REVIEW OF THE DCPRA: Letter Report-01/Rev.2

A REVIEW OF SYSTEM'S ANALYSIS IN THE DCPRA: THE SOLID STATE PROTECTION AND REACTOR PROTECTION SYSTEMS

G. Bozoki
R. Fitzpatrick
M. Sabek

May 1989

Risk Evaluation Group
Department of Nuclear Energy
Brookhaven National Laboratory
Upton, NY 11973

Prepared for
U.S. Nuclear Regulatory Commission
Washington, DC 20555
Contract No. DE-AC02-76CH00016
FIN A-3958

8906010089 890512
PDR ADOCK 05000275
P PDC

1. INTRODUCTION

1.1 Objectives and Background

One of the main tasks to be performed within the framework of reviewing the DCPRA outlined in BNL's approach to the DCPRA review,[1] is to scrutinize the unavailability analyses of several selected support and frontline systems. The objective of the present letter report is to provide the results, to date, of reviewing the unavailability analyses of the Solid State Protection System (SSPS) and the Reactor Protection System (RPS). All findings and insights listed in this report reflect BNL's current understanding of the DCPRA and as such must be considered interim results. Final results for this analysis will be provided in the NUREG/CR document to be issued at the end of the project and will reflect at that time, any additional supporting input submitted by PG&E as well as any direct feedback on these preliminary findings.

According to the DCPRA, the SSPS and RPS represent the only non-plant-specific (i.e., generic) systems analyzed in the PRA. The systems were provided by Westinghouse and belong to designs of fairly recent vintage.

The generic review methodology described in the PRA Review Manual[2] suggests that a comparison be made between the results obtained for the unavailabilities of systems of these types in a PRA under review and the results obtained in unavailability studies (if they exist) dedicated to "generic" systems.

Recently the Westinghouse Electric Corp. conducted very comprehensive unavailability studies on the Solid State Protection[3] (from now on to be referred to as "WOG1") and Reactor Protection Systems[4] (from now on to be referred to as "WOG2") on behalf of the Westinghouse Owners Group. The studies served as bases for requesting certain changes in the surveillance

requirements of the Technical Specifications for these systems from the NRC. Both studies were reviewed by BNL. BNL conducted a thorough audit calculation for the SSPS[5] (to be referred to as "BNL1") and a time-dependent Markovian analysis for the RPS[6] (to be referred to as "BNL2").

Therefore, for a comparative unavailability analysis of the DCPRA models and results, the WOG/BNL models were selected as bases. In order to render these models comparable to the conditions and assumptions used in the DCPRA, both models (WOG and BNL) were modified accordingly prior to the comparative analysis.

1.2 Organization of the Report

The present report documents the results of the comparative analyses noted above and is organized as follows: Chapter 2 describes the SSPS and its testing provisions/methods. Chapter 3 presents the comparison of the approaches used in the DCPRA and in the WOG/BNL calculations to model the SSPS and the results obtained. Chapter 4 discusses the RPS, its testing methods and the results of those comparative analyses.

2. SOLID STATE PROTECTION SYSTEM

2.1 System Description

The Solid State Protection System provides actuation signals to emergency safeguard equipment and to the reactor protection system when process and nuclear parameters exceed certain preset limits ensuring that safe operating conditions exist at all times.

The main components of the SSPS are:

1. the analog channels,
2. the combinational logic units, and
3. the actuation relays.

2.1.1 Analog Channels

An analog channel involves: an analog sensing device (sensor/transmitter), a loop power supply, a signal conditioning circuit, and a signal comparator. The sensing device monitors a given process or nuclear parameter, such as pressure, level, flow, temperature or flux, etc. The parameter signals are converted to proportional voltage signals by the power supply of the loop (Figure 2.1). The sensed signal is "shaped" by the signal conditioning circuit (signal modifiers). The shaped signal is compared with a preset parameter value by the comparator (bistable). The comparator controls two output relays; one of them provides input signals to the combinational logic train A and the other to combinational logic train B.

2.1.2 Combinational Logic Unit and Master Relays

The combinational logic unit is a dual train electronic system. Trains A and B contain several 2/4, 2/3, and 1/2 logic circuits built on universal logic (UL) cards. The analog channel output relays operate grounding contacts at the inputs of the combinational trains. A trip signal is generated in each of the

trains if an appropriate number of card inputs are grounded. Outputs of various logic circuits in each of the trains can be further interconnected by using additional logic circuits to achieve desired reactor trip and safeguard initiator signal combinations. The safeguard initiator signals drive the master relays by creating a current flow which energizes them. The block diagram of a typical SSPS is shown in Figure 2.2.

2.1.3 Slave Relays

Given an initiator signal, the energized master relays close contacts in the slave relay circuits and energize master relays close contacts in the slave relay circuits and energize the associated slave relays. The slave relays activate the safety systems by energizing contacts in motor starters, solenoid circuits, etc. Usually each slave relay activates several safety system components. The number of master and slave relays energized is dependent upon the complexity of a given protective function required by a specific initiating event. The SSPS trains are train oriented: ESFAS train A energizes train A of a safety system, etc.

Figure 2.3 shows the schematics of slave relay arrangements. Figure 2.4 presents the parameter signals and the master and slave relay arrangements modelled in the DCPRA which generate actuation signals for various safety functions.

2.2 Testing of the ESFAS

2.2.1 Testing of the Analog Channels

The functional testing of the analog channels is performed at power. Its purpose is to verify the entire operation of the channel excluding the sensor. Calibration and verification of proper operation of the sensors (the associated electronics included) is usually performed at shutdown. The functional testing

scheme of the analog channels for the SSPS is also shown in Figure 2.1. The sensor is disconnected during testing. By using test jacks, test signals are sent through the circuit. A proving lamp is connected to the output of the bistable; usually the bistable is adjusted to ensure that the whole channel performs as required. The input relays of the logic trains are energized from outside circuits if the channel is tested in bypass. The input relays are de-energized if the channel is tested in trip.

During normal operation, a failure of a sensor or a loop power supply would cause abnormal indication and/or alarms. The status lights are checked by operators every shift, therefore, an analog channel failure is detectable within eight hours.

2.2.2 Testing of the Combinational Logic Units

While a plant is at power, each of the combinational logic trains (located in separate cabinets) is allowed to be tested or maintained separately in "bypass" condition. Time sequenced pulses are applied to the logic circuits through switches located on a logic test panel dedicated to each train (semi-automatic tester). The pulses check the logic, but are of such a short duration that slave relay (or trip breaker) actuation is not possible. The semi-automatic tester allows quick and efficient testing of all the possible logic combinations of actuate or non-actuate conditions as well as the effects of the permissives. If one train is in test or in maintenance, the other is charged with providing all the safety function signals. It is not possible to lock out both logic trains without tripping the reactor. The tests of the combinational logic trains are performed according to a staggered testing schedule.

2.2.3 Testing of the Actuation Relays

The master relays are "continuity" tested as part of the logic test to demonstrate total circuit operation. The master relays are actuated during master relay testing and proper contact operation is checked. Figure 2.3 also shows the test conditions for the actuation relays. Proper contact operation is verified by "continuity" checking of the associated slave relay. This test is performed by applying a voltage to the master relay contact which demonstrates the continuity but which is insufficient to activate the slave relay.

The "actuation" test of a slave relay is performed individually by energizing the relay and demonstrating proper contact operation. Proper contact operation can be demonstrated with or without operating the associated equipment. The slave relay test sometimes requires the reconfiguration of the equipment to be tested in such a way that the test would not cause adverse effects on the plant operation. After the test, the equipment has to be returned to its normal operating configuration. Therefore, associated with each slave relay test there is also a potential for human error in that the personnel conducting the test could fail to return the equipment to its proper operating configuration. At Diablo Canyon the test of the slave relays is (presumably) performed at shutdown. (This condition, therefore, has been considered in the modified WOG/BNL modelling.)

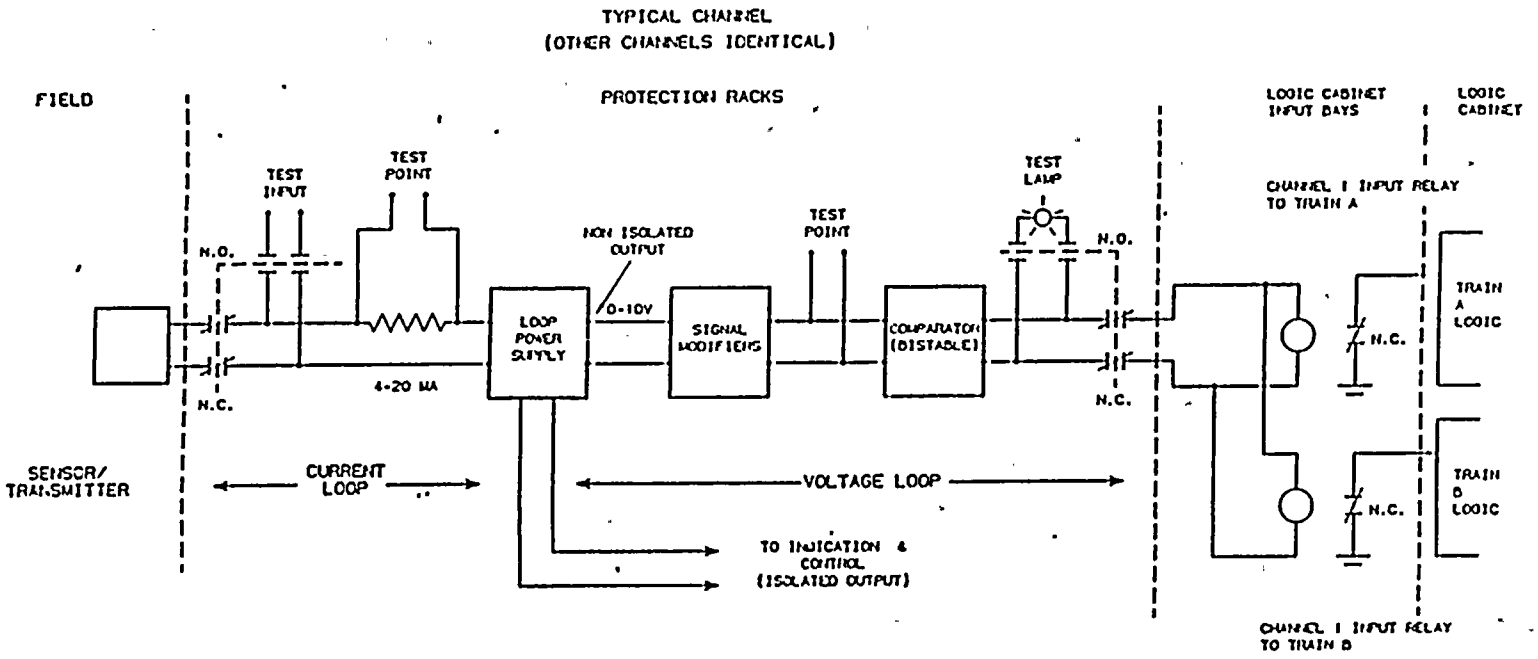


Figure 2.1 Analog channel block diagram.

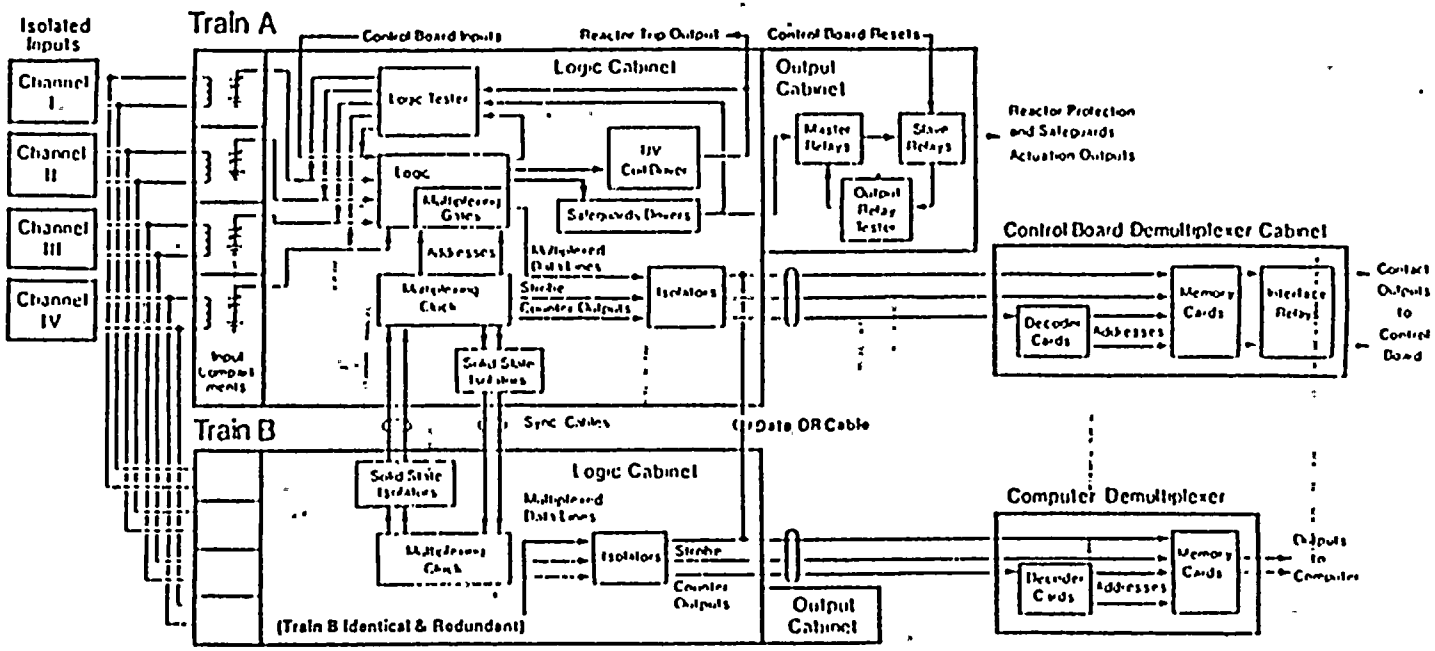


Figure 2.2 Block diagram of a typical Solid State Protection System.

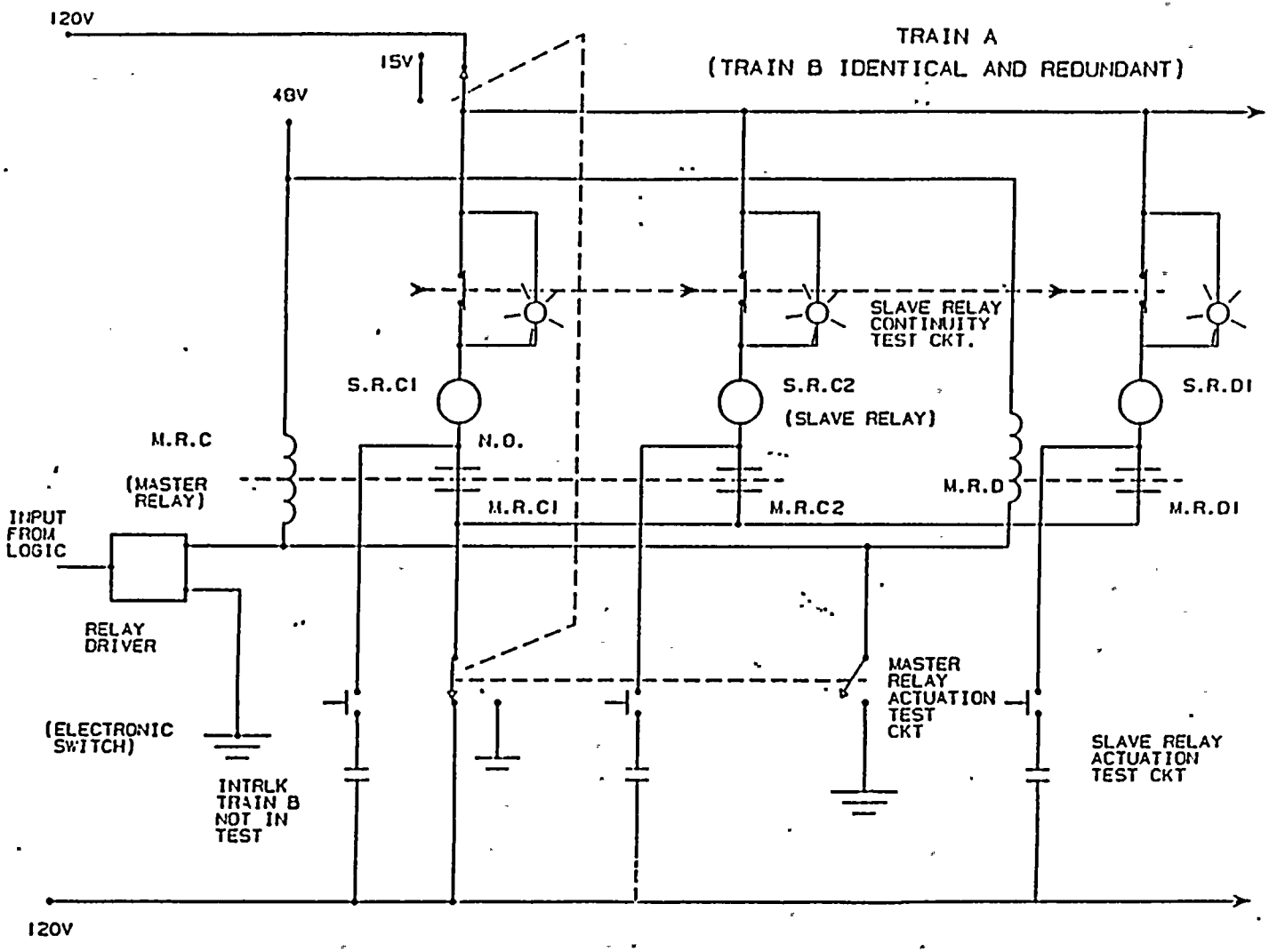
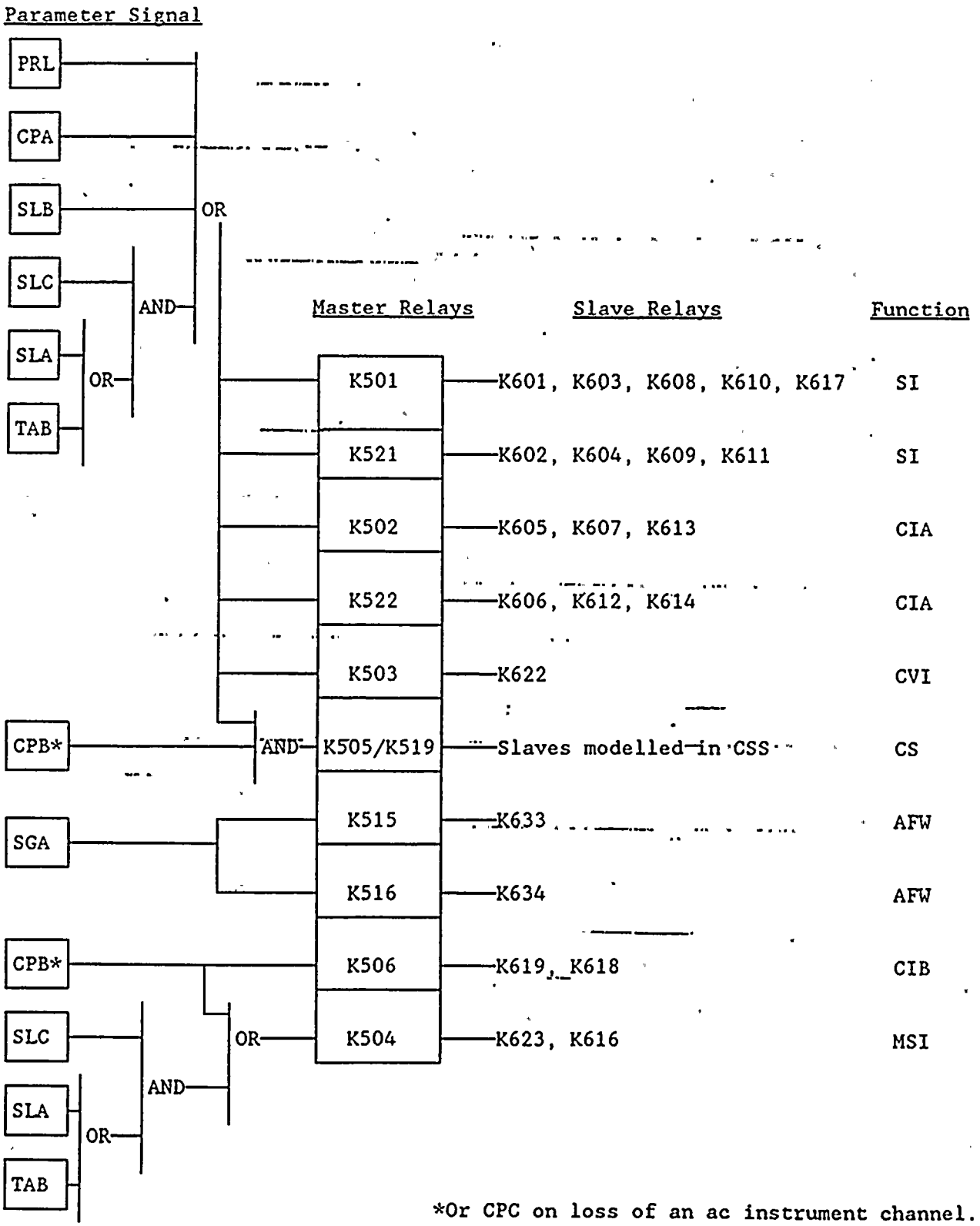


Figure 2.3 Schematic of actuation relays.



*Or CPC on loss of an ac instrument channel.

Figure 2.4 SSPS block logic.

Notes to Figure 2.4

		Logic
CSS	Containment Spray System	
CPA	Containment Pressure High	2/3
CPB	Containment Pressure High-High	2/4
SGA	Steam Generator Level Low-Low	2/3 per SG (for 1/4 SG)
PRL	Pressurizer Pressure Low	2/4
SLA	Steamline Pressure Low	1/1 per loop for 2/4 loops
SLB	Steamline Differential Pressure High	2/3 per loop for 1/4 loops
SLC	Steamline Flow High	1/2 per loop for 2/4 loops
TAB	Low-Low Tang	1/1 per loop for 2/4 loops
AFW	Auxiliary Feedwater Startup	
SI	Safety Injection and Associated Actions	
CIA	Containment Isolation, Phase A	
CIB	Containment Isolation, Phase B	
CVI	Containment Vent Isolation	
CS	Containment Spray	
MSI	Main Steamline Isolation	

3. COMPARISON OF SSP SYSTEMS ANALYSIS OF DCPRA WITH THAT OF WOG/BNL

In this section the SSP systems analysis is compared with that of WOG/BNL. Only those aspects of both approaches are discussed which are deemed to be relevant for clear understanding of the differences.

3.1 Unavailability Modelling of the SSPS Signals in DCPRA

In the DCPRA six classes of initiating events were selected for which the unavailabilities of the SSPS were modelled. This selection was based on a unique set of safety functions required to be actuated by the SSPS given any type of initiating events. Table 3.1 lists the modelled initiating event classes with the required safety functions to be actuated. The table also lists the (minimum) number of master and slave relays per SSPS train which are involved in generating the appropriate safety system responses. The success criterion of the SSPS is: at least one of the two trains must produce an actuation signal for all necessary safety functions; that is; each slave relay (appropriately identified in the DCPRA) must produce actuation signals in at least one SSPS train.

Notice, this DCPRA success criterion is conservative, because it lumps together the success of the diverse safety functions. If any one required safety function fails, all the diverse functions are also assumed to be lost. (This conservatism is also valid at the train level: if one safety function on train A is lost, all train A actuation signals are assumed lost.)

Figure 3.1 shows, as an example, the master fault tree for a class of initiating events: steam generator tube rupture. Given this initiator, the model assumes a diversity of parameter signal failures which may contribute to the failure of an SSPS train (see the SSPS block diagram on Figure 2.4). These are: Pressurizer Low Pressure (2/4), Steam Generator Low-Low Level (2/3 on 2/4

SG), High Steam Flow (2/4), or the combined T Average Low-Low (2/4), and Low Steamline Pressure (2/4) signals. In addition, the whole train is assumed to fail if either the power supply or the logic or any of the master or slave relays (in this case 8 master relays and 20 slave relays) fail.

On the component level, the model includes the failures of the bistables, the input relays, the signal transmitters, the failures of the input, master and slave relays, as well as the power supplies converting instrument ac to 48 and 15V dc. The failure of the logic card is not modelled in terms of the components, it is characterized by a simple failure rate.

The model assumes common cause failures between bistables and input relays for a particular function (there is no assumption for overall failure of the sensor signals). Common cause failures for master and slave relays are modelled for all two-member cutsets based on two or more failures out of the total number of relays (11 master and 22 slave relays). Common cause failure is also considered between the logic cards.

The DCPRA includes the unavailability contribution due to surveillance performed during power operations. This unavailability contribution is apparently considered only for the analog channels and logic cabinets. (The situation concerning the master relays is not yet fully clear.) Table 3.2 presents the relevant data (and their designators). The only maintenance event modelled in the DCPRA is the repair of randomly failing power supplies. The relevant information is also given in Table 3.2. Human error is modelled only for miscalibration of analog channels.

The effects of the unavailability of the ac instrument channels are included in the various boundary conditions, for which the various fault trees (corresponding to the initiating events) were evaluated. Table 3.3 reproduces

the basic SSPS signal unavailabilities (split fractions) of a single train and of the whole system for various boundary conditions. The table separately shows the total unavailability, as well as the unavailability contributions due to independent and dependent hardware failures, test, maintenance, and human errors.

According to this model the leading contributor to a single train unavailability is independent hardware failures (~80%). The leading contributors to total systems failure are: the human errors of miscalibration and dependent hardware failures.

3.2 Unavailability Modelling of SSPS Signals by the WOG/BNL Approach

In the WOG/BNL modelling of the SSPS (WOG1[3] and BNL1[5]) the unavailabilities of the various safety function actuation signals are not lumped together, but rather are individually calculated. Table 3.4 lists the various safety function actuation signals considered in the analyses. The number of master and slave relays per train involved in each of these safety function actuation signals are also given in the table. The success criterion of the system is similar to that used in the DCPRA: each slave relay must produce actuation signals in at least one SSPS train.

The fault tree model of each safety function actuation signal was evaluated for various process parameter signals and logic. Table 3.5 presents a subset of those safety function actuation signals which were selected according to their relevance to Diablo Canyon.

The basic structure of the fault tree models for the various safety function actuation signals is somewhat similar to that of the DCPRA (after all, this structure is essentially determined by the real system's design). However, in contrast with the DCPRA models, the diversity of process parameter

signals was reduced (in most cases only one type of process parameter signal was assumed). On the other hand, the modelling of the permissives, which was neglected in the DCPRA, was considered.

The detailed fault trees are rather intricate and complex. The level of detail is shown to minute electronic parts, therefore, they are not shown here. They can be found in Appendix C of WOG1.[3] The fault trees usually consist of three parts: a top fault tree, one or more middle fault trees, and the analog channel fault trees. The top fault tree describes the master and slave relays. The middle fault trees describe the master relay drivers and the logic cards including the permissive circuits. The analog channel fault trees describe the sensors, the power supply, the signal conditioning and signal comparator circuits. The rates of various failure modes of the components were taken from the Westinghouse data base, Military Handbook 217C, and IEEE 500.

Common cause failures were modelled for the analog channels, the logic cabinets and the master and slave relays. For the analog channels the Atwood/Binomial failure rate method was used. For the logic cabinets as well as the master and slave relays the beta factor method was applied. Human errors such as miscalibration or misposition of sensors, amplifiers, etc., were considered only in the analog channel fault trees, by using the guidelines of Swain's Human Reliability Handbook.

The modelled surveillance conditions are given in Table 3.2. This table also shows the maintenance conditions considered in the WOG1/BNL1 calculations. A comparison with the conditions used in the DCPRA shows two minor differences:

a. The WOG1/BNL1 calculations consider the unavailability contribution of the master relays due to test.

b. In addition, they assume once/year maintenance for the analog channels, logic and master relays. This assumption was deemed to be more conservative than the randomly occurring maintenances modelled in the DCPRA.

Notice that the unavailability contributions due to test and maintenance of the slave relays were not taken into account in either approach.

Table 3.5 gives the system unavailabilities for the various safety function actuation signals for two cases. In the first case the effects of common cause failures are not considered and in the second case when the common cause failures are included in the results.

A breakdown of the results is given in Table 3.6 for two safety function signals: the safety injection signal and the auxiliary feedwater pump signal (the results of the calculations are presented in similar format as those given in the DCPRA).

The analysis provided the following findings: in general, common cause failures (logic trains, master and slave relays) are the main contributors to overall SSPS unavailability. The main contributors to train unavailabilities are: independent hardware failures (mainly master and slave relay failures due to mechanical binding and short circuits) and unavailability due to test. Analog channel contribution to signal unavailability proved to be negligible. Sensitivity calculations assuming more diversity in the parameter signals gave similar results.[3]

3.3 Comparison of the DCPRA and WOG1/BNL1 Results

A comparison of the data given in Table 3.3 with the results shown in Tables 3.5 and 3.6 shows that the DCPRA appears to systematically underestimate the SSPS signal unavailabilities. In the worst case the underestimation

contains a factor of about 4.6, however the situation is exacerbated by the fact that the DCPRA gives the unavailability for a group of safety function signals (i.e., an OR gate) while the WOG1/BNL1 results relate to the unavailability of a single safety function signal alone. In other words, a direct comparison would yield a larger discrepancy.

A possible explanation of the discrepancy could be that conditional unavailabilities (because of the boundary conditions in the DCPRA treatment) are compared with non-conditional ones (BNL/WOG results).* However, sensitivity analyses performed by BNL have shown that such an explanation is not valid as the differences between the two sets of unavailabilities are small.

BNL believes the root cause of the discrepancy is that an oversimplified fault tree model was used for the SSPS in the DCPRA and plans to substitute what is believed to be more appropriate results (BNL/WOG) in any BNL requantification (modified as necessary to reflect the conditional nature of the probabilities required in the DCPRA model) pending any further information from PG&E.

---

*For example in Table 3.3 the DCPRA values were obtained by assuming that all electrical power was available (i.e., failure of electrical power did not contribute to the unavailability), while in the BNL/WOG calculations the occurrences of such failures did contribute to the unavailability.

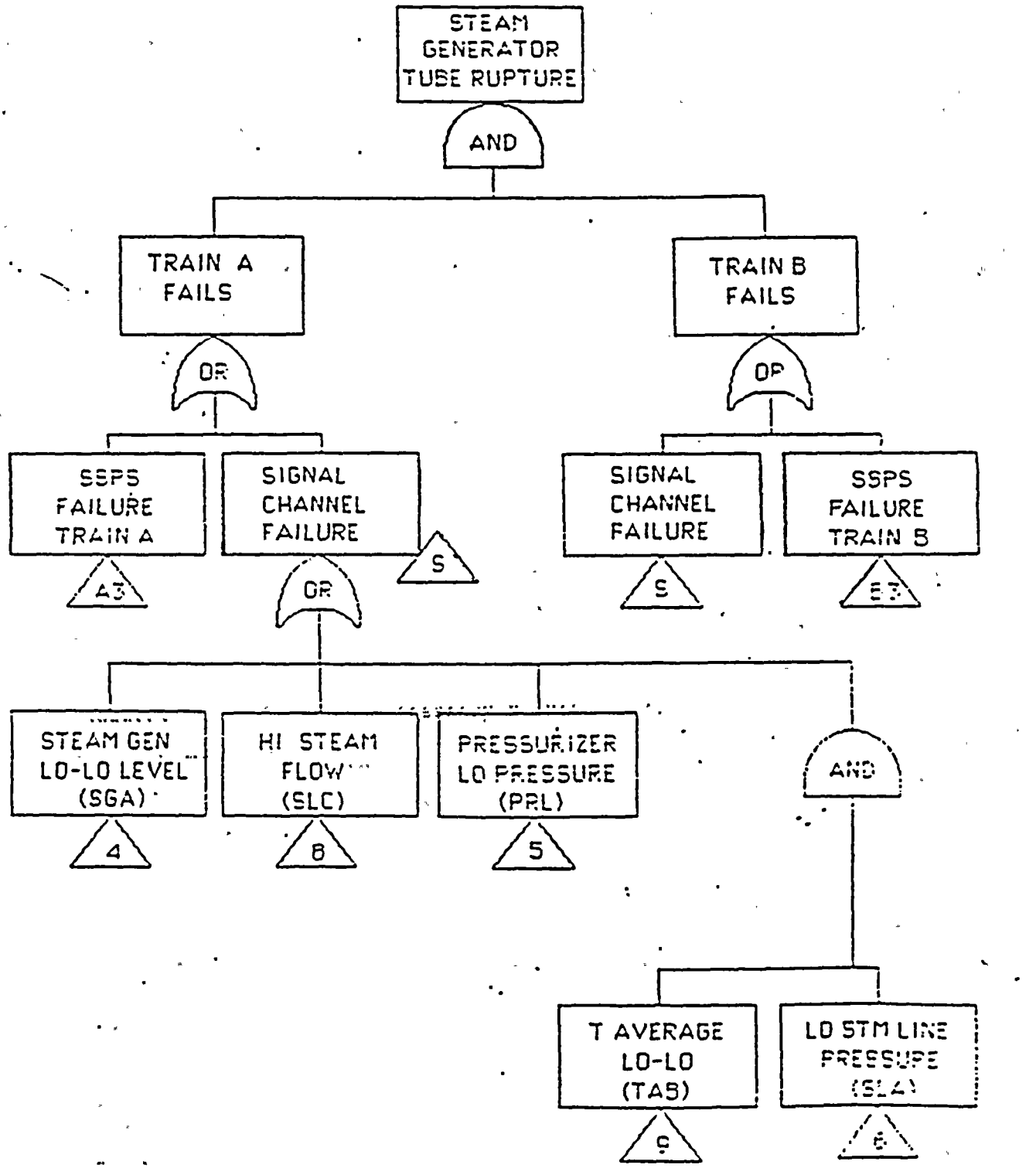


Figure 3.1.a SSPS master fault tree for steam generator tube rupture initiator in DCPRA.

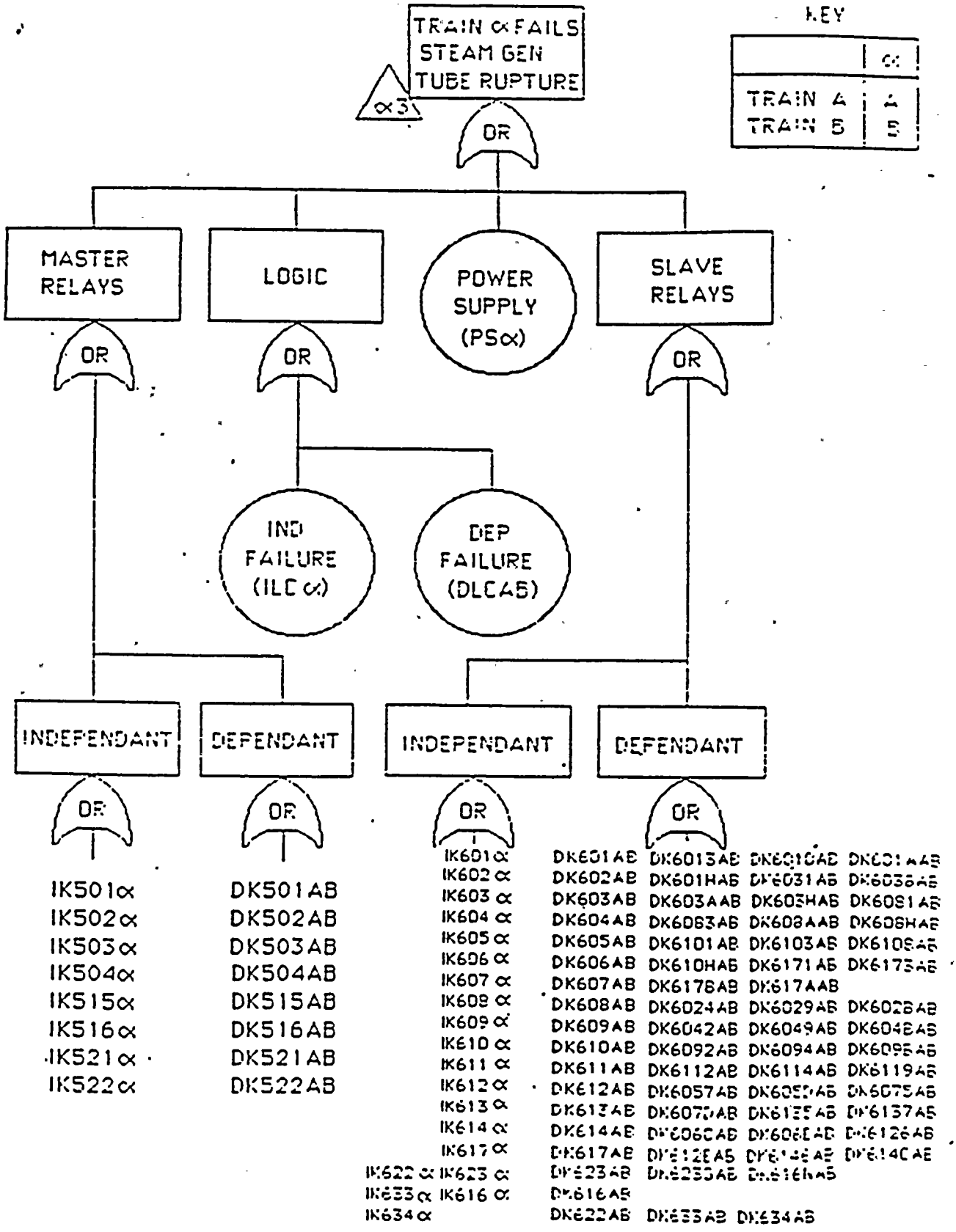


Figure 3.1.b SSPS master fault tree.

Table 3.1
SSPS Safety Functions Modelled in
Diablo Canyon PRA

Initiating Event	Safety Function	Required Master Relays Per Train	Required Slave Relays Per Train
General Transient*	Aux. Feed. Trains	2	2
	Main Steamline Isol. (M)	1	2
	Cont. Isol. Phase A (T)	2	6
	Cont. Vent Isol.	1	1
	Total	6	11
Large LOCA (LLOCA)	Safety Injection (S)	2	9
	Cont. Isol. Phase A (T)	2	6
	Cont. Isol. Phase B (P)	1	2
	Cont. Vent. Isol.	1	1
	Cont. Spray (P)	2	2
	Total	8	18
Steam Gen. Tube Rupture (SGTR)	Safety Injection (S)	2	9
	Cont. Isol. Phase A (T)	2	6
	Cont. Vent Isol.	1	1
	Aux. Feed. Train	2	2
	Main Steamline Isol. (M)	1	2
	Total	8	20
Steamline Break Ins. Cont. (SLBIC)	Safety Injection (S)	2	9
	Aux. Feed. Trains	2	2
	Cont. Isol. Phase A (T)	2	6
	Cont. Isol. Phase B (P)	1	2
	Cont. Vent Isol.	1	1
	Main Steamline Isol. (M)	1	2
	Cont. Spray (P)	2	2
	Total	11	22
Steamline Break Outside Cont. (SLBOC)	Safety Injection (S)	2	9
	Aux. Feed. Trains	2	2
	Cont. Isol. Phase A (T)	2	6
	Cont. Vent Isol.	1	1
	Main Steamline Isol. (M)	1	2
	Total	8	20

Table 3.1 (Continued)

Initiating Event	Safety Function	Required Master Relays Per Train	Required Slave Relays Per Train
Small LOCA (SLOCA)	Safety Injection (S)	2	9
	Cont. Isol. Phase A (T)	2	6
	Cont. Vent Isol.	1	1
	Aux. Feed. Trains	2	2
	Main Steamline Isol. (M)	1	2
	Total	8	20

*Reactor trip, turbine trip signal unavailabilities are modelled presumably with this initiating event.

Table 3.2
SSPS Surveillance Modelling

	Modelled in DCPRA (Designator)	Modelled in WOG1/BNL1
Logic Cabinets		
Test interval (month)	2 (TS2F)	2
Test time (hour)	2 (ZHDSS2)	1.5
Maintenance interval (month)	Unscheduled*	12
Maintenance time (hour)	Plant-specific**	2
Master Relay		
Test interval (month)	?	2
Test time (hour)	?	1.5
Maintenance interval (month)	?	12
Maintenance time (hour)	?	2
Slave Relay		
Test interval (month)	---	---
Test time (hour)	---	---
Maintenance interval (month)	---	---
Maintenance time (hour)	---	---
Analog Channel		
Test interval (month	1 (TS1F)	1
Test time (hour)	2 (ZHDSS2)	2
Maintenance interval (month)	---	12
Maintenance time (hour)	---	1

*ZTPS1R (Power Supply Failure Rate) = 1.71-5/hr.
**ZMGNBF (Time to Repair Failed Power Supply) = Not yet given by PG&E.
?The test and maintenance of master relays are apparently not accounted for in the DCPRA model.

Table 3.3
SSPS Signal Unavailabilities
(Split Fractions in Diablo Canyon PRA)

Case	TTL	HW	HWI	HWD	TS	MN	HE	Comment #
A: Single Train (Train A) Failure								
SA1, SB3	6.47-3	5.68-3	5.68-3	1.48-10	7.89-4	4.23-10	4.18-6	
SA2	9.69-3	8.50-3	8.50-3	1.39-6	7.89-4	4.23-10	3.98-6	
SA4, SBB	9.95-3	9.16-3	9.15-3	1.39-6	7.89-4	4.23-10	6.28-6	
SA5	1.18-2	1.06-2	1.06-2	1.39-6	7.89-4	4.23-10	4.00-4	
SA7	9.95-3	9.15-3	9.15-3	3.20-11	7.89-4	4.23-10	4.18-6	
SA8, SBN	9.95-3	9.15-3	9.15-3	1.48-10	7.89-4	4.23-10	4.18-6	
B: System (Trains A and B) Failure								
SB2'	9.86-5	8.54-5	1.14-5	7.40-5	9.02-6	5.74-12	4.18-6	
SB6'	6.07-4	1.96-4	2.19-5	1.74-4	1.36-5	8.12-12	3.98-4	
SBA'	2.17-4	1.96-4	2.26-5	1.74-4	1.46-5	8.68-12	6.28-6	
SBE'	6.37-4	2.20-4	2.56-5	1.94-4	1.69-5	9.09-12	3.40-4	
SBJ'	2.13-4	1.94-4	2.18-5	1.72-4	1.45-5	8.68-12	4.18-6	
SBM'	2.13-4	1.94-4	2.18-5	1.72-4	1.45-5	8.68-12	4.18-6	

Split Fraction Identification:

SA1, SB3 — General transient, all needed electrical power is available, or ac Instr. Chnl. I is down.
SA2 — Large LOCA, all needed electrical power is available.
SA4, SBB — Steam Generator Tube Rupture (SGTR), all needed electrical power is available, or ac Inst. Chnl. I is down.
SA5 — Steamline Break Inside Containment (SLBIC), all needed electrical power is available.
SA7 — Steamline Break Outside Containment (SLBOC), all needed electrical power is available.
SA8 — Small LOCA, all needed electrical power is available.
SB2' — General transient, both trains, A and B, fail.
SB6' — Large LOCA, both trains, A and B, fail.
SBA' — Steam Generator Tube Rupture (SGTR), both trains, A and B, fail.
SBE' — Steamline Break Inside Containment, both trains, A and B, fail.
SBJ' — Steamline Break Outside Containment, both trains, A and B, fail.
SBM' — Small LOCA, both trains, A and B, fail.

Table 3.3 (Continued)

Notations

TTL =Total unavailability.
HW =Unavailability due to hardware contribution which is the sum of independent failures and common cause failures.
HWI = Unavailability due to independent failures.
HWD = Unavailability due to common cause failures.
TS = Unavailability due to test.
MN = Unavailability due to maintenance.
HE = Unavailability due to human error contribution.

Table 3.4
Master/Slave Relay Arrangements for Various
Safety Function Actuation Signals

Safety Function Actuation Signal	Master Relays*	Slave Relays*
1. Safety Injection	A B	A1, A2, A3 B1, B2, B3
2. Steam Line Isolation	A	A1, A2
3. Main Feedwater Isolation	A	A1, A2
4. Auxiliary Feedwater Pump Start	A	A1, A2
5. Containment Spray	A	A1, A2
6. Containment Isolation	A	A1, A2

*Relays per SSPS train as applied in the unavailability analysis.

Table 3.5
SSPS Signal Unavailabilities (WOG1/BNL1)

Safety Function Actuation Signal	Process Parameter Signal	Unavailability w/o CCF	w/CCF
1. Safety Injection 2 Master Relays, 6 Slave Relays per Train.	1.1 Pressurizer pressure - low - 2/4, interlocked with permissive P11 - 2/3.	1.1-4	1.1-3
	1.2 Steamline pressure - low - 2/4, interlocked with P11 - 2/3.	1.1-4	1.1-3
	1.3 Steamline pressure - low - 2/4, interlocked with P12 - 2/3 or 2/4.	1.1-4	1.1-3
	1.4 Containment pressure - high - 2/3.	1.5-4	1.1-3
	1.5 Differential steamline pressure - high, 3 instr./steamline.	1.1-4	1.1-3
	1.6 Steamflow - high - 1/2 coincident with $T_{avg.}$ - low-low - 2/4 or steamline pressure - low - 2/4, interlocked with P12 - 2/3 or 2/4.	1.8-4	1.3-3
2. Steamline Isolation, 1 Master Relay, 2 Slave Relays per Train.	2.1 Steamline pressure - low - 2/4.	4.7-5	4.9-4
	2.2 Containment pressure - high-high - 2/4.	4.8-5	4.9-4
	2.3 Steamflow - high - 1/2 coincident with $T_{avg.}$ - low-low - 2/4 or steamline pressure - low - 2/4.	1.4-4	8.6-4

Table 3.5 (Continued)

Safety Function Actuation Signal	Process Parameter Signal	Unavailability w/o CCF	w/CCF
	2.4 Steamline pressure - low - 2/4 and steamflow - high - 1/2 coincident with $T_{avg.}$ - low-low - 2/4 interlocked, with P12 - 2/3 or 2/4.	4.7-5	5.0-4
	2.5 Steamflow - high - 1/2 interlocked with P12 - 2/4 coincident with SI.	1.4-4	8.2-4
3. Containment Isolation Phase B, Containment Spray 1 Master Relay, 2 Slave Relays per Train.	3.1 Containment pressure - high-high - 2/4.	1.1-4	9.6-4
4. Auxiliary Feedwater Pump Start Signal, 1 Master Relay, 2 Slave Relays per Train.	4.1 Steam generator water level low-low - 2/4 in one loop.	6.1-5	5.7-4
	4.2 Steam generator water level - low-low - 2/3 in one loop.	1.3-4	6.4-4
	4.3 RCP bus undervoltage - 2/3.	1.8-4	7.6-4
	4.4 RCP bus undervoltage - 1/2 twice.	1.5-4	7.2-4
5. Main Feedwater Isolation, 1 Master Relay, 2 Slave Relays per Train.	5.1 Steam generator water level - high-high - 2/3 in one loop.	1.3-4	6.4-4

CCF = Common cause failures.

Table 3.6
SSPS Signal Unavailabilities Calculated by WOG1/BNL1

Case	TTL	HW	HWI	HWD	TS	MN	HE	Comment #
A: Single Train Failure								
Auxiliary Feedwater Pump Start Signal 1 Master Relay and 2 Slave Relays per Train	8.00-3	6.08-3	6.06-3	1.50-5	1.56-3	3.47-4	4.8-8	1
Safety Injection Signal 2 Master Relays and 6 Slave Relays per Train	1.12-2	7.42-3	7.40-3	1.50-5	3.12-3	6.94-4	5.7-8	2
B: System Failure								
Auxiliary Feedwater Pump Start Signal 1 Master Relay and 2 Slave Relays per Train	5.66-4	5.43-4	3.67-5	5.06-4	1.90-5	4.22-6	4.8-8	1, See also Table 5.
Safety Injection Signal 2 Master Relays and 6 Slave Relays per Train	1.08-3	1.02-3	5.48-5	9.64-4	4.62-5	1.03-5	5.7-8	2, See also Table 5.

1. The process parameter signal is: steam generator level low-low (2/4 in 1 loop). The Auxiliary Feedwater Pump Start Signal is also indicative of Steamline Isolation and Main Feedwater Isolation.
2. The process parameter signal is: low pressurizer pressure (2/4 interlocked with P-11 2/3). The Safety Injection Signal is also indicative of Containment Spray Actuation and Phase B Isolation.

Notations
TTL = Total unavailability.
HW = Unavailability due to hardware contribution which is the sum of independent failures and common cause failures.
HWI = Unavailability due to independent failures.
HWD = Unavailability due to common cause failures.
TS = Unavailability due to test.
MN = Unavailability due to maintenance.
HE = Unavailability due to human error contribution.

4. COMPARISON OF RPS UNAVAILABILITIES OBTAINED IN DCPRA AND IN WOG/BNL CALCULATIONS

4.1 System Description

The Reactor Protection System (RPS) could be considered a continuation of the SSPS in the sense that it trips the reactor on a "trip" signal from the SSPS. The RPS also trips the reactor if loss of power occurs, or the plant operator manually actuates the system. The RPS consists of two trains each containing two undervoltage coils in an energized condition and associated breakers. One undervoltage coil for the reactor trip breaker and one for the bypass breaker. When an SSPS train generates a trip signal the UV coils are de-energized. This will open the reactor trip and bypass (if closed) breakers removing power from the control rods, allowing the rods to fall into the core. A schematic of the RPS at Diablo Canyon is shown in Figure 4.1. The success of the RPS is defined as at least 52 of the 53 control rods successfully inserted into the core on demand.

4.2 Testing of the RPS

Testing of the analog channels and logic is essentially identical with that described in Sections 2.2.1 and 2.2.2. When the breaker actuation test is performed, the associated bypass trip breaker is closed to prevent an unwanted reactor trip. The manual trip test can be performed by using four push buttons.

4.3 Unavailability Modelling of the RPS in the DCPRA and in the WOG/BNL Calculations

4.3.1 The RPS Fault Tree Model in the DCPRA

The RPS fault tree model of the DCPRA is shown in Figure 4.2. It is a block level fault tree with identified common cause events (α-factor model). The block events involve the control rod insertion failure, circuit breaker

failures, undervoltage rely and trip coil failures, bypass undervoltage relay, bypass circuit breaker, and shunt trip coil failures.

The surveillance and maintenance conditions of the RPS modelled in the DCPRA are shown in Table 4.1. The model correctly describes the staggered testing of the trip breakers. The effect of loss of dc power, instrument ac and loss of SSPS signals are considered in the boundary conditions. The quantification indicated that the common cause failures of the circuit breakers and trip coils dominate the system unavailability.

4.3.2 The RPS Unavailability Models in the WOG/BNL Calculations

In the WOG2 calculation[4] a set of fault trees was used to quantify the unavailabilities of the RPS for various trip signals. The fault trees are rather complex as they were developed and updated over many years. The NRC and BNL have scrutinized them and they are therefore not reproduced here. Representative fault trees can be found in Reference 4.

The trip signal unavailabilities obtained in these calculations relate to the whole system including the analog channels and the logic. The fault tree model in the DCPRA does not show these components because that approach considers them by the boundary conditions.

The WOG2 calculations contain the complete set of unavailability contributors; random, common cause, and human errors as well as unavailabilities due to test and maintenance. The common cause and human errors for the analog channels and logic portions of the RPS are identical to those described earlier for the SSPS modelling by WOG1/BNL1 (Section 3). Additional common causes have been quantified for the reactor trip and bypass breakers. The surveillance and maintenance conditions considered are given in Table 4.1 for comparison with those used in the DCPRA.

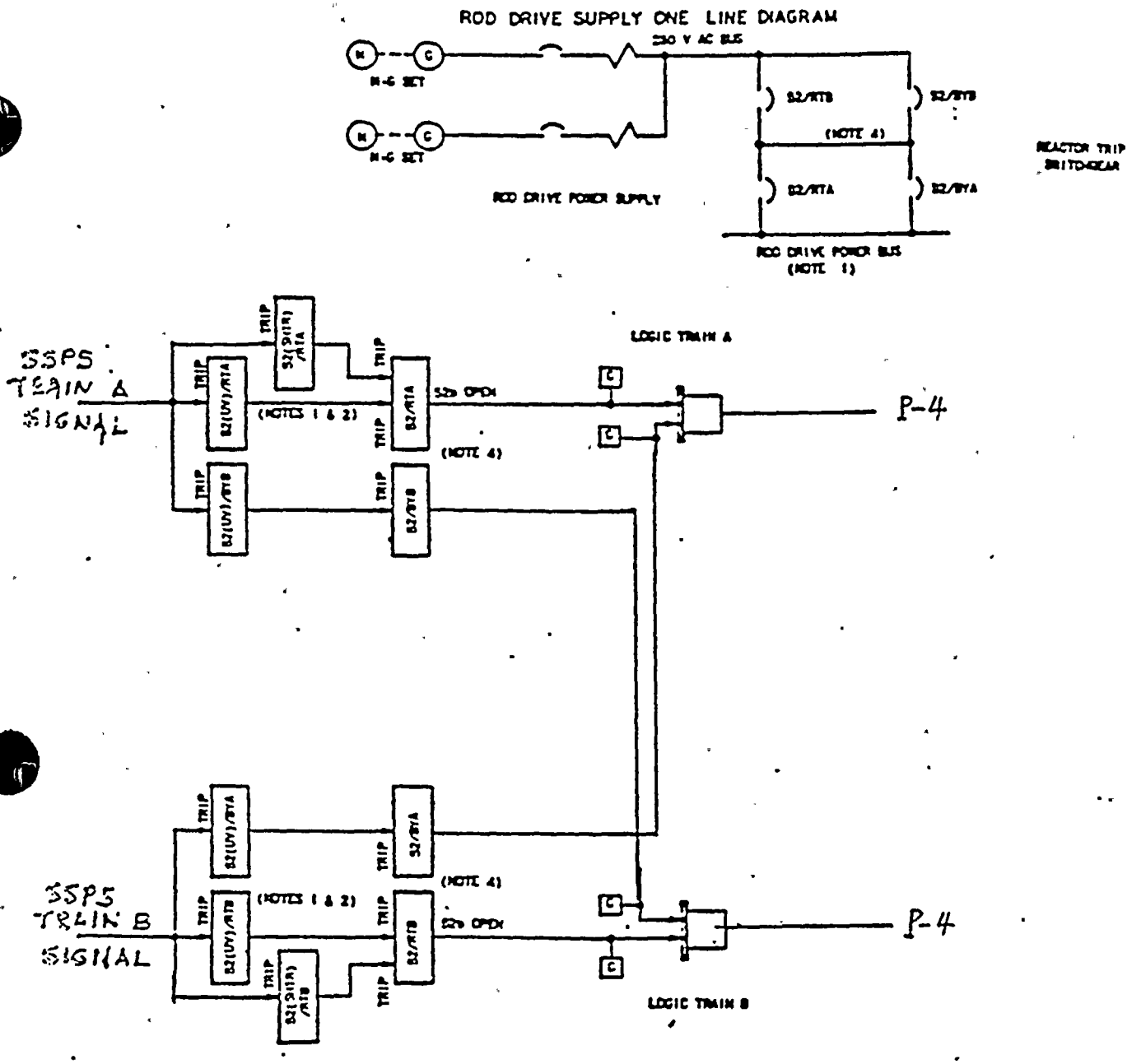
As a representative result, we give here the trip signal unavailability prompted by pressurizer low pressure (2/4) parameter signal - RPS trip failure: 2.9-5/d (w/o CCF) and 1.2-4/d (w/CCF). These values were obtained without considering diversity of parameter signals. With diversity, RPS trip failure became 1.44-5/d.

BNL provided an independent analysis of the unavailability of the RPS in References 6 and 7 (BNL2 results). BNL utilized a time-dependent (Markovian) model. The model thoroughly analyzed the dynamic behavior of the RPS. It also considered the common mode failures of all the main components of the full system (including the analog channels and logic units). The surveillance and maintenance data are identical to those listed in Table 4.1 for the WOG2/BNL2 calculations - RPS trip failure (BNL2-Markov) = 2.9-5/d.

4.3.3. Comparison of the RPS Unavailabilities

In order to compare the DCPRA results with those obtained in the WOG/BNL calculations, a representative DCPRA system unavailability value is reproduced here. This was obtained under boundary condition 1 (i.e., when two SSPS signals are received and all power is available). The total failure of the RPS to initiate reactor trip was calculated in the DCPRA to be : 9.32-6/demand. And, except for the operator-initiated trip given SSPS failure, the other boundary conditions resulted in only slightly increased values.

The results obtained in the DCPRA seem to be somewhat lower than those obtained in the WOG2/BNL2 calculations. Since in the DCPRA calculations the analog channel/logic unavailabilities are not explicitly included (only through the boundary conditions) the obtained conditional unavailability values can be taken as reasonable. Therefore, we do not, at this time, intend to alter the DCPRA split fractions pertaining to the RPS in any BNL requantification.



NOTES:

1. TRIPPING THE REACTOR TRIP BREAKERS 52/RTA AND 52/RTB REDUNDANTLY DE-ENERGIZES THE ROD DRIVES. ALL FULL LENGTH CONTROL RODS AND SHUTDOWN RODS ARE THEREBY RELEASED FOR GRAVITY INSERTION INTO THE REACTOR CORE.
2. NORMAL REACTOR OPERATION IS TO BE WITH REACTOR TRIP BREAKERS 52/RTA AND 52/RTB IN SERVICE AND BY-PASS BREAKERS 52/BYA AND 52/BYB WITHDRAWN.
   DURING TEST, ONE BY-PASS BREAKER IS TO BE PUT IN SERVICE AND THEN THE RESPECTIVE REACTOR TRIP BREAKER IS OPERATED USING A SIMULATED REACTOR TRIP SIGNAL IN THE TRAIN LOGIC TEST. THE REACTOR WILL NOT BE TRIPPED BY THE SIMULATED SIGNAL SINCE THE BY-PASS BREAKER IS CONTROLLED FROM THE OTHER TRAIN. ONLY ONE REACTOR TRIP BREAKER IS TO BE TESTED AT A TIME.
3. ALL CIRCUITS ON THIS SHEET ARE NOT REDUNDANT BECAUSE BOTH TRAINS ARE SHOWN.
4. OPEN/CLOSED INDICATION FOR EACH TRIP BREAKER AND EACH BYPASS BREAKER IN CONTROL ROOM.

Figure 4.1 Schematic of Reactor Protection System in DCPRA.

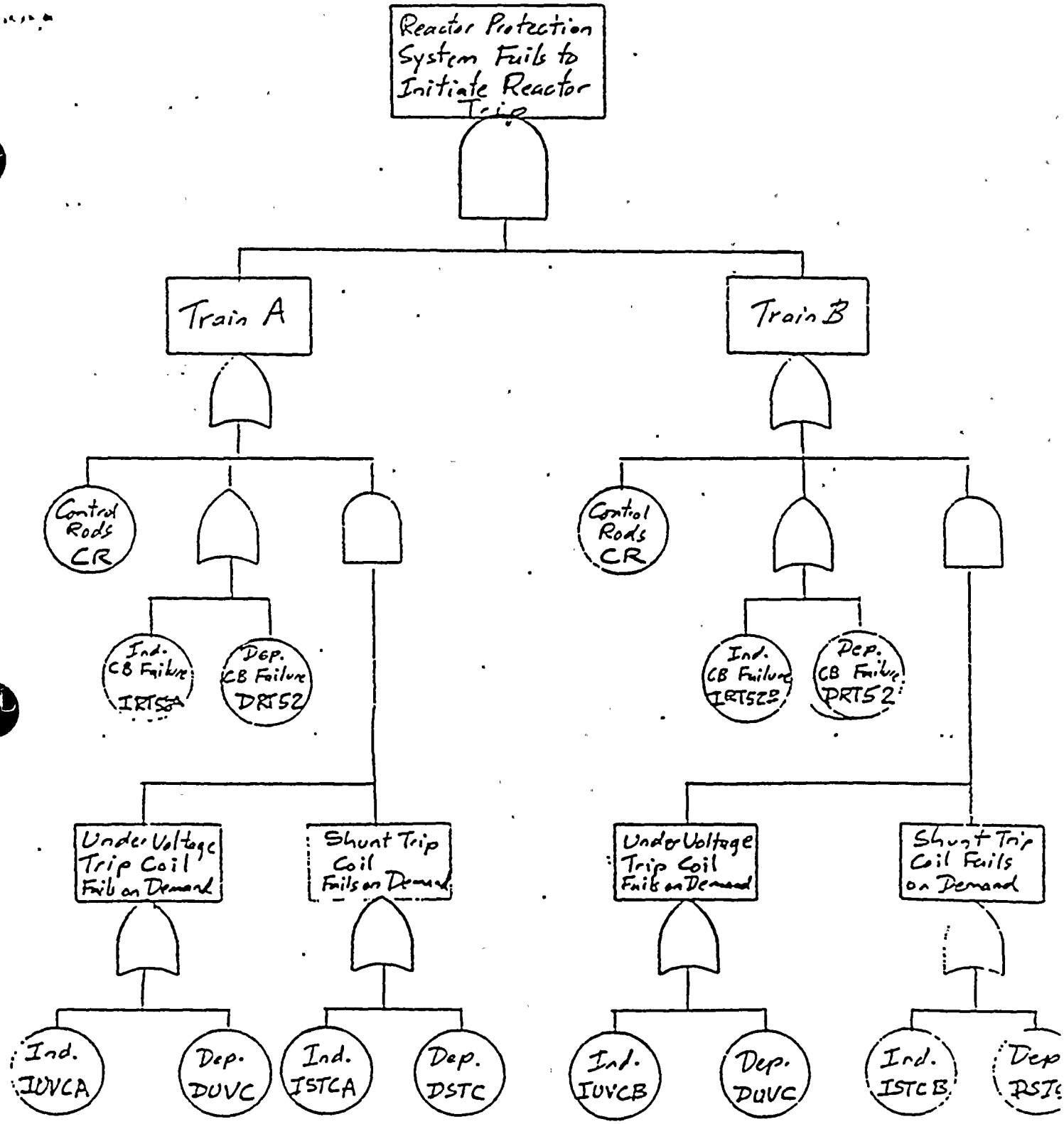


Figure 4.2 RPS fault tree with common cause identified in DCPRA.

Table 4.1
RPS Surveillance Modelling

Component	Modelled in DCPRA (Designator)	Modelled by WOG2/BNL2
Logic for Breaker Actuation:		
Test interval (month)	2 (TS2F)	2
Test time (hour)	2 (2HDSS2)	2
Maintenance interval (month)	Unscheduled*	12
Maintenance time (hours)	Plant-specific**	6
Breakers:		
Test interval (month)	1	2
Test time (hour)	2	2
Maintenance interval (month)	6	12
Maintenance time (hour)	1	6
Analog (Sensor) Channels:		
Test interval (month)	***	1
Test time (hour)	---	2
Maintenance interval (month)	---	12
Maintenance time (hour)	---	1

*2TPS1R (Power Supply Failure Rate) = 1.71-5/hr.
**2MGNFB (Time to Repair Failed Power Supply) = Not yet given by PLG.
***Modelled in the SSPS analysis.

5. REFERENCES

1. Letter of R. Fitzpatrick to N. Chokshi; BNL's proposed approach to the review of the Diablo Canyon PRA; September 1988.
2. El-Bassioni et al., PRA Review Manual, NUREG/CR-3485, September 1985.
3. WOG1; Andre, G., Howard, R., Jensen, R., and Leonelli, K., "Evaluation of Surveillance Frequencies and Out-of-Service Times for the Engineered Safety Features Actuation System," WCAP-10271 Supplement 2, February 1986 and WCAP-10271 Supplement 1, Revision 1, March 1987.
4. WOG2; Jansen, R., Lijewski, L., Masarik, R., "Evaluation of Surveillance Frequencies and Out-of-Service Times for the Reactor Protection Instrumentation System," WCAP-10271-P-A, May 1986.
5. BNL1; Bozoki, G., Aliefendioglu, K., Fitzpatrick, R., Yoon, W., "A Review of the Westinghouse Owner's Group Technical Specification Relaxation Analysis for the Engineered Features Actuation System, Draft Report for NRC, April 1988.
6. BNL2; Papazoglou, I. and Cho, N., "Evaluation of Surveillance Frequencies and Out-of-Service Times for the Reactor Protection System (WCAP-10271)," Letter Report to NRC, July 13, 1983.
7. BNL2; Papazoglou, I. and Cho, N., "Probabilistic Evaluation of Surveillance and Out-of-Service Times for the Reactor Protection Instrumentation System, Draft Report, April 1984.