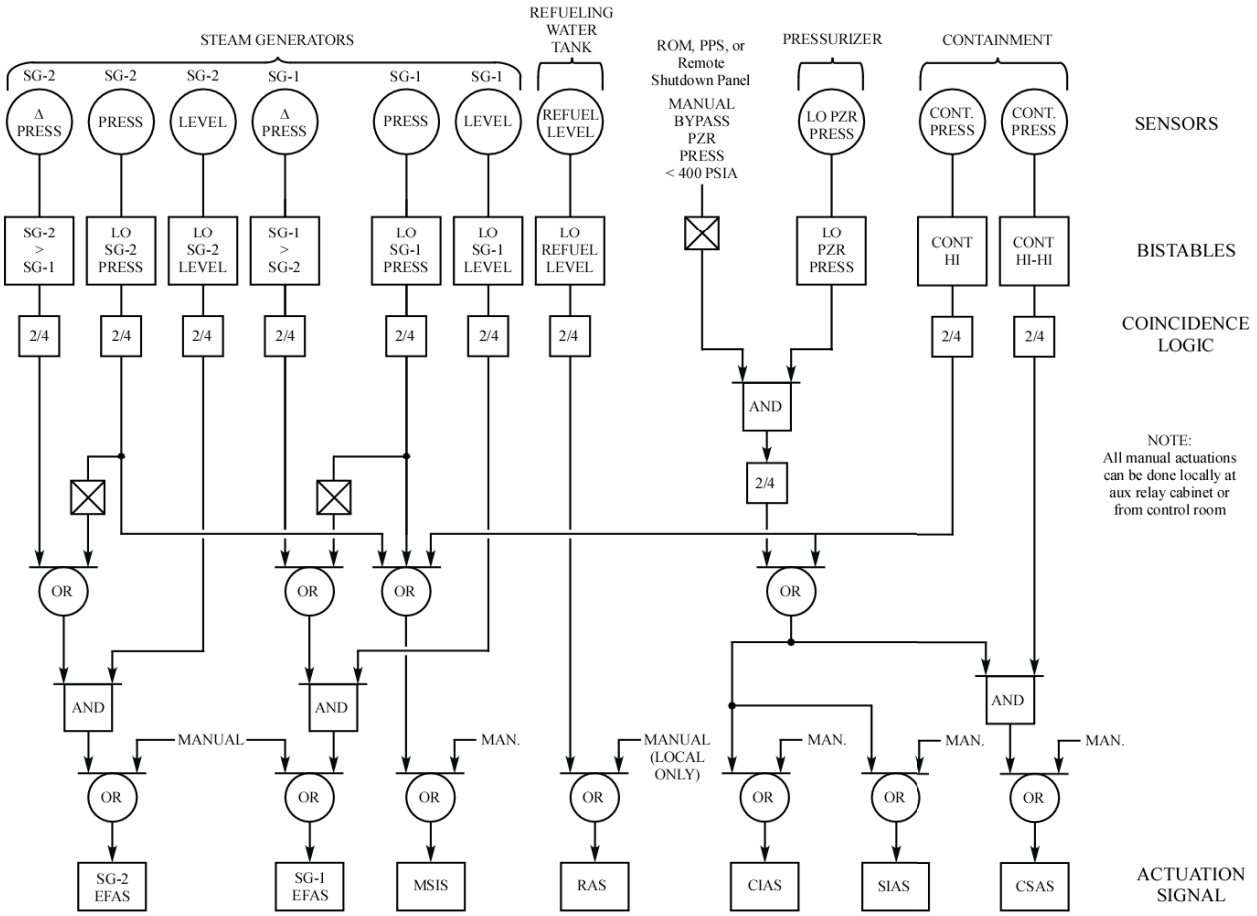


Figure 12.4-18 ESFAS Logic Diagram

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.

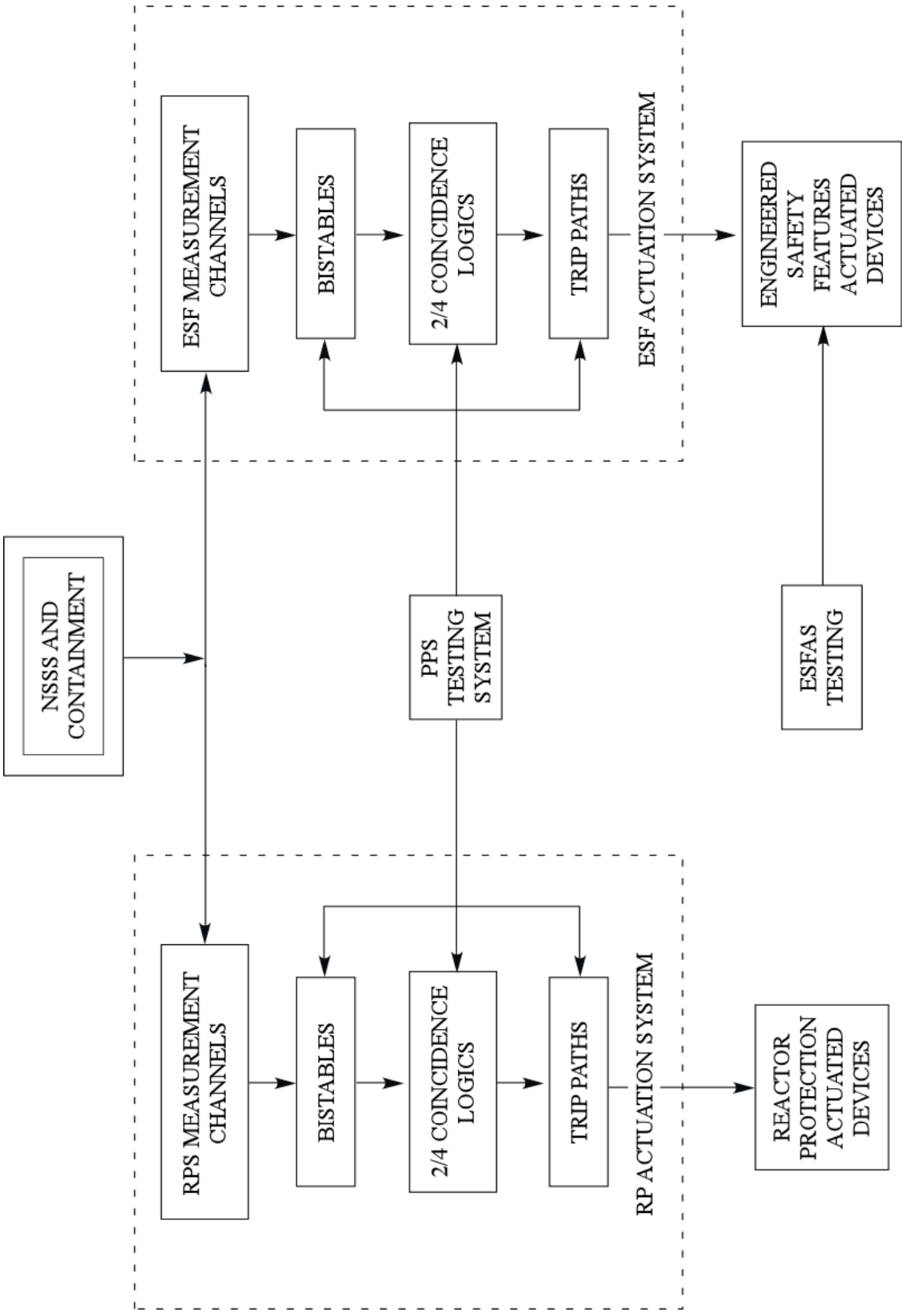


Figure 12.4-1 Plant Protection System Block Diagram

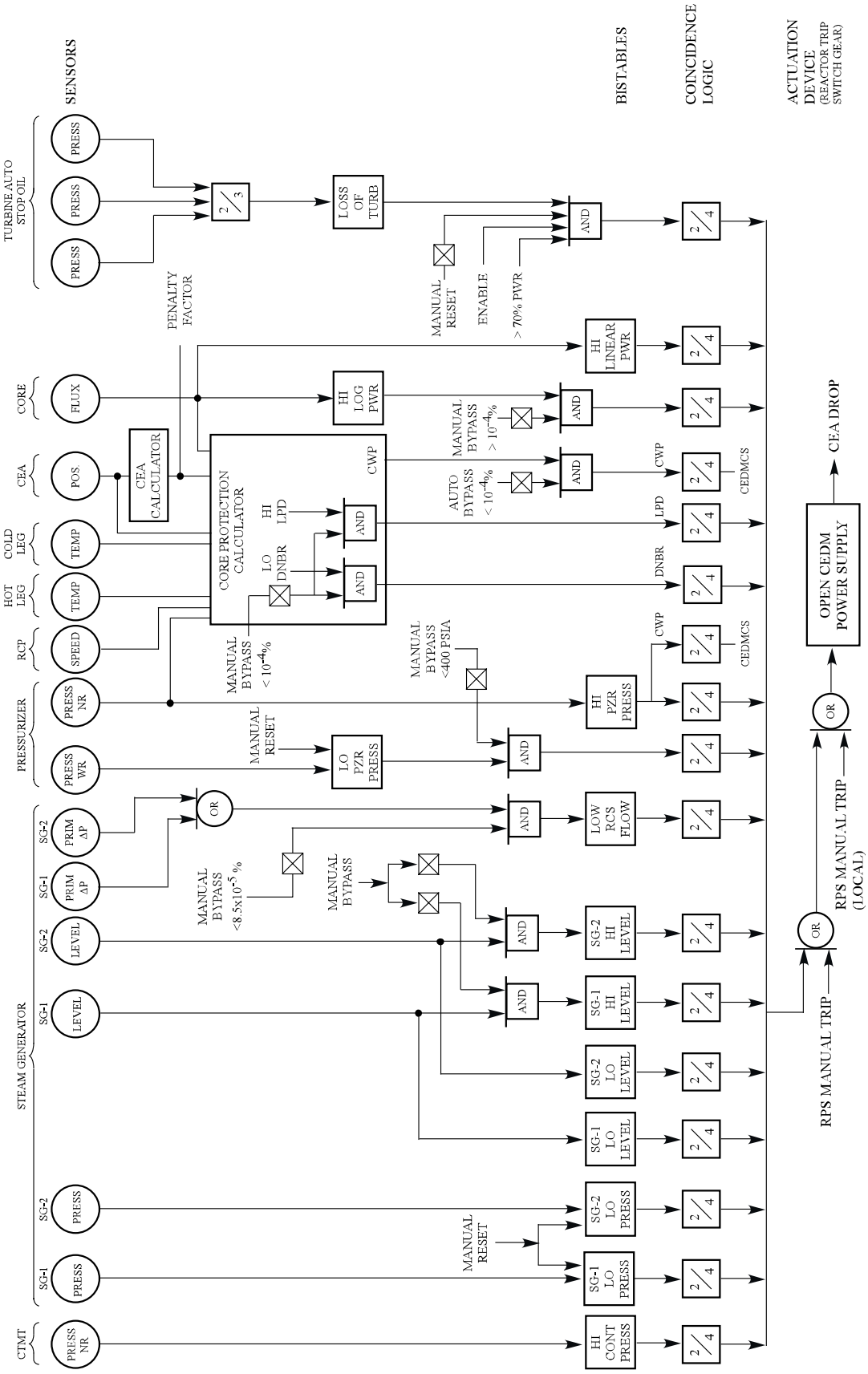


Figure 12.4-2 Reactor Trip Logic Diagram

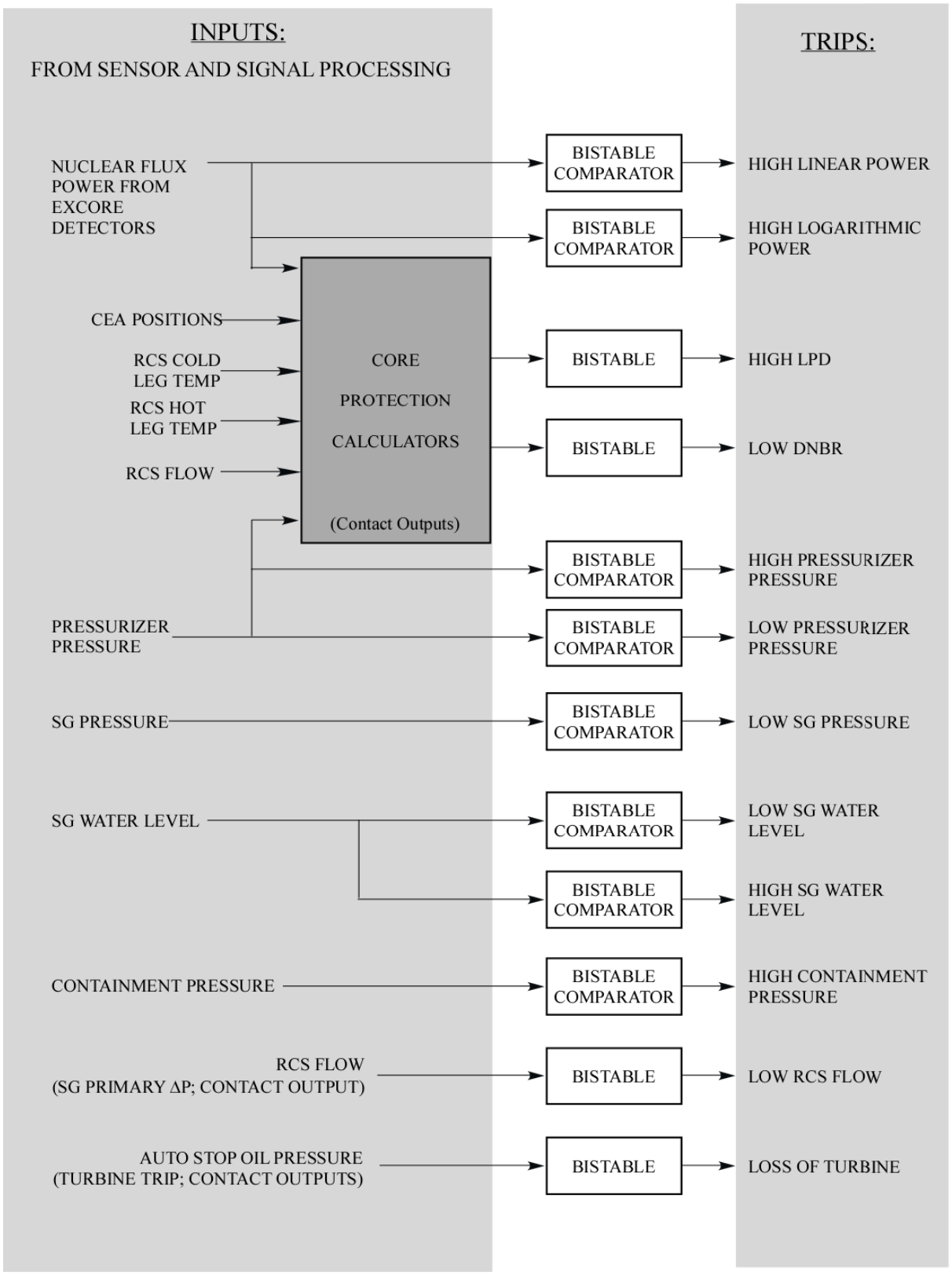


Figure 12.4-3 Bistable Comparator and CPC Process

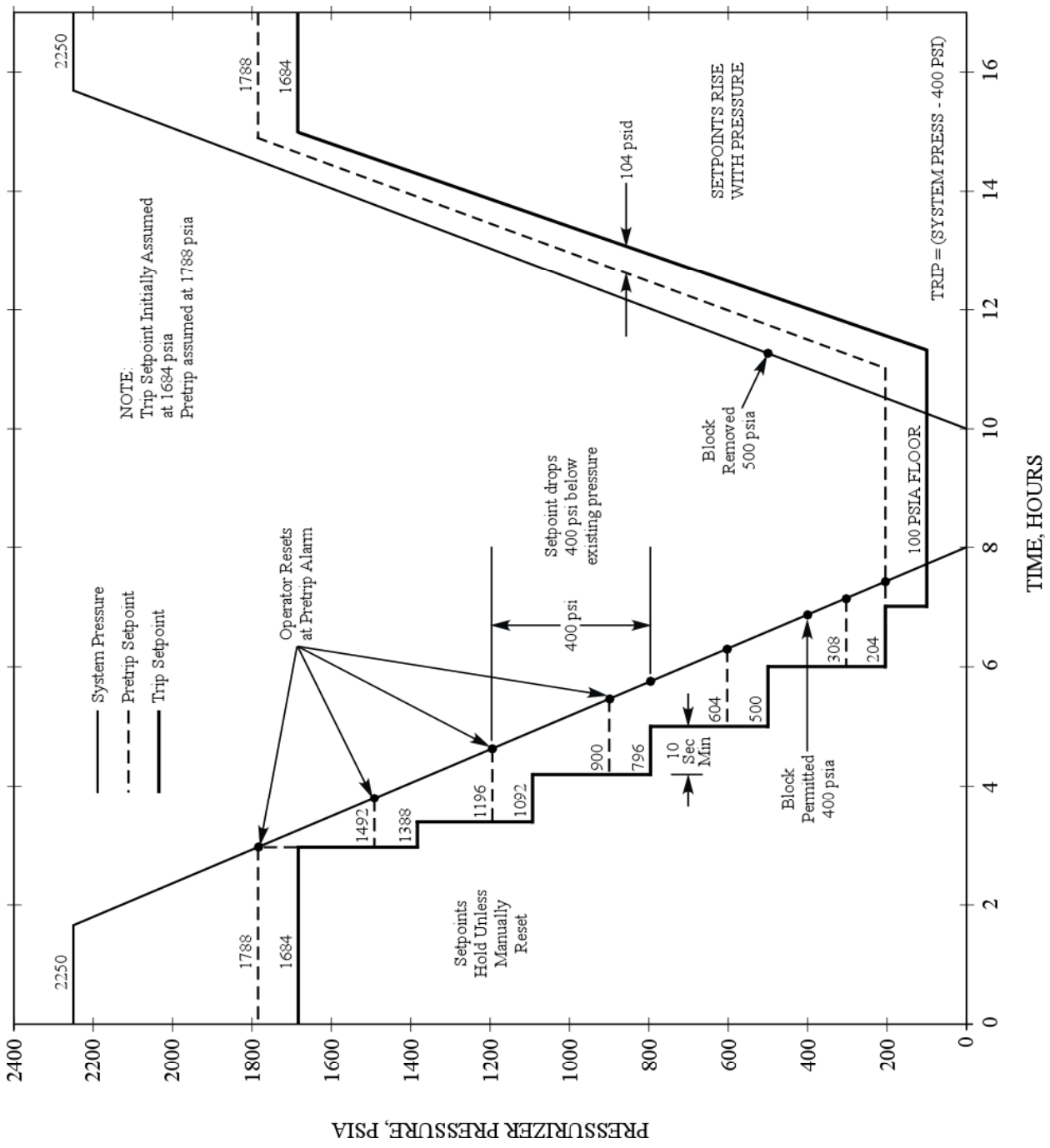


Figure 12.4-4 Low Pressurizer Pressure Variable Setpoint Operation

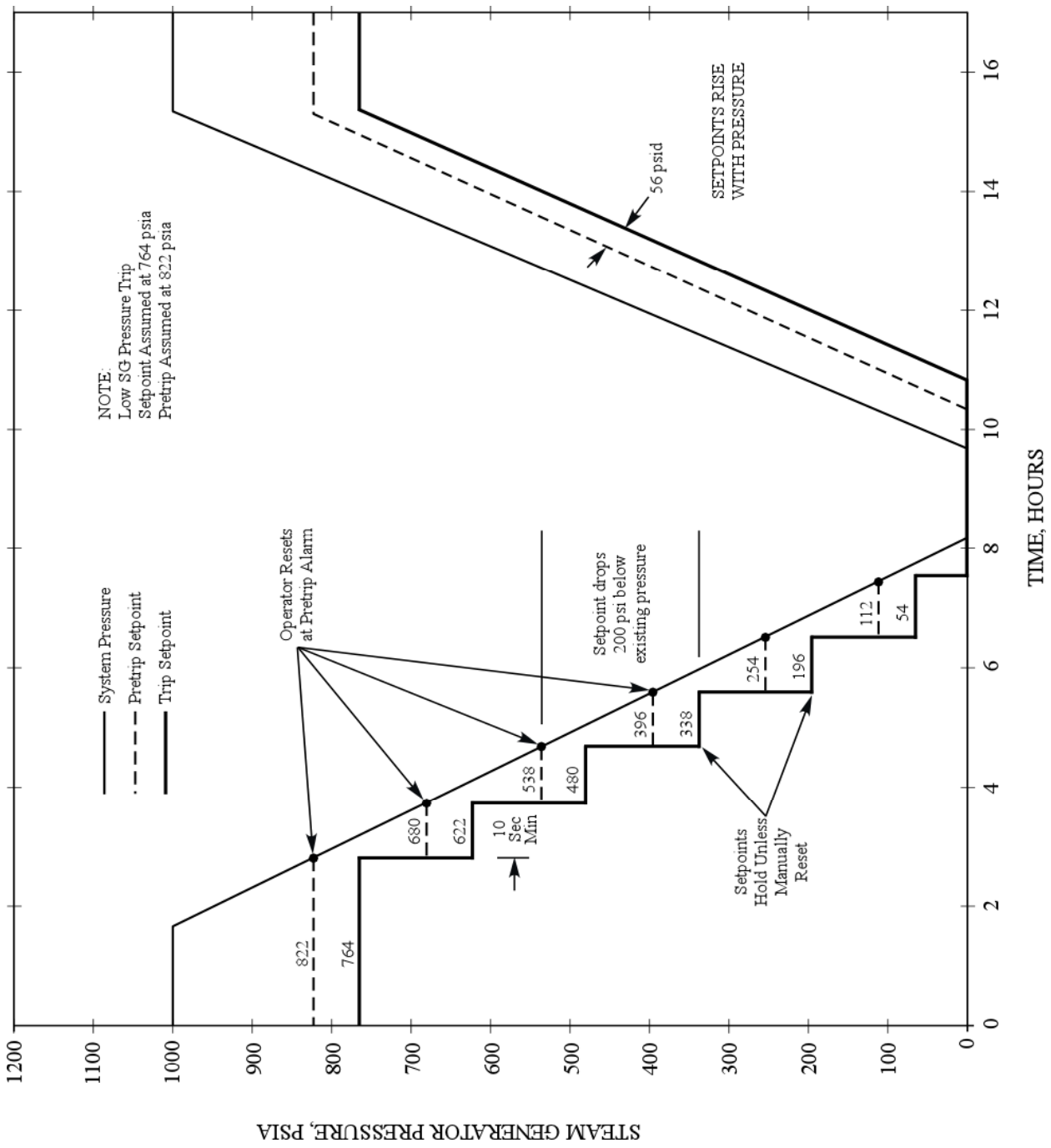
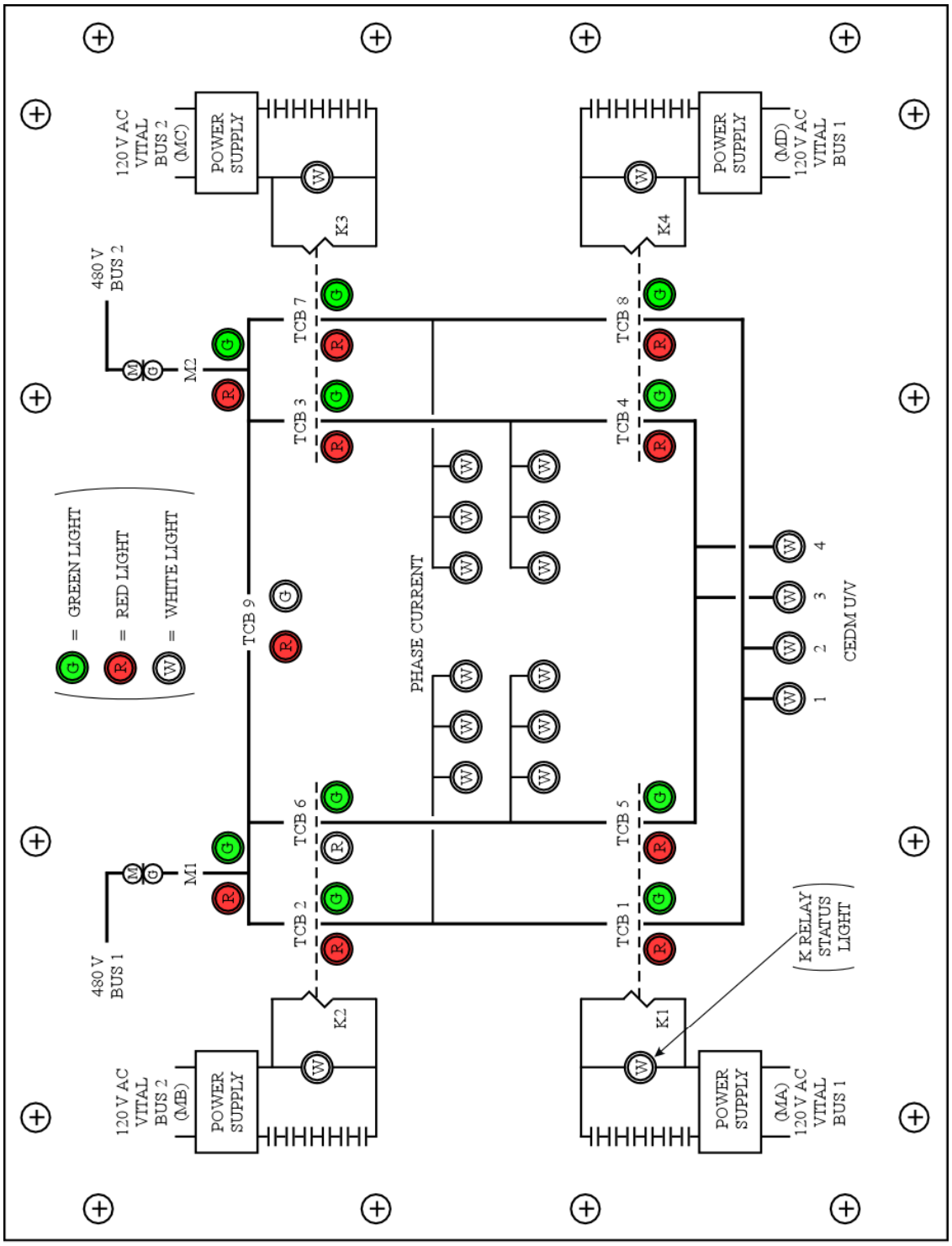


Figure 12.4-5 Low Steam Generator Pressure Variable Setpoint Operation



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

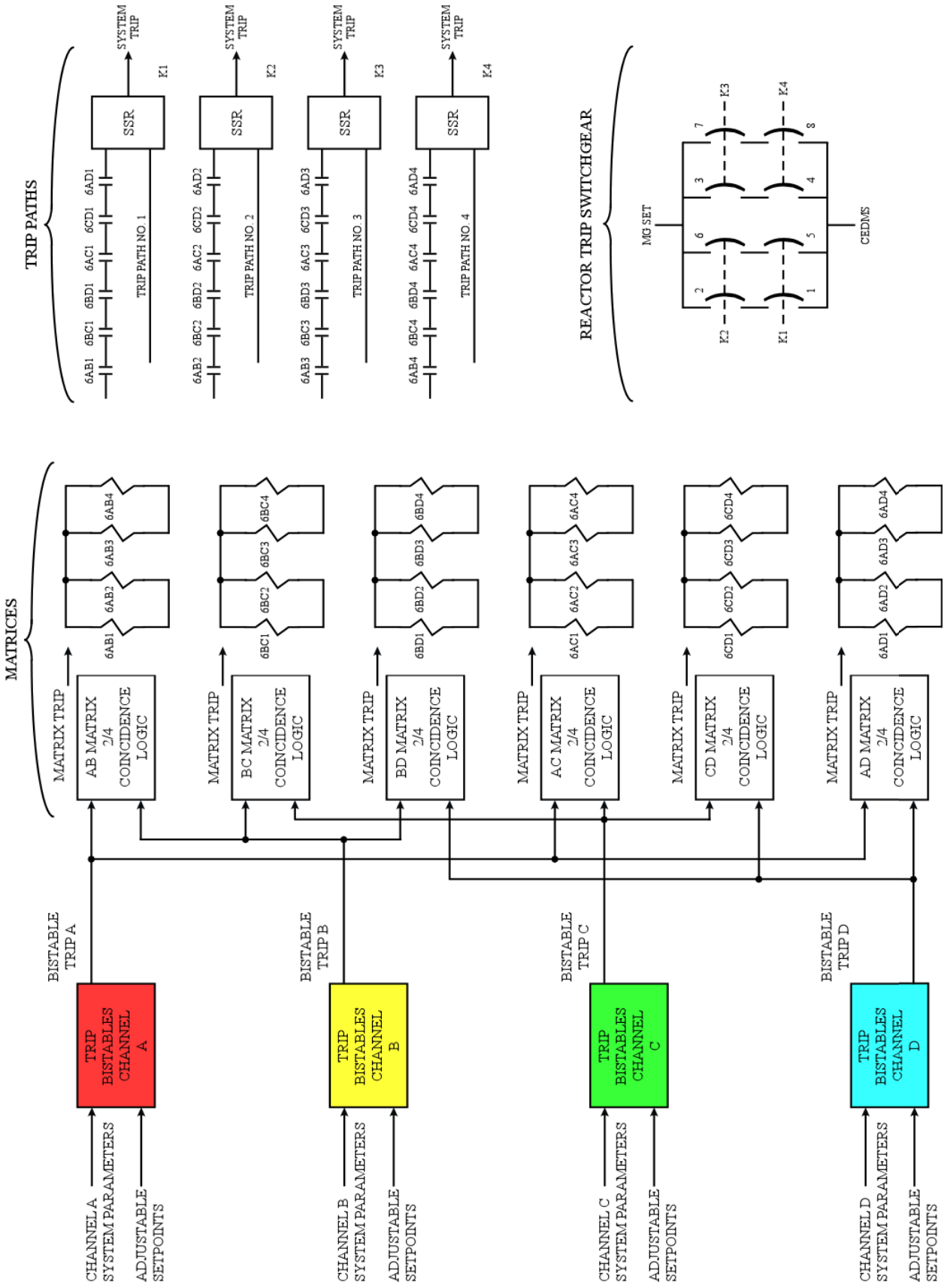


Figure 12.4-7 RPS Trip Signal Flowpath

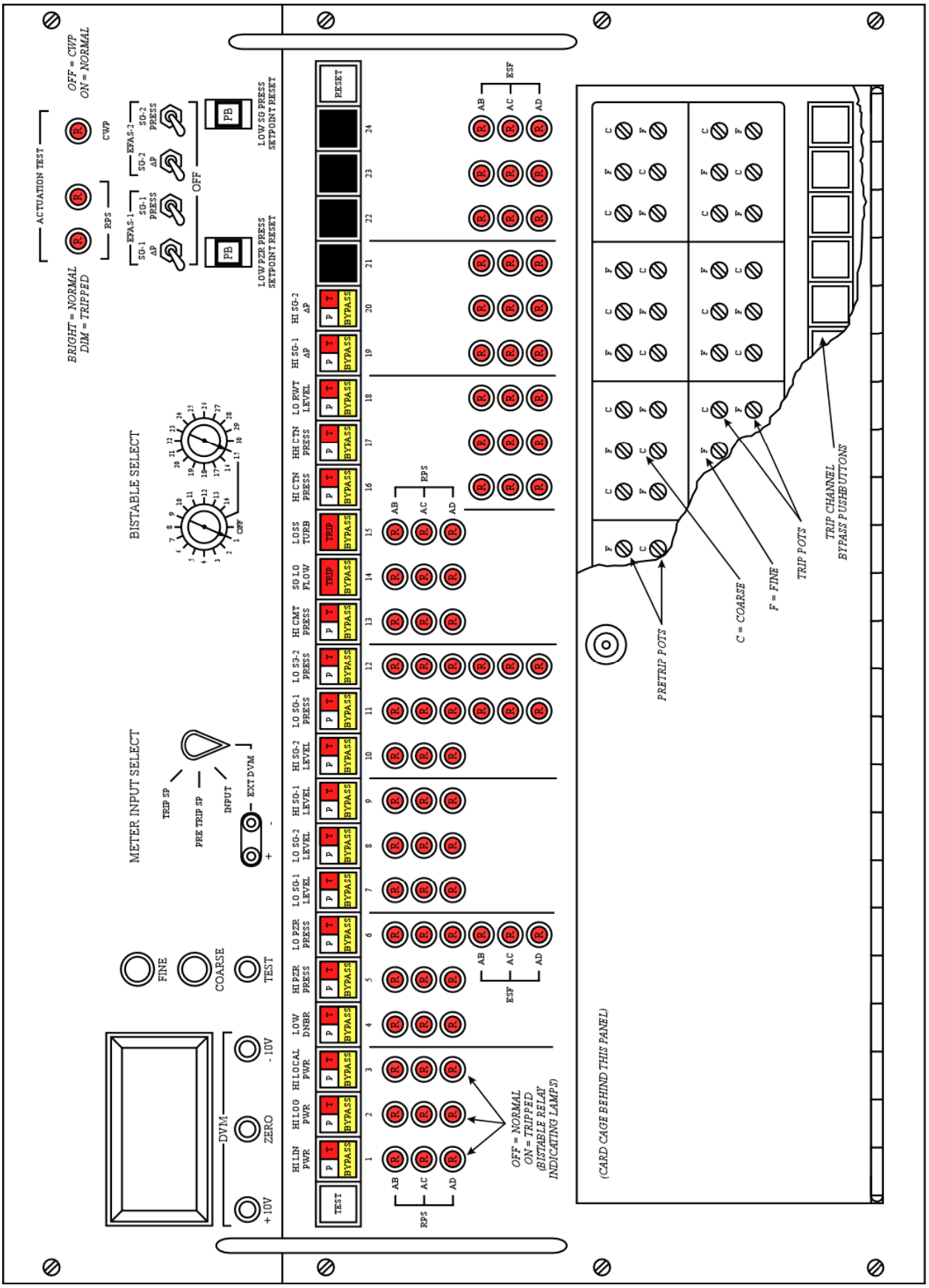


Figure 12.4-8 Bistable Control Panel Channel A

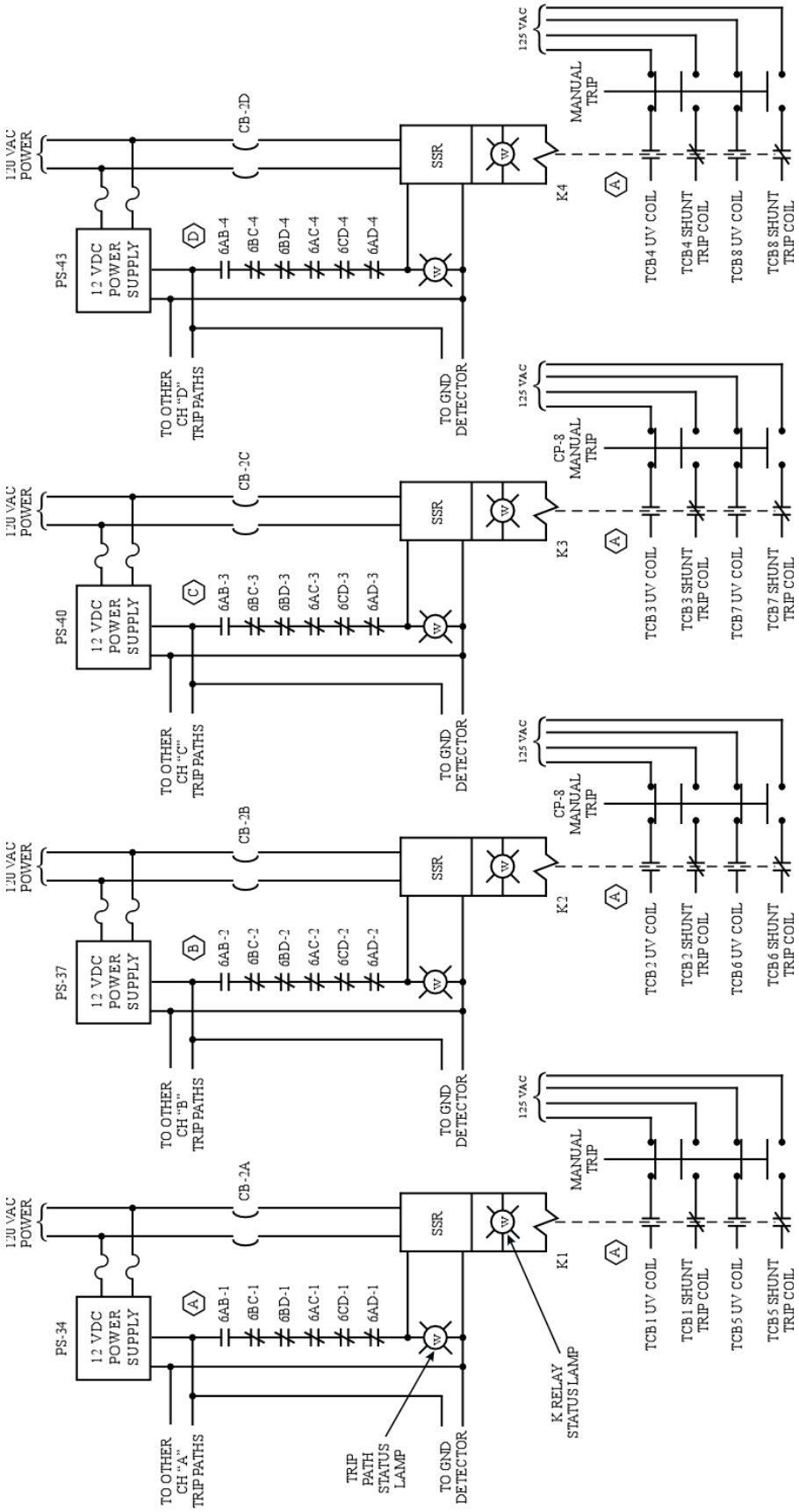


Figure 12.4-9 RPS Trip Path Status With Trip on the AB Matrix

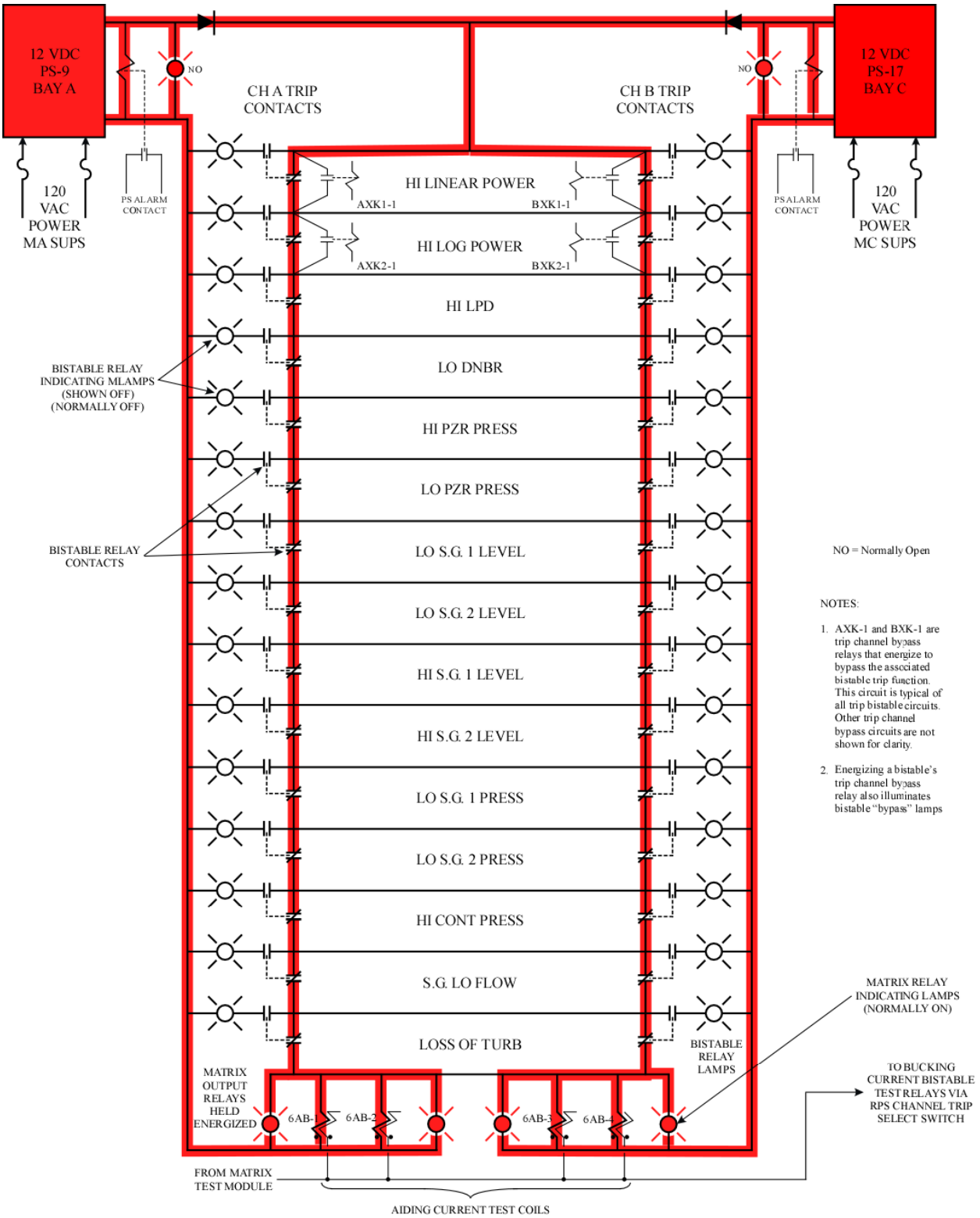


Figure 12.4-10 RPS AB Logic Matrix – Normal (untripped)

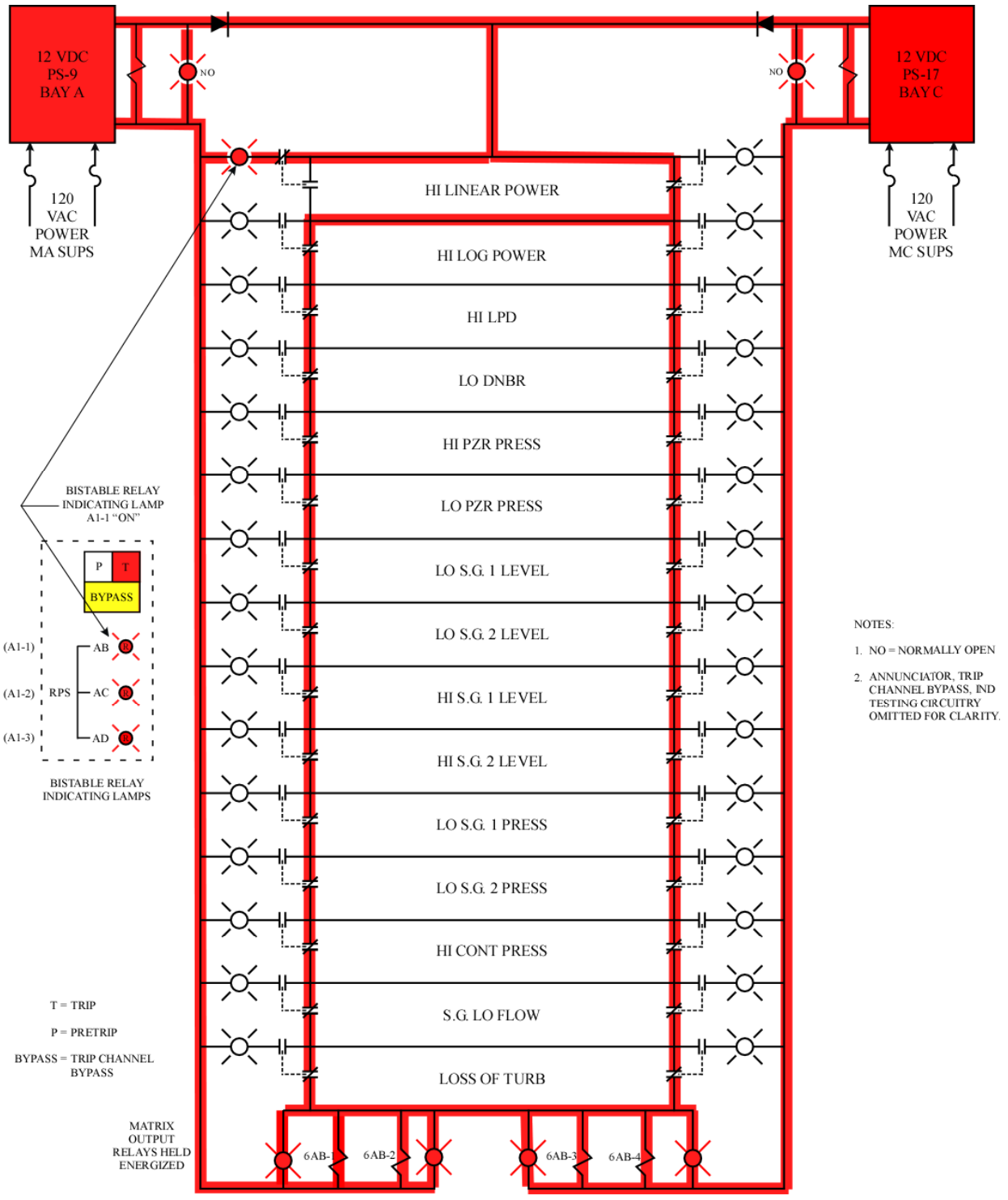


Figure 12.4-11 RPS Logic Matrix With High Linear Power Channel A Tripped

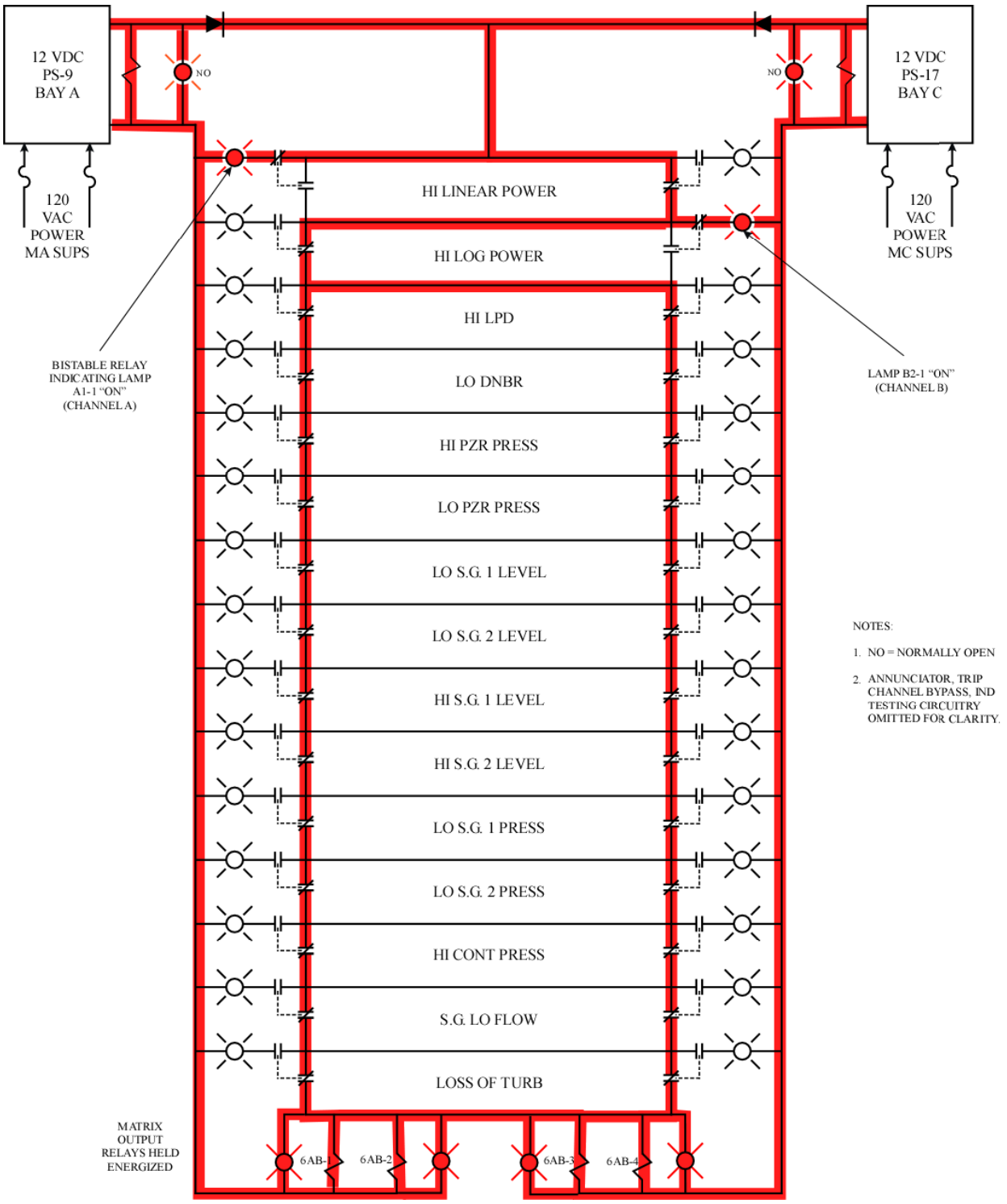


Figure 12.4-12 RPS Logic Matrix With Linear Power Channel A and High Log Power Channel B Tripped.

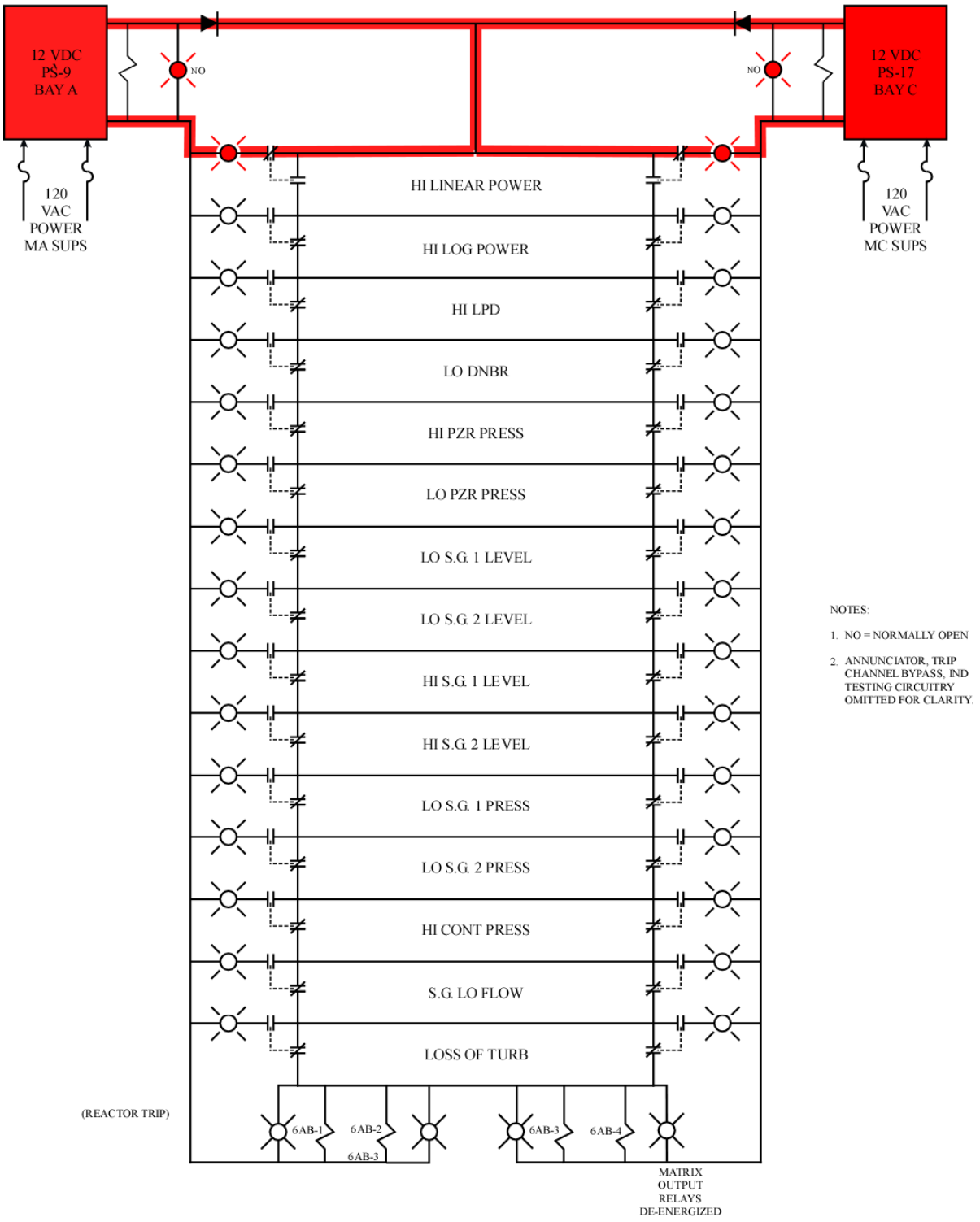


Figure 12.4-13 RPS AB Logic Matrix With High Linear Power Channel A and Channel B Tripped

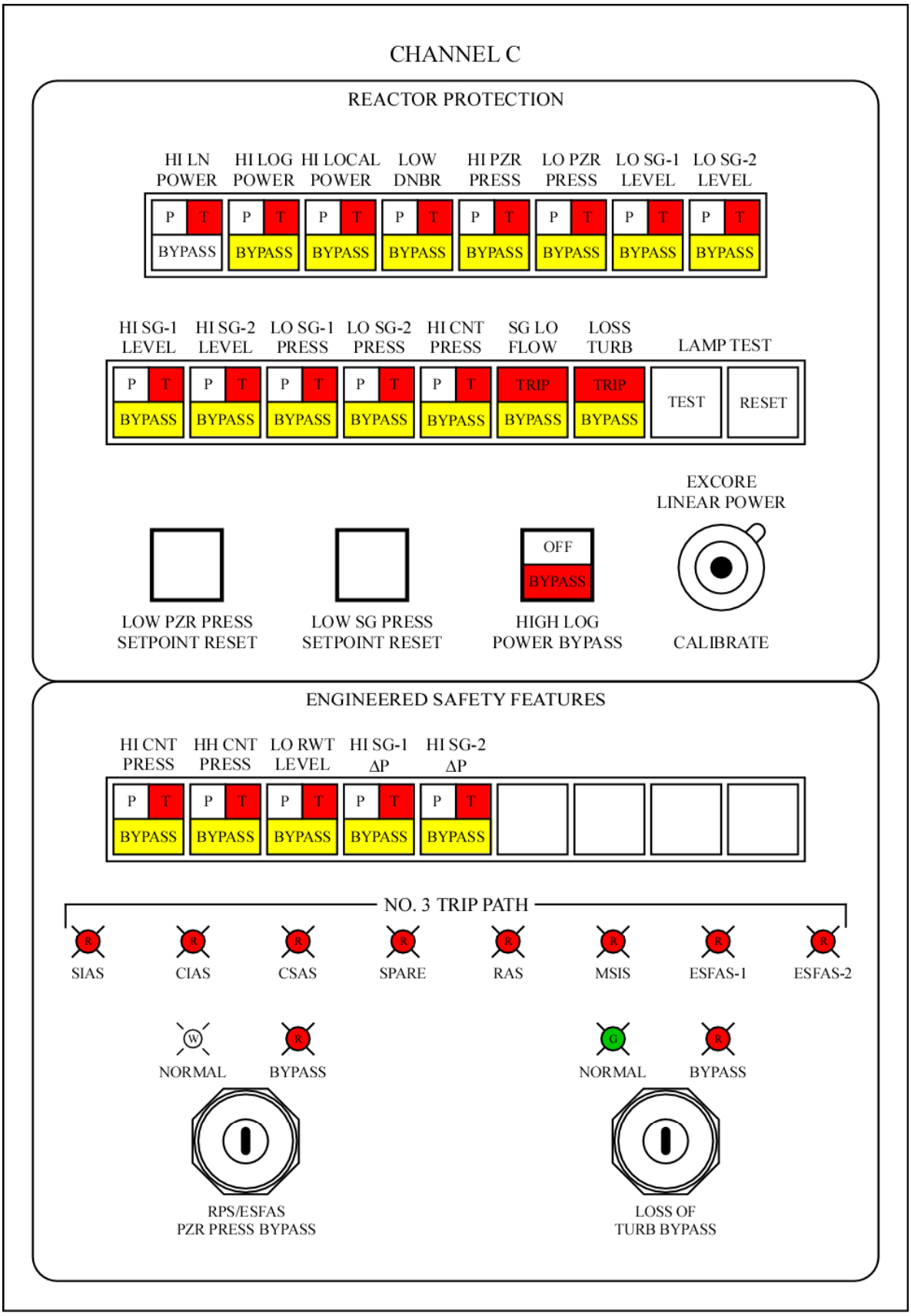


Figure 12.4-14 PPS Remote Operator's Module

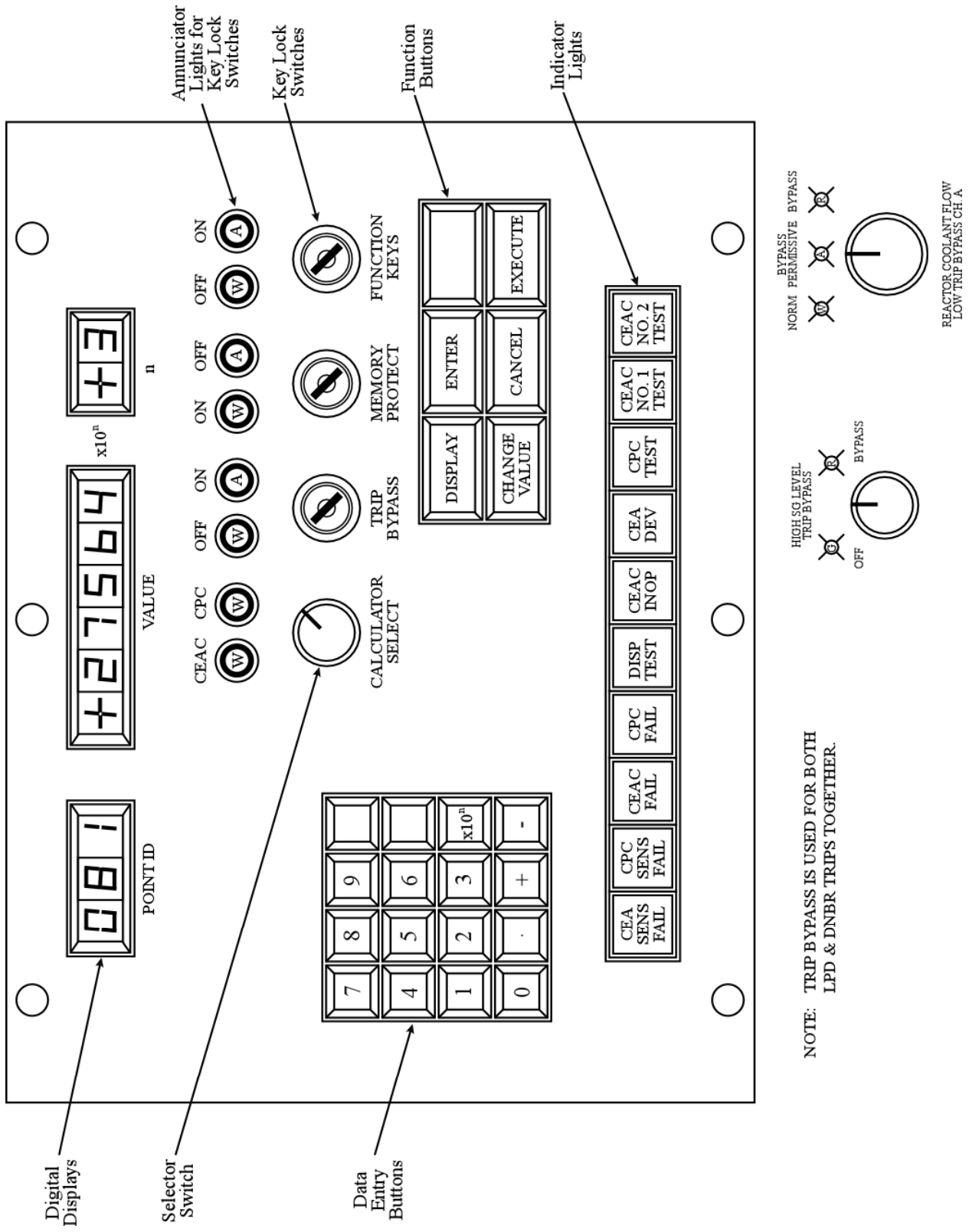


Figure 12.4-15 CPC Remote Operator's Module

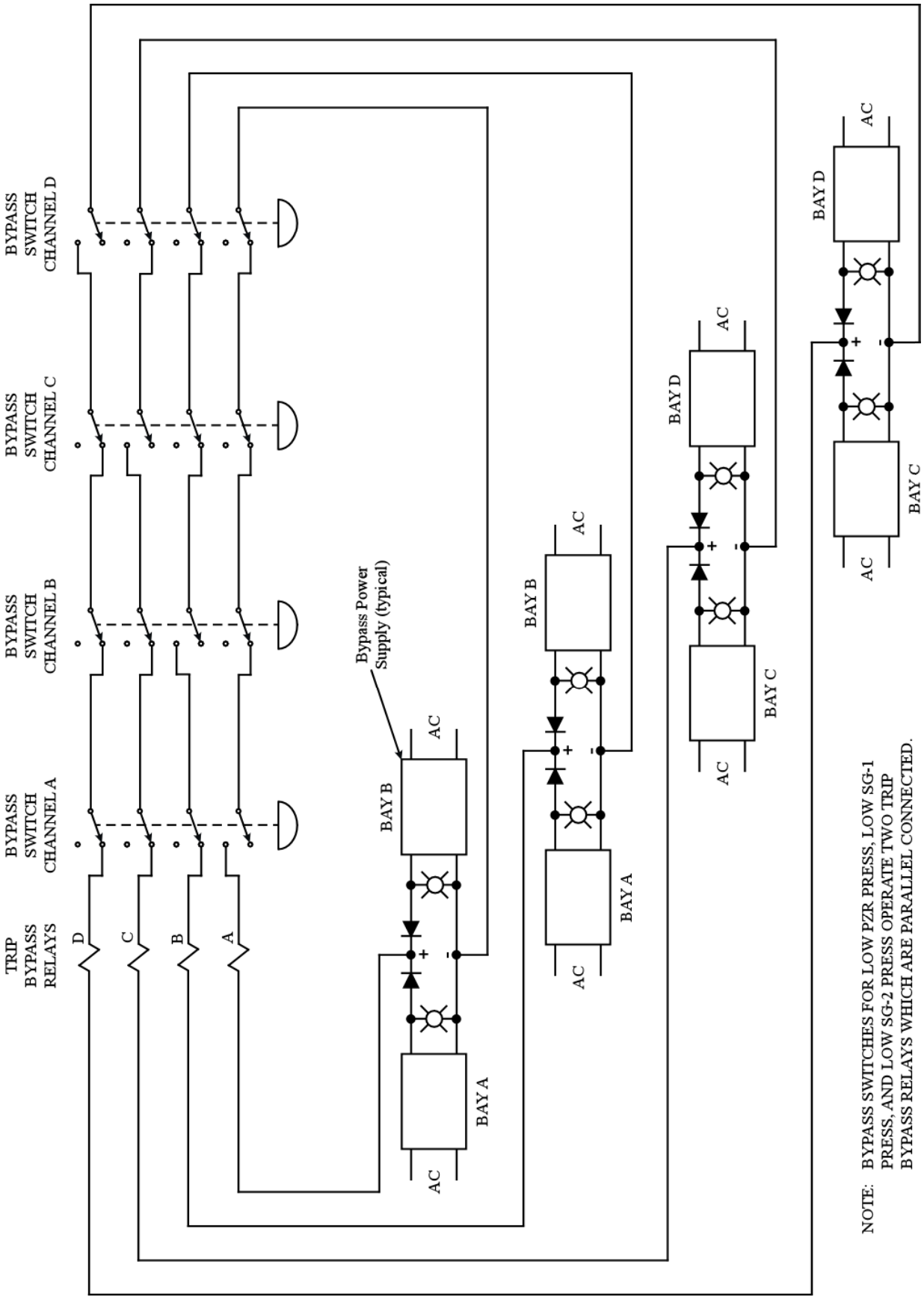


Figure 12.4-16 Trip Channel Bypass Electrical Interlock

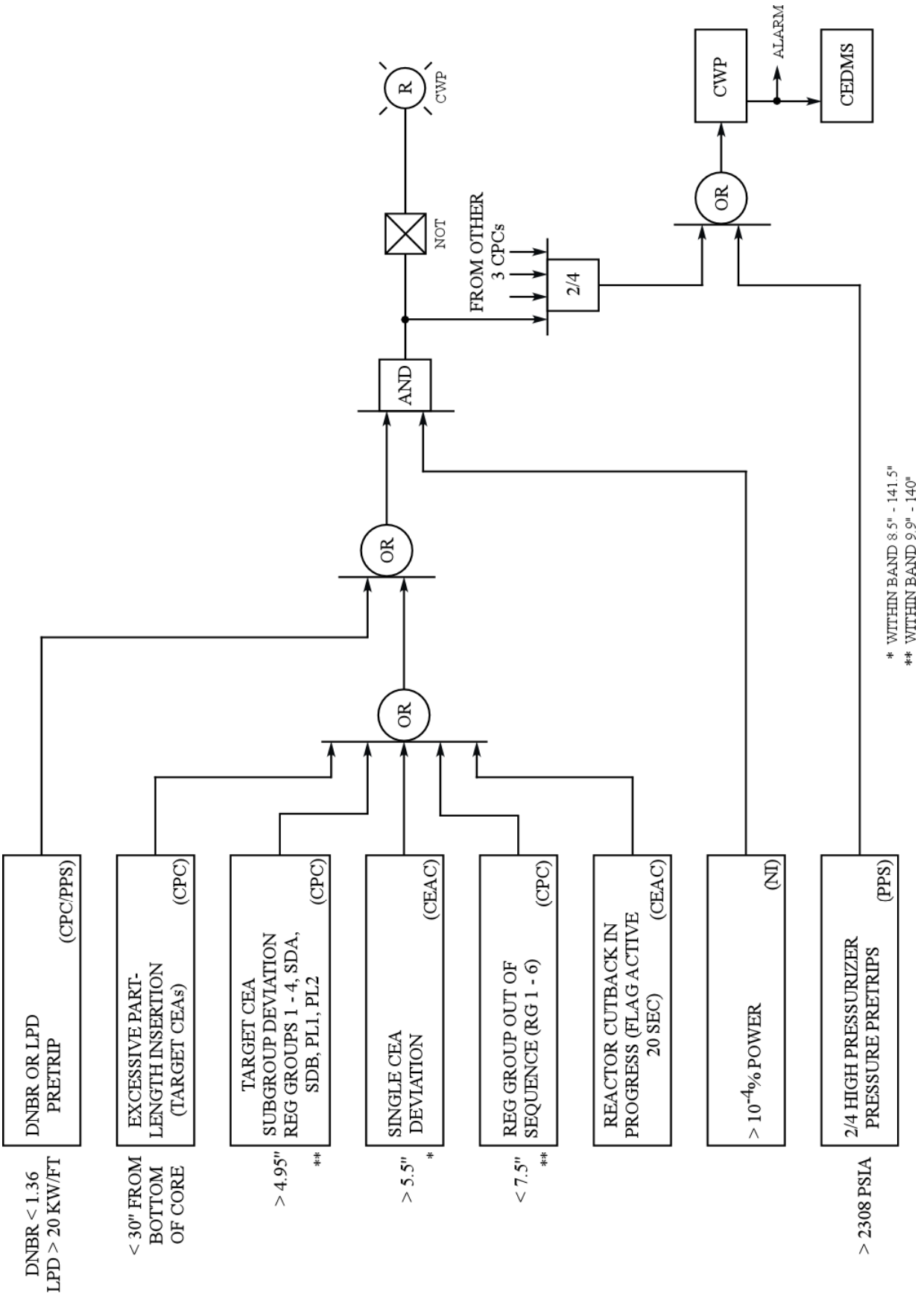


Figure 12.4-17 CEA Withdrawal Prohibit Logic Diagram

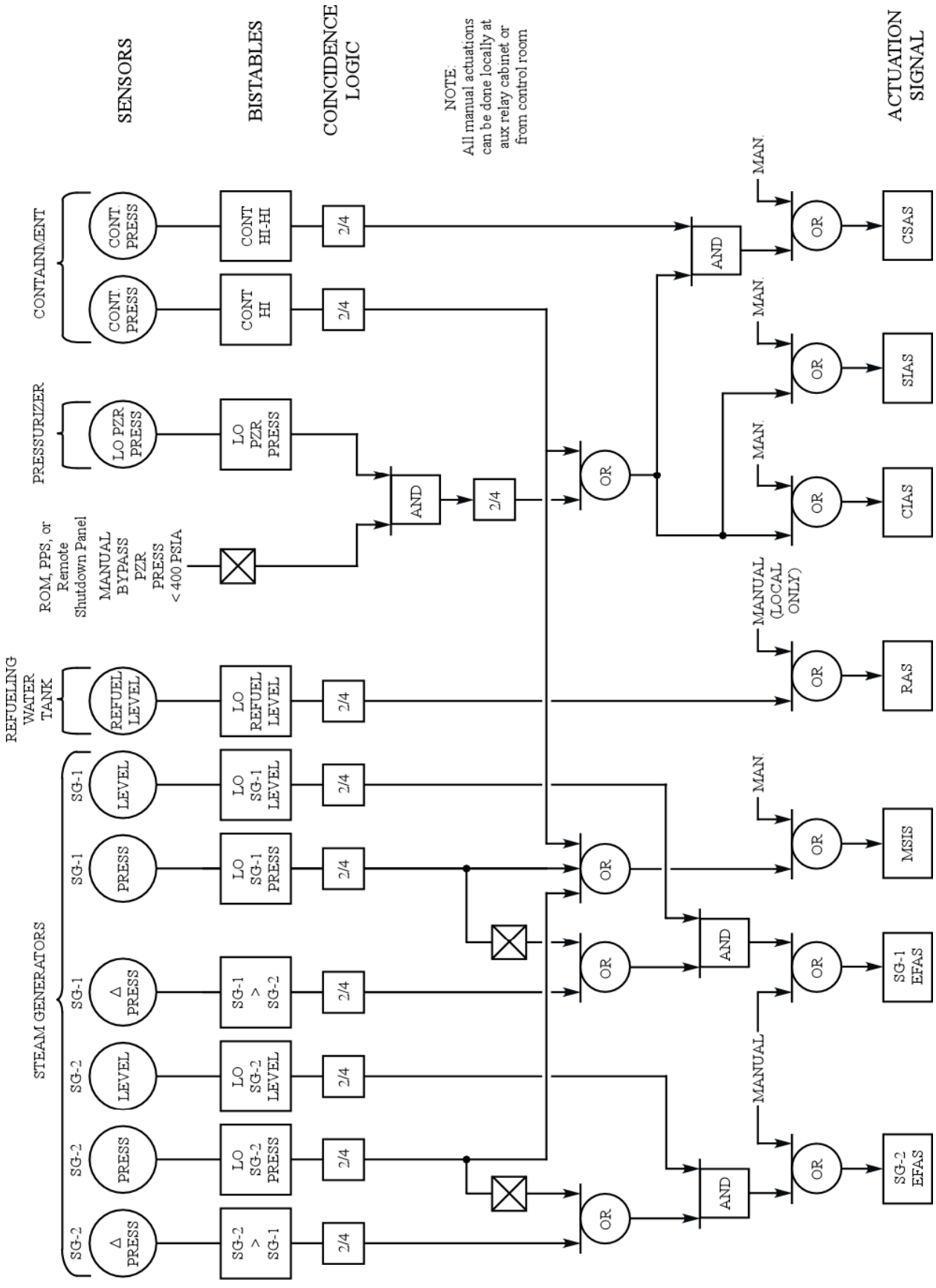


Figure 12.4-18 ESFAS Logic Diagram

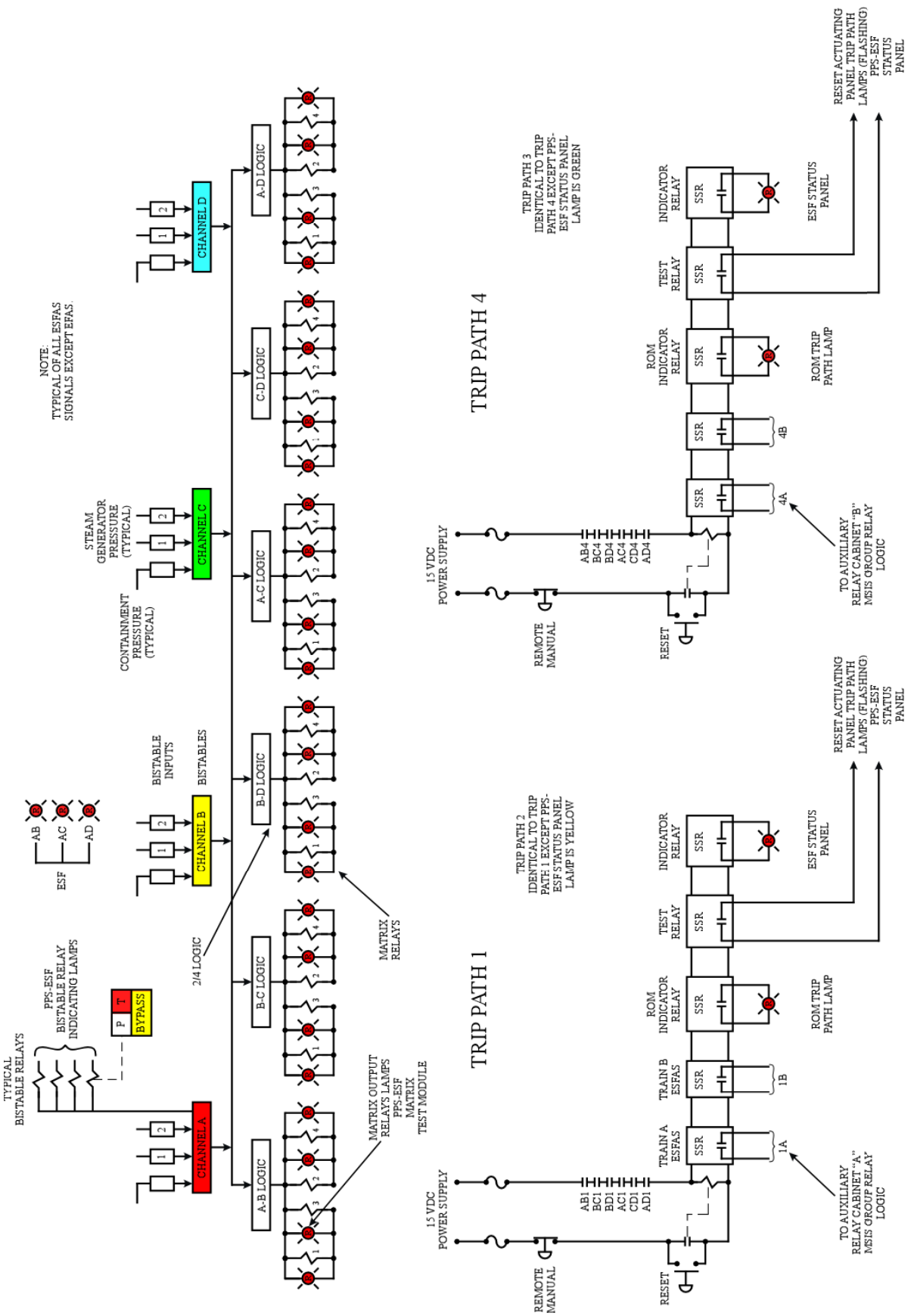


Figure 12.4-19 ESFAS Functional Diagram

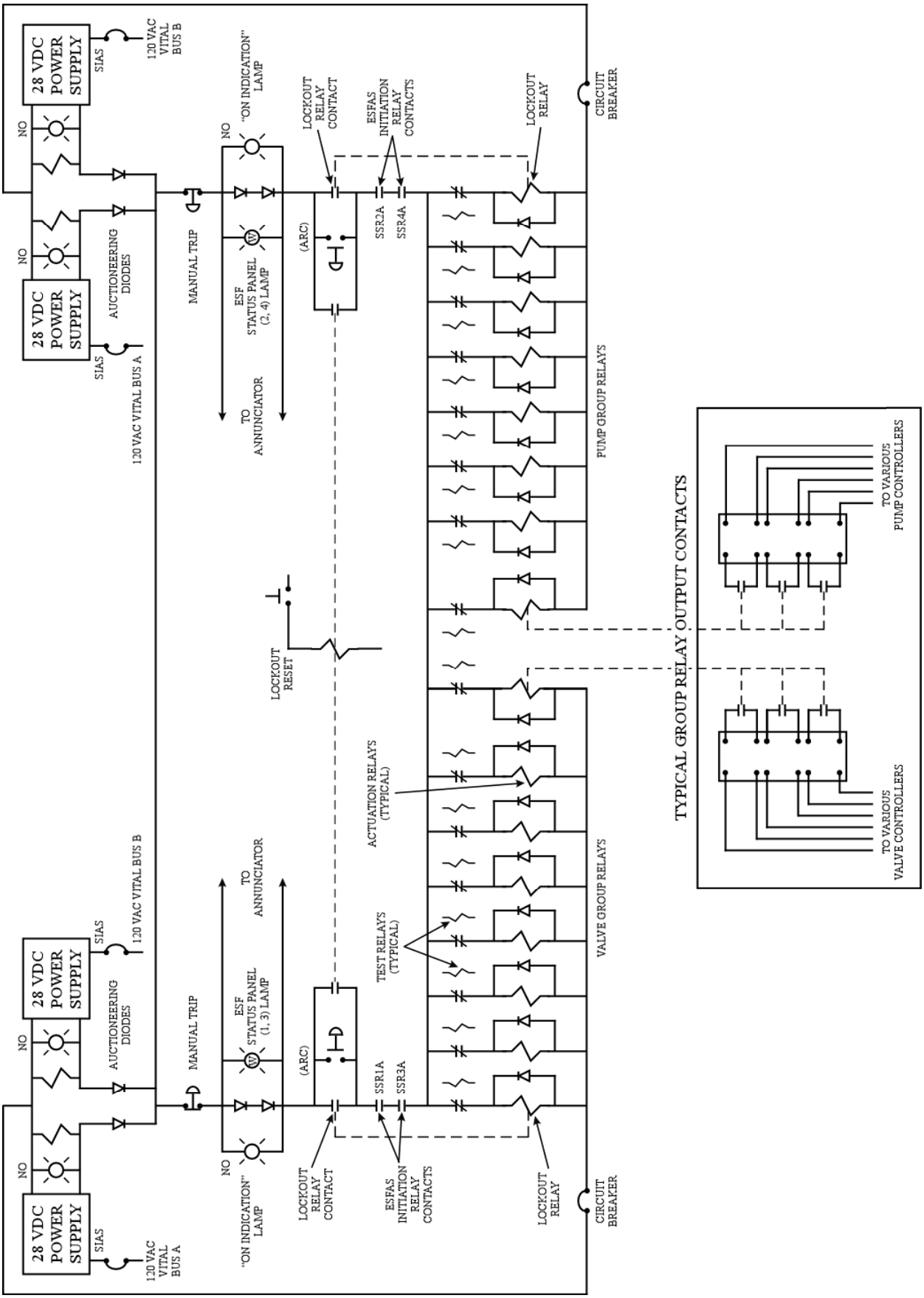


Figure 12.4-20 ESFAS Actuation Relay Cabinet Schematic – SIAS Circuit