2407

Rec'd w/ Ltr 3/3/75

50 - 255

PALISADES PLANT

REACTOR PROTECTION SYSTEM

COMMON MODE FAILURE ANALYSIS

Consumers Power Company

Docket 50 - 255

License DPR - 20

March 1975

PALISADES PLANT
REACTOR PROTECTION SYSTEM
COMMON MODE FAILURE ANALYSIS

CONSUMERS POWER COMPANY
DOCKET 50-255
LICENSE DPR-20

March 1975

TABLE OF CONTENTS

TABLE OF CONTENTS (cont'd)

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES (cont'd)

1.0 INTRODUCTION

In September 1973, the Regulatory Staff of the United States Atomic Energy Commission issued WASH-1270, Technical Report on Anticipated Transients Without Scram for Water-Cooled Power Reactors (Reference 1). Appendix A of WASH-1270 set forth the licensing position on anticipated transients without scram (ATWS) for licensees and for construction or operating permit applicants. Three licensing positions were delineated, with the applicable position for a given plant identified in Appendix B of WASH-1270.

The Palisades Plant is in Class I.C. of the above referenced licensing position statement. Specifically, for the Palisades Plant, the applicable licensing position is:

> "The need for backfitting of plant changes to mitigate the consequences of ATWS in plants for which neither the AEC construction permit-stage Safety Evaluation Report nor the Advisory Committee on Reactor Safeguards Report identify ATWS as a continuing area of review should be considered on an individual case basis."

The corresponding implementation statement presented in Section II.C of WASH-1270 is:

"1. Analysis of ATWS Consequences.

An analysis should be made of the consequences of anticipated plant transients in the event of a postulated failure to scram. The analysis should show whether

a. calculated reactor coolant system transient pressure exceeds a value such that the maximum primary stress in the system boundary is equal to that of the "emergency conditions" as defined in the ASME Nuclear Power Plant Components Code, Section III, or

b. effects of the ATWS event result in significant fuel cladding degradation or significant fuel melting, or

c. calculated containment pressure exceeds the design pressure of the containment structure.

2. Review of Reactor Shutdown System Design.

A review of the reactor shutdown system design should be made with the aim of identifying areas that it might be particularly vulnerable to common mode failures."

This report presents the results of the reactor shutdown system review for the Palisades Plant as required by Section II.C.2 of the above implementation program.

2.0 SUMMARY AND CONCLUSIONS

The Reactor Protection System (RPS) provides for automatic reactor shutdown whenever plant conditions exceed allowable operating limits. In response to Section II.C.2 of WASH-1270 (Reference 1), the Palisades Plant RPS design has been reviewed in detail to determine the system vulnerability to both single and common mode failures. Analyses were performed to determine if hypothesized single and common mode failures could inhibit any of the automatic or the manual reactor trip functions. An integrated RPS Failure Mode and Effects Analysis (FMEA) was generated to establish a baseline for evaluating the system vulnerability to both single and common mode failure. The FMEA was generated at the system level on a functional basis (i.e., signal flow level). This approach evaluates the effects of failures observable at the interfaces between RPS modules (inputs/outputs) and the effect propagated on the total system operation.

The FMEA demonstrated that no single RPS equipment failure could inhibit the actuation of any required protective reactor trip (RT) function. The two RPS anticipatory RT functions, high power rate-of-change, and loss of load-turbine trip, are both vulnerable to single failures which would inhibit the automatic RT actuation.

The high power rate-of-change RT is a precursor to the protective high power level RT function. When only one of the high power rate-of-change RPS channels is in the bypass mode, at least four individual RPS equipment failures would be required to inhibit both the anticipatory and the primary trip functions. If none of the associated RPS channels are in bypass, at least five individual failures would be required to inhibit both trips.

The loss of load, turbine trip RT is a precursor to the protective high pressurizer pressure RT function. At least four individual RPS equipment failures would be required to inhibit both the anticipatory and the primary trip functions.

The Common Mode Failure Analysis (CMFA) was developed for both individual RT modes and for the integrated RPS which incorporated all the RT modes available at the Palisades Plant. Each transient was evaluated separately, considering the trip functions which would initiate reactor trip and the trip system defenses against common mode failures of those trip functions.

Figure 2.1 presents a summary of the ATWS transients considered, their consequences, and the reactor trips which would be expected to interrupt each transient. The consequence analysis for each transient is documented in Reference 2. Because of the conservatisms incorporated into the design of the Palisades Plant, only three of the transients considered would result in a design limit being exceeded if no reactor trip occurred. These are the loss of electrical load, the loss of feedwater, and the loss of normal electrical power. The consequences of these three are such that there would be no release of fission products from the fuel, the primary system pressure would remain less than the hydrostatic test pressure limit, and the containment pressure would remain within its design limit even without reactor trip. Figure 2.1 also shows that a minimum of two trips would be actuated to terminate each transient. The single failure analysis and common mode failure analyses for these transients show that the reactor trip system incorporates recognized defenses against failures which would inhibit a trip. These defenses include functional diversity, equipment diversity, safe failure modes, and periodic inservice testing. It is concluded that there is a high degree of assurance that the system will fulfill its function and interrupt these transients, should they occur.

Of the remaining seven transients which were analyzed, none resulted in a design limit being exceeded. Nevertheless, the ATWS analysis shows that three of these - load increase, complete loss of primary flow, and rod withdrawal at full power - would be interrupted by two or more trip functions. The same defenses against common mode failures in the reactor trip system exist, providing a high degree of assurance that these transients will be interrupted by a reactor trip.

ANTICIPATED TRANSIENT EVENTS	Transient Severity Without Scram			Automatic Reactor Trip Modes Available at the Palisades Plant										
	Fuel Thermal and Hydraulic Condition	Primary Pressure	Containment Pressure	High Power Level RT#1	High Power Rate-of-Change RT#2	Low Flow Reactor Coolant RT#3	Low Water Level SG#1 RT#4	Low Water Level SG#2 RT#5	Low Press., SG#1 RT#6	Low Press., SG#2 RT#7	High Pressurizer Press RT#8	Thermal Margin/ Low Press RT#9	Turbine Trip RT#10	High Containment Press. RT#11
1 Loss of electrical load	D	T	D								E		E	I
2 Load increase	D	D	D	E			L	L	L	L		I	L (7)	
3 Complete loss of feedwater	D	T	D				E	E	I	I	I	I	L (7)	I
4 Complete loss of primary flow	D	D	D			E	L	L	L	L	E	L	L (7)	
5 Loss of normal electrical power	N	T	D			E	E	E			E	L	E	L
6 Inactive primary loop start-up	D	D	D	E										
7 Rod withdrawal at full power	D	D	D	I			L	L	L	L	I	L	L (7)	
8 Primary system depressurization	D	D	D			L	L	L	L	L		I	L (7)	
9 Boron dilution	D	D	D	I			L	L	L	L		L	L (7)	
10 Small line break	D	D	D			L	L	L	L	L		I	L (7)	

NOTES:

1. D designates parameter within design limits during transient.
2. N designates DNBR less than 1.3 during transient. No clad perforation.
3. T designates pressure did not exceed hydrostatic test pressure during transient.
4. E designates trip signal generated early in the transient (within first minute).
5. I designates trip signal generated after 1 minute but before 10 minutes into the transient.
6. L designates trip signal generated late in the transient (after 10 minutes).
7. Low steam generator pressure closes main steam isolation valves and causes turbine trip.

FIGURE 2.1

SUMMARY OF ATWS CONSEQUENCES AND SCRAM FUNCTIONS AVAILABLE TO INTERRUPT THE TRANSIENT

Four transients - inactive primary loop startup, primary system depressurization, boron dilution, and small line break - would result in actuation of only one trip function during the transient and prior to operator action assumed in the ATWS analyses. No reactor design limits are exceeded during any of the transients noted above. Since the effects propagated by each of these transients are so mild, only a single plant operating parameter traverses outside the normal operating envelope and initiates a scram signal. Since only one trip mode is responsive to each of these mild transients, no functional diversity or equipment diversity can exist to provide protection against common mode failures.

Functional and equipment diversity is the primary defense against CMF's caused by design and manufacturing errors. No credit can be taken for equipment diversity in the RPS trip trains. The trip train is defined as all equipment between the output relays in either auxiliary trip units or bistable trip units and the reactor trip relays which remove the AC input power to the rod clutch power supplies. All components that perform an identical function in the trip train (e.g., trip unit output relays, logic matrix trip relays, M coils, ...) have similar design and/or performance specifications. Protection against CMF's due to design or manufacturing deficiencies of the above components is achieved by periodic testing which ensures that all the equipment is operational and would be responsive to valid scram signals.

In consideration of each ATWS transient and its consequences, and the existing defenses against common mode failures, it is concluded that the Palisades Plant RPS incorporates adequate defenses against common mode failures.

3.0 REACTOR PROTECTION SYSTEM DEFINITION

The reactor protection system of the Palisades Plant consists of all the sensor instrumentation, amplifiers, trip units, logic circuits, actuation circuits and other equipment as required to monitor selected nuclear steam suppy system conditions, and is designed to reliably effect a rapid reactor shutdown in the event of an off-normal state of operation. The system functions to protect the reactor core. This rapid shutdown is called a reactor scram.

The reactor is protected against the following conditions which automatically effect a rapid reactor shutdown (see Figure 3.1):

1. High Reactor Power Level
2. High Rate-of-Change of Reactor Power
3. Low Reactor Coolant Flow
4. Low Steam Generator Water Level
5. Low Steam Generator Steam Pressure
6. High Reactor Coolant Pressure
7. Reactor Thermal Margin/Low Reactor Coolant Pressure
8. Loss of Turbine Load
9. High Containment Pressure

In addition, a manual actuation system is provided to allow the operator to scram the reactor.

The high power rate-of-change and the loss of turbine load scram functions are not required as primary reactor protective functions, as defined in the Palisades Plant Technical Specification (Reference 3). The high power rate-of-change RT is provided to protect the reactor against an uncontrolled control rod withdrawal while the core is at very low power levels. This is an anticipatory trip which is not required to protect the reactor since the principal reactor protection function is provided by the high power level trip (Reference 4). The loss of turbine load reactor trip is also an anticipatory trip which is not required to protect the reactor since the primary trip is high primary system pressure (Reference 5).

In general, the reactor protection system consists of four independent protective channels. Each primary safety parameter is monitored by four independent measurement channels. Each of these measurement channels provides a trip signal to a protective channel when the primary safety parameter exceeds allowable limits. A trip signal from any two-out-of-four protective channels causes a reactor scram, except for high rate-of-change of reactor power which requires a one-out-of-two measurement channel trip signal to scram the reactor, and loss of turbine load which requires a one-out-of-one measurement channel trip signal to actuate two relays, each providing a two-out-of-four protective channel trip signal to scram the reactor.

3.1 Reactor Protection System - Overview

Reactor scram in the Palisades Plant functions generally in a two-out-of-four mode. Four independent measurement channels (A, B, C, D) each monitor high reactor power level, low coolant flow, high coolant pressure, thermal margin/low coolant pressure, low steam generator water level, low steam generator pressure and high containment pressure (see Figures 3.3, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11 and 3.13). Individual channel trips occur when the measurement reaches a preselected or an automatically calculated trip setpoint.

The individual channel trips are combined in multiple two-out-of-four logic, meaning all combinations of two-out-of-four channel trips due to the same safety parameter, such as high reactor power level, can initiate a reactor scram. Each two-out-of-four coincidence logic combination provides trip signals to one-out-of-six coincidence logic matrix units (AB, AC, AD, BC, BD, CD), each of which trips and opens the contactors in the AC supply to the control rod drive clutch power supplies (see Figure 3.2). This de-energizes the magnetic clutch holding coils and releases the control rods to drop into the core causing a reactor scram.

3.2 Definition of System Boundary

The Reactor Protection System is housed in four cabinets in the control room. The cabinets consist of the following parts (see Figure 3.14):

- Bistable trip units
- Auxiliary trip units
- Coincidence logic matrices
- Clutch power trip circuits
- Clutch power supplies
- Sensor power supplies
- Reactor protection testing system

There are four measurement channels with remote sensors which are completely independent and isolated from each other. Each of these protective channels monitors the following nuclear steam supply parameters (see Figures 3.3 through 3.13):

1. Reactor Power Level

2. Rate-of-Change of Reactor Power

3. Reactor Primary Coolant Flow

4. Water Level Steam Generator No. 1

5. Water Level Steam Generator No. 2

6. Steam Pressure Steam Generator No. 1

7. Steam Pressure Steam Generator No. 2

8. Pressurizer Pressure

9. Reactor Thermal Margin/Low Pressure

10. Loss of Turbine Load

11. Containment Pressure

The signal output from each measurement channel is fed to the input of either a bistable trip unit or an auxiliary trip unit in the corresponding channel cabinet of the Reactor Protection System (see Figure 3.2).

The sensors for high rate-of-change of power and loss of turbine load are respectively arranged in a one-out-of-two and a one-out-of-one configuration. The bistable trip units, fed from any one nuclear steam supply system parameter, have their output contacts arranged in six coincidence logic matrices, identified as AB, AC, AD, BC, BD and CD to represent all possible two-out-of-four combinations of trip signals (see Figure 3.2). Each coincidence logic

matrix, when tripped, trips four matrix relays, which in turn provide trip signals to each of two trip circuits that interrupt the AC power to the clutch power supplies, thereby de-energizing the magnetic clutches that hold the control rods and causing a reactor scram.

The control rod mechanism clutches are separated into two groups (see Figure 3.2). The clutches in each group are supplied in parallel with low voltage DC power by an ungrounded feed line. Two AC to DC converters supply each feed line to prevent release of the clutches and control rods in the event one converter fails. The converters on each side are each supplied by a preferred (vital) AC bus to assure a continued source of power. Each feed line has two interrupters in series which are each actuated by a trip signal from any one-out-of-six coincidence logic matrix output relays. Although both vital feeds must be de-energized to release the clutches, there are two separate means of interrupting each feed. This arrangement allows the testing of the protective system.

Provisions are made to bypass any one of the four protective channels, associated with a RT mode, with a key-operated switch and change the logic for that particular RT mode to a two-out-of-three logic while maintaining the other protective RT modes in a two-out-of-four logic. If the bypass is not effected, an out-of-service channel assumes a tripped condition, which results in a one-out-of-three RT mode logic.

Provisions are also made to permit periodic testing of the complete reactor protection system, while the reactor is at operating power levels or when shut down. These tests cover the trip actions from sensor input to the protective system to the output to the clutch power supplies. The system test does not inhibit the protective function of the system.

The testing system is completely isolated from the protective system circuitry itself (see Figure 3.2). Failure of any part of the testing system does not prevent proper operation of the reactor protection system.

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

During reactor operation, the measuring channels are checked by comparing the outputs of similar channels and cross-checking with related measurements. The trip units are tested by inserting a voltmeter in the circuit, noting the signal level, and initiating a test input which is also indicated on the voltmeter. This provides the necessary overlap in the testing process and also enables the test to establish that the trip can be effected within the required tolerances. The test signal is provided by an external test signal generator which is connected to the trip unit at the signal input terminals. With the test signal generator connected, the desired signal is selected and then inserted into the trip unit by depressing the manual test switch. The test circuit permits various rates-of-change of signal input to be used. Trip action (opening) of each of the trip unit relays is indicated by individual lights on the front of the trip unit. The pretrip alarm action is indicated by a separate light.

The sets of trip relays at the output of each coincidence logic matrix are tested one at a time. The test circuits in the logic permit only one pair of coincidence matrix logic relays to be tripped while one set of matrix output relays can be held at the same time. The application of hold power to one set of matrix output relays denies the power source to the other sets. In testing a logic trip set, e.g., AB, a holding current is initiated in the test coils of the logic trip relays by turning the matrix relay trip test switch to "off" and depressing

the matrix logic AB test pushbutton switch. Operation of the matrix trip test switch de-energizes a parallel pair of module trip relays. With the ladder-logic relay contacts open, the logic trip relays may be de-energized one at a time (by rotating the matrix relay trip test switch) to initiate a half-trip. Indicator lights on the trip relay coils and on the DC power supply AC feed lines provide verification that coil operation and half-trip conditions have occurred.

The capability to test relays K1 through K4 associated with the reactor protection system "trip/reset" function, has been provided. The zero power mode bypass relays and their contacts can be tested with the reactor at power (see Figure 3.15). These relays can be tested as part of the normal reactor protection system tests by varying the intermediate range channel output above and below 10^{-4}% power.

A manual reactor trip is provided to permit the operators to scram the reactor (see Figure 3.2). Manual actuation of either of two independent reactor scram pushbutton switches in the main control room causes direct interruption of the AC power to the power converter units supplying DC power to the electromagnetic clutches of the drive mechanisms. One manual trip pushbutton interrupts the control power to the holding coils of four M coil relays, whose contacts break AC power to the clutch power supplies. The second pushbutton interrupts power to the undervoltage coils of two circuit breakers which disconnect all AC power to the clutch power supplies.

The boundary of the Reactor Protection System being analyzed includes the sensors, the bistable and auxiliary trip units, the coincidence logic, matrices, the clutch power trip circuits, the clutch power supplies, the reactor protection testing system, and all interconnecting wires, cables, piping and their associated conduits, trays and channels.

3.3 Definition of Reactor Protection System Trip Modes

Rapid reactor trip or scram is effected on the following conditions:

3.3.1 High Power Level - Reactor Trip

See Figures 3.1, 3.2, 3.3 and 3.14. A reactor trip at high power level (neutron flux) is provided to shut down the reactor when the indicated reactor power exceeds a preselected value. The high power trip signals are initiated by two-out-of-four coincidence logic from the four power range safety channels. During normal plant operation with all coolant pumps operating, reactor trips are initiated when the reactor power level exceeds a nominal value of 106.5% of indicated full power. This trip level represents a reactor power of no greater than 112% of full power when instrument and calorimetric errors are taken into account. Provisions are provided to select different trip points for various combinations of primary coolant pump operation.

The power range channels are equipped with a range change switch to increase the indicated power by a factor of 10. By use of the range change switch, indicated power is increased to provide full-scale indication at 12.5% power. This action also decreases the overpower trip from 106.5% to 10.65% to provide overpower trip protection during low power operation.

3.3.2 High Power Rate-of-Change - Reactor Trip

See Figures 3.1, 3.2, 3.4, 3.14, 3.15 and 3.16. A reactor trip for high rate-of-change of reactor power is provided to protect the reactor against an uncontrolled control rod withdrawal while the core is at very low power levels.

Two wide-range channels take signals from fission chambers and cover a range greater than ten decades. The wide range signals are effected by using a combination of counting and mean square variation techniques which also provide good

rejection of background gamma signals to provide an operating range from startup to full power.

A reactor trip is initiated if the rate-of-change of reactor power exceeds 2.6 decades per minute, over a range of about 10^{-4}% to 15% power, by either of the two wide-range channels. The trip signal is automatically bypassed below 10^{-4}% and above 15% power. High rate-of-change of power alarms are initiated at 1.5 dpm over the operating range of 10^{-4}% to 15% power by the two wide-range channels.

This is an anticipatory trip which is not required to protect the reactor since the primary trip is high power level trip (Reference 4).

3.3.3 Low Flow, Reactor Coolant - Reactor Trip

See Figures 3.1, 3.2, 3.5, 3.14 and 3.16. A reactor trip is provided to protect the core from a power to flow mismatch. There are four reactor coolant pumps with flow in each measured by sensing differential pressure between the coolant pump suction line and the primary coolant input line to the associated steam generator. The flow measurement signals are provided by summing the output of the differential pressure transmitters to provide an indication of total coolant flow through the reactor. A reactor trip is initiated by two-out-of-four coincidence logic from either of the four independent measuring channels when the flow function falls below a preselected value.

Provisions are made in the reactor protective system to permit operation at reduced power if one or more coolant pumps are taken out of service. For this mode of operation, the low flow trip points and the overpower trip points are simultaneously changed, thus providing a positive means of assuring that the more restrictive settings are used. The flow trip selector switch is equipped with RPS channel physical separation and electrical isolation.

Pretrip alarms are initiated if the coolant flow function approaches the minimum required for reactor operation at the corresponding power level. The zero power mode bypass switch, a key-operated switch, allows the low reactor coolant flow trip to be bypassed for subcritical testing of control rod drive mechanisms. The zero power mode bypass switch also bypasses both the steam generator low steam pressure trips and the thermal margin/low pressure trip. The zero power mode bypass is automatically reset above 10^{-4}% power by signals from Nuclear Instrumentation (NI) wide range logarithmic Channels 3 and 4. NI Channel 3 resets the zero power mode bypass on RPS Channels A and C. NI Channel 4 resets the bypass on RPS Channels B and D.

3.3.4 Low Water Level, Steam Generator - Reactor Trip

See Figures 3.1, 3.2, 3.6, 3.7, and 3.14. Low steam generator downcomer water levels will cause a loss-of-heat-removal capability from the primary coolant system.

A reactor trip signal is initiated by two-out-of-four logic from four independent downcomer level differential pressure transmitters on each steam generator. Pretrip alarms are actuated to provide for annunciation of approach to reactor trip conditions.

3.3.5 Low Pressure, Steam Generator - Reactor Trip

See Figures 3.1, 3.2, 3.8, 3.9, 3.14 and 3.16. A reactor trip on low steam generator secondary pressure is provided to protect against excessively high steam flow caused by a steam line break. An abnormally high main steam flow from either steam generator will cause the secondary pressure to drop rapidly.

Four pressure transmitters on each steam generator actuate trip units which are connected in a two-out-of-four coincidence logic to initiate the reactor protective action if the steam generator pressure drops below a preselected

value. Signals from any two of the four indicating meter relays from either steam generator will close the main steam isolation valves on both steam generators. Pretrip alarms are also provided.

The zero power mode bypass switch, a key-operated switch, allows the steam generator low steam pressure trips to be bypassed for subcritical testing of control rod drive mechanisms. The zero power mode bypass switch also bypasses the low reactor coolant flow trip and the thermal margin/low pressure trip. The zero power mode bypass is automatically reset above 10^{-4}% power by signals from NI Channels 3 and 4.

3.3.6 High Pressurizer Pressure - Reactor Trip

See Figures 3.1, 3.2, 3.10 and 3.14. A reactor trip for high pressurizer pressure is provided to prevent excessive blowdown of the primary coolant system by relief action through the pressurizer power-operated relief or safety valves.

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

A reactor trip is initiated by two-out-of-four coincidence logic from the four independent measuring channels if the pressurizer pressure exceeds a preset pressure (1950 psia). This signal also opens the power-operated relief valves.

Pretrip alarms are initiated if the pressurizer pressure exceeds a preset pressure (1900 psia).

3.3.7 Thermal Margin/Low Pressure - Reactor Trip

See Figures 3.1, 3.2, 3.10, 3.11, 3.14 and 3.16. A reactor trip is initiated by a continuously computed function of primary coolant pressure and thermal power to prevent reactor conditions from violating a minimum departure from

nucleate boiling ratio (DNBR). At constant coolant flow, the temperature rise in the reactor is a function of power so that the variable trip can be effected by the adjustment of a pressure trip setpoint with reactor inlet and outlet coolant temperatures. At partial flow conditions, the changes in coolant temperature are such that the low thermal margin protection is continued with no change required in the pressure setpoint function. The variable pressure trip setpoint is computed by the function, $P_{Trip} = AT_{Hot} - BT_{Cold} - C$.

The reactor trip signal is initiated by a two-out-of-four coincidence logic from four independent safety channels, and audible and visual pretrip alarms are actuated to provide for annunciation on approach to reactor trip conditions.

The output from temperature transmitters on the hot and cold legs of each steam generator is combined by the summer units. The summer unit subtracts the cold leg temperature from the hot leg temperature. These signals are sent to the auctioneering unit. The auctioneering unit compares the signals from Loop 1 and Loop 2 and passes the one which represents the higher power. The output of the auctioneering unit is limited to a lower value which represents a minimum pressure of 1750 psia at nominal operating pressures of greater than 1800 psia; for nominal operating pressure of 1800 psia, this minimum is set at 1650 psia. This pressure is the minimum pressure, or "floor", below which pressure reactor trip will always occur.

The output of the auctioneering unit is sent to the trip unit and is used as a variable setpoint for the trip unit. The trip unit compares the primary system pressure with the variable setpoint from the auctioneering unit and trips if the system pressure is less than the setpoint. The zero power mode bypass switch, a key-operated switch, allows the thermal margin/low pressure trips and three additional trips to be bypassed at low power level. The zero power mode bypass is automatically reset above 10^{-4}% power by signals from NI Channels 3 and 4.

3.3.8 Loss of Load, Turbine Trip - Reactor Trip

See Figures 3.1, 3.2, 3.3, 3.12, 3.14 and 3.15. A reactor trip will automatically be initiated after a turbine trip occurs. A turbine low auto stop oil condition occurs with all turbine trips. The reactor trip will be initiated when the turbine auto stop oil pressure decreases, causing the auto stop oil pressure switch contacts to close and energize two turbine trip auxiliary relays. Each auxiliary relay will provide a reactor trip signal to two of four protective system channels. The loss of load reactor trip is an anticipatory trip which is not required to protect the reactor since the primary trip is high primary system pressure, and is automatically bypassed when any three of the four power range safety channels indicate less than 15% full power.

3.3.9 High Containment Pressure - Reactor Trip

See Figures 3.1, 3.2, 3.13 and 3.14. A reactor trip is initiated on high containment pressure.

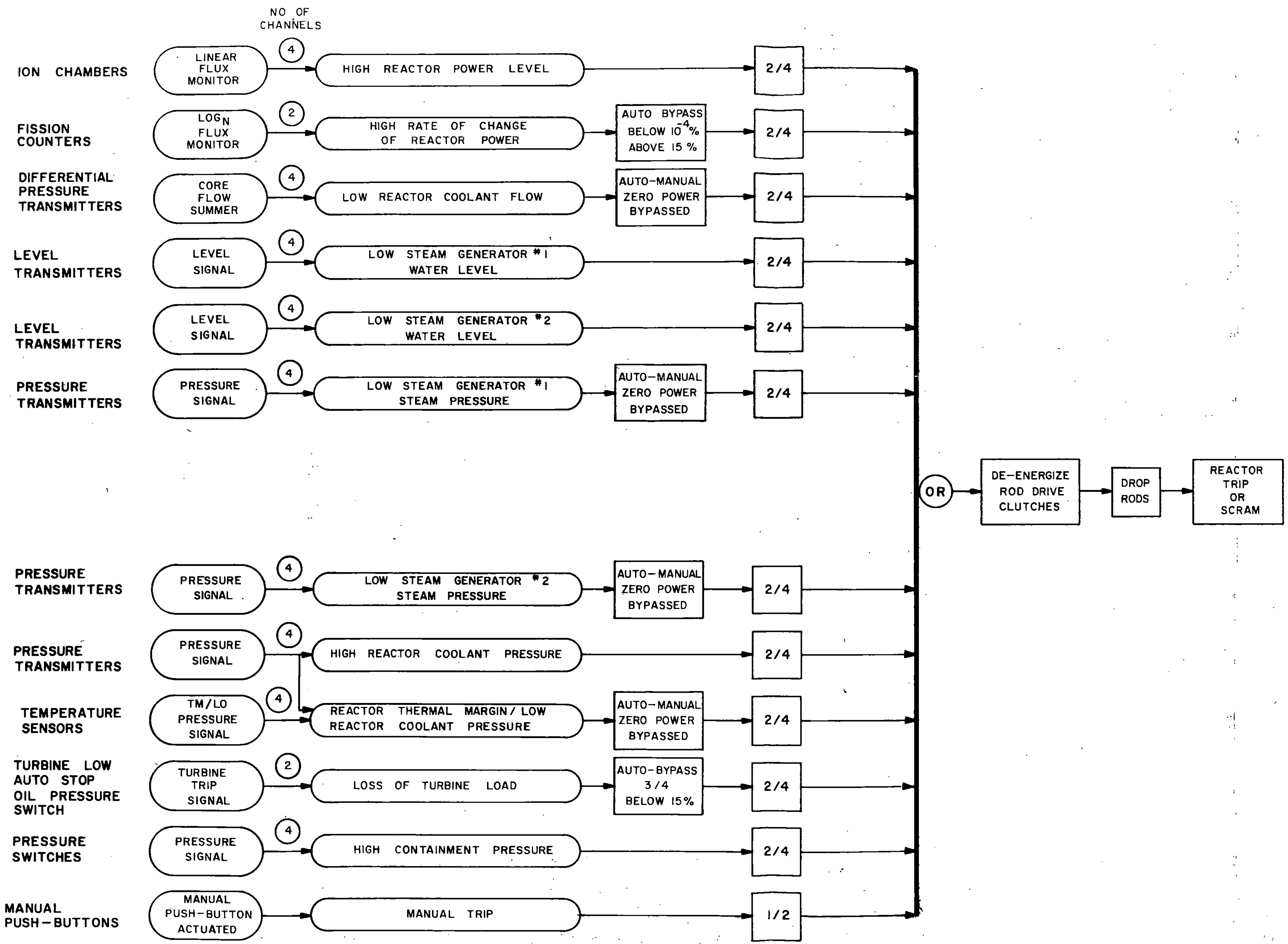
Four independent pressure switches actuate trip units which are connected in a two-out-of-four coincidence logic to initiate the reactor protective action when the containment pressure reaches 5 psig.

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

A pretrip alarm occurs when the containment pressure reaches 3 psig. This alarm is not generated by RPS equipment.

3.3.10 Manual - Reactor Trip

See Figures 3.1 and 3.2. A manual reactor trip is provided to permit the operators to trip the reactor. Manual actuation of either of two reactor trip push-button switches in the main control room causes direct interruption of the AC power to the DC power supplies feeding the electromagnetic clutches of the control rod drive mechanisms.



581-001-0

FIGURE 3.1
REACTOR TRIP LOGIC DIAGRAM

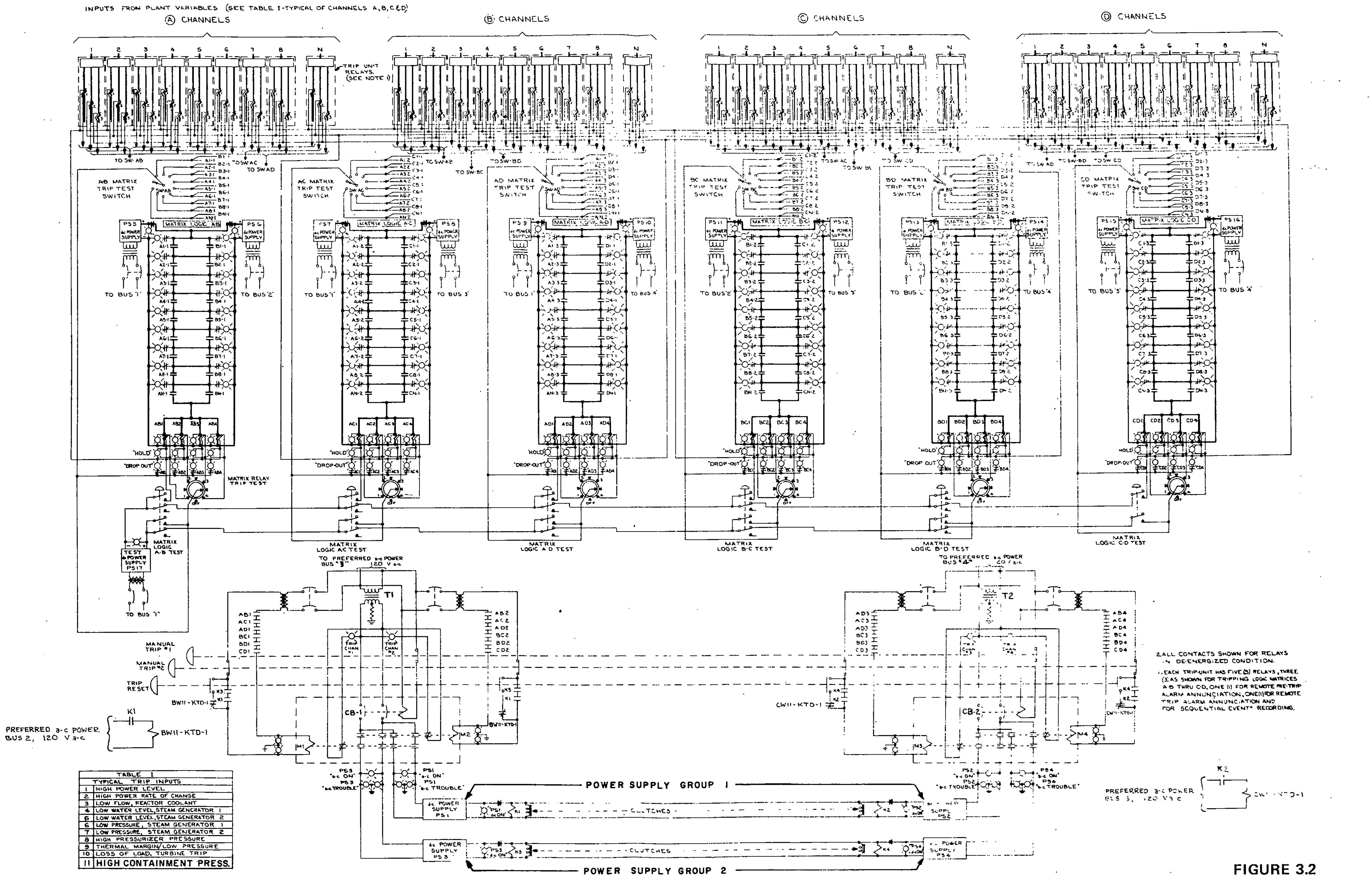


TABLE I	
TYPICAL TRIP INPUTS	
1	HIGH POWER LEVEL
2	HIGH POWER RATE OF CHANGE
3	LOW FLOW, REACTOR COOLANT
4	LOW WATER LEVEL, STEAM GENERATOR 1
5	LOW WATER LEVEL, STEAM GENERATOR 2
6	LOW PRESSURE, STEAM GENERATOR 1
7	LOW PRESSURE, STEAM GENERATOR 2
8	HIGH PRESSURIZER PRESSURE
9	THERMAL MARGIN/LOW PRESSURE
10	LOSS OF LOAD, TURBINE TRIP
11	HIGH CONTAINMENT PRESS.

FIGURE 3.2

REACTOR PROTECTION SYSTEM FUNCTIONAL DIAGRAM

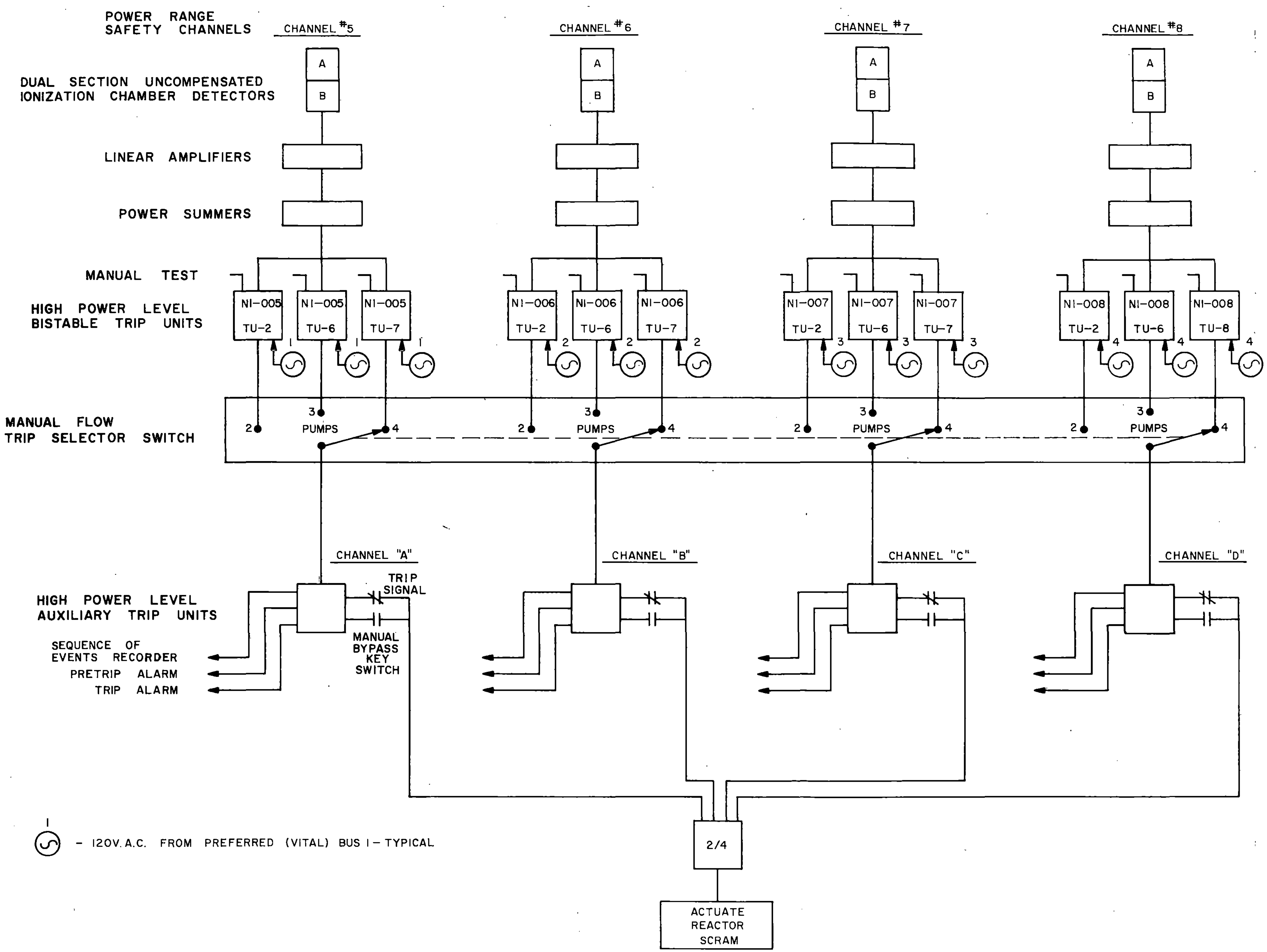


FIGURE 3.3
HIGH POWER LEVEL REACTOR TRIP
LOGIC DIAGRAM

581-002-0

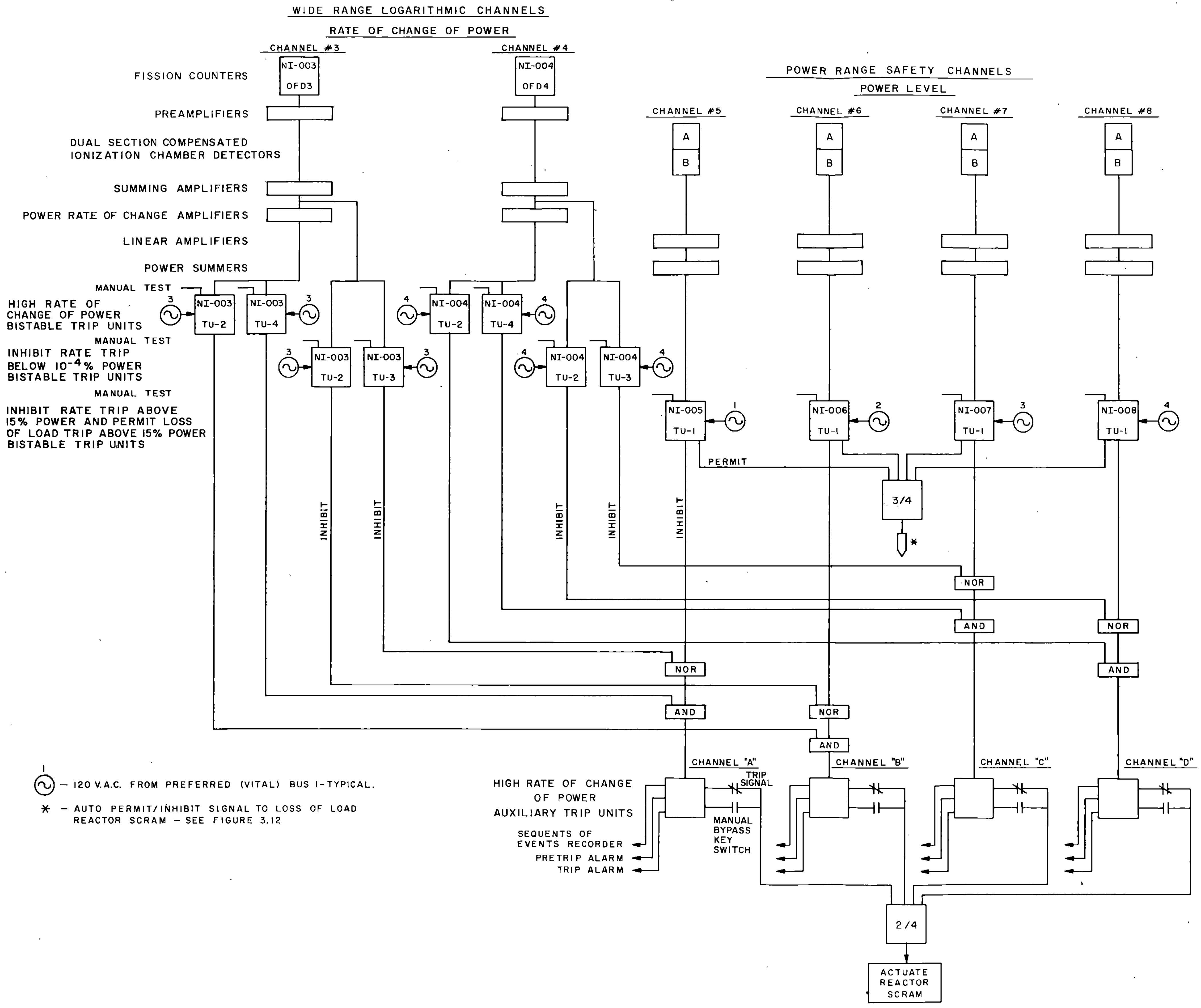


FIGURE 3.4
HIGH RATE OF CHANGE OF POWER REACTOR TRIP LOGIC DIAGRAM

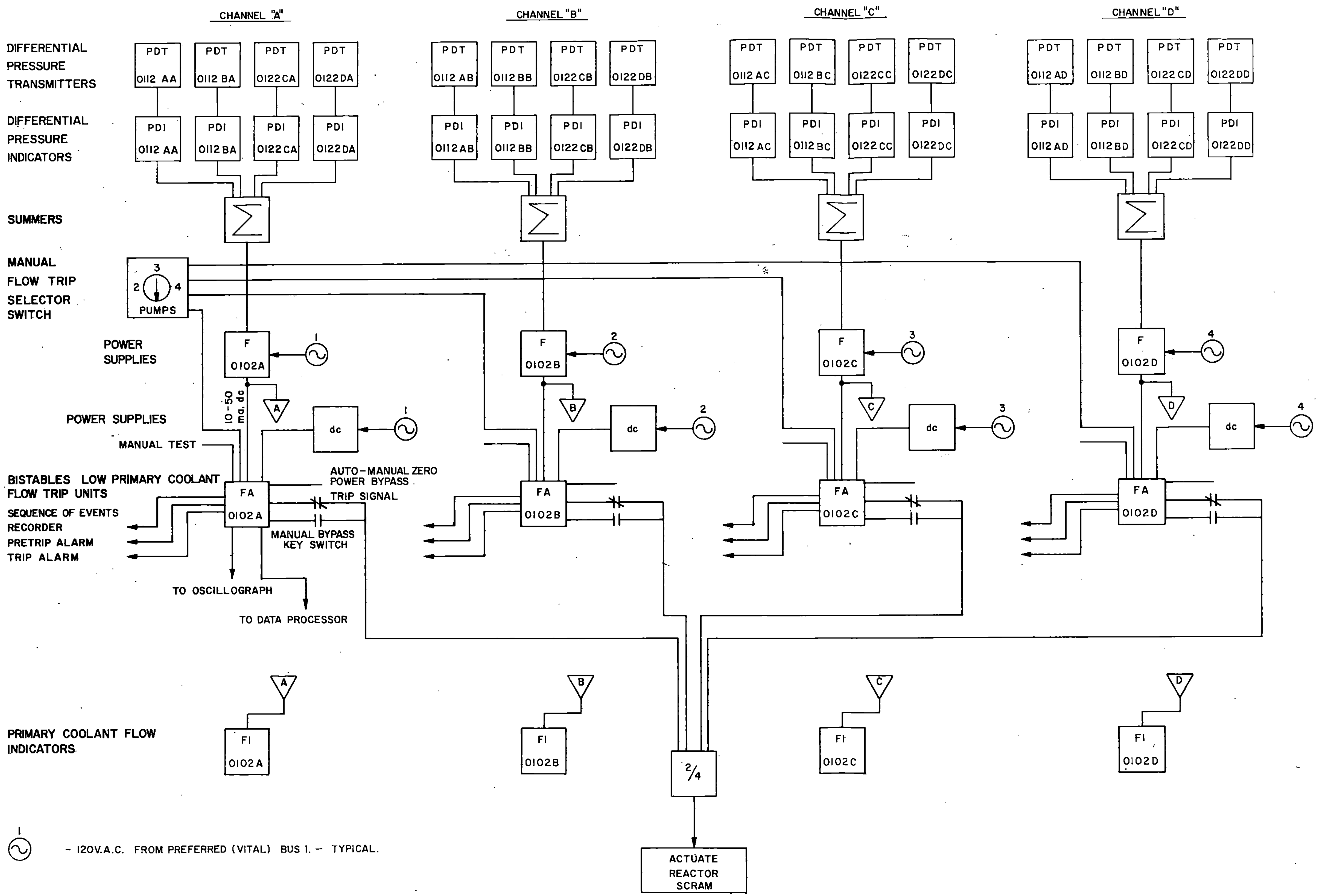


FIGURE 3.5
PRIMARY COOLANT LOW FLOW REACTOR TRIP LOGIC DIAGRAM

581-004-0

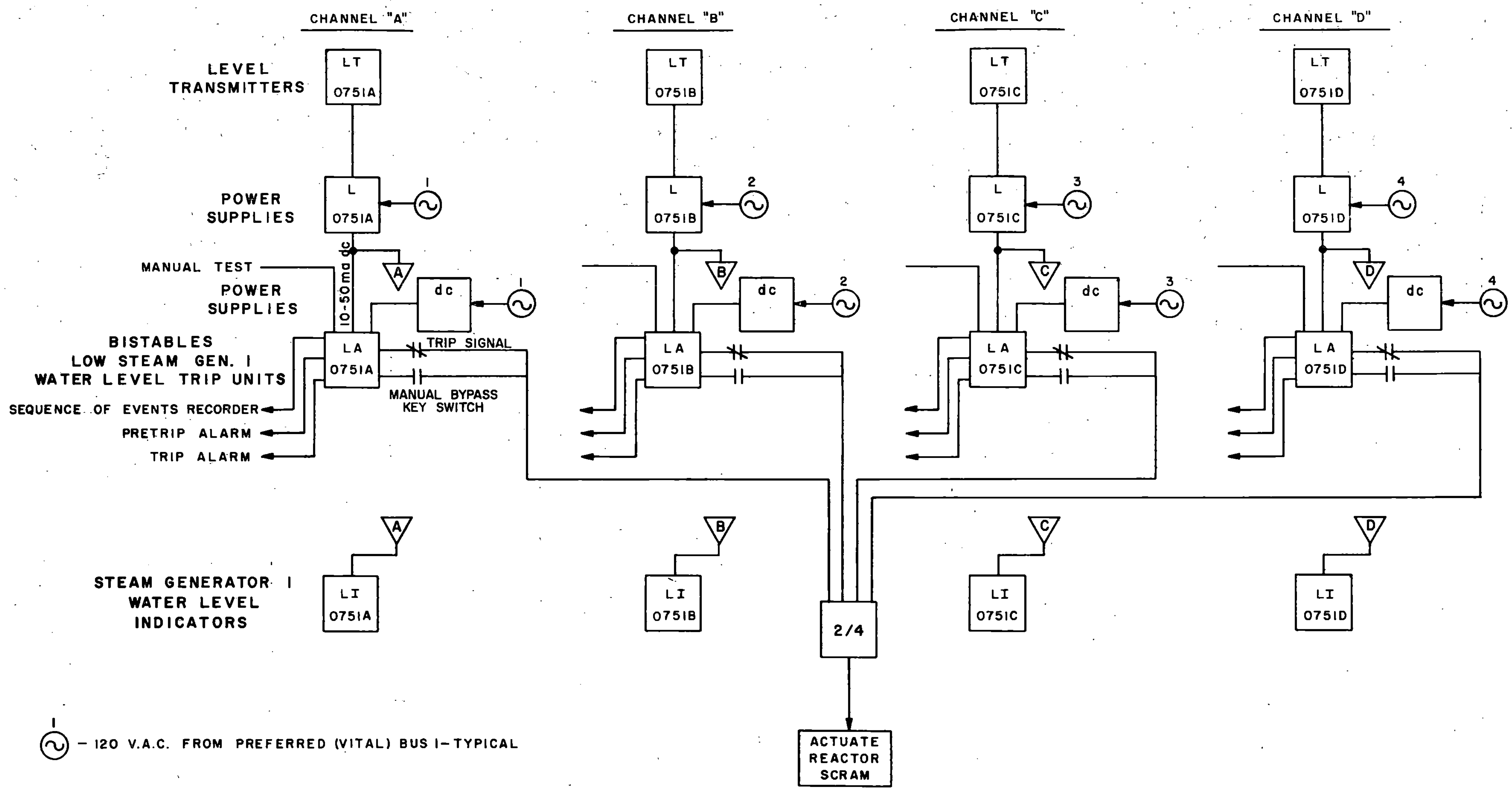


FIGURE 3.6
STEAM GENERATOR I LOW WATER LEVEL REACTOR TRIP LOGIC DIAGRAM

581-005-0

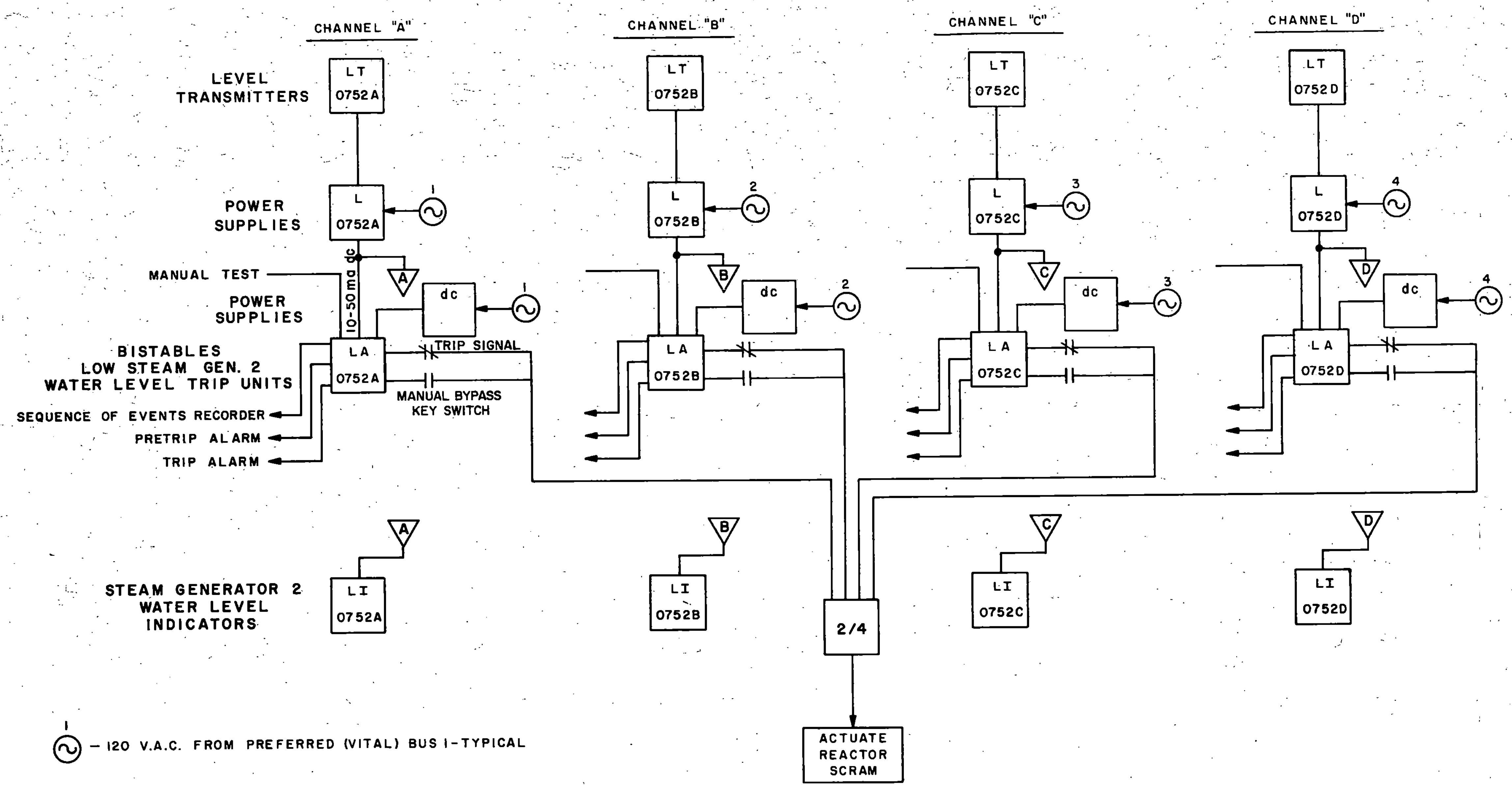


FIGURE 3.7
STEAM GENERATOR 2 LOW WATER LEVEL REACTOR TRIP LOGIC DIAGRAM

581-006-0

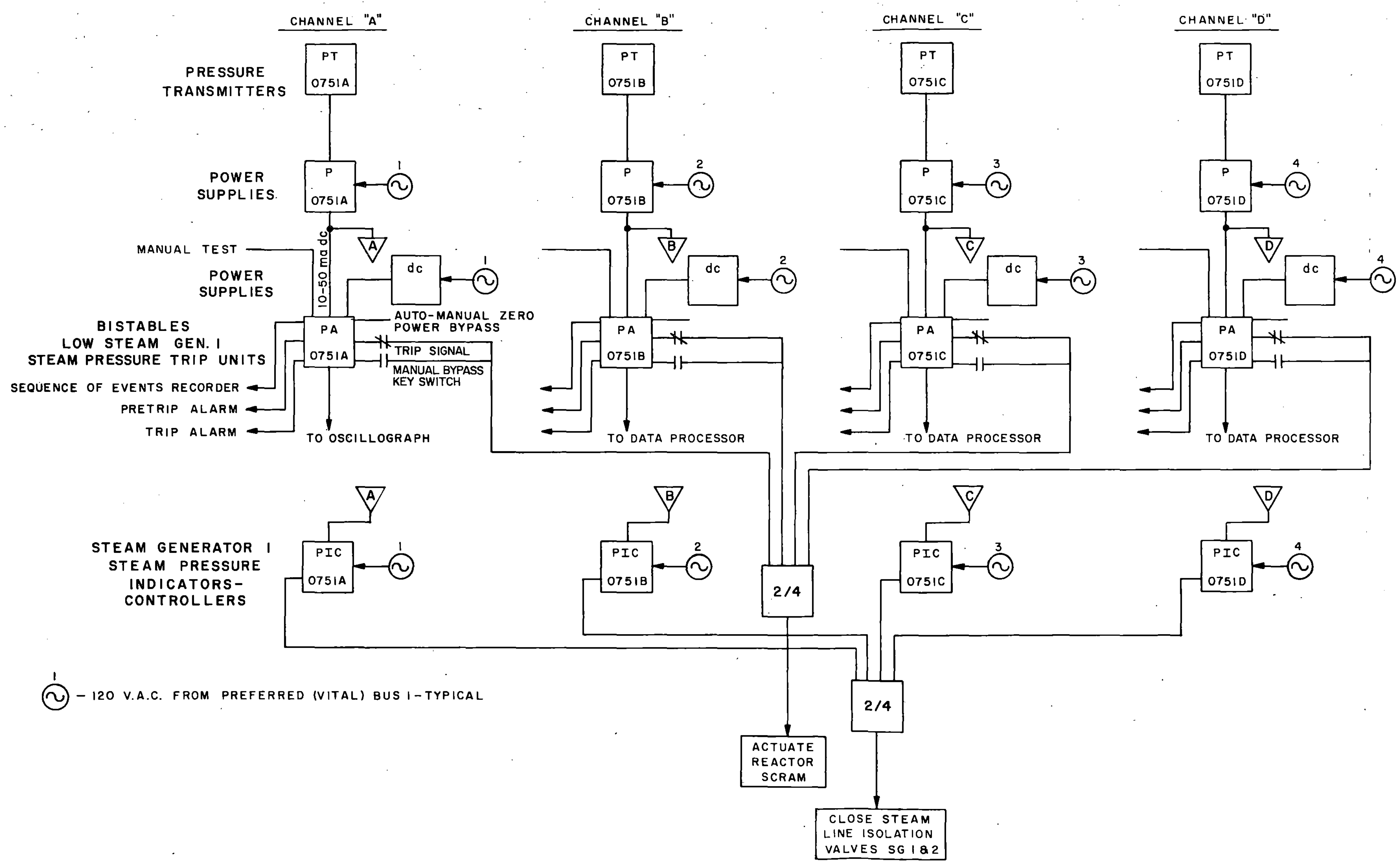
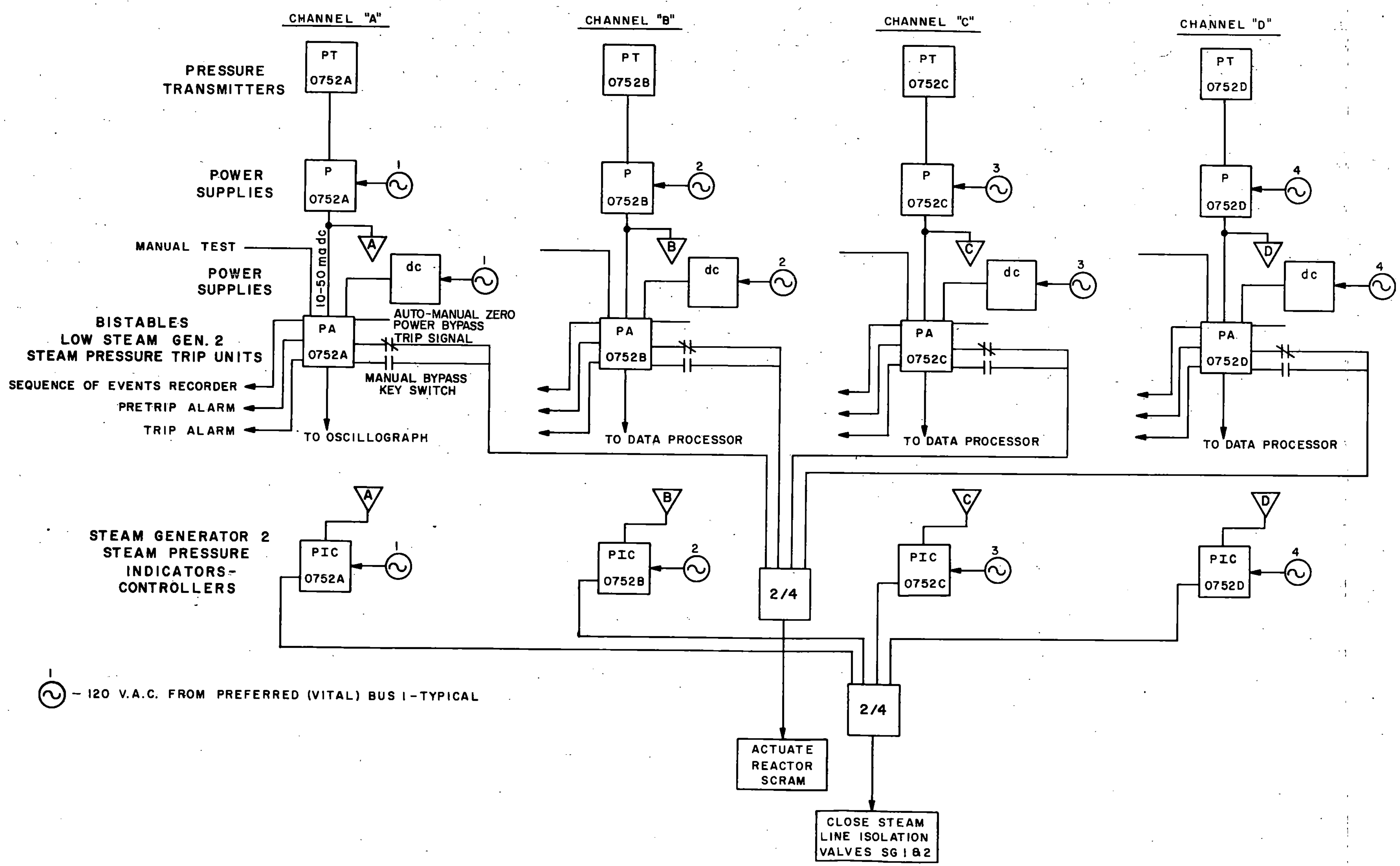


FIGURE 3.8
STEAM GENERATOR I LOW STEAM PRESSURE REACTOR TRIP LOGIC DIAGRAM

581-007-0



581-008-0

FIGURE 3.9
STEAM GENERATOR 2 LOW STEAM PRESSURE REACTOR TRIP LOGIC DIAGRAM

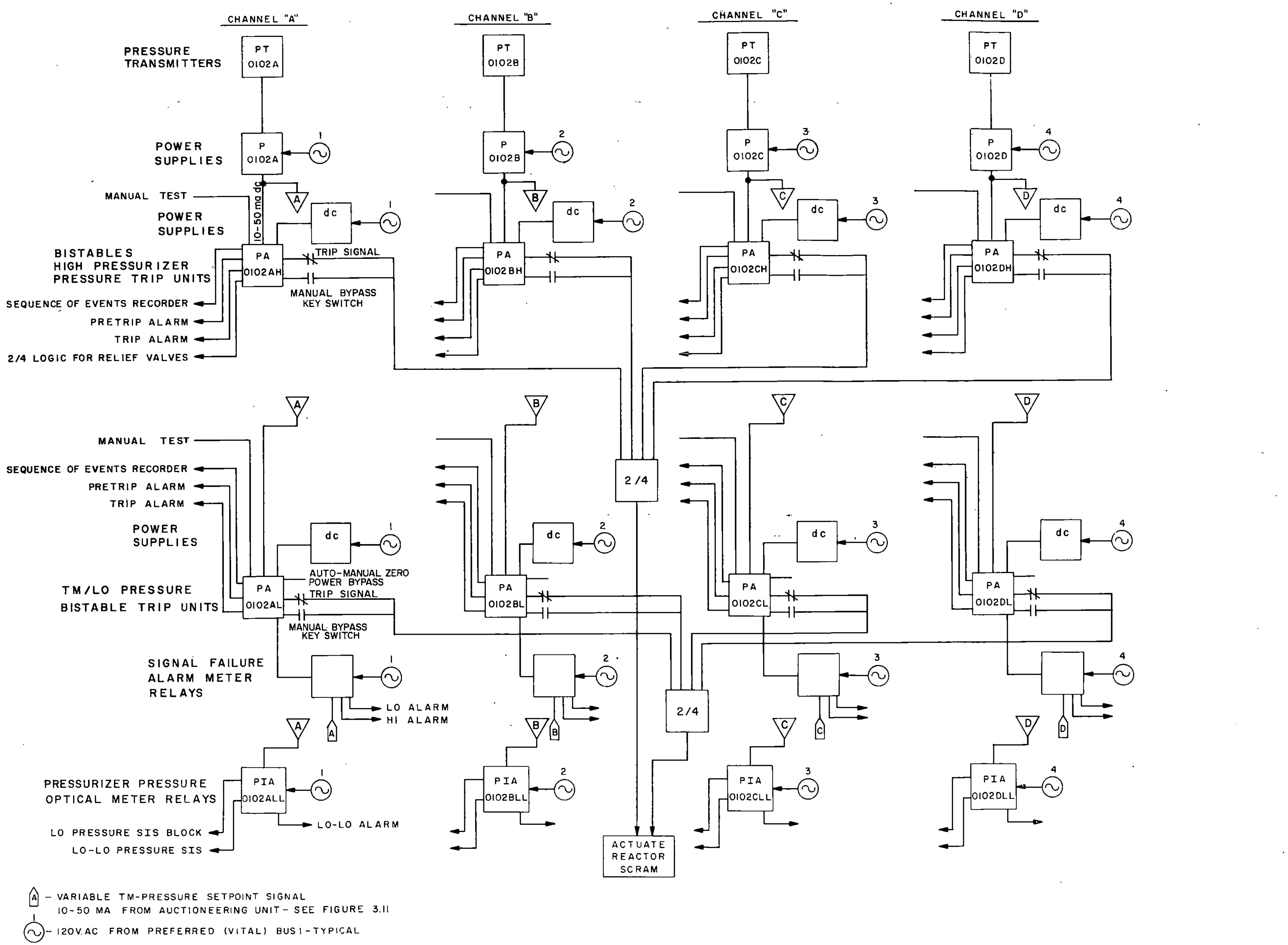
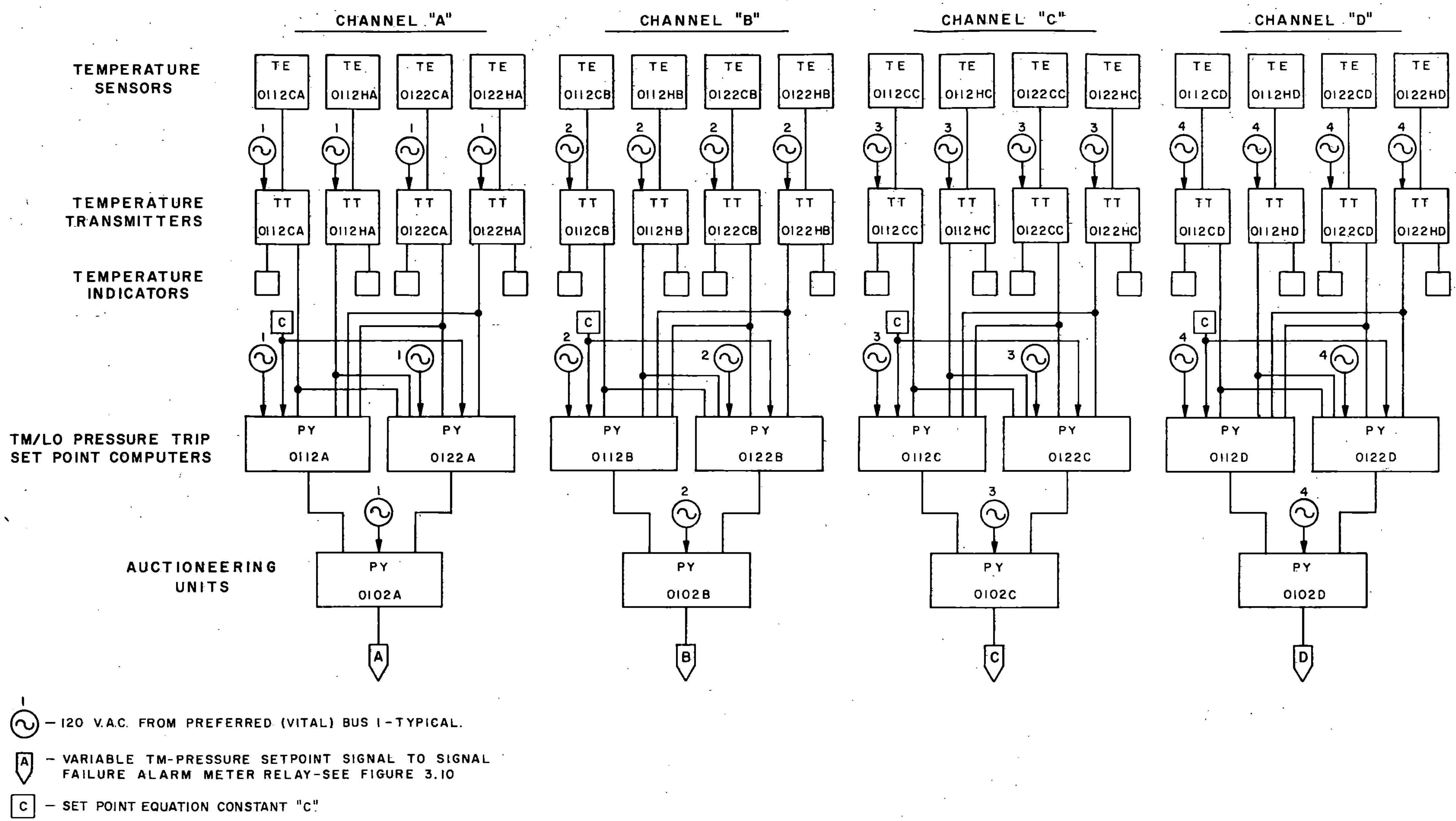


FIGURE 3.10
HIGH PRESSURIZER PRESSURE REACTOR TRIP AND THERMAL MARGIN/LOW PRESSURE REACTOR TRIP LOGIC DIAGRAM

581-009-0



581-010-0

FIGURE 3.11
THERMAL MARGIN/LOW PRESSURE REACTOR TRIP LOGIC DIAGRAM

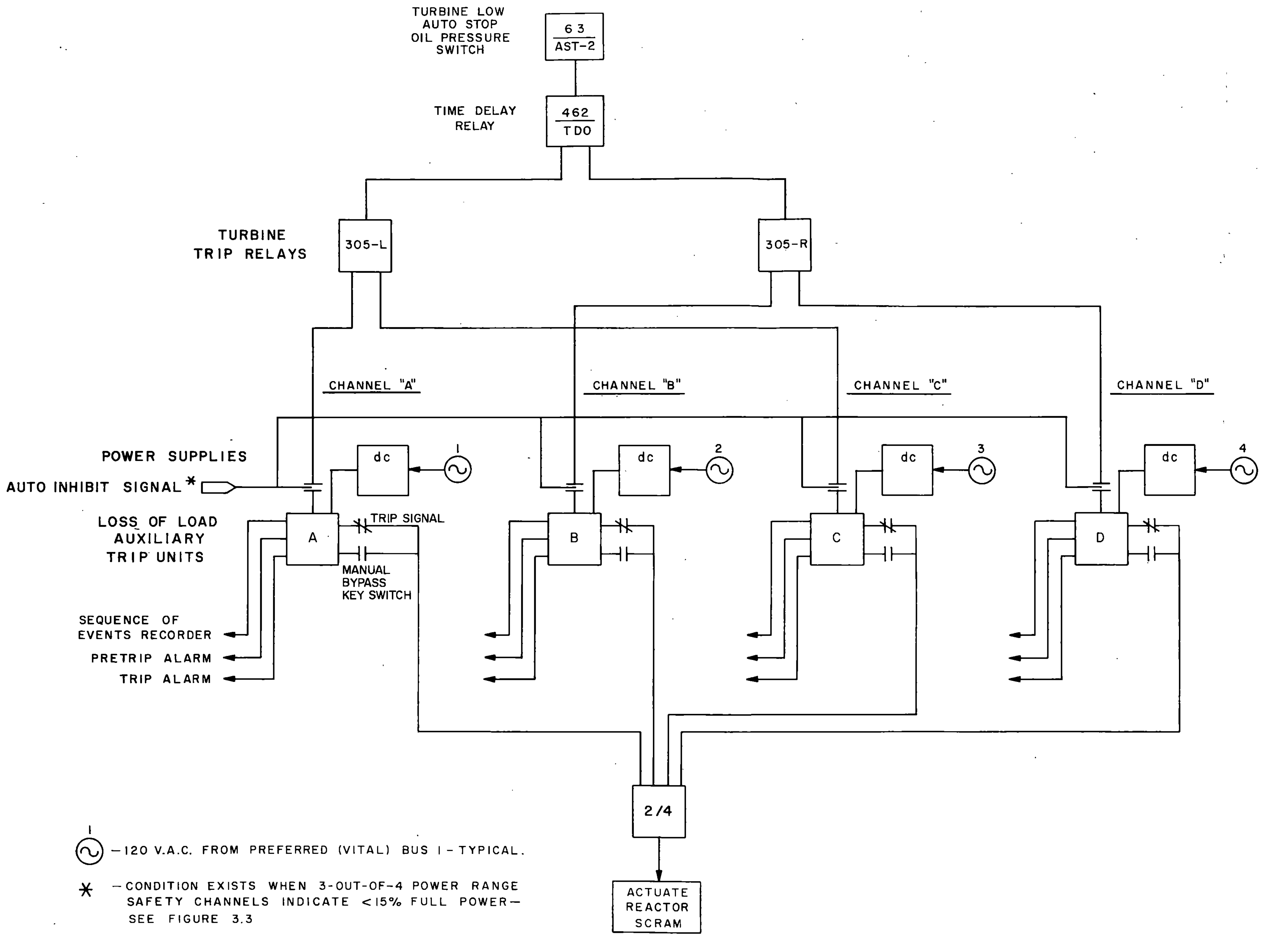


FIGURE 3.12
LOSS OF TURBINE LOAD REACTOR TRIP LOGIC DIAGRAM

581-011-0

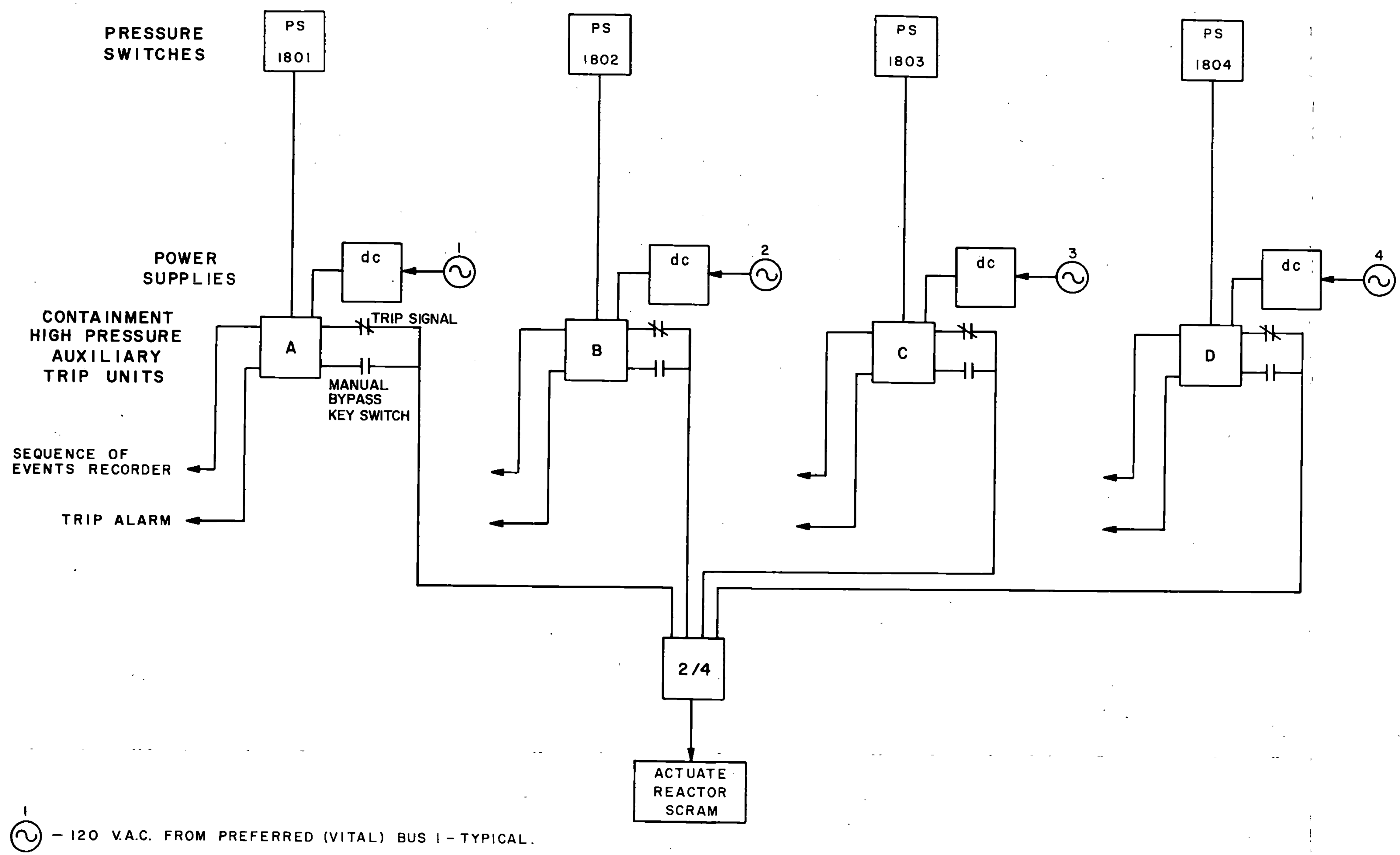
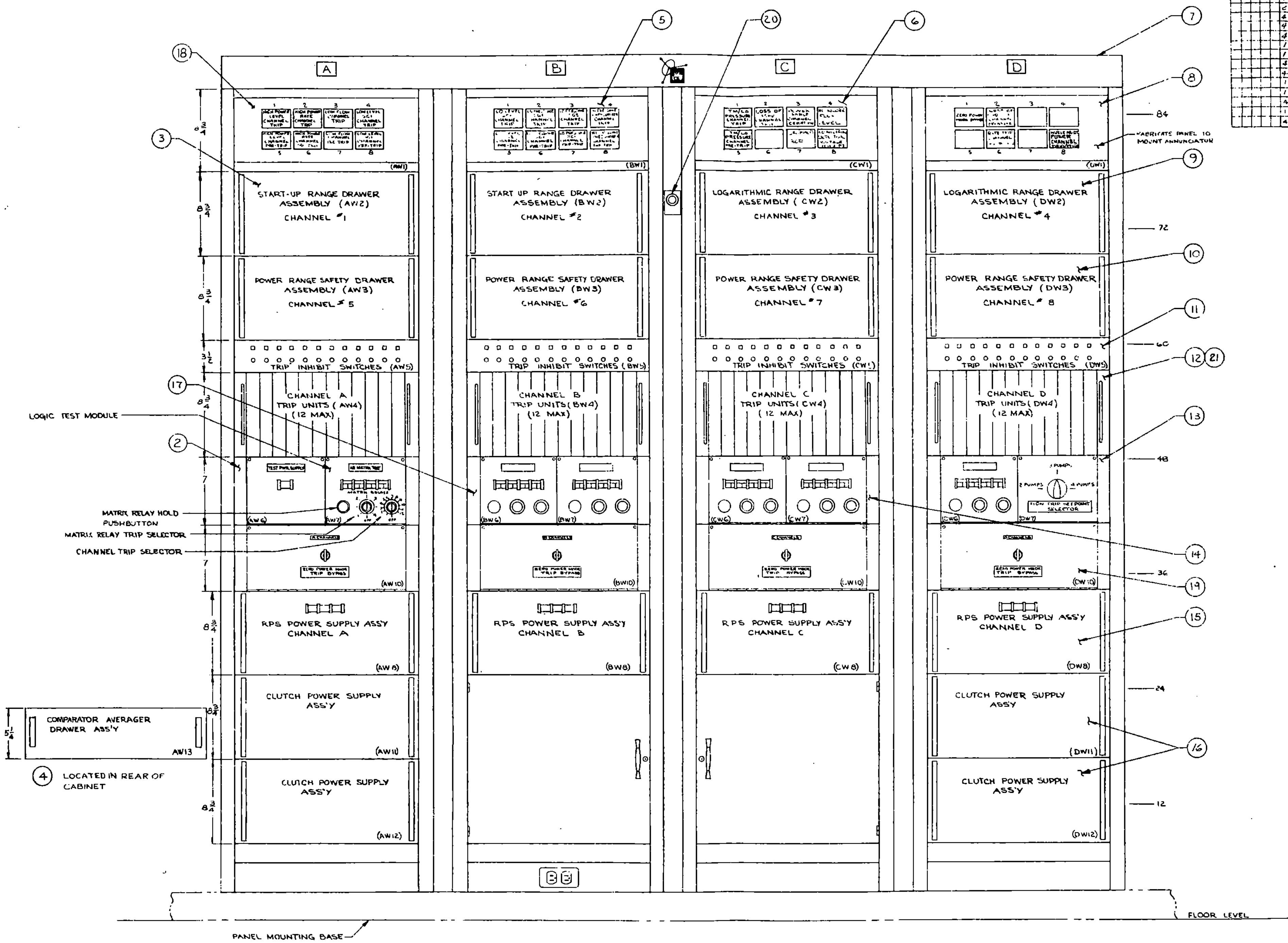


FIGURE 3.13
CONTAINMENT HIGH PRESSURE
REACTOR TRIP LOGIC DIAGRAM

581-012-0

BILL OF MATERIALS QUANTITIES ARE FOR										
GROUP NO & QUANTITY 6	5	4	3	2	1	ITEM NO	NAME	PIECE NO	MATERIAL	REMARKS
					X	1	NUCLEAR INSTRUMENTATION/ REACTOR PROTECTIVE SYSTEM	2966-E-2834-1		SEE SPEC 2966 421 S 001
					1	2	RPS BIN ASSEMBLY (CABINET "A")	2966-E-2855-2		SEE SPEC 2966 421 S 00(RPS-
					2	3	START-UP RANGE DRAWER ASSY	2966-E-2834-3		GULF GENERAL ATOMIC
					1	4	COMPARATOR AVERAGER DWR ASS'Y	-4		GULF GENERAL ATOMIC
					1	5	8 POINT ANNUNCIATOR UNIT	-5		SEE SPEC 2966 421 S 00(RPS-2)
					1	6	8 POINT ANNUNCIATOR UNIT	-6		
					1	7	CABINET ASSEMBLY	2966 E 2152 -1		SEE SPEC 2966-421-S 00(RPS-
					1	8	8 POINT ANNUNCIATOR UNIT	2966 E-2834-8		SEE SPEC 2966-421-S-00(RPS-2)
					2	9	LOGARITHMIC RANGE DRAWER ASSY	-9		GULF GENERAL ATOMIC
					4	10	POWER RANGE DRAWER ASSY	-10		GULF GENERAL ATOMIC
					4	11	TRIP INHIBIT MODULE ASS'Y	2966-E-2861-1		SEE SPEC 2966 421-S-00(RPS-5
					4	12	TRIP-UNIT BIN ASSY	2966-D-3196-1		SEE SPEC 2966-421-S-00(RPS-
					1	13	RPS BIN ASSEMBLY (CABINET "D")	2966-E-2155-5		SEE SPEC 2966-421-S-00(RPS-1)
					1	14	RPS BIN ASSEMBLY (CABINET "C")	2966-E-2155-4		SEE SPEC 2966-421-S-00(RPS-1)
					4	15	RPS POWER SUPPLY ASS'Y	2966-E-2834-15		SEE SPEC 2966-421-S-00(RPS-7)
					4	16	CLUTCH POWER SUPPLY ASS'Y	2966-D-3202-1		SEE SPEC 2966-421-S-00(RPS-6)
					1	17	RPS BIN ASSEMBLY (CABINET "B")	2966-E-2155-3		SEE SPEC 2966-421-S-00(RPS-1)
					1	18	8 POINT ANNUNCIATOR UNIT	2966-E-2834-18		SEE SPEC 2966-421-S-00(RPS-2)
					4	19	AUXILIARY LOGIC ASS'Y	2966-E-2863-1		SEE SPEC 2966-421-S-00(RPS-1
					1	20	REACTOR TRIP SWITCH ASS'Y	2966-E-2853-3		
					4	21	TRIP UNIT INTERCONNECTION MODULE ASS'Y	2966-E-2857-1		SEE SPEC 2966-421-S-00(RPS-1



(1) NUCLEAR INSTRUMENTATION AND REACTOR PROTECTIVE SYSTEM

FIGURE 3.14

REACTOR PROTECTION SYSTEM CABINETS

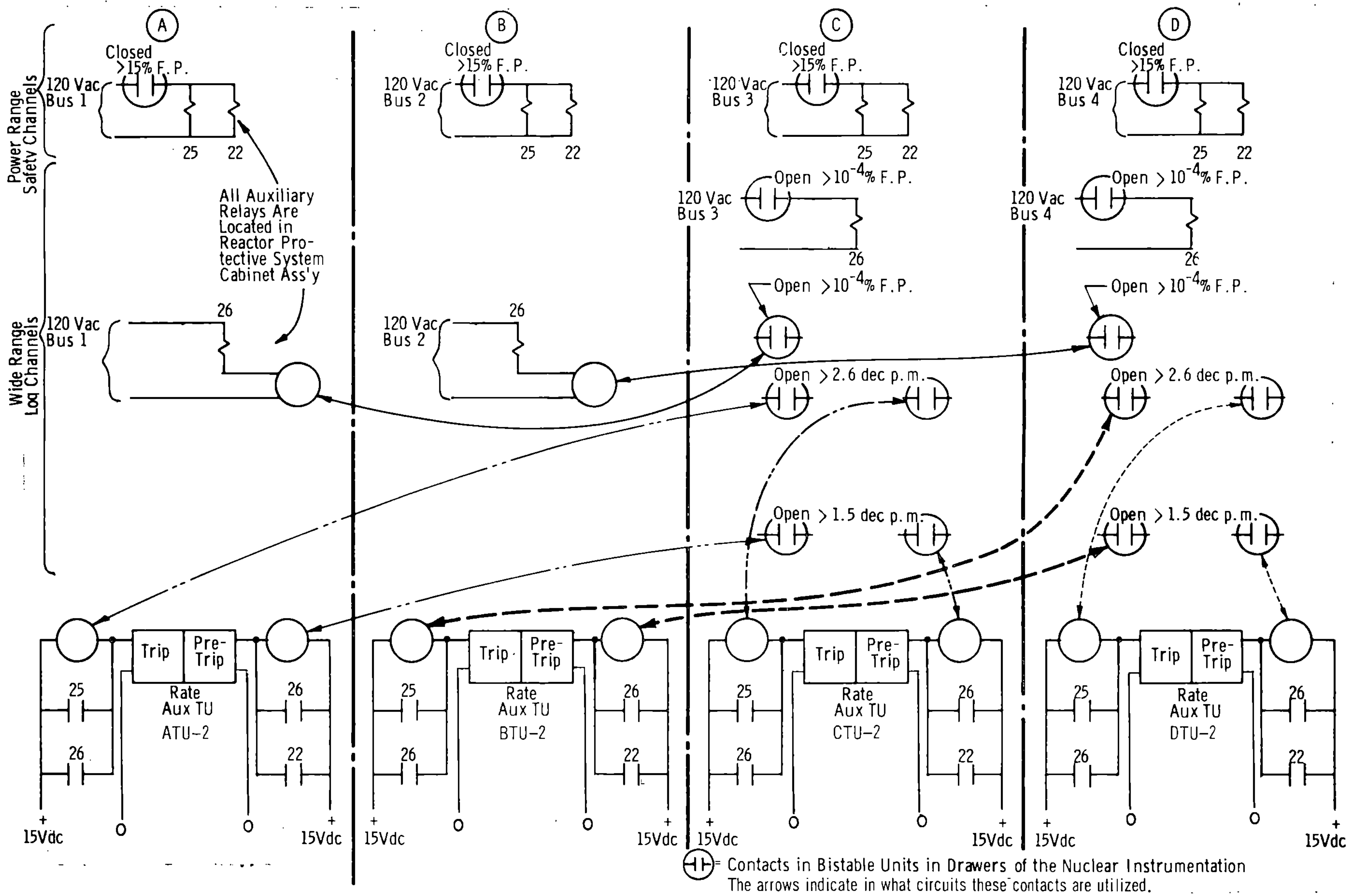
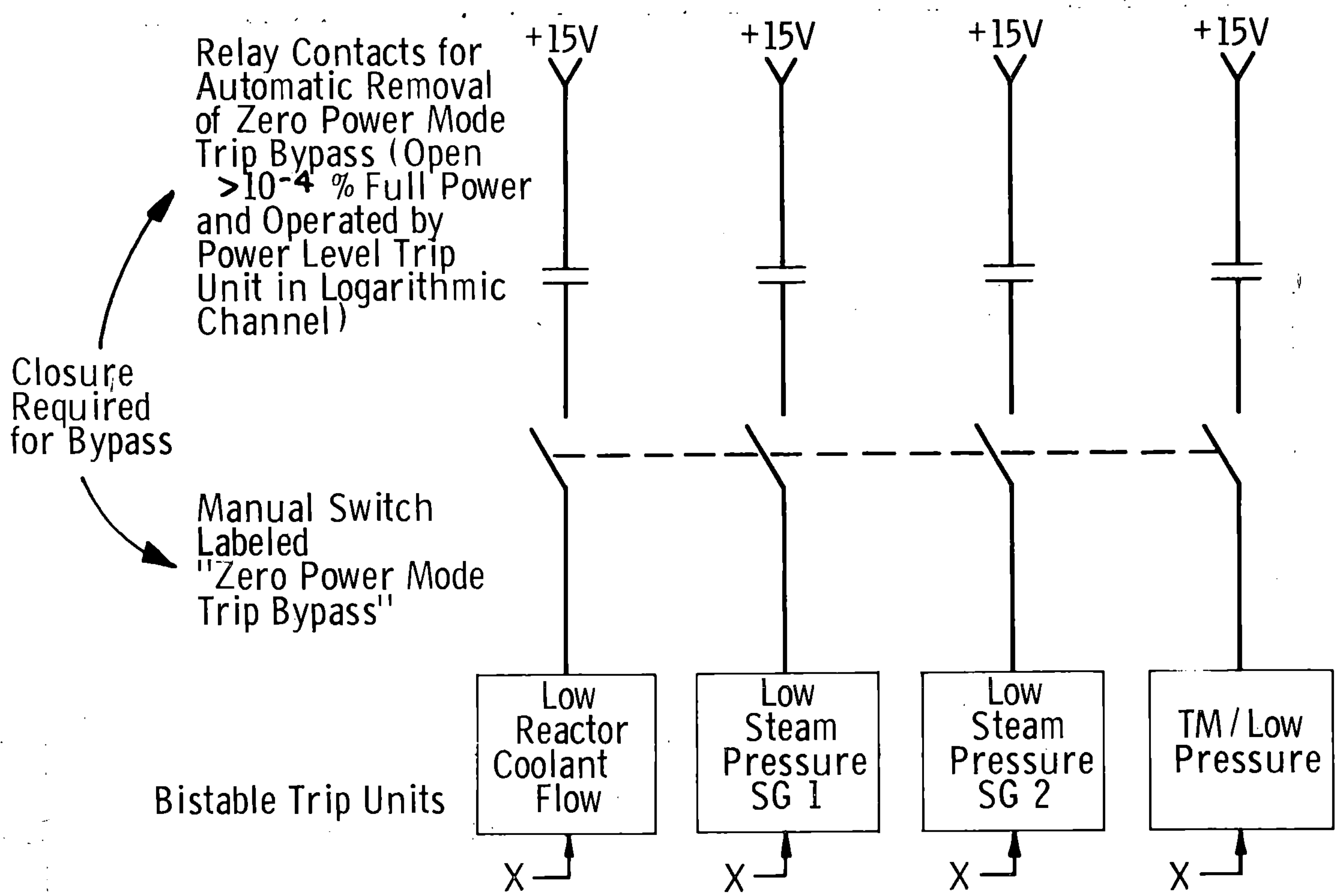


FIGURE 3.15

POWER RATE OF CHANGE TRIP AND PRE–TRIP INTERFACE WITH RPS



X = Analog Input Signal

With +15V Applied to Bistable Trip Unit: No Trip Regardless To Level of Input Analog Signal

Without +15V Applied to Bistable Trip Unit: Trip According to Level of Input Analog Signal

Same Arrangement for Other 3 Channels

FIGURE 3.16

ZERO POWER MODE BYPASS LOGIC DIAGRAM

4.0 REACTOR PROTECTION SYSTEM FAILURE ANALYSIS

4.1 Single Failure Analysis

A Failure Mode and Effects Analysis (FMEA) was generated for the RPS to determine the system vulnerability to single failures and to establish a system performance baseline for the Common Mode Failure Analysis (CMFA). The FMEA investigated each available RPS trip mode to determine if any single equipment failure could inhibit the actuation of a required protective trip. The hypothesized failures were also analyzed to determine the effect on the integrated RPS Reactor Trip (RT) function. The FMEA is attached as Appendix A.

The analysis demonstrated that no single RPS equipment failure could inhibit the actuation of any required protective RT's. The two RPS anticipatory RT's, high power rate-of-change, and loss of load-turbine trip, are both vulnerable to single failures which would inhibit the trip actuation.

The high power rate-of-change RT (RT#2) is provided to protect the reactor against an uncontrolled control rod withdrawal while the core is at very low power levels. This is an anticipatory trip which is not required to protect the reactor since the primary trip is the high power level trip (RT#1) (Reference 4). Review of Appendix A, Table A-2 indicates that RT#2 is vulnerable to single failures which would disable the automatic scram function only if one of the RPS RT#2 channels was in the bypass mode. If no RPS RT#2 channels are in bypass, a single equipment failure cannot inhibit the RT#2 function.

The loss of load, turbine trip RT (RT#10), is an anticipatory trip which is not required to protect the reactor since the primary trip is high primary system pressure (RT#8) (Reference 5). Table A-10, Appendix A, indicates that the following single failures will disable the anticipatory RT#10 function:

- Turbine auto stop pressure switch (63/AST-2) contacts fail open.
- Time delay relay (462/TDO) fails to the tripped state.
- Loss of power to the two turbine trip relays 305-L and 305-R. The relay power source is 125 VDC from panel D21, breaker 72-212.

4.2 Common Mode Failure Analysis

Common mode failures (CMF's) have been generally defined as multiple unit failures due to a single cause. The cause of failure may be separated into five broad and generic categories:

- Functional Deficiency
- Equipment design deficiency
- Operation and maintenance errors
- External phenomena
- External normal environment

Table 4.1 presents a summary of preventive measures which are available to prevent CMF's. Each of the generic failure causes were addressed in the CMFA.

The CMFA was developed for both the individual RT modes and for the integrated RPS which incorporated all the RT modes available at the Palisades Plant. The responsiveness of all available reactor trip modes to each anticipated transient was evaluated. The trip mode sequence evaluation assumed that the preceding trip mode(s) did not actuate. Figure 4.1 presents a summary of the RT's available at the Palisades Plant during each of the transients.

TABLE 4.1

COMMON MODE FAILURE PREVENTIVE MEASURES

FAILURE CATEGORY	POSSIBLE PREVENTIVE MEASURES
External normal environment	Functional diversity Design administrative controls Operational administrative controls Safe failure modes Proven design Standardization Equipment diversity
Design deficiency	Functional diversity Physical separation Design administrative controls Safe failure modes Equipment diversity
Operational or Maintenance errors	Functional diversity Operational administrative controls Equipment diversity
External phenomena	Functional diversity Physical separation Design administrative controls Safe failure modes Equipment diversity
Functional deficiency	Functional diversity Design administrative controls Equipment diversity

ANTICIPATED TRANSIENT EVENTS	AUTOMATIC REACTOR TRIP MODES AVAILABLE AT THE PALISADES PLANT										
	High Power Level	High Power Rate of Change	Low Flow Reactor Coolant	Low Level Level SG#1	Low Level SG#2	Low Press SG#1	Low Press SG#2	High Pressur- izer Press	Thermal Margin/ Low Press	Turbine Trip	High Containment Press
	RT#1	RT#2	RT#3	RT#4	RT#5	RT#6	RT#7	RT#8	RT#9	RT#10	RT#11
1 Loss of electrical load								E		E	I
2 Load increase	E			L	L	L	L		I	L(4)	
3 Complete loss of feedwater				E	E	I	I	I	I	L(4)	I
4 Complete loss of primary flow			E	L	L	L	L	E	L	L(4)	
5 Loss of normal electrical power			E	E	E			E	L	E	L
6 Inactive primary loop start-up	E										
7 Rod withdrawal at full power	I			L	L	L	L	I	L	L(4)	
8 Primary system depressurization			L	L	L	L	L		I	L(4)	
9 Boron dilution	I			L	L	L	L		L	L(4)	
10 Small line break			L	L	L	L	L		I	L(4)	

NOTES:

1. E Designates trip signal generated early in the transient (within first minute).
2 I Designates trip signal generated after 1 minute but before 10 minutes into the transient.
3. L Designates trip signal generated late in the transient (after 10 minutes).
4. Low steam generator pressure closes main steam isolation valves and causes turbine trip.

FIGURE 4.1

AUTOMATIC RPS RESPONSE FOR ANTICIPATED TRANSIENTS AT THE PALISADES PLANT

The detailed results of the CMFA are most significant when evaluated from the viewpoint of the integrated RPS responsiveness to an anticipated reactor transient. Figure 4.1 presents the integrated RPS design baseline for determining the overall impact of potential CMF's on the RPS responsiveness to the anticipated reactor transients.

4.2.1 Combinations of Failures

The first step in the CMFA involves identification of the combinations of failures or events required for system failure. The FMEA generated the baseline data for the analysis of events and failure combinations which must exist to cause the loss of a RT function. Each RT function which is part of the Palisades Plant RPS design was investigated to determine the combination of failures required to inhibit the function. The following sections denote the possible failure combinations which would inhibit each RPS trip function.

4.2.1.1 High Power Level (RT#1)

The RT#1 function was previously described in Section 3.3.1. For the purpose of this analysis, the system components were grouped into the following three major functional elements which could fail to a non-tripped condition and inhibit this required protective RT.

- o Sensor/RPS channels
- o Coincidence logic matrix input relays
- o Clutch power supply trains.

The first functional element, sensor/RPS channels, includes all components from the sensor to the RPS auxiliary trip unit. The second functional element is the three output relays (K1, K2, and K3) of each RPS auxiliary trip unit.

The third group, clutch power supply train, includes all components from the four output trip relays associated with each of the six trip matrices to the four M coils (M1, M2, M3, and M4).

Table 4.2 presents a summary of the RT#1 FMEA (Appendix A, Tables A-1 and A-13) and lists the possible component failures which would propagate a non-tripped state in a major functional element. Figure 4.2 shows the failure combinations of major functional elements which would have to occur to inhibit a RT on high power level (RT#1).

4.2.1.2 High Power Rate-of-Change (RT#2)

The RT#2 function was previously described in Section 3.3.2. For the purpose of this analysis, the system components were grouped into the following four major functional elements which could fail to a non-tripped condition and inhibit this anticipatory RT.

- Sensors
- RPS channels
- Coincidence logic matrix input relays
- Clutch power supply trains.

The first functional element, sensors, includes all components from the sensor to the input of the nuclear instrumentation channel bistable units. The second functional element includes all components from the nuclear instrumentation bistable units to the RPS auxiliary trip unit output relays. The coincidence logic matrix input relay and clutch power supply train functional elements include the same equipment complement that was previously defined for RT#1.

TABLE 4.2

FMEA SUMMARY FOR RT#1

Failed Component	Failure Mode	Failure Effect
Uncompensated ion chamber A or B	Fail low	Sensor/RPS channel functional element fails to untripped state.
"	Output signal constant	
"	Short across signal line	
Linear Amp, ion chamber A or B	Fail low	
"	Output signal constant	
"	Short across signal line	
High voltage power supply	Loss of output	
Bistable Unit 7	Fail untripped (4 pump operation)	
Bistable Unit 6	Fail untripped (3 pump operation)	
Bistable Unit 2	Fail untripped (2 pump operation)	
Auxiliary trip unit	Fail untripped	
RT#1 channel bypass switch	Fail closed	

TABLE 4.2 (cont'd)

Failed Component	Failure Mode	Failure Effect
Auxiliary trip unit output relay K1, K2, or K3	Fails to energized state (hung up)	Coincidence logic matrix input relay circuit fails to untripped state. See Table 4.3 for specific relay/logic matrix schedule.
Logic matrix output relay (e.g., AB1, AB2, AB3, or AB4)	Fails to energized state (hung up)	Clutch power supply train fails to untripped state.
M coil M1, M2, M3, or M4	Fails to energized state (hung up)	

RPS Failure Array ID No.	Sensor/RPS Channels				Logic Matrix Input Relays						Clutch Power Supply Trip Train			
	A	B	C	D	AB	AC	AD	BC	BD	CD	1	2	3	4
1	X	X	X											
2	X	X		X										
3	X		X	X										
4		X	X	X										
5	X	X								X				
6	X		X						X					
7	X			X				X						
8		X	X				X							
9		X		X		X								
10			X	X	X									
11	X							X	X	X				
12		X				X	X			X				
13			X		X		X		X					
14				X	X	X		X						
15					X	X	X	X	X	X				
16											X	X		
17													X	X

X = Trip Inhibiting Failure

FIGURE 4.2

TYPICAL ARRAY OF FAILURES REQUIRED TO INHIBIT RPS RT

TABLE 4.3

TRIP LOGIC MATRIX INPUT RELAY SCHEDULE

RPS Channel ↓ \ Channel Output Relay →	K1	K2	K3
A	AB	AC	AD
B	AB	BC	BD
C	AC	BC	CD
D	AD	BD	CD

Table 4.4 presents a summary of the RT#2 FMEA (Appendix A, Tables A-2 and A-13) and lists the possible component failures which would propagate a non-tripped state in a major functional element. Figure 4.3 shows the combinations of major functional element failures which would have to occur to inhibit a RT on high power rate-of-change (RT#2).

4.2.1.3 Low Flow, Reactor Coolant (RT#3)

The RT#3 function was previously described in Section 3.3.3. For the purpose of this analysis, the system components were grouped into the following three major functional elements which could fail to a non-tripped condition and inhibit this required protective RT.

- Sensor/RPS channels
- Coincidence logic matrix input relays
- Clutch power supply trains.

The first functional element, sensor/RPS channels, includes all components from the sensor to the bistable trip unit output relays. The second functional element is the three output relays (K1, K2, and K3) of each bistable trip unit. The clutch power supply train functional element includes the same equipment that was previously defined for RT#1 (Section 4.2.1.1).

Table 4.5 presents a summary of the RT#3 FMEA (Appendix A, Tables A-3 and A-13) and lists the possible component failures which would propagate a non-tripped state in a major functional element. Figure 4.2 shows the combinations of major functional element failures which would have to occur to inhibit a RT on low reactor coolant flow (RT#3).

TABLE 4.4

FMEA SUMMARY FOR RT#2

Failed Component	Failure Mode	Failure Effect
Fission counter	Fail low	Sensor functional element fails to untripped state.
"	Output signal constant	
"	Short across signal line	
Pre amp	Fail low	
"	Output signal constant	
"	Short across signal line	
High voltage power supply	Loss of output	
Pulse amp and count rate circuits	Loss of output	
"	Fail low	
"	Loss of supply voltage from preferred AC bus	
Summing amp	Low signal level output	
"	Constant signal level output	
"	Loss of supply voltage from preferred AC bus	

TABLE 4.4 (cont'd)

Failed Component	Failure Mode	Failure Effect
Power rate-of-change amp	Low signal level output	Sensor functional element fails to untripped state. (continued)
"	Constant signal level output	
"	Loss of supply voltage from preferred AC bus	
Nuclear inst. sys. bistable unit (#2 or #4)	Fail untripped	RPS channel functional element fails to untripped state.
Auxiliary trip unit	Fail untripped	
RT#3 channel bypass switch	Fail closed	
Auxiliary trip unit output relay K1, K2, or K3	Fails to energized state (hung up)	Coincidence logic matrix input relay circuit fails to untripped state. See Table 4.3 for specific relay/logic matrix schedule.
Logic matrix output relay (e.g., AB1, AB2, AB3, or AB4)	Fails to energized state (hung up)	Clutch power supply train fails to untripped state.
M coil M1, M2, M3 or M4	Fails to energized state (hung up)	

RPS Failure Array ID No.	Sensor Channel 3	4	RPS Channels A	B	C	D	Logic Matrix Input Relays AB	AC	AD	BC	BD	CD	Clutch Power Supply Trip Train 1	2	3	4
1	X	X														
2	X			X												
3	X					X										
4		X	X													
5		X			X											
6			X	X	X											
7			X	X		X										
8			X		X	X										
9				X	X	X										
10			X	X								X				
11			X		X						X					
12			X			X				X						
13				X	X				X							
14				X		X		X								
15					X	X	X									
16			X							X	X	X				
17				X				X	X			X				
18					X		X		X		X					
19						X	X	X		X						
20							X	X	X	X	X	X				
21													X	X		
22															X	X

X = Trip Inhibiting Failure

FIGURE 4.3

FAILURE COMBINATIONS REQUIRED TO INHIBIT RT#2

TABLE 4.5 (cont'd)

Failed Component	Failure Mode	Failure Effect
Bistable trip unit output relay K1, K2, or K3	Fails to energized state (hung up)	Coincidence logic matrix input relay circuit fails to untripped state. See Table 4.3 for specific relay/logic matrix schedule.
Logic matrix output relay (e.g., AB1, AB2, AB3, or AB4) M coil M1, M2, M3, or M4	Fails to energized state (hung up) Fails to energized state (hung up)	Clutch power supply train fails to untripped state.

4.2.1.4 Low Water Level, Steam Generator 1 (RT#4)

The RT#4 function was previously described in Section 3.3.4. The grouping of the major functional elements, which could fail to a non-tripped condition and inhibit this required protective RT, is similar to that presented in Section 4.2.1.3 for RT#3. Table 4.6 presents a summary of the RT#4 FMEA (Appendix A, Tables A-4 and A-13) and lists the appropriate functional element component failure. Figure 4.2 shows the combinations of major functional element failures which would have to occur to inhibit a RT on low water level, steam generator 1 (RT#4).

4.2.1.5 Low Water Level, Steam Generator 2 (RT#5)

The RT#5 function was previously described in Section 3.3.4. The complement of equipment associated with the RT#5 function is identical to that presented for the RT#4 function in Section 4.2.1.4. The analysis summarized in Section 4.2.1.4 is directly applicable to the RT#5 function. The RT#5 FMEA is presented in Appendix A, Table A-5.

4.2.1.6 Low Pressure, Steam Generator 1 (RT#6)

The RT#6 function was previously described in Section 3.3.5. The grouping of the major functional elements, which could fail to a non-tripped condition and inhibit this required protective RT, is similar to that presented in Section 4.2.1.3 for RT#3. Table 4.7 presents a summary of the RT#6 FMEA (Appendix A, Tables A-6 and A-13) and lists the appropriate functional element component failures. Figure 4.2 shows the combinations of major functional element failures which would have to occur to inhibit a RT on low pressure, steam generator 1 (RT#6).

4.2.1.7 Low Pressure, Steam Generator 2 (RT#7)

The RT#7 function was previously described in Section 3.3.5. The complement of equipment associated with the RT#7 function is identical to that presented for

TABLE 4.6

FMEA SUMMARY FOR RT#4

Failed Component	Failure Mode	Failure Effect
Channel SG level transmitter " " Bistable trip unit RT#4 channel bypass switch	Fail high Output signal constant Loss of low pressure tap input Fails untripped Fail closed	Sensor/RPS channel functional element fails to the untripped state.
Bistable trip unit output relay K1, K2, or K3	Fails to energized state (hung up)	Coincidence logic matrix input relay circuit fails to untripped state. See Table 4.3 for specific relay/ logic matrix schedule.
Logic matrix output relay (e.g., AB1, AB2, AB3, or AB4) M coil M1, M2, M3, or M4	Fails to energized state (hung up) Fails to energized state (hung up)	Clutch power supply train fails to untripped state.

TABLE 4.7

FMEA SUMMARY FOR RT#6

Failed Component	Failure Mode	Failure Effect
Channel SG pressure transmitter "	Fail high Output signal constant	Sensor/RPS channel functional element fails to untripped state.
Bistable trip unit	Fail Untripped	
RT#6 channel bypass switch	Fail closed	
Bistable trip unit output relay K1, K2, or K3	Fails to energized state (hung up)	Coincidence logic matrix input relay circuit fails to untripped state. See Table 4.3 for specific relay/logic matrix schedule.
Logic matrix output relay (e.g., AB1, AB2, AB3, or AB4)	Fails to energized state (hung up)	Clutch power supply train fails to untripped state.
M coil M1, M2, M3, or M4	Fails to energized state (hung up)	

the RT#6 function in Section 4.2.1.6. The analysis summarized in Section 4.2.1.6 is directly applicable to the RT#6 function. The RT#7 FMEA is presented in Appendix A, Table A-7.

4.2.1.8 High Pressurizer Pressure (RT#8)

The RT#8 function was previously described in Section 3.3.6. The grouping of the major functional elements, which could fail to a non-tripped condition and inhibit this required protective RT, is similar to that presented in Section 4.2.1.3 for RT#3. Table 4.8 presents a summary of the RT#8 FMEA (Appendix A, Tables A-8 and A-13) and lists the appropriate functional element component failures. Figure 4.2 shows the combinations of major functional element failures which would have to occur to inhibit a RT on high pressurizer pressure (RT#8).

4.2.1.9 Thermal Margin/Low Pressure (RT#9)

The RT#9 function was previously described in Section 3.3.7. The grouping of the major functional elements, which could fail to a non-tripped condition and inhibit this required protective RT, is similar to that presented in Section 4.2.1.3 for RT#3. Table 4.9 presents a summary of the RT#9 FMEA (Appendix A, Tables A-9 and A-13) and lists the appropriate functional element component failures. Figure 4.2 shows the combinations of major functional element failures which would have to occur to inhibit a RT on thermal margin/low pressure (RT#9).

4.2.1.10 Loss of Load, Turbine Trip (RT#10)

The RT#10 function was previously described in Section 3.3.8. For the purpose of this analysis, the system components were grouped into the following major functional elements which could fail to a non-tripped condition and inhibit the anticipatory RT.

TABLE 4.8

FMEA SUMMARY FOR RT#8

Failed Component	Failure Mode	Failure Effect
Channel pressurizer pressure transmitter	Fail low[1]	Sensor/RPS channel functional element fails to the untripped state.
"	Output signal constant	
"	Loss of high pressure tap[2]	
"	Open signal line[1]	
Transmitter power supply	Loss of output[1]	
"	Loss of supply voltage from preferred AC bus[1]	
Bistable trip unit	Fail untripped	
RT#8 channel bypass switch	Fail closed	
Bistable trip unit output relay K1, K2, or K3	Fails to energized state (hung up)	Coincidence logic matrix input relay circuit fails to untripped state. See Table 4.3 for specific relay/ logic matrix schedule.

Notes:

1. The failure will inhibit an RT#8 channel trip but will propagate a RT#9 channel trip (low pressure).
2. In addition to generating an RT#9 channel trip, the failure (e.g., ruptured sensing line) will cause a sudden drop in the primary coolant system pressure and thus generate a scram on low primary coolant pressure (RT#9).

TABLE 4.8 (cont'd)

Failed Component	Failure Mode	Failure Effect
Logic matrix output relay (e.g., AB1, AB2, AB3, or AB4)	Fails to energized state (hung up)	Clutch power supply train fails to untripped state.
M coil M1, M2, M3, or M4	Fails to energized state (hung up)	

TABLE 4.9

FMEA SUMMARY FOR RT#9

Failed Component	Failure Mode	Failure Effect
Channel pressurizer pressure transmitter	Fail high[1]	Sensor/RPS channel functional element fails to the untripped state.
"	Output signal constant	
TM/low pressure bistable trip unit	Fail untripped	
"	Variable setpoint signal fails low	
"	Constant setpoint signal	
Setpoint auctioneer	Open output signal line	
RT#9 channel bypass switch	Fail closed	
Bistable trip unit output relay Kl, K2, or K3	Fails to energized state (hung up)	Coincidence logic matrix input relay circuit fails to untripped state. See Table 4.3 for specific relay/ logic matrix schedule.
Logic matrix output relay (e.g., ABl, AB2, AB3, or AB4)	Fails to energized state (hung up)	Clutch power supply train fails to untripped state.
M coil Ml, M2, M3, or M4	Fails to energized state (hung up)	

Note: 1. The failure will inhibit an RT#9 channel trip but will propagate a RT#8 channel trip (high pressure).

- o Sensor Train
- o Auxiliary relays
- o RPS channels
- o Logic matrix input relays
- o Clutch power supply trains.

The first functional element, sensor train, includes all components from the sensor to the turbine trip auxiliary relays. The second functional element is the turbine trip auxiliary relays. The third element includes all components from the auxiliary relay contact pairs to the auxiliary trip unit output relays. The logic matrix input relay and clutch power supply train functional elements include the same equipment complement that was previously defined for RT#1 through RT#9.

Table 4.10 presents a summary of the RT#10 FMEA (Appendix A, Tables A-10 and A-13) and lists the possible component failures which would propagate a non-tripped state in a major functional element. Figure 4.4 shows the combinations of major functional element failures which would have to occur to inhibit a RT on loss of load, turbine trip (RT#10).

4.2.1.11 High Containment Pressure (RT#11)

The RT#11 function was previously described in Section 3.3.9. The grouping of the major functional elements, which could fail to the non-tripped condition and inhibit this required protective RT, is similar to that presented in Section 4.2.1.1 for RT#1. Table 4.11 presents a summary of the RT#11 FMEA (Appendix A, Tables A-11 and A-13) and lists the appropriate functional element component failures. Figure 4.2 shows the combinations of major functional element failures which would have to occur to inhibit a RT on containment high pressure (RT#11).

TABLE 4.10

FMEA SUMMARY FOR RT#10

Failed Component	Failure Mode	Failure Effect
Pressure switch, turbine auto stop Time delay relay Turbine trip relay power source (125 VDC pnl D21, bkr 72-212) " "	Contacts fail open Contacts fail open Loss of output Short across source Open output line	Sensor train functional equipment fails to untripped state.
Turbine trip relay 305R or 305L	Fails to de-energized state	Auxiliary relays fail to untripped state.
Auxiliary trip unit RT#10 channel bypass switch	Fails untripped Fails closed	RPS channel functional element fails to untripped state.
Auxiliary trip unit output relay K1, K2, or K3	Fails to energized state (hung up)	Coincidence logic matrix input relay circuit fails to untripped state. See Table 4.3 for specific relay/logic matrix schedule.

TABLE 4.10 (cont'd)

Failed Component	Failure Mode	Failure Effect
Logic matrix output relay (e.g., AB1, AB2, AB3, or AB4)	Fails to energized state (hung up)	Clutch power supply train fails to untripped state.
M coil M1, M2, M3, or M4	Fails to energized state (hung up)	

RPS Failure Array ID No.	Sensor Train	Aux. Relay		RPS Channels				Logic Matrix Input Relays						Clutch Power Supply Trip Train			
		L	R	A	B	C	D	AB	AC	AD	BC	BD	CD	1	2	3	4
1	X																
2		X	X														
3		X			X												
4		X					X										
5			X	X													
6			X			X											
7				X	X	X											
8				X		X	X										
9				X	X		X										
10					X	X	X										
11				X	X								X				
12				X		X						X					
13				X			X				X						
14					X	X				X							
15					X		X		X								
16						X	X	X									
17				X							X	X	X				
18					X				X	X			X				
19						X		X		X		X					
20							X	X	X		X						
21								X	X	X	X	X	X				
22														X	X		
23																X	X

X = Trip Inhibiting Failure

FIGURE 4.4

FAILURE COMBINATIONS REQUIRED TO INHIBIT RT#10

TABLE 4.11

FMEA SUMMARY FOR RT#11

Failed Component	Failure Mode	Failure Effect
Channel pressure switch " Auxiliary trip unit RT#11 channel bypass switch	Fails low Open sense line Fails untripped Fails closed	Sensor/RPS channel functional element fails to untripped state.
Auxiliary trip unit output relay K1, K2, or K3	Fails to energized state (hung up)	Coincidence logic matrix input relay circuit fails to untripped state. See Table 4.3 for specific relay/logic matrix schedule.
Logic matrix output relay (e.g., AB1, AB2, AB3, or AB4) M coil M1, M2, M3, or M4	Fails to energized state (hung up) Fails to energized state (hung up)	Clutch power supply train fails to untripped state.

4.2.1.12 Manual (RT#12)

The manual reactor trip function (RT#12) was analyzed to determine if the failure of any equipment associated with this function could inhibit an automatic scram actuated by RT functions #1 through #12. The analysis, which is documented in Appendix A, Table A-12, disclosed that the failure of any single device associated with the RT#12 function would not degrade the capability of the RPS to initiate an automatic scram.

4.2.2 CMFA During Transient

The second step in the CMFA evaluates the overall effect of potential CMF's on the integrated RPS responsiveness to the following anticipated reactor transients.

1. Loss of electrical load
2. Load increase
3. Loss of feedwater
4. Loss of primary flow
5. Loss of normal electrical power
6. Inactive primary loop startup
7. Rod withdrawal
8. Primary system depressurization
9. Boron dilution
10. Small line break.

The Combustion Engineering (CE) Topical Report (Reference 2) was evaluated for each of the postulated ATWS events to determine the severity of the consequences and the potential scrams available at the Palisades Plant that would interrupt the transient. The ATWS consequences calculated for the generic plant in the CE Topical Report are more severe than the consequences propagated by a similar event at the Palisades Plant. The parameters that differ between the Palisades Plant and the CE generic plant which are significant in reducing the severity of the hypothesized transients at the Palisades Plant are:

- Rated thermal power
- Operating pressure
- Pressurizer relief area
- Pressurizer water volume.

Rated thermal power for the Palisades Plant is 2200 Mwt (2560 Mwt for the CE generic plant). Operating RCS pressure for the Palisades Plant is 1800 psia (2250 psia for the CE generic plant). Total relief area for the Palisades Plant is 0.076 ft^2 (0.0541 ft^2 for the CE generic plant). Both the Palisades Plant and the CE generic plant have a total primary pressurized volume of 1500 ft^3. However, the pressurizer water volume is 540 ft^3 for the Palisades Plant as compared to 769 ft^3 for the CE generic plant. The peak primary coolant system pressures calculated for the generic plant during an ATWS are significantly higher than that expected for the Palisades Plant. Figure 4.1, which presents a summary of the RT modes available during each of the ATWS events, provided the integrated RPS design baseline for the CMFA. The generic causes of potential RPS CMF's and the preventive measures existing at Palisades were analyzed and evaluated for each of the postulated transients. The results of the integrated CMFA's are summarized in the following sections.

4.2.2.1 Loss of Electrical Load

The postulated loss of electrical load transient could be caused by generator trip, loss of condenser vacuum, or turbine trip. Loss of condenser vacuum or generator trip will propagate a turbine trip. The most probable cause of the loss of load transient is a turbine trip. After turbine trip, low auto stop oil pressure immediately generates a RT#10 signal. On turbine trip, the turbine isolation valves will close, rapidly increasing secondary pressure and causing the safety valves to open. Due to the decrease in heat transfer capability to the secondary system and the accompanying increase in coolant temperature, the primary pressure will rapidly increase. During the first few seconds of the transient, high pressurizer pressure trip signals will be generated (RT#8) and the pressurizer relief valves will open.

Initially, primary system pressure will increase and it will continue to increase until it peaks at approximately 180 seconds into the transient and then subsequently decreases.

At 600 seconds the operator manually actuates the Safety Injection Actuation Signal (SIAS). The concentrated boron solution will reach the reactor core in approximately 150 seconds and initiate reactor shutdown. At 600 seconds the operator manually actuates the auxiliary feedwater system, which has the capacity of 6% of full power feedwater flow. This will remove the decay heat from the reactor core.

During the initial phase of the transient, steam dump to atmosphere and steam bypass to the condenser (if there is no loss of vacuum) are available to remove energy from the primary coolant system. If no credit is taken for the steam dump and condenser bypass, the pressurizer relief and safety valves in conjunction with the steam generator safety valves and the feedwater system provide an adequate means to remove heat and make the transient consequences acceptable.

The peak reactor coolant system (RCS) pressure generated during this transient will not exceed 2534 psia at the Palisades Plant (Reference 6). The peak RCS pressure does not exceed either the RCS safety limit (2750 psia) or the RCS hydrostatic test limit (3125 psia) for the Palisades Plant (Reference 3). The peak pressure developed during this transient may rupture the pressurizer quench tank rupture disk and pressurize the containment. If the high containment pressure reaches the setpoint for RT#11 and SIAS (5 psig) before 600 seconds into the transient, an automatic SIAS and RT#11 would be independently actuated.

During the course of this transient no unacceptable consequences are reached. The primary coolant system pressure does not exceed the safety limits. The limits. The minimum transient DNBR in the hot channel remains greater than 1.3 and no fuel damage occurs. Containment pressure is controlled by an automatic and independent SIAS if the high pressure setpoint of 5 psig is achieved during the transient. Two reactor trip signals, turbine trip and high pressurizer pressure, would be generated by the RPS early in the transient. High containment pressure RT and SIAS signals may be generated prior to 600 seconds.

Table 4.1 presents a summary of preventive measures which have been successfully utilized to prevent CMF's. Specific preventive measures provided by the existing RPS against the various generic causes of CMF's are discussed in the following paragraphs.

Functional Deficiencies: Both functional diversity and equipment diversity exist in the RPS design. Two independent RT modes (high pressurizer pressure and turbine trip) which monitor dissimilar plant operating parameters can initiate a scram early in the transient. Both RT's are initiated by a change in pressure (turbine auto stop oil pressure and pressurizer pressure), however, the means of generating each RT signal is different. The high pressurizer pressure scram signal is developed by a bistable trip unit which monitors an analog pressure signal generated by a force balance pressure transmitter. The turbine trip scram signal is generated when the turbine auto stop

pressure switch contacts close on low pressure and energize the turbine trip relays. The actual scram signal to the RT coincidence logic matrix is generated by an auxiliary trip unit which monitors the turbine trip relay contacts. No credit was taken for the enhanced RPS functional and equipment diversity available from the high containment pressure RT because containment overpressurization may not exceed 5 psig.

Design or Manufacturing Deficiencies: The functional and equipment diversity discussed in the preceding paragraph is the primary defense against design or manufacturing deficiencies. However, no credit can be taken for equipment diversity between the output relays in either the auxiliary trip units (ATU's) or the bistable trip units (BTU's) through the M coils, because all components that have an identical function in the RPS RT train (e.g., trip unit output relays, logic matrix trip relays, M coils, ...), have similar design and/or performance specifications. Protection against CMF's due to design or manufacturing deficiencies of the above components is achieved by periodic testing which ensures that all the equipment is operational and would be responsive to valid scram signals.

Operating or Maintenance Errors: The functional and equipment diversity between RT#8 and RT#10 is reflected in the differences in calibration and maintenance procedures. No single common mode error was hypothesized that could inhibit both of the RT modes responsive to the loss of electrical load transient.

External Phenomena: External phenomena such as fire, flood, missile, and earthquake could propagate the following effects on the RPS.

- Loss of sensor channel signal
- Severance of sense line
- Open circuiting of sensor channel cables

o Loss of RPS channel signal

o Loss of power.

The effect of these hypothesized functional system level failures was evaluated for each RT mode. The results are summarized in Table 4.12.

The RPS is not vulnerable to CMF's caused by external phenomena during the loss of electrical load transient due to the available safe failure modes, physical separation, functional diversity, and equipment diversity. Even if no credit is taken for the actual separation and isolation that exists in the RPS design, Table 4.12 shows that no single hypothesized generic failure could inhibit both RT#8 and RT#10 due to the complementary safe failure modes.

External Normal Environment: Proven hardware and design concepts have been incorporated as part of the RPS design philosophy. Standard, reliable equipment or components have been included throughout the RPS design. The operating envelope design specifications for all RPS equipment are compatible with both the plant environment during normal operation and the environment propagated by the anticipated reactor transients. In addition to the standardization of components with proven designs, the following measures, which are recognized preventive measures against CMF's propagated by external normal environment, are normally part of the Palisades Plant RPS design and/or part of the day-to-day plant operation routine.

o Functional diversity

o Design administrative controls

o Operational administrative controls

o Safe failure modes

o Equipment diversity.

TABLE 4.12

EFFECT OF EXTERNAL PHENOMENA ON THE RPS

Reactor Trip Mode	Possible Failures				
	Loss of Sensor Channel Signal	Severance of Sense Line	Open Circuiting of Sensor Cables	Loss of RPS Channel Signal	Loss of Trip Circuit Power Supply
1. High Power Level	NT	NA	NT	CT	CT
2. High Power Rate of Change	NT	NA	NT	CT	CT
3. Low Flow, Reactor Coolant	CT	RTA	CT	CT	CT
4. Low Water Level, SG1	CT	CTB	CT	CT	CT
5. Low Water Level, SG2	CT	CTB	CT	CT	CT
6. Low Pressure, SG1	CT	CT	CT	CT	CT
7. Low Pressure, SG2	CT	CT	CT	CT	CT
8. High Pressurizer Pressure	CTA	RTA	CTA	CT	CT
9. Thermal Margain/Low Pressure	CT	RTA	CT	CT	CT
10. Loss of Load, Turbine Trip	NT	RT	NT	CT	CT
11. High Containment Pressure	NT	NT	CT	CT	CT

CT = Failure causes RPS channel trip

RT = Failure causes reactor trip

NT = Failure inhibits RPS channel trip

NA = Not applicable

RTA = Failure causes RT #9 due to low primary pressure

CTA = Failure causes RT #9 channel trip

CTB = Failure causes channel trip if both lines are severed

No CMF, caused by external normal environment, was hypothesized which would inhibit any automatic reactor trip mode (RT#1 through RT#11).

4.2.2.2 Load Increase

The load increase transient, which was analyzed in the CE Topical Report (Reference 2), was initiated by the accidental opening of the steam dump and bypass valves which will relieve 45% of full power steam flow. The transient consequences are less severe for the Palisades Plant because the accidental opening of the steam dump and bypass valves will not relieve more than 40% of full power steam flow. The load increase transient will immediately propagate a high power level trip signal (RT#1). The thermal margin/low pressure trip (RT#9) signals will be generated during the intermediate period of the transient.

Similar to the loss of electrical load transient, the operator will manually initiate safety injection at 600 seconds. After safety injection, reactor power will sharply decrease, and primary coolant pressure will decrease to a level which will generate the low pressurizer pressure trip signals. Simultaneously with the decrease in coolant pressure, the steam generator level and pressure will decrease and ultimately low steam generator level and pressure trip signals will occur (RT#4, #5, #6, and #7). The main steam isolation valves will also close on low pressure signals from any two of the four meter relays associated with either steam generator. A turbine trip will result and generate RT#10 signals.

The consequences of the load increase transient are mild. The power excursion is limited by the negative power coefficient and the minimum transient DNBR in the hot channel will remain well above 1.3. Since the effect propagated by the transient is mild, only one RT mode, high power level (RT#1), will be initiated early in the transient. During the intermediate period of the transient, the thermal margin/low pressure trip (RT#9) is initiated. Late in the transient, after the manual actuation of safety injection, five RT modes will

be initiated; low level-steam generator 1 and 2, low pressure-steam generator 1 and 2 and turbine trip. The CMFA will only take credit for RT#1 and RT#9 because the remaining RT's occur so late in the transient. Specific preventive measures provided by the existing RPS against the various causes of CMF's are discussed in the following paragraphs.

Functional Deficiencies: Two independent RT modes, high power level and thermal margin/low pressure, which monitor dissimilar plant operating parameters, can initiate a scram prior to operator intervention 600 seconds into the transient. These trip modes provide both functional and equipment diversity in the RPS equipment during this transient. The high power level scram signals are developed by bistable trips in the RPS nuclear instrumentation system (NIS) drawers. RPS ATU's which monitor the bistable outputs will trip and propagate the RT#1 scram signal to the RPS trip logic matrix. The thermal margin/low pressure scram signal is developed by a BTU which monitors an analog pressure signal generated by a force balance pressure transmitter. The BTU has a variable trip setpoint which is automatically determined by the hot and cold leg temperatures of the primary coolant loops.

Design or Manufacturing Deficiencies: The functional and equipment diversity discussed in the preceding paragraph is the primary defense against design or manufacturing deficiencies. For the reasons discussed for the loss of electrical load transient, the RPS design between the trip unit output relays and the M coils is vulnerable to design and manufacturing deficiencies. As before, protection against CMF's, caused by these deficiencies, is achieved by periodic testing which ensures that all the equipment is operational and would be responsive to valid scram signals.

Operating and Maintenance Errors: The functional and equipment diversity between RT#1 and RT#9 is reflected in differences in calibration and maintenance procedures. No single common mode error was hypothesized that could inhibit the RT modes responsive to the load increase transient before operator

intervention. It should be noted that an operator error could delay the actuation of RT#1 if the operating plant configuration changed from four coolant pump operation to three and the flow trip select switch was left in the four pump position. While RT#1 could be delayed if the transient occurred simulataneouly with change in pump configuration, the low coolant flow trip (RT#3) would be immediately initiated due to the operator error.

External Phenomena: The RPS is not vulnerable to CMF's caused by external phenomena during the load increase transient due to the available safe failure modes, physical separation and equipment diversity. Even if no credit is taken for the actual separation and isolation that exists in the RPS design, Table 4.12 shows that no single hypothesized generic failure could inhibit both RT#1 and RT#9 due to the complementary safe failure modes.

External Normal Environment: The discussion presented for the loss of electrical load transient (Section 4.2.2.1) is applicable for all the ATWS events.

4.2.2.3 Loss of Feedwater

The loss of feedwater transient was analyzed for two conditions. The first analysis considered partial loss (50%) of feedwater. The second analysis considered the more severe reactor transient, total loss of feedwater.

At the beginning of the partial loss of feedwater transient, steam generator water level will drop in the affected steam generator and initiate the low level trip (either RT#4 or #5). Due to the increase in primary coolant temperature and pressure, the reactor power level will decrease slightly. Once the affected steam generator inventory decreases to the point that the heat transfer coefficient from the primary to secondary decreases, reactor power will decrease at a higher rate until a new equilibrium level of approximately 70% is achieved. A high pressurizer pressure RT signal will be initiated prior to 600 seconds into the transient. The consequences of the partial loss of feedwater transient are not severe. The reactor power level will achieve equilibrium at a new, lower level once the initial transient effects have diminished.

The total loss of feedwater is a severe reactor transient. The CMFA will evaluate the RPS vulnerability to CMF's during the total loss of feedwater transient. The initial reactor response to this transient is similar to that discussed for the partial loss of feedwater transient. At the beginning of the transient a low steam generator water level RT signal will be generated by both steam generators.

Similar to the partial loss of feedwater transient, the heat transfer from primary to secondary starts decreasing as a result of the decrease in steam generator inventory. The primary coolant temperature will increase and reactor power will decrease until a new equilibrium level is achieved at decay heat levels. Concurrent with the increase of reactor primary coolant temperature, the RCS pressure will increase and generate a high pressurizer pressure trip signal (RT#8). RCS pressure will continue increasing rapidly for approximately 200 seconds until a peak pressure is reached. Steam generator pressure will decrease, resulting in low steam generator pressure trip signals (RT#6 and #7) and the closing of the main steam isolation valves. The closing of the valves will generate a turbine trip and the associated scram (RT#10). The thermal margin/low pressure trip signals will also be generated prior to 600 seconds into this severe reactor transient.

The RCS pressure calculated for the CE generic plant during the loss of feedwater transient achieved a maximum value of 3406 psia. Due to the differences between the CE generic and the Palisades Plant which were discussed in Section 4.2.2, the consequence of the loss of feedwater transient for the Palisades Plant is less severe. It is concluded that the peak RCS pressure should not exceed the Palisades Plant RCS hydrostatic test limit of 3125 psia.

The total loss of feedwater transient also propagates the maximum energy release to the primary containment. Discharge through the pressurizer valves will cause the quench tank rupture disk to open and vent into containment. The resultant containment overpressurization will not exceed design limits. No fuel melting or fuel clad damage will occur during this severe transient.

Specific preventive measures provided by the existing RPS against the various causes of CMF's are discussed in the following paragraphs.

Functional Deficiencies: Two RT modes (RT#4 and #5), initiated by low steam generator level, are available to scram the reactor early in the transient. Functional diversity and equipment diversity are achieved by the numerous trip modes listed below, which monitor dissimilar plant operating parameters and can initiate a scram prior to possible operator intervention 600 seconds into the transient.

- o High pressurizer pressure (RT#3)
- o Low steam generator pressure (RT#6 and #7)
- o Turbine trip (RT#10)
- o Thermal margin/low pressure (RT#9)
- o High containment pressure (RT#11).

Design or Manufacturing Deficiencies: The functional and equipment diversity denoted in the preceding paragraph is the primary defense against design or manufacturing deficiencies. The RPS design between the trip unit output relays and the M coils are vulnerable to design and manufacturing deficiencies. As discussed in Section 4.2.2.1, protection against CMF's caused by these deficiencies is achieved by periodic testing which ensures that all equipment is operational and would be responsibe to valid scram signals.

Operating and Maintenance Errors: The functional and equipment diversity derived from all the trip modes responsive to the complete loss of feedwater transient is reflected in differences in calibration and maintenance procedures. No single common mode operating or maintenance error was hypothesized that could inhibit all trip modes responsive to this transient.

External Phenomena: The RPS is not vulnerable to CMF's caused by external phenomena during the complete loss of feedwater transient due to the available safe failure modes, physical separation and equipment diversity. Even if no credit is taken for the actual separation and isolation that exists in the RPS design, Table 4.12 shows that due to the complementary failure modes existing in the RPS design, no single hypothesized generic failure could inhibit all the trip modes responsive to the transient (RT#4, #5, #6, #7, #8, #9, #10, and #11).

External Normal Environment: The discussion presented for the loss of electrical load transient (Section 4.2.2.1) is applicable for all the ATWS events.

4.2.2.4 Loss of Primary Flow

The loss of all coolant pumps was the hypothesized cause for the loss of primary flow transient. During the period of pump coastdown, a low coolant flow trip signal (RT#3) is generated. Primary coolant pressure and temperature will increase and reactor power will decrease during the period of decreasing flow and generate the high pressurizer pressure trip signals (RT#8). The minimum transient hot channel DNBR is also achieved during this period. The minimum DNBR drops below 1.4 but does not achieve the 1.3 threshold. The reactor power level becomes stable at approximately 80% of full power once the natural coolant flow is established.

600 seconds into the transient the operator manually actuates the SIS. The concentrated boron solution will reach the reactor core in approximately 150 seconds and initiates a reactor shutdown. After SI, reactor power decreases rapidly and stabilizes at decay heat levels. Later in the transient, thermal margin/low pressure, low steam generator level, low steam generator pressure and turbine trip signals are generated. The turbine trip is caused by the closure of the main steam isolation valves.

The consequences of this transient are mild. The peak RCS pressure is well below the design limits and the minimum hot channel DNBR is in excess of the 1.3 threshold. The CMFA will only take credit for RT#3 and RT#8 because the remaining RT's occur so late in the transient. Specific preventive measures provided by the existing RPS against the various causes of CMF's are discussed in the following paragraphs.

Functional Deficiencies: Two independent RT modes, high pressurizer pressure and low coolant flow, which monitor dissimilar plant operating parameters are available to scram the reactor early in the transient. These trip modes provide both functional diversity and equipment diversity during this transient. The sensors associated with each trip mode are of the generic force balance transmitter classification. The transmitters and power supplies associated with each trip mode are not only different models, but they are manufactured by different companies. No CMF, caused by functional deficiencies, was hypothesized which would inhibit the actuation of RT#3 and RT#8 during the loss of primary flow transient.

Design or Manufacturing Deficiencies: The functional and equipment diversity discussed in the preceding paragraph is the primary defense against CMF's caused by design or manufacturing deficiencies. Some portions of the RPS design are vulnerable to CMF's caused by design or manufacturing deficiencies. This subject was discussed in detail during the analysis of the loss of electrical load transient (Section 4.2.2.1).

Operating and Maintenance Errors: The functional and equipment diversity between RT#3 and RT#8 is reflected in differences in calibration and maintenance procedures. No single common mode error was hypothesized that could inhibit the RT modes responsive to the loss of primary flow transient before operator intervention. It should be noted that an operator error could delay the actuation of RT#3 if the operating plant configuration changed from three coolant pump operation to four and the flow trip select switch was left in the

three pump position. While RT#3 could be delayed if the transient occurred simultaneously with change in pump configuration, the high power level trip (RT#1) would be immediately initiated due to the operator error.

External Phenomena: The RPS is not vulnerable to CMF's caused by external phenomena during the loss of primary flow transient due to the available safe failure modes, physical separation and equipment diversity. Even if no credit is taken for the actual separation and isolation that exists in the RPS design, Table 4.12 shows that no single hypothesized generic failure could inhibit both RT#3 and RT#8 due to the complementary safe failure modes.

External Normal Environment: The discussion presented for the loss of electrical load transient (Section 4.2.2.1) is applicable for all the ATWS events.

4.2.2.5 Loss of Normal Electrical Power

Upon loss of normal electrical power a turbine trip will occur and initiate the reactor trip signals (RT#10). Shortly thereafter, the low coolant flow trip signals (RT#3) will also occur. In the following seconds both low steam generator level trip signals (RT#4 and #5) and high pressurizer pressure signals (RT#8) occur. The emergency diesel generators start automatically and within 30 seconds will be capable of carrying full load.

The reactor power level will start decreasing and primary coolant pressure will increase. As a result of the increase in primary coolant pressure, the pressurized quench tank rupture disk will open and the containment will begin to pressurize. This will eventually result in the high containment pressure reactor trip signal (RT#11) and an automatic SIAS at approximately 300 seconds. Once the boron reaches the mid-core the transient is essentially terminated.

The increase in reactor coolant temperatures and pressures is terminated prior to the automatic SIAS due to a combination of reduced heat generation-steam

flow mismatch and reactor coolant flow stabilization at natural circulation levels. Late in the transient, thermal margin/low pressure trip signals (RT#9) will occur. During the initial portion of this transient the hot channel DNBR undergoes a rapid decrease as a result of the increased reactor coolant temperature combined with the decreased reactor coolant flow. The resultant minimum DNBR will be slightly less than 1.3.

The RCS pressure calculated for the CE generic plant during the loss of normal electrical power transient reached a maximum value of 2985 psia which is less than the Palisades Plant RCS hydrostatic test limit of 3125 psia. The consequence of the loss of normal electrical power transient for the Palisades Plant is less severe due to the differences between the CE generic plant and the Palisades Plant. These differences are presented in Section 4.2.2.

Analysis of this transient assumed that manual action is taken, based on emergency procedures, to 1) actuate the steam generator atmosphere dump valves 20 minutes subsequent to initiation of the transient, and 2) cool the plant by means of the atmosphere dump valves, to a hot standby temperature of 525F in less than 45 minutes subsequent to initiation of the transient, the maximum possible radioactivity release was determined to be less than the limits given in 10CFR100. During this analysis, it was also assumed that 1) AC offsite power is not restored and action is initiated to put the plant in a cold shutdown condition; 2) Atmosphere release is required until the reactor coolant temperature is reduced to the point where shutdown cooling can be initiated at 300F; 3) The shutdown cooling system is employed to remove decay heat, thus terminating release of steam.

Specific preventive measures provided by the existing RPS against the various causes of CMF's are discussed in the following paragraphs.

Functional Deficiencies: Functional diversity and equipment diversity are achieved by the numerous trip modes listed below, which monitor dissimilar plant operating paramters and can initiate a scram early in the transient.

- High pressurizer pressure (RT#8)
- Low coolant flow (RT#3)
- Low steam generator level (RT#4 and #5)
- Turbine trip (RT#10)

Design or Manufacturing Deficiencies: The functional and equipment diversity denoted in the preceding paragraph is the primary defense against CMF's caused by design or manufacturing deficiencies. Some portions of the RPS design are vulnerable to CMF's caused by design or manufacturing deficiencies. This subject was discussed in detail during the analysis of the loss of electrical load transient (Section 4.2.2.1).

Operating and Maintenance Errors: The functional and equipment diversity between RT#3, #4, #5, #8 and #10 are reflected in differences in calibration and maintenance procedures. No single common mode error was hypothesized that could inhibit all of the RT modes responsive to the loss of normal electrical power transient. It should be noted that an operator error could delay the actuation of RT#3 if the operating plant configuration changed from three coolant pump operation to four and the flow trip select switch was left in the three pump position. While RT#3 could be delayed if the transient occurred simultaneously with change in pump configuration, the high power level trip (RT#1) would be immediately initiated due to the operator error.

External Phenomena: The RPS is not vulnerable to CMF's caused by external phenomena during loss of normal electrical power transient due to the available safe failure modes, physical separation and equipment diversity. Even if no credit is taken for the actual separation and isolation that exists in the RPS design, Table 4.12 shows that no single hypothesized generic failure could inhibit all of the available trip modes due to the complementary safe failure modes.

External Normal Environment: The discussion presented for the loss of electrical load transient (Section 4.2.2.1) is applicable for all the ATWS events.

4.2.2.6 Inactive Primary Loop Startup

The analysis of this transient postulated that the reactor had one loop idle and two pumps in operation. Reactor power was 50% of rated power. The analysis disclosed (Reference 2) that the reactor power level would increase and achieve equilibrium at a new higher level after an inactive loop startup. The only trip mode responsive to this transient is the high power level trip (RT#1). The inactive primary loop transient is very mild. No fuel limits are exceeded.

Since the transient is so mild the resultant perturbation to primary reactor operating parameters is not excessive. Only one parameter (reactor power) traverses outside of the normal operating envelope and initiates scram signals. Since only one trip mode is responsive to this mild transient, no functional diversity or equipment diversity can exist. Table 4.2 presents a listing of equipment failures which would inhibit a RT#1 RPS channel trip. Based on the data presented in Table 4.2, numerous CMF's could be hypothesized which would inhibit the actuation of RT#1. No attempt was made to even evaluate the credibility of any hypothesized CMF because their consequence is not significant.

4.2.2.7 Rod Withdrawal

The rod withdrawal from full power is another mild transient. The rod withdrawal takes place at a relatively slow speed. The high power trip signal (RT#1) does not occur until approximately 90 seconds after the start of the transient. Subsequently, the high pressurizer pressure trip signal (RT#8) is initiated. Once rod withdrawal ceases, the reactor power achieves a new equilibrium at a higher power.

600 seconds into the transient the operator initiates the SIAS. When the boron reaches the mid-core, approximately 150 seconds later, reactor power starts decreasing and eventually achieves a new equilibrium at decay heat levels. The RCS pressure decreases and a thermal margin/low pressure trip signal (RT#9) will also occur. The low steam generator pressure trips (RT#6 and #7) will also occur and the main steam isolation valve will close, tripping the turbine and causing a reactor trip (RT#10) signal. Finally, a low steam generator water level trip signal will occur.

The consequences of this transient are mild. RCS pressure will not exceed design limits and the minimum hot channel DNBR during the transient will remain well above the 1.3 threshold.

The CMFA will only take credit for RT#1 and RT#8 because the remaining RT's occur so late in the transient. Specific preventive measures provided by the existing RPS against the various causes of CMF's are discussed in the following paragraphs.

Functional Deficiencies: Two independent RT modes, high power level and high pressurizer pressure, which monitor dissimilar plant operating parameters can initiate a scram prior to operator intervention 600 seconds into the transient. These trip modes provide both functional and equipment diversity in the RPS equipment during this transient.

Design or Manufacturing Deficiencies: The functional and equipment diversity discussed in the preceding paragraph is the primary defense against CMF's caused by design or manufacturing deficiencies. Some portions of the RPS are vulnerable to CMF's caused by design or manufacturing deficiencies. This subject was discussed in detail during the loss of load transient (Section 4.2.2.1).

Operating and Maintenance Errors: The functional and equipment diversity between RT#1 and RT#8 is reflected in differences in calibration and maintenance procedures. No single common mode error was hypothesized that

could inhibit the RT modes responsive to the rod withdrawal transient before operator intervention. It should be noted that an operator error could delay the actuation of RT#1 if the operating plant configuration changed from four coolant pump operation to three and the flow trip select switch was left in the four pump position. While RT#1 could be delayed if the transient occurred simultaneously with change in pump configuration, the low coolant flow trip (RT#3) would be immediately initiated due to the operator error.

External Phenomena: The RPS is not vulnerable to CMF's caused by external phenomena during the rod withdrawal transient due to the available safe failure modes, physical separation and equipment diversity. Even if no credit is taken for the actual separation and isolation that exists in the RPS design, Table 4.12 shows that no single hypothesized generic failure could inhibit both RT#1 and RT#8 due to the complementary safe failure modes.

External Normal Environment: The discussion presented for the loss of electrical load transient (Section 4.2.2.1) is applicable for all the ATWS events.

4.2.2.8 Primary System Depressurization

This transient is initiated by the unexpected opening of a safety valve. During the initial period of the transient, reactor power will remain constant. RCS pressure decreases and ultimately generates a thermal margin/low pressure trip signal (RT#9). Once the pressure is reduced to the saturation point of the reactor vessel outlet plenum and hot legs, the RCS pressure and temperature will continue to decrease, but at a lower rate.

600 seconds into the transient the operator will initiate SIAS. When the boron solution reaches mid-core, approximately 150 seconds later, reactor power will rapidly decrease until a new equilibrium is established at decay heat levels. Concurrently with the decrease in power level, the steam generator pressure and water levels decrease and initiate trip signals RT#4, #5, #6, and #7. The low steam generator pressure signal will close the main steam isolation valves which will cause turbine trip and the associated scram signal (RT#10).

No unacceptable consequences are generated by this mild transient. The minimum hot channel DNBR is in excess of 2.0. The CMFA will only take credit for RT#9 because the remaining RT signals are generated late in the transient after the operator initiates SIAS. Since only one trip mode is responsive to this mild transient prior to operator intervention, no functional diversity or equipment diversity exists. Table 4.9 presents a listing of equipment failures which would inhibit a RT#9 RPS channel trip. Based on the data presented in Table 4.9, numerous CMF's could be hypothesized which would inhibit the actuation of RT#9. No attempt was made to even evaluate the credibility of any hypothesized CMF because their consequence is not significant.

4.2.2.9 Boron Dilution

As the boron dilution evolves, reactor power will increase slowly causing an increase in the RCS pressure and temperature. The resultant pressure may not be large enough to initiate the high pressurizer pressure trip signal (RT#8). The CMFA takes no credit for RT#8. The postulated boron dilution transient will propagate a high power level trip (RT#1) approximately 600 seconds into the transient.

600 seconds into the transient the operator will initiate SIAS. When the boron solution reaches mid-core, approximately 150 seconds later, reactor power will rapidly decrease until a new equilibrium is established at decay heat levels. The RCS pressure will also decrease rapidly, resulting in a thermal margin/low pressure trip (RT#9). Concurrently with the decrease in power level, the steam generator pressure and water levels decrease and initiate trip signals RT#4, #5, #6, and #7. The low steam generator pressure signal will close the main steam isolation valves which will cause turbine trip and the associated scram signal RT#10.

No unacceptable consequences are generated by this mild transient. The minimum hot channel DNBR is slightly less than 3.0. The CMFA will only take credit for RT#1 because the remaining RT signals are generated late in the

transient after the operator initiates SIAS. Since only one trip mode is responsive to this mild transient prior to operator intervention, no functional diversity or equipment diversity exists. Table 4.2 presents a listing of equipment failures which would inhibit a RT#1 RPS channel trip. Based on the data presented in Table 4.2, numerous CMF's could be hypothesized which would inhibit the actuation of RT#1. No attempt was made to even evaluate the credibility of any hypothesized CMF because their consequence is not significant.

4.2.2.10 Small Line Break

The postulated small line break transient was caused by the rupture of the largest primary instrument or sample line. The available charging flow at the Palisades Plant is not sufficient to balance the reactor coolant lost through the ruptured line. Consequently, RCS pressure and pressurizer level will increase and generate a thermal margin/low pressure trip (RT#9) signal. The reactor power level remains constant during the transient until after SIAS.

600 seconds into the transient the operator will initiate SIAS. When the boron solution reaches mid-core, approximately 150 seconds later, reactor power will rapidly decrease until a new equilibrium is established at decay heat levels. Concurrently with the decrease in power level, the steam generator pressure and water levels decrease and initiate trip signals RT#4, #5, #6, and #7. The low steam generator pressure signal will close the main steam isolation valves which will cause turbine trip and the associated scram signal (RT#10).

No unacceptable consequences are generated by this mild transient. The minimum hot channel DNBR is in excess of 3.0. The CMFA will only take credit for RT#9 because the remaining RT signals are generated late in the transient after the operator initiates SIAS. Since only one trip mode is responsive to this mild transient prior to operator intervention, no functional diversity or equipment diversity exists. Table 4.9 presents a listing of equipment failures which

would inhibit a RT#9 RPS channel trip. Based on the data presented in Table 4.9, numerous CMF's could be hypothesized which would inhibit the actuation of RT#9. No attempt was made to even evaluate the credibility of any hypothesized CMF because their consequence is not significant.

APPENDIX A

PALISADES PLANT REACTOR PROTECTION SYSTEM FAILURE MODE AND EFFECTS ANALYSIS

APPENDIX A

TABLE OF CONTENTS

LIST OF TABLES

1.0 INTRODUCTION

This Appendix presents the Failure Mode and Effects Analysis (FMEA) for the Palisades Plant Reactor Protection System (RPS). The analysis was generated to establish a baseline for evaluating the RPS vulnerability to both single and common mode failures which would inhibit a required reactor trip from going to completion.

2.0 ANALYSIS BASELINE

The RPS reactor trip modes, which are available at the Palisades Plant, are defined in Section 3.0 of the Palisades Plant Reactor Protection System Failure Analysis. The principal source of data utilized for defining the existing RPS configuration was the Palisades Plant Final Safety Analysis Report through Amendment 28 (Docket 50-255), and the Palisades Plant Technical Specifications (Revision date November 27, 1974). Detailed system drawings were utilized to supplement the documentation noted above.

3.0 ANALYSIS WORKSHEETS

To establish a basis for performing a comprehensive reactor protection system failure analysis, a complete and integrated FMEA was conducted on the RPS design. The FMEA was generated at the system level on a functional basis (i.e., signal flow level). This approach evaluates the effects of failures observable at the interfaces between RPS modules (inputs/outputs) and the effect propagated on the total system operation. The significance of each failure on system operation was considered from two aspects:

- Failure of the RPS to function when required
- Inadvertent operation of the RPS when not required.

The analysis worksheets present the following data for each hypothesized failure in a tabular format:

- Failure identification or reference number
- Description of failed component
- Failure mode at the component/system level
- Failure symptoms and local effects (dependent failures included)
- Failure detection
- Inherent compensating provisions
- Effect on RPS.

Individual RPS components, and in some instances a group of components, are assigned a reference number in the analysis worksheets (e.g., 1.0, 2.0,

3.0, ...). When more than one failure mode is applicable to a specific component a secondary level of reference is applied (e.g., 1.1, 1.2, and 1.3 reference the discussions for three failure modes associated with component 1.0). When the discussion and format of the analysis worksheets (e.g., failure symptoms and local effects, failure detection, inherent compensating provisions, and effect on the RPS) are similar or applicable for more than one component failure, the initial discussion is normally referenced in lieu of repeating an identical or similar discussion. If the total FMEA for a component (all failure modes included) is directly applicable for another component, the initial analyses are jointly referenced by the primary component reference number (e.g., 1.0).

The analysis worksheets have been grouped into 13 tables. Tables A-1 through A-12 evaluate those portions of the integrated RPS design that are unique to the 12 reactor trip modes available at the Palisades Plant. Table A-13 evaluates the RPS trip train components that are common to all modes of reactor trip.

TABLE A-1

FAILURE MODE AND EFFECTS ANALYSIS PALISADES PLANT REACTOR PROTECTION SYSTEM
REACTOR TRIP #1, HIGH POWER LEVEL

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
1.1	Uncompensated Ion Chamber A (Channel 5 Nuclear Inst. System, RPS Channel A)	Fail High	The summed output of Chamber A and B will trip the pre-trip and trip bistable units associated with 4, 3, and 2 pump system operation. This will propagate a channel trip signal from the aux. channel trip unit. One of the three pre-trip bistable units will generate a trip signal in the rod withdrawal prohibit logic.	Channel Trip and Pre-Trip Alarms for RT#1	RPS 2/4 logic inhibits spurious RT and rod withdrawal prohibit function. When the failure is diagnosed and isolated by plant personnel, the channel function may be restored by switching the failed ion chamber out of the summing circuit and doubling the signal generated by the operational ion chamber.	RT#1 logic is half tripped and changed to a 1/3 configuration.	One invalid channel trip may be bypassed for RT#1. When one channel is bypassed, RT#1 logic changes to a 2/3 configuration.
1.2	"	Fail Low	The sudden decrease of signal level will generate a dropped rod signal which will initiate turbine runback.	Dropped Rod Alarm	Only 2/4 channels are required to trip to actuate RT#1.	RT#1 logic is changed to a 2/3 configuration.	
1.3	"	Output Signal Constant	The constant signal level generated by the ion chamber will bias the summed channel output.	Flux Tilt Deviation Alarm	See 1.2. While the failure does not inhibit a channel trip, it will delay the trip until the signal level from the associated ion chamber is sufficient to compensate for the low level bias from the failed chamber.	See 1.2	
1.4	"	Short Across Signal Lines or Open Signal Line	The effect of the failure is the same as fail low (1.2).	See 1.2	See 1.2	See 1.2	
2.0	Uncompensated Ion Chamber B (Channel 5)	All Modes	Ion Chambers A and B are identical in configuration. The FMEA for Chamber A is applicable for Chamber B.				
3.0	Linear Amplifier Chamber A	All Modes	The FMEA for Chamber A (item 1.0) is applicable for all modes of the linear amplifier.				

TABLE A-1 (cont'd)

RPS FMEA REACTOR TRIP #1

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
4.0	Linear Amplifier Chamber B	All Modes	See 3.0				
5.1	High Voltage Power Supply	Loss of Output	The power supply is common to both ion Chambers A and B. The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	
5.2	"	Off Nominal Output	Both ion chambers will generate erroneous outputs. No significant operational impact unless the summed output signal is driven to an extreme condition. See 1.1 and 1.2 for details.	See 1.1 and 1.2	See 1.1 and 1.2	See 1.1 and 1.2	See 1.2
5.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #13)	All bistable units will go to the tripped state.	See 1.1	See 1.1	See 1.1	See 1.1
6.0	Power Summer	All Modes	The FMEA for ion Chamber A is applicable for all modes of the summer.				
7.0	Subchannel Comparitor (Chamber A)	All Modes	The subchannel comparitor is buffered from both ion Chamber A and B signals in the RPS circuits. No failure of the comparitor can propagate a fault in the RPS circuits.	-	None required.	None	
8.0	Subchannel Comparitor (Chamber B)	All Modes	See 7.0	-	None required.	None	
9.0	Subchannel Deviation Comparitor	All Modes	See 7.0	-	None required.	None	
10.0	Power Indicator	Invalid Indication	The failure does not induce secondary failures.	Status Check of Power Indicators	The indicator is buffered from the active RPS circuits. No indicator failure can propagate a RPS failure.	None	

TABLE A-1 (cont'd)

RPS FMEA

REACTOR TRIP #1

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
10.1	Bistable Unit 7	Fails Tripped (Setpoint Exceeded)	The bistable output relay is de-energized and drops out. The Channel A aux. trip unit relays (K1, K2, and K3) are de-energized (via the flow trip set-point select switch) when the plant is operating with 4 coolant pumps.	When 2 or 3 Pumps are On Line, Periodic Test or Panel Status Check. When 4 Pumps On Line, Channel Trip Alarm for RT#1.	None required if 2 or 3 pumps are on line. When 4 pumps are on line, RPS 2/4 logic inhibits spurious RT due to a single channel trip.	None when 2 or 3 pumps are on line. When 4 pumps are on line the RT#1 logic is half tripped.	See 1.1
10.2	"	Fails Un-tripped	Channel A trip for RT#1 is disabled when 4 pumps are on line.	Periodic Test	Only 2/4 channels are required to trip to actuate RT#1.	When 4 pumps are on line, RT#1 logic is changed to a 2/3 configuration.	
10.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #13)	The bistable will go to the tripped state. See 10.1.	See 10.1	See 10.1	See 10.1	
11.1	Bistable Unit 3	Fails Tripped (Setpoint Exceeded)	The bistable output relay is de-energized and drops out. The channel aux. trip unit pre-trip relay is de-energized when the plant is operating with 4 pumps.	When 4 Pumps are On Line, Channel A Pre-Trip Alarm	When 4 pumps are on line, RPS 2/4 logic inhibits a spurious rod withdrawal prohibit command.	When 4 pumps are on line, RPS rod withdrawal prohibit function is half tripped. The associated logic is changed to a 1/3 configuration.	
11.2	"	Fails Un-tripped	The Channel A aux. trip unit pre-trip function is disabled when 4 pumps are on line.	Periodic Test	Only 2/4 channels are required to trip to actuate the rod withdrawal prohibit function.	When 4 pumps are on line, the rod withdrawal prohibit logic is changed to a 2/3 configuration.	
11.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #13)	The bistable will go to the tripped state. See 11.1.	See 11.1	See 11.1	See 11.1	
12.1	Bistable Unit 6	Fails Tripped (Setpoint Exceeded)	The bistable output relay is de-energized and drops out. The Channel A aux. trip unit relays (K1, K2, and K3) are de-energized (via the flow trip set-point select switch) when the plant is operating with 3 coolant pumps.	When 2 or 4 Pumps are On Line, Periodic Test or Panel Status Check. When 3 Pumps are On Line, Channel Trip Alarm for RT#1	None required if 2 or 4 pumps are on line. When 3 pumps are on line, RPS 2/4 logic inhibits spurious RT due to a single channel trip.	None when 2 or 4 pumps are on line. When 3 pumps are on line, the RT#1 logic is half tripped.	See 1.1

TABLE A-1 (cont'd)

RPS FMEA | REACTOR TRIP #1

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
12.2	Bistable Unit 6	Fails Un-tripped	Channel A trip for RT#1 is disabled when 3 pumps are on line.	Periodic Test	Only 2/4 channels are required to trip to actuate RT#1.	When 3 pumps are on line, RT#1 logic is changed to a 2/3 configuration.	
12.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #13)	The bistable will go to the tripped state. See 12.1.	See 12.1	See 12.1	See 12.1	
13.1	Bistable Unit 4	Fails Tripped (Setpoint Exceeded)	The bistable output relay is de-energized and drops cut. The Channel A aux. trip unit pre-trip relay is de-energized when the plant is operating with 3 pumps.	When 3 Pumps are One Line, Channel A Pre-Trip Alarm	When 3 pumps are on line, RPS 2/4 logic inhibits a spurious rod withdrawal prohibit command.	When 3 pumps are on line, RPS rod withdrawal prohibit function is half tripped. The associated logic is changed to a 1/3 configuration.	
13.2	"	Fails Un-tripped	The Channel A aux. trip unit pre-trip function is disabled when 3 pumps are on line.	Periodic Test	Only 2/4 channels are required to trip to actuate the rod withdrawal prohibit function.	When 3 pumps are on line, the rod withdrawal prohibit logic is changed to a 2/3 configuration.	
13.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #13)	The bistable will go to the tripped state. See 13.1.	See 13.1	See 13.1	See 13.1	
14.1	Bistable Unit 2	Fails Tripped (Setpoint Exceeded)	The bistable output relay is de-energized and drops out. The Channel A aux. trip unit relays (K1, K2, and K3) are de-energized (via the flow trip set-point select switch) when the plant is operating with 2 coolant pumps.	When 3 or 4 Pumps are On Line, Periodic Test or Panel Status Check. When 2 Pumps are On Line, Channel Trip Alarm for RT#1	None required if 3 or 4 pumps are on line. When 2 pumps are on line, RPS 2/4 logic inhibits spurious RT due to a single channel trip.	None when 3 or 4 pumps are on line. When 2 pumps are on line, the RT#1 logic is half tripped.	See 1.1
14.2	"	Fails Un-tripped	Channel A trip for RT#1 is disabled when 2 pumps are on line.	Periodic Test	Only 2/4 channels are required to trip to actuate RT#1.	When 2 pumps are on line, RT#1 logic is changed to a 2/3 configuration.	

TABLE A-1 (cont'd)

RPS FMEA REACTOR TRIP #1

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
14.3	Bistable Unit 2	Loss of Input Power Supply (Pnl Y10, Bkr #13)	The bistable will go to the tripped state. See 14.1.	See 14.1	See 14.1	See 14.1	
15.1	Bistable Unit 5	Fails Tripped (Setpoint Exceeded)	The bistable output relay is de-energized and drops out. The Channel A aux. trip unit pre-trip relay is de-energized when the plant is operating with 2 pumps.	When 2 Pumps are On Line, Channel A Pre-Trip Alarm	When 2 pumps are on line, RPS 2/4 logic inhibits a spurious rod withdrawal prohibit command.	When 2 pumps are on line, RPS rod withdrawal prohibit function is half tripped. The associated logic is changed to a 1/3 configuration.	
15.2	"	Fails Untripped	The Channel A aux. trip unit pre-trip function is disabled when 2 pumps are on line.	Periodic Test	Only 2/4 channels are required to trip to actuate the rod withdrawal prohibit function.	When 2 pumps are on line, the rod withdrawal prohibit logic is changed to a 2/3 configuration.	
15.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #13)	The bistable will go to the tripped state. See 15.1.	See 15.1	See 15.1	See 15.1	
16.1	Aux. Trip Unit	Fails Tripped	The trip relays (K1, K2, and K3) to the RPS 2/4 logic matrix are de-energized and drop out.	Channel A Trip Alarm for RT#1	RPS 2/4 logic inhibits a spurious RT due to a single channel trip.	RT#1 logic is half tripped and is changed to a 1/3 configuration.	One invalid channel trip may be bypassed for RT#1. When one channel is bypassed, RT#1 changes to a 2/3 configuration.
16.2	"	Fails Untripped	Channel A trip for RT#1 is disabled.	Periodic Test	Only 2/4 channels are required to trip to actuate RT#1.	RT#1 logic is changed to a 2/3 configuration.	
16.3	"	Pre-Trip Fails Tripped	The pre-trip relay, K5, is de-energized and drops out and generates a rod withdrawal prohibit signal.	Pre-Trip Alarm	The rod withdrawal prohibit logic required 2/4 power range pre-trip signal to actuate. This logic inhibits spurious actuation.	No effect on the RPS RT#1 function.	

TABLE A-1 (cont'd)

RPS FMEA

REACTOR TRIP #1

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
16.4	Aux. Trip Unit	Pre-Trip Fails Untripped	The pre-trip relay (K5) cannot drop out and generate a rod withdrawal prohibit signal.	Periodic Test	Only 2/4 power range channel pre-trip signals are required to actuate the rod withdra wal prohibit function.	See 16.3	
16.5	"	Relay K1 or K2 or K3 Fails to Energized State	The Channel A trip function is degraded. Only 2/3 trip relays will drop out when the bistable trips. 1 of 6 RPS trip modules cannot actuate RT#1.	Periodic Test	See 16.2	RT#1 logic is degraded. Channel A trip is only 2/3 effective.	Only 1 of 6 trip modules are required to actuate an RT.
16.6	"	Relay K1 or K2 or K3 Fails to De-energized State	Partial Channel A trip. 1 of the 6 RPS trip modules is half tripped.	Status Check of Bistable Trip Relay Lights	See 16.1	1 of the 6 RPS trip modules is half tripped for RT#1.	
16.7	"	Loss of Input Power Supply (Pnl Y10, Bkr #13)	The aux. trip unit will go to the tripped state. All channel trip and pre-trip relays are de-energized. See 16.1 and 16.3.	Channel A Trip and Pre-Trip Alarm for RT#1	See 16.1 and 16.4	See 16.1 and 16.4	
17.1	Manual Switch (Flow Trip Setpoint Select)	Jams or Binds	Switch position cannot be changed. No effect until required to change the number of coolant pumps on line. The position of this switch determines the fixed setpoints for RT#1 and RT#3.	Cannot Change Switch Position When Required	If number of pumps on line is constant, none are required. If the number of pumps on line changes, either RT#1 or RT#3 will be immediately actuated on all channels. No channel trip is completely inhibited by an invalid setpoint. The channel trip is delayed until a more severe transient condition (e.g., lower flow rate or higher power level) is achieved.	If the number of pumps on line is constant, no effect. If the number of pumps is decreased, RT#3 2/4 logic is actuated and scrams the reactor. If the number of pumps is increased, RT#1 2/4 logic is actuated and scrams the reactor.	3 position switch. Position #1 - 4 pump operation. Position #2 - 3 pump operation. Position #3 - 2 pump operation.
17.2	"	Contact Set Fails Open	The voltage input signal to the aux. trip unit through the bistable output relay is open circuited and trips the channel trip or pre-trip sections of the aux. trip unit. Either channel aux. trip unit trip relays or the pre-trip relays are de-energized and drop out. (The contact set is assumed to be associated with the bistable for channel trip or pre-trip.)	Either Channel Trip Alarm for RT#1 or Channel Pre-Trip Alarm for RT#1	RPS 2/4 logic inhibits either spurious RT or rod withdrawal prohibit function.	Either RT#1 or the rod withdrawal prohibit function is half tripped. The logic changes to a 1/3 configuration.	One invalid channel trip may be bypassed for RT#1. When one channel is bypassed, both the RT and pre-trip logic changes to a 2/3 configuration.

TABLE A-1 (cont'd)

RPS FMEA

REACTOR TRIP #1

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
17.3	Manual Switch (Flow Trip Setpoint Select)	Control Set Fails Closed	No effect. This is the normal contact position. If the switch position cannot be changed due to a contact failing closed, see 17.1.				
18.1	Manual Switch (Trip #1 By-pass Channel A)	Fail Open	The keylock switch is N.O. and is only used to remove an invalid trip and change the RT configuration to 2/3.	Periodic Test	The switch is N.O. during normal plant operation.	An invalid Channel A trip cannot be by-passed to remove the half trip condition. RT#1 logic cannot be changed to a 2/3 con-figuration.	1 key is available for use with the 4 bypass switches (Channel A, B, C, and D). Only 1 channel trip may be bypassed.
18.2	"	Fail Closed	Three separate switch contacts in parallel with the three normally open contacts of the trip unit close and in-hibit a valid channel trip.	Status Check. Light above Switch is Illuminated	See 16.2	See 16.2	
18.3	"	Single Con-tact Set - Fails Open	See 18.1	Periodic Test	See 18.1	1 of the 3 bistable unit trip relays cannot be bypassed after an in-valid channel trip. 1 of the 6 trip logic (2/4) modules will be half tripped.	
18.4	"	Single Con-tact Set - Fails Closed	1 of the 3 bistable trip relays is dis-abled.	Periodic Test	See 16.1	1 of the 6 RPS trip logic modules cannot actuate RT#1.	
19.0	Bistable Unit 8	All Modes	The bistable is not associated with and is buffered from the RPS circuits. No fault in the bistable can propagate the RPS circuits.		None required.	None	
20.1	Bistable Unit 1	Fails Tripped (Setpoint Exceeded)	The bistable unit de-energizes an auxiliary relay when tripped. The relay N.C. contacts provide a signal to rate trip (RT#2) inhibit logic to bypass the trip. The relay N.O. contacts provide a signal to RT #10 to remove the auto-matic bypass. The bistable normally trips when the reactor power level is greater than 15%. When the power level is less than 15%, the channel A trip for RT#2 is bypassed and the trip	Panel Status Check and Bypass Alarm	During normal plant op-eration (reactor power greater than 15%), none are required because the bistable is normally trip-ped. If reactor power level is less than 15%, the RPS 2/4 logic inhibits spurious RT due to a single RT#10 channel trip. Only 2/4 channels are required	During normal plant operation (power above 15%), no effect on RT#2 or RT#10.	

TABLE A-1 (cont'd)

RPS FMEA

REACTOR TRIP #1

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
20.1 (cont'd)	Bistable Unit 1		for RT#10 is not bypassed.		to trip to actuate RT#2 when reactor power is greater than 10^{-4}% and less than 15%.		
20.2	"	Fails Untripped	RT#10 Channel A trip is bypassed. RT#2 Channel A trip is enabled when reactor power is above 10^{-4}%.	Panel Status Check and Bypass Alarm	When reactor power level is greater than 15%, only 2/4 RPS channels are required to trip to actuate RT#10. RPS 2/4 logic inhibits spurious RT due to a single RT#2 channel trip.	The RT#10 logic is changed to a 2/3 configuration. RT#2 logic is half tripped if Channel A RT#2 bistable trips above 10^{-4}% reactor power. If RT#2 Channel A trips, the logic is changed to a 1/3 configuration.	
20.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #13)	The bistable will go to the untripped state. See 20.1.	Status Panel Check	See 20.1	See 20.1	
21.1	Low Voltage Power Supply	Loss of Output	All Channel A power range bistables will go to the tripped state. All bypasses generated by this channel will go to the unbypassed state.	Channel Trip and Pre-Trip Alarms	RPS 2/4 logic inhibits spurious RT due to a single channel trip.	RT#1 logic is half tripped and changes to a 1/3 configuration.	
21.2	"	Off Nominal Output	The ion chamber signal conditioning equipment will generate erroneous outputs. No significant operational impact unless the chamber outputs are driven to an extreme condition. See 1.1, 1.2 and 1.3 for details.	See 1.1 and 1.2	See 1.1 and 1.2	See 1.1 and 1.2	
21.3	"	Loss of Input Power (Pnl Y10, Bkr #13)	The effect of the failure is the same as 21.1.	See 21.1	See 21.1	See 21.1	
22.1	Range Switch	Fails in Low Range Position (X10)	The channel high power level trip is actuated when reactor power is greater than 10.65%. During normal plant operation, a channel trip (RT#1) is generated.	See 16.1	See 16.1	See 16.1	

TABLE A-1 (cont'd)

RPS FMEA

REACTOR TRIP #1

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
22.2	Range Switch	Fails in Normal Range Position (X1)	In low power operation (less than 10.65% reactor power), the channel high power level trip is delayed until the power level exceeds 10.65%.	Status Check of Power Level Meters	None required during normal operation.	During low reactor power operation, the RT#1 logic is changed to a 2/3 configuration.	
23.0	Channel B Components	All Modes	All high pwer level instrumentation and trip channels (A, B, C, D) are identical in configuration. The FMEA for Channel A components (items 1-22) is applicable for all channels.				The Channel B power source is Pnl Y20, Bkr #13.
24.0	Channel C Components	All Modes	See 23.0				The Channel C power source is Pnl Y30, Bkr #13.
25.0	Channel D Components	All Modes	See 23.0				The Channel D power source is Pnl Y40, Bkr # 13.

TABLE A-2

FAILURE MODE AND EFFECTS ANALYSIS PALISADES PLANT REACTOR PROTECTION SYSTEM
REACTOR TRIP #2, HIGH RATE-OF-CHANGE

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
1.1	Channel 3 Fission Counter	Fail High	High signal level to Channel 3 nuclear instrumentation and trip logic circuits. If reactor power is less than 10^{-4}%, the zero power mode switch will be disabled on two RPS channels. Two pretrip and two channel trip signals will be generated and propagate channel trips on two RPS aux trip units.	RT#2 Channel Pre-Trip and Trip Alarms	None	RT#2 when not in automatic bypass.	RT#2 is automatically bypassed below 10^{-4}% and above 15% of full reactor power.
1.2	"	Fail Low	The zero power mode switch will not be automatically disabled on 2 RPS channels. The RT#2 function is disabled on two RPS channels.	Status Check of Channel 3 and 4 Indicators	Only 1/2 Rate of Change Channels (3 or 4) are required to actuate RT#2.	RT#2 sensor inputs are degraded to a 1/1 configuration and the trip logic changes to a 2/2 configuration.	
1.3	"	Output Signal Constant	The constant signal disables the channel RT#2 function.	See 1.2	See 1.2	See 1.2	
1.4	"	Short Across Signal Lines or Open Signal Line	The effect of the failure is the same as fail low.	See 1.2	See 1.2	See 1.2	
2.1	Pre Amp (Channel 3)	Output Signal High	The effect of the failure is the same as 1.1.	See 1.1	See 1.1	See 1.1	
2.2	"	Output Signal Low	The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	
2.3	"	Output Signal Constant	The effect of the failure is the same as 1.3.	See 1.2	See 1.2	See 1.2	
2.4	"	Short Across Signal Lines or Open Signal Line	The effect of the failure is the same as 1.4.	See 1.2	See 1.2	See 1.2	
2.5	"	Loss of Any Input Power Supply (Pnl Y30, Bkr #13)	See 1.2	See 1.2	See 1.2	See 1.2	
3.1	High Voltage Power Supply	Loss of Output	The effect of the failure is the same as 1.2.	Detector Operating Voltage Alarm	See 1.2	See 1.2	

TABLE A-2 (cont'd)

RPS FMEA

REACTOR TRIP #2

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
3.2	High Voltage Power Supply	Off Nominal Output	The fission counter may generate erroneous outputs. If voltage drops 15% below the normal operating level, the voltage supply alarm is actuated. No significant operational impact is propagated by the high voltage failure unless the detector output signal is driven to an extreme condition. See 1.1 and 1.2 for details.	See 1.1 and 1.2. Possible Detector Operating Voltage Alarm	See 1.1 and 1.2	See 1.1 and 1.2	
3.3	"	Loss of Input Power Supply (Pnl Y30, Bkr #13)	All bistables will go to the tripped state.	See 1.1	See 1.1	See 1.1	
4.1	Low Voltage Power Supply	Loss of Output	See 3.1	See 1.2	See 1.2	See 1.2	
4.2	"	Off Nominal Output	See 3.2	See 1.1 and 1.2	See 1.1 and 1.2	See 1.1 and 1.2	
4.3	"	Loss of Input Power Supply (Pnl Y30, Bkr #13)	All bistables will go to the tripped state.	See 1.1	See 1.1	See 1.1	
5.1	Pulse Amp and Count Rate Circuits	Loss of Output (Fail Low)	Low level input to summing amplifier would propagate the same effect as the the channel fission counter failing low. See 1.2.	See 1.2	See 1.2	See 1.2	
5.2	"	High Output Signals	The effect of the failure is the same as 1.1.	See 1.1	None	RT when not in automatic bypass.	
5.3	"	Loss of Power Supply (Pnl Y30, Bkr #13)	See 5.1	See 1.2	See 1.2	See 1.2	
6.1	Summing Amp	High Signal Level Output	The effect of the failure is the same as 1.1.	See 1.1	None	RT#2 when not in automatic bypass.	
6.2	"	Low Signal Level Output	The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	

TABLE A-2 (cont'd)

RPS FMEA

REACTOR TRIP #2

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
6.3	Summing Amp	Constant Signal Level Output	The effect of the failure is the same as 1.3.	See 1.3	See 1.3	See 1.3	
6.4	"	Loss of Power Supply (Pnl Y30, Bkr #13)	See 6.2	See 1.2	See 1.2	See 1.2	
7.1	Power Rate of Change Amplifier	High Signal Level Output	Rate bistable units 1, 2, 3, and 4 trip. Two pre-trip and two channel trip signals (A and C) are generated and propagate channel trips on two RPS aux trip units. The failure does not propagate any effect on the zero power mode bypass switch operation.	RT#2 Channel Trip and Pre-Trip Alarms	None	RT#2 when not in automatic bypass.	
7.2	"	Low Signal Level Output	The RT#2 function is disabled on two RPS channels.	Status Check of Channel 3 and 4 Rate of Change Indicators	See 1.2	See 1.2	
7.3	"	Output Signal Constant	See 7.2	See 7.2	See 1.2	See 1.2	
7.4	"	Loss of Power Supply (Pnl Y30, Bkr #13)	See 7.2	See 7.2	See 1.2	See 1.2	
8.0	HV Bistable Unit	All Modes	The bistable is not associated with and is buffered from the RPS circuits. The bistable provides an alarm if the detector operating voltage falls below 15% of the normal value. No fault in the bistable can propagate a fault in the RPS circuits.	-	None required.	None	
9.1	Flux Bistable Unit 2	Fails Tripped (Setpoint Exceeded)	The bistable is tripped during normal plant operation. When tripped, the unit provides a signal to disable the zero power mode bypass on one of the four RPS channels.	Periodic Test	RPS 2/4 logic inhibits spurious RT during zero power mode testing.	None during normal plant operation.	Bistable trips when reactor power level exceeds 10^{-4}% of full power.

A-17

TABLE A-2 (cont'd)

RPS FMEA — REACTOR TRIP #2

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
9.2	Flux Bistable Unit 2	Fails Un-tripped	The zero power mode bypass is not automatically disabled when reactor power exceeds 10^{-4}%. RT#3, 6, 7, and 9 trips are inhibited on one RPS channel.	Periodic Test	Only 2/4 RPS channels are required to trip to actuate RT#3, 6, 7, and 9. The zero power mode bypass switch is the primary means to enable or disable the function. The bistable unit provides an automatic backup for operator action during controlled testing.	RT#3, 6, 7 and 9 logic is changed to a 2/3 configuration.	
9.3	"	Loss of Input Power Supply (Pnl Y30, Bkr #13)	The bistable will go to the tripped state. See 9.1.	Periodic Test	See 9.1	See 9.1	
10.0	Flux Bistable Unit 3	All Modes	Flux bistable unit 3 is identical to unit 2. Unit 3 provides signals to a different RPS channel. See 9.0 above for details.				
11.0	Flux Bistable Unit 1	All Modes	The bistable is a spare unit with no RPS circuit interface.	-	None required.	None	
12.0	Rate Bistable Unit 1	All Modes	See 11.0	-	None required.	None	
13.1	Rate Bistable Unit 3	Fails Tripped (Setpoint Exceeded)	Unit 3 provides a pre-trip signal and rod withdrawal prohibit signal to two RPS channels. The rod withdrawal prohibit function is actuated.	RT#2 Pre-Trip Alarms on 2 Channels	Bistable unit 5 doesn't interface with the RPS scram function.	No effect which can degrade the RPS capability to scram.	Bistable trips when power rate of change exceeds 1.5 decades per minute.
13.2	"	Fails Un-tripped	Loss of RT#2 pre-trip alarm on 2 RPS channels (A and C). The rod withdrawal prohibit (high rate of power change) function is degraded to a 1/1 configuration. The prohibit trip logic configuration is changed to 1/2.	Periodic Test	See 13.1	See 13.1	
13.3	"	Loss of Input Power Supply (Pnl Y30, Bkr #13)	The bistable will go to the tripped state. See 13.1.	See 13.1	See 13.1	See 13.1	

TABLE A-2 (cont'd)

RPS FMEA — REACTOR TRIP #2

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
14.1	Rate Bistable Unit 2	Fail Tripped (Setpoint Exceeded)	The bistable output relay is de-energized and drops out. The RT#2 aux trip unit input is de-energized and propagates a RPS channel trip.	RT#2 Channel Trip Alarm	RPS 2/4 logic inhibits spurious RT due to a single channel trip.	RT#2 logic is half tripped and is changed to a 1/3 configuration.	One invalid channel trip may be bypassed for RT#2. When one channel is bypassed, RT#2 logic changes to a 2/3 configuration.
14.2	"	Fails Untripped	The associated RPS RT#2 channel is functionally disabled and cannot trip.	Periodic Test	Only 2/4 channels are required to trip to actuate RT#2.	RT#2 logic is changed to a 2/3 configuration.	
14.3	"	Loss of Input Power Supply (Pnl Y30, Bkr #13)	The bistable will go to the tripped state. See 14.1.	See 14.1	See 14.1	See 14.1	
15.0	Rate Bistable Unit 4	All Modes	Rate bistable unit 4 is identical to unit 2. Unit 4 provides trip signals to a different RPS channel. See 14.0.				
16.0	Channel 3 Rate of Change Indicator	Incorrect Indication	This failure does not induce secondary failures or propagate any effect on the RPS function.	Status Check of Channel 3 and 4 Indicators	The indicator is buffered from active RPS circuits.	None	
17.0	Channel 3 Power Indicator	Incorrect Indication	See 16.0	See 16.0	See 16.0	None	
18.0	All Nuclear Channel 4 Components	All Modes	Both wide range logarithmic channels (Channels 3 and 4) are identical in configuration. The FMEA for Channel 3 components (items 1.0-17.0) is applicable for both channels.				The nuclear Channel 4 power source is Pnl Y40, Bkr #13.
19.1	Channel A Aux Trip Unit	Fails Tripped	The trip relays (K1, K2, and K3) to the RPS 2/4 logic matrix are de-energized and drop out. The effect of the failure is the same as 14.1.	See 14.1	See 14.1	See 14.1	The RT#2 trip and pre-trip signals are automatically bypassed when reactor power level is less than 10^{-4}% and greater than 15%. One invalid channel trip may be bypassed at any time for RT#2. When 1 channel is bypassed, the RT#2 trip logic changes to a 2/3 configuration.

TABLE A-2 (cont'd)

RPS FMEA

REACTOR TRIP #2

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
19.2	Channel A Aux Trip Unit	Fails Un-tripped	Channel A trip for RT#2 is disabled. The effect of the failure is the same as 14.2.	Periodic Test	See 14.2	See 14.2	
19.3	"	Pre-Trip Fails Tripped	The pre-trip relay K5 is de-energized and drops out and generates a rod with-drawal prohibit signal. The rod with-drawal prohibit trip function is actuat-ed on any 1/4 rate of change pre-trip signal.	Rod Withdrawal Prohibit Alarm	None	No effect on the RPS RT#2 function.	
19.4	"	Pre-Trip Fails Un-tripped	The pre-trip relay (K5) cannot drop out and generate a rod withdrawal prohibit signal.	Periodic Test	Only 1/4 rate of change pre-trip signals are re-quired to actuate the rod withdrawal prohibit func-tion.	See 19.3	
19.5	"	Relay K1 or K2 or K3 Fails to En-ergized State	The Channel A trip function is degrad-ed. Only 2/3 trip relays will drop out when the trip unit trips. 1 of the 6 RPS trip modules cannot actuate RT#2.	Periodic Test	See 19.2	RT#2 logic degraded. Channel A trip is only 2/3 effective.	Only 1 of 6 trip modules are required to actuate a RT.
19.6	"	Relay K1 or K2 or K3 Fails to De-energized State	Partial Channel A trip. 1 of the 6 RPS trip modules is half tripped.	Status Check of Aux Trip Unit Trip Relay Lights	See 14.1	1 of the 6 RPS trip modules is half trip-ped for RT#2.	
19.7	"	Loss of Input Power Supply (Pnl Y10, Bkr #13)	The aux trip unit will go to the tripped state. All channel trip and pre-trip relays are de-energized. See 19.1 and 19.3.	Channel A Trip and Pre-Trip Alarm for RT#2. Rod With-drawal Prohibit Alarm	See 19.1 and 19.3	See 19.1 and 19.3	See 19.1
20.1	Channel A Aux Relay (K 22)	Fails to De-energized State	When power range bistable unit 8 trips at > 15% reactor power, the aux relay will not pull in and bypass the RT#2 aux trip unit (ATU-2) pre-trip function. When the power rate of change exceeds 1.5 decades/min., the rod withdrawal prohibit function is actuated. See 19.3.	Periodic Test	None	No effect on the RPS	
20.2	"	Fails to Energized State	The aux trip unit pre-trip function is bypassed. The rod withdrawal prohibit function power rate of change actuation	Periodic Test	None	No effect on the RPS RT#2 function.	

TABLE A-2 (cont'd)

RPS FEMA

REACTOR TRIP #2

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
20.2 (cont'd)	Channel A Aux Relay (K 22)	Fails to Energized State	logic changes to a 1/3 configuration.				
21.1	Channel A Aux Relay (K 25)	Fails to De-energized State	When power range bistable unit 8 trips at > 15% reactor power, the aux relay will not pull in or bypass the trip signal to the aux trip unit. When the power rate of change exceeds 2.6 decades/min., the aux trip unit will trip and generate an RPS channel trip. See 14.1.	Periodic Test or Channel A RT#2 Trip Alarm	See 14.1	See 14.1	See 14.1
21.2	"	Fails to Energized State	The aux trip unit channel trip function is bypassed.	Periodic Test	See 14.2	See 14.2	
22.1	Channel A Aux Relay (K 26)	Fails to Energized State	When rate of change bistable unit (#2) trips at > 10^{-4}% reactor power, the aux relay will not drop out and remove the bypass on both the channel trip and pre-trip signal to the aux trip units. The effect of the failure is the same as 20.2 and 21.2.	See 20.2 and 21.2	See 20.2 and 21.2	See 20.2 and 21.2	
22.2	"	Fails to De-energized State	The aux trip unit channel trip and pre-trip is not automatically bypassed when reactor power is less than 10^{-4}%.	See 20.1 and 21.1	See 20.1 and 21.1	See 20.1 and 21.1	
23.1	Manual Switch (Trip #2 Bypass - Channel A)	Fail Open	The keylock switch is N.O. and is only used to remove an invalid trip and to change the RT configuration to 2/3.	Periodic Test	The switch is N.O. during normal plant operation.	An invalid Channel A trip cannot be bypassed to remove the half trip condition. RT#2 logic cannot be changed to a 2/3 configuration.	1 key is available for use with the 4 bypass switches (Channels A, B, C and D). Only 1 channel trip may be bypassed.
23.2	"	Fail Closed	Three separate switch contacts in parallel with the three normally open contacts of the aux trip unit relays close and inhibit a valid channel trip.	Status Check. Light above Switch is Illuminated	See 14.2	See 14.2	
23.3	"	Single Contact Set - Fails Open	See 20.1	Periodic Test	See 23.1	1 of the 3 bistable unit trip relays cannot be bypassed after an invalid channel trip.	

TABLE A-2 (cont'd)

RPS FMEA

REACTOR TRIP #2

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
23.3 (cont'd)	Manual Switch (Trip #2 Bypass - Channel A)	Single Contact Set - Fails Open				1 of the 6 trip logic (2/4) modules will be half tripped.	
23.4	"	Single Contact Set - Fails Closed	1 of the 3 aux trip unit trip relays is disabled.	Periodic Test	See 14.2	1 of the 6 RPS trip logic modules cannot actuate RT#2.	
24.0	Channel B Components	All Modes	All high rate of change (RT#2) RPS trip channels (A, B, C, D) are identical in configuration. The FMEA for Channel A (items 19 - 23) is applicable for all channels.				The Channel B power source is Pnl Y20, Bkr #13.
25.0	Channel C Components	All Modes	See 24.0				The Channel C power source is Pnl Y30, Bkr #13.
26.0	Channel D Components	All Modes	See 24.0				The Channel D power source is Pnl Y40, Bkr #13.

TABLE A-3

FAILURE MODE AND EFFECTS ANALYSIS PALISADES PLANT REACTOR PROTECTION SYSTEM
REACTOR TRIP #3, LOW FLOW, REACTOR COOLANT

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
1.1	Channel A Flow (dp) Transmitter (PDT 0112AA)	Fail High	High analog flow signal (high voltage) to Channel A flow instrumentation and trip logic. The output from 4 Channel A flow transmitters (1 unit for each coolant pump) is summed prior to the flow instrumentation and trip logic.	Status Check of Coolant Flow Indicators (1 Indicator for each channel)	Only 2/4 channels are required to trip to actuate RT#3.	RT#3 logic is changed to a 2/3 configuration.	
1.2	"	Fail Low	Low analog flow signal to channel instrumentation and trip logic.				
			When the flow transmitter is monitoring a coolant loop that has an operating pump, the channel low flow trip will be actuated.	Channel Trip and Pre-Trip Alarms for RT#3	RPS 2/4 logic inhibits spurious RT due to a single channel trip.	RT#3 logic is half tripped and is changed to a 1/3 configuration.	One invalid channel trip may be bypassed for RT#3. When one channel is bypassed, RT#3 logic changes to a 2/3 configuration.
			When the flow transmitter is monitoring a coolant loop with the pump not operating, the differential of the summed signal level will not be sufficient to generate a channel low flow trip.	Status Check of Coolant Flow Indicators	See 1.1	None while the coolant pump remains off.	
1.3	"	Output Signal Constant	Constant analog signal level to channel flow instrumentation and trip logic. Channel A trip is disabled.	Periodic Test/ Calibration	See 1.1	See 1.1	
1.4	"	Open Signal Line	The effect of the failure is the same as fail low.	See 1.2	See 1.2	See 1.2	
1.5	"	Signal Line Shorts to Ground	None	None	The current loop is ungrounded.	None	
1.6	"	Loss of High Pressure Tap Input	The loss of the input will generate a low flow signal. See 1.2.	See 1.2	See 1.2	See 1.2	
1.7	"	Loss of Low Pressure Tap Input	The loss of the input will generate a high flow signal. See 1.1.	See 1.1	See 1.1	See 1.1	
1.8	"	Loss of Both Pressure Tap Inputs	The loss of both inputs will generate a low flow signal. See 1.2.	See 1.2	See 1.2	See 1.2	

TABLE A-3 (cont'd)

RPS FMEA — REACTOR TRIP #3

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
2.0	Channel A Flow (dp) Transmitter (PDT 0112BA)	All Modes	All 4 Channel A flow transmitters are identical. The FMEA for transmitter PDT 0112AA is applicable for all units.				
3.0	Channel A Flow (dp) Transmitter (PDT 0122CA)	All Modes	See 2.0				
4.0	Channel A Flow (dp) Transmitter (PDT 0122DA)	All Modes	See 2.0				
5.1	Power Supply 5 Unit 45 VDC (F 0102A)	Loss of Output	All channel transmitters have this common power supply. The channel low flow trip will be actuated.	Channel Trip and Pre-Trip Alarms for RT#3	RPS 2/4 logic inhibits spurious RT due to a single channel trip.	RT#3 logic is half tripped and is changed to a 1/3 configuration.	
5.2	"	Off Nominal Output	The 4 transmitters will generate erroneous outputs. No significant operational impact unless the summed transmitter output is driven to an extreme condition. See 1.1, 1.2 and 1.3 for details.	See 1.1 and 1.2	See 1.1 and 1.2	See 1.1 and 1.2	See 1.2
5.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #5)	The effect of the failure is the same as 5.1.	See 5.1	See 5.1	See 5.1	
6.0	Coolant Flow Indicator (PDI 0112AA)	Invalid Indication	The indicator monitors flow (dp) transmitter PDT 0112AA. The failure does not induce secondary failures.	Status Check of All Channel Coolant Flow Indicators	The indicator is isolated from the active RPS circuits so that an indicator failure will not propagate an RPS failure. If the meter is shorted out of the instrumentation loop circuit, the transmitter will compensate and maintain valid signal levels for normal RPS operation.	None	

TABLE A-3 (cont'd)

RPS FMEA

REACTOR TRIP #3

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
7.0	Coolant Flow Indicator (PDI 0112BA)	All Modes	All Channel A flow (dp) indicators are identical. The FMEA for PDI 0112AA is applicable for all units.				
8.0	Coolant Flow Indicator (PDI0122CA))	All Modes	See 7.0				
9.0	Coolant Flow Indicator (PDI0122DA)	All Modes	See 7.0				
10.0	Channel A Coolant Flow Indicator	Invalid Indication	The meter indicates the summed Channel A coolant flow. The failure does not induce secondary failures.	See 6.1	See 6.1	None	
11.1	Manual Switch (Zero Power Mode Trip Bypass - Channel A)	Fail Open	The keylock switch is N.O. and is only closed for system tests when the reactor is subcritical (less than 10^{-4}% power). Channel A trips #3, 6, 7 and 9 are not bypassed during zero power reactor tests.	During Zero Power Reactor Tests, Channel Trip and Pre-Trip Alarm for RT 3, 6, 7, and 9	RPS 2/4 logic inhibits spurious RT due to the numerous trips generated in Channel A. During zero power testing, Channels B, C, and D are bypassed and thus eliminate the possibility of a spurious RT.	None	During zero power testing Channel A trips #3, 6, 7, 9 may each be bypassed by the channel bypass switch for each trip mode.
11.2	"	Fail Closed	When the reactor is subcritical, Channel A trips #3, 6, 7, and 9 are inhibited by the application of +15V to the bistable trip units.	Switch Bypass Position is Annunciated	When reactor power is greater than 10^{-4}%, signals from the power level trip units automatically disable the bypass by removing the +15 Volts at the bistable trip units.	None during normal plant operation. During zero power tests, the switch is N.C.	

TABLE A-3 (cont'd)

RPS FMEA

REACTOR TRIP #3

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
11.3	Manual Switch (Zero Power Mode Trip Bypass - Channel A)	Contact Set Fail Open	Contact set 2 only interacts with trip #3. Channel A trip #3 is not bypassed during zero power tests.	During Zero Power Tests, Channel Trip and Pre-Trip Alarms for RT#3	During zero power tests, the RPS 2/4 logic inhibits a spurious RT#3 due to a single channel trip. The 3 other channels are by-passed to eliminate the possibility of a spurious trip.	None	
11.4	"	Contact Set Fail Closed	When the reactor is subcritical, Channel A trip #3 is inhibited by the application of +15 V to the bistable trip unit.	Periodic Test	See 11.2	See 11.2	
12.1	Manual Switch (Flow Trip Setpoint Select)	Jams or Binds	Switch position cannot be changed. No effect until required to change the number of coolant pumps on line. The position of this switch determines the fixed setpoints for RT#1 and RT#3.	Cannot Change Switch Position When Required	If number of pumps on line is constant, none are required. If the number of pumps on line changes, either RT#1 or RT#3 will be immediately actuated on all 4 channels. No channel trip is completely inhibited by an invalid setpoint. The channel trip is delayed until a more severe transient condition (e.g., lower flow rate or higher power level) is achieved.	If number of pumps on line is constant, no effect. If the number of pumps is decreased, RT#3 2/4 logic is actuated and scrams the reactor. If the number of pumps is increased, RT#1 2/4 logic is actuated and scrams the reactor.	3 position switch. Pos #1 - 4 pump operation. Pos #2 - 3 pump operation. Pos #3 2 pump operation.
12.2	"	Contact Set Fail Open	The bistable trip module setpoint reference voltage is lost (zero). The input signal voltage can never be less than the setpoint. The bistable unit trip is disabled.	Periodic Test	Only 2/4 channels are required to trip to actuate RT#3.	RT#3 logic is changed to a 2/3 configuration.	The contact set is assumed to be associated with the RT#3 channel trip setpoint rather than the pre-trip alarm setpoint.
12.3	"	Contact Set Fail Closed	No effect. This is the normal contact position. If the switch position cannot be changed due to a contact failing closed, see 12.1.	Periodic Test	None required.	None	
13.1	Bistable (PA 0102A)	Fails Tripped (Input Below Setpoint)	The bistable trip relays (K1, K2, and K3) to the RPS 2/4 logic matrix are de-energized and drop out. The effect of the failure is the same as 5.1.	See 5.1	See 5.1	See 5.1	

TABLE A-3 (cont'd)

RPS FMEA

REACTOR TRIP #3

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
13.2	Bistable (PA 0102A)	Fails Un-tripped	Channel A trip for RT#3 is disabled. The effect of the failure is the same as 12.2.	Periodic Test	See 12.2	See 12.2	
13.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #5)	The bistable will go to the tripped state. See 13.1.	See 5.1	See 5.1	See 5.1	
13.4	"	Relay K1 or K2 or K3 Fails to Energized State	The Channel A trip function is degraded. Only 2/3 trip relays will drop out when the bistable trips. 1 of the 6 RPS trip modules cannot actuate RT#3.	Periodic Test	See 12.2	RT#3 logic is degraded. Channel A trip is only 2/3 effective.	Only 1 of 6 trip modules are required to actuate a RT.
13.5	"	Relay K1 or K2 or K3 Fails to De-energized State	Partial Channel A trip. 1 of the 6 RPS trip modules is half tripped.	Status Checks of Bistable Trip Relay Lights	See 5.1	1 of the 6 RPS trip modules is half tripped for RT#3.	
14.1	Manual Switch (Trip #3 Bypass - Channel A)	Fail Open	The keylock switch is N.O. and is only used to remove an invalid trip and to change the RT configuration to 2/3.	Periodic Test	The switch is N.O. during normal plant operation.	An invalid Channel A trip cannot be bypassed to remove the half trip condition. RT#3 logic cannot be changed to a 2/3 configuration.	1 key is available for use with the 4 bypass switches (Channels A, B, C, and D). Only 1 channel trip may be bypassed.
14.2	"	Fail Closed	Three separate switch contacts in parallel with the three normally open contacts of the trip unit close and inhibit a valid channel trip.	Status Check. Light above Switch is Illuminated	See 12.2	See 12.2	
14.3	"	Single Contact Set Fail Open	See 14.1	Periodic Test	See 14.1	1 of the 3 bistable unit trip relays cannot be bypassed after an invalid channel trip. 1 of the 6 trip logic (2/4) modules will be half tripped.	
14.4	"	Single Contact Set Fail Closed	1 of the 3 bistable trip relays is disabled.	Periodic Test	See 12.2	1 of the 6 RPS trip logic modules cannot actuate RT#3.	

TABLE A-3 (cont'd)

RPS FMEA

REACTOR TRIP #3

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
15.0	Channel B Components	All Modes	All primary coolant flow instrumentation and trip channels (A, B, C, D) are identical in configuration. The FMEA for Channel A components is applicable for all channels.				The Channel B power source is Pnl Y20, Bkr #5.
16.0	Channel C Components	All Modes	See 15.0				The Channel C power source is Pnl Y30, Bkr #5.
17.0	Channel D Components	All Modes	See 15.0				The Channel D power source is Pnl Y40, Bkr #5.

TABLE A-4

FAILURE MODE AND EFFECTS ANALYSIS PALISADES PLANT REACTOR PROTECTION SYSTEM
REACTOR TRIP #4, LOW WATER LEVEL, SG#1

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
1.1	Channel A Level Transmitter (LT 0751A)	Fail High	Analog high water level signal (high voltage) to channel water level instrumentation and trip logic. Channel A trip is disabled.	Status Check of SG#1 Water Level Indicators or Periodic Test	Only 2/4 channels are required to trip to actuate RT#4.	RT#4 logic is changed to a 2/3 configuration.	
1.2	"	Fail Low	Analog low water level signal to channel trip logic. Channel A low water level trip actuated.	Channel Trip and Pre-Trip Alarms for RT#4	RPS 2/4 logic inhibits spurious RT due to a single channel trip.	RT#4 logic is half tripped and is changed to a 1/3 configuration.	One invalid channel trip may be bypassed for RT#4. When one channel is bypassed, RT#4 logic changes to a 2/3 configuration.
1.3	"	Output Signal Constant	Constant analog water level signal to channel water level instrumentation and trip logic. Channel A trip is disabled.	Periodic Test/ Calibration	See 1.1	See 1.1	
1.4	"	Open Signal Line	The effect of the failure is the same as fail low.	See 1.2	See 1.2	See 1.2	See 1.2
1.5	"	Signal Line Shorts to Ground	None	None	The current loop is ungrounded.	None	
1.6	"	Loss of High Pressure Tap Input	The loss of the input will generate a low level signal. See 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
1.7	"	Loss of Low Pressure Tap Input	The loss of the input will generate a high level signal. See 1.1.	See 1.1	See 1.1	See 1.1	
1.8	"	Loss of Both Pressure Tap Inputs	The loss of both inputs will generate a low level signal. See 1.2.	See 1.2	See 1.2	See 1.2	
2.1	Power Supply (L 0751A)	Loss of Output	The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
2.2	"	Off Nominal Output	The level transmitter will generate erroneous outputs. No significant operational impact unless the transmitter output is driven to an extreme condition. See 1.1, 1.2 and 1.3 for details.	See 1.1 and 1.2	See 1.1 and 1.2	See 1.1 and 1.2	See 1.2

TABLE A-4 (cont'd)

RPS FMEA

REACTOR TRIP #4

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
2.3	Power Supply (L 0751A)	Loss of Input Power Supply (Pnl Y10, Bkr #5)	The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
3.1	Bistable (LA 0751A)	Fails Tripped (Input Below Setpoint)	The bistable trip relays (K1, K2, and K3) to the RPS 2/4 logic matrix are de-energized and drop out. The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
3.2	"	Fails Un-tripped	Channel A trip for RT#4 is disabled. The effect of the failure is the same as 1.1.	Periodic Test	See 1.1	See 1.1	
3.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #5)	The bistable will go to the tripped state. See 3.1.	See 1.2	See 1.2	See 1.2	See 1.2
3.4	"	Relay K1 or K2 or K3 Fails to En-ergized State	The Channel A trip function is degrad-ed. Only 2/3 trip relays will drop out when the bistable trips. 1 of the 6 RPS trip modules cannot actuate RT#4.	Periodic Test	See 1.1	RT#6 logic is degrad-ed. Channel A trip is only 2/3 effective.	Only 1 of 6 trip modules are required to actuate a RT.
3.5	"	Relay K1 or K2 or K3 Fails to De-energized State	Partial Channel A trip. 1 of the 6 RPS trip modules is half tripped.	Status Check of Bistable Trip Relay Lights	See 1.2	1 of the 6 RPS trip modules is half tripped for RT#4.	
3.6	"	Short Across Input	The effect of the failure is the same as the bistable failing tripped (see 3.1). The instrumentation loop transmitter will compensate for the load loss and maintain valid signal levels for the additional instrumentation components in the loop.	See 3.1	See 3.1	See 3.1	
4.0	Indicator (LI 0751A)	Invalid Indi-cation	The failure does not cause local effects or induce secondary failures.	Status Check of SG#1 Water Level Indicators	The indicator is isolated from the active RPS circuits so that an indicator failure will not propagate an RPS failure. If the meter is shorted out of the instru-mentation loop circuit, the transmitter will compen-	None	

TABLE A-4 (cont'd)

RPS FMEA

REACTOR TRIP #4

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
2.3	Power Supply (L 0751A)	Loss of Input Power Supply (Pnl Y10, Bkr #5)	The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
3.1	Bistable (LA 0751A)	Fails Tripped (Input Below Setpoint)	The bistable trip relays (K1, K2, and K3) to the RPS 2/4 logic matrix are de-energized and drop out. The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
3.2	"	Fails Un-tripped	Channel A trip for RT#4 is disabled. The effect of the failure is the same as 1.1.	Periodic Test	See 1.1	See 1.1	
3.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #5)	The bistable will go to the tripped state. See 3.1.	See 1.2	See 1.2	See 1.2	See 1.2
3.4	"	Relay K1 or K2 or K3 Fails to Energized State	The Channel A trip function is degraded. Only 2/3 trip relays will drop out when the bistable trips. 1 of the 6 RPS trip modules cannot actuate RT#4.	Periodic Test	See 1.1	RT#6 logic is degraded. Channel A trip is only 2/3 effective.	Only 1 of 6 trip modules are required to actuate a RT.
3.5	"	Relay K1 or K2 or K3 Fails to De-energized State	Partial Channel A trip. 1 of the 6 RPS trip modules is half tripped.	Status Check of Bistable Trip Relay Lights	See 1.2	1 of the 6 RPS trip modules is half tripped for RT#4.	
3.6	"	Short Across Input	The effect of the failure is the same as the bistable failing tripped (see 3.1). The instrumentation loop transmitter will compensate for the load loss and maintain valid signal levels for the additional instrumentation components in the loop.	See 3.1	See 3.1	See 3.1	
4.0	Indicator (LI 0751A)	Invalid Indication	The failure does not cause local effects or induce secondary failures.	Status Check of SG#1 Water Level Indicators	The indicator is isolated from the active RPS circuits so that an indicator failure will not propagate an RPS failure. If the meter is shorted out of the instrumentation loop circuit, the transmitter will compen-	None	

TABLE A-4 (cont'd)

RPS FMEA

REACTOR TRIP #4

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
4.0 (cont'd)	Indicator (LI 0751A)				sate and maintain valid signal levels for normal RPS operation.		
5.1	Manual Switch (Trip #4 Bypass - Channel A)	Fail Open	The keylock switch is N.O. and is only used to remove an invalid trip and to change the RT configuration to 2/3.	Periodic Test	The switch is N.O. during normal plant operation.	An invalid Channel A trip cannot be by-passed to remove the half trip condition. RT#4 logic cannot be changed to a 2/3 configuration.	1 key is available for use with the 4 bypass switches (Channels A, B, C, and D). Only 1 channel trip may be bypassed.
5.2	"	Fail Closed	Three separate switch contacts in parallel with the three normally open contacts of the trip unit close and inhibit a valid channel trip.	Status Check. Light above Switch is Illuminated	See 1.1	See 1.1	
5.3	"	Single Contact Set - Fails Open	See 5.1	Periodic Test	See 5.1	1 of the 3 bistable unit trip relays cannot be bypassed after an invalid channel trip. 1 of the 6 trip logic (2/4) modules will be half tripped.	
5.4	"	Single Contact Set - Fails Closed	1 of the 3 bistable trip relays is disabled.	Periodic Test	See 1.1	1 of the 6 RPS trip logic modules cannot actuate RT#4.	
6.0	Channel B Components	All Modes	All SG#1 water level instrumentation and trip channels (A, B, C. D) are identical in configuration. The FMEA for Channel A components is applicable for all channels.			The Channel B power source is Pnl Y20, Bkr #5.	
7.0	Channel C Components	All Modes	See 6.0			The Channel C power source is Pnl Y30, Bkr #5.	
8.0	Channel D Components	All Modes	See 6.0			The Channel D power source is Pnl Y40, Bkr #5.	

TABLE A-5

FAILURE MODE AND EFFECTS ANALYSIS PALISADES PLANT REACTOR PROTECTION SYSTEM
REACTOR TRIP #5, LOW WATER LEVEL, SG#2

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
1.1	Channel A Level Transmitter (LT 0752A)	Fail High	Analog high water level signal (high voltage) to channel water level instrumentation and trip logic. Channel A trip is disabled.	Status Check of SG#2 Water Level Indicators or Periodic Test	Only 2/4 channels are required to trip to actuate RT#5.	RT#5 logic is changed to a 2/3 configuration.	
1.2	"	Fail Low	Analog low water level signal to channel trip logic. Channel A low water level trip is actuated.	Channel Trip and Pre-Trip Alarms for RT#5	RPS 2/4 logic inhibits spurious RT due to a single channel trip.	RT#5 logic is half tripped and is changed to a 1/3 configuration.	One invalid channel trip may be bypassed for RT#5. When one channel is bypassed, RT#5 logic changes to a 2/3 configuration.
1.3	"	Output Signal Constant	Constant analog water level signal level to channel water level instrumentation and trip logic. Channel A trip is disabled.	Periodic Test/ Calibration	See 1.1	See 1.1	
1.4	"	Open Signal Line	The effect of the failure is the same as fail low.	See 1.2	See 1.2	See 1.2	See 1.2
1.5	"	Signal Line Shorts to Ground	None	None	The current loop is ungrounded.	None	
1.6	"	Loss of High Pressure Tap Input	The loss of the input will generate a low level signal. See 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
1.7	"	Loss of Low Pressure Tap Input	The loss of the input will generate a high level signal. See 1.1.	See 1.1	See 1.1	See 1.1	
1.8	"	Loss of Both Pressure Tap Inputs	The loss of both inputs will generate a low level signal. See 1.2.	See 1.2	See 1.2	See 1.2	
2.1	Power Supply (L 0752A)	Loss of Output	The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
2.2	"	Off Nominal Output	The level transmitter will generate erroneous outputs. No significant operational impact unless the transmitter output is driven to an extreme condition. See 1.1, 1.2 and 1.3 for details.	See 1.1 and 1.2	See 1.1 and 1.2	See 1.1 and 1.2	See 1.2

TABLE A-5 (cont'd)

RPS FMEA

REACTOR TRIP #5

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
2.3	Power Supply (L 0752A)	Loss of Input Power Supply (Pnl Y10, Bkr #5)	The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
3.1	Bistable (LA 0752A)	Fails Tripped (Input Below Setpoint)	The bistable trip relays (K1, K2, and K3) to the RPS 2/4 logic matrix are de-energized and drop out. The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
3.2	"	Fails Un-tripped	Channel A trip for RT#5 is disabled. The effect of the failure is the same as 1.1.	Periodic Test	See 1.1	See 1.1	
3.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #5)	The bistable will go to the tripped state. See 3.1.	See 1.2	See 1.2	See 1.2	See 1.2
3.4	"	Relay K1 or K2 or K3 Fails to Energized State	The Channel A trip function is degraded. Only 2/3 trip relays will drop out when the bistable trips. 1 of the 6 RPS trip modules cannot actuate RT#5.	Periodic Test	See 1.1	RT#6 logic is degraded. Channel A trip is only 2/3 effective.	Only 1 of 6 trip modules are required to actuate a RT.
3.5	"	Relay K1 or K2 or K3 Fails to De-energized State	Partial Channel A trip. 1 of the 6 RPS trip modules is half tripped.	Status Checks of Bistable Trip Relay Lights	See 1.2	1 of the 6 RPS trip modules is half tripped for RT#5.	
3.6	"	Short Across Input	The effect of the failure is the same as the bistable failing tripped (See 3.1). The instrumentation loop transmitter will compensate for the load loss and maintain valid signal levels for the additional instrumentation components in the loop.	See 3.1	See 3.1	See 3.1	

TABLE A-5 (cont'd)

RPS FMEA

REACTOR TRIP #5

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
4.0	Indicator (LI 0752A)	Invalid Indication	The failure does not cause local effects or induce secondary failures.	Status Check of SG#2 Water Level Indicators	The indicator is isolated from the active RPS circuits so that an indicator failure will not propagate an RPS failure. If the meter is shorted out of the instrumentation loop circuit, the transmitter will compensate and maintain valid signal levels for normal RPS operation.	None	
5.1	Manual Switch (Trip #5 Bypass Channel A)	Fail Open	The keylock switch is N.O. and is only used to remove an invalid trip and to change the RT configuration to 2/3.	Periodic Test	The switch is N.O. during normal plant operation.	An invalid Channel A trip cannot be bypassed to remove the half trip condition. RT#5 logic cannot be changed to a 2/3 configuration.	1 key is available for use with the 4 bypass switches (Channels A, B, C, and D). Only 1 channel trip may be bypassed.
5.2	"	Fail Closed	Three separate switch contacts in parallel with the three normally open contacts of the trip unit close and inhibit a valid channel trip.	Status Check Light Above Switch is Illuminated	See 1.1	See 1.1	
5.3	"	Single Contact Set - Fails Open	See 5.1	Periodic Test	See 5.1	1 of the 3 bistable unit trip relays cannot be bypassed after an invalid channel trip. 1 of the 6 trip logic (2/4) modules will be half tripped.	
5.4	"	Single Contact Set - Fails Closed	1 of the 3 bistable trip relays is disabled.	Periodic Test	See 1.1	1 of the 6 RPS trip logic modules cannot actuate RT#5.	

RPS FMEA | REACTOR TRIP #5

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
6.0	Channel B Components	All Modes	All SG#2 water level instrumentation and trip channels (A, B, C, D) are identical in configuration. The FMEA for Channel A components is applicable for all channels.				The channel B power source is Pnl Y20, Bkr #5.
7.0	Channel C Components	All Modes	See 6.0				The Channel C power source is Pnl Y30, Bkr #5.
8.0	Channel D Components	All Modes	See 6.0				The Channel D power source is Pnl Y40, Bkr #5.

TABLE A-6

FAILURE MODE AND EFFECTS ANALYSIS PALISADES PLANT REACTOR PROTECTION SYSTEM
REACTOR TRIP #6, LOW PRESSURE, SG#1

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
1.1	Channel A Pressure Transmitter (PT 0751A)	Fail High	Analog high pressure signal (high voltage) to channel pressure instrumentation and trip logic. Channel A trip is disabled.	Status Check of SG#1 Pressure Indicators or Periodic Test	Only 2/4 channels are required to trip to actuate RT#6.	RT#6 logic is changed to a 2/3 configuration.	
1.2	"	Fail Low	Analog low pressure signal to channel trip logic. Channel A low pressure trip actuated.	Channel Trip and Pre-Trip Alarms for RT#6	RPS 2/4 logic inhibits spurious RT due to a single channel trip.	RT#6 logic is half tripped and is changed to a 1/3 configuration.	One invalid channel trip may be bypassed for RT#6. When one channel is bypassed, RT#6 logic changes to a 2/3 configuration.
1.3	"	Output Signal Constant	Constant analog pressure signal level to channel pressure instrumentation and trip logic. Channel A trip is disabled.	Periodic Test/ Calibration	See 1.1	See 1.1	
1.4	"	Open Signal Line	The effect of the failure is the same as fail low.	See 1.2	See 1.2	See 1.2	See 1.2
1.5	"	Signal Line Shorts to Ground	None	None	The current loop is ungrounded.	None	
1.6	"	Loss of Pressure Tap Input	See 1.4	See 1.2	See 1.2	See 1.2	See 1.2
2.1	Power Supply (P 0751A)	Loss of Output	The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
2.2	"	Off Nominal Output	The pressure transmitter will generate erroneous outputs. No significant operational impact unless the transmitter output is driven to an extreme condition. See 1.1, 1.2 and 1.3 for details.	See 1.1 and 1.2	See 1.1 and 1.2	See 1.1 and 1.2	See 1.2
2.3	"	Loss of Input Power Supply (Pnl Y10 Bkr #5)	The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
3.1	Bistable (PA 0751A)	Fails Tripped (Input Below Setpoint)	The bistable trip relays (K1, K2 and K3) to the RPS 2/4 logic matrix are deenergized and drop out. The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2

TABLE A-6 (cont'd)

RPS FMEA

REACTOR TRIP #6

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
3.2	Bistable (PA 0751A)	Fails Untripped	Channel A trip for RT#6 is disabled. The effect of the failure is the same as 1.1.	Periodic Test	See 1.1	See 1.1	
3.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #5)	The bistable will go to the tripped state. See 3.1.	See 1.2	See 1.2	See 1.2	See 1.2
3.4	"	Relay K1 or K2 or K3 Fails to Energized State	The Channel A trip function is degraded. Only 2/3 trip relays will drop out when the bistable trips. 1 of the 6 RPS trip modules cannot actuate RT#6.	Periodic Test	See 1.1	RT#6 logic is degraded. Channel A trip is only 2/3 effective.	Only 1 of 6 trip modules are required to actuate a RT.
3.5	"	Relay K1 or K2 or K3 Fails to De-energized State	Partial Channel A trip. 1 of the 6 RPS trip modules is half tripped.	Status Check of Bistable Trip Relay Lights	See 1.2	1 of the 6 RPS trip modules is half tripped for RT#6.	
3.6	"	Short Across Input	The effect of the failure is the same as the bistable failing tripped (see 3.1). The instrumentation loop transmitter will compensate for the load loss and maintain valid signal levels for the additional instrumentation components in the loop.	See 3.1	See 3.1	See 3.1	
4.1	Indicator (PIC 0751A)	Invalid Indication	The failure does not induce secondary failures. 2/4 pressure meter relays are required to trip on low pressure to automatically shut both SG1 and SG2 isolation valves. Depending on the direction of the meter error, this function is changed to either a 1/3 or 2/3 logic configuration.	Status Check of SG#1 Pressure Indicators	The indicator is isolated from the active RPS circuits so that an indicator failure will not propagate an RPS failure. If the meter is shorted out of the instrumentation loop circuit, the transmitter will compensate and maintain valid signal levels for normal RPS operation.	None	
4.2	"	Loss of Power Source (Pnl Y10 Bkr #5)	The meter reading remains valid. The meter relay is de-energized and changes the isolation valve close logic to a 1/3 configuration.	None	None required for RPS operation.	None	

TABLE A-6 (cont'd)

RPS FMEA

REACTOR TRIP #6

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
5.1	Manual Switch (Trip #6 Bypass Channel A)	Fail Open	The keylock switch is N.O. and is only used to remove an invalid trip and to change the RT configuration to 2/3.	Periodic Test	The switch is N. O. during normal plant operation.	An invalid Channel A trip cannot be by-passed to remove the half trip condition. RT#6 logic cannot be changed to a 2/3 configuration.	1 key is available for use with the 4 bypass switches (Channels A, B, C, and D). Only 1 channel trip may be bypassed.
5.2	"	Fail Closed	Three separate switch contacts in parallel with the three normally open contacts of the trip unit close and inhibit a valid channel trip.	Status Check. Light above Switch is Illuminated	See 1.1	See 1.1	
5.3	"	Single Contact Set - Fails Open	See 5.1	Periodic Test	See 5.1	1 of the 3 bistable unit trip relays cannot be bypassed after an invalid channel trip. 1 of the 6 trip logic (2/4) modules will be half tripped.	
5.4	"	Single Contact Set - Fails Closed	1 of the 3 bistable trip relays is disabled.	Periodic Test	See 1.1	1 of the 6 RPS trip logic modules cannot actuate RT#6.	
6.1	Manual Switch (Zero Power Mode Trip Bypass - Channel A)	Fail Open	The keylock switch is N.O. and is only closed for system tests when the reactor is subcritical (less than 10^{-4}% power). Channel A trips #3, 6, 7, and 9 are not bypassed during zero power reactor tests.	During Zero Power Reactor Tests, Channel Trip and Pre-Trip Alarm for RT #3, 6, 7, and 9	RPS 2/4 logic inhibits spurious RT due to the numerous trips generated in Channel A. During zero power testing, Channels B, C, and D are bypassed and thus, eliminate the possibility of a spurious RT.	None	During zero power testing Channel A trips #3, 6, 7, 9 may each be bypassed by the channel bypass switch for each trip mode.
6.2	"	Fail Closed	When the reactor is subcritical, Channel A trips #3, 6, 7, and 9 are inhibited by the application of +15 V to the bistable trip units.	Switch Bypass Position is Annunciated	When reactor power is greater than 10^{-4}%, signals from the power level trip units automatically disable the bypass by removing the +15 Volts at the bistable trip units.	None during normal plant operation. During zero power tests, the switch is N.C.	

TABLE A-6 (cont'd)

RPS FMEA

REACTOR TRIP #6

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
6.3	Manual Switch (Zero Power Mode Trip Bypass - Channel A)	Contact Set 2 Fail Open	Contact set 2 only interacts with trip #6. Channel A trip #6 is not bypassed during zero power tests.	During Zero Power Tests, Channel Trip and Pre-Trip Alarms for RT#6	During zero power tests, the RPS 2/4 logic inhibits a spurious RT#6 due to a single channel trip. The 3 other channels are by-passed to eliminate the possibility of a spurious trip.	None	
6.4	"	Contact Set 2 Fail Closed	When the reactor is subcritical, Channel A trip #6 is inhibited by the application of +15 V to the bistable trip unit.	Periodic Test	See 6.2	See 6.2	
7.0	Channel B Components	All Modes	All SG#1 pressure instrumentation and trip channels (A, B, C, D) are identical in configuration. The FMEA for Channel A components is applicable for all channels.				The Channel B power source is Pnl Y20, Bkr #5.
8.0	Channel C Components	All Modes	See 7.0				The Channel C power source is Pnl Y30, Bkr #5.
9.0	Channel D Components	All Modes	See 7.0				The Channel D power source is Pnl Y40, Bkr #5.

TABLE A-7

FAILURE MODE AND EFFECTS ANALYSIS PALISADES PLANT REACTOR PROTECTION SYSTEM
REACTOR TRIP #7, LOW PRESSURE, SG#2

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
1.1	Channel A Pressure Transmitter (P 0752A)	Fail High	Analog high pressure signal (high voltage) to channel pressure instrumentation and trip logic. Channel A trip is disabled.	Status Check of SG#2 Pressure Indicators or Periodic Test	Only 2/4 channels are required to trip to actuate RT#7.	RT#7 logic is changed to a 2/3 configuration.	
1.2	"	Fail Low	Analog low pressure signal to channel trip logic. Channel A low pressure trip actuated.	Channel Trip and Pre-Trip Alarms for RT#7	RPS 2/4 logic inhibits spurious RT due to a single channel trip.	RT#7 logic is half tripped and is changed to a 1/3 configuration.	One invalid channel trip may be bypassed for RT#7. When one channel is bypassed, RT#7 logic changes to a 2/3 configuration.
1.3	"	Output Signal Constant	Constant analog pressure signal level to channel pressure instrumentation and trip logic. Channel A trip is disabled.	Periodic Test/ Calibration	See 1.1	See 1.1	
1.4	"	Open Signal Line	The effect of the failure is the same as fail low.	See 1.2	See 1.2	See 1.2	See 1.2
1.5	"	Signal Line Shorts to Ground	None	None	The current loop is ungrounded.	None	
1.6	"	Loss of Pressure Tap Input	See 1.4	See 1.2	See 1.2	See 1.2	See 1.2
2.1	Power Supply (P 0752A)	Loss of Output	The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
2.2	"	Off Nominal Output	The pressure transmitter will generate erroneous outputs. No significant operational impact unless the transmitter output is driven to an extreme. See 1.1, 1.2 and 1.3 for details.	See 1.1 and 1.2	See 1.1 and 1.2	See 1.1 and 1.2	See 1.2
2.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #5)	The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
3.1	Bistable (PA 0752A)	Fails Tripped (Input Below Setpoint)	The bistable trip relays (K1, K2 and K3) to the RPS 2/4 logic matrix are de-energized and drop out. The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2

TABLE A-7 (cont'd)

RPS FMEA

REACTOR TRIP #7

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
3.2	Bistable (PA 0752A)	Fails Untripped	Channel A trip for RT#7 is disabled. The effect of the failure is the same as 1.1.	Periodic Test	See 1.1	See 1.1	
3.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #5)	The bistable will go to the tripped state. See 3.1.	See 1.2	See 1.2	See 1.2	See 1.2
3.4	"	Relay K1 or K2 or K3 Fails to Energized State	The Channel A trip function is degraded. Only 2/3 trip relays will drop out when the bistable trips. 1 of the 6 RPS trip modules cannot actuate RT#7.	Periodic Test	See 1.1	RT#7 logic is degraded. Channel A trip is only 2/3 effective.	Only 1 of 6 trip modules are required to actuate a RT.
3.5	"	Relay K1 or K2 or K3 Fails to De-energized State	Partial Channel A trip. 1 of the 6 RPS trip modules is half tripped.	Status Check of Bistable Trip Relay Lights	See 1.2	1 of the 6 RPS trip modules is half tripped for RT#7.	
3.6	"	Short Across Input	The effect of the failure is the same as the bistable failing tripped (see 3.1). The instrumentation loop transmitter will compensate for the load loss and maintain valid signal levels for the additional components in the loop.	See 3.1	See 3.1	See 3.1	
4.1	Indicator (PIC 0752A)	Invalid Indication	The failure does not induce secondary failures. 2/4 pressure meter relays are required to trip on low pressure to automatically shut both SG1 and SG2 isolation valves. Depending on the direction of the meter error, this function is changed to either a 1/3 or 2/3 logic configuration.	Status Check of SG#2 Pressure Indicators	The indicator is isolated from the active RPS circuits so that an indicator failure will not propagate an RPS failure. If the meter is shorted out of the instrumentation loop circuit, the transmitter will compensate and maintain valid signal levels for normal RPS operation.	None	
4.2	"	Loss of Power Source (Pnl Y10, Bkr #5)	The meter reading remains valid. The meter relay is de-energized and changes the isolation valve close logic to a 1/3 configuration.	None	None required for RPS operation.	None	

TABLE A-7 (cont'd)

RPS FMEA

REACTOR TRIP #7

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
5.1	Manual Switch (Trip #7 Bypass - Channel A)	Fail Open	The keylock switch is N.O. and is only used to remove an invalid trip and to change the RT configuration to 2/3.	Periodic Test	The switch is N.O. during normal plant operation.	An invalid Channel A trip cannot be bypassed to remove the half trip condition. RT#7 logic cannot be changed to a 2/3 configuration.	1 key is available for use with the 4 bypass switches (Channels A, B, C, and D). Only 1 channel trip may be bypassed.
5.2	"	Fail Closed	Three separate switch contacts in parallel with the three normally open contacts of the trip unit close and inhibit a valid channel trip.	Status Check. Light above Switch is Illuminated	See 1.1	See 1.1	
5.3	"	Single Contact Set - Fails Open	See 5.1	Periodic Test	See 5.1	1 of the 3 bistable unit trip relays cannot be bypassed after an invalid channel trip trip. 1 of the 6 trip logic (2/4) modules will be half tripped.	
5.4	"	Single Contact Set - Fails Closed	1 of the 3 bistable trip relays is disabled.	Periodic Test	See 1.1	1 of the 6 RPS trip logic modules cannot actuate RT#7.	
6.1	Manual Switch (Zero Power Mode Trip Bypass - Channel A)	Fail Open	The keylock switch is N.O. and is only closed for system tests when the reactor is subcritical (less than 10^{-4}% power). Channel A trips #3, 6, 7, and 9 are not bypassed during zero power reactor tests.	During Zero Power Reactor Tests, Channel Trip and Pre-Trip Alarm for RT 3, 6, 7, and 9	RPS 2/4 logic inhibits spurious RT due to the numerous trips generated in Channel A. During zero power testing, Channels B, C, and D are bypassed and thus, eliminate the possibility of a spurious RT.	None	During zero power testing Channel A trips #3, 6, 7, 9 may each be bypassed by the channel bypass switch for each trip mode.
6.2	"	Fail Closed	When the reactor is subcritical, Channel A trips #3, 6, 7, and 9 are inhibited by the application of +15 V to the bistable trip units.	Switch Bypass Position is Annunciated	When reactor power is greater than 10^{-4}%, signals from the power level trip units automatically disable the bypass by removing the +15 Volts at the bistable trip units.	None during normal plant operation. During zero power tests, the switch is N.C.	
6.3	"	Contact Set 3 Fail Open	Contact set 3 only interacts with trip #7. Channel A trip #7 is not bypassed during zero power tests.	During Zero Power Tests, Channel Trip and Pre-Trip Alarms	During zero power tests, the RPS 2/4 logic inhibits a spurious RT#7 due to a	None	

TABLE A-7 (cont'd)

RPS FMEA

REACTOR TRIP #7

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
6.3 (cont'd)	Manual Switch (Zero Power Mode Trip Bypass - Channel A)	Contact Set 3 Fail Open		for RT#7	single channel trip. The 3 other channels are by-passed to eliminate the possibility of a spurious trip.		
6.4	"	Contact Set 3 Fail Closed	When the reactor is subcritical, Channel A trip #7 is inhibited by the application of +15 V to the bistable trip unit.	Periodic Test	See 6.2	See 6.2	
7.0	Channel B Components	All Modes	All SG#2 pressure instrumentation and trip channels (A, B, C, D) are identical in configuration. The FMEA for Channel A components is applicable for all channels.				The Channel B power source is Pnl Y20, Bkr #5.
8.0	Channel C Components	All Modes	See 7.0				The Channel C power source is Pnl Y30, Bkr #5.
9.0	Channel D Components	All Modes	See 7.0				The Channel D power source is Pnl Y40, Bkr #5.

TABLE A-8

FAILURE MODE AND EFFECTS ANALYSIS PALISADES PLANT REACTOR PROTECTION SYSTEM
REACTOR TRIP #8, HIGH PRESSURIZER PRESSURE

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
1.1	Channel A Pressure Transmitter (PT 0102A)	Fail High	High analog pressure signal (high voltage) to channel pressure instrumentation and trip logic. Safety Injection System low pressure coincidence logic changes from 2/4 to 2/3. The logic to open the pressurizer power operated relief valves is half tripped and changes from 2/4 to 1/3.	Channel Trip and Pre-Trip Alarms for RT#8	RPS 2/4 logic inhibits spurious RT#8 trip due to a single channel trip. Only 2/4 channels are required to actuate RT#9.	RT#8 logic is half tripped and is changed to a 1/3 configuration. RT #9 logic is changed to a 2/3 configuration.	One invalid channel trip may be bypassed for RT#8. When one channel is bypassed, RT#8 logic changes to a 2/3 configuration.
1.2	"	Fail Low	Low analog pressure signal (low voltage) to channel pressure instrumentation and trip logic. Safety Injection System low pressure coincidence logic is half tripped and changes from 2/4 to 1/3.	Channel Trip and Pre-Trip Alarms for RT#9	RPS 2/4 logic inhibits spurious RT#9 trip due to a single channel trip. Only 2/4 channels are required to actuate RT#8.	RT#9 logic is half tripped and is changed to a 1/3 configuration. RT#9 logic is changed to a 2/3 configuration.	One invalid channel trip may be bypassed for RT#9 When one channel is bypassed, RT#9 logic changes to a 2/3 configuration.
1.3	"	Output Signal Constant	Constant analog pressure signal to channel pressure instrumentation and trip logic. All Channel A trip logic is disabled. Safety Injection System low pressure coincidence logic changes from 2/4 to 2/3. The power operated relief valve logic also changes from 2/4 to 2/3.	Periodic Test/ Calibration	Only 2/4 channels are required to trip and actuate either RT#8 or RT#9.	RT#8 logic is changed to a 2/3 configuration. RT#9 logic is changed to a 2/3 configuration.	
1.4	"	Open Signal Line	The effect of the failure is the same as fail low.	See 1.2	See 1.2	See 1.2	See 1.2
1.5	"	Signal Line Shorts to Ground	None	None	The current loop is ungrounded.	None	
1.6	"	Loss of High Pressure Tap Input	See 1.4	See 1.2	See 1.2	See 1.2	
2.1	Power Supply (P 0102A)	Loss of Output	The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
2.2	"	Off Nominal Output	The pressure transmitter will generate erroneous outputs. No significant operational impact unless the transmitter output is driven to an extreme condition. See 1.1, 1.2 and 1.3 for details.	See 1.1 and 1.2	See 1.1 and 1.2	See 1.1 and 1.2	See 1.2

TABLE A-8 (cont'd)

RPS FMEA

REACTOR TRIP #8

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
2.3	Power Supply (P 0102A)	Loss of Input Power Supply (Pnl Y10 Bkr #5)	The effect of the failure is the same as 1.2.	See 1.2	See 1.2	See 1.2	See 1.2
3.1	Bistable (PA 0102AH)	Fails Tripped (Setpoint Exceeded)	The bistable trip relays (K1, K2, and K3) to the RPS 2/4 logic matrix are de-energized and drop out. The logic to open pressurizer relief valves changes from 2/4 to 1/3.	Channel Trip and Pre-Trip Alarms for RT#8	RPS 2/4 logic inhibits spurious RT due to a single channel trip.	RT#8 logic is half tripped and is changed to a 1/3 configuration.	One invalid channel trip may be bypassed for RT#8. When one channel is bypassed, RT#8 logic changes to a 2/3 configuration.
3.2	"	Fails Untripped	Channel A trip for RT#8 is disabled. The logic to open pressurizer relief valves changes from 2/4 to 2/3.	Periodic Test	Only 2/4 channels are required to trip to actuate RT#8.	RT#8 logic is changed to a 2/3 configuration.	
3.3	"	Loss of Input Power Supply (Pnl Y10, Bkr #5)	The bistable will go to the tripped state. See 3.1.	See 3.1	See 3.1	See 3.1	See 3.1
3.4	"	Relay K1 or K2 or K3 Fails to Energized State	The Channel A trip function is degraded. Only 2/3 trip relays will drop out when the bistable trips. 1 of the 6 RPS trip modules cannot actuate RT#8.	Periodic Test	See 3.2	RT#8 logic is degraded. Channel A trip is only 2/3 effective.	Only 1 of 6 trip modules are required to actuate a RT.
3.5	"	Relay K1 or K2 or K3 Fails to De-energized State	Partial Channel A trip. 1 of the 6 RPS trip modules is half tripped.	Status Check of Bistable Trip Relay Lights	See 3.1	1 of the 6 RPS trip modules is half tripped for RT#8.	
3.6	"	Short Across Input	The effect of the failure is the same as the bistable failing untripped (see 3.2). The instrumentation loop transmitter will compensate and maintain valid signal levels for all additional instrumentation and trip components in the loop.	See 3.2	See 3.2	See 3.2	
4.1	Pressure Indicator (PIA 0102ALL)	Invalid Indication	The failure does not cause local effects or induce secondary RPS failures.	Status Check of Pressurizer Pressure Indicators	The indicator is isolated from the active RPS circuits so that an indicator failure will not propagate an RPS failure.	None	

TABLE A-8 (cont'd)

RPS FMEA

REACTOR TRIP #8

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
4.2	Pressure Indicator (PIA 0102ALL)	Short Across Input	The meter will indicate low. The Safety Injection System (SIS) low pressure coincidence logic is half tripped and changes from 2/4 to 1/3.	Lo-Lo Pressure Alarm and Status Check of Pressure Indicators	The instrumentation loop transmitter will compensate for the loss of load and maintain valid signal levels for normal RPS operation.	No effect on the RPS.	
4.3	"	Loss of Power Source (Pnl Y10, Bkr #5)	The meter reading remains valid. All meter relays are de-energized. The SIS low pressure coincidence logic changes from 2/4 to 1/3.	Lo-Lo Pressure Alarm	None required for RPS	None	
5.1	Manual Switch (Trip #8 Bypass - Channel A)	Fail Open	The keylock switch is N.O. and is only used to remove an invalid trip and to change the RT configuration to 2/3.	Periodic Test	The switch is N.O. during normal plant operation.	An invalid Channel A trip cannot be bypassed to remove the half trip condition. RT#8 logic cannot be changed to a 2/3 configuration.	1 key is available for use with the 4 bypass switches (Channels A, B, C, and D). Only 1 channel trip may be bypassed.
5.2	"	Fail Closed	Three separate switch contacts in parallel with the three normally open contacts of the trip unit close and inhibit a valid channel trip.	Status Check. Light above Switch is Illuminated	See 3.1	See 3.1	
5.3	"	Single Contact Set - Fails Open	See 5.1	Periodic Test	See 5.1	1 of the 3 bistable unit trip relays cannot be bypassed after an invalid channel trip. 1 of the 6 trip logic (2/4) modules will be half tripped.	
5.4	"	Single Contact Set - Fails Closed	1 of the 3 bistable trip relays is disabled.	Periodic Test	See 3.1	1 of the 6 RPS trip logic modules cannot actuate RT#8.	
6.0	Channel B Components	All Modes	All pressurizer pressure instrumentation and trip channels (A, B, C, D) are identical in configuration. The FMEA for Channel A components is applicable for all channels.				The Channel B power source is Pnl Y20, Bkr #5.

TABLE A-8 (cont'd)

RPS FMEA

REACTOR TRIP #8

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
7.0	Channel C Components	All Modes	See 6.0				The Channel C power source is Pnl Y30, Bkr #5.
8.0	Channel D Components	All Modes	See 6.0				The Channel D power source is Pnl Y40, Bkr #5.

TABLE A-9

FAILURE MODE AND EFFECTS ANALYSIS PALISADES PLANT REACTOR PROTECTION SYSTEM
REACTOR TRIP #9, THERMAL MARGIN/LOW PRESSURE

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
1.0	Channel A Pressure Transmitter (PT 0102A)	All Modes	Common pressurizer pressure instrumentation loops are associated with RPS RT#8 and RT#9 trip circuits. See the FMEA presented on Table A-8 (item 1.0) for the detailed analysis.				
2.0	Pressure Transmitter Power Supply	All Modes	See 1.0 above and Table A-8, item 2.0.				
3.0	Pressure Indicator (PIA 0102ALL)	All Modes	See 1.0 above and Table A-8, item 4.0.				
4.1	TM/Low Pressure Bistable (PA 0102A)	Fails Tripped (Input Signal Below Setpoint)	The bistable trip relays (K1, K2, and K3) to the RPS 2/4 logic matrix are de-energized and drop out. RT#9 channel trip signals are generated.	Channel Trip and Pre-Trip Alarms for RT#9	RPS 2/4 logic inhibits spurious RT due to a single channel trip.	RT#9 logic is half tripped and is changed to a 1/3 configuration.	One invalid channel trip may be bypassed for RT#9. When one channel is bypassed, RT#9 logic changes to a 2/3 configuration.
4.2	"	Fails Untripped	Channel A TM/low pressure trip for RT#9 is disabled.	Periodic Test	Only 2/4 channels are required to trip to actuate RT#9.	RT#9 logic is changed to a 2/3 configuration.	
4.3	"	Variable Setpoint Signal Fails High	The high setpoint will cause the bistable to trip when the input pressure signal falls below the setpoint. See 4.1.	High Setpoint Signal Alarm and Channel Trip and Pre-Trip Alarms	See 4.1	See 4.1	
4.4	"	Variable Setpoint Signal Fails Low	The low setpoint signal inhibits a valid channel trip. The effect of the failure is the same as 4.2.	Low Setpoint Signal Alarm	See 4.2	See 4.2	
4.5	"	Constant Setpoint Signal	The constant level setpoint signal will not impact RPS RT#9 operation significantly unless the signal level goes to an extreme (high or low). See 4.1 and 4.2 for details.	Periodic Test/ Calibration	See 4.1 and 4.2	See 4.1 and 4.2	
4.6	"	Relay K1 or K2 or K3 Fails to Energized State	The Channel A trip function is degraded. Only 2/3 trip relays will drop out when the bistable trips. 1 of the 6 RPS trip modules cannot actuate RT#9.	Periodic Test	See 4.2	RT#9 logic is degraded. Channel A trip is only 2/3 effective.	Only 1 of 6 trip modules are required to actuate a RT.

TABLE A-9 (cont'd)

RPS FMEA

REACTOR TRIP #9

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
4.7	TM/Low Pressure Bistable (PA 0102A)	Relay K1 or K2 or K3 Fails to De-energized State	Partial Channel A trip. 1 of the 6 RPS trip modules is half tripped.	Status Check of Bistable Trip Relay Lights	See 4.1	1 of the 6 RPS trip modules is half tripped for RT#9.	
4.8	"	Loss of Input Power Supply (Pnl Y10, Bkr #5)	The bistable will go to the tripped state. See 4.1.	See 4.1	See 4.1	See 4.1	
4.9	"	Short Across Input	The effect of the failure is the same as the bistable failing tripped (see 4.1). The instrumentation loop transmitter will compensate for the load loss and maintain valid signal levels for all additional instrumentation and trip components in the loop.	See 3.2	See 3.2	See 3.2	
5.1	Variable Setpoint Indicator (PIA 0102A)	Invalid Indication	The failure does not cause local effects or induce secondary RPS failures.	Status Check of All Setpoint Indicators	The indicator is isolated from the active RPS circuits so that an indicator failure will not propagate an RPS failure.	None	
5.2	"	Short Across Input	The meter will indicate low and initiate low pressure annuncaitor.	Lo Pressure Alarm and Status Check of Indicator	The instrumentation loop transmitter will compensate for the loss of load and maintain valid signal levels for normal RPS operation.	No effect on the RPS.	
5.3	"	Loss of Power Source (Pnl Y10, Bkr #5)	The meter reading remains valid. All meter relays are de-energized. Both the hi and lo pressure alarms are actuated.	Hi and Lo Pressure Alarms	None required for RPS operation.	None	
6.1	Setpoint Auctioneer Unit (PY 0102A)	Output Fails High	The effect of the failure is the same as 4.3.	See 4.3	See 4.1	See 4.1	
6.2	"	Output Fails Low	The low output disables the channel thermal margin trip function. The output of the unit is limited to a lower value which represents a minimum pres-	Low Setpoint Signal Alarm	See 4.2	See 4.2	

TABLE A-9 (cont'd)

RPS FMEA

REACTOR TRIP #9

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
6.2 (cont'd)	Setpoint Auctioneer Unit (PY 0102A)		sure of 1750 psia at nominal operating pressures of > 1800 psia; for nominal operating pressure of 1800 psia, this minimum is set at 1650 psia.				
6.3	"	Constant Output Signal	The effect of the failure is the same as 4.5.	See 4.5	See 4.5	See 4.5	
6.4	"	Open Output Signal Line	The effect of the failure is the same as 4.4.	See 4.4	See 4.2	See 4.2	
6.5	"	Loss of Pvar 1 Input	The auctioneer will pass the largest signal (either Pvar 1 of Pvar 2) if the level is greater than the preset floor limit.	Periodic Test or Status Check of Setpoint Indicators	The failure will not inhibit a channel trip. The channel trip will be delayed if the failure propagates a setpoint lower than the nominal value.	Possible delay of the channel trip. Only 2/4 channel trips are required to actuate RT#9.	
6.6	"	Loss of Pvar 2 Input	See 6.5	See 6.5	See 6.5	See 6.5	
6.7	"	Loss of Power Supply (Pnl)Y10, Bkr #5)	The effect of the failure is the same as 4.4.	See 4.4	See 4.4	See 4.4	
7.1	Pvar 1 Setpoint Computer (PY 0112A)	Low Output Signal	The effect of the failure is the same as 6.5.	Periodic Test	See 6.5	None	
7.2	"	High Output Signal	The auctioneer will select the largest of the two setpoint computer outputs to generate the TM trip setpoint. The effect of the failure is the same as 4.3.	See 4.3	See 4.1	See 4.1	
7.3	"	Loss of Constant Current Input (P 0112A)	See 7.1	Periodic Test	See 6.5	None	
7.4	"	Loss of Loop 1 or 2 Hot Leg Input	The computer will generate a signal equivalent to a low pressure value. The effect of the failure is the same as 7.1.	Periodic Test	See 6.5	None	

TABLE A-9 (cont'd)

RPS FMEA

REACTOR TRIP #9

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
7.5	Pvar 1 Setpoint Computer (PY 0112A)	Loss of Loop 1 or 2 Cold Leg Input	The computer will generate a signal equivalent to a high pressure value. The effect of the failure is the same as 7.2.	See 4.3	See 4.1	See 4.1	
7.6	"	Loss of Power Supply (Pnl Y10, Bkr #5)	The effect of the failure is the same as 6.5.	Periodic Test	See 6.5	None	
8.0	Pvar 2 Setpoint Computer (PY 0122A)	All Modes	The FMEA for PY 0112A (item 7.0 above) is applicable for PY 0122A.				
9.1	Constant Current Source (P 0112A)	Loss of Output to Loop 1	The effect of the failure is the same as 7.3.	Periodic Test	See 6.5	None	
9.2	"	Loss of Output to Loop 2	See 9.1	Periodic Test	See 6.5	None	
9.3	"	Loss of Output to Both Loops	The output of the auctioneer unit goes to the low limit signal level. This limit generates the channel low pressure trip setpoint at 1750 psia at nominal operating pressure > 1800 psia; or 1650 psia for a nominal operating pressure at 1800 psia.	Low Setpoint Signal Alarm	See 4.2	See 4.2	
9.4	"	Loss of Input Power Supply (Pnl Y10, Bkr # 5)	The effect of the failure is the same as 9.3.	Low Setpoint Signal Alarm	See 4.2	See 4.2	
9.5	"	High Output to Loop 1	The effect of the failure is the same as 7.2.	See 4.3	See 4.1	See 4.1	
9.6	"	High Output to Loop2	See 9.5	See 4.3	See 4.1	See 4.1	
9.7	"	High Output to Both Loops	See 9.5	See 4.3	See 4.1	See 4.1	

TABLE A-9 (cont'd)

RPS FMEA

REACTOR TRIP #9

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
10.1	Temp Transmitter Loop 1 Hot Leg (TT-0112HA)	Fail High	High signal level to the loop setpoint computer. The computer will generate a high signal level output. See 7.2.	See 4.3	See 4.1	See 4.1	
10.2	"	Fail Low	Low signal level to the loop setpoint computer. The computer will generate a low signal level output. See 7.1.	Periodic Test	See 6.5	None	
10.3	"	Constant Output Signal	The constant output signal will not impact RPS RT#9 operation significantly unless the signal level goes to an extreme (high or low). See 10.1 and 10.2.	See 10.1 and 10.2	See 10.1 and 10.2	See 10.1 and 10.2	
10.4	"	Loss of Input Power Supply (Pnl Y10, Bkr #4)	The effect of the failure is the same as fail low. See 10.2.	Periodic Test	See 6.5	None	
11.1	Temp Element Loop 1 Hot Leg (TE 0112HA)	Fail High	The effect of the failure is the same as 10.1.	See 4.3	See 4.1	See 4.1	
11.2	"	Fail Low	The effect of the failure is the same as 10.2.	Periodic Test	See 6.5	None	
11.3	"	Constant Output Signal	The effect of the failure is the same as 10.3.	See 10.1 and 10.2	See 10.1 and 10.2	See 10.1 and 10.2	
12.1	Temp Transmitter Loop 1 Cold Leg (TT-0112CA)	Fail Low	High signal level to the loop setpoint computer. The computer will generate a high signal level output. See 7.2.	See 4.3	See 4.1	See 4.1	
12.2	"	Fail High	Low signal level to the loop setpoint computer. The computer will generate a low signal level output. See 7.1.	Periodic Test	See 6.5	None	
12.3	"	Constant Output Signal	The constant output signal will not impact RPS RT#9 operation significantly unless the signal level goes to an extreme (high or low). See 12.1 and 12.2.	See 12.1 and 12.2	See 12.1 and 12.2	See 12.1 and 12.2	

RPS FMEA

REACTOR TRIP #9

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
12.4	Temp Transmitter Loop 1 Cold Leg (TT-0112CA)	Loss of Input Power Supply (Pnl Y10, Bkr #4)	The effect of the failure is the same as fail low. See 12.1.	Periodic Test	See 6.5	None	
13.1	Temp Element Loop 1 Cold Leg (TE 0112CA)	Fail Low	The effect of the failure is the same as 12.1.	See 4.3	See 4.1	See 4.1	
13.2	"	Fail High	The effect of the failure is the same as 12.2.	Periodic Test	See 6.5	None	
13.3	"	Constant Output Signal	The effect of the failure is the same as 12.3.	See 12.1 and 12.2	See 12.1 and 12.2	See 12.1 and 12.2	
14.0	Loop 1 Cold Leg Temp Indicator (TI 0112CA)	Invalid Indication	The failure does not cause local effects or induce secondary RPS failures.	Status Check of Temp Indicators	The indicator is isolated from the RPS circuits so that an indicator failure will not propagate an RPS failure.	None	
15.0	Loop 1 Hot Leg Temp Indicator (TI 0112HA)	Invalid Indication	See 14.0	See 14.0	See 14.0	None	
16.0	Loop 2 Components	All Modes	Both loop 1 and loop 2 temperature instrumentation and signal processing channels are identical in configuration. The FMEA for loop 1 components (items 10 - 15) is applicable for loop 2 components.				
17.1	Manual Switch (Trip #9 Bypass - Channel A)	Fail Open	The keylock switch is N.O. and is only used to remove an invalid trip and to change the RT configuration to 2/3.	Periodic Test	The switch is N.O. during normal plant operation.	An invalid Channel A trip cannot be bypassed to remove the half trip condition. RT#9 logic cannot be changed to a 2/3 configuration.	1 key is available for use with the 4 bypass switches (Channels A, B, C, and D). Only 1 channel trip may be bypassed.
17.2	"	Fail Closed	Three separate switch contacts in parallel with the three normally open contacts of the trip unit close and inhibit a valid channel trip.	Status Check. Light above Switch is Illuminated	See 4.2	See 4.2	

TABLE A-9 (cont'd)

RPS FMEA

REACTOR TRIP #9

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
17.3	Manual Switch (Trip #9 Bypass - Channel A)	Single Contact Set - Fails Open	See 17.1	Periodic Test	See 17.1	1 of the 3 bistable unit trip relays cannot be bypassed after the invalid channel trip. 1 of the 6 trip logic (2/4) modules will be half tripped.	
17.4	"	Single Contact Set - Fails Closed	1 of the 3 bistable trip relays is disabled.	Periodic Test	See 4.2	1 of the 6 RPS trip logic modules cannot actuate RT#9.	
18.1	Manual Switch (Zero Power Mode Trip Bypass - Channel A)	Fail Open	The keylock switch is N.O. and is only closed for system tests when the reactor is subcritical (less than 10^{-4}% power). Channel A trips #3, 6, 7, and 9 are not bypassed during zero power reactor tests.	During Zero Power Reactor Tests, Channel Trip and Pre-Trip Alarm for RT#3, 6, 7, and 9	RPS 2/4 logic inhibits spurious RT due to the numerous trips generated in Channel A. During zero power testing, channels B, C, and D are bypassed and thus eliminate the possibility of a spurious RT.	None	During zero power testing, Channel A trips #3, 6, 7,9 may each be bypassed by the channel bypass switch for each trip mode.
18.2	"	Fail Closed	When the reactor is subcritical, Channel A trips #3, 6, 7, and 9 are inhibited by the application of +15 V to the bistable trip units.	Switch Bypass Position is Annunciated	When reactor power is greater than 10^{-4}%, signals from the power level trip units automatically disable the bypass by removing the +15 volts at the bistable trip units.	None during normal plant operation. During zero power tests, the switch is N.C.	
18.3	"	Contact Set 4 Fail Open	Contact set 4 only interacts with trip #9. Channel A trip #9 is not bypassed during zero power tests.	During Zero Power Tests, Channel Trip and Pre-Trip Alarms for RT#9	During zero power tests, the RPS 2/4 logic inhibits a spurious RT#9 due to a single channel trip. The 3 other channels are bypassed to eliminate the possibility of a spurious trip.		
18.4	"	Contact Set 4 Fail Closed	When the reactor is subcritical, Channel A trip #9 is inhibited by the application of +15 V to the bistable trip unit.	Periodic Test	See 6.2	See 6.2	

TABLE A-9 (cont'd)

RPS FMEA

REACTOR TRIP #9

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
19.0	Channel B Components	All Modes	All thermal margin and low pressure instrumentation and trip channels (A, B, C, D) are identical in configuration. The FMEA for Channel A components (items 1 - 18) is applicable for all channels.				The Channel B power source is Pnl Y20, Bkr #4 and 5.
20.0	Channel C Components	All Modes	See 19.0				The Channel C power source is Pnl Y30, Bkr #4 and 5.
21.0	Channel D Components	All Modes	See 19.0				The Channel D power source is Pnl Y40, Bkr #4 and 5.

TABLE A-10

FAILURE MODE AND EFFECTS ANALYSIS PALISADES PLANT REACTOR PROTECTION SYSTEM
REACTOR TRIP #10, LOSS OF LOAD, TURBINE TRIP

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
1.1	Pressure Switch, Turbine Auto Stop (63/ AST-2)	Contacts Fail Open	The pressure switch is N.O. when the turbine is operating.	Periodic Test	None	RT#10 is inhibited.	Single fault inhibits RT#10. The loss of load reactor trip is an anticipatory trip which is not required to protect the reactor since the primary trip is high system pressure (FSAR 7.2.3.6).
1.2	"	Fail Closed	The switch is normally closed when there is a loss of pressure in the auto stop oil. RT#10 is actuated if reactor power is greater than 15%.	RT#10 is Actuated	None	RT#10 is actuated when reactor power is greater than 15%.	
2.1	Time Delay Relay (462/TDO)	Fails to Energized and Tripped State	The relay normally cuts out (de-energizes) turbine trip relays (305L and 305R) 3 seconds after the auto stop pressure switch closes. When the relay (TDO) fails to the tripped state, RT#10 cannot be actuated.	Periodic Test	None	RT#10 is inhbited.	See 1.1
2.2	"	Fails to Untripped State	The turbine trip relays 305L and 305R are constantly energized when the the auto stop pressure switch is closed.	Periodic Test	None required for the RPS function.	None	
3.1	Turbine Trip Relay Power Source (125 VDC Pnl D21, Bkr 72-212)	Loss of Output	The effect of the failure is the same as 1.1.	Control Circuit U.V. Relay 374 UI Alarm	None	RT#10 is inhibited.	See 1.1
3.2	"	Off Nominal Output	No effect if turbine trip relays L and R can be pulled in when required. If the relays cannot be pulled in, the effect of the failure is the same as 1.1.	See 3.1	None	RT#10 is inhibited.	See 1.1
3.3	"	Short Across Output Lines or Open Output Line	The effect of the failure is the same as 1.1.	Periodic Test	None	RT#10 is inhibited.	See 1.1

TABLE A-10 (cont'd)

RPS FMEA

REACTOR TRIP #10

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
4.1	Turbine Trip Relay 305L	Fails to Energized State	N.C. contacts open and remove voltage from the Channel A and C aux trip unit relays (K1, K2, and K3).	Channel A and C Trip Alarms for RT#10	None	Spurious reactor trip results when reactor power level is above 15%.	
4.2	"	Fails to De-energized State	Channel A and C aux trip units cannot be tripped.	Periodic Test	1/2 turbine trip relays are required to actuate RT#10.	RT#10 trip logic is changed to a 2/2 configuration.	
5.1	Turbine Trip Relay 305R	Fails to Energized State	N.C. contacts open and remove voltage from Channel B and D aux trip unit relays (K1, K2, and K3).	Channel A and B Trip and Pre-Trip Alarms for RT#10	None	See 4.1	
5.2	"	Fails to De-energized State	Channel B and D aux trip units cannot be tripped.	Periodic Test	See 4.2	See 4.2	
6.1	Channel A Aux Trip Unit	Fails Tripped	The trip relays (K1, K2, and K3) to the RPS 2/4 logic matrix are de-energized and drop out.	Channel Trip and Pre-Trip Alarms for RT#10	RPS 2/4 logic inhibits spurious RT#10 due to a single channel trip.	RT#10 logic is half tripped and is changed to a 1/3 configuration.	One invalid channel trip may be bypassed for RT#10. When a channel is bypassed, RT#10 logic changes to a 2/3 configuration.
6.2	"	Fails Untripped	Channel A trip for RT#10 is disabled.	Periodic Test	Only 2/4 channels are are required to trip to actuate RT#10.	RT#10 logic is changed to a 2/3 configuration.	
6.3	"	Loss of Input Signal Power Supply (Pnl Y20, Bkr #13)	The aux trip unit will go to the tripped state. See 6.1.	See 6.1	See 6.1	See 6.1	
6.4	"	Relay K1 or K2 or K3 Fails to Energized State	The Channel A trip function is degraded. Only 2/3 trip relays will drop out when the aux trip unit trips. 1 of the 6 RPS trip modules cannot actuate RT #10.	Periodic Test	See 6.1	RT#10 logic is degraded. Channel A trip is only 2/3 effective.	Only 1 of 6 trip modules are required to actuate a RT.
6.5	"	Relay K1 or K2 or K3 Fails to De-energized State.	Partial Channel A trip. 1 of the 6 RPS trip modules is half tripped.	Status Check of Aux Trip Unit Trip Relay Lights	See 6.2	1 of the 6 RPS trip modules is half tripped for RT#10.	

TABLE A-10 (cont'd)

RPS FMEA

REACTOR TRIP #10

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
7.1	Manual Switch (Trip #10 Bypass - Channel A)	Fail Open	The keylock switch is N.O. and is only used to remove an invalid trip and to change the RT configuration to 2/3.	Periodic Test	The switch is N.O. during normal plant operation.	An invalid Channel A trip cannot be by-passed to remove the half trip condition. RT#10 logic cannot be changed to a 2/3 con-figuration.	1 key is available for use with the 4 bypass switches (Channels A, B, C, and D). Only 1 channel trip may be bypassed.
7.2	"	Fail Closed	Three separate switch contacts in par-allel with the three normally open con-tacts of the aux trip unit relays close and inhibit a valid channel trip.	Status Check. Light above Switch is Illuminated	See 6.1	See 6.1	
7.3	"	Single Con-tact Set - Fails Open	See 7.1	Periodic Test	See 7.1	1 of the 3 bistable unit trip relays can-not be bypassed after an invalid channel trip. 1 of the 6 trip logic (2/4) modules will be half tripped.	
7.4	"	Single Con-tact Set - Fails Closed	1 of the 3 aux trip unit trip relays is disabled.	Periodic Test	See 6.1	1 of the 6 RPS trip logic modules cannot actuate RT#10.	
8.0	Channel B Components	All Modes	All loss of load (turbine trip) instru-mentation and trip channels (A, B, C, D) are identical in configuration. The FMEA for Channel A components (items 6.0 and 7.0) is applicable for all chan-nels.				The Channel B power source is Pnl Y20, Bkr #13.
9.0	Channel C Components	All Modes	See 8.0				The Channel C power source is Pnl Y30, Bkr #13.
10.0	Channel D Components	All Modes	See 8.0				The Channel D power source is Pnl Y40, Bkr #13.

TABLE A-11

FAILURE MODE AND EFFECTS ANALYSIS PALISADES PLANT REACTOR PROTECTION SYSTEM
REACTOR TRIP #11, HIGH CONTAINMENT PRESSURE

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
1.1	Pressure Switch - Channel A (PS 1801)	Fail High	The N.C. pressure switch contacts open and remove voltage from the aux trip unit trip relays (K1, K2, and K3).	Channel Trip Alarms for RT#11	RPS 2/4 logic inhibits spurious RT#11 due to a single channel trip.	RT#11 logic is half tripped and is changed to a 1/3 configuration.	One invalid channel trip may be bypassed for RT#11. When one channel is bypassed, RT#11 logic changes to a 2/3 configuration.
1.2	"	Fail Low	The N.C. pressure switch contacts remain closed. Channel A high containment trips are disabled for RT#11.	Periodic Test	Only 2/4 channels are required to trip to actuate RT#11.	RT#11 logic is changed to a 2/3 configuration.	
1.3	"	Open Signal Line	The effect of the failure is the same as fail high. See 1.1.	See 1.1	See 1.1	See 1.1	See 1.1
1.4	"	Open Sense Line	The effect of the failure is the same as fail low. See 1.2.	Containment High Pressure Test	See 1.2	See 1.2	See 1.2
2.1	Aux Trip Unit Channel A	Fails Tripped	The trip relays (K1, K2, and K3) to the RPS 2/4 logic matrix are de-energized and drop out.	See 1.1	See 1.1	See 1.1	See 1.1
2.2	"	Fails Untripped	Channel A trip for RT#11 is disabled.	Periodic Test	See 1.2	See 1.2	
2.3	"	Loss of Input Signal Power Supply (Pnl Y10, Bkr #13)	The aux trip unit will go to the tripped state. See 2.1.	See 1.1	See 1.1	See 1.1	See 1.1
2.4	"	Relay K1 or K2 or K3 Fails to Energized State	The Channel A trip function is degraded. Only 2/3 trip relays will drop out when the trip unit trips. 1 of the 6 RPS trip modules cannot actuate RT#11.	Periodic Test	See 1.2	RT#11 logic is degraded. Channel A trip is only 2/3 effective.	Only 1 of 6 trip modules are required to actuate an RT.
2.5	"	Relay K1 or K2 or K3 Fails to De-energized State	Partial Channel A trip. 1 of the 6 RPS trip modules is half tripped.	Status Check of Aux Trip Unit Trip Relay Lights	See 1.1	1 of the 6 RPS trip modules is half tripped for RT#11.	
3.1	Manual Switch (Trip #11 Bypass - Channel A)	Fail Open	The keylock switch is N.O. and is only used to remove an invalid trip and to change the RT configuration to 2/3.	Periodic Test	The switch is N.O. during normal plant operation.	An invalid Channel A trip cannot be bypassed to remove the half trip condition. RT#11 logic cannot be changed to a 2/3 configuration.	1 key is available for use with the 4 bypass switches (Channels A, B, C, and D). Only 1 channel trip may be bypassed.

TABLE A-11 (cont'd)

RPS FMEA

REACTOR TRIP #11

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
3.2	Manual Switch (Trip #11 Bypass - Channel A)	Fail Closed	Three separate switch contacts in parallel with the three normally open contacts of the aux trip unit relays close and inhibit a valid channel trip.	Status Check. Light above Switch is Illuminated	See 1.1	See 1.1	
3.3	"	Single Contact Set - Fails Open	See 3.1	Periodic Test	See 3.1	1 of the 3 bistable unit trip relays cannot be bypassed after the invalid channel trip. 1 of the 6 trip logic (2/4) modules will be half tripped.	
3.4	"	Single Contact Set - Fails Closed	1 of the 3 aux trip unit trip relays is disabled.	Periodic Test	See 1.1	1 of the 6 RPS trip logic modules cannot actuate RT#11.	
4.0	Channel B Components	All Modes	All high containment pressure trip channels (A, B, C, D) are identical in configuration. The FMEA for Channel A components is applicable for all channels.				The Channel B power source is Pnl Y20, Bkr #13.
5.0	Channel C Components	All Modes	See 4.0				The Channel C power source is Pnl Y30, Bkr #13.
6.0	Channel D Components	All Modes	See 4.0				The Channel D power source is Pnl Y40, Bkr #13.

TABLE A-12

FAILURE MODE AND EFFECTS ANALYSIS PALISADES PLANT REACTOR PROTECTION SYSTEM
REACTOR TRIP #12, MANUAL

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
1.1	Reactor Trip Pushbutton #1	Contact Set 1-1 Fail Closed	Cannot de-energize the undervoltage coil of breaker CB-1 which powers clutch power supplies PS1 and PS3.	Periodic Test	Manual trip switch 2 provides a backup capability to remove power from clutch supplies PS1 and PS3.	The RT#12 actuation function is reduced to a 1/1 configuration.	
1.2	"	Contact Set 1-1 Fail Open	Clutch power supplies PS1 and PS3 are de-energized.	Clutch Power Supply Alarm	Redundant power supplies PS-2 and PS-4 can support the clutch power requirements and inhibit a spurious RT.	One of the two pairs of redundant clutch power supplies remains operative.	
1.3	"	Contact Set 1-2 Fail Closed	Cannot de-energize the undervoltage coil of breaker CB-2 which powers clutch power supplies PS2 and PS4.	Periodic Test	Manual trip switch 2 provides a backup capability to remove power from clutch supplies PS2 and PS4.	The RT#12 actuation function is reduced to a 1/1 configuration.	
1.4	"	Contact Set 1-2 Fail Open	Clutch power supplies PS2 and PS4 are de-energized.	Clutch Power Supply Alarm	Redundant power supplies PS1 and PS3 can support the clutch power requirements and inhibit a spurious RT.	One of the two pairs of redundant clutch power supplies remains operative.	
1.5	"	Switch Fails Open	Spurious RT.	RT Alarms	None	Spurious RT.	
1.6	"	Switch Fails Closed	The switch is closed during plant operation and would not be detected.	Periodic Test	Only 1/2 trip switches are required to actuate a manual scram (RT#12).	RT#12 actuation is reduced to a 1/1 configuration.	
2.1	Reactor Trip Pushbutton #2	Contact Set 2-1 Fail Closed	Cannot de-energize relay M1 and thus remove the AC input power to clutch power supplies PS1 and PS3.	Periodic Test	Contact set 2-2 can de-energize relay M2 which is redundant to relay M1.	None. Either manual trip switches can actuate a scram.	
2.2	"	Contact Set 2-1 Fail Open	Relay M1 is de-energized and drops out. The AC input power to clutch power supplies PS1 and PS3 is removed.	Clutch Power Supply Alarm	Redundant power supplies PS2 and PS4 can support the clutch power requirements and inhibit a spurious RT.	One of the two pairs of redundant clutch power supplies remains operative.	
2.3	"	Contact Set 2-2 Fail Closed	Cannot de-energize relay M2 and thus remove the AC input power to clutch power supplies PS1 and PS3.	Periodic Test	Contact set 2-1 can de-energize relay M1 which is redundant to relay M2.	None. Either manual trip switches can actuate a scram.	

TABLE A-12 (cont'd)

RPS FMEA — REACTOR TRIP #12

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
2.4	Reactor Trip Pushbutton #2	Contact Set 2-2 Fail Open	Relay M2 is de-energized and drops out. The AC input power to clutch power supplies PS1 and PS3 is removed.	Clutch Power Supply Alarm	Redundant power supplies PS2 and PS4 can support the clutch power requirements and inhibit a spurious RT.	One of the two pairs of redundant clutch power supplies remains operative.	
2.5	"	Contact Set 2-3 Fail Closed	Cannot de-energize relay M3 and thus remove the AC input power to clutch power supplies PS2 and PS4.	Periodic Test	Contact set 2-4 can de-energize relay M4 which is redundant to relay M3.	None. Either manual trip switches can actuate a scram.	
2.6	"	Contact Set 2-3 Fail Open	Relay M3 is de-energized and drops out. The AC input power to clutch power supplies PS2 and PS4 is removed.	Clutch Power Supply Alarm	Redundant power supplies PS1 and PS3 can support the clutch power requirements and inhibit a spurious RT.	One of the two pairs of redundant clutch power supplies remains operative.	
2.7	"	Contact Set 2-4 Fail Closed	Cannot de-energize relay M4 and thus remove the AC input power to clutch power supplies PS2 and PS4.	Periodic Test	Contact set 2-3 can de-energize relay M3 which is redundant to relay M4.	None. Either manual trip switches can actuate a scram.	
2.8	"	Contact Set 2-4 Fail Open	Relay M4 is de-energized and drops out. The AC input power to clutch power supplies PS2 and PS4 is removed.	Clutch Power	Redundant power supplies PS1 and PS3 can support the clutch power requirements and inhibit a spurious RT.	One of the two pairs of redundant clutch power supplies remains operative.	
2.9	"	Switch Fails Open	Spurious RT.	RT Alarms	None	Spurious RT.	
2.10	"	Switch Fails Closed	The switch is closed during plant operation and would not be detected.	Periodic Test	Only 1/2 trip switches are required to actuate a manual scram (RT#12).	RT#12 actuation is reduced to a 1/1 configuration.	

TABLE A-13

FAILURE MODE AND EFFECTS ANALYSIS PALISADES PLANT REACTOR PROTECTION SYSTEM
REACTOR TRIP MATRIX AND TRIP TRAIN

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
1.0	Clutch Power Supply PS1	Loss of Output	Relay K1 is de-energized and drops out. This causes relays M1 and M2 to be de-energized. AC power from panel Y30 is removed from PS1 and PS3.	Clutch Power Supply Alarm	Redundant clutch power supplies PS2 and PS4 inhibit spurious RT.	One of the two pairs of redundant clutch power supplies remain operative.	
2.0	Clutch Power Supply PS2	Loss of Output	Relay K3 is de-energized and drops out. This causes relays M1 and M2 to be de-energized. See 1.0.	See 1.0	See 1.0	See 1.0	
3.1	Relay K1	Fails to Energized State	Relay is normally energized when PS1 and PS3 are operational. When PS1 and PS3 are de-energized via a scram, the relay is de-energized. When de-energized, contacts from the relay inhibit automatic reset of the scram (energize power supplies PS1 and PS2) after the conditions that initiated the scram are removed. The automatic time delay associated with manual scram reset (relay BW11-KTD-1) is disabled.	Periodic Test	Relays K1 and K3 both provide the inhibit to automatic reset.	Loss of automatic time delay of scram manual reset function. The logic to inhibit automatic reset of scram is changed to a 1/1 configuration.	
3.2	"	Fails to De-energized State	The effect of the failure is the same as 1.0.	See 1.0	See 1.0	See 1.0	
4.1	Relay K3	Fails to Energized State	Relay is normally energized when PS1 and PS3 are operational. When PS1 and PS3 are de-energized via a scram, the relay is de-energized. When de-energized, contacts from the relay inhibit automatic reset of the scram (energize power supplies PS1 and PS2) after the conditions that initiated the scram are removed.	Periodic Test	Relays K1 and K3 both provide the inhibit to automatic reset.	The logic to inhibit automatic reset of scram is changed to a 1/1 configuration.	
4.2	"	Fails to De-energized State	The effect of the failure is the same as 2.0.	See 1.0	See 1.0	See 1.0	
5.1	Time Delay Relay (BW11-KTD-1)	Fails to Energized State	The trip reset switch cannot enable PS1 and PS3 to be energized after a scram.	Periodic Test	Redundant power supplies PS2 and PS4 can be energized after a scram by the reset switches.	One of the two pairs of redundant clutch power supplies remain operative after scram reset.	

TABLE A-13 (cont'd)

RPS FMEA

REACTOR TRIP MATRIX AND TRAIN

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
5.2	Time Delay Relay (BW11-KTD-1)	Fails to De-energized State	The automatic time delay associated with manual scram reset is disabled.	Periodic Test	None	Loss of automatic time delay on scram reset function.	
5.3	"	Loss of Power Supply (Pnl Y20)	The effect of the failure is the same as 5.2.	Periodic Test	None	See 5.2	
6.1	M Coil, Relay M1	Fails to Energized State	RT signals from AB1, AC1, AD1, BC1, BD1, CD1, and manual trip switch 1-1 are disabled.	Periodic Test	Redundant signals to redundant relay M2 remove AC input power to clutch power supplies PS1 and PS3.	RT logic to PS1 and PS3 changes from a 1/2 configuration to 1/1.	
6.2	"	Fails to De-energized State	The clutch power supplies PS1 and PS3 are disabled.	Clutch Power Supply Alarm	Redundant clutch power supplies PS2 and PS4 inhibit spurious RT.	One of the two pairs of redundant clutch power supplies remain operative.	
7.1	Trip Relay AB1	Fails to Energized State	Relay M1 cannot be de-energized when the associated logic matrix (e.g., AB) is tripped.	Periodic Test	The tripped logic matrix relay #2 (e.g., AB2) will de-energize relay M2 and remove power from power supplies PS1 and PS3.	See 6.1	
7.2	"	Fails to De-energized State	Relay M1 is de-energized and drops out. See 6.2.	See 6.2	See 6.2	See 6.2	
8.1	Trip Relay AC1	Fails to Energized State	See 7.1	See 7.1	See 7.1	See 6.1	
8.2	"	Fails to De-energized State	See 7.2	See 6.2	See 6.2	See 6.2	
9.1	Trip Relay AD1	Fails to Energized State	See 7.1	See 7.1	See 7.1	See 6.1	
9.2	"	Fails to De-energized State	See 7.2	See 6.2	See 6.2	See 6.2	

TABLE A-13 (cont'd)

RPS FMEA

REACTOR TRIP MATRIX AND TRAIN

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
10.1	Trip Relay BC1	Fails to Energized State	See 7.1	See 7.1	See 7.1	See 6.1	
10.2	"	Fails to De-energized State	See 7.2	See 6.2	See 6.2	See 6.2	
11.1	Trip Relay BD1	Fails to Energized State	See 7.1	See 7.1	See 7.1	See 6.1	
11.2	"	Fails to De-energized State	See 7.2	See 6.2	See 6.2	See 6.2	
12.1	Trip Relay CD1	Fails to Energized State	See 7.1	See 7.1	See 7.1	See 6.1	
12.2	"	Fails to De-energized State	See 7.2	See 6.2	See 6.2	See 6.2	
13.1	Isolation Transformer	Loss of Output	Relay M1 is de-energized. See 6.2.	See 6.2	See 6.2	See 6.2	
13.2	"	Loss of Input Power Supply (Pnl Y30)	The effect of the failure is the same as 13.1.	See 6.2	See 6.2	See 6.2	
13.3	"	Open Output Line or Short Across Output	See 13.2	See 6.2	See 6.2	See 6.2	
13.4	"	Single Short to Ground on Output Line	None	Ground Fault Light	The system has a floating ground.	None	
14.0	Isolation Transformer Fuse	Fail Open	Relay M1 is de-energized. See 6.2	See 6.2	See 6.2	See 6.2	

TABLE A-13 (cont'd)

RPS FMEA

REACTOR TRIP MATRIX AND TRAIN

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
15.1	M Coil, Relay M2	Fails to Energized State	RT signals from AB2, AC2, AD2, BC2, BD2, CD2 and manual trip switch 1-2 are disabled.	Periodic Test	Redundant signals to redundant relay M2 remove AC input power to clutch power supplies PS1 and PS3.	RT logic to PS1 and PS3 changes from a 1/2 configuration to 1/1.	
15.2	"	Fails to De-energized State	The clutch power supplies PS1 and PS3 are disabled.	Clutch Power Supply Alarm	Redundant clutch power supplies PS2 and PS4 inhibit spurious RT.	One of the two pairs of redundant clutch power supplies remain operative.	
16.1	Trip Relay AB2	Fails to Energized State	Relay M2 cannot be de-energized when the associated logic matrix is tripped.	Periodic Test	The tripped logic matrix will de-energize matrix relay #1 (e.g., AB1) will de-energize relay M2 and remove power from power supplies PS1 and PS3.	See 15.1	
16.2	"	Fails to De-energized State	Relay M2 is de-energized and drops out. See 15.2.	See 15.2	See 15.2	See 15.2	
17.1	Trip Relay AC2	Fails to Energized State	See 16.1	See 16.1	See 16.1	See 16.1	
17.2	"	Fails to De-energized State	See 16.2	See 15.2	See 15.2	See 15.2	
18.1	Trip Relay AD2	Fails to Energized State	See 16.1	See 16.1	See 16.1	See 16.1	
18.2	"	Fails to De-energized State	See 16.2	See 15.2	See 15.2	See 15.2	
19.1	Trip Relay BC2	Fails to Energized State	See 16.1	See 16.1	See 16.1	See 15.1	

RPS FMEA

REACTOR TRIP MATRIX AND TRAIN

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
19.2	Trip Relay BC2	Fails to De-energized State	See 16.2	See 15.2	See 15.2	See 15.2	
20.1	Trip Relay BD2	Fails to En-ergized State	See 16.1	See 16.1	See 16.1	See 15.1	
20.2	"	Fails to De-energized State	See 16.2	See 15.2	See 15.2	See 15.2	
21.1	Trip Relay CD2	Fails to En-ergized State	See 16.1	See 16.1	See 16.1	See 15.1	
21.2	"	Fails to De-energized State	See 16.2	See 15.2	See 15.2	See 15.2	
22.1	Isolation Transformer	Loss of Out-put	Relay M2 is de-energized. See 15.2.	See 15.2	See 15.2	See 15.2	
22.2	"	Loss of Input Power Supply (Pnl Y30)	The effect of the failure is the same as 22.1.	See 15.2	See 15.2	See 15.2	
22.3	"	Open Output Line or Short Across Out-put	See 22.2	See 15.2	See 15.2	See 15.2	
22.4	"	Single Short to Ground on Output Line	None	Ground Fault Light	The system has a floating ground.	None	
23.0	Isolation Transformer Fuse	Fail Open	Relay M2 is de-energized. See 15.2.	See 15.2	See 15.2	See 15.2	

TABLE A-13 (cont'd)

RPS FMEA

REACTOR TRIP MATRIX AND TRAIN

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
24.1	Transformer T1	Loss of Output	CB1 undervoltage coil will drop out, open CB1 and de-energize the input to PS1 and PS3.	Clutch Power Supply Alarm	See 15.2	See 15.2	
24.2	"	Loss of Input (Pnl Y30)	See 24.1	See 24.1	See 15.2	See 15.2	
24.3	"	Open Output Line or Short Across Output	See 24.1	See 24.1	See 15.2	See 15.2	
24.4	"	Single Short to Ground on Output Line	None	Ground Fault Light	The system has a floating ground.	None	
25.1	Circuit Breaker CB1	Fail Open	Clutch power supplies PS1 and PS2 are de-energized.	Clutch Power Supply Alarm	See 15.2	See 15.2	
25.2	"	Fail Closed	Manual trip switch #1 is disabled. CB will not drop out due to undervoltage or overcurrent.	Periodic Test	Redundant reactor trip switch can actuate scram.	Manual reactor trip switch configuration reduced to 1/1.	
26.0	Reactor Trip Train #2 Components	All Modes	Both reactor trip trains #1 and #2 are identical in configuration. The only difference is in preferred bus interfaces. Panel Y40 supplies power to the clutch power supplies and panel Y30 supplies power to the automatic reset inhibit time delay relay. The FMEA for the train #1 components (items 1 - 25) is applicable for train #2.				
27.1	AB Matrix Power Supply PS5	Loss of Output	None	Rack Status Light Check	Redundant power supply PS6 will hold in the 4 matrix trip relays.	The power supplies available to hold in the 4 trip relays are reduced to a 1/1 configuration. The reactor will scram if the remaining power supply output fails.	
27.2	"	Loss of Input Power Supply (Pnl Y10)	None	See 27.1	See 27.1	See 27.1	

TABLE A-13 (cont'd)

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
27.3	AB Matrix Power Supply PS5	Short Across Output	All 4 matrix trip relays are de-energized and cause relays M1, M2, M3, and M4 to be de-energized and drop out. Power is then removed from the input to all clutch power supplies.	RT Alarm	None	Spurious RT.	
27.4	"	Single Short to Ground on Output Line	None	None	The system has a floating ground.	None	
28.1	PS5 Isolation Transformer	Loss of Output	None	See 27.1	See 27.1	See 27.1	
28.2	"	Loss of Input Power Supply (Pnl Y10)	None	See 27.1	See 27.1	See 27.1	
28.3	"	Open Output Line or Short Across Output	None	See 27.1	See 21.1	See 27.1	
28.4	"	Single Short to Ground on Output Line	None	Periodic Test	The system has a floating ground.	None	
29.0	PS5 Fuse	Fail Open	None	See 27.1	See 27.1	See 27.1	
30.1	AB Matrix Power Supply PS6	Loss of Output	None	See 27.1	Redundant power supply PS5 will hold in the 4 matrix trip relays.	See 27.1	
30.2	"	Loss of Input Power Supply (Pnl Y20)	None	See 27.1	See 30.1	See 27.1	
30.3	"	Short Across Output	See 27.3	RT Alarm	None	Spurious RT.	

TABLE A-13 (cont'd)

RPS FMEA

REACTOR TRIP MATRIX AND TRAIN

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
30.4	AB Matrix Power Supply PS6	Single Short to Ground on Output Line	None	None	See 27.4	None	
31.1	PS6 Isolation Transformer	Loss of Output	None.	See 27.1	See 30.1	See 27.1	
31.2	"	Loss of Input Power Supply (Pnl Y20)	None	See 27.1	See 30.1	See 27.1	
31.3	"	Open Output Line or Short Across Output	None	See 27.1	See 30.1	See 27.1	
31.4	"	Single Short to Ground on Output Line	None	None	See 27.4	None	
32.0	PS6 Fuse	Fail Open	None	See 27.1	See 27.1	See 27.1	
33.1	Matrix Logic AB Test Switch	Fail Open	The switch is N.O. and only closed during test of AB logic. During test, the test power supply (PS17) cannot hold in the matrix trip relays.	At the Start of Logic Test, the Trip Relay "Hold" Lights Would Not Illuminate	None	Unable to test trip logic without generating a spurious RT.	
33.2	"	Fail Closed	The AB trip matrix relays are held in when the test power supply is energized. No hold in power can be applied to the trip relays of any other matrix.	When PS17 is Energized, the Matrix AB Trip Relay "Hold" Lights Are Illuninated	None	See 33.1	
34.1	AB2 Matrix Relay Trip Test Switch	Jams or Binds	Cannot continue test of AB matrix. If the switch binds in the off position, power will remain on all holding coils for the trip relays. The AB matrix logic relay may still be tested. If the switch binds in position 1, 2, 3 or 4, the associated trip relay will drop out when the matrix logic relays are tested. See 7.2 for details.	Periodic Test	See 6.2	See 6.2	

TABLE A-13 (cont'd)

RPS FMEA

REACTOR TRIP MATRIX AND TRAIN

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
34.2	AB2 Matrix Relay Trip Test Switch	Contact Set Fails Open (Position 1, 2, 3, or 4)	The selected trip relay will not drop out when the matrix logic relays are cycled.	Periodic Test	The failure has no effect on the operational RPS equipment.	RPS tests erroneously indicate a trip relay is hung up.	
34.3	"	Contact Set Fails Open (Off Position)	None	Switch Checkout	None required.	None	
35.1	AB Logic Matrix Trip Test Switch	Jams or Binds in Off Position	Cannot test AB matrix logic relay.	Periodic Test	None	Unable to test AB matrix trip logic relays.	
35.2	"	Jams or Binds in Position 1, 2, ... or N	When in test mode, the relay pair (e.g. A1-1 and B1-1) associated with the switch positions will drop out.	Periodic Test	The tripped relays will be restored to the untripped state when the AB matrix logic test switch is opened. However, when the switch is opened, a race condition will exist which may generate a spurious scram.	See 35.1. Possible spurious scram when the system is taken out of test.	
35.3	"	Fails Open (Position 1, 2, ... or N)	The selected pair of matrix logic relays will not drop out during test.	Periodic Test	The failure has no effect on the operational RPS equipment.	RPS tests erroneously indicate a trip relay is hung up.	
35.4	"	Contact Set Fails Open in Off Position	None	Switch Checkout	None required.	None	
36.0	AC Trip Matrix Components	All Modes	All six reactor trip matrices (AB, AC, AD, BC, BD, CD) are identical in configuration except for the AC preferred bus interfaces. The FMEA for the AB trip matrix components (items 27 - 35) is applicable for all matrices.				AC trip matrix power supply interfaces are: PS7 - Pnl Y10; PS8 - Pnl Y30
37.0	AD Trip Matrix Components	All Modes	See 36.0				AD trip matrix power supply interfaces are: PS9 - Pnl Y10; PS10 - Pnl Y40
38.0	BC Trip Matrix Components	All Modes	See 36.0				BC trip matrix power supply interfaces are: PS11 - Pnl Y20; PS12 - Pnl Y30

TABLE A-13 (cont'd)

RPS FMEA

REACTOR TRIP MATRIX AND TRAIN

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
39.0	BD Trip Matrix Components	All Modes	See 36.0				BD trip matrix power supply interfaces are: PS13 - Pnl Y20 PS14 - Pnl Y40
40.0	CD Trip Matrix Components	All Modes	See 36.0				CD trip matrix power supply interfaces are: PS15 - Pnl Y30 PS16 - Pnl Y40
41.1	Test Power Supply PS17	Loss of Output	The power supply is normally de-energized except during test. During test, the matrix trip relays cannot be held in.	During Test, the Trip Relay "Hold" Lights Would Not Illuminate	The power supply is only required for trip logic testing when the plant is in operation.	Unable to test trip logic without generating a spurious RT.	
41.2	"	Loss of Input Power Supply (Pnl Y10)	The effect of the failure is the same as loss of output. See 41.1.	See 41.1	See 41.1	See 41.1	
41.3	"	Open Output Line or Short Across Output	See 41.2	See 41.1	See 41.1	See 41.1	
41.4	"	Single Short to Ground on Output Line	None	Periodic Test	The system has a floating ground.	None	
42.1	PS17 Isolation Transformer	Loss of Output	See 41.2	See 41.1	See 41.1	See 41.1	
42.2	"	Loss of Input Power Supply (Pnl Y10)	See 41.2	See 41.1	See 41.1	See 41.1	
42.3	"	Open Output Line or Short Across Output	See 41.2	See 41.1	See 41.1	See 41.1	
42.4	"	Single Short to Ground on Output Line	None	None	The system has a floating ground.	None	

TABLE A-13 (cont'd)

RPS FMEA

REACTOR TRIP MATRIX AND TRAIN

No.	Name	Failure Mode	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects on RPS	Remarks and Other Effects
43.0	PS17 Fuse	Fail Open	The effect of the failure is the same as 41.2.	See 41.1	See 41.1	See 41.1	

APPENDIX B

REFERENCES

REFERENCES

1. WASH-1270, Technical Report on Anticipated Transients Without Scram, Regulatory Staff, U. S. Atomic Energy Commission, September 1973.

2. Topical Report, Anticipated Transients Without Scram, Combustion Engineering, Inc., CENPD-158.

3. Palisades Plant Technical Specifications, Revised February 11, 1975, Section 2.3.

4. Palisades Plant, Final Safety Analysis Report, Consumers Power Company, Section 7.2.3.1.

5. Ibid, Section 7.2.3.6.

6. Personal communication from R. B. Sewell, Nuclear Licensing Administrator, Consumers Power Company, to A. Giambusso, Deputy Director for Reactor Projects, Directorate of Licensing, USAEC, Docket 50-255, November 1, 1974.

7. Palisades Plant Technical Specifications, Revised February 11, 1975, Section 2.2.