DRAFT

INDIAN POINT 3
REACTOR PROTECTION SYSTEM

A. SUMMARY

A.1 INTRODUCTION

The reactor protection system (RPS) is evaluated in the context of a small LOCA or plant transients. The function of the RPS is to protect the core from overpower conditions resulting from infrequent transients.

The analysis is carried out under the following conditions:

- The conditions in the plant require a reactor scram.
- No operator action is taken to scram the plant.

A.2 RESULTS

Table 1, "Reactor Protection System Failure to Scram," presents the results of the analysis of the RPS for Indian Point 3. The analysis has revealed the following dominant contributors to RPS failure:

	Mean
• Random coincident failures of two trains of the trip system (50%)	2.1×10^{-5}
• Failure of the rod control cluster assemblies to enter the core (24%)	9.2×10^{-6}
• Failures while in test or maintenance (23%)	8.9×10^{-6}

A comparison of the results of this analysis and the RPS analysis of the Reactor Safety Study, WASH-1400, is presented below.

Frequency of Failure to Scram	Indian Point 3	WASH-1400
5th	6.0×10^{-7}	1.3×10^{-5}
Median	6.5×10^{-6}	3.6×10^{-5}
95th	1.7×10^{-4}	1.0×10^{-4}

A.3 CONCLUSIONS

The failure of the RPS is dominated by random coincident failures in the logic trains, predominately wiring faults, and reactor trip breaker failures. Operator action to manually scram the plant bypasses all logic train failures (except reactor trip breaker failures). By locally opening the output breakers of the rod drive motor generator sets, failure of the reactor trip breakers can be corrected.

Failure of the rod control cluster assemblies (RCCA) to insert is not immediately correctable with operator action; however, the mean frequency of this event occurring is 9×10^{-6} per demand, which equates to one failure to scram due to RCCA multiple failures about every one hundred thousand demands.

B. SYSTEM DESCRIPTION

B.1 SYSTEM FUNCTION

The reactor protection system (RPS) and the engineered safety features (ESF) make up the protective systems of Indian Point 3.

The RPS performs the following primary functions:

- Protects the reactor core against fuel rod cladding damage caused by departure from nucleate boiling or high power density.
- Protects against reactor coolant system damage caused by high primary system pressure.
- Protects the reactor coolant system from sudden loss of its heat sink through the steam generators.
- In conjunction with ESF, detects a failure of the reactor coolant system and initiates actions to mitigate the consequences of the accident.

A simplified block diagram of the RPS is presented in Figure 1. Figure 2 presents a simplified system arrangement diagram. Figure 3 presents a typical reactor trip breaker schematic diagram.

B.2 SYSTEM OPERATION

The RPS utilizes trip signals from various process sensors to deenergize undervoltage devices in two, series-connected reactor trip breakers. The reactor trip breakers open and remove power from the control rod drive mechanism magnetic coils. When power is removed from the magnetic coils, the rod control cluster assemblies fall into the active fuel region of the reactor core; thereby inserting negative reactivity and making the reactor subcritical.

The parameters measured by the process instrumentation and their associated scram setpoints are presented in Table 2. Also included in Table 2 is the required scram logic for the process sensors; for example, two out of four indicates at least two trains out of four available trains must indicate that a scram condition exists before a scram signal is generated.

The process instrumentation is separated into a number of trains (maximum of four trains) with each train receiving power from a different 120 VAC instrument bus. Upon loss of power, an instrumentation train is designed to fail in the mode that generates a scram signal.

The signal generated in the instrumentation loop is sent to the trip bistable for that loop. As the setpoint is reached, the bistable changes state from on to off which deenergizes the associated scram

logic relays in the reactor protection logic racks. In addition to the instrument loop bistable, the loops also provide indication, alarm, and interlock functions.

There are two trains of actuation logic. Each reactor trip bistable drives two relays, one in each actuation logic train. The logic trains are duplicates of each other and are physically separated.

The logic trains are energized from separate 125 VDC buses. Loss of power from a 125 VDC bus deenergizes the undervoltage trip device in the reactor trip breaker, causing the reactor trip breaker to open.

The scram logic relay contacts are arranged in a matrix to develop the required logic configuration for each reactor trip signal. The output of a logic matrix is fed to two reactor trip relays arranged in parallel. The parallel arrangment prevents a scram from a failed open trip relay. There are eight parallel reactor trip relay sets. These sets are arranged as shown in Figure 2. The logic matrices supplying each set of reactor trip relays is presented in Table 3.

Each logic train energizes the undervoltage trip device in two reactor trip breakers. The two reactor trip breakers and the two trip bypass breakers are arranged in a series-parallel arrangement as shown in Figure 1. During normal operation, reactor trip breakers RTA and RTB are closed and power from the rod drive motor generator sets must pass through both trip breakers. During testing, a trip bypass breaker, either BYA or BYB, is closed to allow testing of the associated reactor trip breaker. In this condition, a single logic train supplies both the normal reactor trip breaker and the opposite trip bypass breaker. This arrangement allows one logic train to be tested to the reactor trip breaker. The trip bypass breakers are electrically interlocked to prevent more than one bypass breaker from being closed at a time. If one bypass breaker is closed, closing the other bypass breaker causes both bypass breakers to trip.

The reactor trip breakers are operated by 125 VDC from separate DC sources. To close a reactor trip breaker or trip bypass breaker, DC power must be available and the undervoltage coil must be energized.

Manual reactor trip is provided by two trip switches in the control room. These switches deenergize the trip breaker undervoltage coils through the logic system and energize separate trip coils which are part of the breaker control circuit. An individual trip switch for each breaker at the breaker panels mechanically trips the reactor trip or reactor trip bypass breakers.

Power from the rod drive motor generator sets is supplied through the reactor trip breakers to the rod control panels. The rod control panels convert the power from AC to DC and distribute it to the individual control rod drive mechanisms. During normal operation the control rods are fully withdrawn from the reactor core and the stationary gripper coils are energized from the rod control panels. Upon a loss of power,

all coil assemblies are deenergized, the stationary gripper latches disengage from the control rod drive shaft, and the control rod drive shaft and rod control cluster assemblies drop into the active core region, thus shutting down the reactor.

B.3 TECHNICAL SPECIFICATIONS

The plant technical specifications identify:

- The maximum or minimum trip setpoints.
- The frequency of testing of the various RPS components.
- The number of out-of-service instrumentation or logic channels.
- Limits on the number of channel tests that may be performed at the same time.

B.4 SUPPORT SYSTEMS

The RPS is independent of any supporting systems.

B.5 INTERFACING SYSTEMS

The RPS interfaces with the 120 VAC instrument power supply system and the 125 VDC battery power system.

The instrument buses supply power to the RPS instrument trains as shown in Table 4. Table 4 also shows the battery system supplies to the RPS logic trains and the reactor trip and bypass breakers.

B.6 TESTING AND MAINTENANCE

The various components in the reactor protection system undergo periodic testing and surveillance. Maintenance is performed as required.

1. The process instrumentation trains are periodically tested to satisfy plant technical specifications as indicated below:

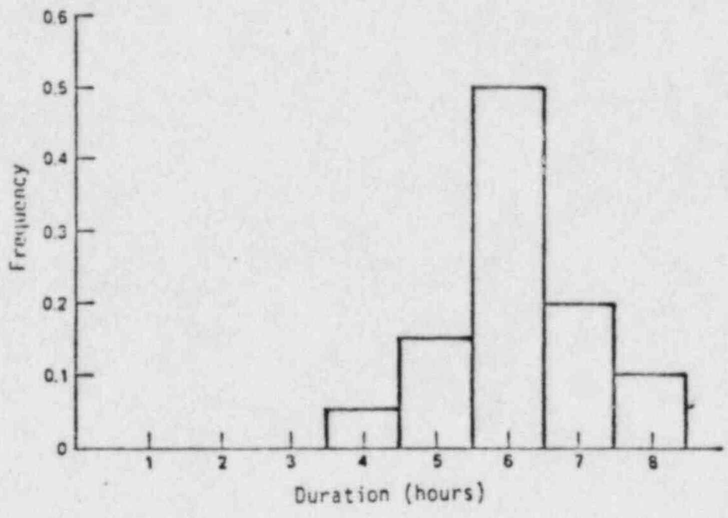
    a. Train checks are performed every shift (8 hours). A train check is a qualitative determination of acceptable operability by observation of the instrument behavior during operation.

    b. Train functional tests are performed monthly. A train functional test involves the injection of a simulated signal(s) into the train to verify operability, including alarm, and/or trip initiating signals.

    c. Train calibration for the instrumentation loops is performed during refueling outages. Train calibration is the adjustment of train output(s) such that it responds, within acceptable range and accuracy, to known values of the parameter(s) which the train monitors. Calibration encompasses the entire train, including all train outputs, and includes the train functional test.

2. The reactor protection logic trains are periodically tested to satisfy plant technical specification requirements as indicated below:

Logic Train Functional Test. Logic train functional tests are performed monthly. A logic train functional test is the application of input signals, or the operation of relays or switch contacts, in all the combinations required to produce the required decision outputs including the operation of all actuation devices. For the reactor protection system logic trains, the actuated devices include the reactor trip breakers. During the logic train test the bypass reactor trip breaker for the logic train under test is racked into position and closed. Testing of the train then proceeds with the final actuation device, the reactor trip breaker, tripping as the required trip logic is made up. After the first trip actuation, the reactor trip breaker remains open, and the required logic actuation is verified by test lights. This testing normally requires 6 hours per train with a range of 4 to 8 hours. The histogram presented below is based on discussions with plant personnel and presents the frequency distribution of test duration.



The mean duration from the above histogram is 6.15 hours. Since the tests are performed once per month, this histogram leads to an unavailability distribution characterized by the following mean and variance:

Mean: $\frac{6.15 \text{ hrs./month}}{720 \text{ hrs./month}} = 8.54 \times 10^{-3}$ Single train unavailability due to test

Variance: 1.79×10^{-6}.

0468A040781/1

3. The rod drive mechanisms and rod control cluster assemblies are exercised biweekly if no other rod insertion has occured during the past two-week period to ensure freedom of movement and to satisfy technical specification requirements.

B.7 OPERATOR INTERACTION

Operator action to manually scram the plant is excluded from this analysis. Operator errors during calibration are quantified in Section D.4, Common Cause Failure.

B.8 COMMON CAUSE EFFECT

The logic and instrumentation cabinets associated with the RPS are located in the control room behind the flight panels at Indian Point 3.

The reactor trip breakers and the rod drive motor generator sets are located at elevation 15' of the control building.

Common generic components of the RPS are supplied by the same manufacturers, are subject to common test and maintenance procedures, and have common susceptibility to secondary causes of failure (grit, moisture, vibration, etc.).

Further discussion of the effects of common cause failures on system failures is presented in Section D.4 of this analysis.

C. LOGIC MODEL

C.1 TOP EVENT

The fault tree is developed for the event "Reactor Protection System Failure to Scram." This event appears in the small LOCA event tree and all transient event trees.

C.2 SYSTEM FAULT TREE

Figure 4 presents the fault tree developed for the RPS. The tree identifies the hardware failures that must occur to fail the RPS. Discussion of these events is presented in Section D of this report.

The fault tree was developed for the event "Turbine Trip Without Bypass." All other transient events which require RPS action have similar fault tree logic.

C.3 FAULT TREE CODING

Table 5 identifies the basic events and the basic event coding that was used in this analysis. Also included in Table 5 are the failure rates associated with the basic events.

D. QUANTIFICATION

D.1 SINGLE FAILURES

Three single failures are identified and defined for the RPS. These defined events are:

- Reactor Core Misalignment Causes Rod Not to Insert. For the small LOCA and the transient event trees that require RPS action the probability of this failure occuring is quantitatively insignificant ($\ll 10^{-8}$) and does not contribute to system failure to scram.

- Wiring Fault Provides Sufficient Power to Hold RCCAs in Position. The rod drive motor generator sets supply three phase, nonsynchronous power to the rod control panels through the reactor trip breakers. No power source exists at the plant that is capable of being paralleled with the rod control power. In addition, the bus itself is completely metal enclosed from the rod drive motor-generator sets to the rod control panels. For these reasons, the probability of this failure occurring is quantitatively insignificant ($\ll 10^{-8}$) and does not contribute to system failure to scram.

- Rod Control Cluster Assemblies Fail to Insert. In NUREG/CR-1331 a review of Licensee Event Reports for control rods and drives is presented. Our use of this report is presented below.

  There have been three reported failures of rod control cluster assemblies (RCCAs) to fully insert* during a reactor scram condition for Westinghouse pressurized water reactors for the period reviewed. Using the data from NUREG/CR-1331, there were 50,987 individual rod demands (number of rods per plant times the number of scrams per plant) in this period. This data is used to establish a prior population variability distribution. For Indian Point 3 there have been zero failures in 1,908 demands (through June, 1980). A population variability analysis and update based on Indian Point 3 experience was performed. The results of this procedure lead to the following mean and variance for the rate of failure of an individual RCCA to insert on demand:

  Mean: 4.72×10^{-5}

  Variance: 4.92×10^{-9}.

  Using the binomial probability theorem, the probability of any two or more RCCAs not fully inserting on demand is:

  Mean: 9.19×10^{-6}.

*Fully insert is defined as inserting to 96% position.

This result describes the random coincident failure of two or more rods. We must note however, that failure of two RCCAs to insert does not constitute failure to scram. In fact, failure of ten to twenty RCCAs to fully insert would probably not constitute failure to scram as those RCCAs that do insert may reduce power sufficiently to allow mitigation of the accident.

With respect to common cause failures, we are only considering here failures of the RCCAs themselves, the logic, instrumentation and the trip breaker contributions to common cause failure are considered in Section D.4 of this analysis. We have for evidence the fact that there has not been a multiple rod failure to insert during scram in Westinghouse reactors. (From NUREG/CR-1331 zero multiple rod failures in 1,110 scrams and zero multiple rod failures in 50,987 individual rod scrams.) We cannot envision any credible mechanism by which such a common cause failure could occur for the events of interest (external events, such as earthquake, are treated separately in this report). Common mechanisms for such common cause failures as wearout or manufacturing defects are possible; however, the following points should be made:

- During refueling, the drive mechanisms and RCCAs are inspected and replaced if excessive wear or other unusual conditions are present.

- If these mechanisms for failure exist they will occur in the plants with similar mechanisms that have been on-line for a longer period of time than Indian Point 3.

For the above reasons we assign as the probability of multiple rod failures to insert during scram, the value obtained from the binomial theorem for failure of two or more rods to fully insert on demand, of:

Mean: 9.19×10^{-6}

Variance: 5.58×10^{-9}.

D.2 DOUBLE FAILURES

Double failures consist of failures in RPS train A and train B. The quantification for a single train and the train combination are presented below.

Train A consists of the following basic components:

- Reactor Trip Breaker A - RTA.

- Reactor Trip Bypass Breaker A - BYA.

- Logic Train A which consists of the logic matrix and trip relays for Train A.

- Wiring for the logic train and trip breakers.

Train B contains similar components.

NOTE: The analog instrumentation system is common to trains A and B. Discussion of the effect of failure of the instrumentation portion of the RPS is discussed in Section D.2.1.f.

The train arrangement simplifies the calculations for system failure. A train can be thought of as a block of series connected basic events, failure of any one basic event results in train failure. Quantification of the basic events is presented below.

1. RTA fails closed. Based upon a review of plant data, the probability of this event occurring is:

   Mean: 1.17×10^{-3}

   Variance: 8.86×10^{-5}.

2. BYA fails closed. This event is separate from the test or maintenance condition where the bypass breakers are intentionally closed to facilitate testing.

   (NOTE: Because the bypass breakers are manually operated, normally open, racked out, and locked in the racked out position, no probability of failure is assigned.)

3. Logic train A failures. This event consists of logic matrix failures or trip relay failures.

   a. Trip relay failures. Our mean and variance for the probability of failing to open for a trip relay is:

      Mean: 6.28×10^{-6}

      Variance: 2.49×10^{-11}.

      Failure of a single trip relay to open on demand does not cause system failure. Although the relays for a particular scram are arranged in parallel, diversity of scram signals requires coincident failure of two or more relays in series. This results in a mean and variance for trip relay contribution to RPS failure of:

      Mean: 6.33×10^{-11}

      Variance; 2.28×10^{-20}.

   b. Logic matrix failures. The logic matrices for the reactor trip signals consist of groupings of contacts which are opened by relays actuated by the analog instrumentation system. Failure

[illegible] these relays to open will result in matrix failure. From [illegible] the minimum number of relay failures that will cause failure of a logic matrix is two for the small LOCA and transient events under consideration. These relays are similar to the reactor trip relays and the same mean and variance for two relays failing to open on demand is assigned. Diversity of scram signals requires coincident failure of two or more logic matrices in order to fail the RPS logic. The coincident failure of two matrices occurs with a mean frequency of:

Mean: 2.68×10^{-20}.

This value is insignificant when compared to other causes of RPS failure.

4. Wiring faults leading to RPS failure. Two general locations exist for possible wiring faults that fail the RPS.

   a. Wiring shorts to power. Undervoltage trip coil - a wiring short to power in the portion of the reactor trip circuit that supplies the undervoltage trip device could result in power being maintained to this trip device when a reactor trip is demanded. Our mean and variance for this event is:

      Mean: 3.22×10^{-6} Failures per hour

      Variance: 8.96×10^{-11}.

      To determine the contribution to system failure, we must convert from a probability of failure per hour to a frequency of failure on demand. The fault detection time (MTTR) for this event is one half the test cycle ($t = 360$ hours). This results in the following frequency of failure on demand due to wiring shorts to power:

      Mean: 1.16×10^{-3}

      Variance: 1.16×10^{-5}.

   b. Wiring shorts to ground. WASH-1400 postulated nine possible locations where a possible short to ground would result in failure of the RPS. Our review of the RPS did not reveal a location where a single wiring fault to ground results in failure of the system, due primarily to the fact that the RPS logic and breaker power supplies are ungrounded. To set up a parallel loop which would bypass contacts and maintain current flow, at least two shorts to ground in the correct location are required. Our mean and variance for this event is:

      Mean: 7.52×10^{-6} Failures per hour

      Variance: 4.88×10^{-10}.

To determine the contribution to system failure, we must convert from a probability of failure per hour to a frequency of failure on demand. The fault detection time (MTTR) for this event is one half the test cycle (t = 360 hours). This results in the following frequency of failure on demand due to a single wiring short to ground:

Mean: 2.71×10^{-3}

Variance: 5.63×10^{-5}.

For two faults to ground we obtain for mean and variance:

Mean: 5.77×10^{-5}

Variance: 3.35×10^{-6}.

And for nine possible locations we have:

Mean: 5.20×10^{-4}

Variance: 4.43×10^{-4}.

The total contribution to train failure due to wiring faults is the sum of wiring faults to power and wiring faults to ground, which is:

Mean: 1.68×10^{-3}

Variance: 5.41×10^{-5}.

5. For Train A failure using DPD arithmetic we have:

$$Q_{\text{Train A}} = Q_{\text{RTA}} + Q_{\text{BYA}} + Q_{\text{Logic}} + Q_{\text{Wiring to power}} + Q_{\text{Wiring to und}}$$

$$Q_{\text{Train A}} = 2.85 \times 10^{-3}$$

$$\beta^2_{\text{Train A}} = 7.06 \times 10^{-5}.$$

Train B mean and variance are the same. For the double contribution to RPS failure, we have:

$$Q_{AB} = 2.08 \times 10^{-5}$$

$$\beta^2_{AB} = 3.18 \times 10^{-9}.$$

6. To this value we must include the probability of failure of the instrumentation trains. We use for the probability of a single instrument train failing to provide a trip signal, $\lambda = 1 \times 10^{-4}$ failures per demand. We take the value as a median value and assign an error factor of 10 to express our uncertainty concerning this value. Taking the values obtained with this error factor as our 5th and 95th percentiles we obtain for a single instrument train failure the following mean and variance:

   Mean: 2.66×10^{-4}

   Variance: 4.32×10^{-7}.

   As was the case for logic matrices failure, we must fail at least two out of three instruments to cause a single scram signal failure. For two instruments failing we have for mean and variance:

   Mean: 4.61×10^{-7}

   Variance: 1.43×10^{-10}.

   Scram signal diversity requires failure of two or more different instrumentation groups. For failure of two instrumentation groups we have the following mean value:

   Mean: 1.43×10^{-10}

   which is insignificant when compared to other causes of RPS failure.

D.3 TEST AND MAINTENANCE FAILURE

The test contribution to RPS failure is obtained by multiplying the unavailability of a single train due to test times the probability of wiring faults in the other logic train. This results in a mean and variance of:

Mean: 4.44×10^{-6}

Variance: 3.34×10^{-9}.

For the total system contribution we must double the contribution of a single train. This results in the following mean and variance:

Mean: 8.87×10^{-6}

Variance: 1.34×10^{-8}.

Maintenance on the RPS is not quantified for the following reasons:

- The components requiring the most maintenance are those located in the logic trains. Prior to performing maintenance on a component in the logic train, the associated trip relay is placed in the

"tripped" condition which sets up part of the logic matrix required for scram signal development. This maintenance does not affect the RPS analysis.

- Maintenance on the reactor trip breakers occurs infrequently. If we assume one maintenance act per year lasting for four hours, the resulting unavailability due to maintenance is 1/12 the contribution due to testing. This does not significantly affect the results of the system analysis.

D.4 COMMON CAUSE FAILURE

D.4.1 INSTRUMENT TRAIN MISCALIBRATION

There is a potential for common miscalibration errors to be applied to all instruments of a particular set. During the periodic calibrations, a single technician or group of technicians perform the tests necessary to ensure instrument accuracy. These tests are usually performed sequentially among identical trains. This leads to an extremely close coupling between the acts. However, most calibration activities, even if performed in error do not result in an instrument that fails to provide a trip. In addition, the diversity in the types of instruments that provide trip signals limit the effect of these common cause miscalibrations. If we take the value of a single instrument train failing, 2.66×10^{-4}, as the probability of common cause miscalibration of a set of instruments, failure of two sets of instrumentation due to miscalibration of this type would result in a mean and variance of:

Mean: 4.61×10^{-7}

Variance: 1.43×10^{-10}.

This value is used as the probability of common cause miscalibration errors.

D.4.2 MONTHLY LOGIC TRAIN TESTING

During the monthly logic train testing, it can be seen from the fault tree that a single logic train failure can cause failure of the RPS. Both trains of logic are tested sequentially which, in principle, could introduce common cause coupling between the trains. However, the logic testing does not involve the changing of trip set points or logic arrangements. For this reason, these testing failures are treated as independent events which do not affect system unavailability.

D.5 SYSTEM QUANTIFICATION

The probability of the RPS failing to scram on demand is presented below:

$$Q_{RPS} = Q_{Singles} + Q_{Doubles} + Q_{Test\ and\ Maintenance} + Q_{Common\ Cause}$$

$$= 3.93 \times 10^{-5}$$

$$\beta^2_{RPS} = 1.78 \times 10^{-8}.$$

Table 6 summarizes the results of the quantification of the RPS by cause.

0468A040881/1

TABLE 1

RESULTS TABLE - REACTOR PROTECTION SYSTEM FAILURE TO SCRAM

	Mean	Variance	5th Percentile	95th Percentile	Median	WASH-1400 (Median Values)
Singles	9.2×10^{-6}	5.6×10^{-9}	1.8×10^{-8}	2.2×10^{-5}	8.9×10^{-7}	1.7×10^{-5}
Doubles	2.1×10^{-5}	3.2×10^{-9}	1.3×10^{-8}	1.2×10^{-4}	9.8×10^{-7}	5.4×10^{-6}
Test and Maintenance	8.9×10^{-6}	1.3×10^{-8}	6.6×10^{-10}	1.0×10^{-5}	1.7×10^{-7}	1.2×10^{-5}
Common Cause	4.6×10^{-7}	1.4×10^{-10}	5.0×10^{-11}	6.0×10^{-7}	1.0×10^{-8}	ϵ*
System Failure to Scram on Demand	3.9×10^{-5}	1.8×10^{-8}	6.0×10^{-7}	1.7×10^{-4}	6.5×10^{-6}	3.4×10^{-5}

*Epsilon used in WASH-1400 to signify insignificant contributors to failure.

TABLE 2

REACTOR PROTECTION SYSTEM INSTRUMENTATION LOGIC AND SETPOINTS

Reactor Trip	Coincidence Circuitry and Interlocks	Setpoint	Comments
1. Manual	1/2, no interlocks	NA	
2. High power range neutron flux	2/4, low setpoint interlocked with P-10.	Hi ≤109% power Low ≤25% power	Low power range setting manual block. Automatic reset by P-10.
3. Overtemperature ΔT	2/4, no interlocks	ΔT > program	
4. Overpower ΔT	2/4, no interlocks	ΔT > program	
5. Low pressurizer pressure	2/4, blocked by P-7	≥1,800 psig	
6. High pressurizer pressure	2/3, no interlocks	≤ 2,385 psig	
7. High pressurizer water level	2/3, interlocked with P-7	≤ 92% span	
8. Low reactor coolant flow	2/3 signals per loop, interlocked with P-7, P-8, respectively	≥ 90% flow	Blocked below P-7. Low flow in 1 loop permitted below P-8.

TABLE 2 (continued)

REACTOR PROTECTION SYSTEM INSTRUMENTATION LOGIC AND SETPOINTS

Reactor Trip	Coincidence Circuitry and Interlocks	Setpoint*	Comments
9. Monitored electrical supply to reactor coolant pumps:			
9a. Undervoltage 6.9 KV bus	2/4, interlocked with P-7	≥ 70% normal	1/bus.
9b. Low frequency 6.9 KV bus	2/4, interlocked with P-7	≥ 55.0 cps	2/4 underfrequency signals will trip all reactor coolant pumps and indirectly activate reactor trip. Blocked below P-7.
9c. Reactor coolant pump breakers	Interlocked with P-7 and P-8		
10. Safety injection signal	2/3 low pressurizer	≥ 1,700 psig	Trips main feedwater pump. Closes all feedwater control valves. Closes feedwater isolation valves and initiates Phase A isolation.
	2/3 high containment pressure	≤ 3.5 psig	
	2/3 differential steam line pressure low compared to two high, four channels	≥ 150 psid	
	2/4 high steam flow in coincidence with:	programmed	
	2/4 low T_{avg}	≥ 540°F	
	2/4 low steam line pressure	≥ 600 psig	
	1/2 manual	NA	
11. Turbine generator trip	2/3 low auto stop oil pressure interlocked with P-7 or all stop valves closed.		

TABLE 2 (continued)

REACTOR PROTECTION SYSTEM INSTRUMENTATION LOGIC AND SETPOINTS

	Reactor Trip	Coincidence Circuitry and Interlocks	Setpoint*	Comments
12.	Low feedwater flow and low S/G water level	1/2 steam/feedwater flow mismatch in coincidence with 1/2 low steam generator water level per loop.	≥ 5.8 x 10^5 lb/hr. and 30% of span	
13.	Low-low steam generator water level	2/3, per loop	≥ 17% span	
14.	Intermediate range neutron flux	1/2, manual block permitted by P-10	≤ 25% power	Manual block and automatic reset.
15.	Source range neutron flux	1/2, manual block permitted by P-10 and P-6	≤ 10^5 cps	Manual block and automatic reset.

TABLE 3

LOGIC MATRIX TO REACTOR TRIP RELAY MATCHING

Trip Relay Number*	Reactor Trip Logic Matrix
RT1,2	Intermediate range trip Source range trip Power range low level trip
RT3,4	Overtemperature ΔT trip Overpressure ΔT trip Safety injection trip
RT5,6	Steam generator low-low level trip
RT7,8	Steam generator feedflow/level mismatch trip
RT9,10	High pressurizer level trip Power range high level trip High pressurizer pressure trip Low pressurizer pressure trip
RT11,12	Low loop flow trip Manual trip
RT13,14	Undervoltage RCP breakers trip
RT15,16	Turbine trip

*See Figures 1 or 2 for the arrangement of the Trip Relays in the logic matrix.

TABLE 4

INSTRUMENT AND LOGIC POWER SUPPLIES

Instrument Bus 32 Reactor Analog Prot. Train 1 Nuclear Inst. Train 1 Steam Generator Analog Train 1 Reactor Protection Cabinets E-6, F-6 Containment Inst. & Prot. Train 1	Instrument Bus 31 Reactor Analog Prot. Train 2 Nuclear Inst. Train 2 Steam Generator Analog Train 2 Reactor Protection Cabinets E-5, F-5 Reactor Protection Logic Status Lights Containment Inst. & Prot. Train 2
Instrument Bus 34 Reactor Prot. Analog Train 3 Nuclear Inst. Train 3 Safeguard Relay Test (F-7, E-8) Reactor Prot. Cabinets E-4, F-4	Instrument Bus 33 Reactor Prot. Analog Train 4 SIS Inst. Analog Nuclear Inst. Train 4 Reactor Prot. Cabinets E-3, F-3
DC Distribution Panel 31 Reactor Trip Breaker Open/Close Circuits Logic B (RTB and BYA)	DC Distribution Panel 32 Reactor Trip Breaker Open/Close Circuits Logic A (RTA and BYB)

TABLE 5

BASIC EVENT DATA

Event Description and Failure Mode	Fault Tree Coding	Failure Data					Comments
		Mean	H/D	Variance	MTTR	Reference*	
Reactor Core Misalignment Causes Rods Not To Insert	1EDCOREF	$\ll 10^{-8}$	-	-	-	-	Developed in text
Rod Control Cluster Assemblies Fail To Insert	1ED0001F		D			NUREG	Developed in text
Wiring Fault Provides Sufficient Power To Hold RCCAs In Position	1WR0001Q	$\ll 10^{-8}$	-	-	-	CR-1331	Developed in text
Reactor Trip Breaker, RTA, Fails Closed	1CB0005Q	1.17×10^{-3}	D	8.86×10^{-5}	-	50	
Reactor Trip Breaker, RTB, Fails Closed	1CB0004Q	1.17×10^{-3}	D	8.86×10^{-5}	-	50	
Trip Bypass Breaker, BYA, Fails Closed	1CB0003C	-	D	-	-	-	Developed in text
Trip Bypass Breaker, BYB, Fails Closed	1CB0002C	-	D	-	-	-	Developed in text
Trip Bypass Breaker, BYA, Closed for Test	1CB0003X	8.54×10^{-3}	-	1.79×10^{-6}	-	-	Developed in text
Trip Bypass Breaker, BYB, Closed for Test	1CB0002X	8.54×10^{-3}	-	1.79×10^{-6}	-	-	Developed in text
No Turbine Trip Signal	1TT0001S	4.61×10^{-7}	D	1.43×10^{-10}	-	-	Developed in text
No Pressurizer High Pressure Signal	1PHPT00S	4.61×10^{-7}	D	1.43×10^{-10}	-	-	Developed in text
No Pressurizer Low Level Signal	1PLLT00S	4.61×10^{-7}	D	1.43×10^{-10}	-	-	Developed in text
No Overtemperature ΔT Trip Signal	1OTDT00S	4.61×10^{-7}	D	1.43×10^{-10}	-	-	Developed in text
Trip Relay, RT3A, Fails Closed	1RE003AQ	6.28×10^{-6}	D	2.49×10^{-11}	-	46	
Trip Relay, RT3B, Fails Closed	1RE003BQ	6.28×10^{-6}	D	2.49×10^{-11}	-	46	
Trip Relay, RT4A, Fails Closed	1RE004AQ	6.28×10^{-6}	D	2.49×10^{-11}	-	46	
Trip Relay, RT4B, Fails Closed	1RE004BQ	6.28×10^{-6}	D	2.49×10^{-11}	-	46	
Trip Relay, RT9A, Fails Closed	1RE009AQ	6.28×10^{-6}	D	2.49×10^{-11}	-	46	
Trip Relay, RT9B, Fails Closed	1RE009BQ	6.28×10^{-6}	D	2.49×10^{-11}	-	46	
Trip Relay, RT10A, Fails Closed	1RE010AQ	6.28×10^{-6}	D	2.49×10^{-11}	-	46	
Trip Relay, RT10B, Fails Closed	1RE010BQ	6.28×10^{-6}	D	2.49×10^{-11}	-	46	
Trip Relay, RT15A, Fails Closed	1RE015AQ	6.28×10^{-6}	D	2.49×10^{-11}	-	46	
Trip Relay, RT15B, Fails Closed	1RE015BQ	6.28×10^{-6}	D	2.49×10^{-11}	-	46	
Trip Relay, RT16A, Fails Closed	1RE016AQ	6.28×10^{-6}	D	2.49×10^{-11}	-	46	
Trip Relay, RT16B, Fails Closed	1RE016BQ	6.28×10^{-6}	D	2.49×10^{-11}	-	46	
Wiring Faults In Logic A	1WRLOGAQ	1.68×10^{-3}	-	5.41×10^{-5}	-	-	Developed in text
(Includes Short to Power		3.22×10^{-6}	H	8.96×10^{-11}	360 hours	44	
and Short to Ground)		7.52×10^{-6}	H	4.88×10^{-10}	360 hours	45	
Wiring Faults In Logic B	1WRLOGBQ	1.68×10^{-3}	-	5.41×10^{-5}	-	-	Developed in text
(Includes Short To Power		3.22×10^{-6}	H	8.96×10^{-11}	360 hours	44	
and Short to Ground)		7.52×10^{-6}	H	4.88×10^{-10}	360 hours	45	

*Reference refers to item numbers in the Failure Data Section of this report.

TABLE 6

CAUSE TABLE - INDIAN POINT 3 REACTOR PROTECTION SYSTEM

Failure to Scram on Demand

Cause	Mean	Variance	System Effect	Mean (RPS Failure to Scram)	Variance
Singles					
Core misalignment	$\ll 10^{-8}$	$\ll 10^{-8}$	Failure to Scram	$\ll 10^{-8}$	$\ll 10^{-8}$
Rod control wiring faults	$\ll 10^{-8}$	$\ll 10^{-8}$	Failure to Scram	$\ll 10^{-8}$	$\ll 10^{-8}$
RCCAs fail to insert	9.19×10^{-6}	5.58×10^{-9}	Failure to Scram	9.19×10^{-6}	5.58×10^{-9}
Single Train					
Reactor trip breaker	1.17×10^{-3}	8.86×10^{-5}	Loss of one train, no system failure	--	
Trip bypass breaker	--	--	Loss of one train, no system failure	--	
Wiring faults (ground) (9)	5.20×10^{-4}	4.43×10^{-4}	Loss of one train, no system failure	--	
Wiring short (power)	1.16×10^{-3}	1.16×10^{-5}	Loss of one train, no system failure	--	
Logic failure	6.33×10^{-11}	2.28×10^{-20}	Loss of one train, no system failure	--	
TOTAL	2.85×10^{-3}	7.06×10^{-5}			
Doubles					
Combinations of single train failures	2.08×10^{-5}	3.18×10^{-9}	Failure to Scram	2.08×10^{-5}	3.18×10^{-9}
Test and Maintenance					
Train in test and logic wiring faults (2)	8.87×10^{-6}	1.34×10^{-8}	Failure to Scram	8.87×10^{-6}	1.34×10^{-8}
Common Cause					
Instrumentation miscalibration	4.61×10^{-7}	1.43×10^{-10}	Failure to Scram	4.61×10^{-7}	1.43×10^{-10}
System Failure to Scram on Demand				3.93×10^{-5}	1.78×10^{-8}

0536A040781/1

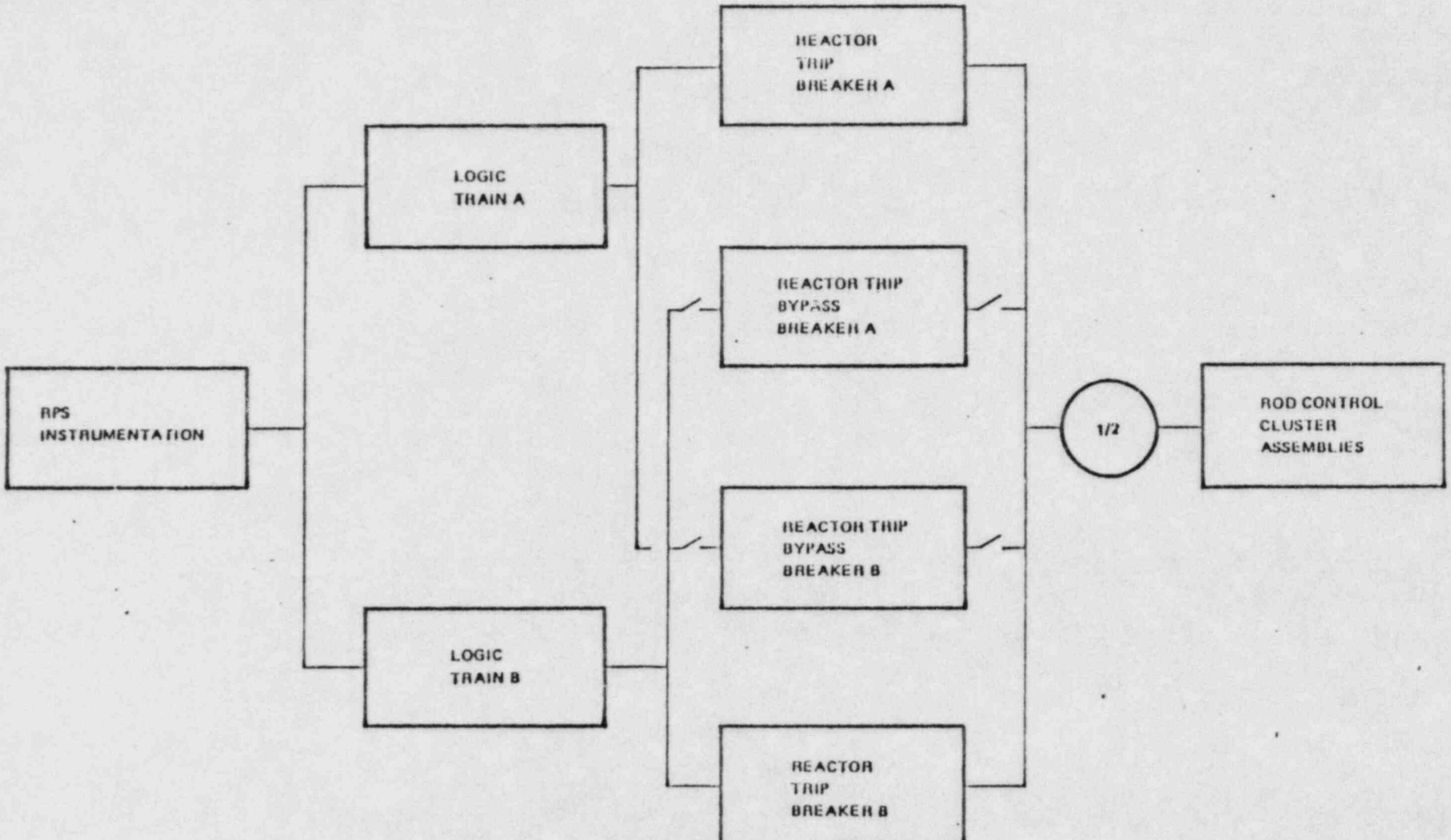


Figure 1. Simplified Block Diagram, Reactor Protection System

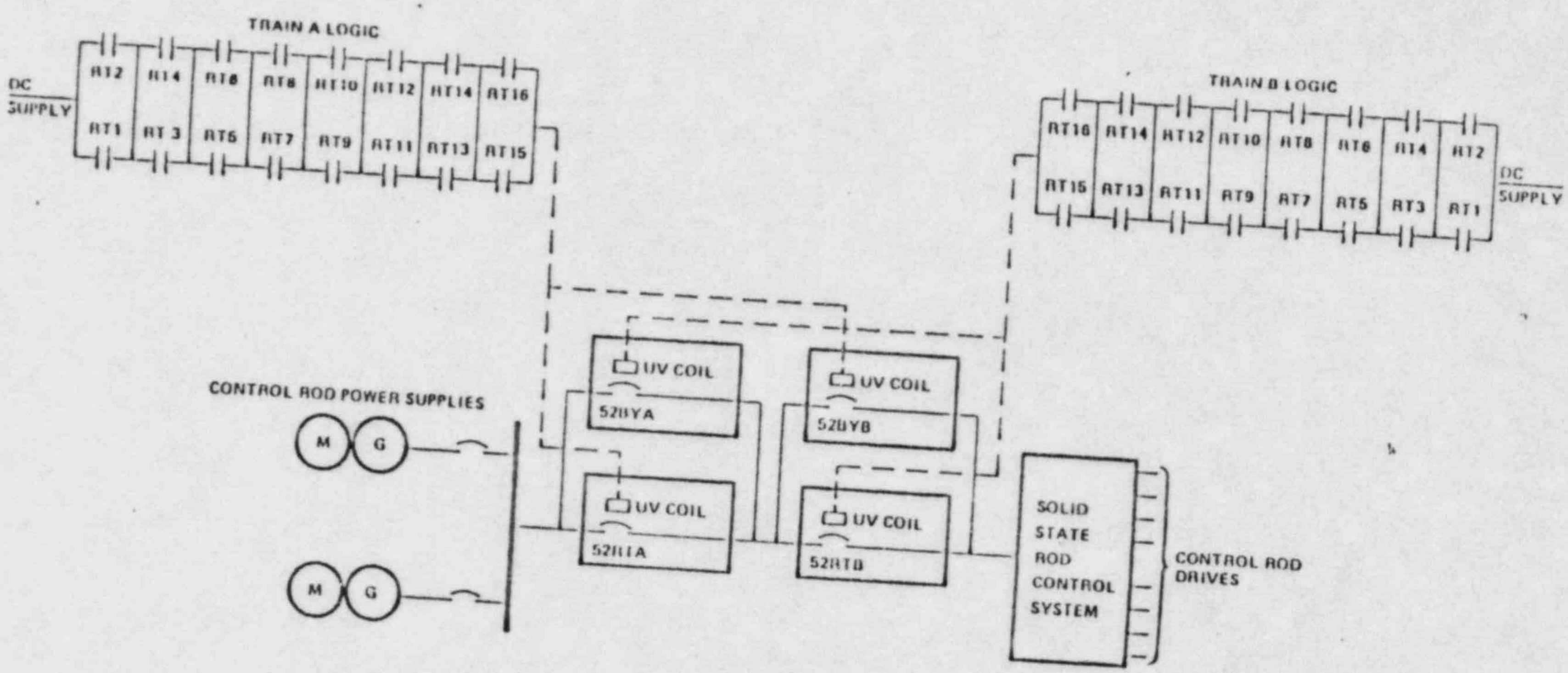


Figure 2. Simplified System Arrangement Indian Point 3 Reactor Protection System

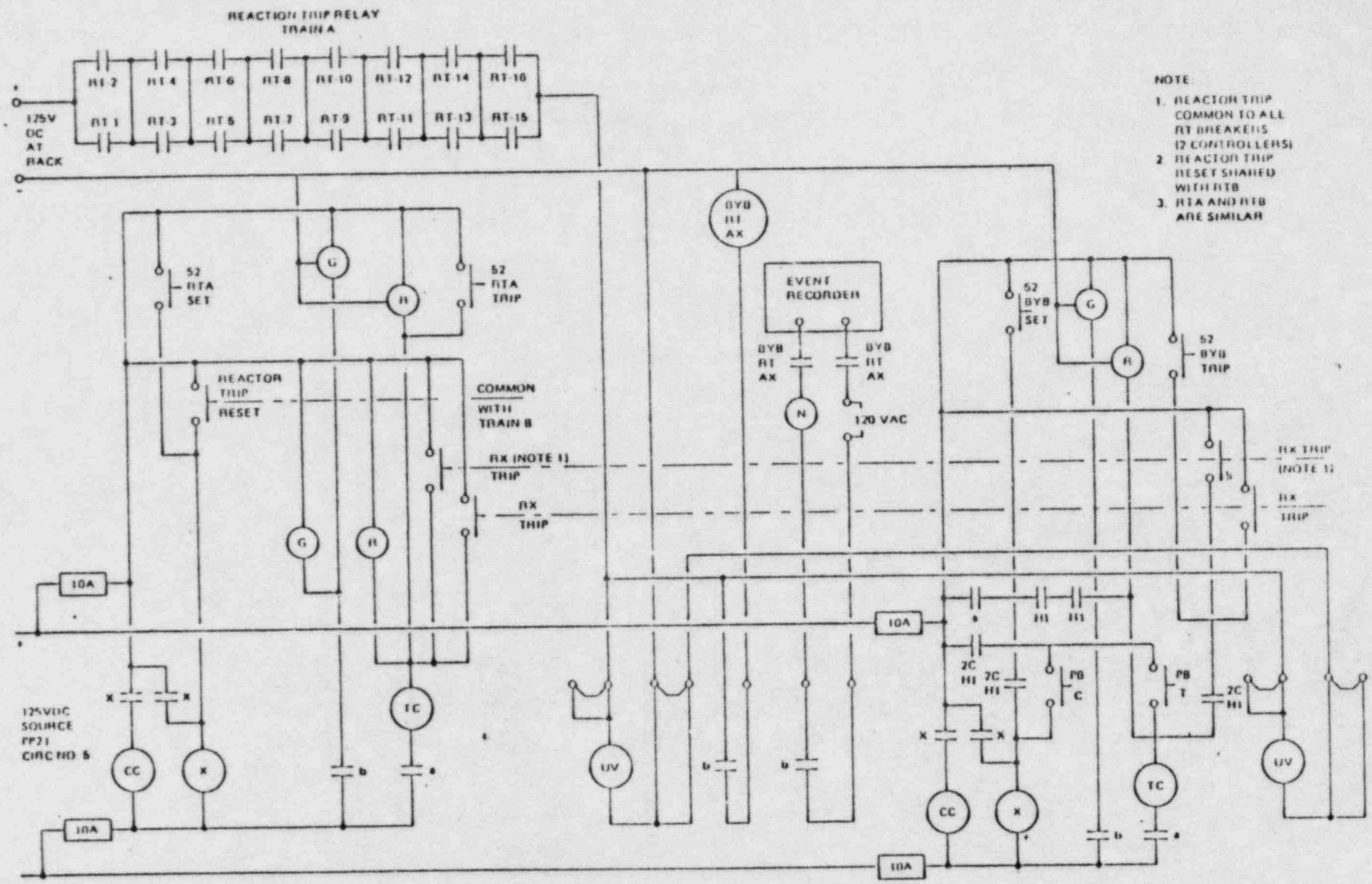


Figure 3. Reactor Trip Breaker Schematic

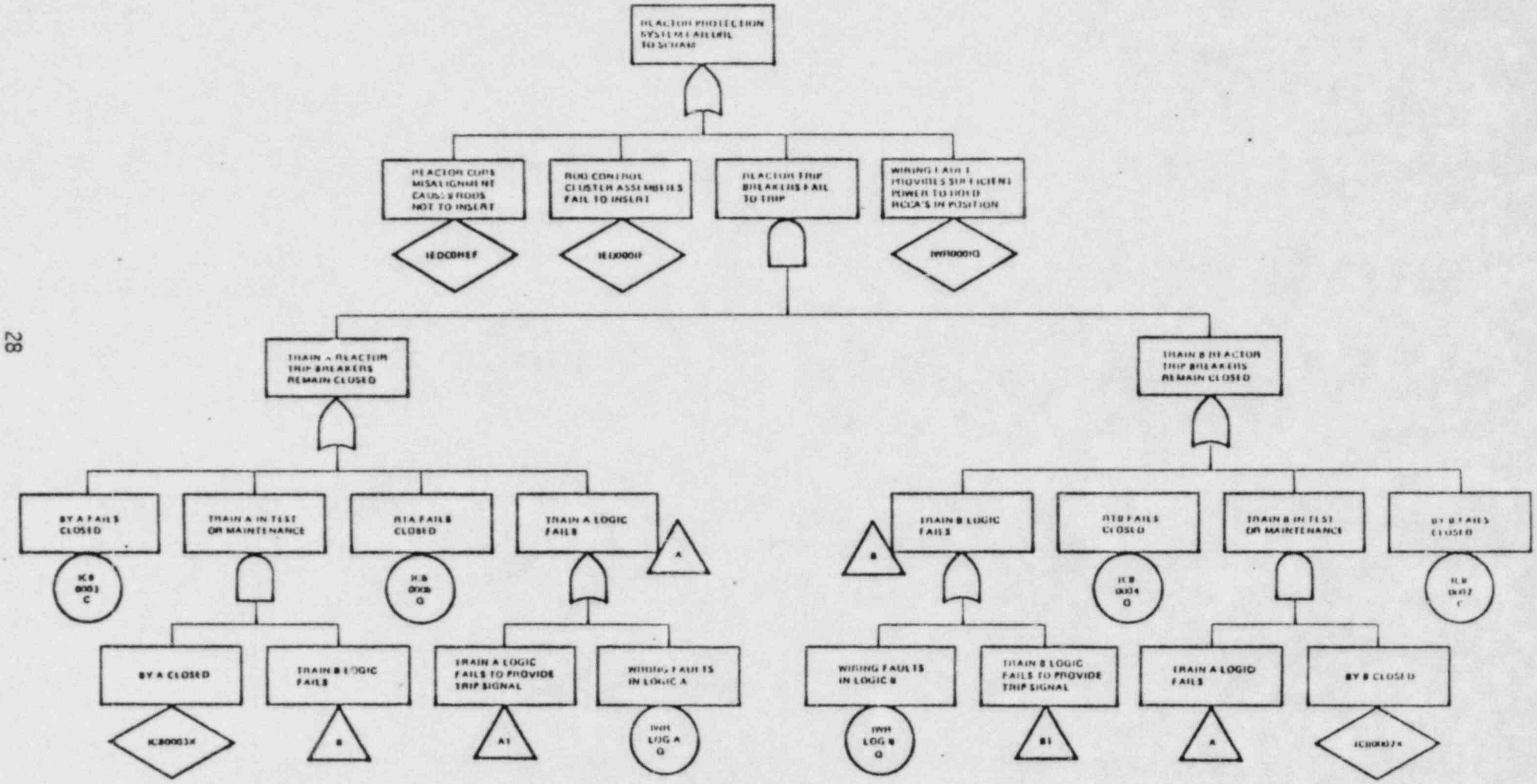


Figure 4. Reactor Protection System Fault Tree
(Sheet 1 of 2)

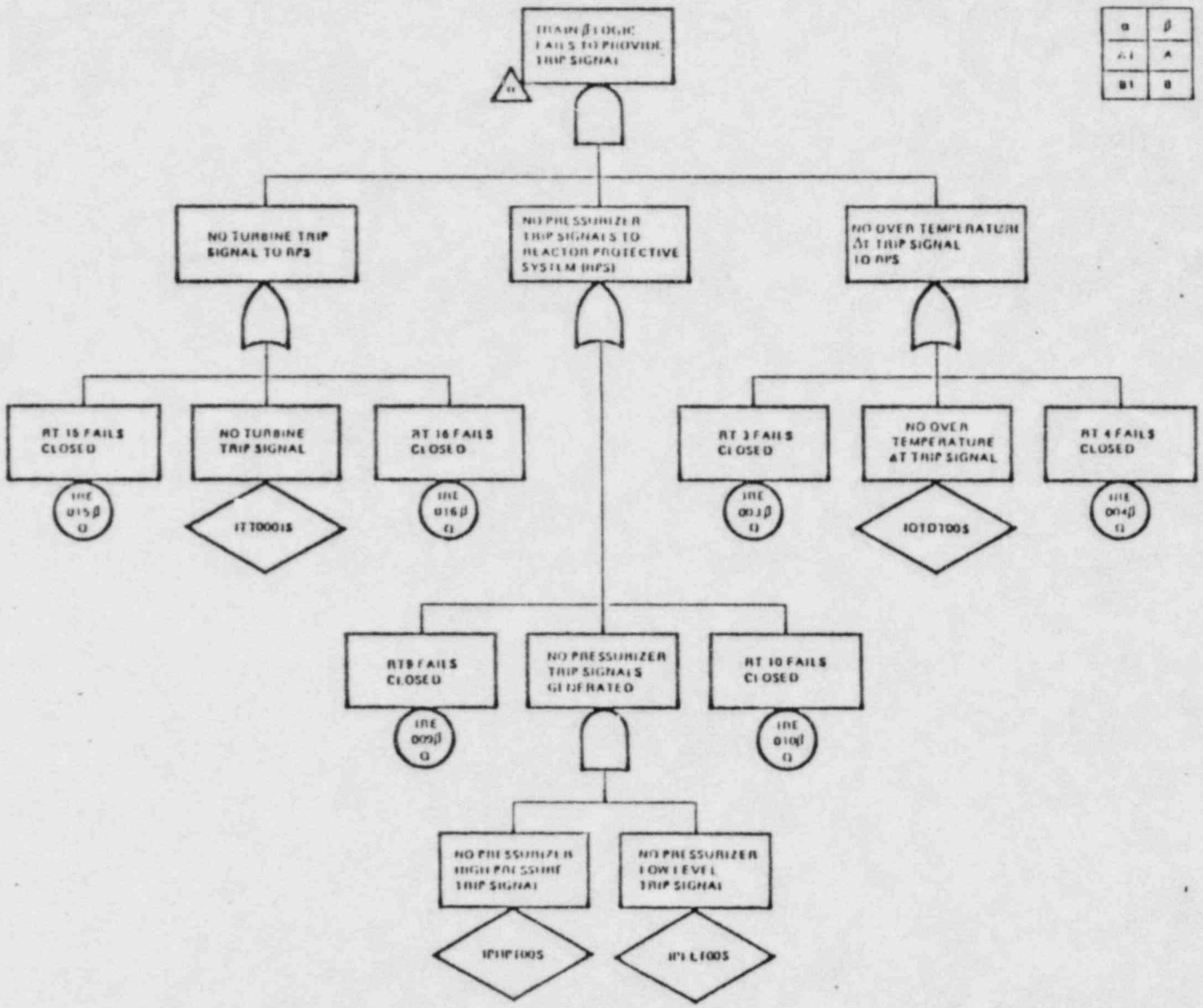


Figure 4. (Sheet 2 of 2)