

NUREG/CR-2515

SAND81-7229/II

AN

Printed December 1981

CONTRACTOR REPORT

Crystal River-3 Safety Study Volume II – Appendices

A. A. Garcia, Principal Investigator
R. T. Liner, P. J. Amico, E. V. Lofgren
Science Applications, Inc.
7315 Wisconsin Ave, Suite 1200 W
Bethesda, MD 20814

Prepared for
U. S. NUCLEAR REGULATORY COMMISSION

8204010534 820331
PDR ADOCK 05000302
P PDR

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-2515/II of II
SAND81-7229/II of II

CRYSTAL RIVER-3 SAFETY STUDY

VOLUME II

APPENDICES

1 December 1981

Prepared by:

Science Applications, Inc.
7315 Wisconsin Avenue, Suite 1200W
Bethesda, Maryland 20814

Principal Investigator:

A. A. Garcia

Principal Authors:

R. T. Liner
P. J. Amico
E. V. Lofgren

Funded by
Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
Under Memorandum of Understanding DOE 40-550-75
NRC FIN No. A1241 (Sandia)
A6296 (EG&G)

TABLE OF CONTENTS

	<u>Page</u>
<u>VOLUME I - MAIN REPORT</u>	
Foreword	I-i
Acknowledgements	I-ii
Table of Contents	I-iii
List of Figures	I-vi
List of Tables	I-viii
Glossary	I-x
1.0 INTRODUCTION	1-1
2.0 SUMMARY OF RESULTS	2-1
2.1 Frequency of Radioactivity Releases	2-1
2.2 Dominant Sequences	2-3
2.3 Functional and System Dependencies	2-16
2.4 Limitations of the Analysis	2-21
3.0 GENERAL PLANT DESCRIPTION	3-1
3.1 Reactor Coolant System (RCS)	3-6
3.2 Reactor Protection System (RPS)	3-6
3.3 Engineered Safeguards Actuation System (ESAS)	3-7
3.4 Engineered Safeguards Systems	3-7
3.4.1 Emergency Core Cooling System (ECCS)	3-8
3.4.2 Reactor Building Cooling and Spray Systems	3-11
3.5 Emergency Feedwater System (EFS)	3-12
3.6 Emergency Auxiliary Systems	3-12
3.6.1 Electric Power	3-13
3.6.2 Emergency Cooling Systems	3-13
3.7 Connections Between CR-3 and Coal-Fired Units 1 and 2	3-15

TABLE OF CONTENTS

	<u>Page</u>
4.0 EVENT TREES	4-1
4.1 Initiating Events	4-1
4.1.1 Transient Initiators	4-2
4.1.2 LOCA Initiators	4-3
4.2 Transient Event Tree	4-4
4.3 LOCA Event Tree	4-13
4.4 Special Events	4-19
4.4.1 Interfacing Systems LOCA (Event V)	4-19
4.4.2 Vessel Rupture	4-21
4.4.3 Steam Generator Tube Rupture	4-24
4.5 Containment Failure Modes	4-24
4.6 Radioactive Release Categories	4-27
5.0 FAULT AND EVENT TREE QUANTIFICATION PROCEDURES	5-1
5.1 Analytical Methods for Estimating Primary Event Probabilities	5-1
5.1.1 Fault Tree Development	5-1
5.1.2 Quantification Data Base	5-4
5.1.3 Evaluation of Hardware Faults	5-11
5.1.4 Evaluation of Human Faults	5-11
5.1.5 Evaluation of Common-Cause Faults	5-12
5.1.6 Evaluation of Test and Maintenance Outages	5-13
5.1.7 Evaluation of Interfacing System Faults	5-14
5.1.8 Evaluation of System Unreliability During Recirculation	5-15
5.2 Fault Tree Organization and Structure	5-17
5.2.1 A Fault Tree Hierarchy	5-18
5.2.2 System and Subsystem-Level Faults	5-20
5.2.3 Functional Level Faults	5-27
5.2.4 Fault Tree Quantification Tables	5-29

TABLE OF CONTENTS

	<u>Page</u>
5.3 Sequence Analysis	5-34
5.3.1 Boolean Reduction of Event Tree Sequences	5-34
5.3.2 Initiating Event Frequencies	5-37
5.3.3 Probabilities for Special Events in the Transient Event Tree	5-38
5.3.4 Analysis of ATWS Sequence	5-40
5.3.5 Containment Failure Probabilities	5-46
5.3.6 Accident Sequence Analysis Results	5-48
5.4 Analysis of Selected Operator Faults	5-66

VOLUME II - APPENDICES

Table of Contents	II-i
Glossary	II-iv
Introduction	II-1
Appendix A - Reactor Protection System (RPS)	A-1
Appendix B - Engineered Safeguards Actuation System (ESAS)	B-1
Appendix C - DC Power System	C-1
Appendix D - Class I.E. AC Power System	D-1
Appendix E - Nuclear Services Closed Cycle Cooling System (NSCCCS)	E-1
Appendix F - Decay Heat Closed Cycle Cooling System (DHCCCS)	F-1
Appendix G - High Pressure Injection and Recirculation System	G-1
Appendix H - Core Flood System (CFS)	H-1
Appendix K - Low Pressure Injection and Recirculation System	K-1
Appendix L - Reactor Building Emergency Cooling System (RBECS)	L-1
Appendix M - Reactor Building Spray System (RBSS)	M-1
Appendix N - Reactor Building Isolation System (RBIS)	N-1
Appendix P - Emergency Feedwater System (EFS)	P-1

GLOSSARY OF ABBREVIATIONS

A/E	Architect Engineer
ATWS	Anticipated Transient Without Scram
BWST	Borated Water Storage Tank
CRA	Control Rod Assembly
CFT	Core Flood Tanks
CR-3	Crystal River Unit 3
CRDM	Control Rod Drive Mechanism
DHCCCS	Decay Heat Closed Cycle Cooling System
DHCWS	Decay Heat Services Cooling Water System
DHSWS	Decay Heat Sea Water System
ECCS	Emergency Core Cooling System
ECF	Emergency Cooling Functionability
ECI	Emergency Coolant Injection
ECR	Emergency Coolant Recirculation
EFS	Emergency Feedwater System
EPRI	Electric Power Research Institute
ESAS (ESFAS)	Engineered Safeguards Actuation System
FSAR	Final Safety Analysis Report
HE	Heat Exchanger
HP, HPI, HPR	High Pressure (Injection) (Recirculation)
ICS	Integrated Control System
LOCA	Loss of Coolant Accident
LOSP	Loss of Offsite Power
LP, LPI, LPR	Low Pressure (Injection) (Recirculation)

GLOSSARY OF ABBREVIATIONS (CONT.)

MFW	Main Feedwater
MOV	Motor Operated Valve
NC, N.C.	Normally Closed
NO, N.O.	Normally Open
NPSH	Net Positive Suction Head
NRC	Nuclear Regulatory Commission
NSCWS	Nuclear Service Cooling Water System
NSCCCS	Nuclear Services Closed Cycle Cooling System
NSSS	Nuclear Steam Supply System
NSSWS	Nuclear Services Sea Water System
OTSG	Once Through Steam Generator
PAHR	Post Accident Heat Removal
PARR	Post Accident Radioactivity Removal
PCS	Power Conversion System
PORV	Power Operated Relief Valve
RB(E)CS	Reactor Building (Emergency) Cooling System
RBIC	Reactor Building Isolation and Cooling
RBIS	Reactor Building Isolation System
RBSS, RBSI, RBSR	Reactor Building Spray System (Injection) (Recirculation)
RCS	Reactor Coolant System
RPS	Reactor Protection System
RSS	Reactor Safety Study (WASH-1400)
RSSMAP	Reactor Safety Study Methodology Applications Program
S/RV	Safety/Relief Valve


APPENDICES: SYSTEM DESCRIPTION AND FAULT TREE ANALYSES

INTRODUCTION

This Volume consists of a collection of Appendices of system descriptions and fault tree analyses, including the unavailability quantifications for all systems designed to mitigate accident consequences and the auxiliary systems which support the "front-line" systems. The various systems are individually presented in Appendices A through P, which immediately follow the generic descriptive material below.

This introductory material and discussion is provided to assist the reader in understanding the overall structure of the CR-3 Safety Study and the organization and format of the individual Appendices. It is also intended to explain what kind of information and results the reader can expect to find in these Appendices.

The flow chart presented in Figure II.1 shows the main steps involved in the risk assessment of CR-3. It also shows the structure of the fault tree analysis contained in a typical Appendix¹. The following discussion is a step-by-step account of the quantification process for the fault tree analysis of each system. The steps are keyed to the numbers shown in diamonds in Figure II.1.

- STEP  The starting point was the collection, review and study of plant information to gain a thorough understanding of the system designs and capabilities, and interactions between systems.

¹In the following discussion, a typical Appendix is generally referred to as Appendix X.

The main sources of information were²:

- Plant Design Information - CR-3 FSAR (II-1)³ System Drawings (e.g., P&IDs, One Line Diagrams, Elementaries), FPC System Descriptions, etc.
- Technical Specifications (II-2)
- Plant Visit - gain familiarity with the equipment layout (possibly common mode failures due to common location); extensive discussions with plant personnel about plant operation, test and maintenance practices, operating experience, etc.
- Plant Procedures - Examples of procedures used are: Operating-, Maintenance-, Surveillance-, Emergency-Procedures, etc. These procedures (1) provide insight into the general plant operation and (2) support the operators during abnormal occurrences (especially the Emergency-Procedures). The procedures are also important to the quantification effort because they describe what is done to the various plant systems and how it is done.
- Expert Opinion and Experience - Collect information on plant and systems behavior, containment failure modes, etc., from experts available at FPC, B&W, NRC, and National Laboratories.

Section X.1, the first section of each appendix, summarizes the information collected during Step $\diamond 1$. The intent of this section is to convey to the reader all information necessary to follow the system's fault tree quantification.

STEP $\diamond 2$ With the information gathered in Step $\diamond 1$ the construction of the event trees, based on the system functions required for accident mitigation, can begin.

STEP $\diamond 3$ The success requirements for each event tree heading (or function) are determined in this step. Where possible, the requirements are defined in terms of systems.

²Not shown in the chart are the many iterations and exchanges among the various sources and other project personnel throughout the duration of this project.

³Numbers shown in parentheses in the text, e.g., (II-1) indicate references.

- STEP \diamond 4 At this point, all the systems, including the supporting systems, contributing to the mitigation of an accident are shown. Special studies, performed in parallel with the steps described thus far may allow exclusion of certain systems from detailed fault tree analysis. These special studies and their conclusions are discussed in Volume I.
- STEP \diamond 5 Detailed fault trees for all the systems selected in Step \diamond 4 are constructed. The definition of the top event for each tree is based on the success requirements developed in Step \diamond 3. The detailed fault trees are developed for each system to a level of detail sufficient to identify possible common mode or common cause failures.
- STEP \diamond 6 Simplified fault trees are developed from the detailed trees of Step \diamond 5. The basic fault elimination criteria for the simplification process results in simplified trees containing only single active and passive faults, double active faults, test and maintenance outages, and common mode failures. The simplification process eliminates other faults, including those whose contributions to the top event is negligible (on the basis of relative probability values) compared to other contributors. Thus the detailed trees are "pruned" to simplified trees which contain only the dominant cutsets, i.e., failure combinations, leading to the occurrence of the top event.

The simplified fault trees are presented in Section X.2 of each appendix, together with the top event definition and any assumptions made for the development of the detailed trees.

Sections X.1 and) complete the basic information necessary to proceed to the fault tree quantification process presented in Section X.3. The first subsection, X.3.1, discusses the system reliability characteristics. The results of the system quantification are summarized by highlighting the dominant contributor to the system's unavailability.

Each of the following steps discussed is presented in the Appendix either in table form or as a figure(s) in the logical sequence of development. Extensive use of notes, attached to the tables and figures as required, was made to explain and substantiate entries in the tables and figures.

Two distinct phases in a post accident environment exist: the injection phase and, in most cases, the recirculation phase. Sections X.3.2 and X.3.3 contain the quantification for the two post-accident phases. The steps in the quantification process, which are the same for both phases, are discussed below. The reason for the construction of modularized fault trees is discussed in Section 5.1 of Volume I.

- STEP $\diamond 7$ The appropriate event tree heading success requirements developed in Step $\diamond 3$, and presented in Volume I, Tables 4.4 and 4.6, formed the basis for the definition of the success requirements for the individual systems.
- STEP $\diamond 8$ The top events for the modularized fault trees are defined in this step. The selection of top events for systems and/or system trains is based on Step $\diamond 7$. Intermediate top events are frequently defined for (1) portions of system trains which are shared with other systems, and (2) for convenience of analysis.
- STEP $\diamond 9$ Construction of the modularized fault trees consists of grouping the faults which appear on the simplified fault tree, step $\diamond 6$, by type into modules, e.g., single hardware faults, system interfacing faults, etc. The construction of the modules is also governed by the requirements of the sensitivity analysis to be performed. Some modules have to be separated to accommodate events of different sensitivity types. The event sensitivity types are discussed in Step $\diamond 11$.




STEP \diamond 10 The Boolean equations, representing the modularized fault trees, are developed in this step. The equations are Boolean reduced by hand whenever practicable; otherwise a Boolean reduction computer code, such as WAMCUT (II-3), is used. All crossterms prohibited by Technical Specifications are eliminated from the reduced equation since the crossterms represent simultaneous outage of both trains of a redundant two train system due to test, maintenance, or any combination thereof. (It is assumed that the plant does not intentionally violate applicable Technical Specifications.) The Boolean equations are input to the event tree sequence analysis.

STEP \diamond 11 This step represents the quantification of each module appearing on the modularized fault tree. The WASH-1400 data base (II-4) is used in general; in a few instances other data sources are used as indicated in the notes to the quantification tables.

The calculation of maintenance and test outages is discussed in Section 5.1 of Volume I and is, in several cases, contained in the notes. Otherwise, standard methods such as those shown in WASH-1400 (II-4), and IEEE Standard 352 (II-5), for example, were used to calculate unavailabilities.

A "D" in the "failure rate" column of the quantification tables means "demand", and "ε" means negligible contribution. The code for the abbreviations used for the sensitivity type (or subgroup) in the column labeled "SENS." is as follows:

- O - Operator Error (defined in Volume I, Section 5.1)
- H - Human Error (defined in Volume I, Section 5.1)
- B - Hardware Coupling (defined in Volume I, Section 5.1)
- M - Maintenance Outage
- S - Selected Components (e.g., components in severe environment)

The last table in Section X.3.2 or X.3.3 is the quantification summary and contains the event unavailability point estimates. Steps  through  are repeated for systems required to operate during the recirculation phase. Step  completes the input required to perform the event tree sequence analysis.

Appendices A and B do not follow exactly the step-by-step outline above. The simplified fault tree is used in a slightly modified form instead of a modularized fault tree for the quantification of the Reactor Protection System (RPS) in Appendix A, and the simplified fault trees are used for the quantification of the Engineered Safeguards Actuation System (ESAS) in Appendix B.

References

- II-1 Florida Power Corporation, "Crystal River Unit 3 Nuclear Generating Plant Final Safety Analysis Report," Docket 50-302, 1971 (as amended through March 26, 1976).
- II-2 Technical Specifications; Appendix A to the Operating License for Crystal River-Unit 3.
- II-3 R. C. Erdmann, F. L. Leverenz, H. Kirch and G. S. Lellouche, Electric Power Research Institute, "WAMCUT, A Computer Code for Fault Tree Evaluation," EPRI NP-803, 1978.
- II-4 U. S. Nuclear Regulatory Commission, "Reactor Safety Study- An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Appendix III, WASH-1400 (NUREG-75/014), October 1975.
- II-5 Institute of Electrical and Electronics Engineers, Inc., "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems," IEEE Std 353-1975, April 1975.

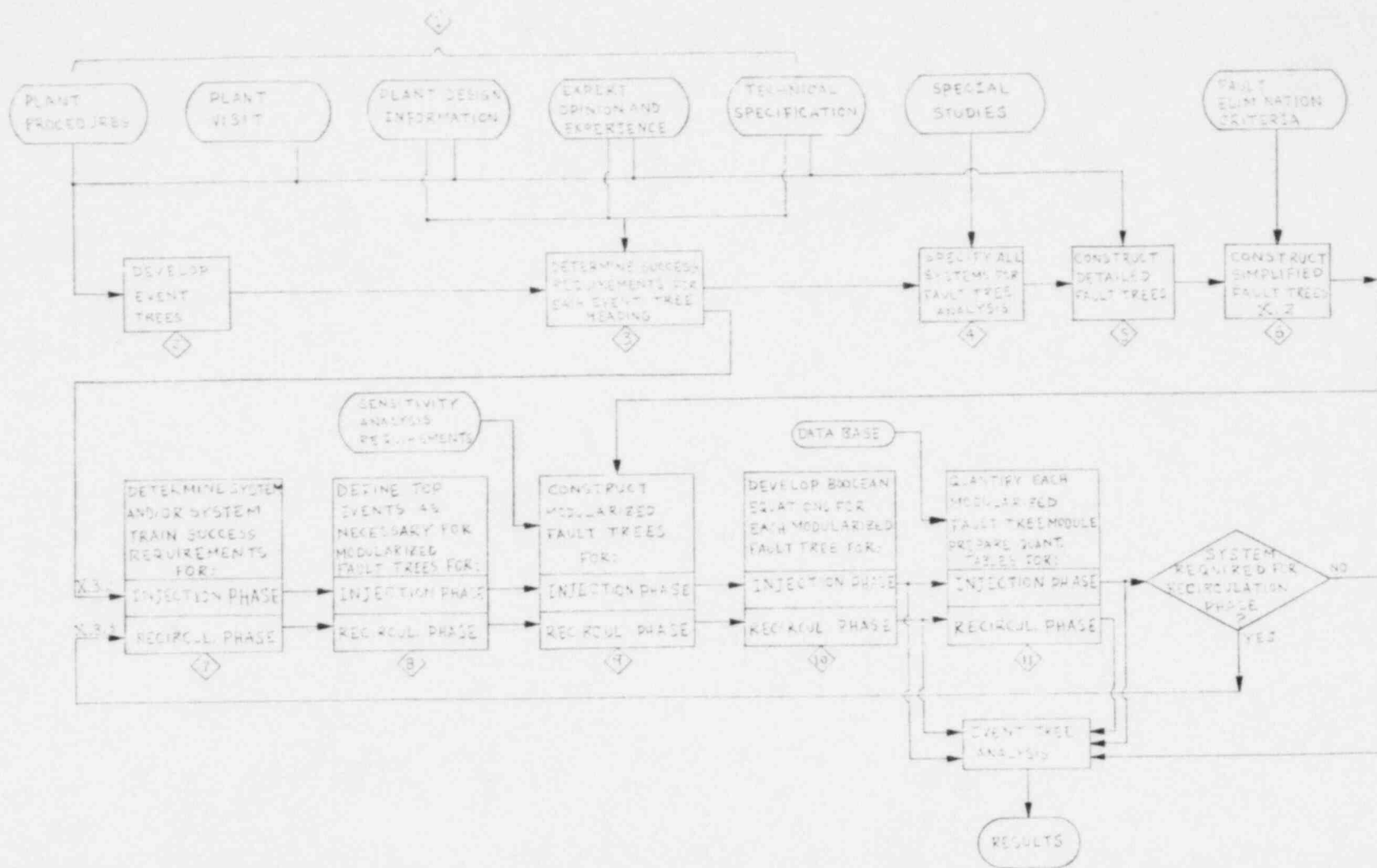


Figure II.1 Main Steps Involved in the Risk Assessment of Crystal River-3

APPENDICES

SYSTEM DESCRIPTIONS AND FAULT TREE ANALYSES

APPENDIX A

REACTOR PROTECTION SYSTEM (RPS)

APPENDIX A REACTOR PROTECTION SYSTEM (RPS)

A.1 SYSTEM DESCRIPTION AND OPERATION

The Reactor Protection System (RPS) monitors parameters related to reactor operation and trips the reactor by control rod insertion into the core to protect the core against fuel rod cladding damage. In addition, it protects against reactor coolant system damage from high system pressure through rod insertion, thereby limiting energy input to the system.

A.1.1 SYSTEM DESCRIPTION

The RPS consists of control rod assemblies (CRA), circuit breakers, instrumentation and electronic logic. The logic, in response to input signals from the instrumentation, shuts down the reactor by removing power from the control rod drive mechanism (CRDM) motors. The control rods then drop into the core under the influence of gravity. A schematic of the RPS is shown in Figure A.1.

There are a total of 69 CRA's, arranged in eight groups including four safety groups, three regulating groups and one axial power shaping group. The rod drive control system includes (1) five identical, dual channel DC supplies which power the regulating and axial power shaping groups and (2) two DC holding power supplies which power the safety groups. The DC supplies are fed from two 480VAC, 3 ϕ sources; i.e., a main bus and a secondary bus. Two primary breakers (A,B), two secondary breakers (C,D), and contactors (E,F) interrupt power to the CRA drive motors when a trip is commanded.

The trip logic includes four identical channels, each consisting of logic circuits and trip relays, which maintain the trip breakers and contactors energized under normal operating conditions. In response to input signals from sensors (See Table A.1), the channel logic deenergizes associated trip relays which in turn deenergize the trip breakers and contactors thereby removing power to the CRDM motors and causing the regulating and safety CRA's (61) to drop into the core. The axial power shaping rods do not drop into the core when their associated drive motors are deenergized.

CONTROL ROD ASSEMBLY

The CRA includes 16 control rods, mounted in a stainless-steel spider, and a control rod drive mechanism. The CRDM, which positions the CRA in the reactor core, is a non-rotating translating lead screw coupled to the CRA. The screw is driven by split roller nut assemblies which are rotated magnetically by a motor stator located outside the pressure boundary. For rapid insertion, power is removed from the drive motor causing the nut halves to separate and release the screw and CRA which then drop into the reactor core under the influence of gravity.

The CRAs are arranged into groups at the control rod drive control system patch panel. Typically twenty-eight CRAs are assigned to the regulating groups (Groups 5,6,7,8) while forty-one CRAs are assigned to the safety rod groups (groups 1,2,3,4). Group 8 includes eight axial power shaping rod assemblies which do not drop into the core when power is removed from their drive motors during a reactor trip.

The rod drive control system (RDC), which is shown in Figure A.2 consists of (1) drive motor DC power supplies, (2) system control logic, and (3) trip breakers and contactors. The DC power system includes four group power supplies. Identical power supplies are used for the regulating groups and the auxiliary power supply. The DC power supplies are fed from two 480VAC, 3 ϕ sources; i.e., a main bus and a secondary bus.

The system logic encompasses those functions which command control rod motion in the manual or automatic modes of operation, including CRD sequencing, safety and protection features, and the manual trip function. Major components of the logic system are the Operator's Control Panel, CRA position indication panels, automatic sequencer, and relay logic. Switches are provided at the operator's control panel for selection of the desired rod control mode. Control modes are: (1) Automatic mode -- where CRA motion is commanded by an integrated control system; and (2) Manual mode -- where CRA motion is commanded by the operator. Manual control permits operation of a single CRA or a group of CRAs. Alarm lamps on the RDC panel

alert the operator to the systems status at all times. The group 8 control rods can only be controlled manually, even when the remainder of the system is in automatic control. The sequence section of the logic system utilizes rod position signals to generate control interlocks which regulate group withdrawal and insertion. The sequencer operates in both automatic and manual modes of reactor control, and controls the regulating groups only. Analog position signals are generated by the read switch matrix on the CRA, and an average group position, generated by an averaging network. This average signal serves as an input to electronic trip units which are activated at approximately 25 and at 75 per cent of group withdrawal. Two bistable units are provided for each regulating group. Outputs of these bistables actuate "enable" relays which permit the groups to be commanded in automatic or manual mode. The automatic sequencer circuit can control only CRA groups 5,6 and 7. The safety CRA groups, groups 1-4, are controlled manually, one group at a time. In addition, the operator must select the safety group to be controlled and transfer it to the auxiliary power supply before control is possible. There is no way in which the automatic sequencer can affect the operations required to move the safety CRA. Automatic insertion of rods can only be commanded by the integrated control system when the control rod drive system is in the automatic mode.

Positioning of regulating CRAs is accomplished by silicon controlled rectifier switching via a motor driven multichannel photo-optic encoder. The safety CRAs are positioned via the auxiliary power supply and maintained in the desired position by the holding power supplies.

Trip breakers and contactors are provided for removing power to the CRDM motors. The AC power feed breakers are of the three-pole, stored-energy type and are equipped with instantaneous undervoltage trip coils. Each AC feed breaker is housed in a separate metal clad enclosure. The secondary trip breakers are also of the stored-energy type with two parallel-connected instantaneous undervoltage trip coils consisting of two 2-pole breakers mechanically ganged to interrupt DC busses. All breakers are motor-driven-

reset to provide remote reset capability. Each undervoltage trip coil is operated from the Reactor Protection System. The trip breakers are tested monthly.

TRIP LOGIC

The system shown in Figure A.1 consists of four identical channels, each terminating in a trip relay within a reactor trip module. The primary source of AC power for the RPS comes from four vital 120VAC buses, one for each protective channel. In the normal untripped state, each channel maintains the trip relay energized via the closed normally open (N/O) contacts of bistables associated with the various reactor sensors. Should any bistable become deenergized the trip relay deenergizes. Each trip relay has four N/O contacts, each controlling a logic relay in one reactor trip module. Therefore, each reactor trip module has four logic relays controlled by the four channels. The four logic relays combine to form a 2-out-of-4 coincidence network in each reactor trip module.

Manual trip may be accomplished from the control console by a trip switch. This trip is independent of the automatic trip system. Power from the control rod drive power breakers' undervoltage coils comes from the RT modules. The manual trip switches are between the reactor trip module output and the breaker undervoltage coils. Opening of the switches opens the lines to the breakers, tripping them. There is a separate switch in series with the output of each reactor trip module. All switches are actuated through a mechanical linkage from a single pushbutton.

Each channel is provided with two key-operated bypass switches, a channel bypass switch and a shutdown bypass switch. The channel bypass switch enables a channel to be bypassed without initiating a trip. Actuation of the switch initiates a visual alarm on the main console which remains in effect during any channel bypass. This switch is used to bypass one protective channel during on-line testing. Thus, during on-line testing the system will operate in 2-out-of-3 coincidences. An electric interlock circuit prevents placing two channels in bypass simultaneously. The use of the channel bypass key switch is under administrative control.

The shutdown bypass switch enables the power/imbalance/flow, power/RC pumps, low pressure, and pressure-temperature trips to be bypassed, allowing control rod drive tests to be performed after the reactor has been shutdown and depressurized below the low reactor coolant pressure trip point. Before the bypass may be initiated, a high pressure trip bistable - which is incorporated in the shutdown bypass circuitry - must be manually reset. The set point of the high pressure bistable (associated with shutdown bypass) is set below the low pressure trip point. If pressure is increased with the bypass initiated, the channel will trip when the high pressure bistable (associated with shutdown bypass) trips. The use of the shutdown bypass key switch is under administrative control.

Each of the four channels is physically separate and electrically isolated from the regulating instrumentation. The modules, logic, and analog equipment associated with a single protective channel are contained wholly within two Reactor Protection System cabinets. Within these cabinets, there is a meter for every analog signal employed by the protective channel, and a visual indication of the state of every logic element. At the top of one cabinet, and visible at all times, is a protective channel status panel. Lamps on this panel give a quick visual indication of the trip status of the particular protective channel and of the RT module associated with it. Additional lamps on the panel give visual indication of a channel bypass or a fan failure.

The RPS equipment is designed for continuous operation in a room environment of 40⁰F to 110⁰F and up to 75% relative humidity. All modules are designed for a 30⁰F temperature rise inside the equipment cabinets over the ambient room conditions. Two 100% capacity fans with filter banks and chilled water coils, two 100% capacity central station type chilled water systems, and two 50% capacity outside air booster fans are provided for environmental control of the equipment area.

A.1.2 SYSTEM OPERATION

The coincidence logic contained in the RPS channel A controls trip breaker A in the control rod drive system, channel B controls breaker B, channel C controls breaker C and contactor E, and channel D controls breaker D and contactor F. The control rod drive circuit breaker combinations that initiate reactor trip include (1) AB, (2) ADF, (3) BCE, and (4) CDEF. This is a 1-out-of-2 twice logic. When any 2-out-of-4 channels trip, all reactor trip modules trip (deenergize) all control rod drive breakers and contactors. The four RPS channels trip whenever the reactor conditions tabulated in Table A.1 exist.

The use of 2-out-of-4 logic between protective channels permits a channel to be tested on-line without initiating a reactor trip. Maintenance to the extent of removing and replacing any module within a protective channel may also be accomplished in the on-line state without a reactor trip. Each logic channel is tested monthly. The RPS sensors are checked during each shift and are tested monthly. To prevent either the on-line testing or maintenance features from creating a means for unintentionally negating protective action, a system of interlocks initiates a protective channel trip whenever a module is placed in the test mode or is removed from the system. However, provisions are made to bypass any one protective channel (i.e., supply an input signal which leaves the channel in a non-tripped condition) for testing or maintenance. The test scheme for the reactor protective system is based upon the use of comparative measurements between like variables in the four protective channels, and the substitution of digital and analog test signals as required, together with measurements of actual protective function trip points. The test signals are provided from built-in test circuits in the logic instrumentation system. A digital voltmeter (not cabinet-mounted) is used for making accurate measurements of trip point and analog signal voltages.

Plant annunciator windows provide the operator with immediate indications of changes in the status of the reactor protective system.

The following conditions are annunciated for each reactor protective system channel:

- a. channel trip
- b. fan failure in channel
- c. channel on test
- d. shutdown bypass initiated
- e. manual bypass initiated

Any time a test switch is in other than the operate position, annunciator "c" will be lit and the associated protection channel will be tripped. Under this condition, annunciator "a" will be lit unless annunciator "e" is lit (i.e., the channel is bypassed).

TEST AND MAINTENANCE

Each RPS channel, including the associated instrumentation, reactor trip module (RTM), and CRD breaker and contactor, is demonstrated operable by performance of functional tests once each month.

Functional testing of each of the four channels requires approximately four hours to complete and is performed on a weekly rotation by different test personnel.*

* Per discussion with plant personnel.

Following are several notes related to test and maintenance.

Notes on Reactor Trip Module

- Prior to start of functional testing of the instrumentation and RTM associated with the particular channel under test, the channel is placed in bypass via the "Manual Bypass" switch located in the RTM. This reduces the RPS trip logic to a 2-out-of-3 system.
- When RTM is placed in bypass via manual bypass switch, indication of this condition is provided in the control room (RPS Panel).
- Operator can leave channel in bypass state but indication on RPS panel should alert operator. Same applies to inadvertent bypass.
- An electric interlock circuit prevents placing two channels in bypass simultaneously.
- Only one channel is permitted to be bypassed at any given time under administrative control.

Notes on Control Rod Drive (CRD) Power Train

- Functional testing of the CRD power train consists of causing the CRD breaker to trip. A jumper is momentarily placed across the trip coil of the breaker. The power train is restored to operational status by locally resetting the breaker.
- A breaker can be racked out for maintenance without channel trip.

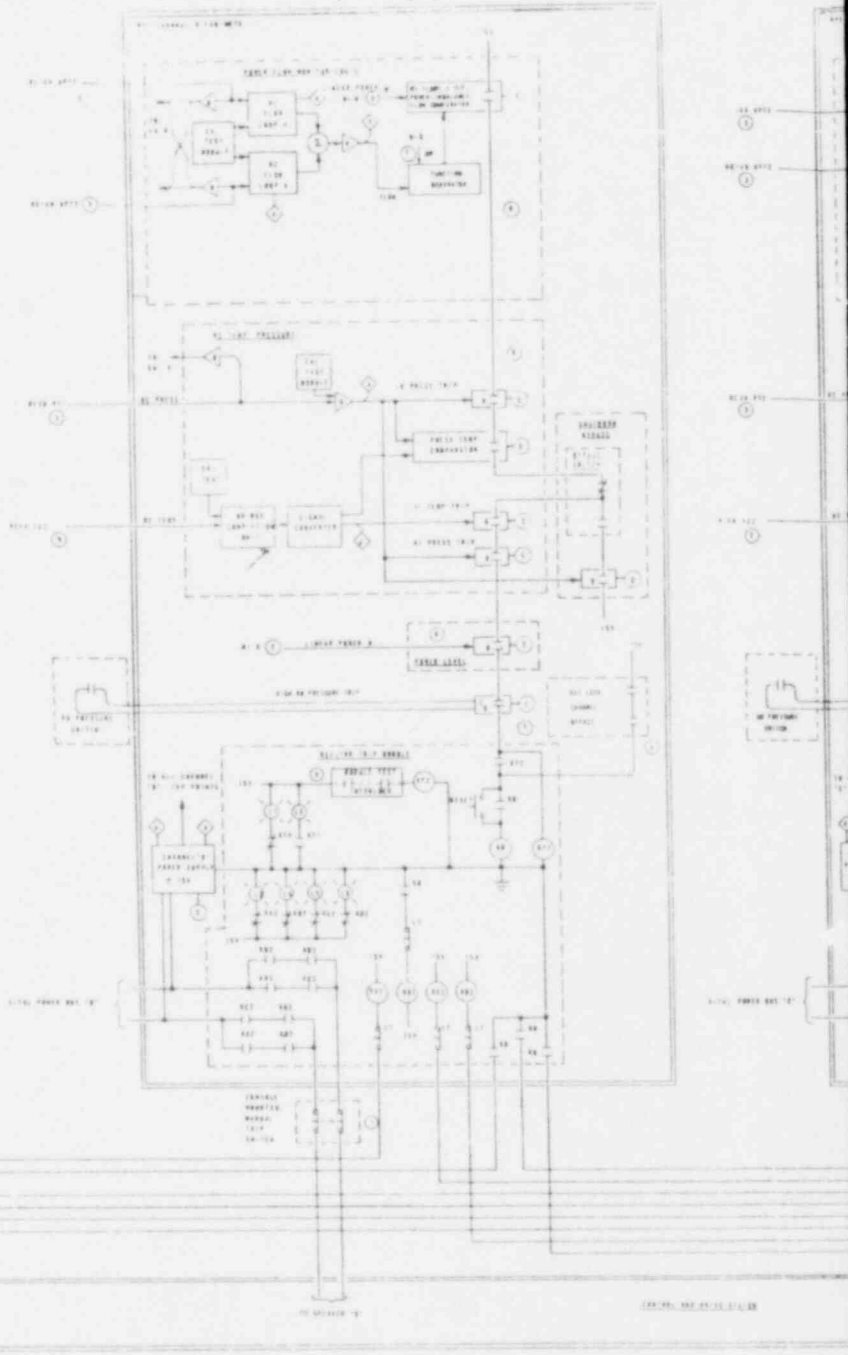
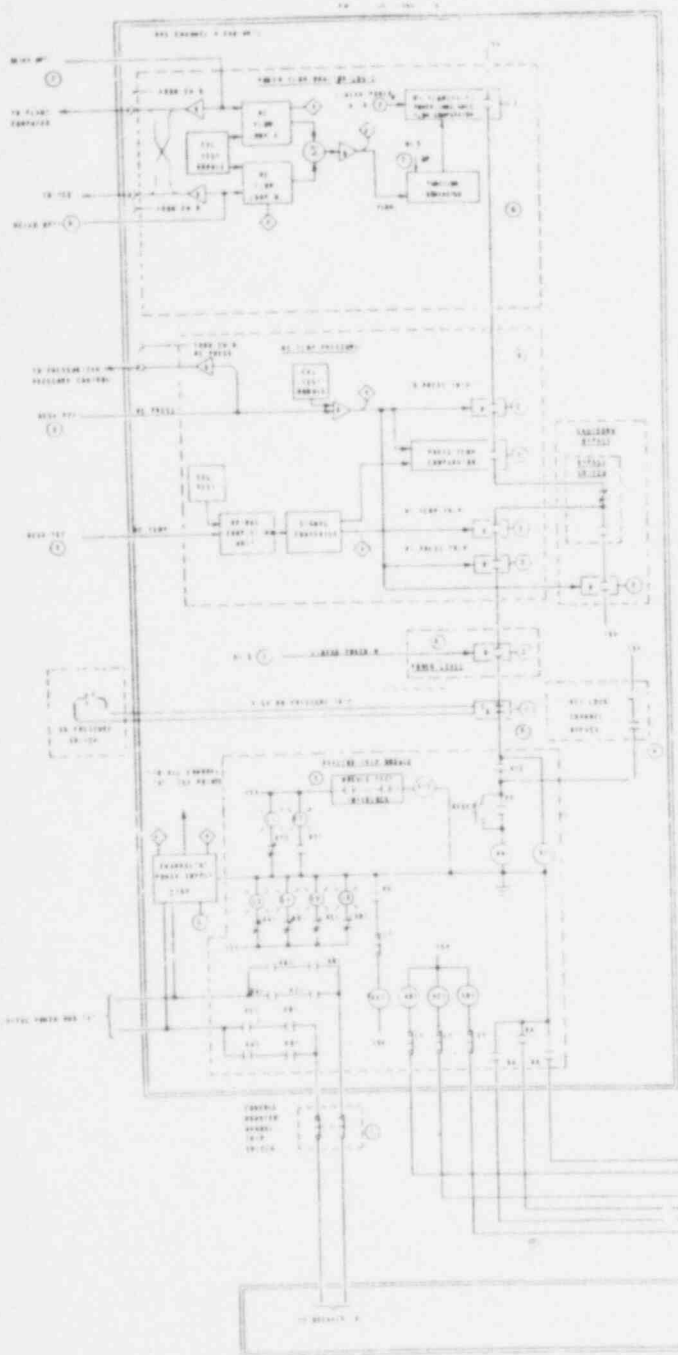
Notes on Instrumentation

- If a reactor sensor requires maintenance to correct for a defect, the work will be done during a shutdown.
- Work can be performed on the circuitry of the instrumentation signal processing electronics (such as the power supply, signal conditioners, etc.), but the associated channel will probably be bypassed.
- Calibration errors in the signal processing electronics can result in a circuit being unavailable to trip the reactor. (Calibration is performed on each channel on a weekly rotation basis, by different personnel.)

Table A.1 Reactor Trip Summary

<u>Trip Variable</u>	<u>No. of Sensors</u>	<u>Steady-State Normal Range</u>	<u>Trip Value or Condition for Trip</u>
Overpower	4 flux sensors	2-100%	$\geq 105.5\%$ of rated power
Nuclear overpower based on flow and imbalance	4 two-section flux sensors, 8 ΔP flow	NA	1.045 times flow minus reduction due to imbalance
Reactor outlet temperature	4 temperature sensors	532-604 F	$\geq 620F$
Pressure/temperature	4 pressure sensors, 4 temperature sensors	Variable	$(16.25T - 7838) \geq P^{(a)}$
Reactor coolant pressure	4 pressure sensors	2,090-2,220 psig	$\geq 2,355$ psig (high), $\leq 1,800$ psig (low)
Reactor building pressure	4 pressure switches	0 psig	4 psig

(a) T is in F and P is in psig.



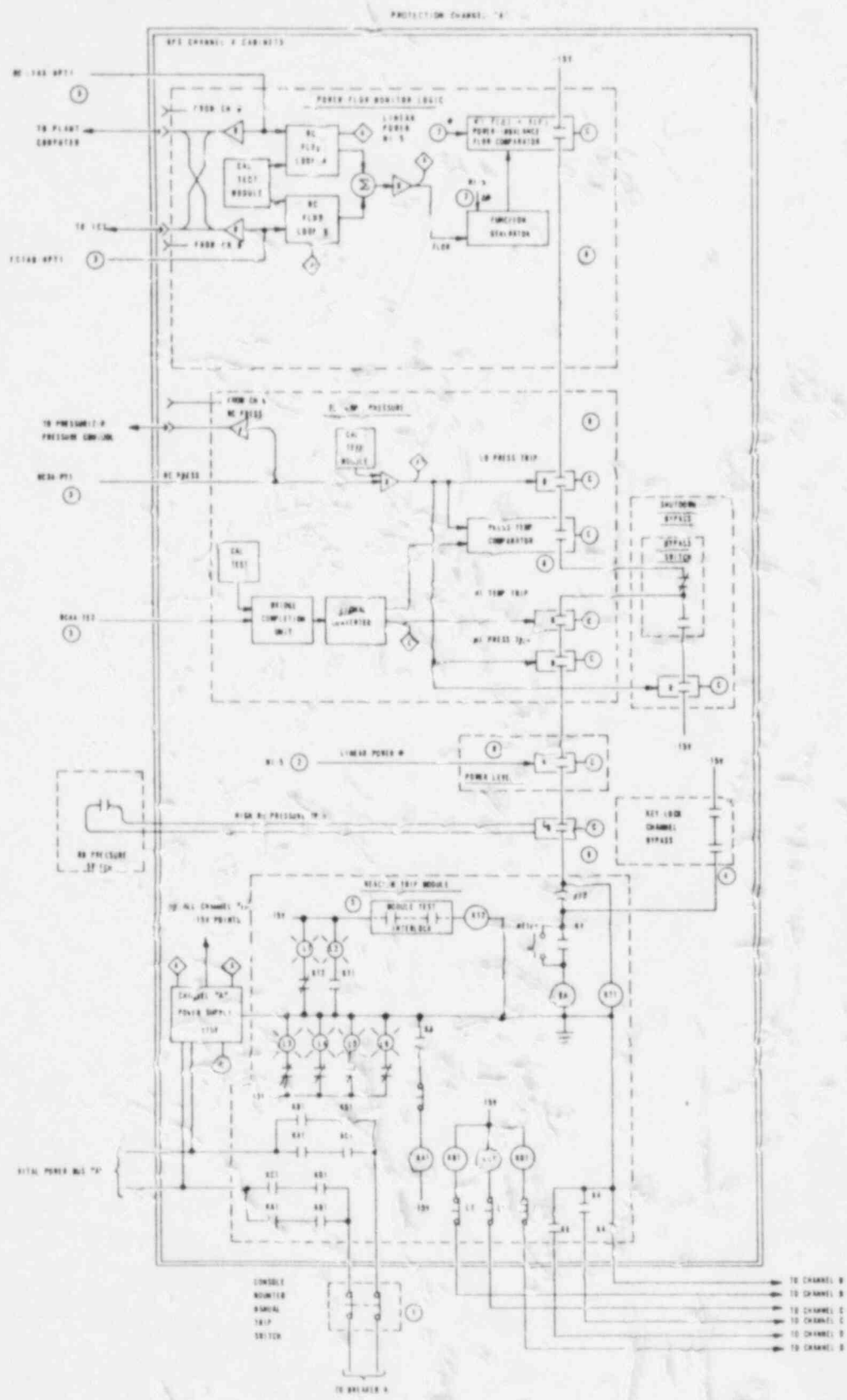
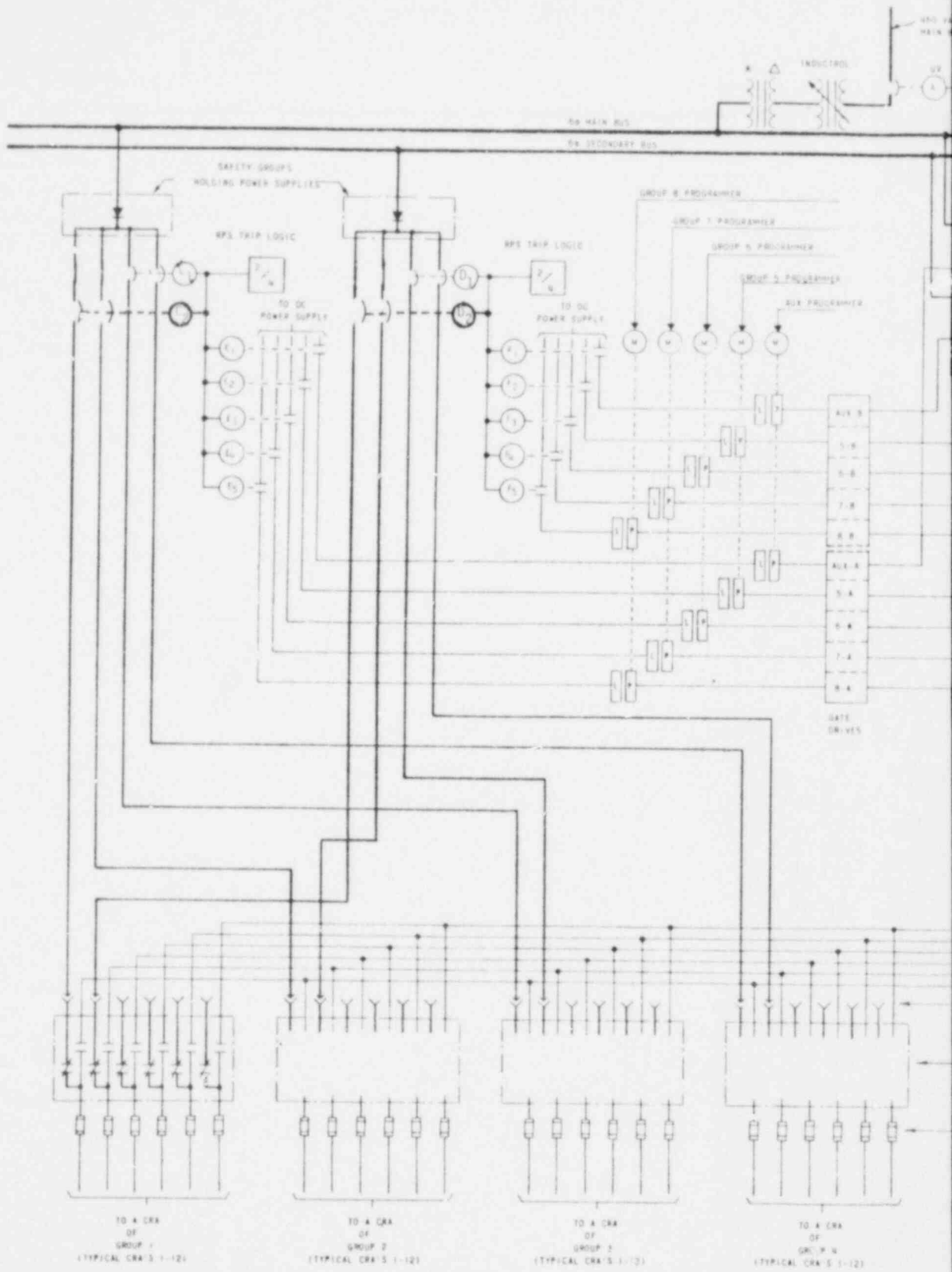


Figure A.1 (2/2) Reactor Protection System Schematic Diagram



1

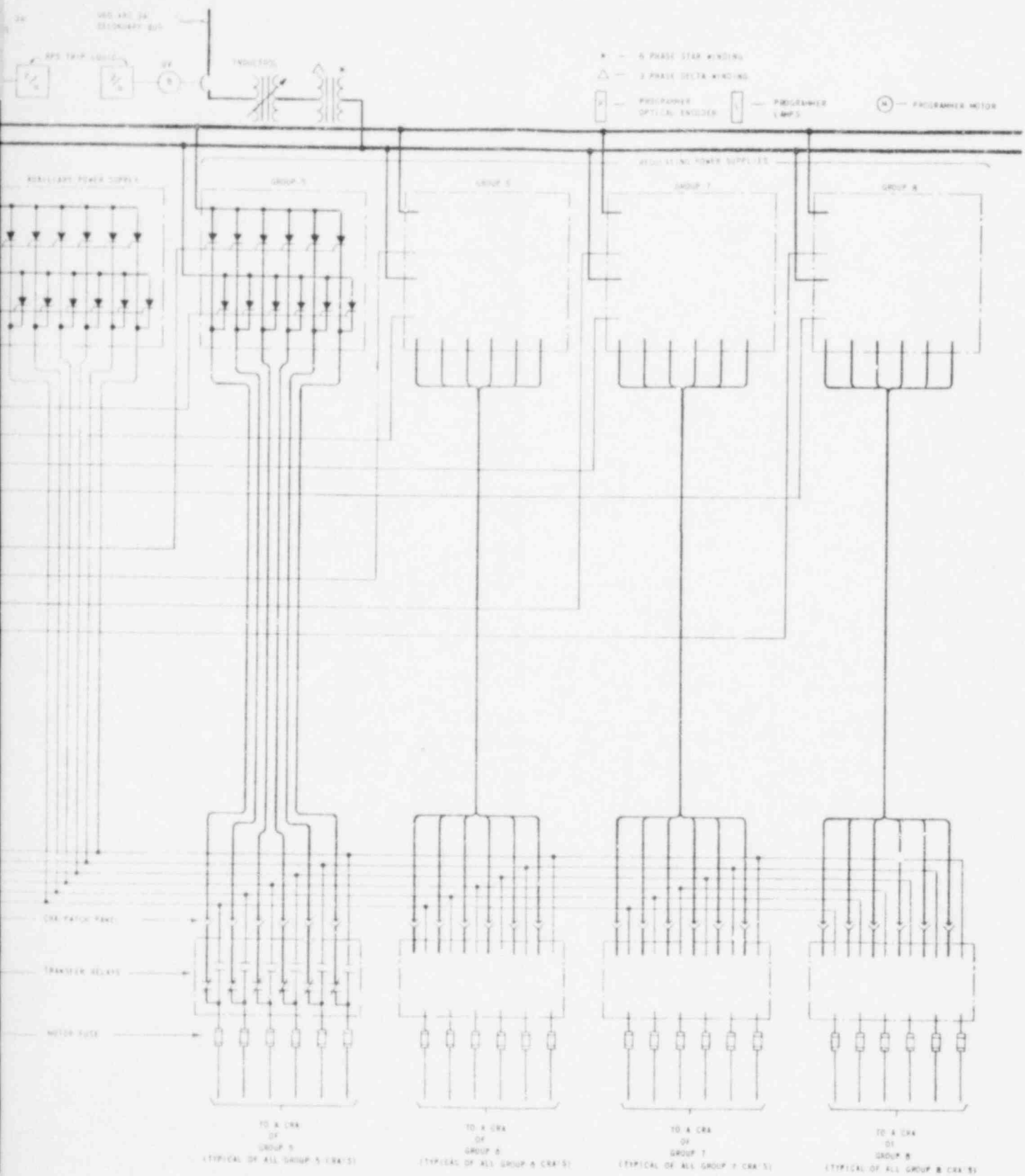


Figure A.2 Rod Drive Control System Schematic Diagram

A.2 SYSTEM SIMPLIFIED FAULT TREE

A detailed fault tree for the RPS was constructed, identifying the events which contribute to the failure to insert the control and safety rods into the core when required by reactor conditions.

Failure to automatically remove power to all of the safety and control rods constituted RPS failure. In addition, such faults as core disruption, which would inhibit rod insertion, or stuck rods were included as contributors to reactor trip failures.

The top event of the fault tree is defined as:

"FAILURE TO INSERT SIX OR MORE CONTROL ROD GROUPS"

The simplified fault tree is shown in Figure A.3.

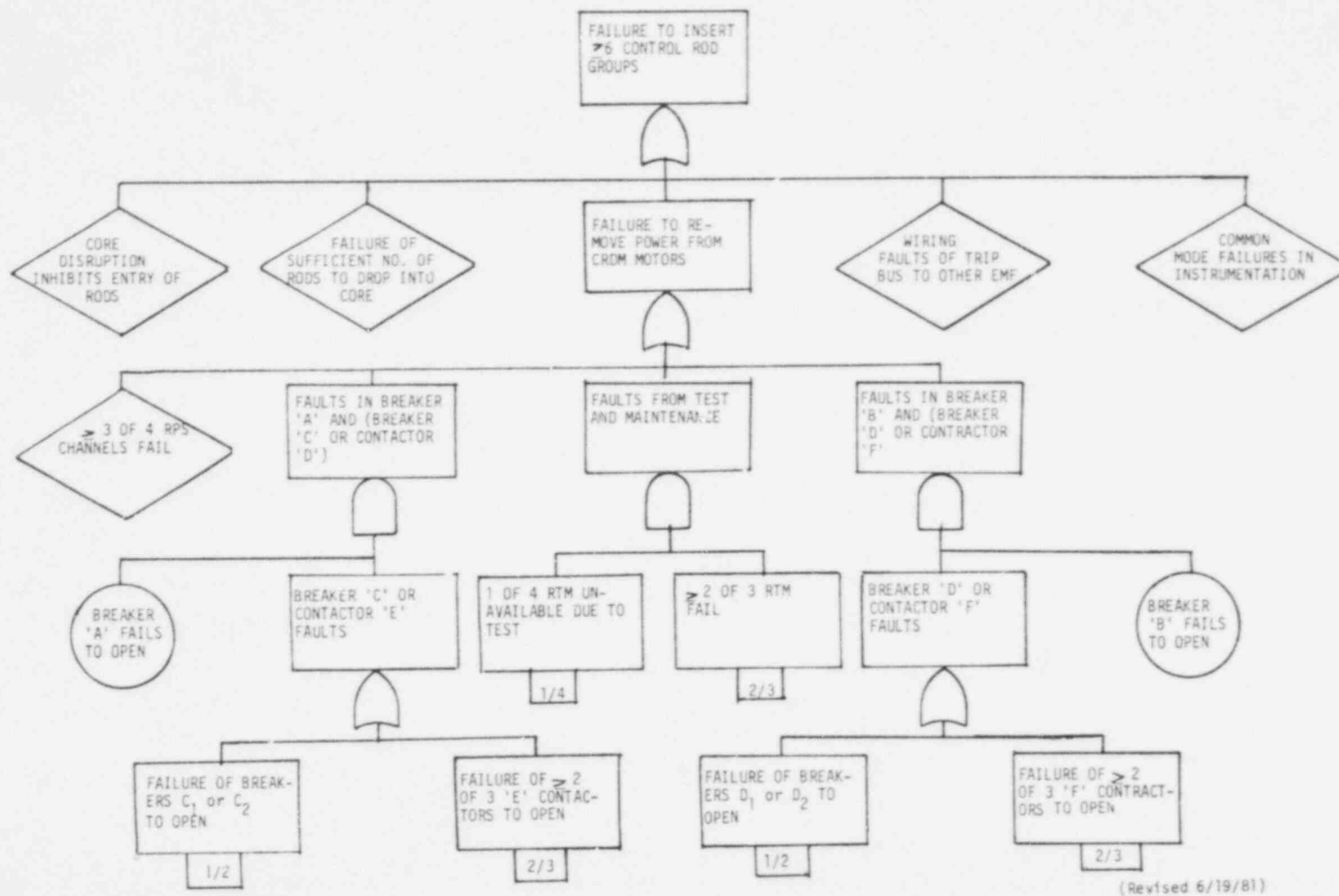


Figure A.3 Simplified Fault Tree - Reactor Protection System

A.3 SYSTEM QUANTIFICATION

A.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The RPS consists of eight groups of control rods, of which seven groups comprise the emergency safety system. Insertion of six of the seven emergency safety system groups is required for success. Thus, from the standpoint of failures that would fail individual groups, the system is configured in two-out-of-seven redundancy. Failures of this type were assessed to not contribute to RPS unavailability.

The dominant contribution to RPS unavailability was assessed to be due to test of the reactor trip modules (RTM). Faults in the CRD power train primary (AC) breakers and secondary (DC) breakers makeup approximately 35% of the total unavailability. All other contributors are negligible.

A.3.2 SYSTEM FAULT TREE QUANTIFICATION

The Reactor Protection System does not interact with any other system. The independence from any other system does not require a Boolean reduction in the event tree sequence analysis. Therefore, no modularized fault tree was constructed. The simplified fault tree in Figure A.3 was used in slightly modified form for quantification purposes. The modified tree is shown in Figure A.4.

Table A.2 shows the RPS success requirements. Table A.3 contains the top event definitions for the simplified fault tree. The unavailability of each gate is shown on the tree, Figure A.4. Table A.4 shows the Boolean equations that represent the fault tree. Table A.5 shows the quantification of each gate by component and failure mode. Table A.6 summarizes the point estimates and error factors for each gate.

Table A.2 Reactor Protection System

SUCCESS REQUIREMENTS

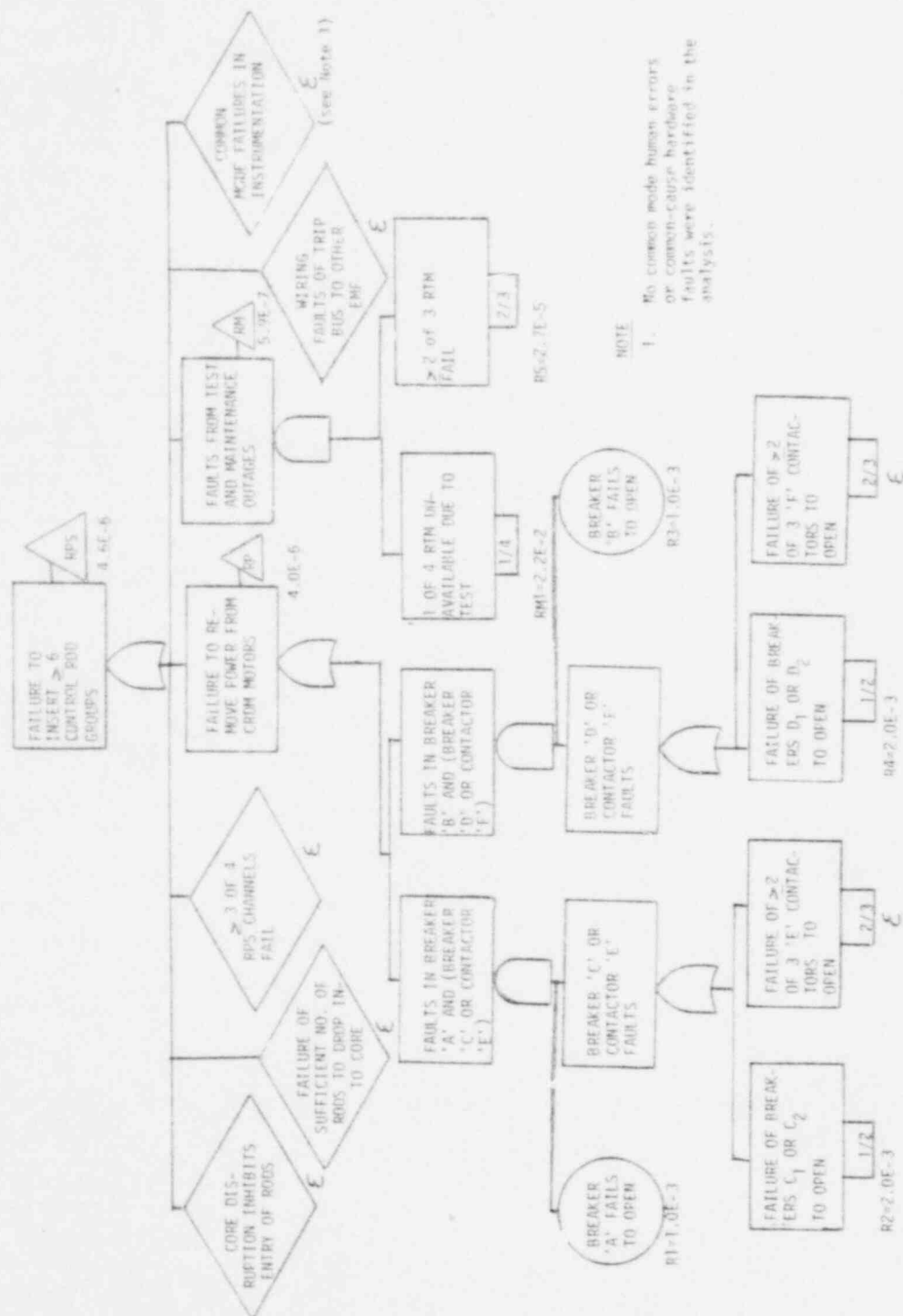
<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B ₄ , Transients	Failure to automatically or manually insert at least six control rod groups.	
B ₁ , B ₂ , B ₃	None	1

NOTES: 1 For B₁, B₂, B₃ LOCAs it is assumed that the effects of reactor coolant blowdown (removal of moderator) is sufficient to achieve reactor subcriticality. The reactor vessel will be refilled with borated water of sufficient boron concentration to keep the reactor subcritical.

Table A.3 Reactor Protection System

TOP EVENT DEFINITION

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
RPS	Failure to insert at least six control rod groups	
RP	Failure to remove power from CRDM motors	
RM	Faults from test and maintenance outages	



(Rev. 6/19/81)

Figure A.4 Simplified Fault Tree (Modified) - Event "RPS"

Table A.4 Reactor Protection System

BOOLEAN EQUATIONS BASED ON SIMPLIFIED FAULT TREE

<u>TOP EVENT</u>	<u>NOTES</u>
$RPS = RP + RM$	(1)
$RP = R1 \cdot R2 + R3 \cdot R4$	
$RM = RM1 \cdot R5$	

NOTES: 1. All basic events that are assessed to be negligible contributors (ϵ) were not included in the Boolean equation.

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
RP		FAILURE (HARDWARE) TO REMOVE POWER FROM CRDM MOTORS			4.0 E-6			
R1	BREAKER	FAILS TO OPEN	D		1.0 E-3	3 ⁺ ,3 ⁻		
R2	BREAKERS "C"	FAIL TO OPEN (1/2)	D		$\frac{2.0 E-3}{\Psi=2.0 E-6}$	3 ⁺ ,3 ⁻		
R3	BREAKER "B"	FAILS TO OPEN	D		1.0 E-3	3 ⁺ ,3 ⁻		
R4	BREAKERS "D"	FAIL TO OPEN (1/2)	D		$\frac{2.0 E-3}{\Psi=2.0 E-6}$ $\Sigma=4.0 E-6$	3 ⁺ ,3 ⁻		
RM		TEST AND MAINTENANCE RELATED FAULTS			5.9 E-7			
RM1	RTM	UNAVAILABLE DUE TO TEST (1/4)			2.2 E-2		1	
R5	RTM	≥ 2 OF 3 RTM FAIL (2/3)			$\frac{2.7 E-5}{\Psi=5.9 E-7}$	3 ⁺ ,3 ⁻	2	

Table A.5 Events "RP" and "RM" Quantification

Table A.5 Reactor Protection System

QUANTIFICATION TABLES

NOTES

- 1 Each of the four reactor trip modules (RTM) is assumed to be unavailable for an average of four hours per month due to test. The total test outage for the RTM channels is thus 16 hours and the total unavailability from these tests is $(16)/(720) = 2.2 \text{ E-2}$.
- 2 Failure of (2/3) RTMs was assessed to be 2.7 E-5 . The individual RTM failure probability was assessed at 3.0 E-3 rather than the more normal assessment of 1.0 E-2 due to the simplification of the calibration procedure which results from the built-in test and calibration circuits in the equipment. The multiple failures of the RTM were assumed to be independent due to staggered test and calibration, thus the total unavailability of (2/3) RTMs is $3(3.0 \text{ E-3})^2 = 2.7 \text{ E-5}$.

Table A.6 RPS - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
R1	1.0 E-3
R2	2.0 E-3
R3	1.0 E-3
R4	2.0 E-3
R5	2.7 E-5
RMT	2.2 E-2

APPENDIX B

ENGINEERED SAFEGUARDS ACTUATION SYSTEM

APPENDIX B ENGINEERED SAFEGUARDS ACTUATION SYSTEM (ESAS)

B.1 SYSTEM DESCRIPTION AND OPERATION

The Engineered Safeguard Actuation System (ESAS) monitors two variables -- reactor coolant pressure and reactor building pressure -- to detect loss of coolant system boundary integrity. Upon detection of "out-of-limit" conditions of these variables, it initiates operation of the high pressure injection (HPI), low pressure injection (LPI), reactor building isolation and cooling (RBIC), and reactor building spray system (RBSS). The ESAS also starts the engineered safeguards diesel generators A and B.

B.1.1 SYSTEM DESCRIPTION

The ESAS consists of two separate redundant actuation subsystems (trains) A and B, each of which is dedicated to a corresponding ES equipment train. Each ESAS train consists of three sets of channel cabinets, an actuation relay cabinet and the appropriate section of the engineered safeguard operating panel. The equipment in each of the channel cabinets is comprised of the bistable trip units, bistable auxiliary relays, bypass relays, test relays, relay status lights and test switches.

The actuation relay cabinet is divided into four separate compartments to contain the relays for each actuation subsystem and manual actuation output relays. Each of the output signals from a train (the actuation signals for the equipment) is generated by combining the inputs from the three channels in a two out of three matrix as shown in the simplified ESAS logic diagram presented in Figure B.1. Each ESAS train generates five types of output signals: RBSS, RBIC, LPI, HPI and the diesel generator emergency loading sequence, which is provided for sequential starting of large electrical loads following detection of an "out-of-limit" condition.

The following is a simplified description of system operation of train A (or B):

Each actuation train employs three logic channels and the outputs of these channels are used in two-out-of-three coincidence networks for equipment actuation. The channels are actuated by receiving signals (information) from the various on-going processes within the reactor plant and containment. The signal actuates the channel logic by de-energizing to trip the instrumentation channel output relays by opening the contacts, e.g., relay R3 (these output relays are normally energized with closed contacts). See Figure B.2.

Similarly, the logic matrices (actuation relays) in the actuation channels are de-energized to trip -- contacts close, e.g., relay Z1A -- and actuate the engineered safeguards equipment. (The actuation relays are normally energized with contacts open).

Separate essential service and DC power supplies are used for each actuation channel.

The following paragraphs contain a discussion of the specific relay logic implementation used in the actuation channels of each of the five types of ESAS actuation signals.

HIGH PRESSURE INJECTION (HPI) AND DIESEL GENERATOR EMERGENCY LOADING SEQUENCE (DGELS)

Referring to one of three independent reactor coolant pressure transmitters shown in Figure B.3, a signal proportional to the reactor coolant pressure is applied to a safeguards bistable (BT1) and to a bypass bistable. The design of safeguard bistables is such that when the reactor coolant pressure is above the setpoint and control power is available, bistable interposing relay R3 is energized.

HPI is initiated by de-energizing the multiple contact output relays constituting loading sequence block 1 in two-out-of-three channels. (Block 1 consists of HP Injection pumps, Injection and Nuclear Services Valves, and LP Injection pumps). The multiple contact output relays can be de-energized by the manual actuation relay by their related test contact, or by an "OR" function made up of contacts which open when the reactor coolant pressure is below 1500 psig (R3), the building pressure exceeds 4 psig (R12), or the reactor coolant pressure is below 500 psig.

Blocks 2, 3, and 4 de-energize through an "AND" function, combining an "OR" function similar to the one described above and undervoltage relay contacts from corresponding 4160 volt safeguard bus. Block 2 consists of Reactor Building Fans and Emergency Nuclear Service Seawater pumps. Block 3 consists of Emergency Nuclear Services Closed Cycle Cooling Water pumps. Block 4 consists of spray pump start permit, reactor building ventilation recirculation unit, Decay Heat Closed Cycle Cooling water pump, and Decay Heat Service Seawater pumps.

LOW PRESSURE INJECTION (LPI)

The channels of low pressure injection are equipped with bistables similar to those used for HPI but which are adjusted to actuate at a lower setpoint. A typical channel is shown in Figure B.3. The output of the bistables will de-energize the same output relay as the HPI bistables at 500 psig.

The bypass enabling contact of the bistable closes when the reactor coolant pressure is below its setpoint (900 psig) and control power is available. This action permits manual bypass of the channel for normal shutdown of the system.

REACTOR BUILDING ISOLATION AND COOLING (RBIC)

The channels of Reactor Building Isolation and Cooling are similar in design to the channels of HPI and loading sequence except for the bistable and bypass circuit, as shown in Figure B.4. When the reactor building pressure is below 4 psig and control power is available, pressure switch

interposing relay R10 is energized to the reset state by means of the bypass reset pushbutton. A subsequent loss of power or rise in building pressure above setpoint will drop out R10.

The continuous bypass of a channel is possible only after a two-out-of-three actuation. De-energizing the output relays of two-out-of-three channels initiates reactor building isolation, starts reactor building emergency cooling and opens all valves required for reactor building spray. The reactor building pressure is sensed by two sets of three pressure switches, and the bypass can only be energized after a two-out-of-three actuation.

REACTOR BUILDING SPRAY (RBSS)

RBSS is initiated by starting the pumps when reactor building pressure is over 30 psig. This is achieved, as shown on Figure B.5, by sensing the reactor building pressure with two sets of three pressure switches. Each set of three pressure switches, which are wired in a two-out-of-three matrix, controls the closing coils of the circuit breaker of one spray pump along with actuation of the spray pump start permit matrix from HPI.

While independence between individual channels within ESAS actuation trains is realized, a dependency exists between actuation trains which include reactor coolant pressure trip signals (HPI, DGELS, LPI, and RBSS). This dependency can be observed by noticing that the channel pressure transducer shown in Figure B.3 provides pressure signals to both LPI and HPI bistables, and that those bistables are common to both actuation trains. Failures of the pressure transducer or bistables affects both actuation trains. Another interface is the undervoltage relay contact appearing in the loading sequence circuitry which represents a dependency on the 4160V ES bus.

The ESAS is not dependent on control power to accomplish equipment actuation since loss of power will de-energize the output relays and activate the associated equipment.

B.1.2 SYSTEM OPERATION

Table B.1 illustrates ESAS equipment actuation signals as a function of reactor coolant pressure and reactor building pressure. Table B.2

lists the trip parameters met, along with ES equipment actuated during various size LOCA events. Loss of power to the ESAS circuitry results in the generation of trip signals by the ESAS (except for RBSS).

The ESAS is designed to allow every component in the system to be tested during plant operation. Typically, monthly surveillance tests are performed to insure all components are operating correctly. System calibration is performed during refueling. The pressure transducers and buffer amplifiers in the system are monitored at shift changes by observing a meter which indicates reactor pressure sensed by the system.

Monthly surveillance tests are performed for the entire system except for the reactor coolant pressure transducers and most of the actuation matrix relay contacts. Each of the ESAS channels is checked individually by generating trip signals. These signals de-energize the output relays of the channel and cause 1 of the 3 relays in the 2 of 3 relay matrices to trip. Equipment will be actuated upon receipt of a trip signal from either of the other 2 channels. Testing of the system does not disable it or reduce its capability to trip. Only one channel can be tested at a time.

During each refueling (every 18 months) tests are done which trigger the ES actuation system one actuation system (train A or B) at a time, then phase into a diesel generator test. These tests are performed using any two (of the three) associated RBIS pressure test switches to introduce an artificial high reactor building pressure signal. These signals de-energize the actuation relays of two out of three channels in the equipment matrices and consequently actuate the equipment.

Table B.1 ESAS Actuation Signals for RCS and RB Pressure Set Points

<u>RCS Pressure Set Point (psig)</u>	<u>ESAS Actuation Description</u>	<u>RB Pressure Set Point (psig)</u>	<u>ESAS Actuation Description</u>
1700	By-pass is enabled	4	Trip - (HPI, LPI pumps, LPI valves, RB isolation) initiated
1500	Trip can be by-passed (HPI, LPI pump)		
1500	Trip HPI, LPI pumps initiated	30	Start containment spray pumps if HPI trip not by-passed
900	Trip can be by-passed (HPI, LPI)		
500	Trip (HPI, LPI pumps, LPI valves) initiated		

Table B.2 ESAS Trip Parameters Met and Systems Actuated for Various Sizes of LOCA Initiating Events

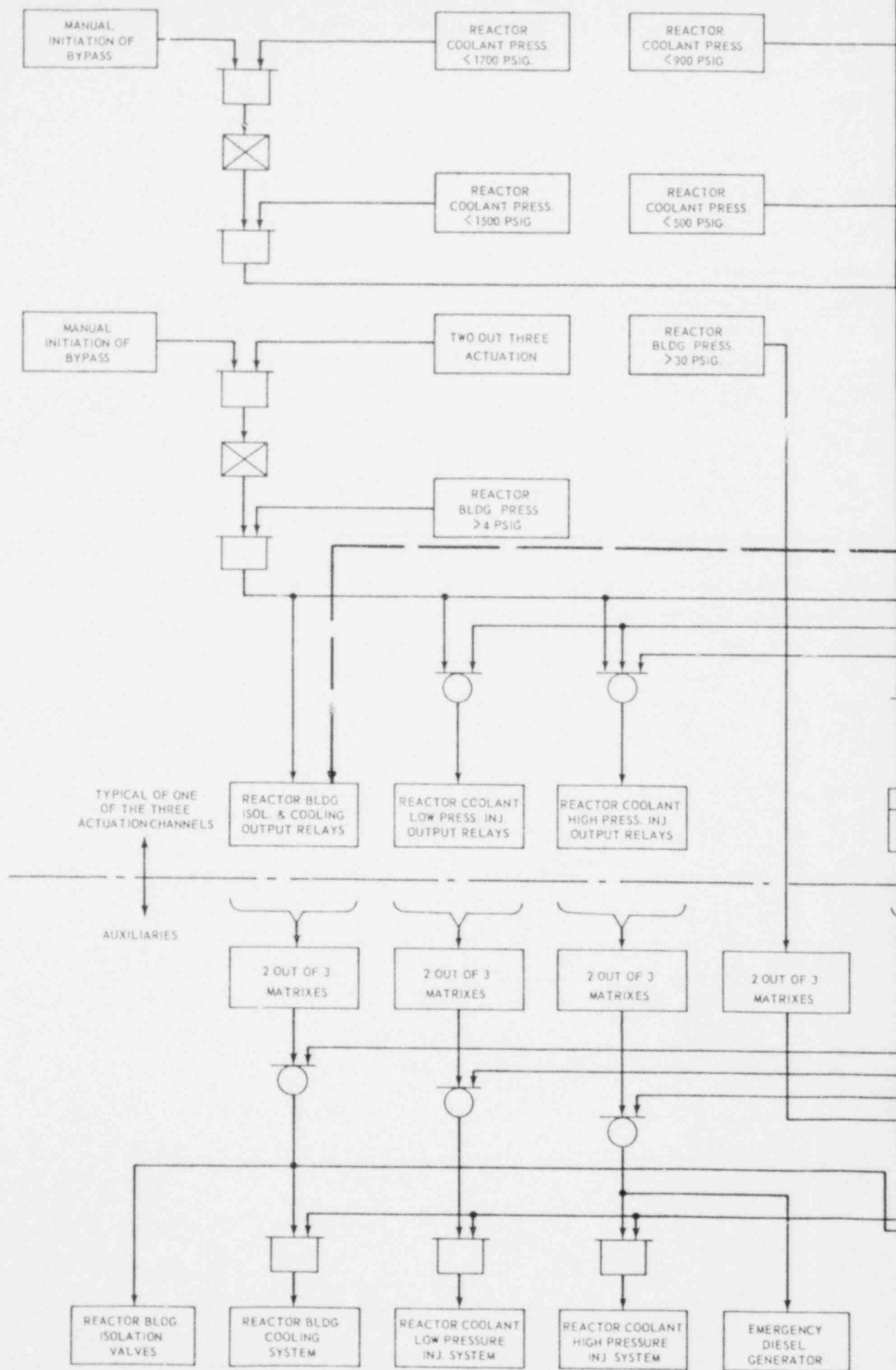
INITIATING EVENTS	TRIP PARAMETERS MET				SYSTEM ACTUATION			
	500 PSI TRIP	1500 PSI TRIP	4PSI TRIP	30PSI TRIP	LPI	HPI	RBIC	RBSS
B ₁ Large LOCA	X	X	X	X	X	X	X	X
B ₂ Medium LOCA	X	X	X	X [†]	X	X	X	X
B ₃ Small LOCA		X	X		X	X	X	X [*]
B ₄ Small small LOCA		X			X ^{**}	X ^{***}		

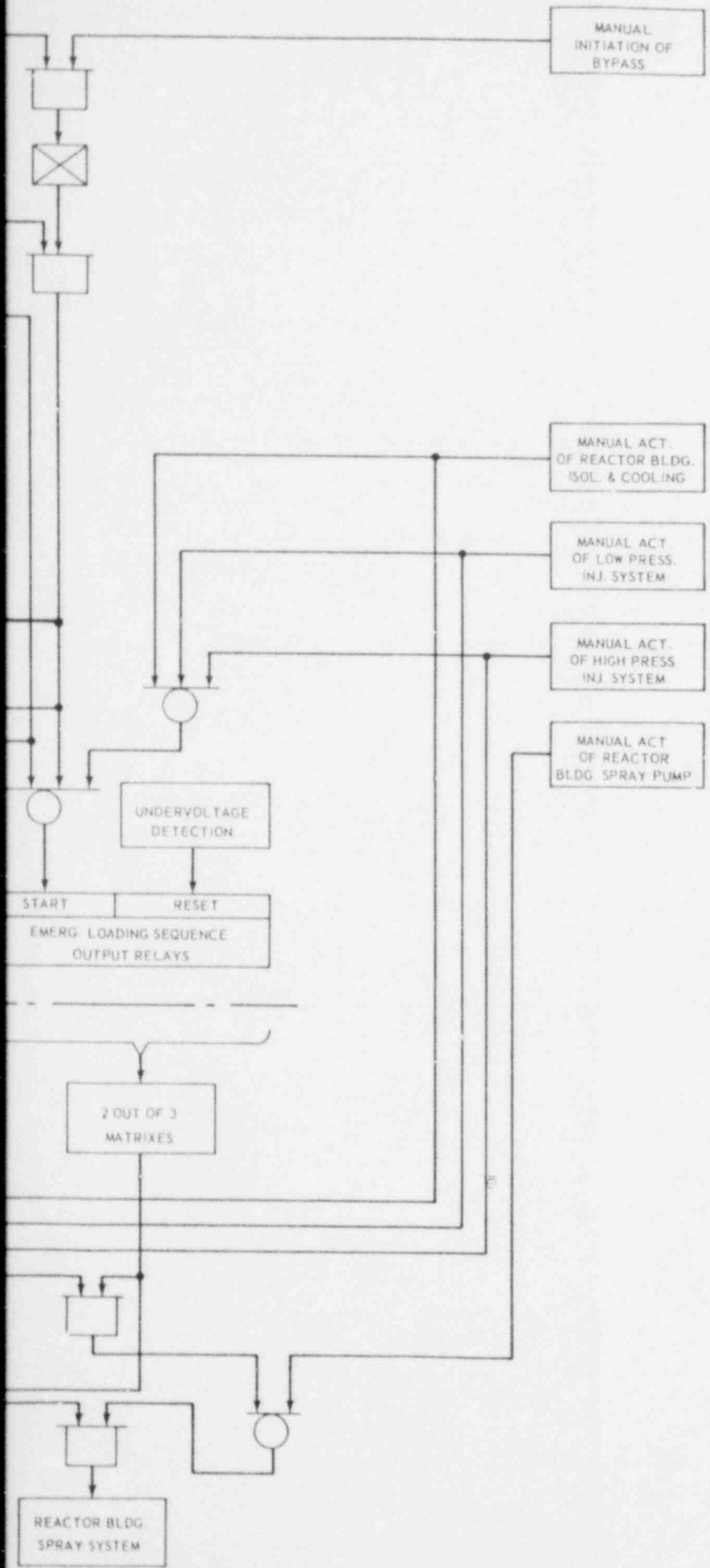
[†]Based on conservative FSAR calculations.

*RBSS spray line injection valves are actuated (opened) by the 4 psi trip signal. The RBSS pumps do not receive an actuation signal.

**LPI pumps start, but the LPI injection valves do not receive an actuation signal.

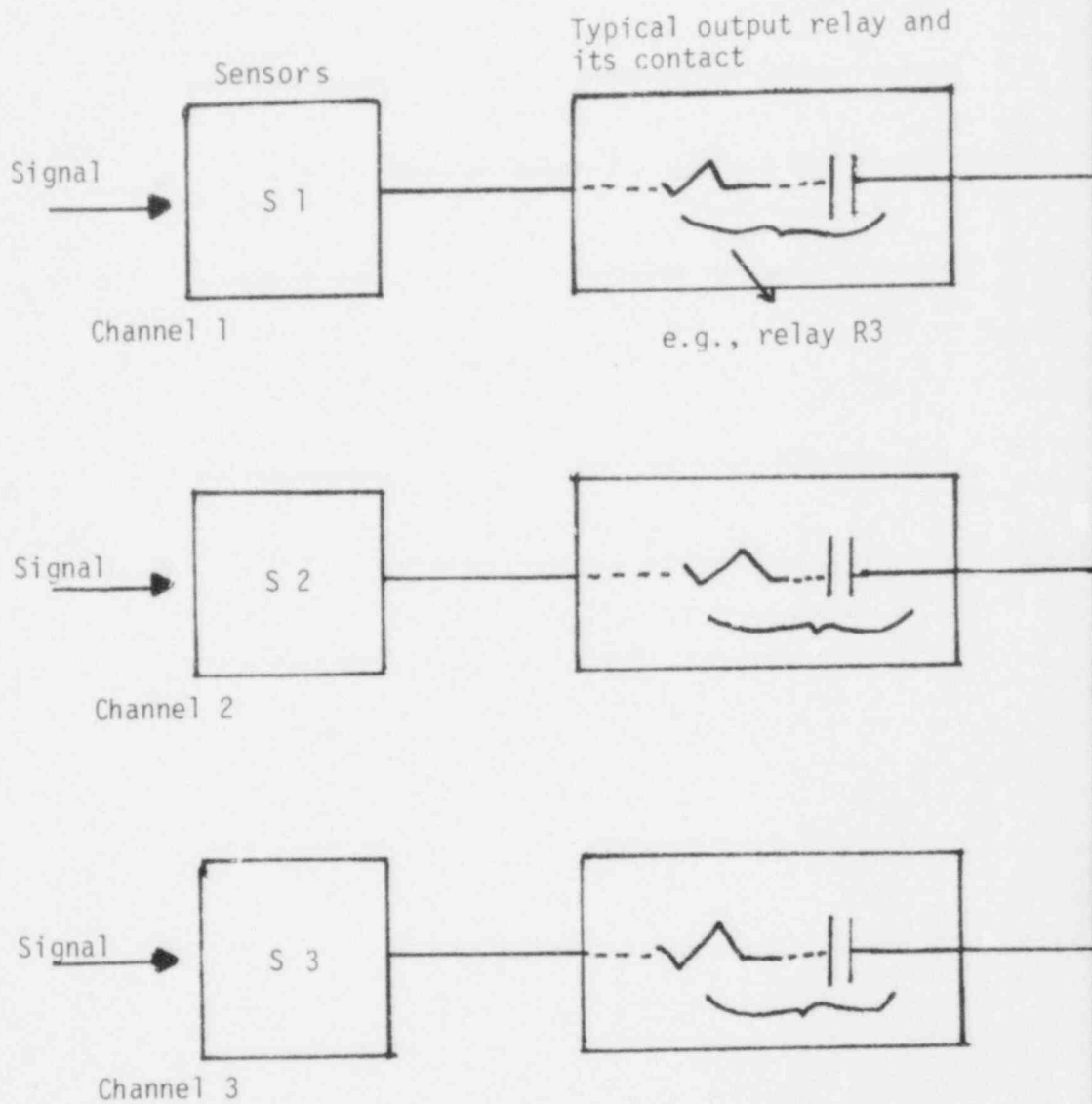
***Also isolates those RB isolation valves not associated with containment or RCS heat removal.





- OR GATE
- AND GATE
- ⊗ NOT

Figure B.1 Engineered Safeguards Actuation A (B similar) Simplified Logic



The circuits are shown tripped

- NOTE 1 Contacts 1, 2, 3, ...n belong to matrixes of other equipmen
 NOTE 2 Each relay closes two contacts (one U and one Z)

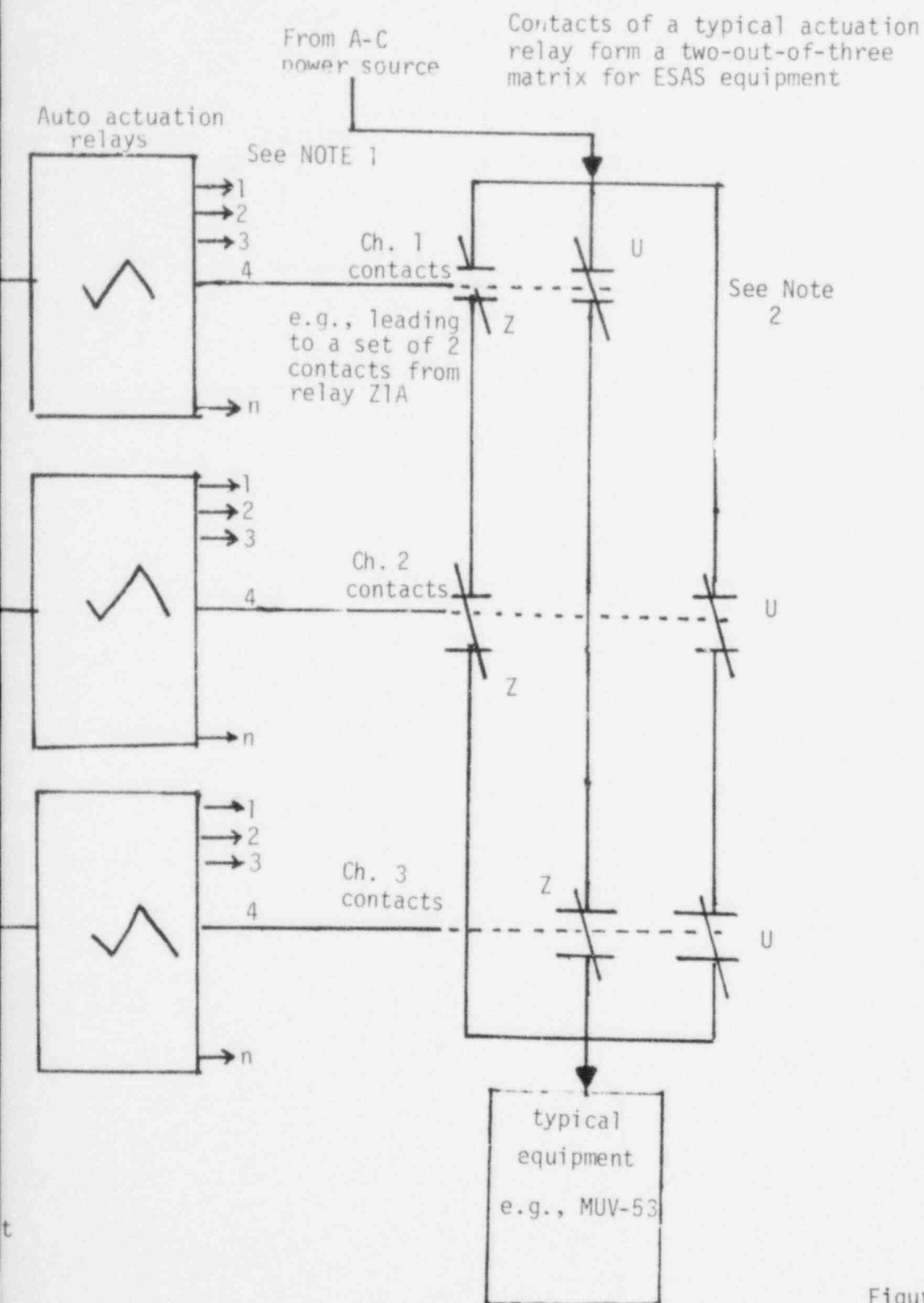


Figure B.2 ESAS-Simplified Circuitry

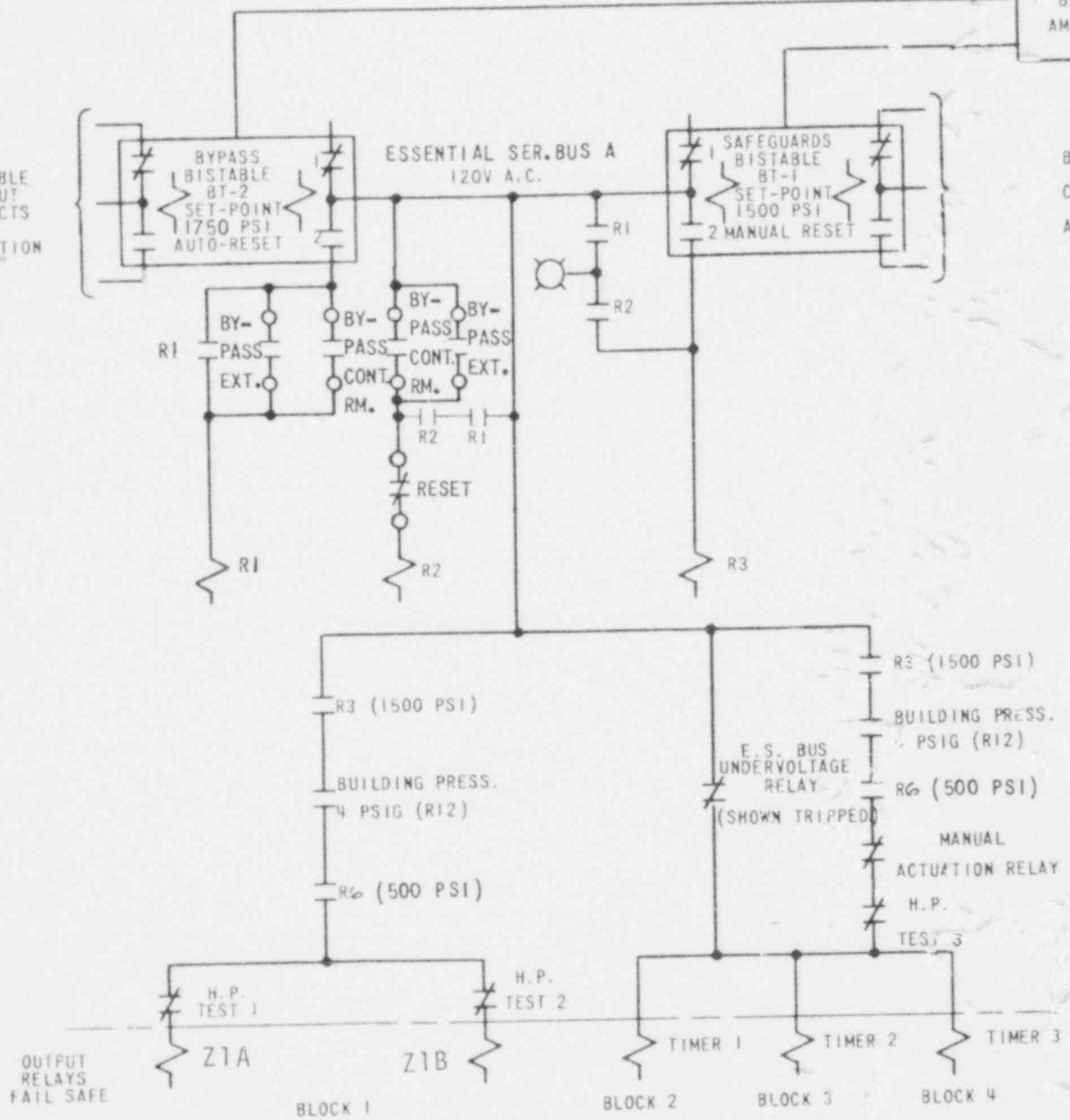
TYPICAL REACTOR COOLANT PRESSURE TRANSMITTER

P.T. 1 (1 OF 1)

BUFFER AMPLIFIER

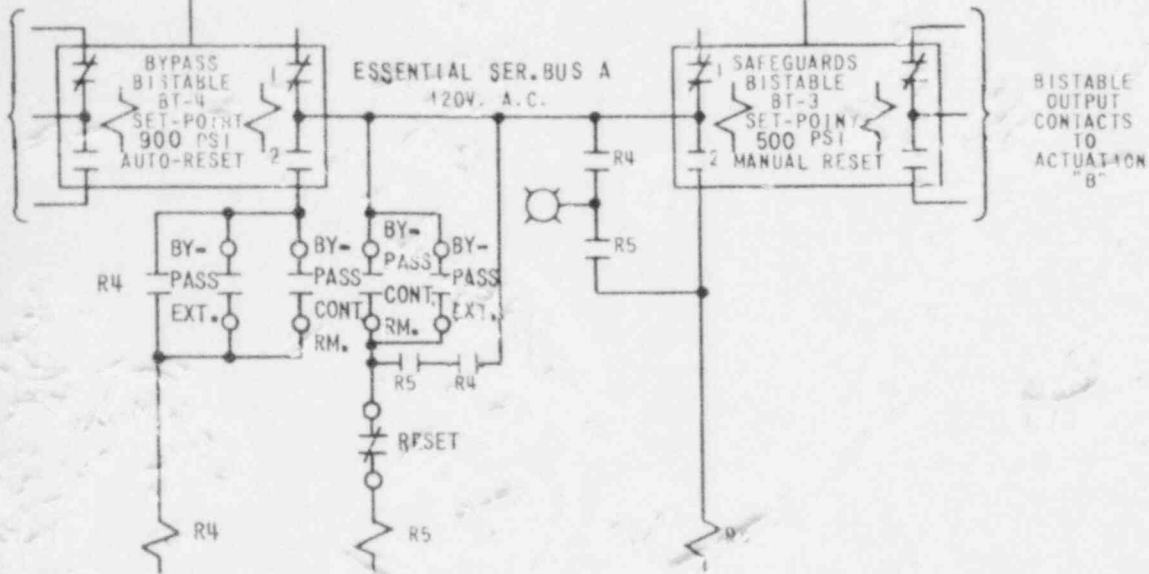
BISTABLE OUTPUT CONTACTS TO ACTUATION "B"

BISTABLE OUTPUT CONTACTS TO ACTUATION "B"



TYPICAL OF 3 CHANNELS
HIGH PRESSURE INJECTION & LOADING SEQUENCE A

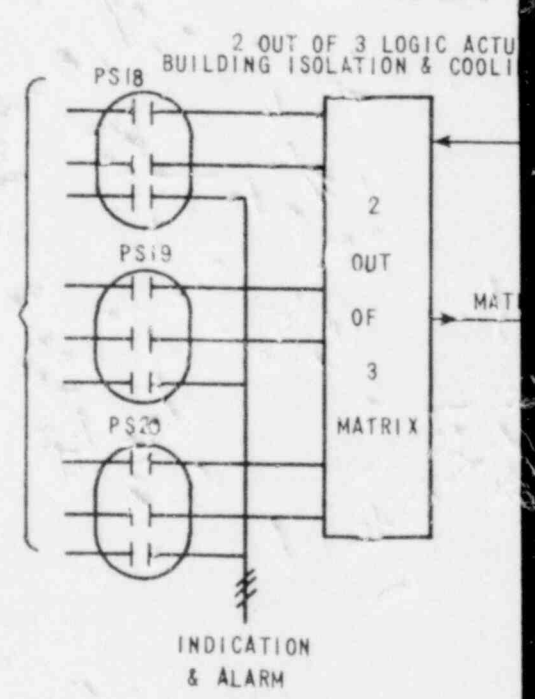
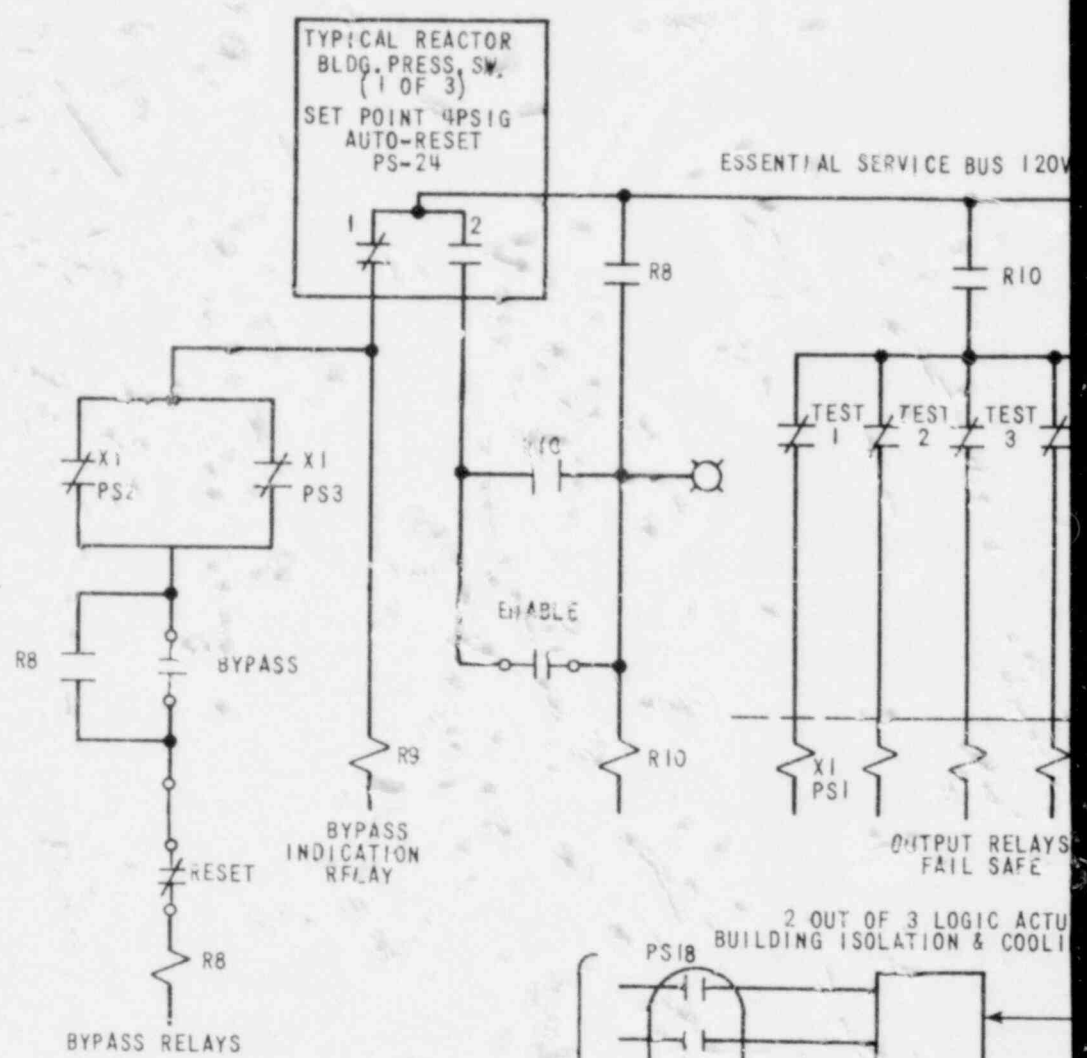
NOTE: 2 OUT OF 3 LOGIC



TYPICAL OF 3 LOW PRESSURE CHANNELS

STARTS EACH AUXILIARY

Figure B.3 (1/2)
Safeguards Actuation System



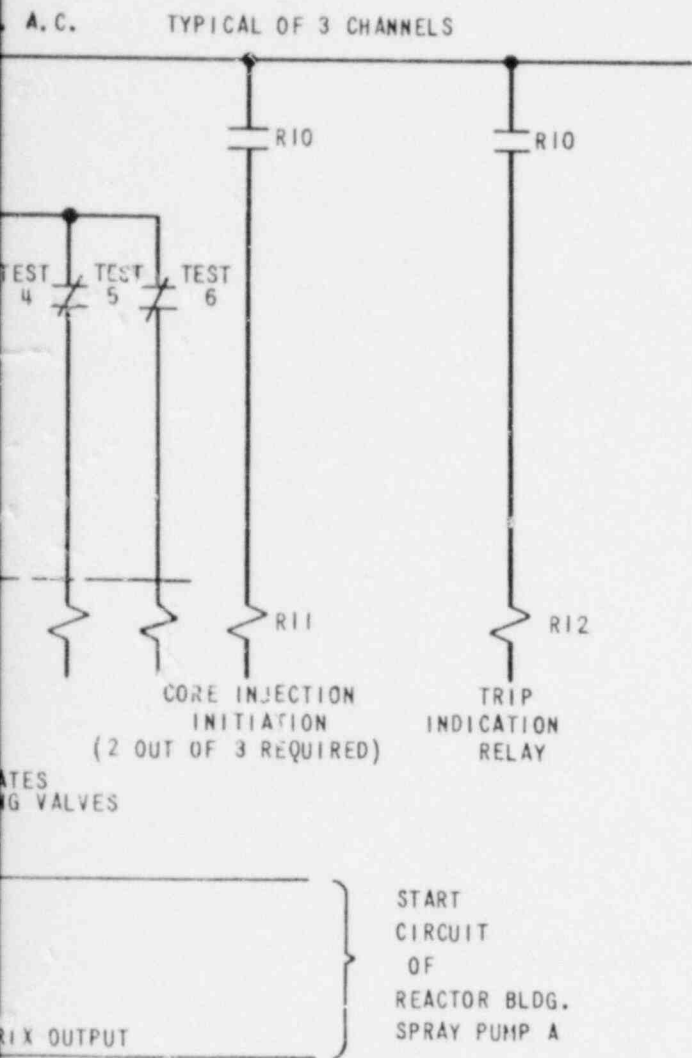


Figure B.3 (2/2)
Safeguards Actuation System

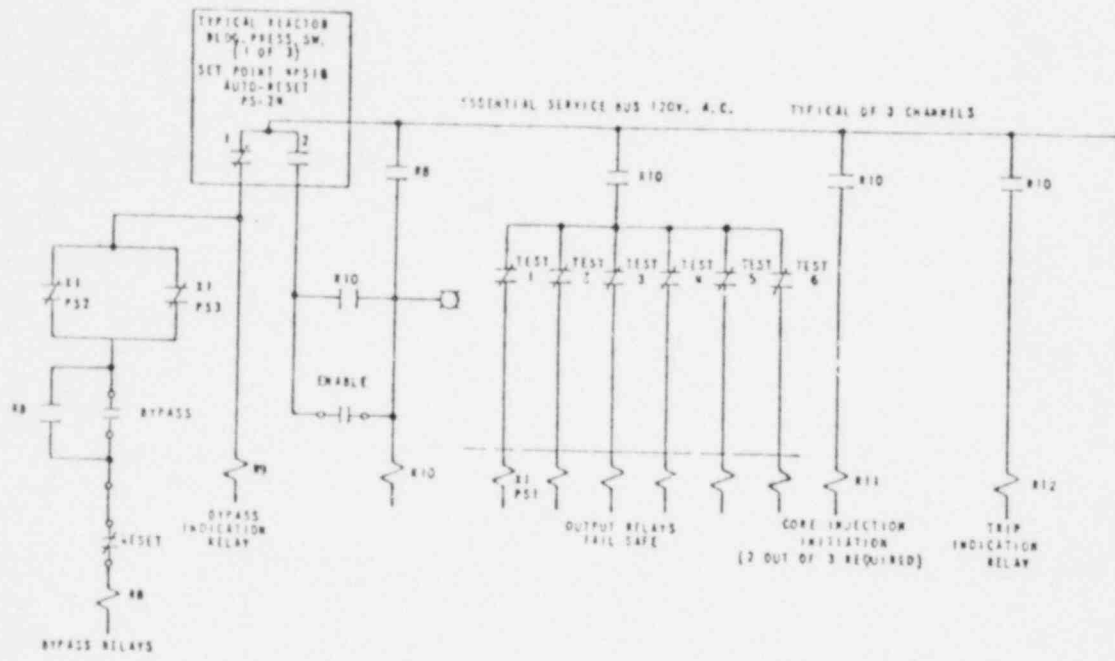


Figure B.4 Reactor Building Isolation (RBIS) and Cooling (RBCS) Actuation Circuit (1 channel of 1 train)

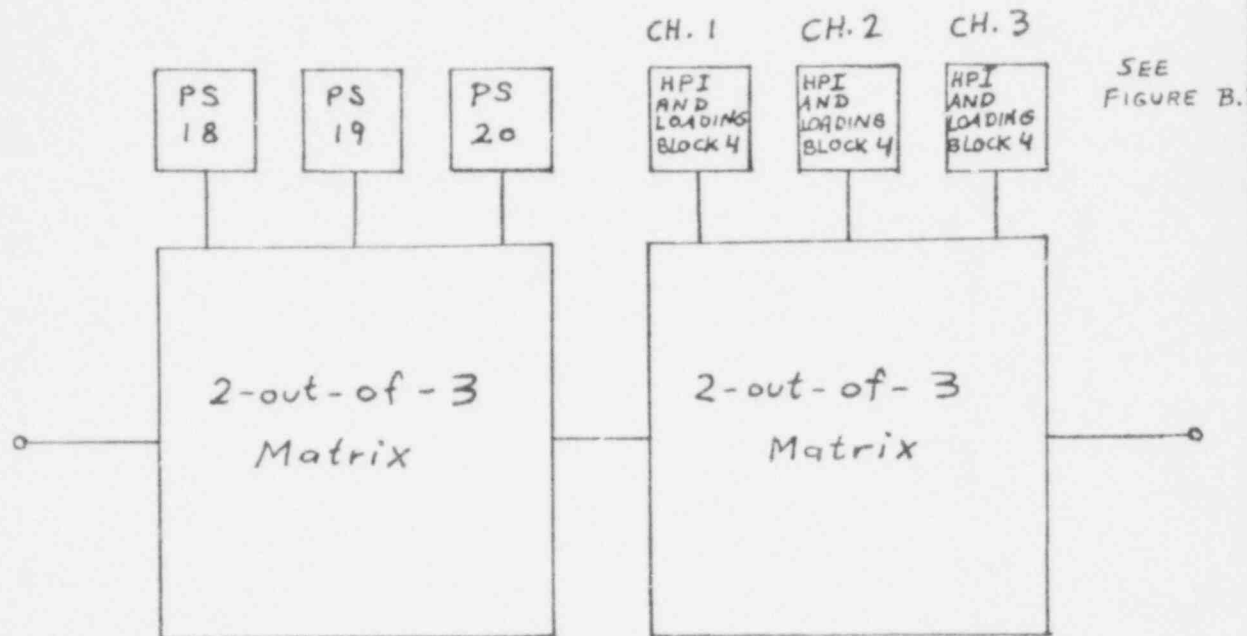


Figure B.5 ESAS - Reactor Building Spray Actuation (1 Train)

B.2 SYSTEM SIMPLIFIED FAULT TREE

Fault trees were constructed to model ESAS failure to actuate ESF equipment during LOCAs. The ESAS responds to a B₄ LOCA by actuating the HPI equipment group (including the LPI pumps). All other ESF functions (LPI injection line valves, RBIC, and RBSS) are not actuated. If a larger LOCA (B₁, B₂, or B₃) is the initiating event, it is expected that all ESF equipment will be given actuation signals.

A set of two fault trees was constructed for ESAS failure to actuate HPI, given a B₄ LOCA. One top event is defined as the failure of a single piece of HPI equipment to receive an actuation signal from the ESAS (Event ISS). This top event is necessary to provide an interface to individual equipment appearing in system fault trees. Evaluation of this tree provides a failure-to-actuate probability for use in conjunction with individual equipment failures appearing in the HPI system fault tree. The fault tree structure developed in this tree is valid for both immediate and loading sequence time delayed equipment actuation. The differences in circuitry involved are taken into account by modifying the unavailabilities of the group logic and the output relay to reflect the differences in hardware configuration.

The top event for the second fault tree for ESAS to actuate HPI, given a B₄ LOCA, is defined as failure of both HPI actuation trains to generate actuation signals (Event ISB). Evaluation of this tree provides the probability that equipment in both HPI trains will not be actuated. This event appears as a common mode fault in the HPI system fault trees.

A second set of two fault trees similar to those described above, was constructed for ESAS failure to actuate each ESF, given a B₁, B₂, or B₃ LOCA (Event ILB and ILS). The basic fault tree structure for these trees is defined by the fact that all ESF equipment is actuated by providing continuity to control circuits with two-out-of-three relay matrices. Each type of actuation circuit, however, contains a slightly different equipment configuration which is included in the models. In addition, these models include a common mode human error for actuation of the RBIC and RBSS. This error is the miscalibration of all pressure switches and pressure regulators used to test pressure switches.

The detailed fault trees were simplified by the elimination of failure combinations containing more than two active failures, since these fault combinations are not expected to contribute to the system failure. The resulting simplified fault trees for ESAS failure to actuate HPI, given a B₄ LOCA, are shown in Figures B.6 and B.7; those for ESAS failure to actuate each ESF, given a B₁, B₂, or B₃ LOCA*, are shown in Figures B.8 and B-9. The top event definitions for the simplified fault trees are shown in Table B.3.

*The RBSS pumps do not receive an ESAS actuation signal from the B₃ LOCA initiator; however, the spray line injection valves are actuated (opened) by the RB 4 psi trip signal.

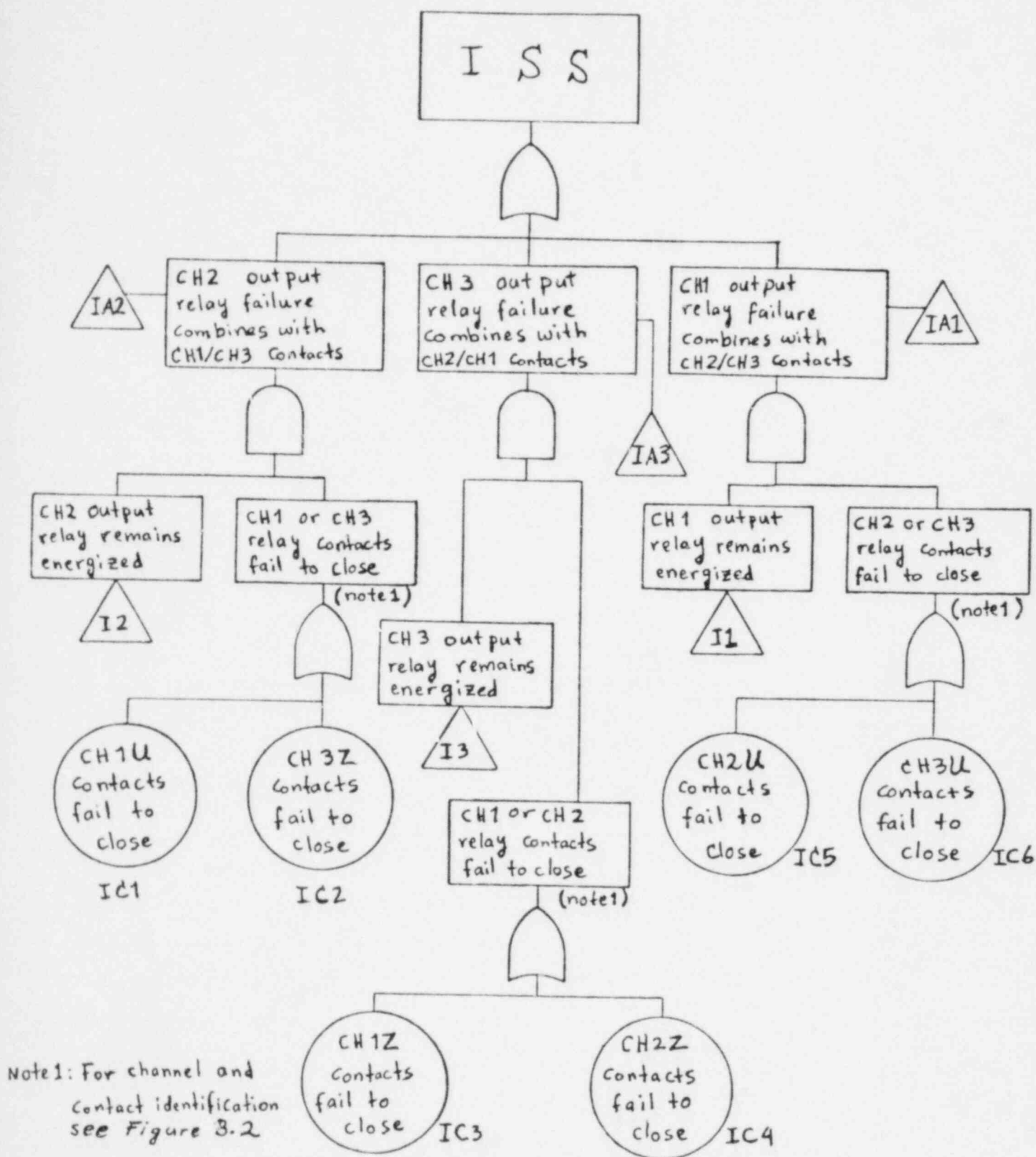
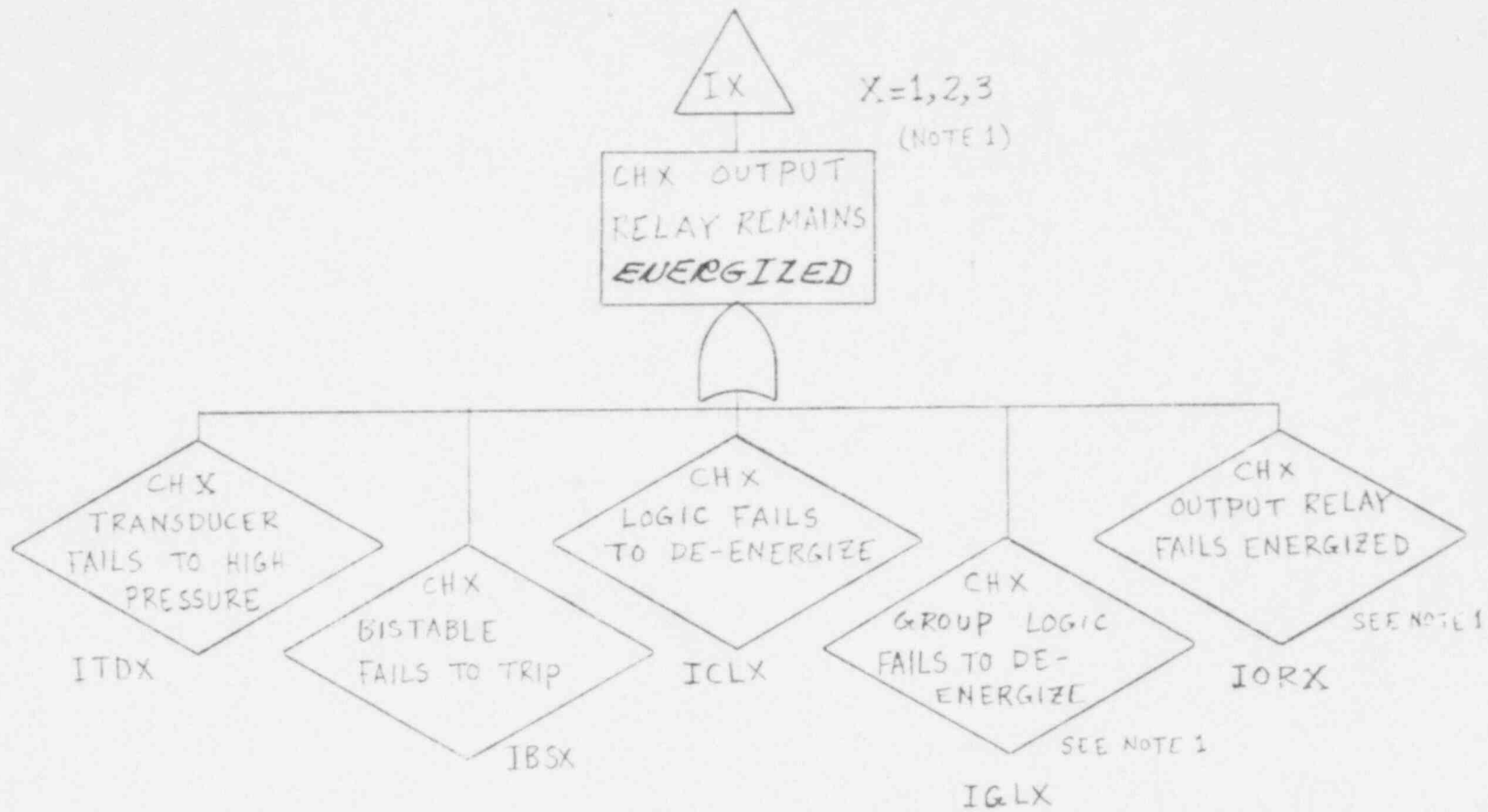


Figure B.6 (1/2) Simplified Fault Tree - ESAS (Event "ISS", B₄ LOCA)



NOTE 1: Unavailability used here depends on equipment configuration; time delay or immediate actuation.

Figure B.6 (2/2) Simplified Fault Tree - ESAS (Event "IX", X = 1, 2, 3; B₄ LOCA)

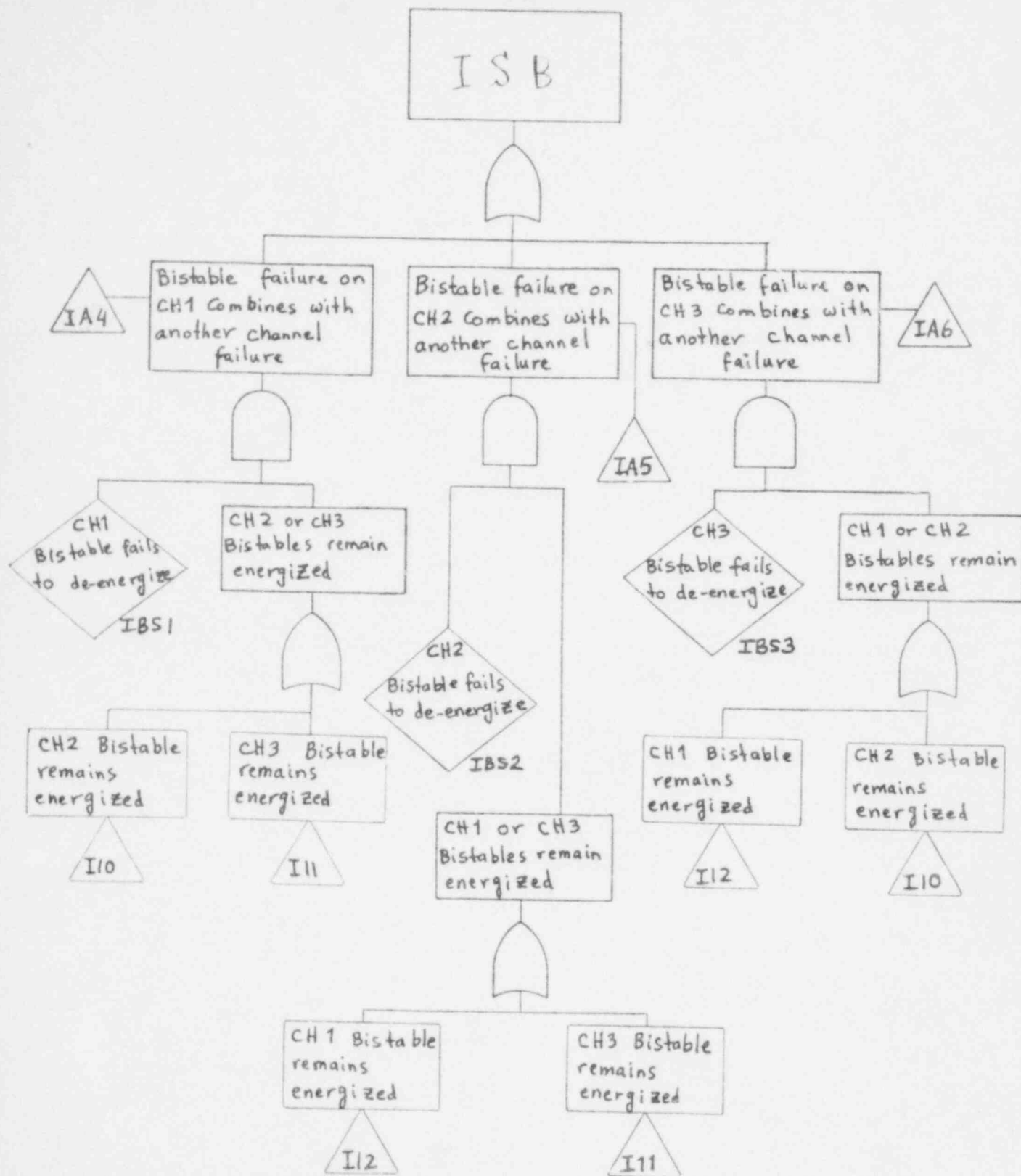


Figure B.7 (1/2) Simplified Fault Tree - ESAS (Event "ISB"; B₄ LOCA)

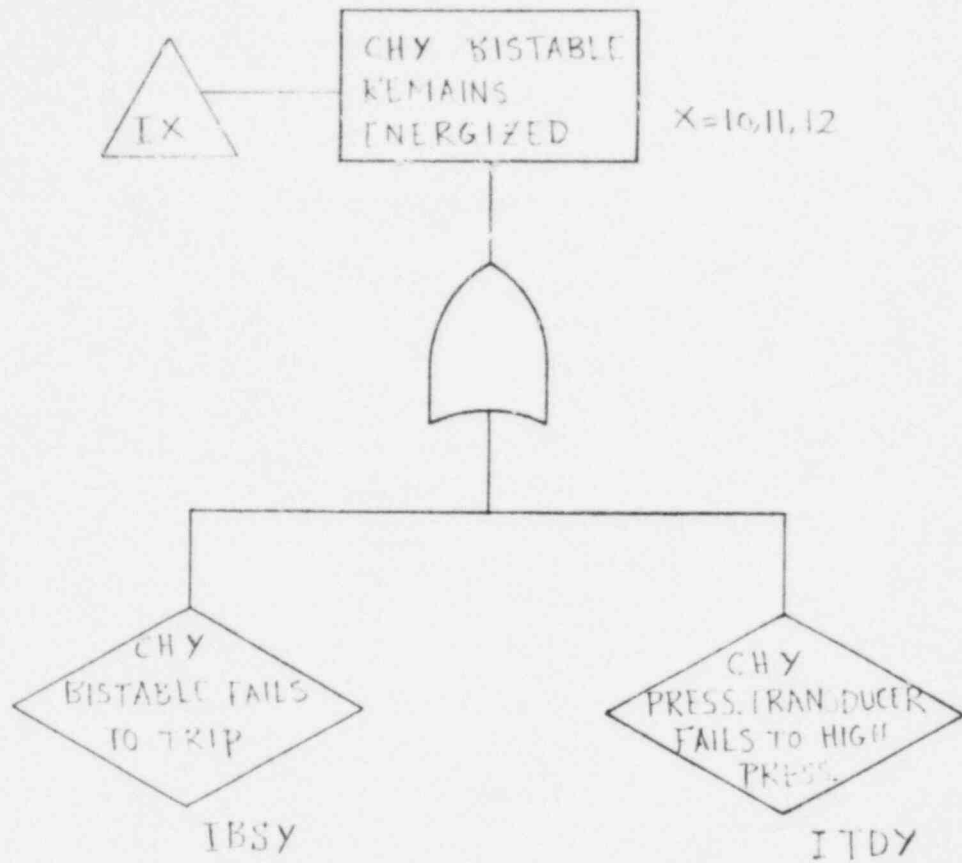
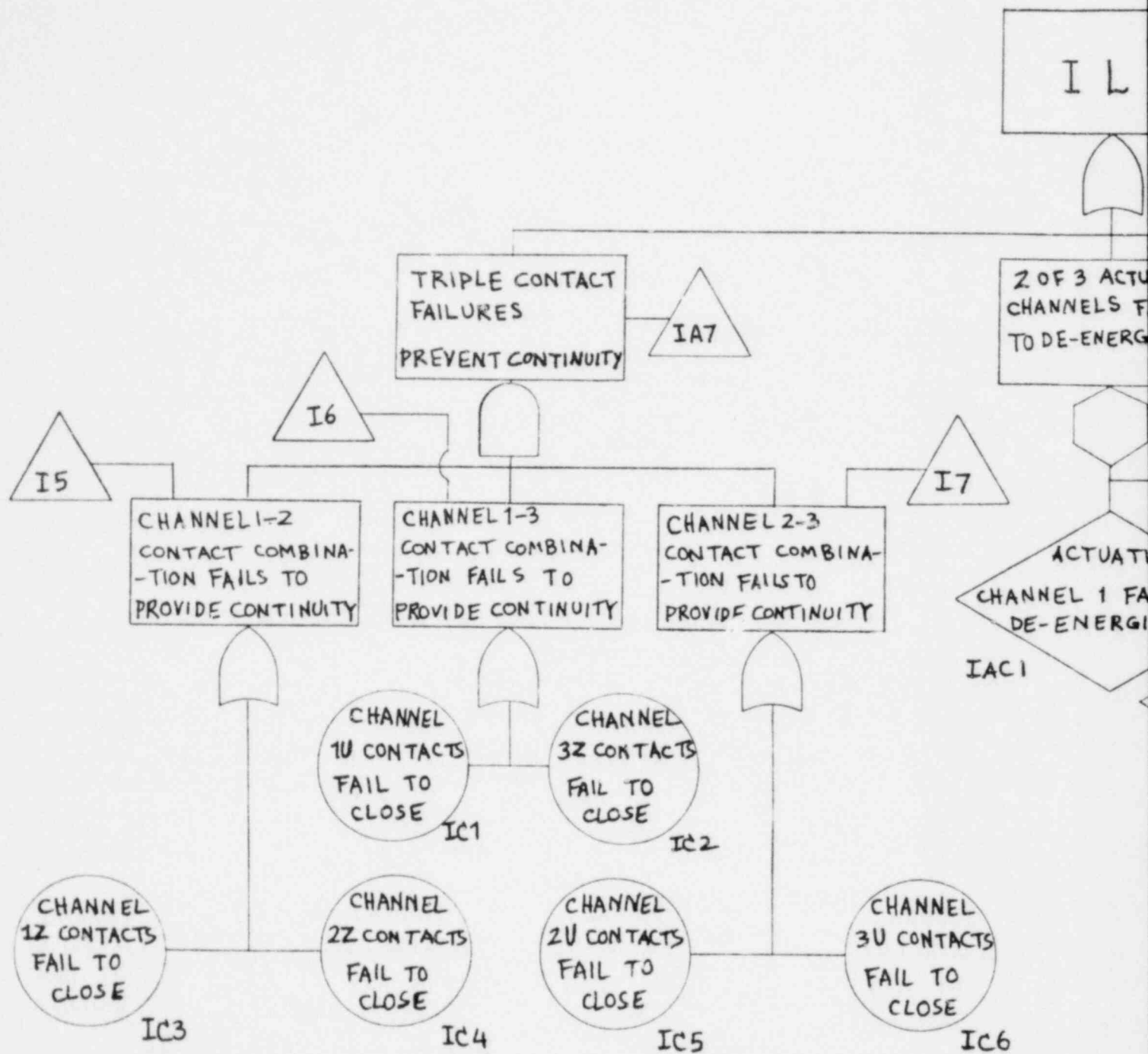


Figure B.7 (2/2) Simplified Fault Tree - ESAS (Event "IX", X = 10 and Y = 2, X = 11 and Y = 3, X = 12 and Y = 1; B₄ LOCA)



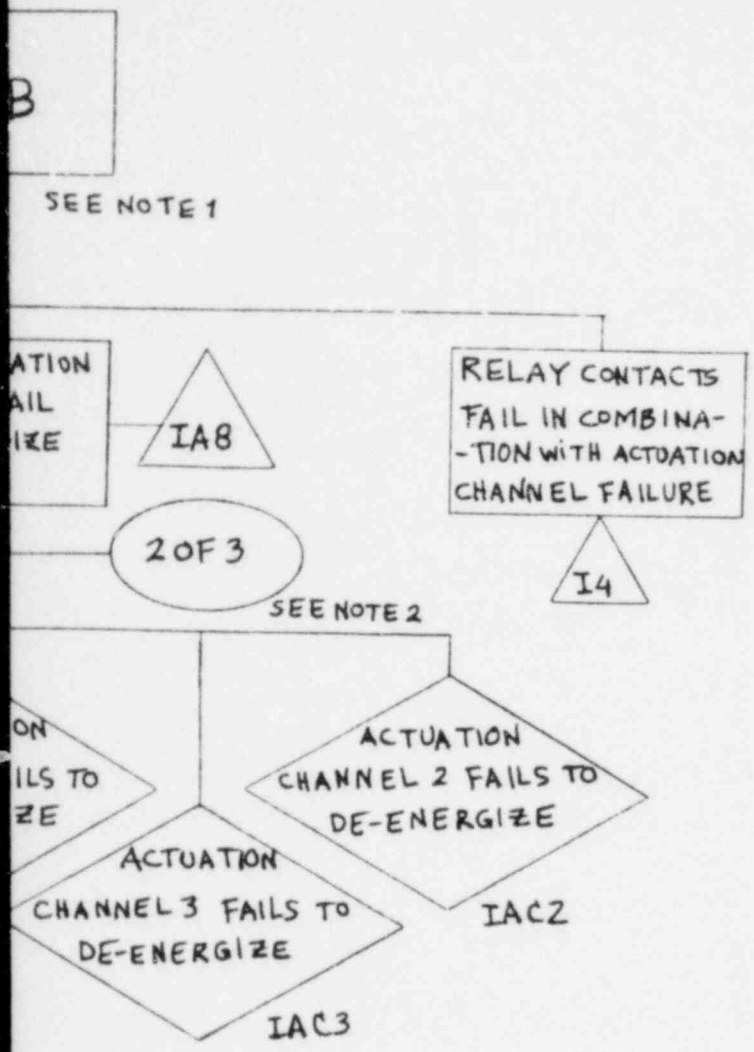
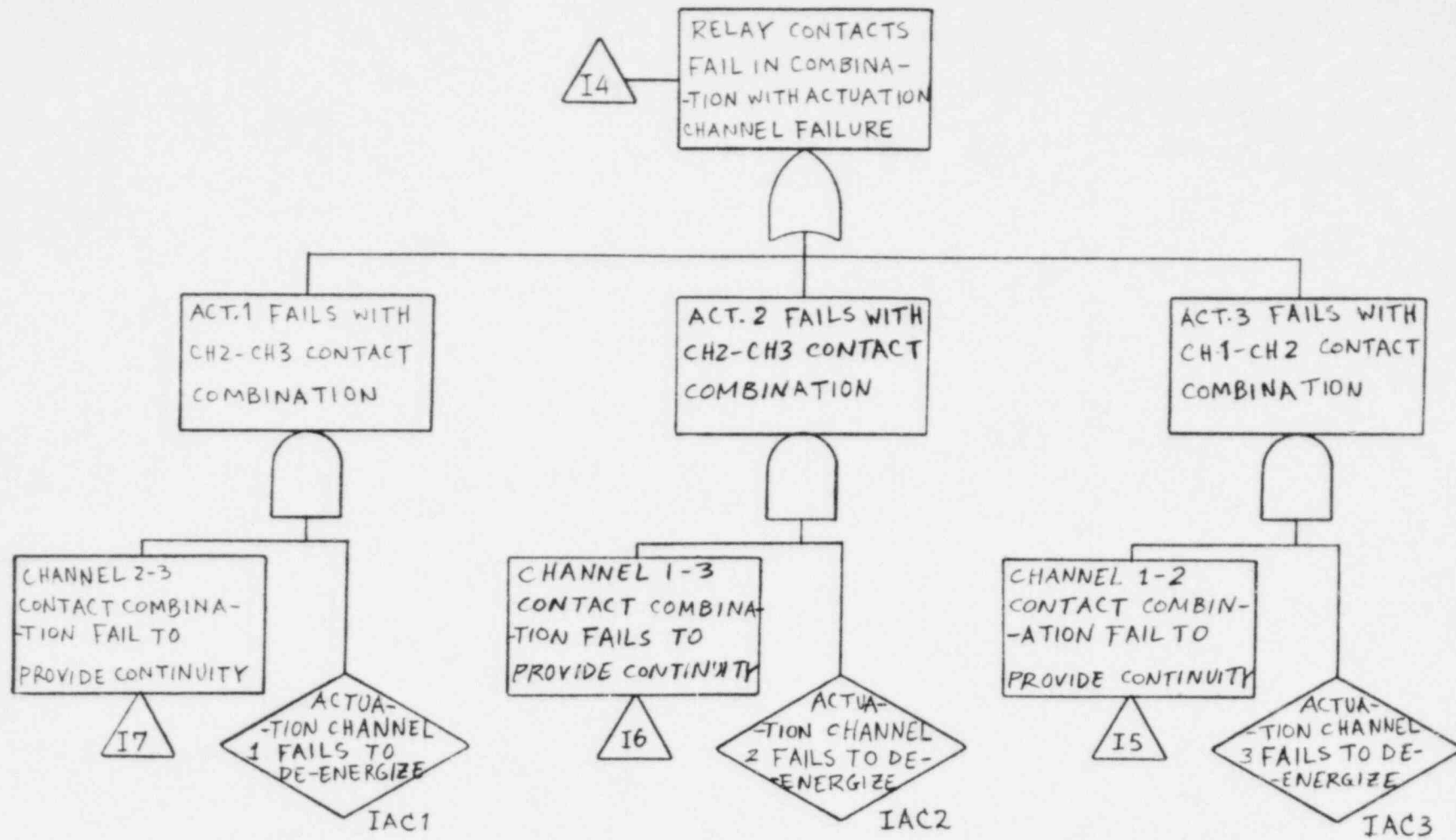


Figure B.8 (1/2) Simplified Fault Tree - ESAS (Event "ILB"; B₁, B₂, or B₃ LOCA)



B-27

Figure B.8 (2/2) Simplified Fault Tree - ESAS (Event "I4"; B₁, B₂ or B₃ LOCA)

Figure B.8 Simplified Fault Tree - ESAS
(Event "ILB")

NOTES:

- 1 The RBSS pumps do not receive an ESAS actuation signal for the B₃ LOCA initiator; however, the spray line injection valves are actuated (opened).
- 2 This event is failure of automatic actuation of all equipment in one train.

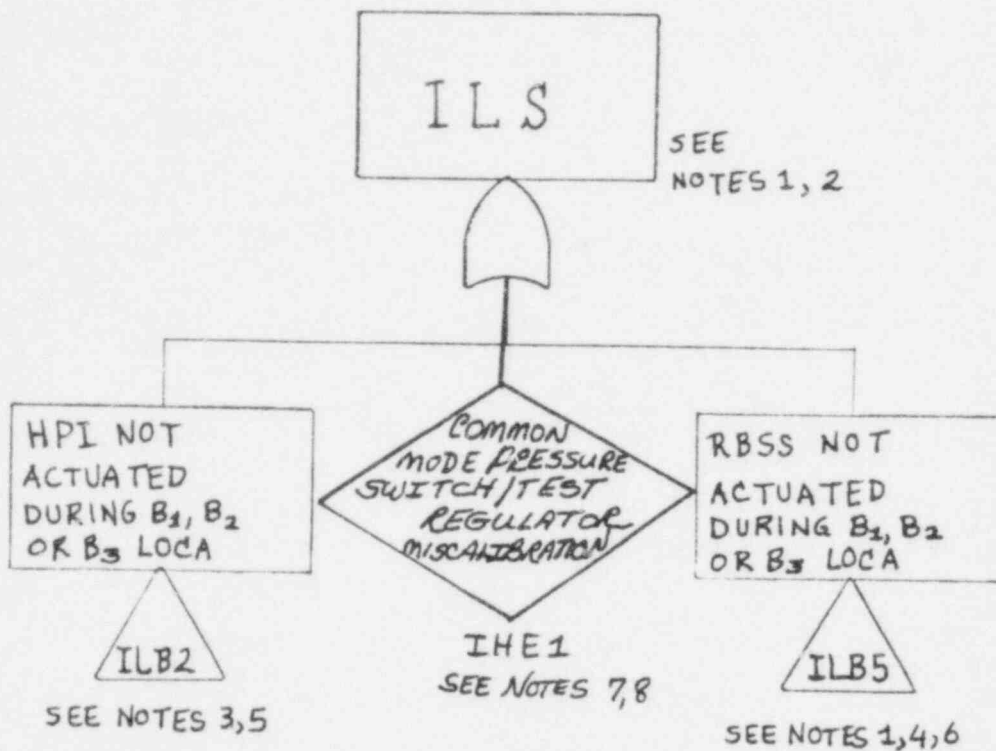


Figure B.9 Simplified Fault Tree - ESAS (Event "ILS"; B₁, B₂ or B₃ LOCA)

Figure B.9 Simplified Fault Tree - ESAS
(Event "ILS")

NOTES

- 1 The RBSS pumps do not receive an ESAS actuation signal for the B₃ LOCA initiator; however, the spray line injection valves are actuated (opened).
- 2 This fault tree combines a RBSS and HPI fault tree to model the entire RBSS actuation circuit.
- 3 ESAS fault tree evaluated for HPI 15 sec time delay (B₁, B₂, or B₃ LOCA).
- 4 ESAS fault tree evaluated for RBSS switch matrix (B₁, B₂, or B₃ LOCA)
- 5 See quantification table for event ILB2.
- 6 See quantification table for event ILB5.
- 7 This event is miscalibration of all pressure switches (both 4 psi and 30 psi) and pressure-switch-test pressure regulators due to a maintenance error during a refueling outage. This event disables the RBSS and RBIC actuation trains because the actuation logic circuit for the RBIC is a required part of the actuation logic circuit for the RBSS. It does not affect the LPI or HPI actuation trains.
- 8 This event results in failure to actuate all equipment in both trains in RBSS and both trains in RBIC.

B.3 SYSTEM QUANTIFICATION

B.3.1 SYSTEM RELIABILITY CHARACTERISTICS

Table B.3 contains the results of the evaluation of the fault trees for the top events in the ESAS fault trees. The results in most cases are dominated by failures within the ESAS output matrices which provide actuation signals to individual pieces of equipment. Two types of ESAS actuation signal top events shown in the table appear as common mode faults in the fault trees for the systems receiving the actuation signals. The first, for the B_4 LOCA, is "HPI Actuation Signal Not Available to Any Equipment" (Event ISB). The second of these faults, for the B_1 , B_2 , or B_3 LOCA is "All RBIC, RBSS Systems Do Not Receive Actuation Signal" (Event ILS). This fault can result from equipment miscalibration due to a common-mode human error.

The dominant failure mode for ESAS failure to actuate one piece of HPI equipment, given a B_4 LOCA (Event ISS), is due to combinations of output relay matrix contact failures and failure to trip of a bistable in another channel. The dominant failure mode of both HPI actuation trains, given a B_4 LOCA (Event ISB) is a combination of two bistables failing to trip.

The dominant reason for ESAS failure to actuate LPI, HPI, and RBIC, given a B_1 , B_2 or B_3 LOCA, is combinations of three output relay contacts failing to close when their associated relays are de-energized. In addition to the triple contact failure, the time delay HPI actuation system of 1 relay contact failure and failure of the actuation channel is found to be a significant contributor. The common mode pressure switch miscalibration event dominates all failures of the RBIC and RBSS actuation systems. The most likely failure event for automatic actuation of these systems is total loss of actuation signals to both systems (Event ILS).

B.3.2 SYSTEM FAULT TREE QUANTIFICATION

The Engineered Safeguards Actuation System does not depend on any other system (i.e., power failure would cause an ESAS signal). The independence from any other system does not require a Boolean reduction in the event tree sequence analysis. Therefore, no modularized fault tree was constructed. The simplified fault trees presented in Section B.2 are used for the quantification purposes.

Table B.4 shows the ESAS success requirement. Table B.5 contains the top event definitions for the simplified fault trees (Figures B.6 through B.9). Table B.6 shows the Boolean equations that represent the fault trees. Table B.7 shows the quantification of each gate by component and failure mode. Table B.8 summarizes the point estimates of the top events.

Table B.3 Results of ESAS Quantification

INITIATING EVENT	TOP EVENT**	FAULT TREE TOP EVENT	UNAVAILABILITY
B ₄ LOCA	ISS1	Non-time delayed HPI actuation signal not available to exactly 1 piece of equipment	2.1 x 10 ⁻⁴
	ISS2	Time delayed HPI actuation signal not available to exactly 1 piece of equipment	2.2 x 10 ⁻⁴
	ISB	HPI actuation signal not available to any equipment (Both trains failed)	7.2 x 10 ⁻⁴
B ₁ , B ₂ , or B ₃ LOCA	ILB1	Non-time delayed HPI actuation signal not available to exactly 1 piece of equipment	1.0 x 10 ⁻⁷
	ILB2	Time delayed HPI actuation signal not available to exactly 1 piece of equipment	5.6 x 10 ⁻⁶
	ILB3	LPI actuation signal not available to exactly 1 piece of equipment	1.0 x 10 ⁻⁷
	ILB4	RBIC actuation signal not available to exactly 1 piece of equipment	1.3 E-6
	ILB5	Reactor building high pressure signal not available to actuate exactly 1 piece of RBSS equipment*	1.2 E-6
	ILS	All RBIC and RBSS equipment does not receive actuation signal*,*** (ILS=ILB2 + ILB5 + IHE1)	1.1 E-4

*The RBSS pumps do not receive an ESAS signal for the B₃ LOCA initiator; however, the spray line injection valves do receive signal.

**The top events for the simplified fault trees, Figures B.6 through B.9, are defined in Table B.5, and quantified in Table B.7.

***The actuation logic circuit for the RBIC is a required part of the actuation logic circuit for the RBSS. Thus, if the RBIC actuation logic circuit fails, the RBSS actuation logic circuit will also fail.

Table B.3 ESAS - System Success Requirements

<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
all	2/3 channels to each equipment	

Table B.5 ESAS - Top Event Definitions

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
ISSa	See below for a equal to 1 or 2	1
ISS1	Non-time delayed HPI actuation signal not available to exactly one piece of equipment (B ₄ LOCA)	1
ISS2	Time delayed HPI actuation signal not available to exactly one piece of equipment (B ₄ LOCA).	1
ISB	HPI actuation signal not available to any HPI equipment (B ₄ LOCA)	
ILBa	See below for a equal to 1, 2, 3, 4 and 5	3
ILB1	Non-time dependent HPI signal not available to exactly one piece of equipment (B ₁ , B ₂ , B ₃ LOCAs)	3
ILB2	Time delayed HPI actuation signal not available to exactly one piece of equipment (B ₁ , B ₂ , B ₃ LOCAs)	3
ILB3	LPI actuation signal not available to exactly one piece of equipment (B ₁ , B ₂ , B ₃ LOCAs)	3
ILB4	RBIC actuation signal not available to exactly one piece of equipment (B ₁ , B ₂ , B ₃ LOCA)	3
ILB5	Reactor building high pressure signal not available to actuate exactly one piece of RBSS equipment (B ₁ , B ₂ , B ₃ LOCAs)	2,3
ILS	All RBIC and RBSS equipment does not receive actuation signal during B ₁ , B ₂ , or B ₃ LOCAs.	2

Table B.5 ESAS - Top Event Definitions

NOTES

- 1 The numerical evaluation is different for ISS1 and ISS2; however, the same tree with top event ISS is used.
- 2 The RBSS pumps do not receive an ESAS actuation signal for the B₃ LOCA initiator; however, the spray line injection valves are actuated (opened).
- 3 The numerical evaluation is different for ILB1, 2, 3, 4, and 5; however, the same tree with top event ILB is used.

Table B.6 ESAS

BOOLEAN EQUATIONS BASED ON SIMPLIFIED FAULT TREES

TOP EVENTS

NOTES

B_4 - LOCA

$$ISS = ISS1 = ISS2 = IA1 + IA2 + IA3$$

$$ISB = IA4 + IA5 + IA6$$

B_1, B_2, B_3 - LOCAs

$$ILB = ILBX = I5 \cdot I6 \cdot I7 + I4 + (IAC1 \cdot IAC2 + IAC1 \cdot IAC3 + IAC2 \cdot IAC3)$$

for $X = 1, 2, 3, 4, 5$

(1)

$$ILS = ILB2 + ILB5 + IHE1$$

(4)

INTERMEDIATE EVENTS

B_4 - LOCA

$$IA1 = I1 \cdot (IC5 + IC6)$$

$$IA2 = I2 \cdot (IC1 + IC2)$$

$$IA3 = I3 \cdot (IC3 + IC4)$$

$$IX = ITDX + IBSX + ICLX + IGLX + IORX$$

for $X = 1, 2, 3$

(2)

$$IA4 = IBS1 \cdot (I10 + I11)$$

$$IA5 = IBS2 \cdot (I11 + I12)$$

$$IA6 = IBS3 \cdot (I10 + I12)$$

$$IX = IBSY + ITDY$$

for $X = 10$ and $Y = 2$, $X = 11$ and $Y = 3$, $X = 12$ and $Y = 1$

(3)

B_1, B_2, B_3 - LOCA

$$I4 = IAC1 \cdot I7 + IAC2 \cdot I6 + IAC3 \cdot I5$$

$$I5 = IC3 + IC4$$

$$I6 = IC1 + IC2$$

$$I7 = IC5 + IC6$$

Table B.6 ESAS

BOOLEAN EQUATIONS BASED ON SIMPLIFIED FAULT TREE

NOTES

- 1 The expression in parenthesis reflects the possible "2-out-of-3" failure combinations.
- 2 For further definition of the parameter "X" see also quantification tables.
- 3 For further definition of the parameters "X" and "Y" see also quantification tables.
- 4 Event IHE1 contributes only to ILB4 and ILB5.

Table B.7 (1/9) Event "ISS1" Quantification (B₄ LOCA, Non Time Delayed)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ISS1		NON-TIME DEPENDENT HPI SIGNAL NOT AVAILABLE TO EXACTLY ONE PIECE OF EQUIPMENT DURING B ₄ LOCA			2.1 E-4			
IA1		CHANNEL 1 OUTPUT RELAY FAILURE COMBINES WITH CHANNEL 2 AND 3 CONTACT FAILURES			7.0 E-5			
IA2		CHANNEL 2 OUTPUT RELAY FAILURE COMBINES WITH CHANNEL 1 AND 3 CONTACT FAILURES			7.0 E-5			
IA3		CHANNEL 3 OUTPUT RELAY FAILURE COMBINES WITH CHANNEL 1 OR CHANNEL 2 CONTACT FAILURES			7.0 E-5			
IAX		CHANNEL X OUTPUT RELAY FAILURE COMBINES WITH CHANNEL Y OR CHANNEL Z CONTACT FAILURES			<u>7.0 E-5</u> ε = 2.1 E-4			
ICY	CH. UA	CHANNEL U/CONTACT A FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10 ⁺ , 10 ⁻		1
ICZ	CH. VB	CHANNEL V/CONTACT B FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10 ⁺ , 10 ⁻		1, 2, 3
IX	CH. X OUTPUT RELAY	REMAINS ENERGIZED			<u>3.9 E-3</u>			1, 2, 3
ITDX	CH. X TRANS-DUCER	FAILS TO HIGH PRESSURE (SHIFT IN CALIBRATION)	3.0 E-5	4	1.8 E-2	10 ⁺ , 10 ⁻		
IBSX	CH. X BISTABLE	FAILS TO TRIP (SET POINT DRAFT)	3.0 E-5	360	1.1 E-2	10 ⁺ , 10 ⁻		
ICLX	CH. X LOGIC	FAILS TO DE-ENERGIZE (2 SWITCHES)	(2)(1.0 E-5)	360	7.2 E-3	3 ⁺ , 3 ⁻		
IGLX	CH. X GROUP LOGIC	FAILS TO DE-ENERGIZE	1.0 E-8	360	3.6 E-6	10 ⁺ , 10 ⁻		
IORX	CH. X OUTPUT RELAY	FAILS ENERGIZED	1.0 E-8	360	3.6 E-6	10 ⁺ , 10 ⁻		
					<u>1.8 E-2</u> ε = 1.8 E-2 η = 7.0 E-5			

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ISS2		TIME DELAYED HPI SIGNAL NOT AVAILABLE TO ONE PIECE OF EQUIPMENT DURING B ₄ LOCA			2.2 E-4			
IA1		CHANNEL 1 OUTPUT RELAY FAILURE COMBINES WITH CHANNEL 2 AND 3 CONTACT FAILURES			7.4 E-5			
IA2		CHANNEL 2 OUTPUT RELAY FAILURE COMBINES WITH CHANNEL 1 AND 3 CONTACT FAILURES			7.4 E-5			
IA3		CHANNEL 3 OUTPUT RELAY FAILURE COMBINES WITH CHANNEL 1 AND 2 CONTACT FAILURES			<u>7.4 E-5</u> =2.2 E-4			
IAX		CHANNEL X OUTPUT RELAY FAILURE COMBINES WITH CHANNEL Y OR CHANNEL Z			7.4 E-5			1
ICY	CH. UA	CHANNEL U/CONTACT A FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10 ⁺ , 10 ⁻		1, 2, 3
ICZ	CH. VB	CHANNEL V/CONTACT B FAILS TO CLOSE	1.0 E-7	1.9 E+4	<u>1.9 E-3</u> =3.9 E-3	10 ⁺ , 10 ⁻		1, 2, 3
IX	CH. X OUTPUT RELAY	REMAINS ENERGIZED			1.9 E-2			
ITDX	CH. X TRANS-DUCER	FAILS TO HIGH PRESSURE (SHIFT IN CALI-BRATION)	3.0 E-5	4	1.2 E-4	10 ⁺ , 10 ⁻		
IBSX	CH. X BISTABLE	FAILS TO TRIP (SET POINT DRIFT)	3.0 E-5	360	1.1 E-2	10 ⁺ , 10 ⁻		
ICLX	CH. X LOGIC	FAILS TO DE-ENERGIZE (2 SWITCHES)	(2)(1.0 E-5)	360	7.2 E-3	3 ⁺ , 3 ⁻		
IGLX	CH. X GROUP LOGIC	FAILS TO DE-ENERGIZE			1.1 E-4			
	1 RELAY COIL	ENERGIZED	1.0 E-8	360	3.6 E-6	10 ⁺ , 10 ⁻		
	2 SETS RELAY CONTACTS	FAILURE OF N.O. CONTACTS TO OPEN	1.0 E-8	360	3.6 E-6	10 ⁺ , 10 ⁻		
	1 RELAY	FAILS TO ENERGIZE	D		<u>1.0 E-4</u> =1.1 E-4	3 ⁺ , 3 ⁻		
					3.7 E-4			
IORX	OUTPUT RELAY	FAILS ENERGIZED			3.6 E-6	10 ⁺ , 10 ⁻		
	1 RELAY COIL	ENERGIZED	1.0 E-8	360				
	1 SET RELAY CONTACTS	FAILURE OF N.O. CONTACTS TO OPEN	1.0 E-8	360	3.6 E-6	10 ⁺ , 10 ⁻		
	1 TIME DELAY	FAILS TO DE-ENERGIZE	1.0 E-6	360	<u>3.6 E-4</u> =3.7 E-4			

Table B.7 (2/9) Event "ISS2" Quantification (B₄ LOCA, Non Time Delayed)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ISB		HPI ACTUATION SIGNAL NOT AVAILABLE TO ANY EQUIPMENT DURING B ₄ LOCA			7.2 E-4			
IA4		BISTABLE FAILURE ON CHANNEL 1 COMBINES WITH ANOTHER CHANNEL FAILURE			2.4 E-4			
IA5		BISTABLE FAILURE ON CHANNEL 2 COMBINES WITH ANOTHER CHANNEL FAILURE			2.4 E-4			
IA6		BISTABLE FAILURE ON CHANNEL 3 COMBINES WITH ANOTHER CHANNEL FAILURE			2.4 E-4			
					$\Sigma=7.2 E-4$			
IAX		BISTABLE FAILURE ON CHANNEL X COMBINES WITH ANOTHER CHANNEL FAILURE			2.4 E-4			4
IBSY		SEE EVENT "ISS" QUANTIFICATION			1.1 E-2	10 ⁺ , 10 ⁻		4
ITDY		SEE EVENT "ISS" QUANTIFICATION			1.2 E-4	10 ⁺ , 10 ⁻		4
IBSZ		SEE EVENT "ISS" QUANTIFICATION			1.1 E-2	10 ⁺ , 10 ⁻		4
ITDZ		SEE EVENT "ISS" QUANTIFICATION			1.2 E-4	10 ⁺ , 10 ⁻		4
					$\Sigma=2.2 E-2$			
IBSU		SEE EVENT "ISS" QUANTIFICATION			1.1 E-2	10 ⁺ , 10 ⁻		
					$\Sigma=2.4 E-4$			

Table B.7 (3/9) Event "ISB" Quantification (B₄ LOCA)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ILB1		NON-TIME DEPENDENT HPI SIGNAL NOT AVAILABLE TO EXACTLY ONE PIECE OF EQUIPMENT DURING B ₁ , B ₂ OR B ₃ LOCA			1.0 E-7			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			
IA8		2-OUT-OF-3 ACTUATION CHANNELS FAIL TO DE-ENERGIZE						
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			$\frac{4.2 \text{ E-8}}{\tau = 1.0 \text{ E-7}}$			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.3 E-8			7
IX		CHANNEL 1 OR 2 CONTACT COMBINATIONS FAIL TO PROVIDE CONTINUITY			3.9 E-3			6
ICY	CH. UA	FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10 ⁺ , 10 ⁻		2, 3, 6
ICZ	CH. VA	FAILS TO CLOSE	1.0 E-7	1.9 E+4	$\frac{1.9 \text{ E-3}}{\tau = 3.9 \text{ E-3}}$	10 ⁺ , 10 ⁻		2, 3, 6
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			4.2 E-8			8
IAC1	1 RELAY COIL	ENERGIZED (ACTUATION CHANNEL 1)	1.0 E-8	360	3.6 E-6			
I7		SEE ABOVE EVENT "IX"			$\frac{3.9 \text{ E-3}}{\tau = 1.4 \text{ E-8}}$			

Table B.7 (4/9) Event ILB1 "Quantification (B₁, B₂ LOCA, Non-Time Dependent)"

Table B.7 (5/9) Event "1LB2" Quantification (B₁, B₂ LOCA, Time Delayed)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
1LB2		TIME DELAYED HPI SIGNAL NOT AVAILABLE TO EXACTLY ONE PIECE OF EQUIPMENT DURING B ₁ , B ₂ OR B ₃ LOCA			5.6 E-6			
1A7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			
1A8		2-OUT-OF-3 ACTUATION CHANNELS FAIL TO DE-ENERGIZE			e			
14		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			5.5 E-6			
					<u>Σ=5.6 E-6</u>			
1A7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			7
1X		CHANNEL 1 OR 2 CONTACT COMBINATIONS FAIL TO PROVIDE CONTINUITY			3.9 E-3			6
1CY	CH. UA	FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10 ⁺ , 10 ⁻		2, 3, 6
1CZ	CH. VB	FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10 ⁺ , 10 ⁻		2, 3, 6
					<u>Σ=3.9 E-3</u>			
14		RELAY CONTACTS 1 IL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			5.5 E-6			8
1AC1		ENERGIZED (ACTUATION CHANNEL 1)			4.7 E-4	10 ⁺ , 10 ⁻		
	2 RELAY COILS	ENERGIZED	1.0 E-8	360	3.6 E-6	10 ⁺ , 10 ⁻		
	2 SETS RELAY CONTACTS	FAILURE OF N.O. CONTACT TO OPEN	1.0 E-8	360	3.6 E-6	10 ⁺ , 10 ⁻		
	1 TIME DELAY	FAILS TO OPERATE	1.0 E-6	360	3.6 E-4	10 ⁺ , 10 ⁻		
	1 RELAY	FAILS TO ENERGIZE	D		1.0 E-4	3 ⁺ , 3 ⁻		
					<u>Σ=4.7 E-4</u>			
17		SEE ABOVE EVENT "1X"			3.9 E-3			
					<u>Σ=1.8 E-6</u>			

B-43

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ILB3		LP1 SIGNAL NOT AVAILABLE TO EXACTLY ONE PIECE OF EQUIPMENT DURING B ₁ , B ₂ OR B ₃ LOCA			1.0 E-7			
IA7		TRIPLE CONTACT FAILURES PERMIT CONTINUITY			5.9 E-8			
IA8		2-OUT-OF-3 ACTUATION CHANNELS FAIL TO DE-ENERGIZE			e			
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			4.2 E-8			
					=1.0 E-7			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			7
IX		CHANNEL 1 OR 2 CONTACT COMBINATIONS FAILS TO PROVIDE CONTINUITY			3.9 E-3			6
ICY	CH. UA	FAILS TO CLOSE	1.0 E-7	1.8 E+5	1.9 E-3	10 ⁺ , 10 ⁻		2, 3, 6
ICZ	CH. VB	FAILS TO CLOSE	1.0 E-7	1.8 E+5	1.9 E-3	10 ⁺ , 10 ⁻		2, 3, 6
					=3.4 E-3			
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			4.2 E-8			8
IAC1	1 RELAY COIL	ENERGIZED (ACTUATION CHANNEL 1)	1.0 E-8	360	3.6 E-6	10 ⁺ , 10 ⁻		
I7		SEE ABOVE EVENT "IX"			3.9 E-3			
					=1.4 E-8			

Table B.7 (6/9) Event "ILB3" Quantification (B₁, B₂ LOCA)

B-45

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
1LB4		RBIC SIGNAL NOT AVAILABLE TO EXACTLY ONE PIECE OF EQUIPMENT DURING B ₁ , B ₂ OR B ₃ LOCA			1.3 E-6			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			
IA8		2-OUT-OF-3 ACTUATION CHANNELS FAIL TO DE-ENERGIZE			e			
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			1.3 E-6			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			$\tau=1.3 E-6$			
IX		CHANNEL 1 OR 2 CONTACT COMBINATIONS FAILS TO PROVIDE CONTINUITY			5.9 E-8			7
ICY	CH. UA	FAILS TO CLOSE	1.0 E-7	1.9 E+4	3.9 E-3			6
ICZ	CH. VB	FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10 ⁺ , 10 ⁻		2, 3, 6
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			1.9 E-3	10 ⁺ , 10 ⁻		2, 3, 6
IAC1		ENERGIZED (ACTUATION CHANNEL 1)			$\tau=3.9 E-3$			
	3 RELAY COILS	ENERGIZED			1.3 E-6			8
	2 SETS RELAY CONTACTS	FAILURE OF N.O. CONTACT TO OPEN	1.0 E-8	360	1.1 E-4			
	1 PRESSURE SWITCH	FAILURE TO ACTUATE	1.0 E-8	360	3.6 E-6			
I7		SEE ABOVE EVENT "IX"	0		1.0 E-4			
					$\tau=1.1 E-4$			
					3.9 E-3			
					$\tau=4.3 E-7$			

Table B.7 (7/9) Event 1LB4" Quantification (B₁, B₂ LOCA)

B-46

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	S. NS.	NOTES
1LB5		REACTOR BURNING HIGH PRESSURE SIGNAL NOT AVAILABLE TO EXACTLY ONE PIECE OF RBSS EQUIPMENT DURING B ₁ , B ₂ OR B ₃ LOCA			1.2 E-6			
1A7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			
1A8		2-OUT-OF-3 ACTUATION CHANNELS FAIL TO DE-ENERGIZE			c			
14		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			1.2 E-6			
					<u>1.2 E-6</u>			
1A7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			7
1X		CHANNEL 1 OR 2 CONTACT COMBINATIONS FAILS TO PROVIDE CONTINUITY			3.9 E-3			6
1CY	CH. UA	FAILS TO CLOSE	1.0 E-7	1.9 E-4	1.9 E-3	10 ⁺ , 10 ⁻		2, 3, 6
1CZ	CH. VB	FAILS TO CLOSE	1.0 E-7	1.9 E-4	1.9 E-3	10 ⁺ , 10 ⁻		2, 3, 6
					<u>3.9 E-3</u>			
14		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			1.2 E-6			8
1AC1	PRESSURE SWITCH	FAILS TO ACTUATE	D		1.0 E-4	10 ⁺ , 10 ⁻		
17		SEE ABOVE EVENT "1X"			3.9 E-3			
					<u>3.9 E-3</u>			

Table B.7 (8/9) Event "1LB5" Quantification (B₁, B₂ LOCA)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ILS		ALL RBIC AND RBSS EQUIPMENT DOES NOT RECEIVE ACTUATION SIGNAL DURING B ₁ , B ₂ OR B ₃ LOCA			1.1 E-4			
ILB5		RB HIGH PRESSURE SIGNAL NOT AVAILABLE TO RBSS EQUIPMENT			1.2 E-6			
ILB2		TIME DELAYED HPI SIGNAL NOT AVAILABLE			5.6 E-6			
THE1	ALL 4 PSI AND 30 PSI PRESSURE SWITCHES	COMMON MODE MISCALIBRATION OF ALL PRESSURE SWITCHES			1.0 E-4 r=1.1 E-4			

Table B.7 (9/9) Event "ILS" Quantification (B₁, B₂ LOCA)

Table B.7 ESAS

QUANTIFICATION TABLES

NOTES

- 1 $X = 1,2,3$; if $X = 1$ then $Y = 5, Z = 6, UA = 2A, VB = 3A$
 $X = 2$ then $Y = 1, Z = 2, UA = 1A, VB = 3B$
 $X = 3$ then $Y = 3, Z = 4, UA = 1B, VB = 2B$

- 2 The failure rate of 1.0 E-7/hour is the lower bound of the failure rate given in Appendix III of WASH-1400. The fault duration time of 27 months (1/2 of once every three refuelings-54 months) is based on a review of plant procedure SP-417. According to this procedure, these relays are tested every refueling (18 months) by closing the contacts in one out of three paths through the actuation matrices. Thus, every three refuelings, all contacts in the actuation matrices are tested.

- 3 For channel and contact identification see Figure B.2

- 4 $X = 4,5,6$; if $X = 4$ then $Y = 2, Z = 3, U = 1$
 $X = 5$ then $Y = 1, Z = 3, U = 2$
 $X = 6$ then $Y = 1, Z = 2, U = 3$

- 5 Failure of one channel is $(1 \cdot \text{E-}8/\text{hr}) (360 \text{ hrs}) =$
 $= 3.6 \text{E-}6$; therefore 2-out-of-3 is approximately ϵ .

- 6 $X = 5,6,7$; if $X = 5$ then $Y = 3, Z = 4, UA = 1B, VB = 2B$
 $X = 6$ then $Y = 1, Z = 2, UA = 1A, VB = 3B$
 $X = 7$ then $Y = 5, Z = 6, UA = 2A, VB = 3A$

- 7 $IA7 = I5 \cdot I6 \cdot I7$

- 8 $I4 = IAC1 \cdot I7 + IAC2 \cdot I6 + IAC3 \cdot I5$; where
 $IAC1 = IAC2 = IAC3$ and $I5 = I6 = I7$
 therefore $p(I4)$ was assessed equal to
 $(3)p(IAC1) \cdot p(I7)$

Table B.8 ESAS - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
ISS1	2.1 x E-4
ISS2	2.2 x E-4
ISB	7.2 x E-4
ILB1	1.0 x E-7
ILB2	5.6 x E-6
ILB3	1.0 x E-7
ILB4	1.3 E-6
ILB5	1.2 E-6
ILS	1.1 E-4

APPENDIX C

DC POWER SYSTEM

APPENDIX C DC POWER SYSTEM

C.1 SYSTEM DESCRIPTION AND OPERATION

The DC power system (DCPS), which consists of two isolated buses, provides a continuous source of 250V and 125V DC power for DC pump motors, control, and instrumentation.

The 250V supply provides power to the DC pump motors and certain motor operated valves. The 125V supply provides power for control and instrumentation functions.

C.1.1 SYSTEM DESCRIPTION

Figure C.1 shows a simplified schematic diagram of the CR-3 DC power system.

The DCPS consists of two separate and independent 250/125V DC supplies, each of which includes a battery and associated battery chargers and DC distribution panels.

Each 250/125V DC supply includes two 125V batteries wired to produce one 250V source and two 125V sources. A battery charger is provided for each 125V battery section. A spare charger is also provided as backup to the primary chargers and its output may be fed to either of the 125V battery sections.

DC power from each 250/125V supply is distributed to the various user equipment via distribution panels including a main panel and seven individual panels. The outputs of the batteries and chargers are fed to the main panel where the DC power is, in turn, fed to the individual panels for distribution to the user equipments. The vital inverters are fed directly from the main panel.

Each battery charger is sized to continuously deliver 200 amperes to its associated battery section at 125VDC. Input power to the chargers consists of 480VAC, 1Ø from motor control centers. MCC3A-1 feeds chargers A, C and E (spare) which serve 250/125VDC supply 3A and MCC3B-2 feeds

chargers B, D and F (spare) which serve 250/125VDC supply 3B. Switches are provided at the input and output of each charger to permit off-line test and maintenance. In addition, fuses at the input and output of each charger provide overload protection.

Each 125V battery section consists of 58 cells rated at 2.2 volts/cell minimum. The capacity of each 250/125V battery supply provides the capability to deliver the loads listed in Tables C.1 and C.2 continuously for two hours and perform three complete cycles of safeguards breaker closures with subsequent tripping (1020 ampere-hours).

The distribution panels consist of switches, fuses and associated wiring for DC power distribution. The switches provide the capability for on-line checkout of user equipment as well as general maintenance and checkout of various elements of the DC system by permitting disconnection from power. The fuses provide overload protection for the DC supply and user equipment.

C.1.2 SYSTEM OPERATION

During normal plant operation the battery chargers supply the normal DC loads while maintaining float charge on the batteries. In the event of loss of AC input to the chargers the batteries will automatically supply the required DC loads.

A high and low voltage alarm is provided in the control room via high/low voltage relay contact closures. The high alarm is set at 137VDC to protect against battery overcharging during normal plant operation. The low voltage alarm is set at 210VDC for DC motor bus voltage and 121VDC for instrumentation and control bus voltage.

Battery discharge is monitored by contact making ammeters located in the main DC panels. This provides a remote alarm when the battery is supplying power to the user equipments.

In the event that a primary charger becomes unavailable due to malfunction, test or maintenance the spare charger is manually switched on-line. This will maintain the float charge on the battery section and supply the DC loads associated with the unavailable charger.

BATTERY TEST AND MAINTENANCE

The individual 125 volt battery sections are given the following tests and inspections:

- (a) The voltage, specific gravity and electrolyte level of each cell are measured once each quarter.
- (b) During refueling each battery is inspected for physical damage and integrity of intercell connections.
- (c) Battery discharge is monitored continually via the contact making ammeters.
- (d) Maintenance is performed on the batteries as required to correct for defects.

BATTERY CHARGER TEST AND MAINTENANCE

The individual battery chargers are given the following tests and inspections:

- (a) During refueling each charger is demonstrated to be operable via an eight hour load test.
- (b) Maintenance is performed on the chargers as required to correct for defects. During maintenance the defective charger is taken off-line and replaced by the spare charger.
- (c) Charger performance is continually monitored via high/low voltage alarms in the control room.

Table C.1 Battery 3A Loads (DC unavailable) from CR-3 FSAR

Load Description	Volts	Hp/KVA	Cycle Time(min.)	No. of Breakers
Feedwater Pump 3B Turbine Emergency Oil Pump	250	5 Hp	0-10	
Feedwater Booster Pump 3B Emergency Oil Pump	250	5 Hp	0-10	
Reactor Coolant Pump DC Oil Lift Pump	250	3 Hp	0-60	
Reactor Coolant Pump DC Oil Lift Pump	250	3 Hp	0-60	
Turbine Generator Air Side Seal Oil Pump	250	25 Hp	60-120	
Emergency Diesel Generator Fuel Transfer Pump	250	1 Hp	1-20	
Makeup Pump 3B Lube Oil Pump	250	1 Hp	0-20	
Makeup Pump 3C Lube Oil Pump	250	1 Hp	0-20	
Motor Driven Pump to Hotwell Isolation Valve	250	.09 Hp	10-11	
Auxiliary Feedwater Pump Turbine Steam Supply Isolation Valve	250	1.81 Hp	10-11	
Alterrex Excitation Cabinet	125	6.25 Hp	0-120	
Feedwater Pump 3B Turbine Motor Speed Changer	125	1/6 Hp	0-10	
6900 Volt Switchgear 3B Control	125	*		3
4160 Volt Switchgear 3B Control	125	*		10
4160 Volt Engineered Safeguards Switchgear 3B Control	125	*		10
480 Volt Reactor Auxiliary Bus 3B Control	125	*		2
480 Volt Turbine Auxiliary Bus 3B Control	125	*		7
480 Volt Intake Auxiliary Bus 3B Control	125	*		4
480 Volt Engineered Safeguards Bus 3B Control	125	*		3
Inverter 3B	125	15 KVA	0-120	
Inverter 3D	125	15 KVA	0-120	
Inverter 3E	125	15 KVA	0-120	
Control Room Panels	125	1.25 KVA	0-120	
Hydrogen Panel	125	.625 KVA	0-120	
Engineered Safeguards Channel 3B Cabinets	125	.625 KVA	0-120	
Relay Racks	125	12.5 KVA	0-120	
Engineered Safeguards Actuation 3B Cabinets	125	.625 KVA	0-120	
Emergency Lighting	125	1.25 KVA	0-120	
Substation Loads	125	7.5 KVA	0-120	
Miscellaneous Cabinets	125	1.25 KVA	0-120	

*Power Required to trip breakers as listed (10 amps/breaker for one minute).

Table C.2 Battery 3B Loads (AC unavailable) from CR-3 FSAR

<u>Load Description</u>	<u>Volts</u>	<u>Hp/KVA</u>	<u>Cycle Time(min.)</u>	<u>No. of Breakers</u>
Turbine Emergency Bearing Oil Pump	250	60 Hp	10-60	
Feedwater Pump 3A Turbine Emergency Oil Pump	250	5 Hp	0-10	
Feedwater Booster Pump 3A Emergency Oil Pump	250	5 Hp	0-10	
Reactor Coolant Pump DC Oil Lift Pump	250	3 Hp	0-60	
Reactor Coolant Pump DC Oil Lift Pump	250	3 Hp	0-60	
Emergency Diesel Generator Fuel Transfer Pump	250	1 Hp	1-20	
Makeup Pump 3A Lube Oil Pump	250	1 Hp	0-20	
Makeup Pump 3B Lube Oil Pump	250	1 Hp	0-20	
Vacuum Breaker	250	.135 Hp	0-10	
Turbine Driven Emergency Feedwater Pump to Hotwell Isolation Valve	250	.09 Hp	10-11	
Auxiliary Feedwater Pump Turbine Steam Supply Isolation Valve	250	1.81 Hp	10-11	
Turbine Thrust Bearing Wear Detector Motor	125	.05 Hp	0-10	
EHC Cabinet	125	1 KVA	0-120	
Feedwater Pump Turbine Speed Changer	125	.166 Hp	0-10	
6900 Volt Switchgear 3A Control	125	*		3
4160 Volt Switchgear 3A Control	125	*		10
4160 Volt Engineered Safeguard Switchgear 3A Control	125	*		10
480 Volt Plant Auxiliary Bus 3 Control	125	*		-
480 Volt Reactor Auxiliary Bus 3A Control	125	*		2
480 Volt Turbine Auxiliary Bus 3A Control	125	*		7
480 Volt Heating Auxiliary Bus 3 Control	125	*		-
480 Volt Intake Auxiliary Bus 3A Control	125	*		4
480 Volt Engineered Safeguards Bus 3A Control	125	*		3
Inverter 3A	125	15 KVA	0-120	
Inverter 3C	125	15 KVA	0-120	
Condensate Demineralizer Control Panel	125	.625 KVA	0-120	
Instrument Repair Shop Receptacles	125	.625 KVA	0-120	
Engineered Safeguards Channel 3A Cabinets	125	.625 KVA	0-120	
Engineered Safeguards Actuation 3A Cabinets	125	.625 KVA	0-120	
Relay Racks	125	12.5 KVA	0-120	
Substation Loads	125	7.5 KVA	0-120	
Emergency Lighting	125	1.25 KVA	0-120	

* Power required to trip breakers as listed (10 amps/breaker for one minute).

C-7

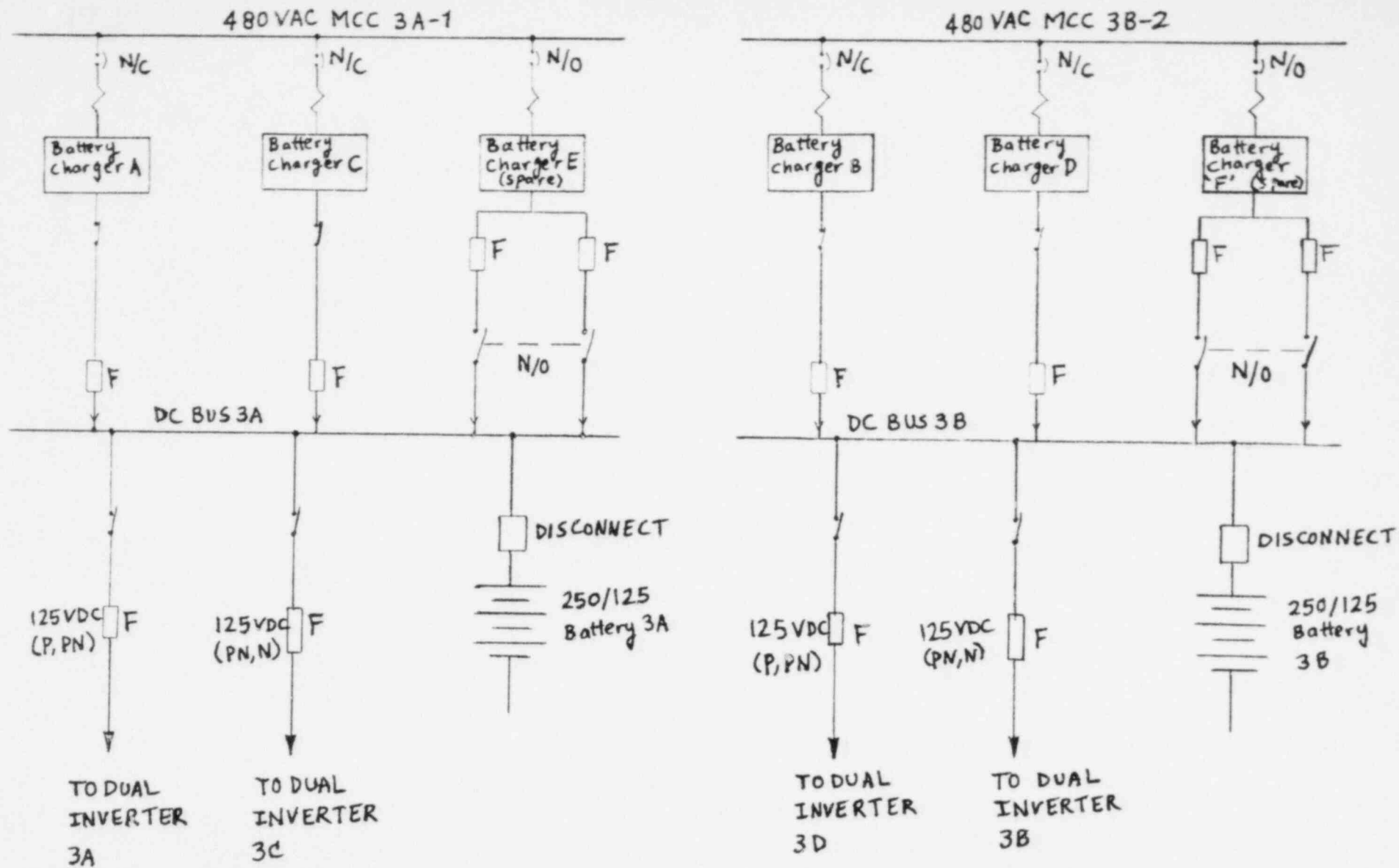


Figure C.1 DC Power System One Line Diagram

C.2 SYSTEM SIMPLIFIED FAULT TREE

The DCPS fault tree analysis consisted of developing trees which would serve as sub-trees (i.e., plug in modules) for the fault trees which were developed for the various systems that require DC power during normal plant operation and accident conditions including transients and loss of coolant accidents. Accordingly, fault trees were developed to identify the hardware and human failures which could inhibit the distribution of DC power from the individual DC panels to the associated systems.

TOP EVENT DEFINITION

The undesired event for which the DCPS fault trees were developed was:

"Insufficient Power at DC Panel DPDP-XX"

where: DPDP-XX represents the DC distribution panel associated with the particular system for which DC power was required.

ASSUMPTIONS

The underlying assumptions governing the development of the DCPS fault trees include:

1. Insufficient DC power is defined as loss of either of the 125VDC supplies provided by a 125VDC battery section and the associated charger.
2. Hardware failures, such as circuit breaker, switch or fuse failing open, are not immediately repairable. The failed hardware must be replaced in order to place the associated circuit back on-line.
3. The down time resulting from failures such as inadvertent switch opening or failure to re-close a switch is a function of detectability; i.e., DC system alarms and user equipment monitoring features.
4. Calibration failures such as mis-setting of one or more charges result in a down time after detection equal to the initial calibration period. Further, calibration errors are assumed detectable after associated equipment is placed on-line.

The simplified fault trees for the DCPS are presented in Figure C.2, sheets 1 through 15. Notes to the simplified fault trees are in Table C.3.

Table C.3 (1/4) Fault Tree Notes

GENERAL NOTES

- (a) High and Low voltage alarm is provided in the control room for each of the six chargers employed for the two DC buses.
 - o High alarm set point = 137VDC
 - o Low alarm set point = 121VDC
- (b) Reactor shall not be made critical unless both 250/125 volt DC supplies (bus 3A and 3B) are energized.
- (c) During power operation one of the two 250/125 volt DC supplies may not be out of service for more than two hours.
- (d) Charging current and load on each of the buses (3A&3B) are checked each shift.
- (e) Battery discharge is monitored each shift by contact making ammeters located in each of the main DC panels (DPDP-1A&-1B).
- (f) Voltage, specific gravity and electrolyte level of each battery cell are measured once each quarter. Pilot cells are checked weekly.
- (g) Maintenance is performed on the batteries and chargers as required to correct for defects.
- (h) During refueling each charger is demonstrated to be operable via an eight hour load test.
- (i) Plant batteries are of the lead-calcium type.

Table C.3 (2/4) Fault Tree Notes

SPECIFIC NOTES

- (1) Unless all equipment obtaining DC from a particular panel were on standby the likelihood is believed low that the panel input switch would be opened for maintenance on associated equipment. Most likely individual switches in the panel would be used to disable DC to equipment for maintenance.
- (2) Those malfunctions would be immediately detected since operating systems would be disabled.
 - If all equipment obtaining DC from the disabled panel are on standby then malfunction could go undetected until demand for the equipment occurred.
 - Elapsed time to affect repairs depends on time to detect cause of DC loss and time to place switch in proper position.
- (3) These malfunctions would have same effect as (2) above. A longer time would be required to affect repairs since failed hardware would have to be repaired or replaced.
- (4) This malfunction causes loss of all DC from the associated 250/125VDC supply resulting in disabling of all equipment powered by this supply. Down time for the supply would be a function of time to detection and repair time.

Table C.3 (3/4) Fault Tree Notes

BATTERY CHARGER - NOTE 1

- Since work on a charger requires that it be disconnected from the DC bus, maintenance personnel may leave the switch, which disconnects charger from bus, in the "off" position. However, when work is being done on a charger a spare charger is switched on line. After work is completed the original charger might not be placed back on line even though spare charger has been disconnected.
- This condition can be discovered during daily check of charging voltage and/or charging current. During the time a battery is not on float charge, loads (DC) will be supplied directly by the battery (instead of by the charger) causing degradation in battery capability. This event will usually occur, if at all, during normal plant operation.

DC DISTRIBUTION PANELS

-
- NOTES:
1. DC distribution panels consist of cabling and switches for applying DC to various user equipment. Maintenance personnel can inadvertently open a switch thereby removing the DC power from the associated user equipment.
 2. If a particular component requires DC for its operation and Test and/or maintenance requires removal of DC power, maintenance personnel may fail to restore power.

Table C.3 (4/4) Fault Tree Notes

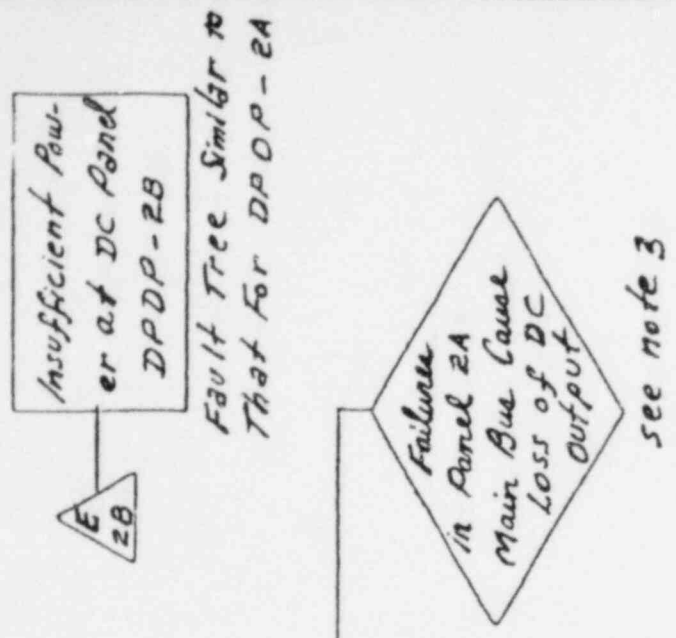
BATTERY

NOTE 1

- Batteries are housed in rooms requiring ventilation to prevent build-up of hydrogen which develops during float charging. Loss of ventilation can cause batteries to fail or degrade and possibly a significant (explosive) mixture of hydrogen can develop if charging continues after loss of ventilation.

NOTE 2

- During equalizing charge excess voltage may be applied. This can severely damage battery.
- During tests for grounds (system is ungrounded) all or part of the battery may be taken off line (momentarily).
- Too much electrolyte can be added.
- Cells may be "jumpered" for T&M and jumper may not be removed. This has the effects of degrading battery capability.



Insufficient Power at DC Panel DDDP-2A

E 2A

Fault Tree Similar to That For DDDP-2A

Insufficient Power at Main Panel DDDP-1A

E 1A

From sheet 10

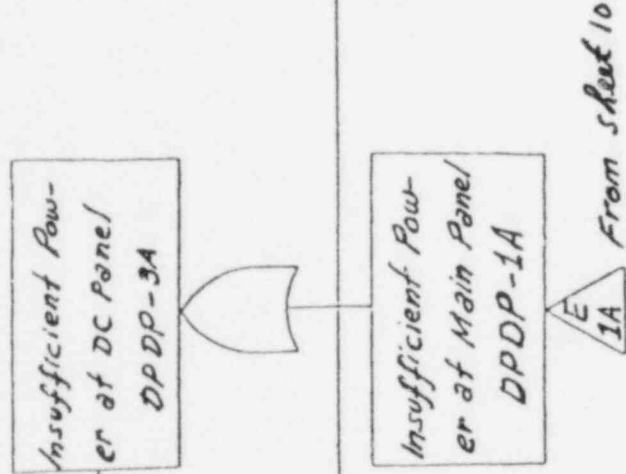
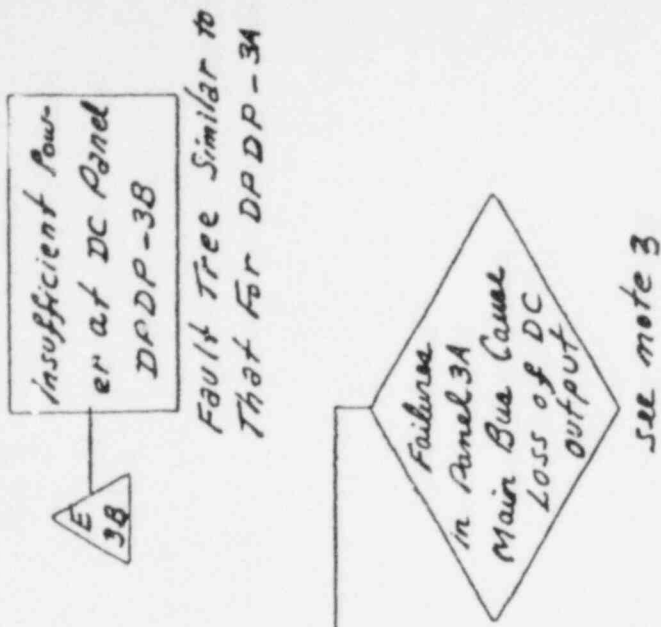
Loss of DC Input to Panel DDDP-2A

Failure in Panel 2A Main Bus Cause Loss of DC Output

see note 3

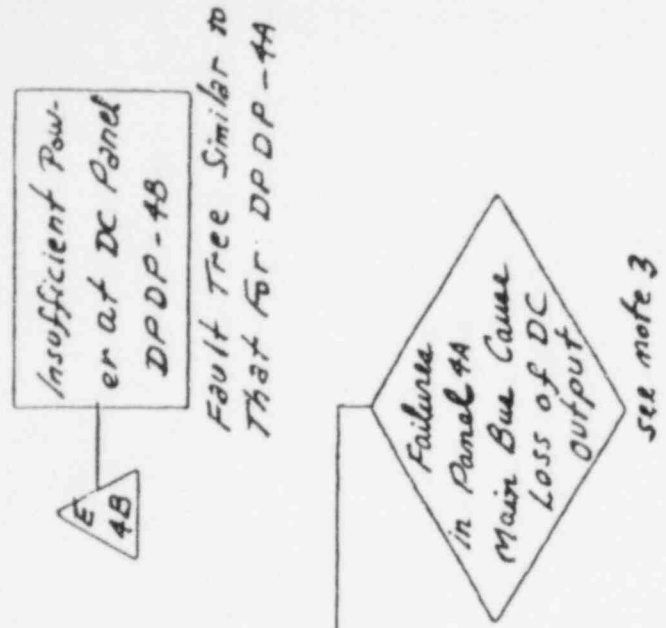
- panel 1A output switch to panel 2A fails open - see note 3
- Operator fails to re-close panel 1A output switch after TOM - see note 1
- Operator inadvertently opens panel 1A output switch - see note 2
- panel 1A output fuse to panel 2A fails open - see note 3
- Failure in cable DPE-11 cause loss of DC input - see note 3

Figure C.2 (1/15) Simplified Fault Tree DC Power System, Events "E2A" and "E2B"



- panel 1A output switch to panel 3A fails open - see note 3
- Operator fails to re-close panel 1A output switch after TOM - see note 1
- Operator inadvertently opens panel 1A output switch - see note 2
- panel 1A output fuse to panel 3A fails open - see note 3
- Failure in cable DPE-10 causes loss of DC input - see note 3

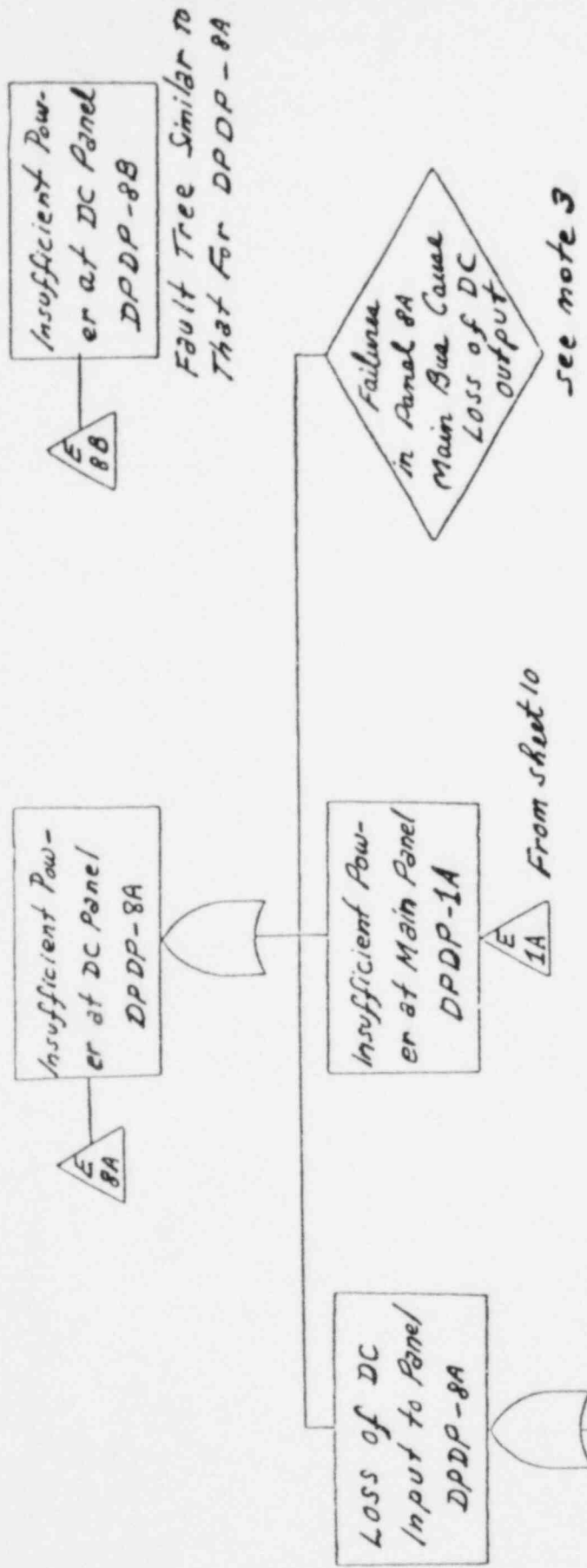
Figure C.2 (2/15) Simplified Fault Tree DC Power System, Events "E3A" and "E3B"



Insufficient Power at DC Panel DPDP-4A
Fault Tree Similar to That for DPDP-4A

- panel 1A output switch to panel 4A fails open - see note 3
- Operator fails to re-close panel 1A output switch after TOM - see note 1
- Operator inadvertently opens panel 1A output switch - see note 2
- panel 1A output fuse to panel 4A fails open - see note 3
- Failures in cable DPE-17 cause loss of DC input - see note 3

Figure C.2 (3/15) Simplified Fault Tree DC Power System, Events "E4A" and "E4B"



C-16

- panel 1A Output switch to panel 8A Fail Open - see note 3
- Operator Fails To Re-close Panel 1A Output Switch After T&M - see note 1
- Operator Inadvertently Opens panel 1A Output switch - see note 2
- panel 1A Output Fuse to panel 8A Fails Open - see note 3
- Failure in Cab & DPE-74 Cause loss of DC Input - see note 3

Figure C.2 (4/15) Simplified Fault Tree DC Power System.

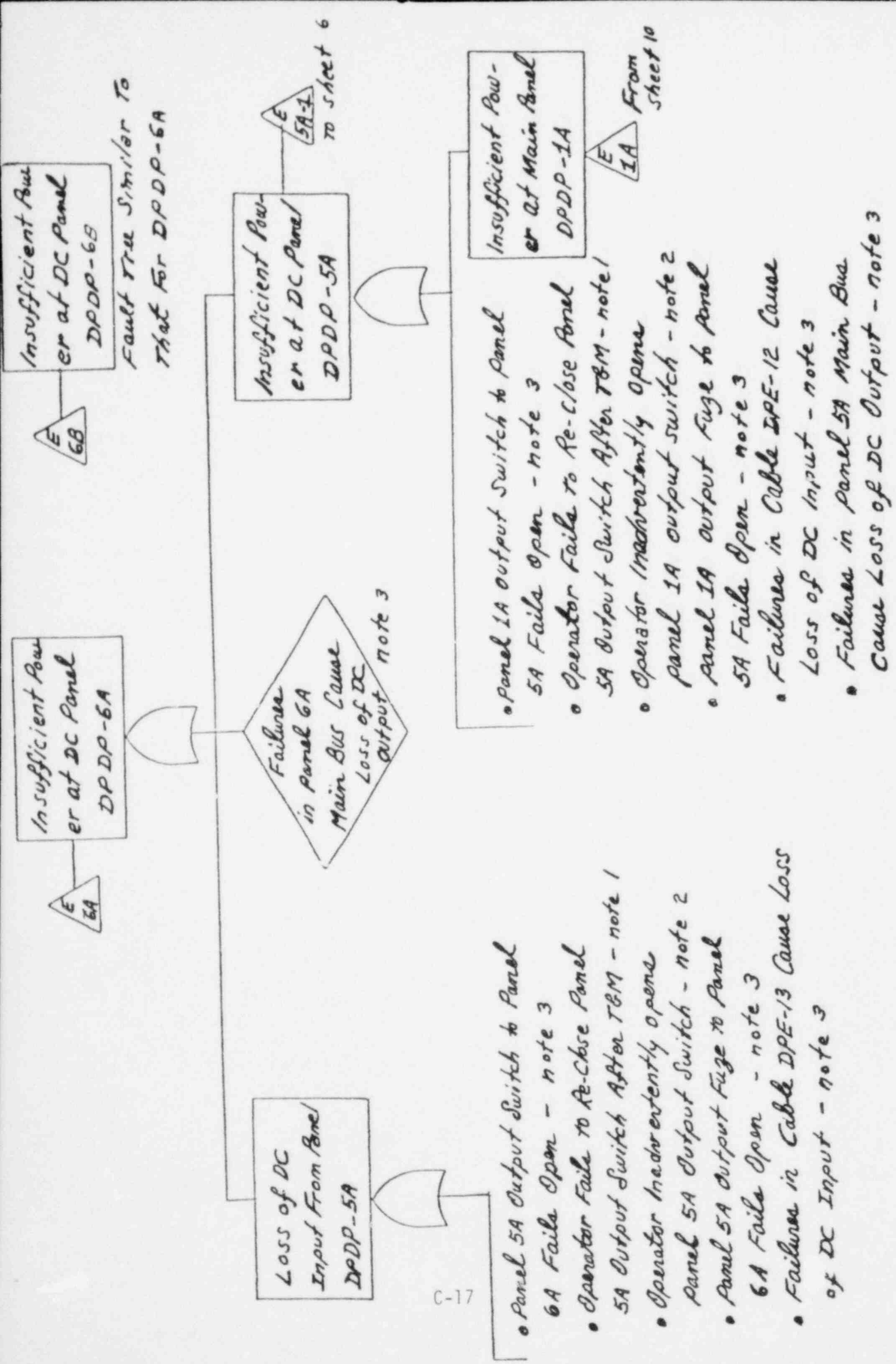
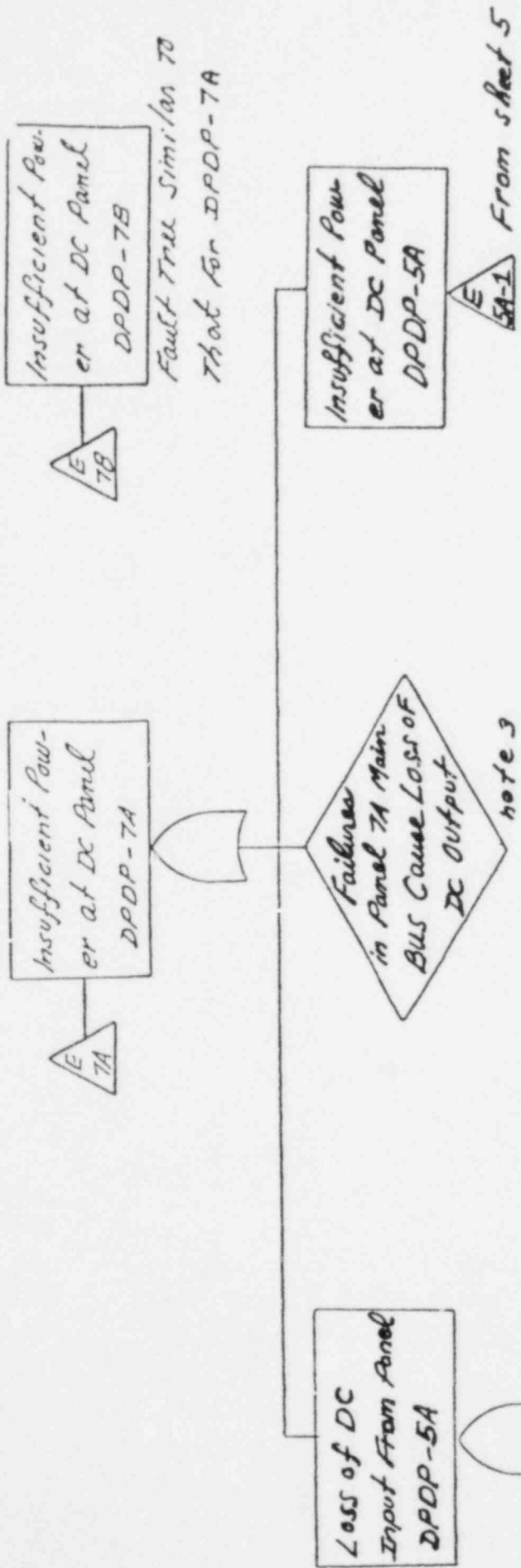


Figure C.2 (5/15) Simplified Fault Tree DC Power System, Events "E6A" and "E6B"



- Panel 5A Output Switch to panel 7A fails open - note 3
- Operator fails to re-close panel 5A output switch after TEM - note 1
- Operator inadvertently opens panel 5A output switch - note 2
- Panel 5A output fuse fails open - note 3
- Failures in cable DPE-14 cause loss of DC input - note 3

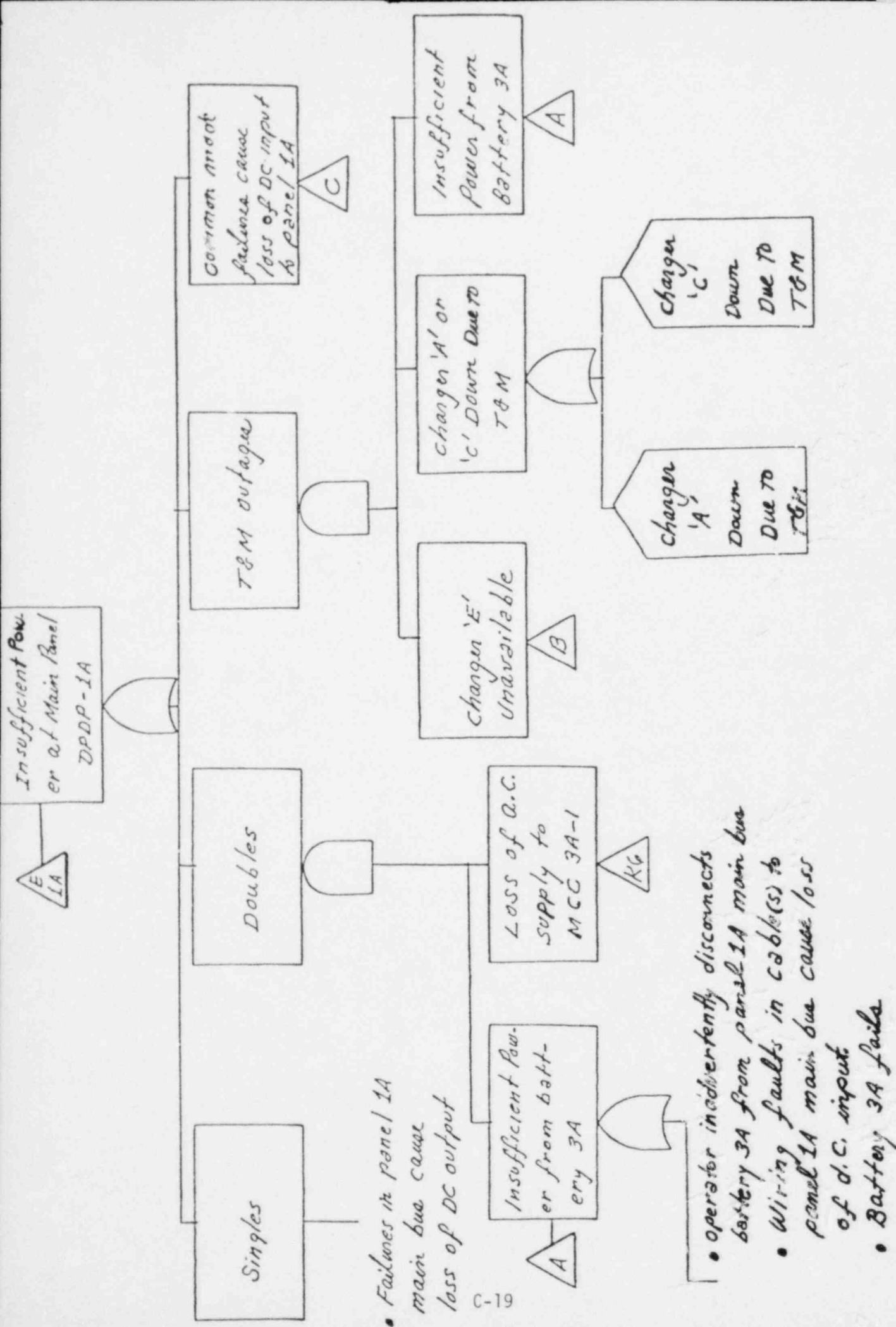
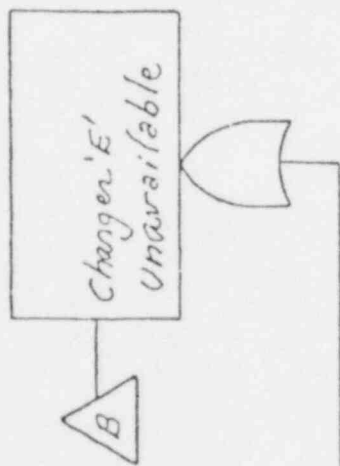


Figure C.2 (7/15) Simplified Fault Tree DC Power System, Event "E1A"



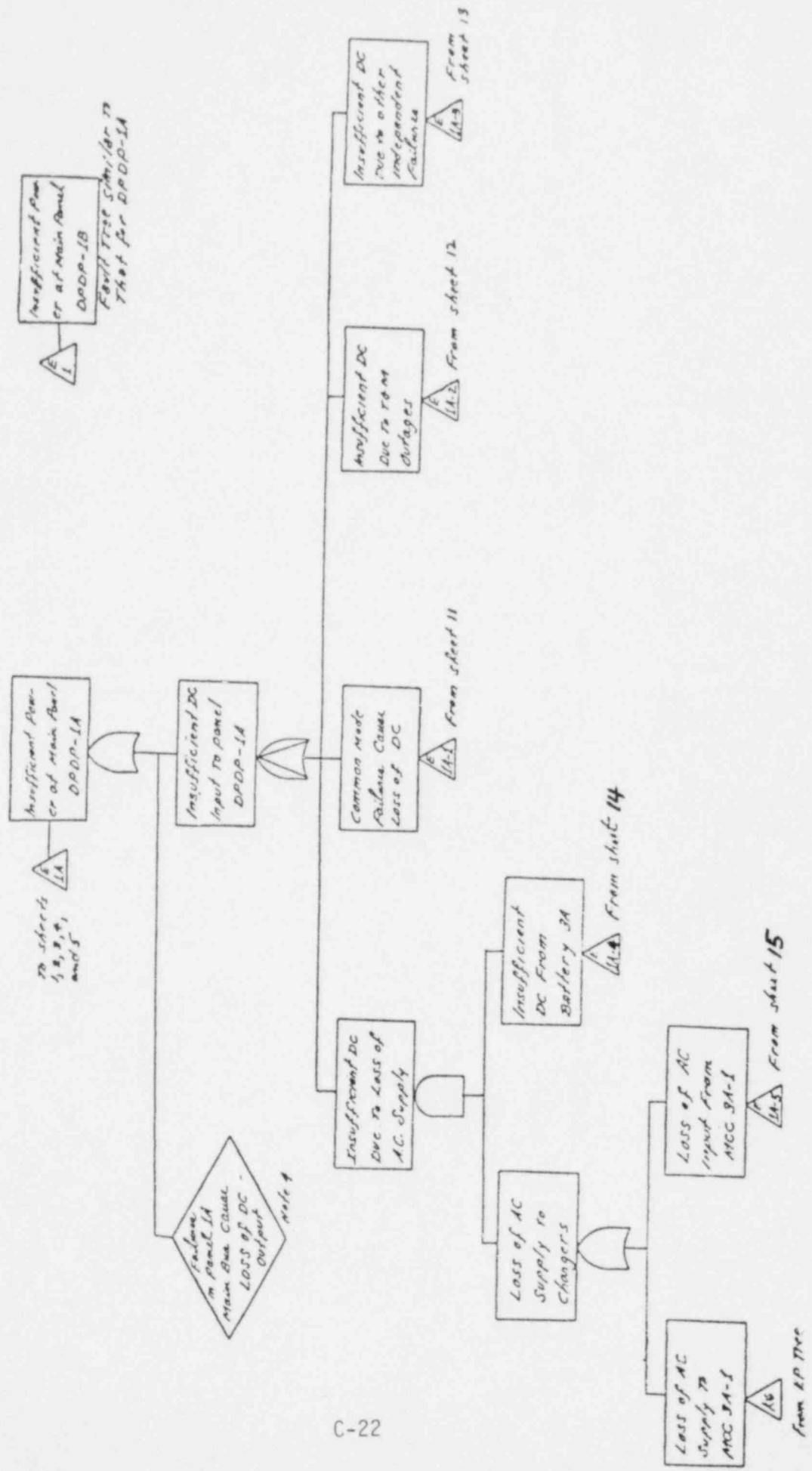
- Input CB from MCC 3A-1 fails open
- Charger fails
- panel 1A input switch to charger fails open
- panel 1A input fuse to charger fails open
- Failure in cable DPC-3 (input cable) cause loss of A.C. input
- Failure in cable DPE-9 (output cable) cause loss of D.C. output
- Operator fails to close panel 1A input switch to charger
- Incorrect charging level set by operator
 - low level results in low bus voltage to battery section
 - high level results in charger trip-off

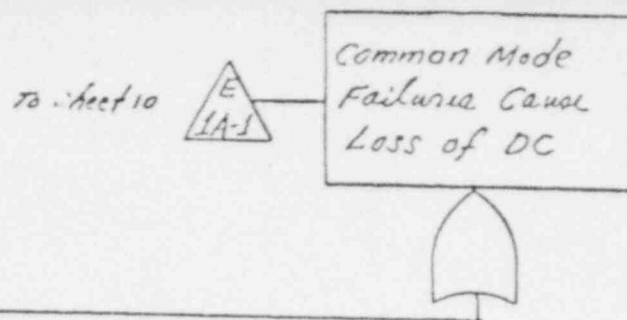
Common Mode
Failure Cause
Loss of DC

C



- Operator inadvertently deenergizes main bus in panel 1A
- Loss of d.c. due to low charging level - Low voltage on main bus in panel 1A
 - Low Charging Level on all Chargers set by Operator
 - Low battery voltage due to low charging level
 - Low charging level (voltage and current) monitored
- Loss of d.c. due to high charging level - No d.c. on main bus in panel 1A
 - High Charging Level on all chargers set by operator
 - Battery fails due to high charging level
 - High charging level (voltage and current) monitored
 - Chargers trip off due to high charging level
- Loss of d.c. due to ventilation system failure
 - Battery failure due to loss of ventilation
 - Chargers trip off due to battery overload
 - ventilation and battery failure undetected before charger trip-off
- Common mode piece-part, material, design or manufacturing defects
 - cause all chargers or battery to fail
 - Battery failure causes charger trip-off due to overload
 - Charger failure causes battery damage

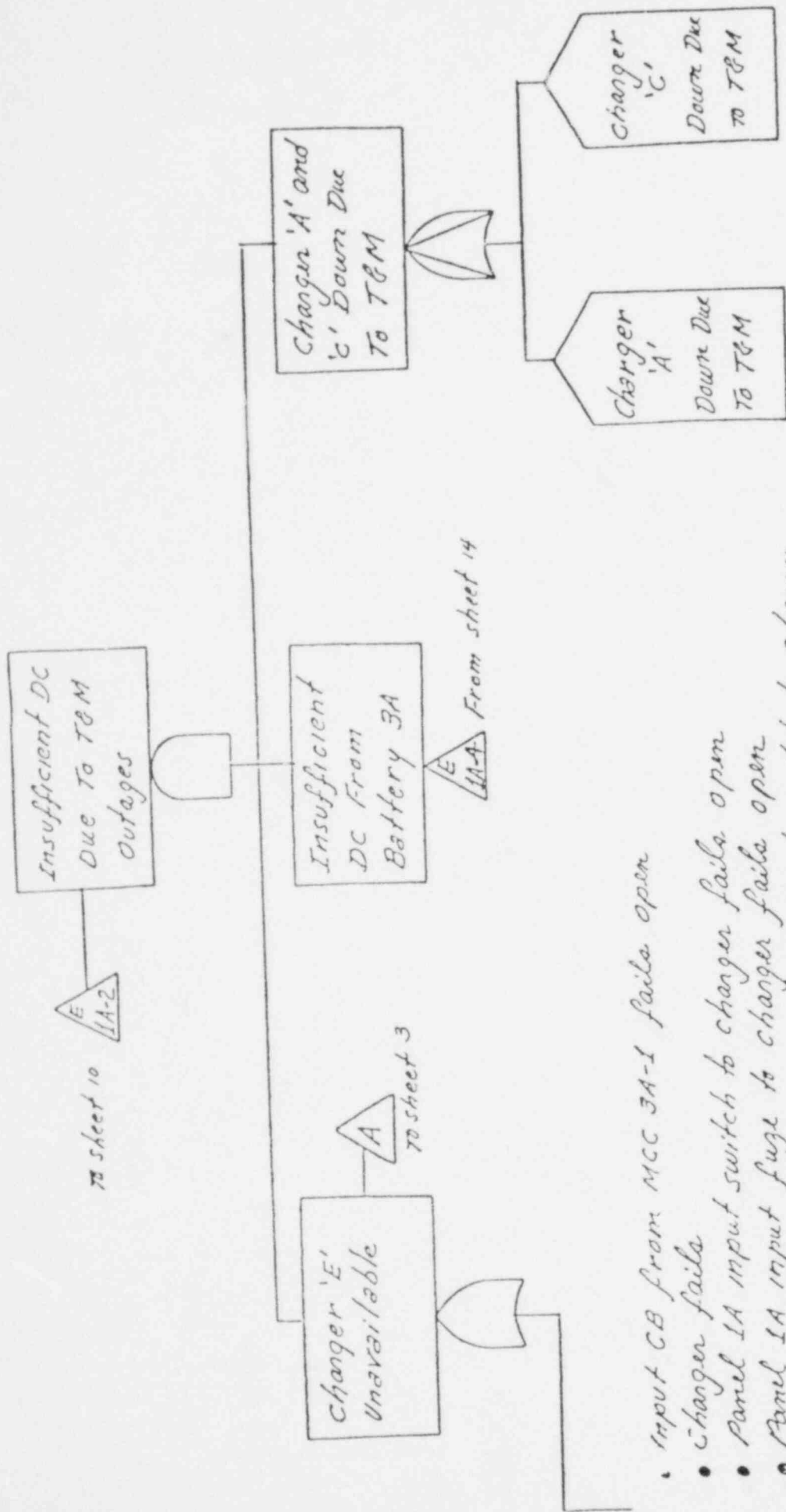




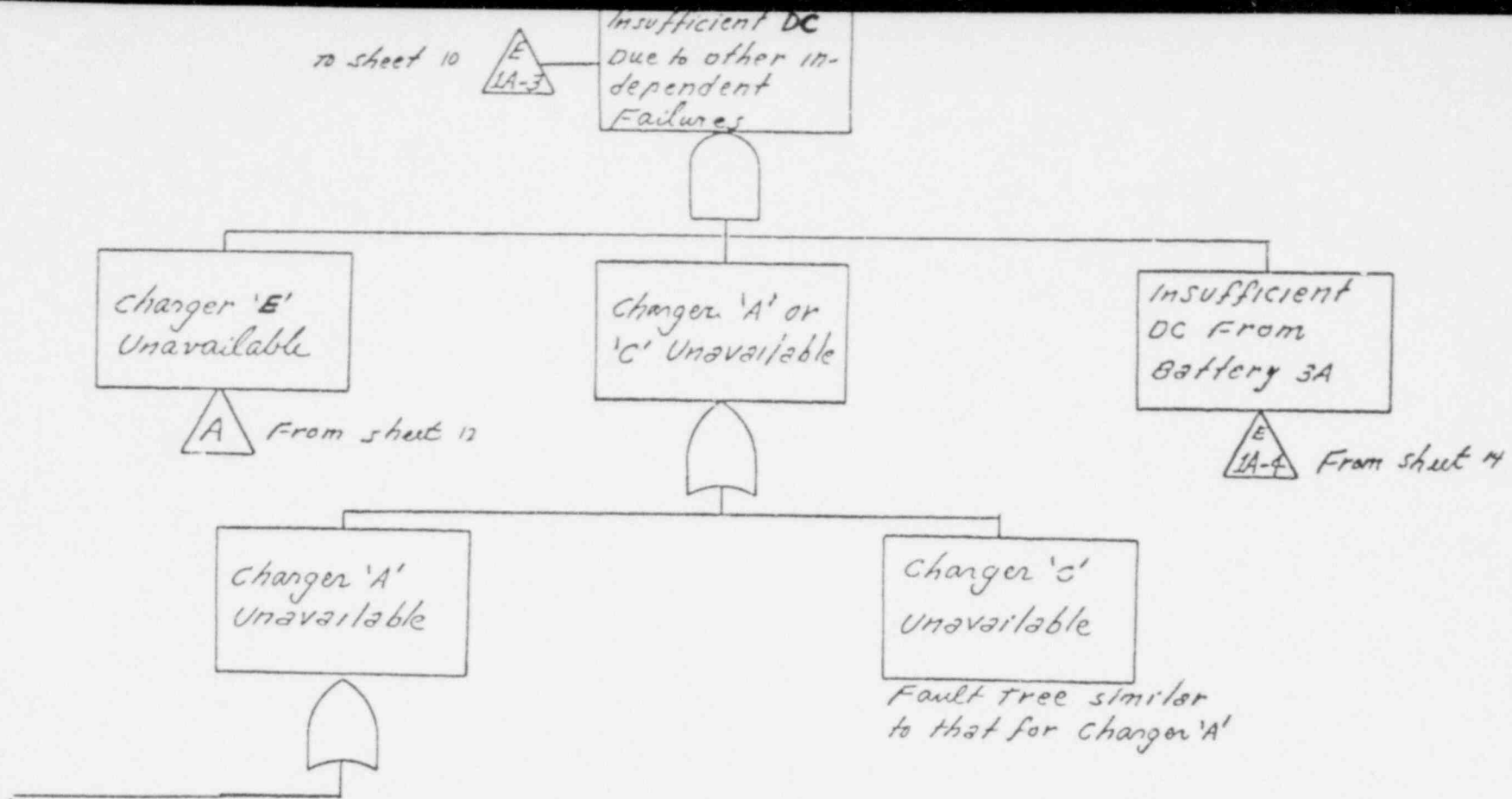
- Operator inadvertently deenergizes main bus in panel 1A
- Loss of d.c. due to low charging level - Low voltage on main bus in panel 1A
 - Low Charging Level on all chargers set by operator
 - Low battery voltage due to low charging level
 - Low charging level (voltage and current) monitored
- Loss of d.c. due to high charging level - No d.c. on main bus in panel 1A
 - High Charging Level on all chargers set by operator
 - Battery fails due to high charging level
 - High charging level (voltage and current) monitored
 - Chargers trip off due to high charging level
- Loss of d.c. due to ventilation system failure
 - Battery failure due to loss of ventilation
 - Chargers trip off due to battery overload
 - ventilation and battery failure undetected before charger trip-off
- Common mode piece-part, material, design or manufacturing defects cause all chargers or battery to fail
 - Battery failure causes charger trip-off due to overload
 - Charger failure causes battery damage

C-23

Figure C.2 (11/15) Simplified Fault Tree DC Power System, Event "E1A-1"



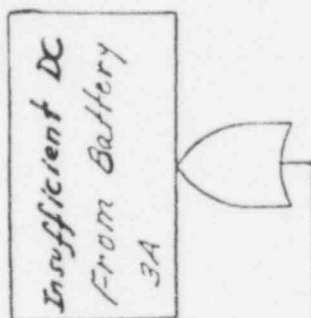
- Input CB from MCC 3A-1 fails to open
- Charger fails
- Panel IA input switch to charger fails open
- Panel IA input fuse to charger fails open
- Operator fails to close panel IA input switch to charger
- Incorrect charging level set by operator
 - Low level results in charger trip off
 - High level results in charger trip off
- Failures in cable DPC-3 cause loss of a.c. input to charger
- Failures in cable DPE-9 cause loss of d.c. input to panel IA



- Input CB from MCC 3A-1 fails open
- Charger fails
- Panel 1A input switch to charger fails open
- Panel 1A input fuse to charger fails open
- Operator fails to re-close input CB or panel 1A input switch after TBM
- Operator inadvertently opens input CB or panel 1A input switch
- Incorrect charging level set by operator
 - low level results in low bus voltage
 - high level results in charger trip-off

- Failures in cable DPC-1 cause loss of A.C. input to charger
- Failures in cable DPE-7 cause loss of d.c. output to panel 1A

Figure C.2 (13/15) Simplified Fault Tree DC Power System, Event "E1A-3"



- Operator inadvertently disconnects battery from Panel IA main bus
- Wiring faults in cables to panel IA cause loss of battery input
- Battery 3A fails

Figure C.2 (14/15) Simplified Fault Tree DC Power System, Event "EIA-4"

C-27

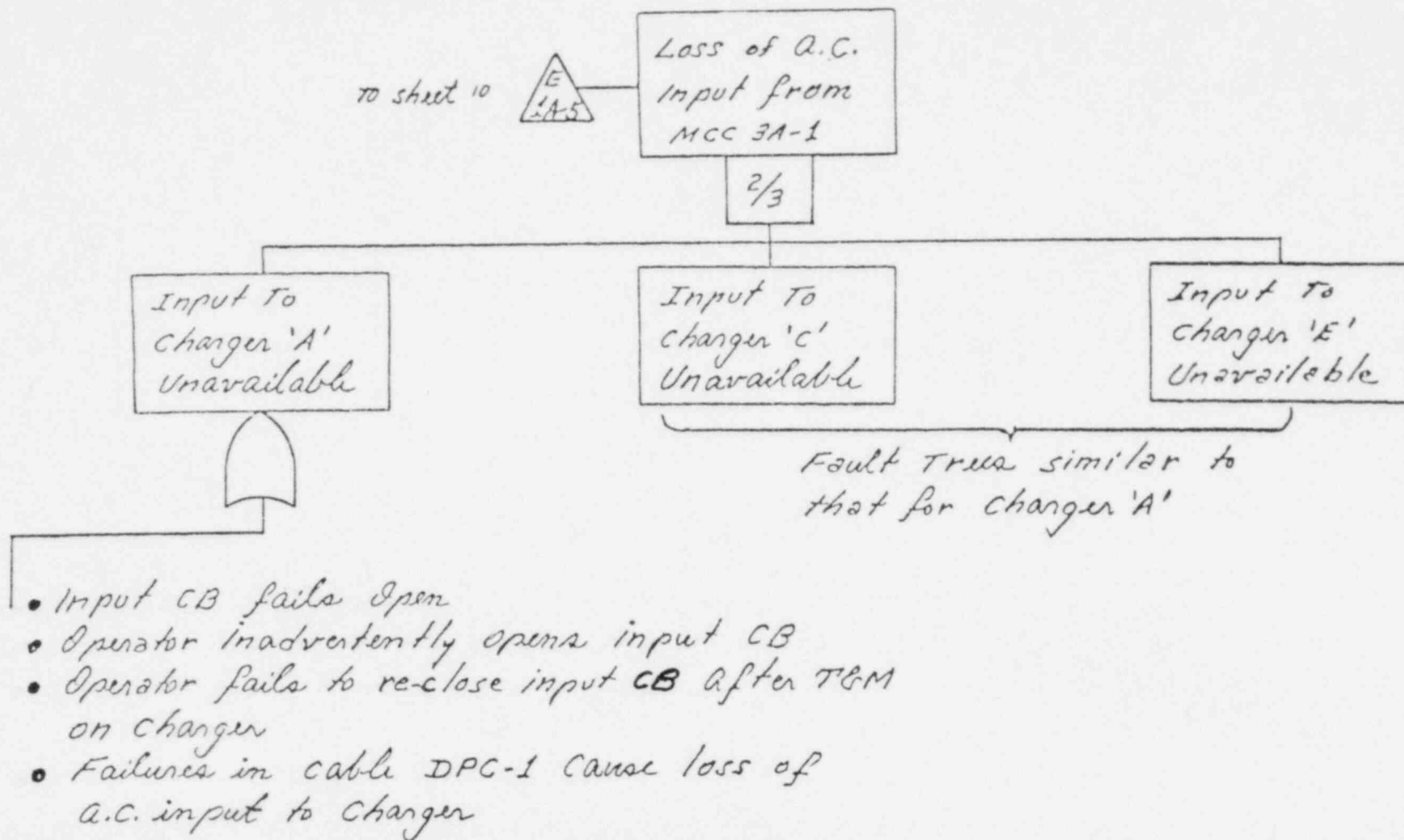


Figure C.2 (15/15) Simplified Fault Tree DC Power System, Event "E1A-5"

C.3 SYSTEM QUANTIFICATION

C.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The DC Power Distribution System is a two train system consisting of independent batteries, battery chargers and buses. DC power is normally supplied by the independent battery chargers. A third battery charger can be manually switched to either train should one of the chargers normally in operation be removed from service. The battery chargers are normally driven by AC power. Should an AC power train be lost resulting in the loss of one charger, the battery assumes the DC loads on that train.

The battery charger voltage and battery internal current are normally monitored. Each DC bus was assumed to be effectively monitored, since loss of DC voltage at a bus would result in the loss of instrumentation that is normally operational, and it was assumed that this would be detected by the operators. Thus, during normal operation the DC system was assumed to be monitored.

For the case where offsite power is available, the unavailability of each DC bus was assessed based on a two hour bus outage time allowed by Technical Specifications. The unavailability in this case was small, and assessed to be primarily due to loss of a fuse.

For the loss of offsite power case, the unavailability of all buses on a single train is dominated by failure of the battery supplying that train. Since the battery is also required for the corresponding train of AC power, failure of a battery would fail one train of DC power and the corresponding train of AC power (see AC power fault tree quantification tables).

The failure of the DC power distribution system during the recirculation phase of a postulated accident was evaluated to be negligible for both the cases where offsite power is available or lost, since offsite power is assumed to be recovered by this phase.

C.3.2 SYSTEM FAULT TREE QUANTIFICATION

This section presents the quantification of the DC power system unavailability for required emergency operation. The quantitative results are presented in table form with attached notes outlining the assumptions. To perform the quantification, the simplified fault tree presented in Section E.2 was rearranged and is presented in this section in modular form.

Modularized fault trees were constructed for each DC bus for the case where offsite power is available. For the case where offsite power is lost, a single fault tree was constructed for the DC power system, since the dominant faults are loss of the batteries, which fail all buses.

Table C.4 shows the DC power success requirements, Table C.5 contains the top event definition for the modularized fault trees, and Figures C.4 through C.12 show the modularized fault trees. The unavailability of each gate is shown on these trees, as well as the top event unavailabilities. Table C.6 shows the Boolean equations that represent each fault tree. Table C.7, the quantification table, shows the quantification of each gate by component and failure mode. The attached notes explain the assumptions used in the quantification. Table C.8 summarizes the point estimates for each gate, and the error factors that were used in the sensitivity analysis.

Table C.4 DC Power Success Requirements

<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
A11	DC power on all DC buses	1

NOTES: 1. Failure of any DC bus would fail instrumentation and circuit breaker's power from that bus.

Table C.5 DC Power Top-Event Definitions*

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENTS</u>	<u>NOTES</u>
<u>Non-LOSP Case</u>		
DPDP-1A (1B)	Insufficient power on bus DPDP-1A (1B)	1
DPDP-2A (2B)	" " " " DPDP-2A (2B)	2
DPDP-3A (3B)	" " " " DPDP-3A (3B)	2
DPDP-8A (8B)	" " " " DPDP-8A (8B)	2
DPDP-4A (4B)	" " " " DPDP-4A (4B)	2
BC-3A (3B)	" " " " BC-3A (3B)	2
BC-3C (3D)	" " " " BC-3C (3D)	2
BC-3E (3F)	" " " " BC-3E (3F)	2
DPDP-5A (5B)	" " " " DPDP-5A (5B)	2
DPDP-6A (6B)	" " " " DPDP-6A (6B)	3
DPDP-7A (7B)	" " " " DPDP-7A (7B)	3
<u>Loss of Offsite Power Case</u>		
DCA	Insufficient power on DC Train A buses	4
DCB	" " " " " B "	5
DC	Loss of both trains of DC power	6

* See Figure C.3 for bus dependencies.

Table C.5 DC Power

TOP EVENT DEFINITIONS

NOTES

- 1 DC - buses DPDP-1A and DPDP-1B are the main DC-panels for the A- and B-trains of DC-power. All other buses are connected to these.
- 2 These buses are connected directly to the main DC-power buses.
- 3 DPDP-6A and 7A are connected to subpanel DPDP-5A. DPDP-6B and -7B are connected to subpanel DPDP-5B.
- 4 This top event is evaluated for loss of all buses on DC-Train A.
- 5 This top event is evaluated for loss of all buses on DC-Train B.
- 6 This top event represents loss of all DC-power.

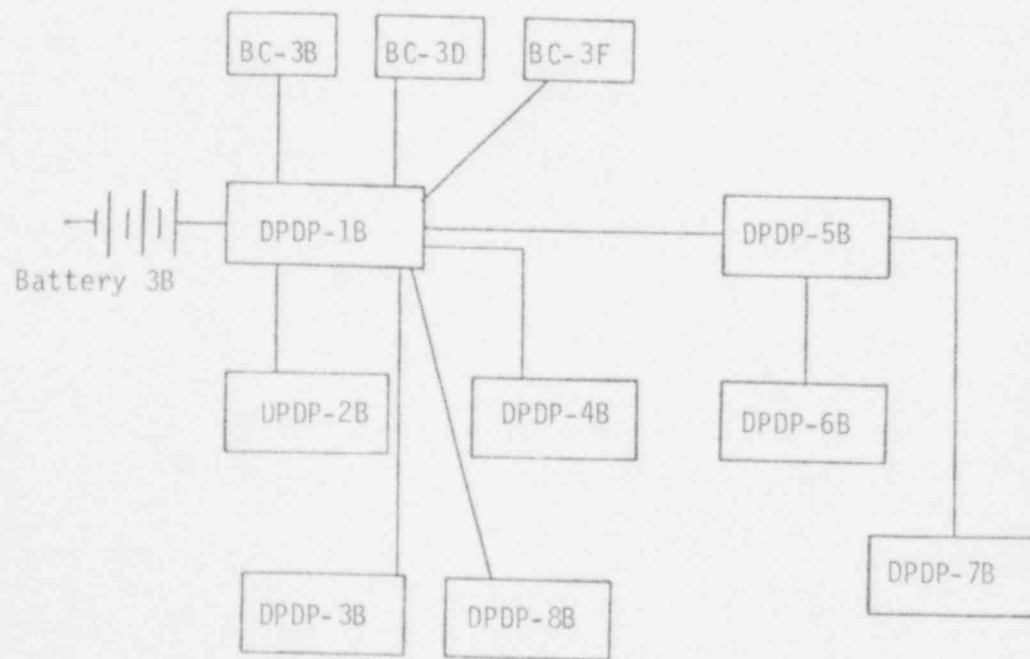
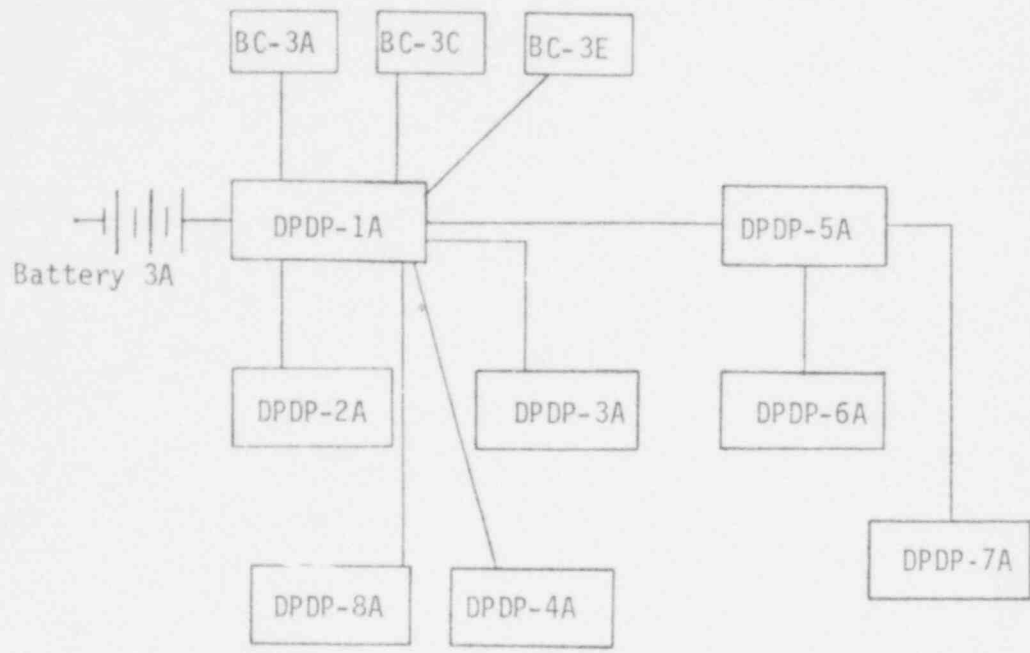


Figure C.3 DC Power - Bus Dependencies

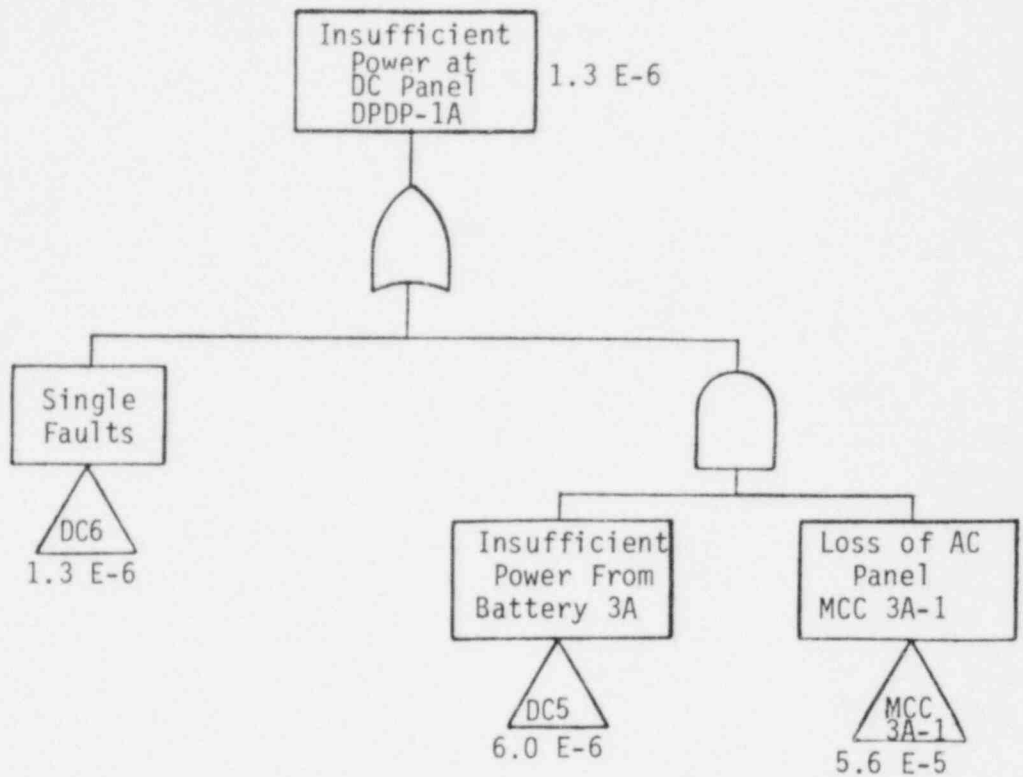


Figure C.4 Modularized Fault Tree for Event "DPDP-1A" (Non-LOSP)

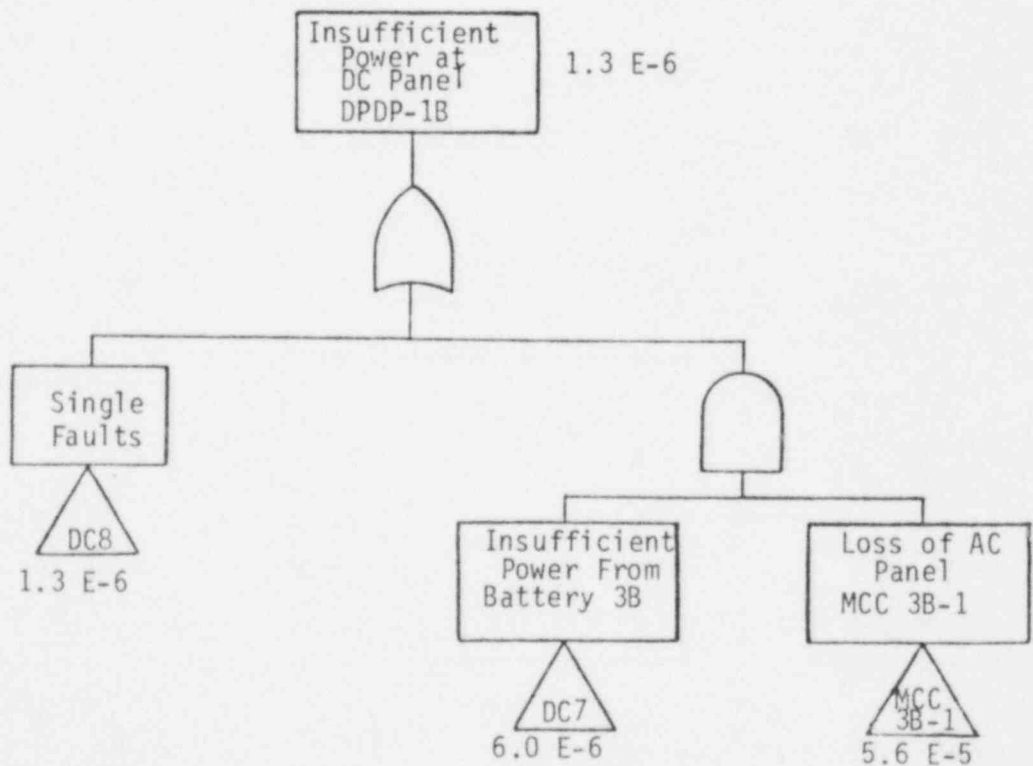


Figure C.5 Modularized Fault Tree for Event "DPDP-1B" (Non-LOSP)

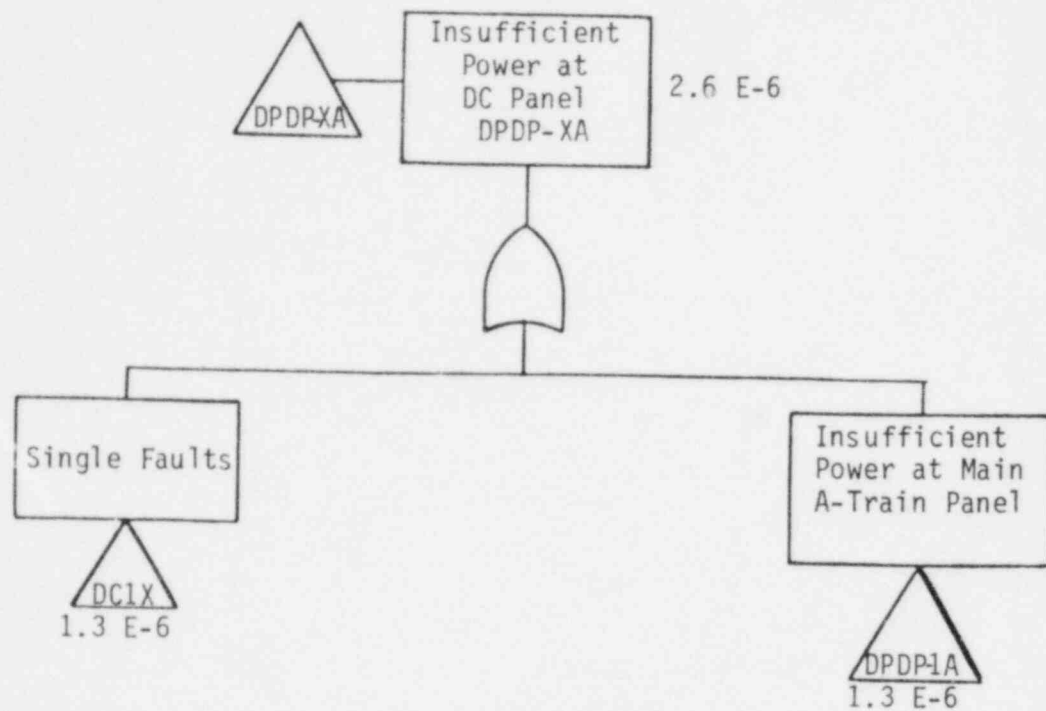


Figure C.6 Modularized Fault Tree for Event "DPDP-XA"
 (X = 2,3,4,5,8; Non-LOSP)

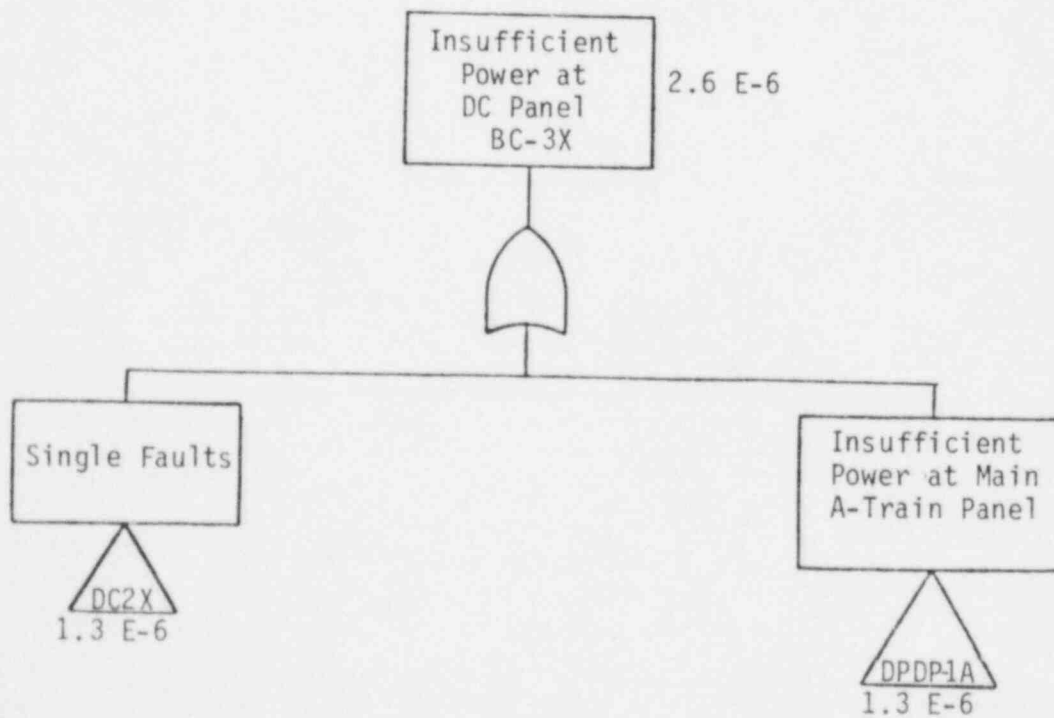


Figure C.7 Modularized Fault Tree for Event "BC-3X"
 (X = A,C,E; Non-LOSP)

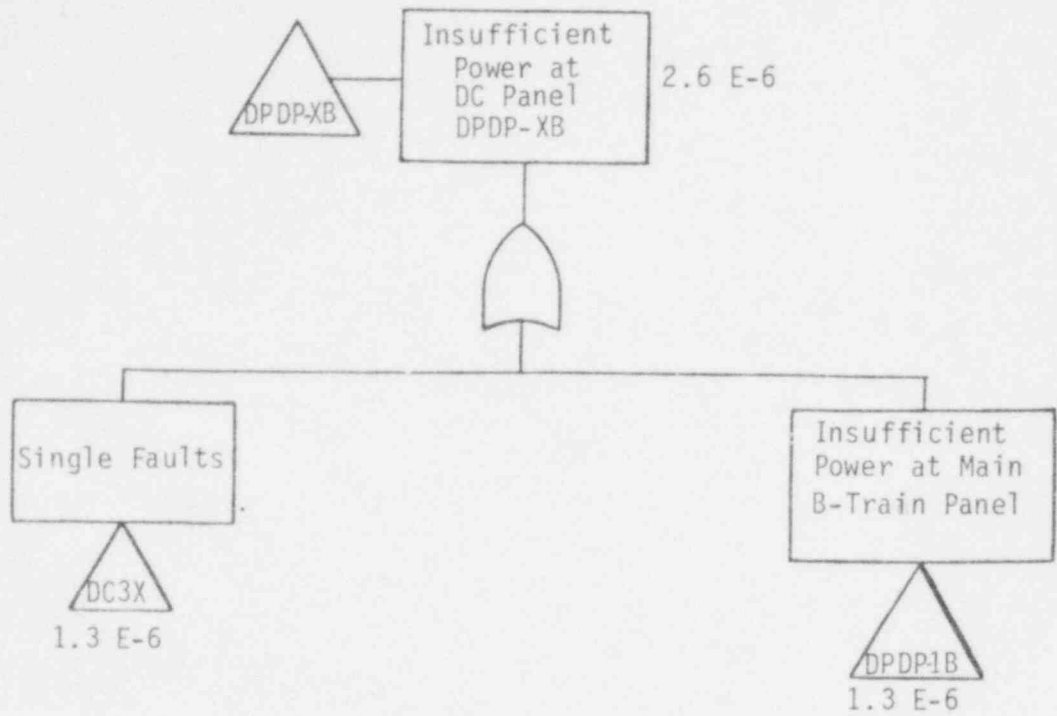


Figure C.8 Modularized Fault Tree for Event "DPDP-XB"
(X = 2,3,4,5,8; Non-LOSP)

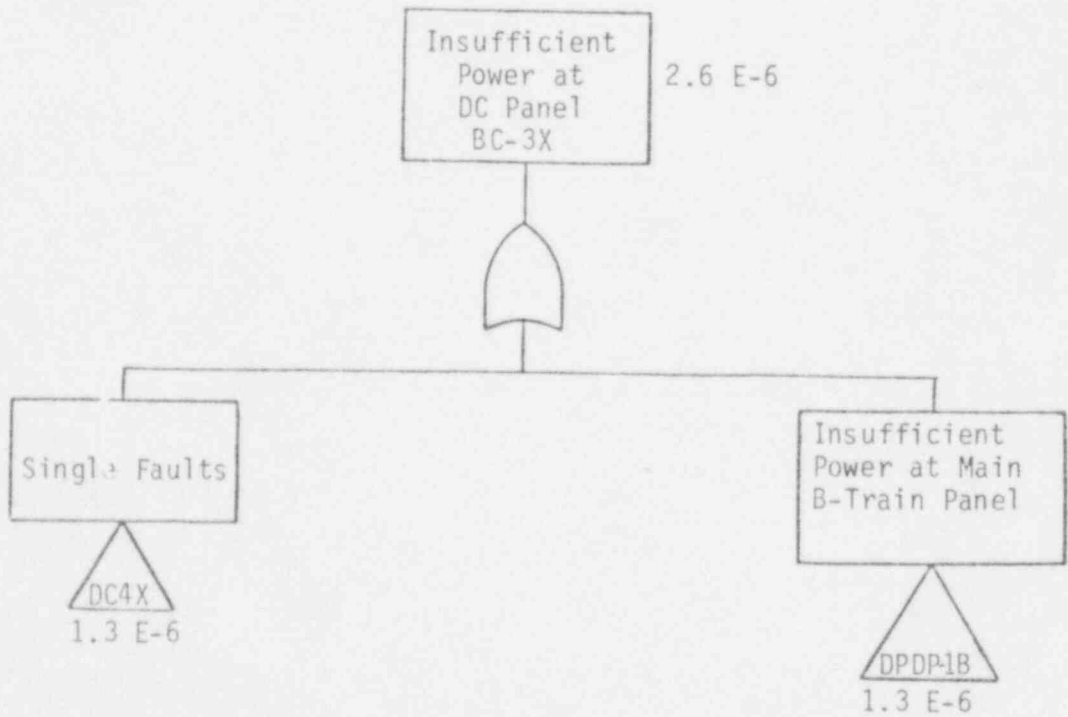


Figure C.9 Modularized Fault Tree for Event "BC-3X"
(X = B,D,F; Non-LOSP)

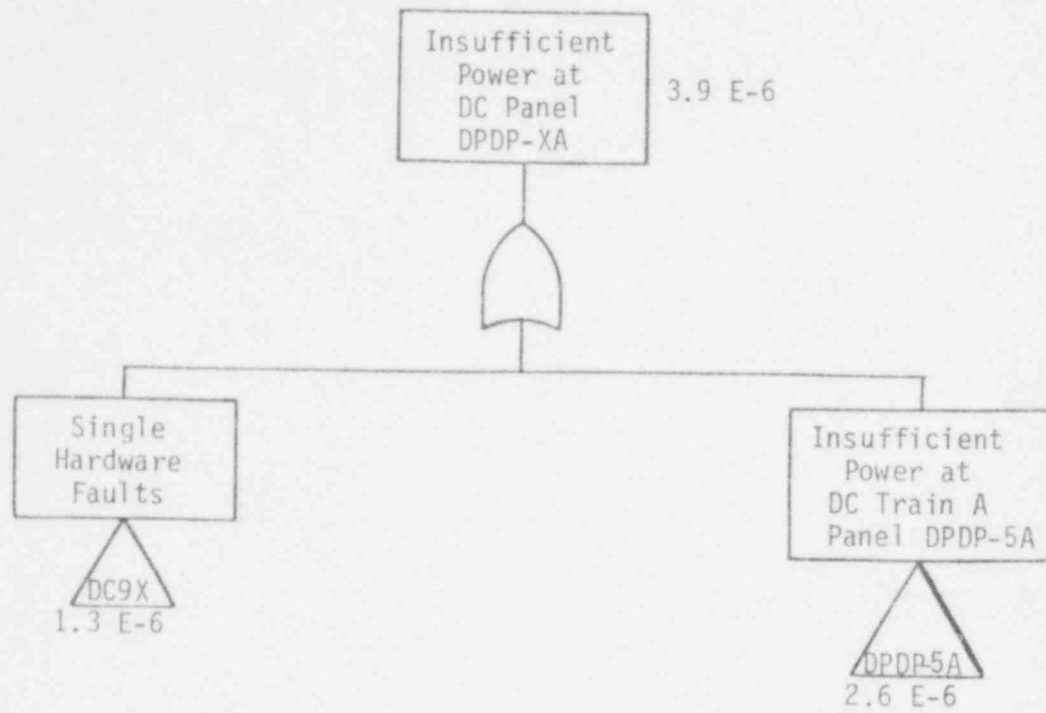


Figure C.10 Modularized Fault Tree for Event "DPDP-XA"
(X = 6,7; Non-LOSP)

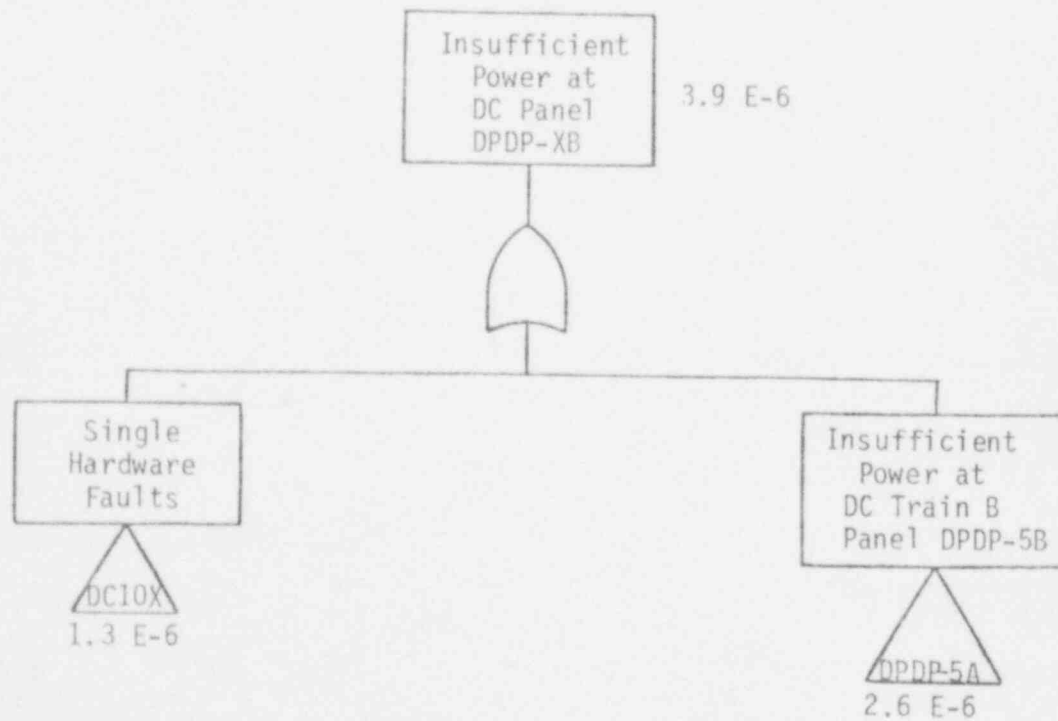


Figure C.11 Modularized Fault Tree for Event "DPDP-XB"
(X = 6,7; Non-LOSP)

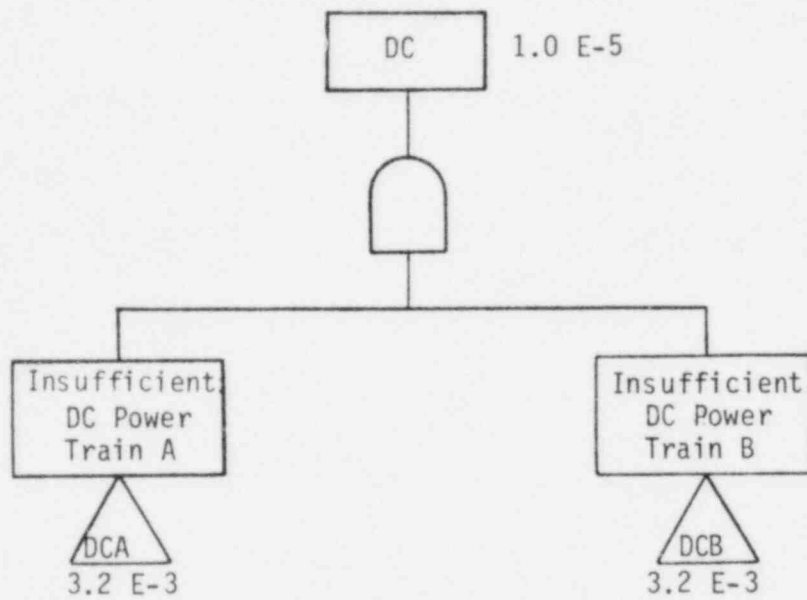


Figure C.12 Modularized Fault Tree for Event "DC" (LOSP)

Table C.6 DC Power

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

NON-LOSP

DPDP-XA	=	DC1X + DPDP-1A	X = 2,3,4,5,8
BC-3X	=	DC2X + DPDP-1A	X = A,C,E
DPDP-XB	=	DC3X + DPDP-1B	X = 2,3,4,5,8
BC-3X	=	DC4X + DPDP-1B	X = B,D,F
DPDP-1A	=	DC6 + DC5·MCC3A-1	
DPDP-1B	=	DC8 + DC7·MCC3B-1	
DPDP-XA	=	DC9X + DPDP-5A	X = 6,7
DPDP-XB	=	DC10X + DPDP-5B	X = 6,7

LOSP

$$DC = DCA + DCB$$

Table C.7 (1/2) Events "DPDP-XA" and "DPDP-XB" (for X=2, 3, 4, 5, 8), "BC-3X" (for X=A, B, C, D, E, F), and "DPDP-1A,-1B" Quantifications

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
DC1X, DC2X, DC3X, DC4X		SINGLE HARDWARE FAULTS TO PANEL DPDP-XA			1.3 E-6			1
DC6, DC8	FUSE	OPENS	1.0 E-6	1	1.0 E-6	3 ⁺ , 3 ⁻		2
DC9X, DC10X	SWITCH	CONTACTS N.C. FAILS OPEN	3.0 E-8	1	3.0 E-8	10 ⁺ , 10 ⁻		2
	WIRING	SHORT TO GROUND	3.0 E-7	1	3.0 E-7	10 ⁺ , 10 ⁻		2
DC5, DC7		INSUFFICIENT POWER FROM BATTERY 3A (3B)			$\frac{1}{2} = 1.3 E-6$			
	BATTERY	INSUFFICIENT POWER	3.0 E-6	2	6.0 E-6	3 ⁺ , 3 ⁻		3
ICC3A-1		ICC BUS 3A UNAVAILABLE			6.0 E-6	3 ⁺ , 3 ⁻		5
ICC3B-1		ICC BUS 3B UNAVAILABLE			5.6 E-5			5
					5.6 E-5			5

Table C.7 (2/2) Events "DCA" and "DCB" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
DCA	BATTERY	INSUFFICIENT POWER ALL BUSES DC TRAIN A	3.0 E-6	1080	3.2 E-3	3 ⁺ , 3 ⁻		4
		INSUFFICIENT POWER			3.2 E-3			
DCB	BATTERY	INSUFFICIENT POWER ALL BUSES DC TRAIN B	3.0 E-6	1080	3.2 E-3	3 ⁺ , 3 ⁻		4
		INSUFFICIENT POWER			3.2 E-3			

Table C.7 DC Power

QUANTIFICATION TABLES

NOTES

- 1 The structure of the fault tree for events DPDP-2A, 3A, 4A, 5A, 8A and DPDP-2B, 3B, 4B, 5B, 8B and BC-3A, 3B, 3C, 3D, 3E, and 3F are all similar.

Each of these events are comprised of the same three single hardware faults and failure of the main DC bus in the train.
- 2 The DC-system is essentially a monitored system since failures would be detected when they occur. Technical Specifications limit bus outages to two hours. Event unavailability was estimated as the product of event failure frequency and assumed average fault repair time of one hour.
- 3 The event unavailability was estimated as above (in Note 2), except that the average repair time was assumed to be two hours.
- 4 For the case of loss of offsite power the unavailability of the batteries dominates the unavailability of each DC-train. The batteries are checked quarterly and it was assumed that battery faults could be discovered at this time. The average fault duration time was thus 1/2 of 3 months.
- 5 See AC-Power Quantification Tables.

Table C.8 DC Power System - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
DC1X ¹	1.3 E-6
DC2X ¹	1.3 E-6
DC3X ¹	1.3 E-6
DC4X ¹	1.3 E-6
DC6	1.3 E-6
DC8	1.3 E-6
DC9X ¹	1.3 E-6
DC10X ¹	1.3 E-6
DC5	6.0 E-6
DC7	6.0 E-6
MCC3A-1	5.6 E-5
MCC3B-1	5.6 E-5
DCA	3.2 E-3
DCB	3.2 E-3

¹X=2, 3, 4, 5, 8

APPENDIX D

CLASS I.E. AC POWER SYSTEM

D.1 SYSTEM DESCRIPTION AND OPERATION

The purpose of the class IE electrical system is to provide electric power to those systems required to shut down the reactor and limit the release of radioactive material following a transient or design basis event. AC power is required to operate valves and provide motive power for pumps and fans for all safety systems. The turbine-driven pump in the Emergency Feedwater System is the only safety system pump that does not require AC power. AC power is required during both the injection and recirculation phases of accident sequences. AC power is also supplied to the battery chargers for the 250/125 VDC Battery and Distribution System.

D.1.1 SYSTEM DESCRIPTION

Figure D.1 presents a simplified one line diagram for AC power distribution (the DC power distribution system is also displayed). The preferred power supply for the two redundant 4.16kV Engineered Safeguards (ES) Buses 3A and 3B is the connection to the 230kV substation by means of the Unit 3 startup transformer. The 230kV substation is connected to the existing FPC transmission network by five circuits. The 4.16kV ES buses can also be fed from the Unit 1 and 2 startup transformer provided one of the two units is operating. Similarly, Unit 3 auxiliary transformer can also be used as a source provided the Unit 3 turbine generator is in operation.

Upon loss of electric power due to a separation of the 230kV system, shutdown of the nuclear generating unit electric power will be supplied from the standby power supply which consists of two independent diesel generators. Each diesel generator feeds one of the 4.16kV ES buses. Various ES motor loads are connected to the 4.16kV ES buses by spring breakers. The safeguards auxiliary transformer connections are provided to step-down the 4.16kV for the 480VAC engineered safeguards switchgear centers 3A and 3B. Motor control centers 3A-1, 3A-2, 3A-B, 3B-1 and 3B-2 are provided to feed associated safeguards equipment. MCC 3A-B is switchable between 480V ES Bus 3A or 3B. MCC 3A-1 and 3B-2 supply power to the DC battery chargers as well as power to the inverters in order to provide four independent 120VAC vital buses.

D.1.2 SYSTEM OPERATION

The normal supply for the 4.16kV ES buses 3A and 3B is from the Unit 1 & 2 230kV substation via the Unit 3 startup transformer and "normally closed" feeder breakers 3205 and 3206. The backup connection to Units 1 and 2 startup transformer can be accomplished by manually closing breakers 3211 and 3212.

In the event of the loss of the Unit 3 startup transformer or power at the 230kV substation (resulting in a loss of power on the buses) the following automatic actions occur: breakers 3205 and 3206 open and all breakers on the buses trip with the exception of a pre-selected block (block 1 of Table D.1) of feeder breakers and the 4160/480V ES auxiliary transformer feeder breaker, both diesels start and energize their associated safeguards buses when "normally open" breakers 3209 and 3210 close. Additional equipment is manually reconnected as required for safe plant operation. If there is a requirement for safeguards system operation coincident with the loss of voltage on a 4160V bus, the bus is cleared as before and the diesels are started to energize the bus. However, the remaining selected safeguard loads (Table D.2) are automatically connected within 30 seconds by an orderly sequencing of load timers. In the event the motor driven emergency feedwater pump is required, various decay heat associated loads are disconnected (Table D.2) prior to starting the motor driven emergency feedwater pump to avoid overloading the diesel generator.

Breaker auxiliary contacts and protective relaying are used to supervise contact closures in other safeguards circuits to initiate signals and control opening and closing circuits for breakers in order to prevent bus ties and inadvertent "live" bus transfers.

The 480V engineered safeguards distribution system is contained in two separate 480V unit switch gear rooms 3A and 3B. From these buses, motor control centers 3A-1, 3A-2, 3A-B, 3B-1 and 3B-2 are provided to feed associated safeguards equipment. Although MCC 3A-B is switchable between 480V ES Bus 3A or 3B through a manual transfer switch, it is normally configured to Bus

3A. MCC 3A-1 (and MCC 3B-2) supply redundant DC battery chargers for 250/125VDC Battery and distribution system. MCC 3A-1 also supplies two dual input inverters which in turn supply two 120VAC vital buses 3A and 3C. On loss of AC power the inverter is supplied by the 125VDC batteries to prevent a loss of power on the vital buses. If an inverter is inoperable, a redundant backup path to (MCC 3A-1 supplied) regulated 120VAC is available by manually switching transfer switch VBXS.

Allowable outages for the AC power system are defined by the following general comments on limiting conditions for operation of the class IE AC Electrical Power System. (For a complete description refer to Section 3/4.8.1 of the Technical Specifications.)

- Minimum conditions for operation require:
 - 2 operable circuits between offsite transmission network and the onsite class IE Distribution System.
 - 2 Diesel Generators (DG's) with associated fuel supplies.

Although various combinations of the above can be inoperable for short durations, the most significant combination allows both DG's to be inoperable for up to two hours provided two offsite AC circuits are shown to be operable. If one DG is not restored within the 2 hour time period, the reactor must be brought to Hot Standby within 6 hours and in Cold Shutdown within the following 30 hours. If only one diesel is inoperable, it must be restored within 72 hours or the reactor must be in Hot Standby within the next 6 hours and in Cold Shutdown within the following 30 hours.

- In addition to the above, all of the Class IE Vital and Safeguards buses must be operable and energized from their normal sources of power. An inoperable bus must be restored to operable status within 8 hours or be in Hot Standby within the next 6 hours and in Cold Shutdown within the following 30 hours.
- Minimum conditions for shutdown require the following buses to be operable and energized from sources of power other than a DG but aligned to an operable DG:

- 1 - 4160V Emergency Bus.
- 1 - 480V Emergency Bus.
- 2 - 120V AC Vital Buses.

Containment integrity must be established within 8 hours if less than the above combination of AC are operable.

Test and surveillance requirements are defined as:

- Each independent circuit between the offsite transmission network and the onsite Class IE Distribution System shall be:
 - Determined operable at least once per 7 days by verifying correct breaker alignments, and sump pumps in tunnel containing DC control feeds to 230kV switchgear are operable.
 - Demonstrated operable at least once per 18 months during shutdown by transferring unit power supply from the normal circuit to the alternate circuit.
- Each diesel generator shall be demonstrated operable at least once per 31 days by verifying fuel level and the diesel is started, synchronized, loaded, and operated for more than 60 minutes. This test can be run during normal operations.
- At least once per 18 months during shutdown:
 - Perform preventive maintenance in accordance with manufacturer's recommendations.
 - Simulate LOSP and ESAS signal to verify automatic load shedding, bus tie breakers open, diesel starts and energizes the auto-connected emergency loads through the load sequencer.
- Emergency AC buses determined operable and energized from normal AC sources at least once per 7 days by verifying correct breaker alignment and indicated power availability.

Table D.1 Block Loading Sequence

<u>Loading Sequence</u>	<u>Quantity</u>	<u>Description</u>
Block 1	1	Makeup and Purification Pump (High Pressure Inj.)
	1	Decay Heat Pump (Low Pressure Inj.)
		Miscellaneous Valves, Emergency Lighting
	2	Inverters
	1/2	Control Complex Lighting
Block 2	2	Battery Chargers
	2	Reactor Building Fan Assemblies
Block 3	1	Emergency Nuclear Services Sea Water Pump
	1	Emergency Nuclear Services Closed Cycle Cooling Pump
Block 4	1	Decay Heat Service Sea Water Pump
	1	Reactor Building Spray Pump
	1	Decay Heat Closed Cycle Cooling Water Pump

Table D.2 Disconnect Loads and Additional Loads Required

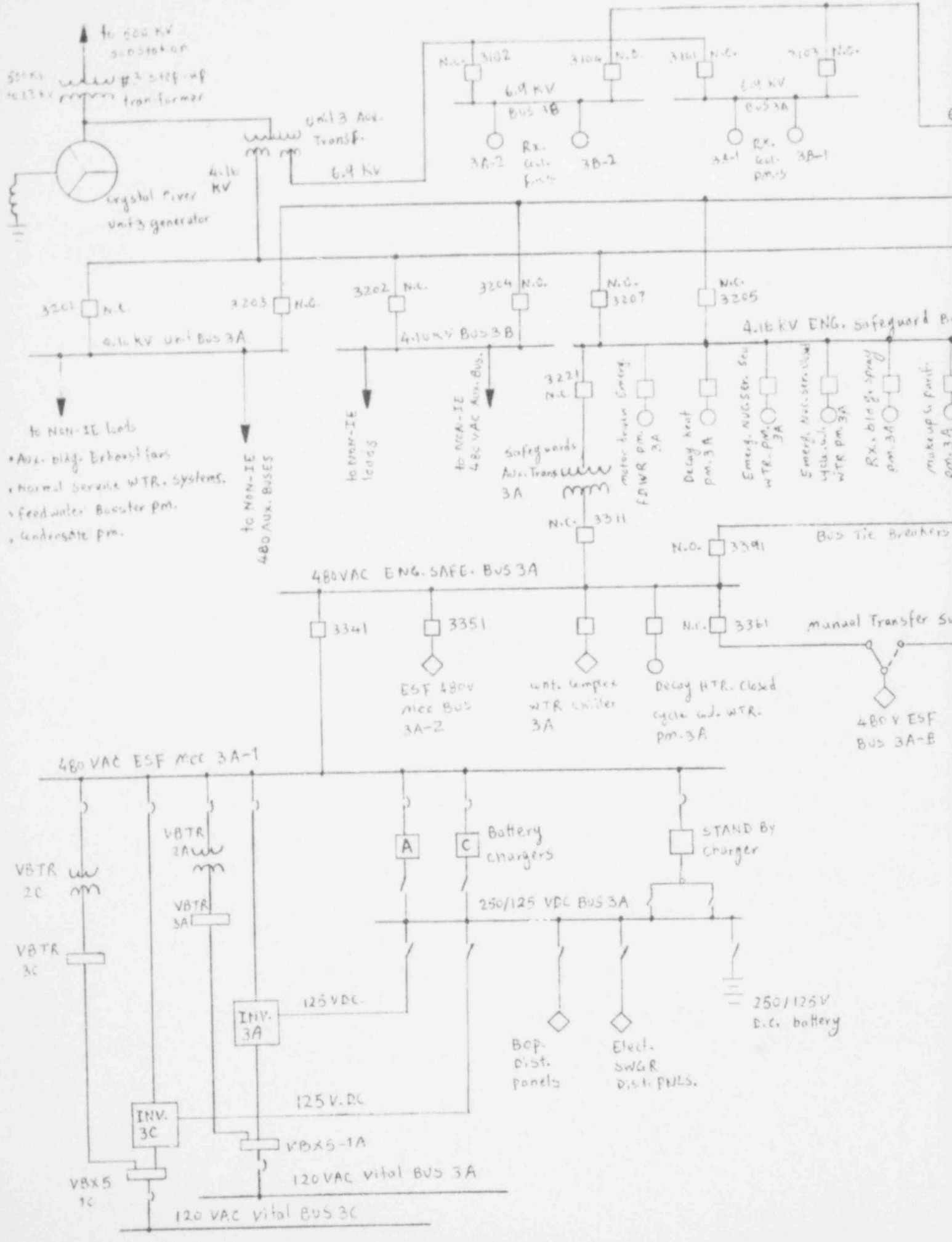
LOADS DISCONNECTED

Decay heat pump

Reactor building spray pump

Decay heat service sea water pump

Decay heat closed cycle cooling water pump



to 500 KV substation
 500KV 412.7KV
 #3 step-up transformer
 4.16 KV
 crystal river unit 3 generator

Unit 3 Aux. Transf. 6.9 KV

6.9 KV BUS 1B
 3A-2 Rx. Cont. F-4 3B-2
 6.9 KV BUS 3A
 3A-1 Rx. Cont. PM-3 3B-1

3201 N.C. 4.16 KV unit BUS 3A
 3203 N.C.

3202 N.C. 4.16 KV BUS 3B
 3204 N.C. 3207 N.C. 3205 N.C.

4.16 KV ENG. Safeguard Bus

- to Non-IE loads
- Aux. diag. Exhaust fans
- Normal Service WTR. systems.
- Feedwater Booster pm.
- Condensate pm.

to Non-IE BUSES
 480 AUX. BUSES

to Non-IE loads

to Non-IE 480 VAC Aux. Bus.

Safeguards Aux. Transf. 3A

3221 N.C. motor driven Energ. FDWR pm. 3A

Decay heat pm. 3A

Emerg. AUG. Str. Sec. WTR. pm. 3A

Emerg. Aux. Str. Sec. WTR. pm. 3A

Rx. bldg. spray pm. 3A

makeup to Purif. pm. 3A

480VAC ENG. SAFE. BUS 3A

3341

3351

ESF 480V MCC BUS 3A-2

unit. temp. WTR. cooler 3A

3361 N.C. Decay HTR. Closed cycle wd. WTR. pm. 3A

Bus Tie Breakers

Manual Transfer Sw

480V ESF BUS 3A-B

480 VAC ESF MCC 3A-1

VBTR 2C

VBTR 2A

VBTR 3C

VBTR 3A

INV. 3A

INV. 3C

VBX5-1A

VBX5 1C

120 VAC vital BUS 3A

120 VAC vital BUS 3C

Battery chargers

STAND BY charger

250/125 VDC BUS 3A

Bop. Dist. panels

Elect. SWGR Dist. PNLs.

250/125V D.C. battery

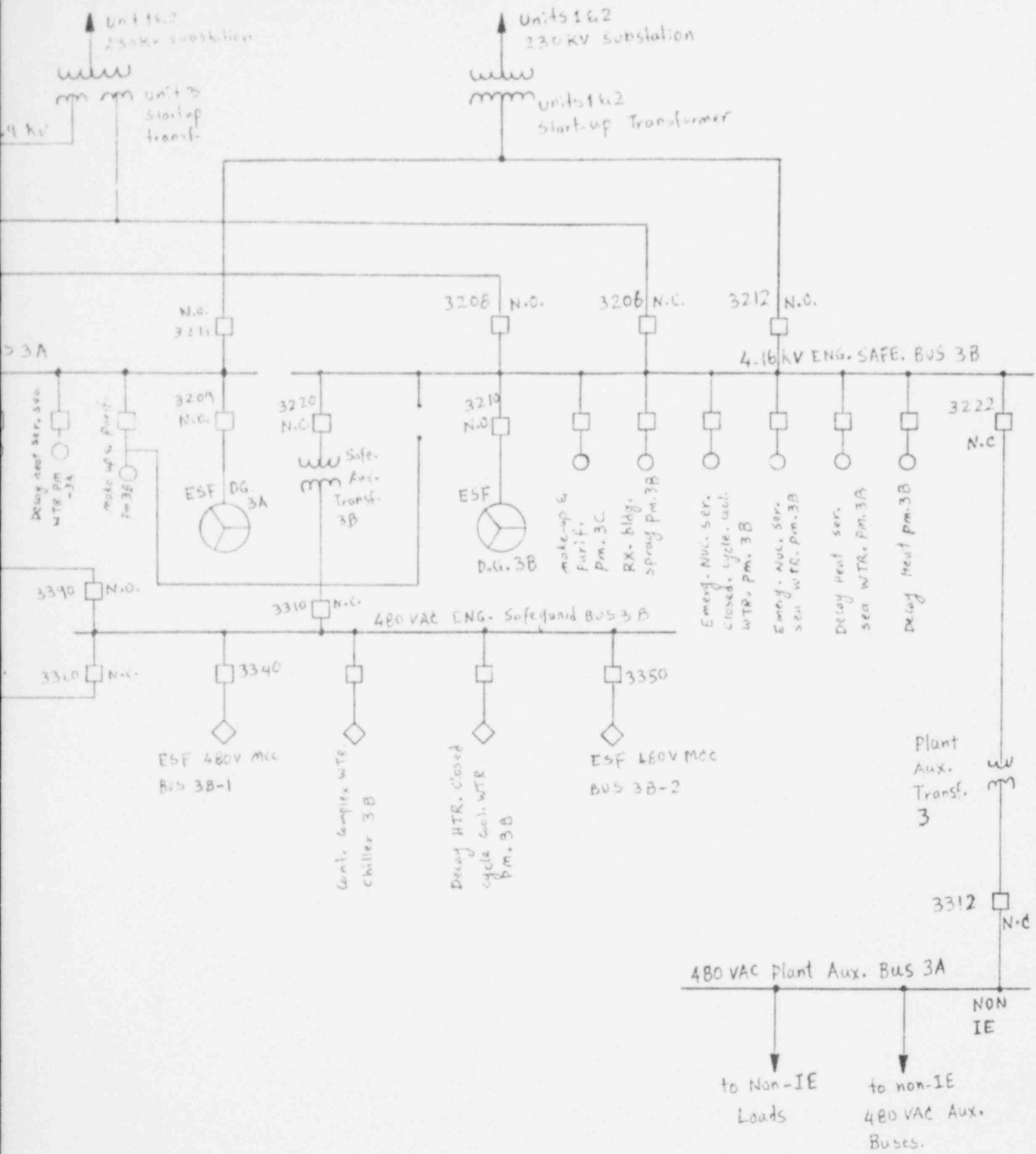


Figure D.1 Class IE AC Power System - Simplified One-Line Diagram

D.2 SYSTEM SIMPLIFIED FAULT TREES

Fault Trees were drawn for each of three levels of emergency power distribution: 4160V, 480V and 120VAC. The simplified fault trees are shown in Figure D.2. The fault summary is shown in Table D.3.

4160V FAULT TREE

Two fault trees were developed: one for loss of offsite power (LOSP) as the initiating event, and the other for accident initiators other than LOSP. The difference being, of course, that in the latter case offsite power must fail in addition to the diesels. No credible single failures could be postulated which would fail both DG buses. Dominant cut sets for loss of both buses involve failure of the diesels to start, or to continue to run. Some of the faults associated with loss of power on the 4.16kV buses are due to failures with protective relaying and logic such that automatic starting, load sequencing and circuit breaker trips are not accomplished. Common mode events include diesel common mode and hardware double failures such as the bus tie circuit breakers not opening.

One major assumption for this tree is that turbine trip occurs on LOSP which leaves only Units 1 and 2 and the DG's available to provide emergency power. Technical Specifications require as a minimum two 4.16kV buses, two 480VAC buses (3A&3B), and four 120VAC vital buses available unless the plant is in cold shutdown or refueling.

480VAC FAULT TREES

Individual simplified trees were constructed for each of the seven MCC ES 480V buses. In keeping with the simplified tree requirements, general cable and bus open and short to power or ground were not considered on the basis of probability of occurrence. Thus, for the most part, each individual 480V MCC tree is represented by faults associated with its feeder breaker or loss of power supplied to the bus. Transfers are provided for other ES systems whose components require power from one or more of these buses. Bus operability is also discussed in Section D.1.2 of this report.

120VAC VITAL BUSES

Similarly as was done for the 480VAC buses, each of the four 120VAC vital buses were modeled individually to facilitate transfers. Single failures for these buses are associated with faults which cause a disruption of power to the vital bus, e.g., fuse and breaker faults, switch failures, etc. Double failures (due to symmetry each of the trees are exactly alike) are associated with loss of power from the inverter system and loss of power from the backup 120VAC redundant regulated power supplies. This backup source is provided essentially only for maintenance purposes on the inverter and requires switching the manual transfer switch VBXS by the operator. This human interface is reflected on the tree. The inverter system failures are represented by single faults with the inverter itself or doubles reflecting the loss of the normal inverter 480VAC input and the "uninterruptible" backup connection to the DC power system.

Table D.3 (1/4) AC Power Fault Summary - 4.16kV Buses 3A, 3B

SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
K000001W	Loss of Offsite Power	Conditional Event
KDL0013R	Diesel Generator A	Does Not Run
KDL0013S	Diesel Generator A	Does Not Start
KLC0013W	Relay Logic for Automatic Start	Fails to Function
KLC003AW	Bus 3A Load Shedding Logic	Fails to Function
KCB0010P	Circuit Breaker 3206	Does Not Open
KLC0010W	Relay Logic for CB 3206	Fails to Function
KCB0011P	Circuit Breaker 3205	Does Not Open
KLC0011W	Relay Logic for CB 3205	Fails to Function
KCB0012N	Circuit Breaker 3209	Does Not Close
KCB0012W	Relay Logic for CB 3209	Fails to Function
E0000DC1	DC Control Power "A"	DC Power Not Available
KDL0023R	Diesel Generator B	Does Not Run
KDL0023S	Diesel Generator B	Does Not Start
KLC0023W	Relay Logic for Automatic Start	Fails to Function
KLC003BW	Bus 3B Load Shedding Logic	Fails to Function
KCB0024N	Circuit Breaker 3210	Does Not Close
KLC0024W	Relay Logic for CB 3210	Fails to Function
KCB0025P	Circuit Breaker 3222	Does Not Open
KLC0025W	Relay Logic for CB 3222	Fails to Function
T000ESA1	Engineering Safeguards Signal	No Actuation Signal
E0000DC2	DC Control Power "B"	DC Power Not Available
K0000DLW	Diesel Generators 3A, 3B	Common Mode
K House 01	Electrical Train "B" Out for Service	Not a Fault Event
K House 02	Electrical Train "A" Out for Service	Not a Fault Event
E0000DCW	Loss of all DC Power	Conditional Event

Table D.3 (2/4) AC Power Fault Summary - 480V MCC Buses

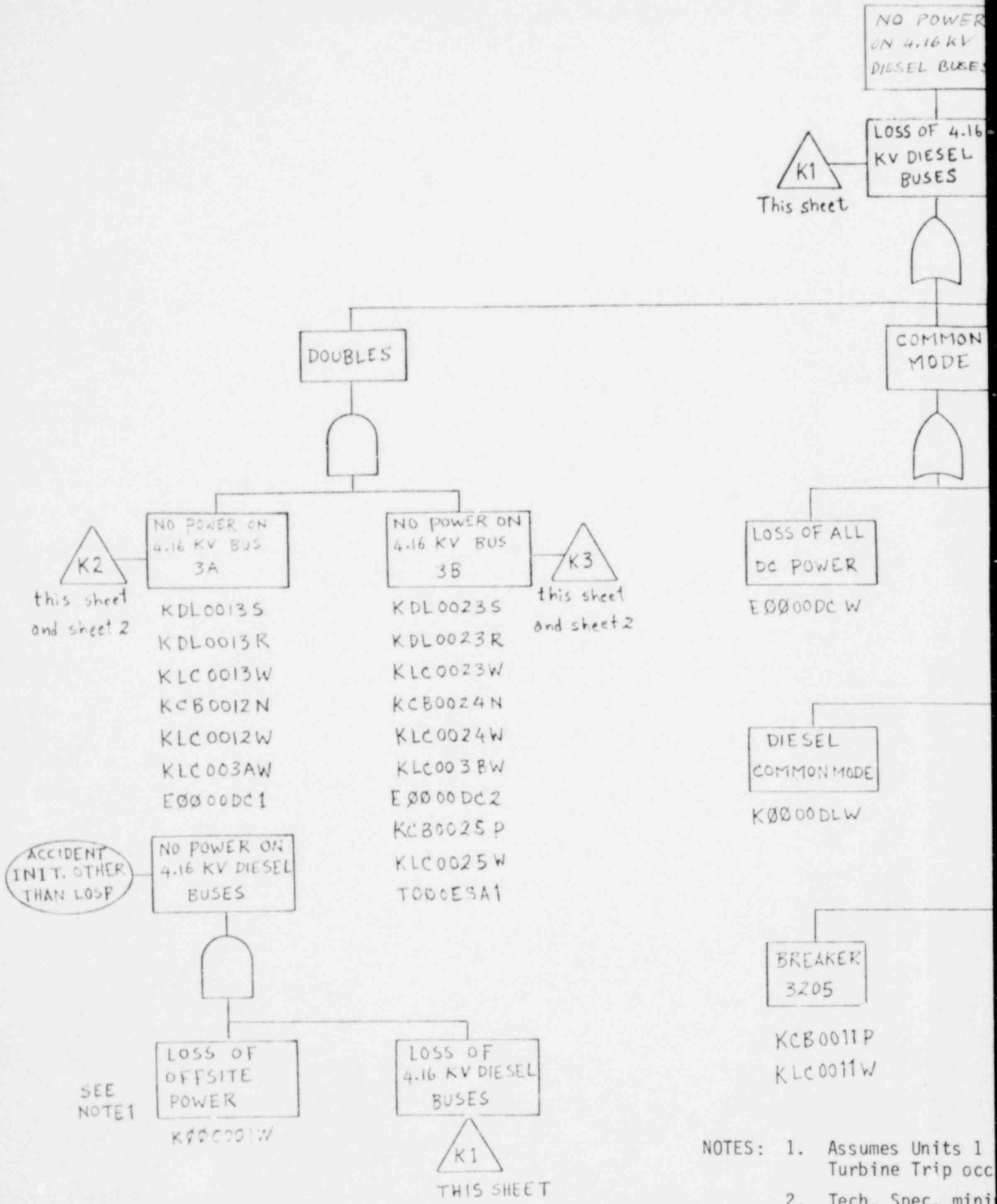
SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
KCB0006X	Circuit Breaker 3341	Operator Error (Commission)
KLC0006W	Relay Logic for CB 3341	Premature Transfer
KCB0007X	Circuit Breaker 3311	Operator Error (Commission)
KLC0007W	Relay Logic for CB 3311	Premature Transfer
KCB0008X	Circuit Breaker 3221	Operator Error (Commission)
KLC0008W	Relay Logic for CB 3221	Premature Transfer
KCB0014X	Circuit Breaker 3351	Operator Error (Commission)
KLC0014W	Relay Logic for CB 3351	Premature Transfer
KCB0015X	Circuit Breaker 3361	Operator Error (Commission)
KLC0015W	Relay Logic for CB 3361	Premature Transfer
KSW0016X	MCC 3A-B Transfer Switch	Operator Error (Omission)
KSW0016N	MCC 3A-B Transfer Switch	Does Not Close
KCB0017X	Circuit Breaker 3360	Operator Error (Commission)
KLC0017W	Relay Logic for CB 3360	Premature Transfer
KCB0018X	Circuit Breaker 3340	Operator Error (Commission)
KLC0018W	Relay Logic for CB 3340	Premature Transfer
KCB0019X	Circuit Breaker 3310	Operator Error (Commission)
KLC0019W	Relay Logic for CB 3310	Premature Transfer
KCB0020X	Circuit Breaker 3220	Operator Error (Commission)
KLC0020W	Relay Logic for CB 3200	Premature Transfer
KCB0021X	Circuit Breaker 3350	Operator Error (Commission)
KLC0021W	Relay Logic for CB 3350	Premature Transfer
KTR0030D	Safeguards Auxiliary Transformer 3A	Shorts
KTR0031D	Safeguards Auxiliary Transformer 3B	Shorts

Table D.3 (3/4) AC Power Fault Summary - 120VAC Vital Bus 3A and 3C

SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
KCB00A1X	Circuit Breaker 3601	Operator Error (Commission)
KFU00A6B	Fuse VBF1	Opens
KSW00A2B	Manual XFR Switch 3A VBXS-1A	Opens
KSW00A2X	Manual XFR Switch 3A VBXS-1A	Operator Error (Omission)
KSW00A2W	Manual XFR Switch 3A VBXS-1A	Does Not Close
KIV00A5W	Inverter 3A	Fails to Function
KFU00A7B	Fuse VBF45	Opens
KCB00A8X	Breaker to Inverter 3A	Operator Error (Commission)
KLC00A8W	Relay Logic for Inverter 3A CB	Fails to Function
KFU00A9B	Fuse VBF 36	Opens
KVRC10W	VBTR-3A 15W Power Supply/Regulator 3A	Fails to Function
KFU0A11B	Fuse VBF35	Opens
KTROA12D	Voltage Transformer VBTR-2A	Shorts
KCB00A4X	Circuit Breaker to VBTR-2A	Operator Error (Commission)
KLC00A4W	Relay Logic for CB to VBTR-2A	Fails to Function
KCB00C1X	Circuit Breaker 3603	Operator Error (Commission)
KFU00C6B	Fuse VBF 2	Opens
KSW00C2B	Manual XFR Switch VBXS-3C	Opens
KSW00C2X	Manual XFR Switch VBXS-3C	Operator Error (Omission)
KSW00C2N	Manual XFR Switch VBXS-3C	Does Not Close
KIV00C5W	Inverter 3C	Fails to Function
KFU00C7B	Fuse VBF 49	Opens
KCB00C7X	Breaker to Inverter 3C	Operator Error (Commission)
KLC00C8W	Relay Logic for Inverter 3C CB	Fails to Function
KFU00C9B	Fuse VBF 40	Opens
KVROC10W	VBTR-3C 15W Redundant PS Regulator 3C	Fails to Function
KFU0C11B	Fuse VBF 39	Opens
KTROC12D	Voltage Transformer VBTR-2C	Shorts
KCB00C4X	Circuit Breaker to VBTR-2C	Operator Error (Commission)
KLC00C4W	Relay Logic for CB to VBTR-2	Fails to Function

Table D.3 (4/4) AC Power Fault Summary - 120VAC Vital Bus 3B and 3D

SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
KCB00B1X	Circuit Breaker 3602	Operator Error (Commission)
KFU00B6B	Fuse VBF 3	Opens
KSW00B2B	Manual XFR Switch VBXS-3B	Opens
KSW00B2X	Manual XFR Switch VBXS-3B	Operator Error (Omission)
KSW00B2N	Manual XFR Switch VBXS-3B	Does Not Close
KIV00B5W	Inverter 3B	Fails to Function
KFU00B7B	Fuse VBF 47	Opens
KCB00B8X	Breaker to Inverter 3B	Operator Error (Commission)
KLC00B8W	Relay Logic for Inverter 3B CB	Fails to Function
KFU00B9B	Fuse VBF 38	Opens
KVROB10W	VBTR 3B 15W Redundant PS Regulator 3B	Fails to Function
KFU0B11B	Fuse VBF 37	Opens
KTROB12D	Voltage Transformer VBTR-2B	Shorts
KCB00B4X	Circuit Breaker to VBTR-2B	Operator Error (Commission)
KLC00B4W	Relay Logic for CB to VBTR-2B	Fails to Function
KCB00D1X	Circuit Breaker 3604	Operator Error (Commission)
KFU00D6B	Fuse VBF 4	Opens
KSW00D2B	Manual XFR Switch VBXS-1D	Opens
KSW00D2X	Manual XFR Switch VBXS-1D	Operator Error (Omission)
KSW00D2N	Manual SFR Switch VBSX-1D	Does Not Close
KIV00D5W	Inverter 3D	Fails to Function
KFU00D7X	Fuse VBF 51	Opens
KCB00D8X	Breaker to Inverter 3D	Operator Error (Commission)
KLC00D8W	Relay Logic for Inverter 3D CB	Fails to Function
KFU00D9B	Fuse VBF 42	Opens
KVROD10W	VBTR-3D 15W Redundant PS Regulator 3D	Fails to Function
KFU0D11B	Fuse VBF 41	Opens
KTROD12D	Voltage Transformer VBTR-2D	Shorts
KCB00D4X	Circuit Breaker to VBTR-2D	Operator Error (Commission)
KLC00D4W	Relay Logic for CB to VBTR-2D	Fails to Function



- NOTES: 1. Assumes Units 1 Turbine Trip occ
 2. Tech. Spec. mini shutdown: one 4. bus (3A or 3B);

INITIATING EVENT: LOSF (NOTES 1,2)

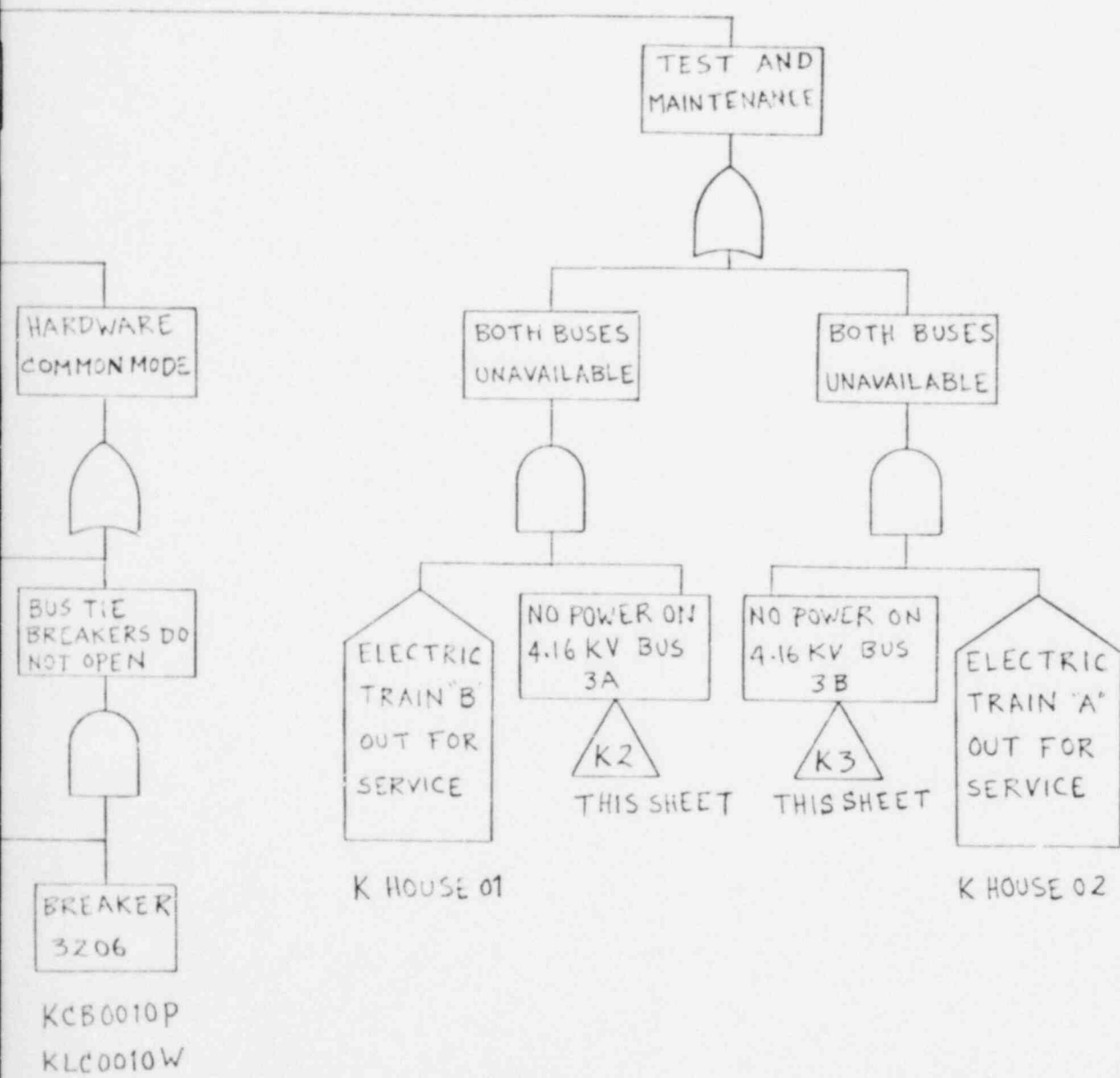
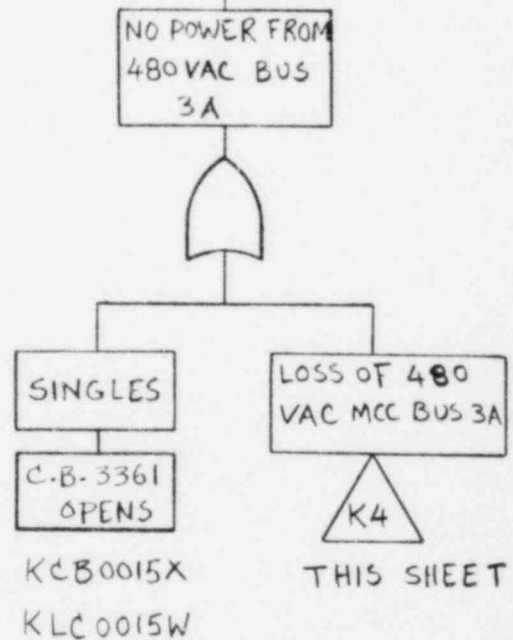
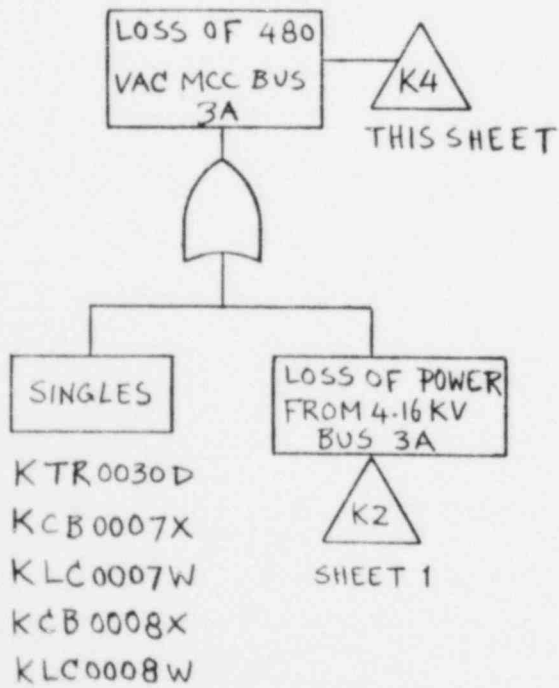
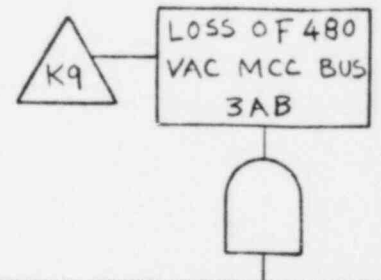
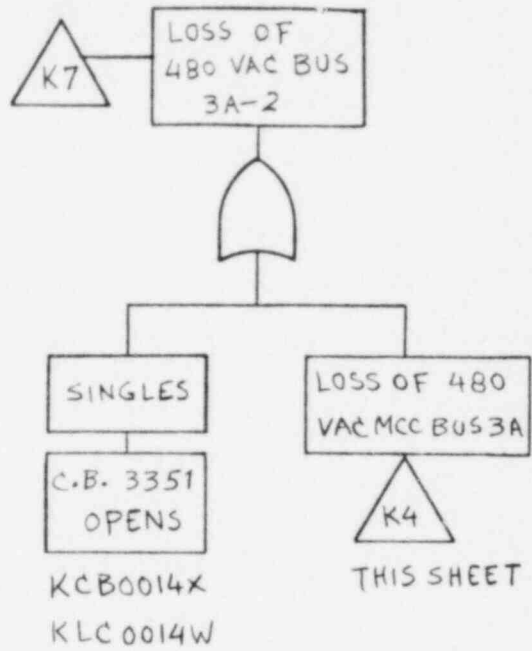
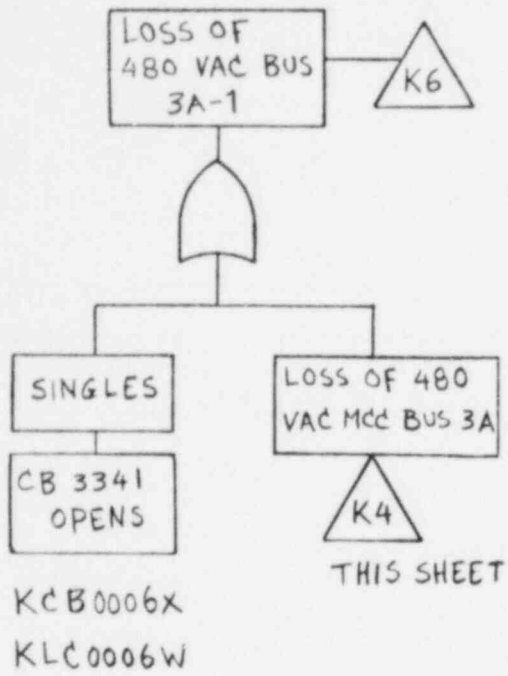


Figure D.2 (1/4) Simplified Fault Tree - AC Power System (4160VAC Buses)

& 2 are down and
 2 are on LOSP
 num required for
 1kV bus; one 480VAC
 two 120VAC vital buses.



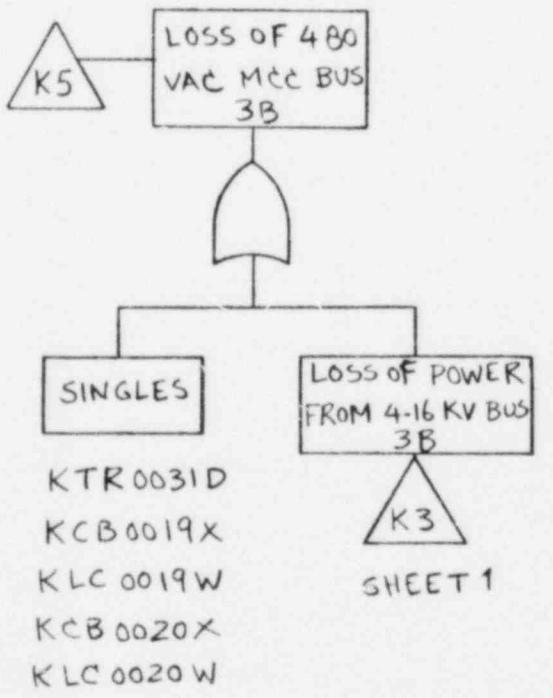
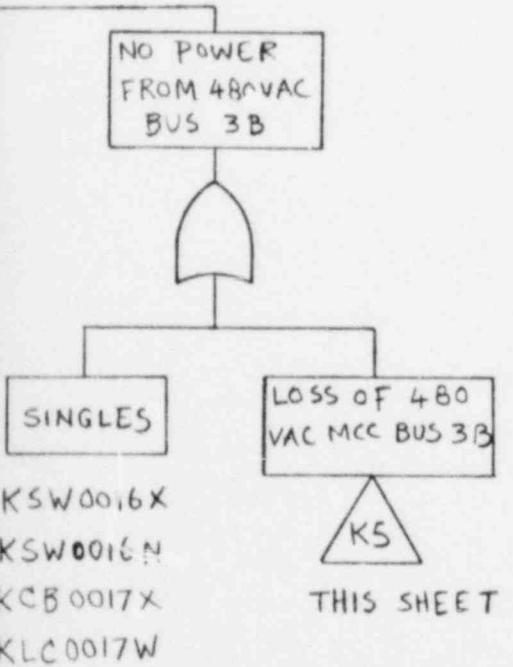
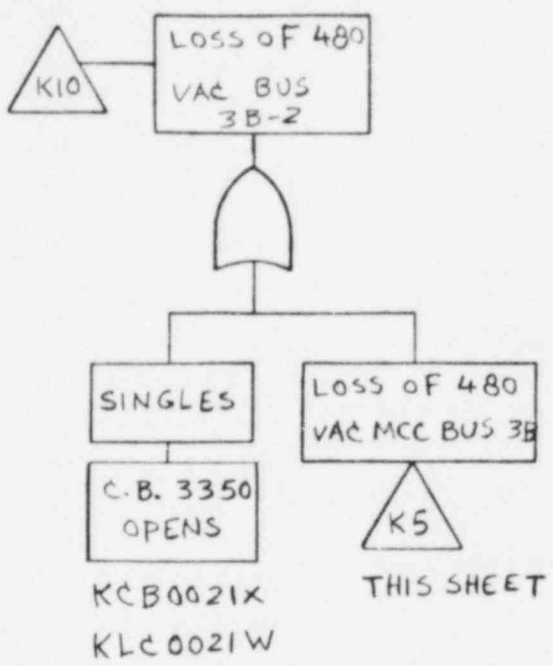
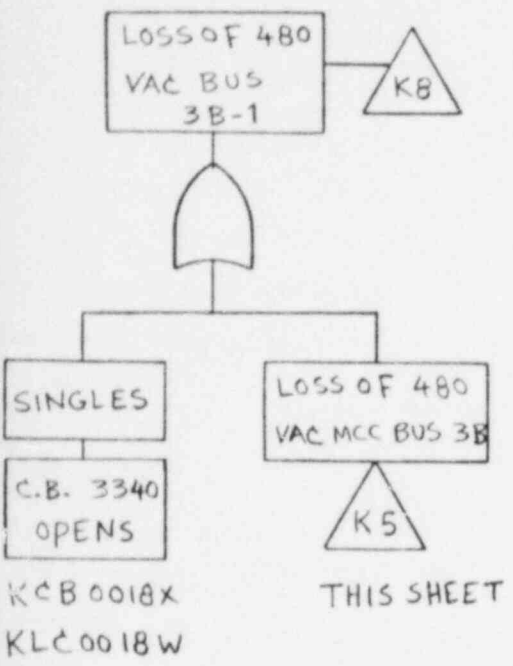


Figure D.2 (2/4) Simplified Fault Tree - AC Power System (Individual 480VAC MCCs)

LOSS OF 120
VAC VITAL
BUS 3A

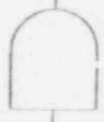


SINGLES

KCB00A1X
KFU00A6B
KSW00A2B

DOUBLES

NO POWER
SUPPLIED TO
VBXS-1A



NO POWER
FROM
INVERTER 3A

NO POWER
FROM REG.
XTRM 3A



SINGLES

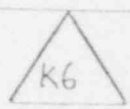
DOUBLES

LOSS OF
480 VAC
BUS 3A-1

SINGLES

INV. 3A
FAULTS

NO POWER
SUPPLIED TO
INV. 3A



SHEET 2

KSW00A2X
KSW00A2N
KFU00A9B
KYR0A10W
KFU0A11B
KTR0A12D
KCB00A4X
KLC00A4W

KIV00A5W
KFU00A7B

NO 480 VAC
POWER TO
INV. 3A

LOSS OF
BACKUP DC
POWER SOURCE

LOSS OF 125
VDC MAIN
PANEL



DC POWER
TREE

LOSS OF
480 VAC BUS
3A-1

CIRCUIT
BREAKER OPENS

LOSS OF
480 VAC
BUS 3A-1



SHEET 2

KCB00A8X
KLC00A8W



SHEET 2

NO
POW
INV

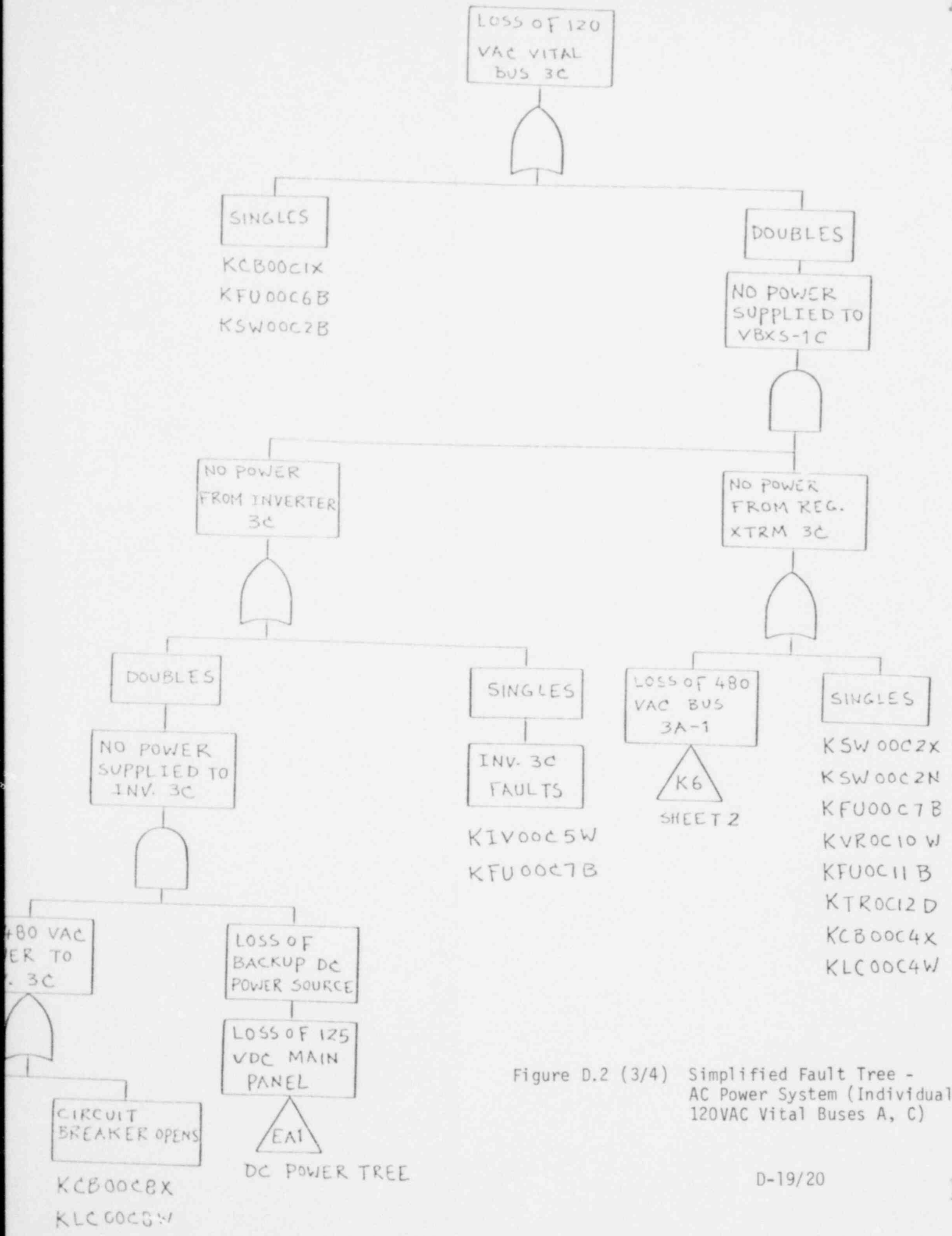


Figure D.2 (3/4) Simplified Fault Tree - AC Power System (Individual 120VAC Vital Buses A, C)

LOSS OF 120
VAC VITAL
BUS 3B



SINGLES

KCB00BIX
KFU00B6B
KSW00B2B

DOUBLES

NO POWER
SUPPLIED TO
VBXS-1B



NO POWER
FROM
INVERTER 3B

NO POWER
FROM REG.
XTRM 3B



SINGLES

DOUBLES

LOSS OF
480 VAC
BUS 3B-2

SINGLES

INV. 3B
FAULTS

NO POWER
SUPPLIED TO
INV. 3B

K10
SHEET 2

KSW00B2X
KSW00B2N
KFU00B9B
KVR0B10W
KFU0B11B
KTR0B12D
KCB00B4X
KLC00B4W

KIV00B5W
KFU00B7B



NO 480 VAC
POWER TO
INV. 3B

LOSS OF
BACKUP DC
MAIN PANEL



LOSS OF 480
VAC BUS
3B-2

CIRCUIT
BREAKER OPENS
KCB00B8X
KLC00B8W

LOSS OF 125
VDC MAIN
PANEL

E1B
DC POWER
TREE

LOSS OF
480 VAC
BUS 3B-2

SHEET 2



SHEET 2

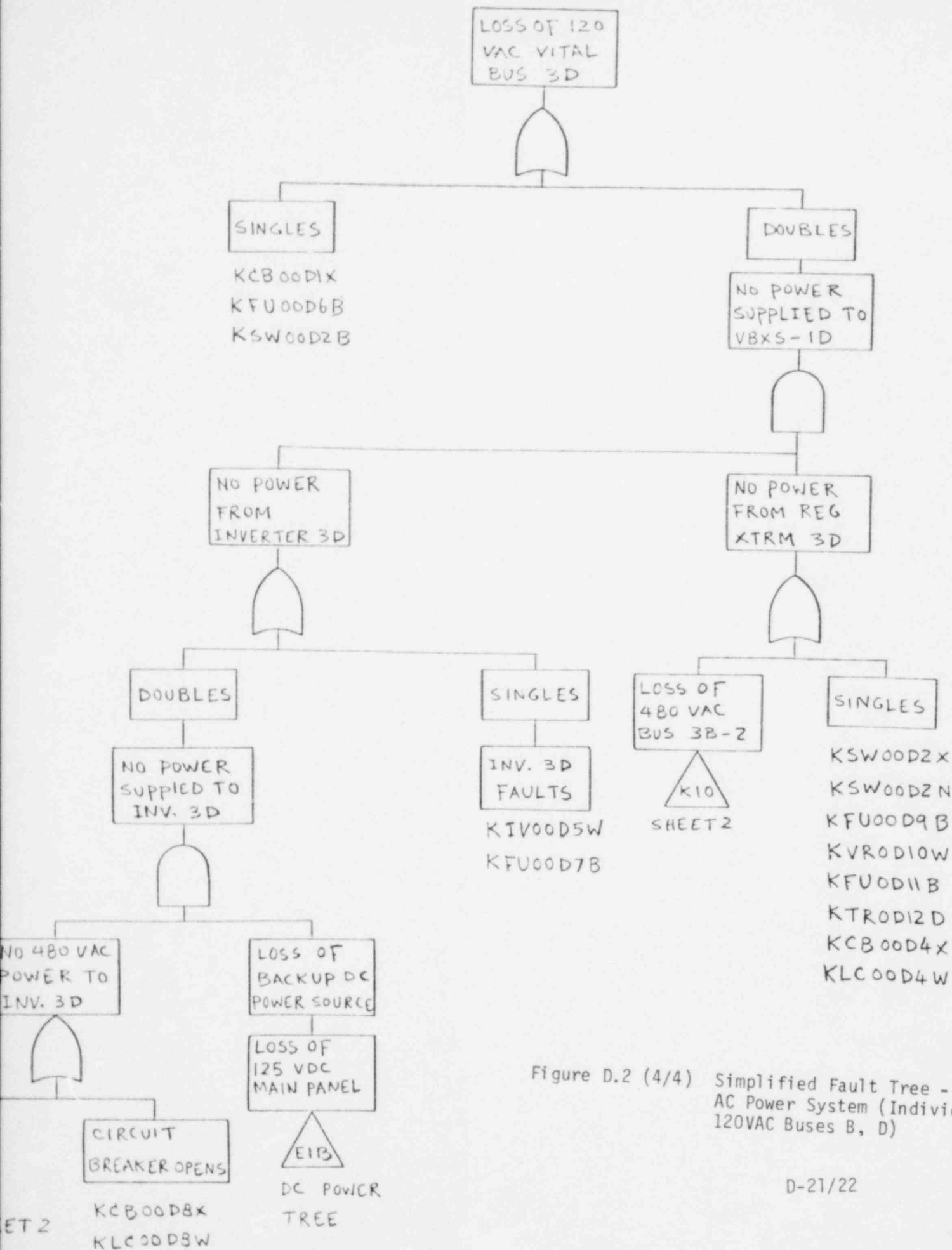


Figure D.2 (4/4) Simplified Fault Tree - AC Power System (Individual 120VAC Buses B, D)

D.3 SYSTEM QUANTIFICATION

D.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The Crystal River AC power distribution system is a two train system with the capability of being energized by multiple sources. The preferred source, and the one that the distribution system is normally aligned with, is the 230kV substation through the Unit 3 startup transformer. However, if power from the 230kV substation is not available, the distribution system may be aligned to receive power from either Units 1 or 2 (if they are available) or from the onsite diesel generators. This realignment requires the availability of DC power. AC power is supplied to the various safety systems from a variety of buses on both (independent) trains.

For the case where offsite power is available, the unavailability of the major AC buses was assessed to be primarily due to premature transfer of breakers and transformer shorts during a time window that would make the bus unavailable, but would not require the plant to be shut down (by Technical Specification limits). Since these faults are relatively rare in occurrence, and since the fault exposure time is small, the unavailability of individual buses was assessed to be small compared to other faults. The unavailability of an entire train of AC power is smaller still.

For the loss of offsite power case the unavailability of the AC power trains was assessed to be a contributor to safety system unavailability. The major contributors to AC power unavailability (both single trains and both trains) were assessed to be due to failures and maintenance outages of the diesel generators coupled with the unavailability of power from Units 1 and 2. Failure of a battery in the DC power distribution system was a less important contributor.

D.3.2 SYSTEM FAULT TREE QUANTIFICATION

This section presents the quantification of the AC power fault tree for emergency operation in response to an accident or transient. Only AC power availability during the injection phase of an accident or transient is presented. AC power failure during the recirculation phase was assessed to be of negligible probability compared to other safety system failures for the following reasons:

- For the case where offsite power is available, failure of individual AC buses by premature breaker transfers could probably be recovered within an acceptable time frame to mitigate the accident. These failures are of small probability compared to other safety system failure modes, at any rate. Loss of an entire train of AC power is an even smaller probability event.
- For the case where loss of offsite power is the initiating event, it was assumed that offsite power would be restored by the time that the recirculation phase started. This assumption was based on WASH 1400 data that show that the probability of restoration of offsite power three to ten hours after offsite power is lost is very high. Other options for recovering power by the recirculation phase include restoration of diesels that may have failed at the onset of the accident (Units 1 and 2 require offsite power for restart).

Modularized fault trees were constructed for each of the 4160VAC and 480VAC buses with offsite power available. For the loss of offsite power case, modularized fault trees were constructed for AC power Trains A and B, and for total loss of AC power.

Table D.4 shows the success requirements for AC power distribution, Table D.5 contains the top event definition for the modularized fault trees, and Figures D.3 through D.9 show the modularized fault trees for both the LOSP and Non-LOSP cases. The unavailability of each gate is shown on these trees, as well as the unavailability of the top events. Table D.6 presents the Boolean equations that represent the fault trees. Table D.7, the quantification table, shows the quantification of each gate, by component and failure mode. The attached notes describe the assumptions used in the quantification. Table D.8 summarizes the point estimates and the error factors for each gate.

Table D.4 AC Power

SUCCESS REQUIREMENTS

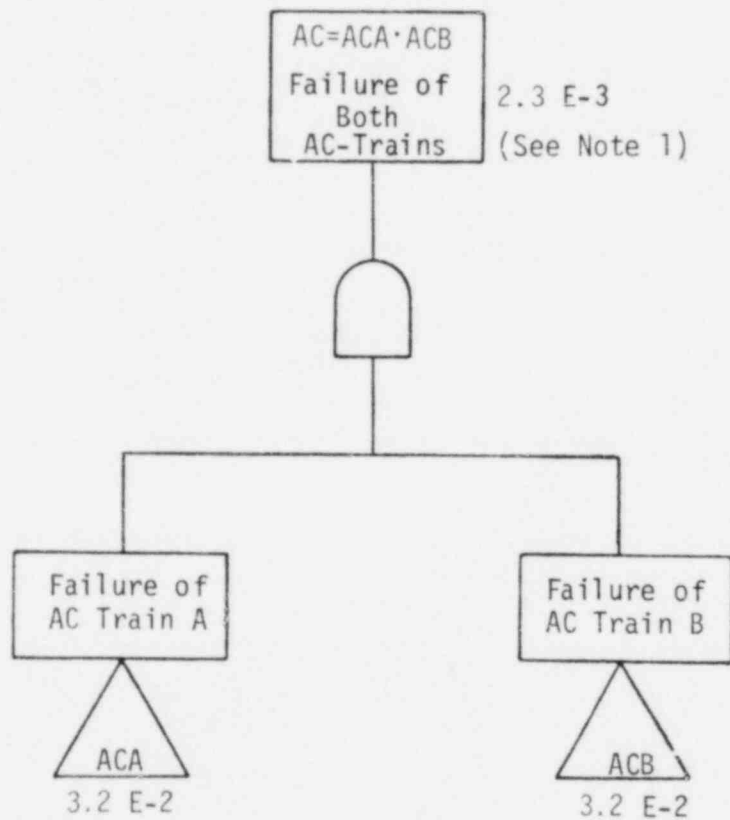
<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B1, B2, B3, B4 All Transients	1/1 480V, 4160V buses	1,2
LOSP	1/2 AC power trains	1,2,3

-
- NOTES: 1. Train A of AC power supplies power to the A trains of engineered safety systems. Train B supplies power to the B trains of these systems.
2. Analysis was performed for individual 480V buses for the case where offsite power is available. Analysis was performed for the A and B trains of AC power for the loss of offsite power case. No analysis was performed for the 120V AC vital buses for the offsite power available case, since these involve failures of the 480V buses, coupled with additional failures, which make the failure probabilities negligible.
3. For the loss of offsite power case, credit is given for obtaining power from units 1 and 2 through the auxiliary transformer. An assessment of the availability of this additional backup power source is contained in the analysis.

Table D.5 AC Power

TOP EVENT DEFINITIONS

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
Non-LOSP-CASE		
3A1	No power on 480VAC bus 3A-1	
MCC3A	No power on 480VAC bus MCC3A	
3A2	No power on 480VAC bus 3A-2	
3B1	No power on 480VAC bus 3B-1	
MCC3B	No power on 480VAC bus MCC-3B	
3B2	No power on 480VAC bus 3B-2	
MCC3AB	No power on 480VAC bus 3AB	
LOSP-CASE		
ACA	No power on 4160V ESF bus 3A	
ACB	No power on 4160V ESF bus 3B	
AC	No power on either 4160V ESF bus 3A and 3B	
A2	No power available from Units 1 and 2	



NOTE: (1) ACA and ACB are not independent, thus Boolean reduction is required to evaluate AC.

Figure D.3 Modularized Fault Tree for Event "AC" (LOSP)

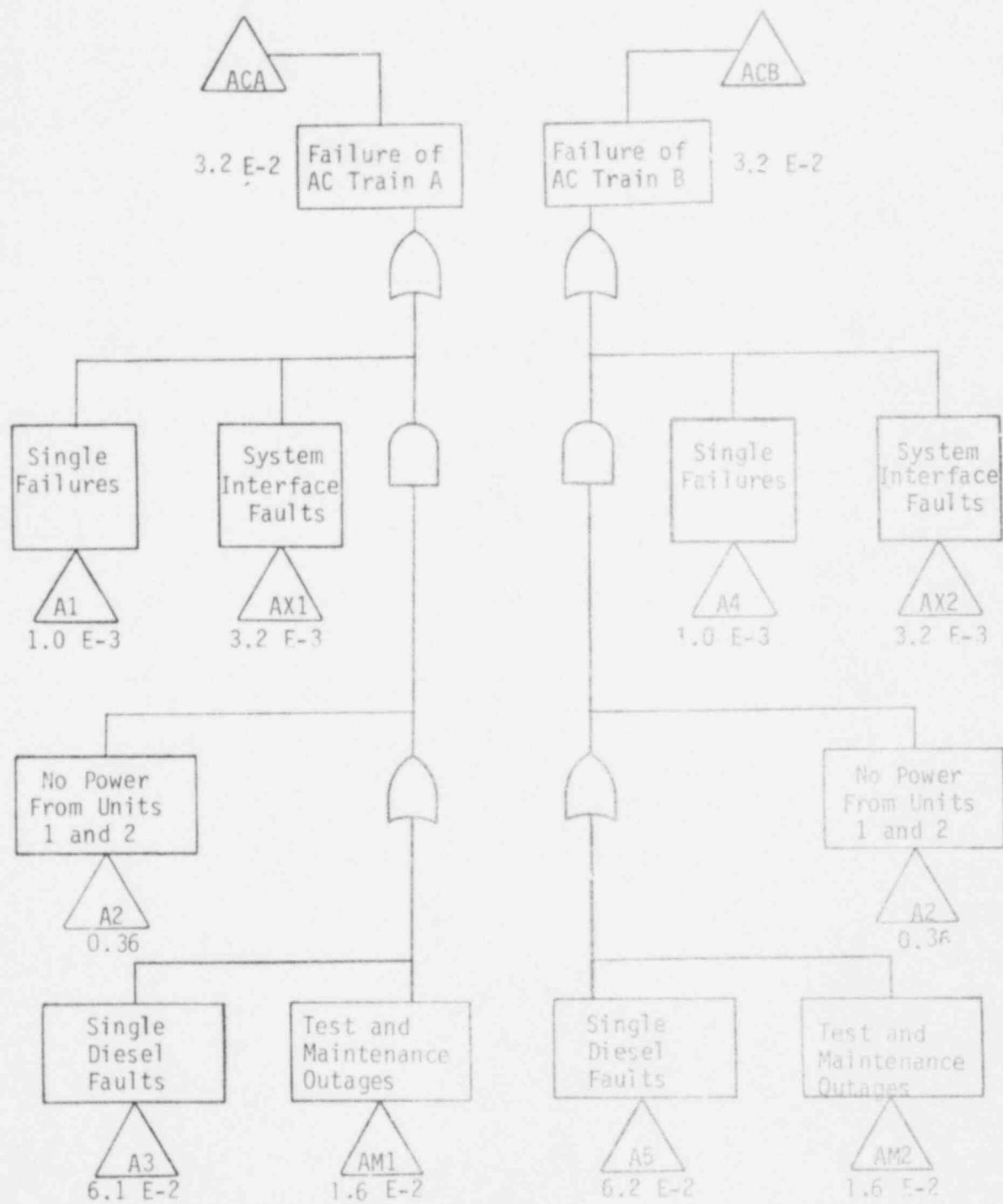


Figure D.4 Modularized Fault Trees for Events "ACA" and "ACB" (LOSP)

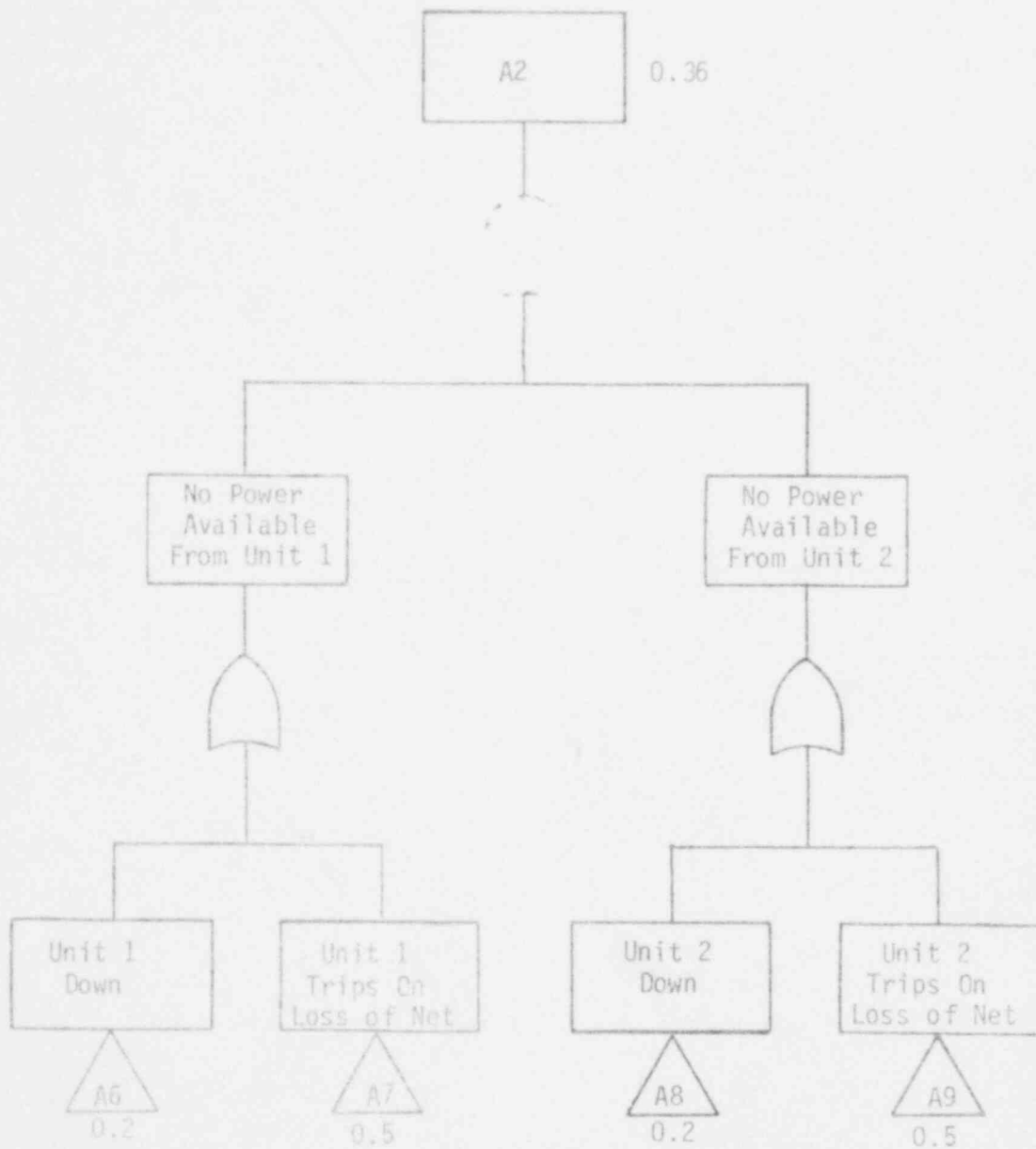


Figure D.5 Modularized Fault Tree for Event "A2" (LOSP)

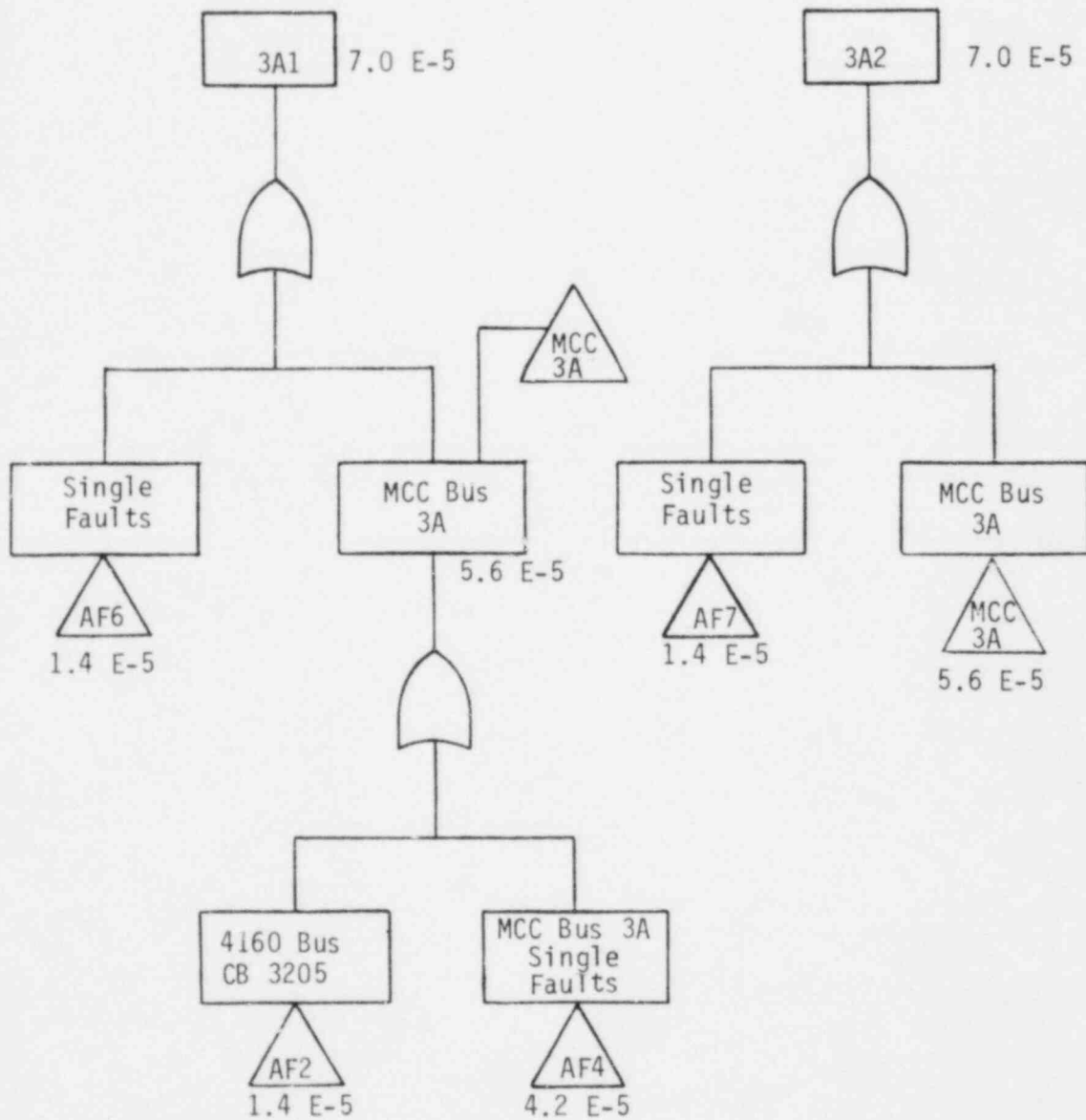


Figure D.6 Modularized Fault Trees for Events "3A-1" and "3A-2" (Non-LOSP)

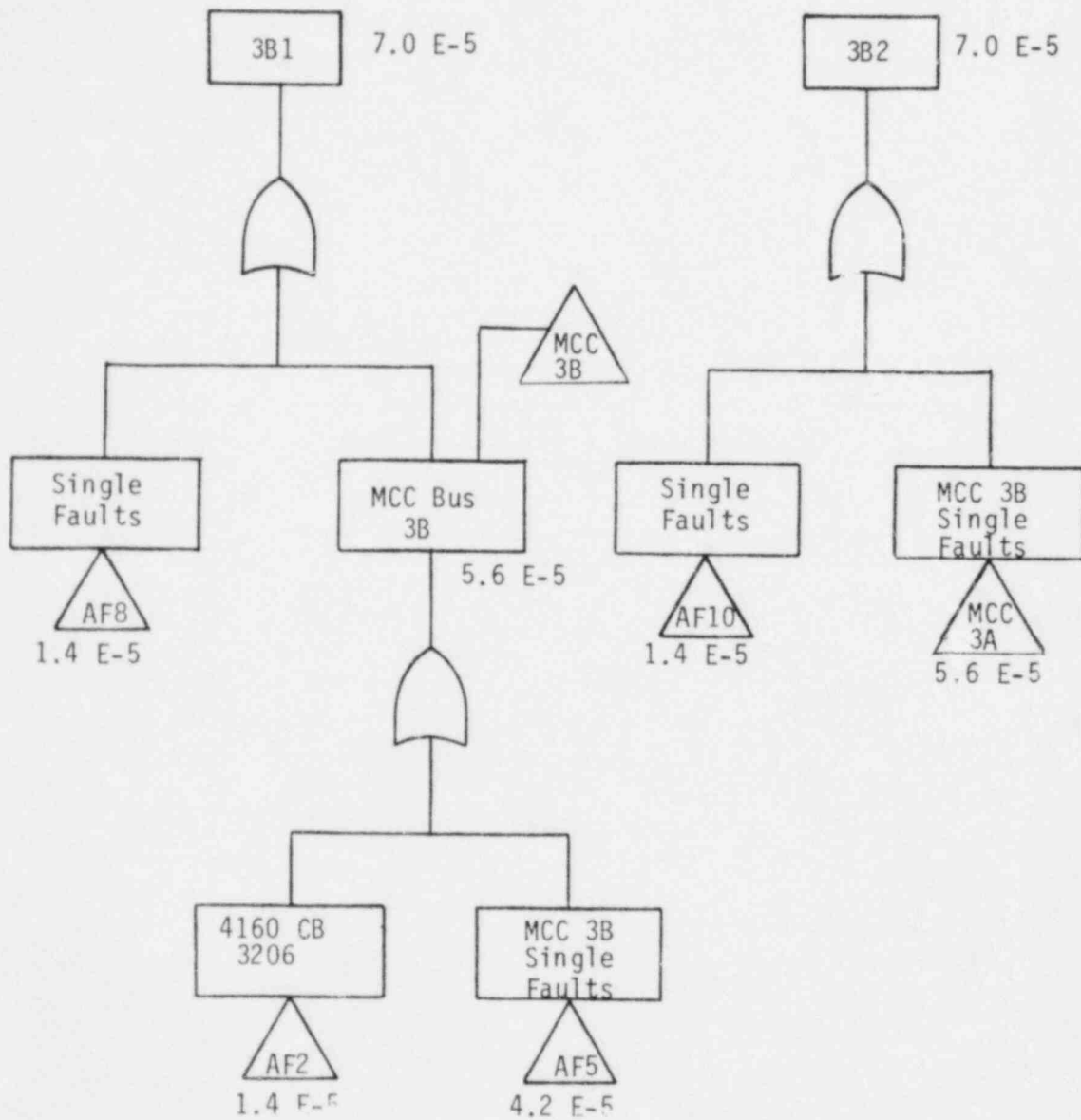


Figure D.7 Modularized Fault Trees for Events "3B-1" and "3B-2" (Non-LOSP)

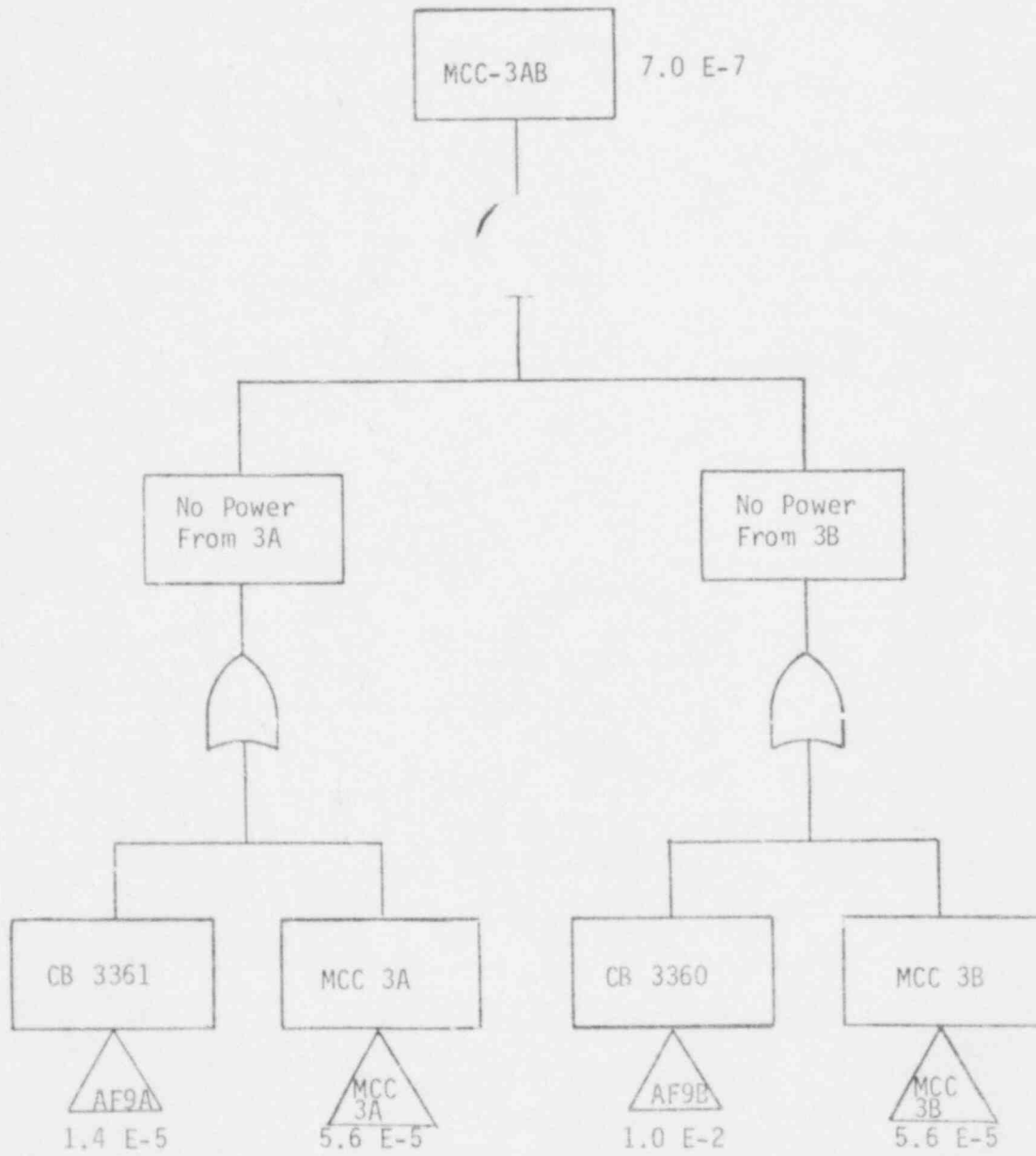


Figure D.8 Modularized Fault Tree for Event "MCC-3AB" (Non-LOSP)

Table D.6 (1/2) AC - Power LOSP

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

$$AC = ACA \cdot ACB$$

NOTES

(1)

INTERMEDIATE EVENTS

$$ACA = A1 + AX1 + A2 \cdot (A3 + AM1)$$

$$ACB = A4 + AX2 + A2 \cdot (A5 + AM2)$$

$$A2 = (A6 + A7) \cdot (A8 + A9)$$

$$AX1 = DCA$$

$$AX2 = DCB$$

BOOLEAN EQUATIONS REGROUPED FOR BOOLEAN REDUCTION

TOP EVENT

$$AC = (A1 + AX1) \cdot [A4 + AX2 + A2 \cdot (A5 + AM2)] + A2 \cdot [(A4 + AX2) \cdot (A3 + AM1) + A5 \cdot A3 \cdot AM2 + A5 \cdot AM1] \quad (2)$$

INTERMEDIATE EVENTS

SAME AS ABOVE

- NOTES: 1. This event AC is not Boolean reduced.
2. The event $AM1 \cdot AM2$ is prohibited by Technical Specifications and is therefore not included.

Table D.6 (2/2) AC - Power Non-LOSP

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

$$3A1 = AF6 + MCC3A$$

$$3A2 = AF7 + MCC3A$$

$$3B1 = AF8 + MCC3B$$

$$3B2 = AF10 + MCC3B$$

$$3AB = (AF9A + MCC3A) \cdot (AF9B + MCC3B)$$

INTERMEDIATE EVENTS

$$MCC3A = AF1 + AF4$$

$$MCC3B = AF2 + AF5$$

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
A1	CIRCUIT BKR 3205	SINGLE FAILURES TO TRAIN A			1.0 E-3			
		FAILS TO TRANSFER	D		1.0 E-3	3 ⁺ , 3 ⁻		
A2		POWER FROM UNITS 1 AND 2 NOT AVAILABLE			0.36			
A6	UNIT 1	DOWN	D		0.2			6
A7	UNIT 1	TRIPS ON LOSS OF NET	D		0.5			7
A8	UNIT 2	DOWN	D		0.2			6
A9	UNIT 2	TRIPS ON LOSS OF NET	D		0.5			7
					$\mu(\pm) = 0.36$			
A3		SINGLE FAULTS THAT FAIL POWER FROM DIESEL 3A			6.1 E-2			
	DG-3A	FAILS TO START	D		3.0 E-2	3 ⁺ , 3 ⁻		
	DG-3A	FAILS TO RUN	3.0 E-3	10	3.0 E-2	10 ⁺ , 10 ⁻		1
	RELAY LOGIC	AUTO START FAILS TO FUNCTION			NOT SIGNIFICANT			2
	CIRCUIT BKR 3209	FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
	RELAY LOGIC	CIRCUIT BREAKER FAILS TO FUNCTION			NOT SIGNIFICANT			2
	LOAD SHED, LOGIC	FAILS TO FUNCTION			NOT SIGNIFICANT			2
					$\Sigma = 6.1 E-2$			
AX1		SYSTEM INTERFACE FAULTS			3.2 E-3			
DCA	DC TRAIN A	FAILS ON LOSP			3.2 E-3			8
AF1		TRAIN A TEST & MAINTENANCE OUTAGES			1.6 E-2			3
	DG-3A	OUT FOR TEST	3/720	3	1.3 E-2	3 ⁺ , 3 ⁻	H	
	DG-3A	OUT FOR UNSCHEDULED MAINTENANCE	2/8760	15	3.5 E-3	3 ⁺ , 3 ⁻	M	
					$\Sigma = 1.6 E-2$			

Table D.7 (1/5) Events "ACA" and "A2" Quantification (LOSP)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
A4		SINGLE FAILURES TO TRAIN B			1.0 E-3			
	CIRCUIT BKR 3206	FAILS TO TRANSFER	D		1.0 E-3	3 ⁺ , 3 ⁻		
A2		POWER FROM UNITS 1 AND 2 NOT AVAILABLE (SEE EVENT A4)			0.36			
A5		SINGLE FAULTS THAT FAIL POWER FROM DIESEL 3B			6.2 E-2			
	DG-3B	FAILS TO START	D		3.0 E-2	3 ⁺ , 3 ⁻		
	DG-3B	FAILS TO RUN	3.0 E-3	10	3.0 E-2	10 ⁺ , 10 ⁻		1
	RELAY LOGIC	AUTO START FAILS TO FUNCTION			NOT SIGNIFICANT			2
	CIRCUIT BKR 3210	FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
	RELAY LOGIC	CIRCUIT BREAKER LOGIC FAILS TO FUNCTION			NOT SIGNIFICANT			2
	LOAD SHED. LOGIC	FAILS TO FUNCTION			NOT SIGNIFICANT			2
	CIRCUIT BKR 3312	FAILS TO OPEN	D		1.0 E-3	3 ⁺ , 3 ⁻		2
	RELAY LOGIC	CIRCUIT BREAKER FAILS TO FUNCTION			NOT SIGNIFICANT			2
	ESAS-B	NO ESAS SIGNAL AND NO RECOVERY	D		NOT SIGNIFICANT			2
					$\bar{t}=6.2 \text{ E-2}$			
AX2		SYSTEM INTERFACE FAULTS			3.2 E-3			
DCB	DC TRAIN B	FAILS ON LOSP			3.2 E-3			8
A12		TRAIN B TEST & MAINTENANCE OUTAGES			1.6 E-2			3
	DG-3B	OUT FOR TEST	3/720	3	1.3 E-2	3 ⁺ , 3 ⁻	M	
	DG-3B	OUT FOR UNSCHEDULED MAINTENANCE	2/8760	15	3.5 E-3	3 ⁺ , 3 ⁻	M	
					$\bar{t}=1.6 \text{ E-2}$			

Table D.7 (2/5) Event "ACB" Quantification (LOSP)

Table D.7 (3/5) Events "3A-1" and "MCC-3A" Quantification (Non-LOSP)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
AF6	CIRCUIT BKR 3341	SINGLE FAULTS TO EVENT 3A-1	1.0 E-6	14	1.4 E-5	3 ⁺ , 3 ⁻		4
FCC3A		PREMATURE TRANSFER (OPEN)			1.4 E-5			
AF1	MCC BUS 3A UNAVAILABLE				5.6 E-5			
	SINGLE FAULTS, 5160V BUS A				1.4 E-5			
AF4	CIRCUIT BKR 3205	PREMATURE TRANSFER	1.0 E-6	14	1.4 E-5	3 ⁺ , 3 ⁻		4
	MCC BUS 3A SINGLE FAULTS				4.2 E-5			
	TRANSFORMER 3A	SAFEGUARD AUX. TRANSFORMER 3A SHORTS	1.0 E-6	4	4.0 E-6	3 ⁺ , 3 ⁻		4
	TRANSFORMER 3A	FAILS TO OPERATE	1.0 E-6	10	1.0 E-5	3 ⁺ , 3 ⁻		5
	CIRCUIT BKR 3311	PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	3 ⁺ , 3 ⁻		4
	CIRCUIT BKR 3221	PREMATURE TRANSFER (OPEN)	1.0 E-5	1	1.4 E-5	3 ⁺ , 3 ⁻		4
					<u>Σ=4.2 E-5</u>			

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
AF7	CIRCUIT BKR 3351	SINGLE FAULTS TO EVENT 3A-2			1.4 E-5			
		PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	3 ⁺ , 3 ⁻		4
AF8	CIRCUIT BKR 3340	SINGLE FAULTS TO EVENT 3B-1			1.4 E-5			
		PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	3 ⁺ , 3 ⁻		4
AF2	CIRCUIT BKR 3206	MCC BUS 3B UNAVAILABLE			5.6 E-5			
		SINGLE FAULTS, 4160V BUS B			1.4 E-5			
AF5	TRANSFORMER 3B	PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	3 ⁺ , 3 ⁻		4
		MCC BUS 3B SINGLE FAULTS			4.2 E-5			
	TRANSFORMER 3B	SAFEGUARD AUX. TRANSFORMER 3B SHORTS	1.0 E-6	4	4.0 E-6	3 ⁺ , 3 ⁻		4
	TRANSFORMER 3B	FAILS TO OPERATE	1.0 E-6	10	1.0 E-5	3 ⁺ , 3 ⁻		5
	CIRCUIT BKR 3310	PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	3 ⁺ , 3 ⁻		4
	CIRCUIT BKR 3220	PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	3 ⁺ , 3 ⁻		4
					$\Sigma=4.2 E-5$			
AF10	CIRCUIT BKR 3350	SINGLE FAULTS TO EVENT 3B-2			1.4 E-5			
		PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	3 ⁺ , 3 ⁻		4

Table D.7 (4/5) Events "3A-2", "3B-1", and "3B-2" Quantification (Non-LOSP)

Table D.7 (5/5) Event "MCC-3AB" Quantification (Non-LOSP)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
AF9A		SINGLE FAULTS TO BUS 3A			1.4 E-5			
	CIRCUIT BKR 3361	PREMATURE TRANSFER	1.0 E-6	14	1.4 E-5	3 ⁺ , 3 ⁻		4
AF9B		SINGLE FAULTS TO BUS 3B, AND OPERATOR FAILS TO TRANSFER			1.0 E-2			
	CIRCUIT BKR 3360	PREMATURE TRANSFER	1.0 E-6	14	1.4 E-5	3 ⁺ , 3 ⁻		4
	SWITCH MCC3A-B	TRANSFER SWITCH FAILS TO CLOSE	D		1.0 E-5	3 ⁺ , 3 ⁻		
	OPERATOR	FAILS TO TRANSFER	D		1.0 E-2	3 ⁺ , 10 ⁻	0	
					<u>Σ=1.0 E-2</u>			

Table D.7 AC Power

QUANTIFICATION TABLES

NOTES

- 1 Times for the injection phase can vary from 0.5 to 10 hours depending on LOCA size. A fault duration time of 10 hours was conservatively chosen for the injection time.
- 2 This fault was not evaluated but was assumed to be of lower probability than other faults in this gate.
- 3 Testing occurs approximately three times a month with an average duration of three hours. Testing itself does not remove the diesel from service; however, loss of offsite power during testing would present the diesel with a full-load reject situation, which is assumed to trip the diesel off-line. Unscheduled maintenance occurs approximately two times per year with an average duration of 15 hours.
- 4 Technical Specifications require the plant to go to hot shutdown within eight hours after loss of AC-bus. This fault was assessed as an unavailability of a failed equipment.
- 5 Ten hours fault duration time was conservatively assumed to represent the injection phase.
- 6 Availability for unit is defined as portion of time plant is producing power or in spinning reserve. Plant records show this to be about 80% of the time for CR-1 and CR-2.
- 7 Unit has experienced two opportunities to run back on loss of offsite power, and has been successful once. Hence, the probability of a successful runback was estimated as 0.5.
- 8 See DC Power Distribution System quantification tables for LOSP case.

Table D.8 AC Power Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
A1	1.0 E-3
A2	0.36
A6	0.2
A7	0.5
A8	0.2
A9	0.5
A3	6.1 E-2
AX1	3.2 E-3
DCA	3.2 E-3
AM1	1.6 E-2
A4	1.0 E-3
A5	6.2 E-2
AX2	3.2 E-3
DCB	3.2 E-3
AM2	1.6 E-2
AF6	1.4 E-5
MCC3A	5.6 E-5
AF1	1.4 E-5
AF4	4.2 E-5
AF7	1.4 E-5
AF8	1.4 E-5
MCC3B	5.6 E-5
AF2	1.4 E-5
AF5	4.2 E-5
AF10	1.4 E-5
AF9A	1.4 E-5
AF9B	1.0 E-2

APPENDIX E

NUCLEAR SERVICES CLOSED CYCLE COOLING SYSTEM

APPENDIX E NUCLEAR SERVICES CLOSED CYCLE COOLING SYSTEM (NSCCCS)

E.1 SYSTEM DESCRIPTION AND OPERATION

The Nuclear Services Closed Cycle Cooling System (NSCCCS) is a safety related system which provides cooling to various nuclear oriented equipment during normal and emergency operation. Typical loads during emergency operation are makeup pumps MUP-1A and 1B (part of the HPI system), reactor building fan assembly cooling coils, ventilation fan motor coolers, and control complex chillers. In addition, the NSCCCS provides cooling to its own pumps and to the pumps of the Nuclear Services Seawater System (NSSWS). The NSSWS is part of the Raw Seawater System and serves as a heat sink for the NSCCCS.

E.1.1 SYSTEM DESCRIPTION

The NSCCCS, shown in Figure E.1, is a single closed loop system that removes heat from the containment atmosphere and component heat. The once-through Nuclear Services Seawater System (NSSWS), shown in Figure E.2 takes suction from the seawater sump, removes heat from the closed cycle loop, and discharges into the seawater discharge canal. Component design information for the major components in these systems is given in Table E.1

The NSCCCS consists of one normally operating pump, SWP-1C, and two 100% rated emergency pumps, SWP-1A and -1B. The non-safety pump SWP-1C is sized to supply the normal flowrate of 6900 gpm — which is insufficient for emergency operation. The emergency flow rate of 11,000 gpm can be delivered by each of the two emergency pumps. SWP-1A and -1B each consists of two half-sized pumps driven by a single shaft. Each of the five pumps has a check valve in the discharge line and a manual blocking valve on either side. The pumps discharge into a single header. The main line is 18 inches in diameter. At each heat load center, smaller lines supply water to the individual components. Most of the major heat load centers can be isolated by manual block valves.

The heat absorbed by the NSCCCS is transferred to the NSSWS by a bank of four one-third capacity heat exchangers (HE). Three operable heat exchangers are required for both emergency and normal operation. The HE's have no automatic isolation capability. Each HE has an inlet and outlet manual blocking valve on both the seawater side and the primary side. The heat exchangers are of the shell and tube type, with seawater flow through the tubes. The NSCCCS emergency flow rate of 3700 gpm per HE results in a heat rejection rate of 92×10^6 BTU/hr per heat exchanger. Outlet temperature of the HE's is 105°F under emergency operation.

The NSSWS has one non-safety pump for normal operation and two 100% redundant emergency pumps. The non-safety pump RWP-1 is sized for a normal flow rate of 10,800 gpm and cannot supply the emergency flow rate of 14,100 gpm (4700 gpm/HE). Each pump is provided with a check valve on the discharge side and with manual blocking valves on both sides for isolation purposes. The inlet temperature is determined by the Gulf of Mexico. Technical Specification prohibits operation if the inlet temperature rises above 105°F . For environmental reasons, the temperature rise through the heat exchanger is limited to a maximum of 6°F . Seawater flows by gravity from the intake canal to the seawater sump, through 48 inch pipes. The emergency pumps are installed in separate compartments of the seawater sump to allow the isolation of either compartment for service without disabling the system.

The pump motors are cooled by the NSCCCS. The bearing is cooled by the domestic water supply. If that system fails, the demineralized water supply can provide water through the domestic water lines. If both of these systems fail, seawater will back into the bearing. This provides adequate cooling although it is not desirable for long-term cooling because of corrosion considerations.

The NSSWS has no MOV's or remotely operated valves. There are no locked valves in the system. Manual valves are locally indicated.

The pumps in the NSCCCS and NSSWS are powered from the 4160V ESF buses.

E.1.2 SYSTEM OPERATION

The NSCCCS and the NSSWS are continuously operating systems required for normal plant operation. Upon ESAS, the nonessential loads on the NSCCCS are isolated by closing the inlet and outlet valves in the appropriate line. These loads are primarily isolated to protect against missile damage to the NSCCCS and subsequent drainage of the system. The loads involved are not active during post-LOCA time periods. The ESAS will start both NSCCCS pumps (SWP-1A, -1B) and both Raw Water Pumps (RWP-2A, -2B). Fifteen seconds after either emergency pump in each system starts, the corresponding non-safety pump is tripped.

If one HE is inoperable due to rupture, blockage, or electrolytic erosion/corrosion, the HE-bank can be reconfigured during plant operation by isolating the faulty exchanger on both sides and opening the block valves on both sides of the inactive heat exchanger. The inactive HE is not required to be tested for operability. There is a procedure for freshwater layup on the seawater side to prevent marine growth for long periods of time.

The pumps SWP-1A, -B and RWP-2A, -2B are required to be started once a month (SP-344). The pumps are tested on a two-week staggered basis. Testing of the pumps does not disrupt system service. Technical Specifications require that two emergency pumps be operable in each system. Plant operation can continue for not more than 72 hours if only one emergency pump is available in the NSCCCS or in the NSSWS.

Table E.1

Component Design Information

Nuclear Service Heat Exchangers

Number	4
Type	Shell and Tube
Sea Cooling Water Flow (tubeside), gpm	4700 Emerg; 3600 Normal
Sea Cooling Water Temperature, F	85
Closed Cycle Cooling Water Outlet Temp, F	105 Emerg; 90 Normal
Closed Cycle Cooling Water Flow (shell side), gpm	3700 Emerg; 2300 Normal
Tube Material	90-10 Cu-Ni
Shell Material	Welded Carbon Steel
Channel Material	2% Nickel Cast Iron
Design Pressure, Shell/Tube, psig	200/100
Design Temperature, Shell/Tube, F	180/150
Code/Seismic Class	ASME Section VIII/I
Duty Btu/h	92×10^6 Emergency

Nuclear Service Seawater Pumps

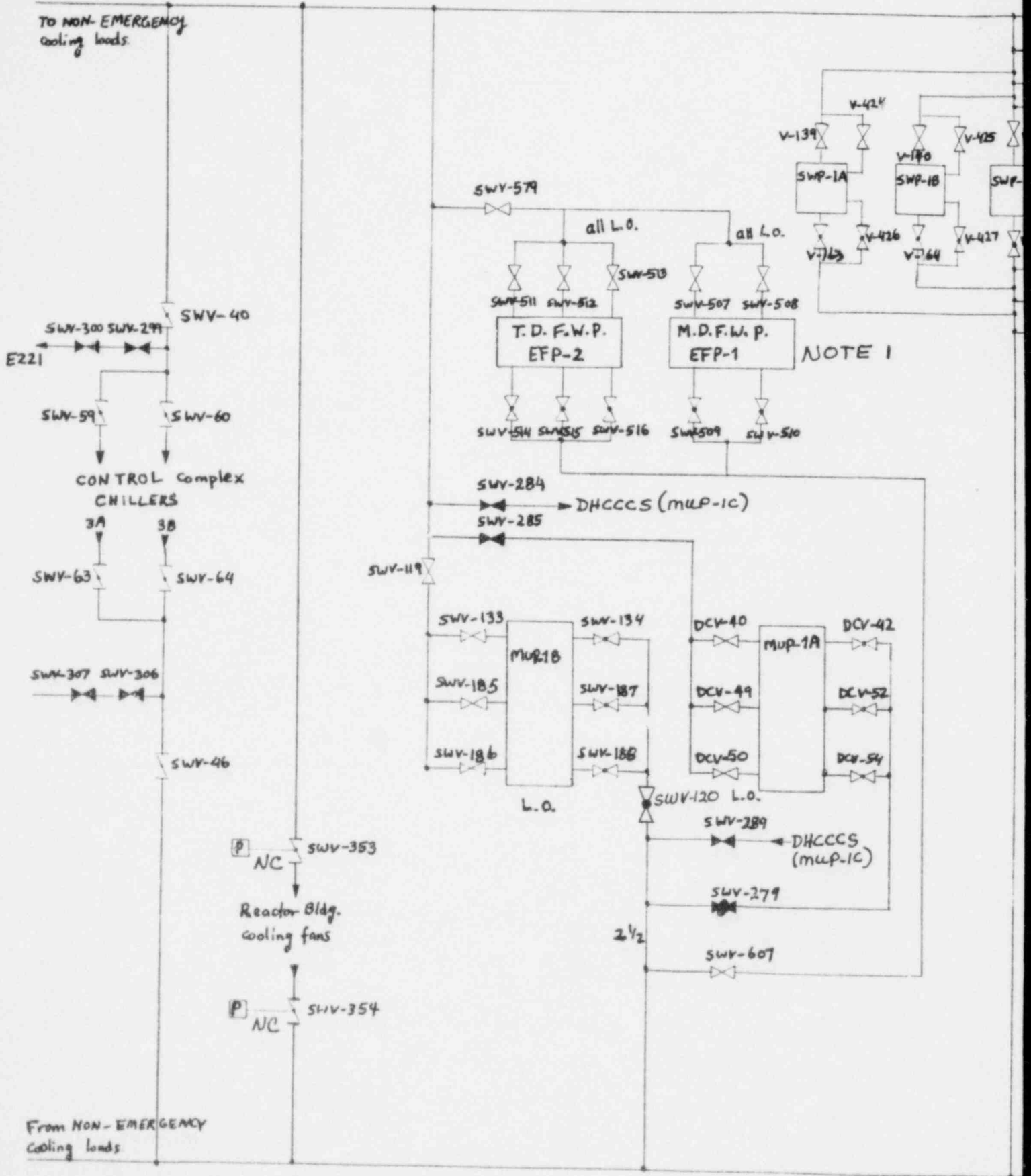
Number	2 Emerg; 1 Normal
Flow, gpm	14,100 Emerg; 10,800 Normal
Design Head, ft	144 Emerg; 98 Normal
Design Pressure, psig	100
Design Temperature, F	109
Seismic Class	I

Nuclear Service Closed Cycle Cooling Pumps

Number	2 Emerg; 1 Normal
Flow, gpm	11,000 Emerg; 6,900 Normal
Design Head, ft	190 Emerg; 110 Normal
Design Pressure, psig	200
Design Temperature, F	135
Seismic Class	I

Nuclear Service Closed Cycle Surge Tank

Number	1
Capacity, gal.	10,000
Design Temperature, F	135
Design Pressure, psig	100
Material	Carbon Steel, ASTM
Code/Seismic Class	ASME Section VIII/I



NOTE 1: Piping for cooling of EFP -1 and -2 still exists but pumps are self-cooled

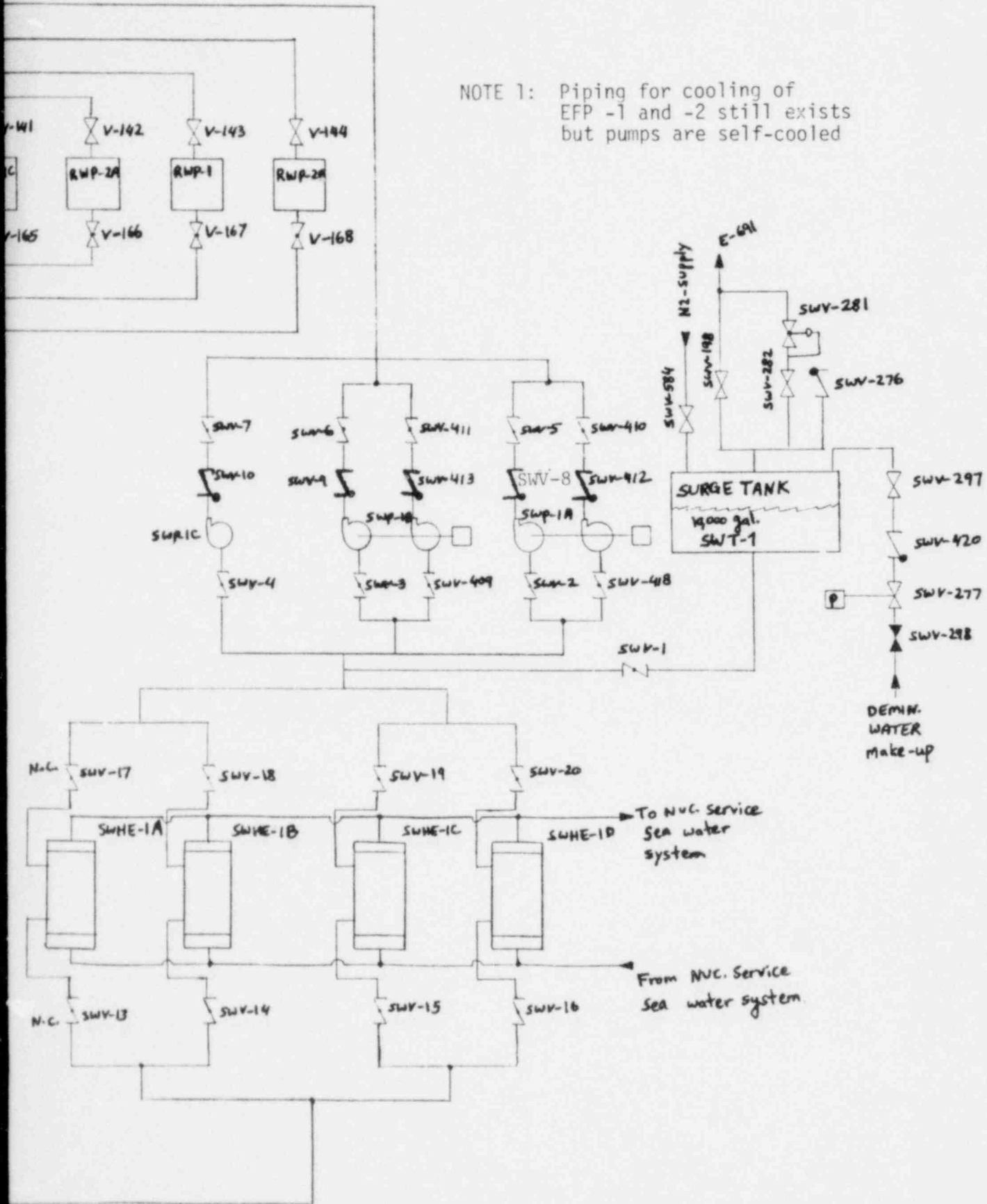


Figure E.1 Nuclear Services Closed Cycle Cooling System Schematic Diagram

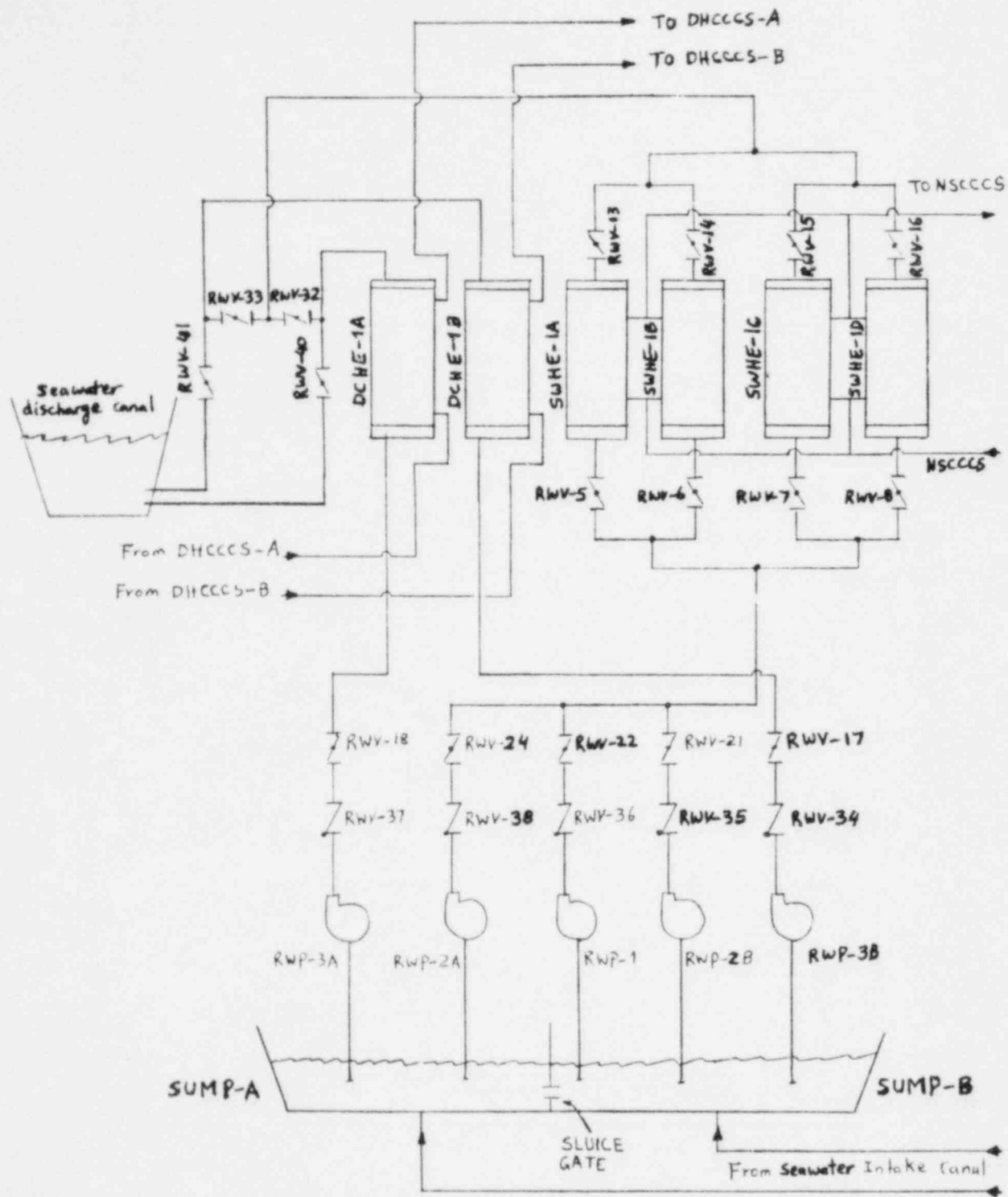


Figure E.2 Nuclear Services Seawater System Schematic Diagram

E.2 SYSTEM SIMPLIFIED FAULT TREE

Detailed fault trees were initially drawn for both the NSCCCS and the NSSWS. The detailed trees were simplified and combined in a series of intermediate steps to arrive at a single simplified tree. The top event for this fault tree is defined as:

NSCCCS Failure - failure of the NSCCCS to produce rated emergency flow at the rated temperature and head at the pump discharge header.

Because of the fact that several pump operability states are possible, several separate simplified fault trees were constructed to describe these cases. Figure E.3 is the simplified fault tree for the normally operating configuration, with the non-emergency pumps (SWP-1C and RWP-1) in service. Figure E.4 is the simplified fault tree for one of the four possible cases where both non-emergency pumps are not in service and one emergency pump is running in each system. Figures E.5 and E.6 are the simplified fault trees for two of the four possible cases where one system is operating with an emergency pump in service and the other system is operating with a normal (non-emergency) pump in service. The evaluation was performed only for the normally operating configuration (the tree shown in Figure E.3), which is the most conservative case. Since it was subsequently found that this system is not a dominant contributor to any of the dominant sequences, it was unnecessary to evaluate the other cases.

MAJOR ASSUMPTIONS

The assumptions used to construct the detailed fault trees for NSCCCS and NSSWS before they were combined in the simplified trees are listed in the following two subsections.

NSCCCS - Fault Tree

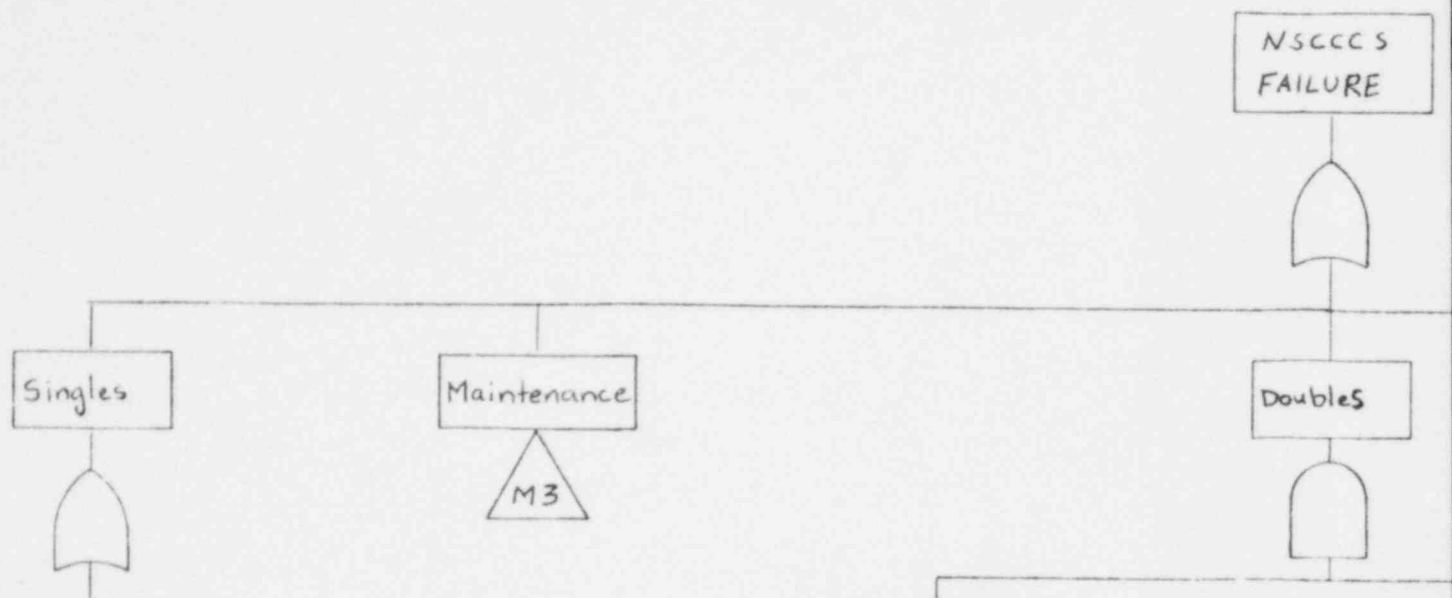
1. The NSCCCS is normally in operation. Correct valve alignment in the major flow lines is assumed to exist at the time of an ESAS signal. For the purpose of this analysis it is assumed that pump SWP-1C is running (see also Section E.1). The emergency pumps are not normally in operation. Therefore, mispositioning of the block valves in the emergency pump lines is addressed.
2. If pressure is lost in the surge tank, the pumps will not cavitate.

3. The normal nuclear service pump can not supply the emergency flow rate.
4. Failure to isolate nonessential loads from the NSCCCS is not necessarily a failure (these loads being the CRDM coolers, RCP motor coolers, waste evaporators, etc.). The loads are not isolated for heat load or hydraulic considerations. Isolation is desirable because the components are not missile protected and are located in LOCA-missile susceptible areas.
5. SWP-1A and 1B and the associated check valves (SWV-9, 413, 8, 412) are each tested once a month on a staggered basis.
6. The pumps are self-cooled. Blockage of the NSCCCS pump motor cooling lines when these pumps are in service was not considered. Blockage of these lines was considered for standby pumps.
7. The system does not require reconfiguration for testing.
8. Components, lines, and valves that were considered to be insignificant were omitted from the fault trees.

NSSWS - Fault Tree

1. The system is normally in operation. Correct valve alignment in the major flow lines is assumed to exist at the time of an ESAS signal. For the purpose of this analysis it is assumed that pump RWP-1 is running. The emergency pumps are not normally in operation. Therefore, mispositioning of the block valves in the emergency pump lines is addressed.
2. RWP-2A and 2B are cooled by the NSCCCS. If the motor loses cooling, it is assumed to fail immediately. Loss of cooling to the bearing is not significant for this study. The bearing pot is supplied by three sources. Cooling is accomplished by circulation of water through the bearing pot. The primary source of water is the domestic water system. The demineralized water system backs up the domestic water supply system. If both of these systems fail, seawater will back into the bearing. This provides adequate cooling. It is not done on a permanent basis because it is undesirable from a corrosion standpoint.
3. The Auxiliary Building contains the two DHCCCS pumps, the four NSCCCS heat exchangers, the two DHCCCS heat exchangers, and the three surge tanks. Common causative damage events could result in significant flooding of the room. This is a single fault for both RWP-2A and 2B. However, the pump room is large and is equipped with a sump pump.

4. Pump cavitation was considered unlikely enough to be ignored.
5. The normal seawater service pump cannot supply the emergency flow rate.
6. Pump and check valve testing do not cause the system to be unavailable.
7. It was assumed the intake canal never goes dry while the plant is operating. T.S. 3.4.7.5 limits the bottom of the canal to EL 74 and the minimum water level to EL 81. T.S. 4.7.5.1 requires the inlet water temperature and water level to be checked every 24 hours. It was further assumed the seawater sump never goes dry. Either section may be taken out of service for maintenance, one at a time. There is a 48" pipe which gravity feeds the seawater sump from the intake structure. A separate pipe goes from the intake structure to each sump. A sluice gate also connects the two sumps. The canal is wide enough to preclude blockage by shipwreck. There are large grates on the intake structure which remove trash, seaweed, flotsam, and jetsam from the seawater. It was assumed that blockage of these grates to the extent that they block flow is not possible.
8. OP-416 contains a procedure for the lay-up of the seawater side of the inactive NSCCCS heat exchanger (SWHE) to prevent marine growth. This basically is a gravity drain and flush with domestic water. It involves opening and closing of drain valves, vent valves, and fill valves. Because these lines are very small, discharge rates would be very small if a valve was inadvertently left in the wrong position. For this reason, improper filling procedure was not considered a possible fault.
9. Due to its nature, the seawater system is exposed to a very corrosive-marine growth environment. Equipment in the system was therefore assigned higher failure rates (an order of magnitude) than would have been the case for equipment operating in freshwater. Failure (plugging, blockage, marine-encrustation) of equipment in the dormant state was also considered. However, plugging and blockage of equipment while in operation was not considered likely.
10. Components, lines, and valves that were considered to be insignificant were omitted from the fault trees.



1. Pipe Rupture - NSCCCS

2. Pipe Rupture - NS seawater

3. Non-Isolable valve rupture - fans

4. Non-isolable valve rupture - NSCCCS

5. Non-isolable valve rupture - seawater

6. Non-Isolable expansion joint rupture - seawater

7. Expansion tank SWT-1, rupture expansion

8. Failure of N2 pressure in expansion Tank.

- | | | | |
|---------------------------------|---------------------------------|----------|---------|
| | (note10) | (note10) | |
| 1. RWP-2A fail to start | 1. RWP-2B fail to start | 13. SWV | |
| 2. RWP-2A fail to run | 2. RWP-2B fail to run | 14. SWV | |
| 3. 4160 ES-3A fail | 3. 4160 ES-3B fail | | |
| (note4) 4. ESAS - train A fail | 4. ESAS train B fail (note4) | 1. SWHE | |
| (note2) 5. RWV-38 fail to open | 5. RWV-35 fail to open (note2) | 2. SWHE | |
| note 1 { 6. RWV-24 closed | 6. RWV-21 closed | 3. SWHE | |
| 7. SWV-142 closed | 7. SWV-149 closed | 4. SWHE | |
| (note6) 8. SWV-166 closed | 8. SWV-168 closed | 5. SWHE | |
| 1. SWP-1A fail to start | 1. SWP-1B fail to start | 6. SWHE | |
| 2. SWP-1A fail to run | 2. SWP-1B fail to run | | |
| 3. 4160 ES-3A fail | 3. 4160 ES-3B fail | | |
| (note4) 4. ESAS - train A fail | 4. ESAS train B fail (note4) | | |
| (note3) 5. SWV-8 fail to open | 5. SWV-9 fail to open (note3) | | |
| (note3) 6. SWV-412 fail to open | 6. SWV-413 fail to open (note3) | | |
| note 1 { 7. SWV-5 closed | 7. SWV-6 closed | 1. Missi | cooler |
| 8. SWV-410 closed | 8. SWV-411 closed | | |
| 9. SW-2 closed | 9. SWV-3 closed | 1. Missi | or cool |
| 10. SWV-408 closed | 10. SWV-409 closed | | |
| 11. SWV-139 closed | 11. SWV-140 closed | | |
| 12. SWV-424 closed | 12. SWV-425 closed | | |

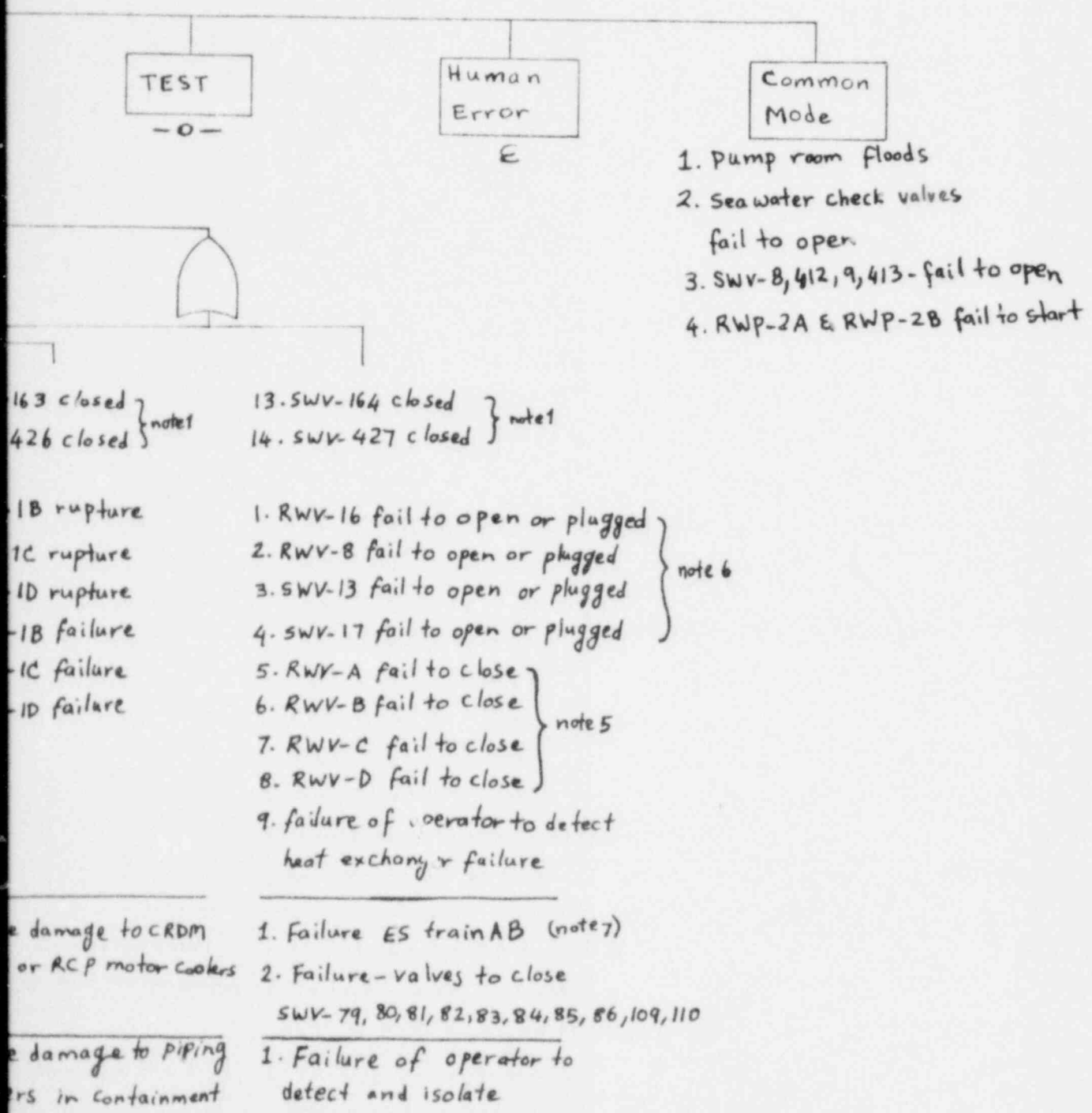


Figure E.3 (1/2) Simplified Fault Tree - NSCCCS SWP-1C, RWP-1 Operating (Normal System Configuration)

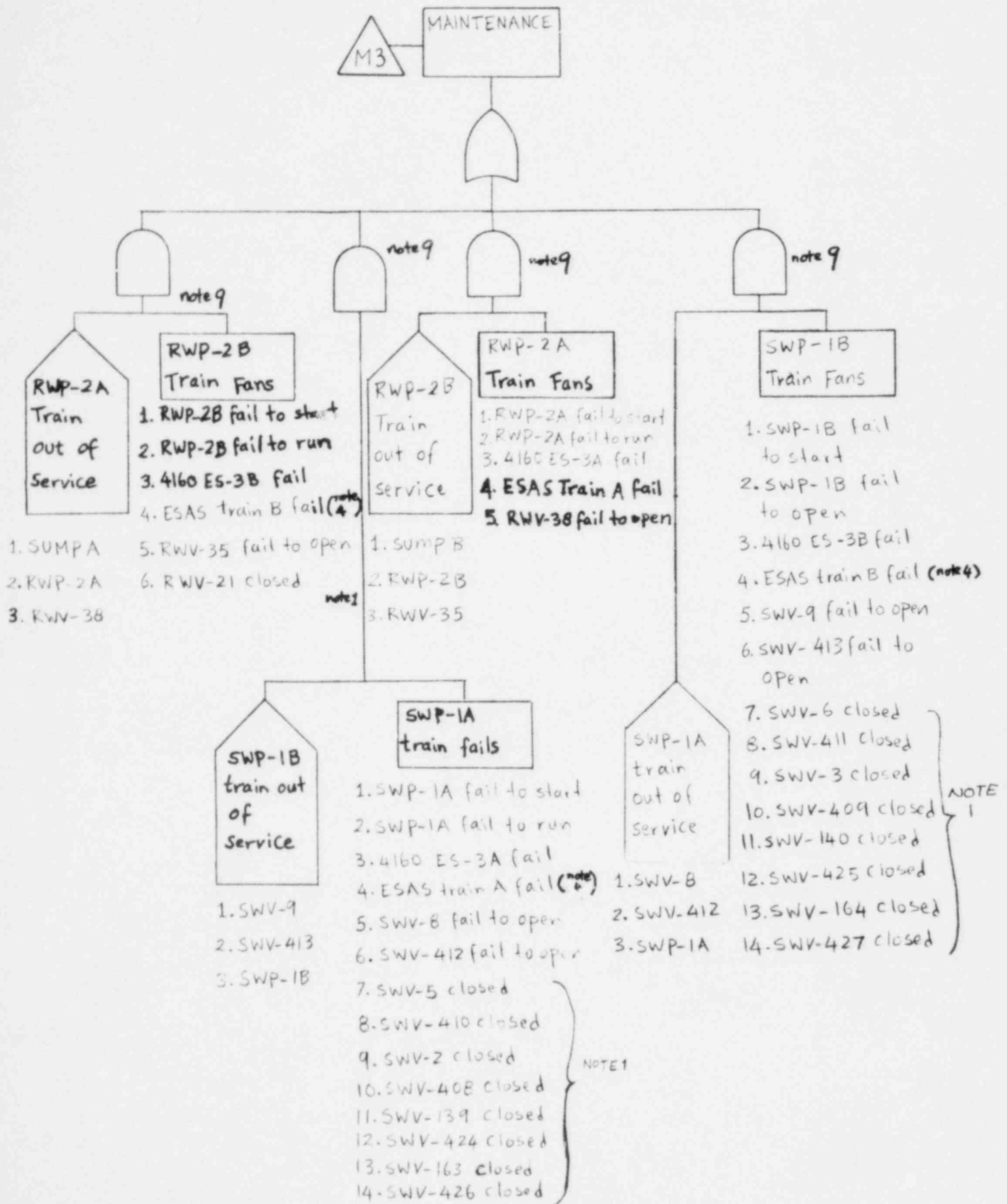


Figure E.3 (2/2) Simplified Fault Tree - NSCCCS SWP-1C, RWP-1 Operating (Normal System Configuration)

FAILURE NSCCCS

Singles

MAINTENANCE

DOUBLES

M4

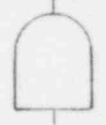
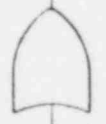
- 1. Pipe rupture-NSCCCS
- 2. pipe rupture- NS seawater
- 3. Non-isolable valve rupture-fans
- 4. Non-isolable valve rupture-NSCCCS
- 5. Non-isolable valve rupture-seawater
- 6. Non-isolable expansion joint rupture-seawater
- 7. Expansion tank SWT-1 rupture

- 1. RWP-2A fails to run
- 2. 4160 ES-3A fail

- 1. RWP-2B fails to start (note 10)
- 2. RWP-2B fails to run
- 3. 4160 ES-3B fails
- 4. ESAS train B fail (note 4)
- 5. RWV-35 fail to open (note 2)
- 6. RWV-21 closed
- 7. SWV-149 closed
- 8. SWV-168 closed

- 1. SWP-1A fails to run
- 2. 4160 ES-3A fail

- 1. SWP-1B fail to start
- 2. SWP-1B fail to run
- 3. 4160 ES-3B fail
- 4. ESAS train B fails note 4
- 5. SWV-9 fails to open note 3
- 6. SWV-413 fails to open note 3
- 7. SWV-6 closed
- 8. SWV-411 closed
- 9. SWV-3 closed
- 10. SWV-409 closed



1. S
2. S
3. S
4.
5. S
6. S
1. M
CR
m
1. M
Pi
in

TEST

HUMAN
ERROR

COMMON
MODE

1. pump room floods



- 11. SWV-140 closed
 - 12. SWV-425 closed
 - 13. SWV-164 closed
 - 14. SWV-427 closed
- } note 1

SWHE-1B rupture
SWHE-1C rupture
SWHE-1D rupture
SWHE-1B failure
SWHE-1C failure
SWHE-1D failure

- 1. RWV-16 fail to open or plugged
 - 2. RWV-B fail to open or plugged
 - 3. SWV-13 fail to open or plugged
 - 4. SWV-17 fail to open or plugged
- } note 6

- 5. RWV-A fail to close
 - 6. RWV-B fail to close
 - 7. RWV-C fail to close
 - 8. RWV-D fail to close
- } note 5

9. failure of operator to detect - heat exchanger failure

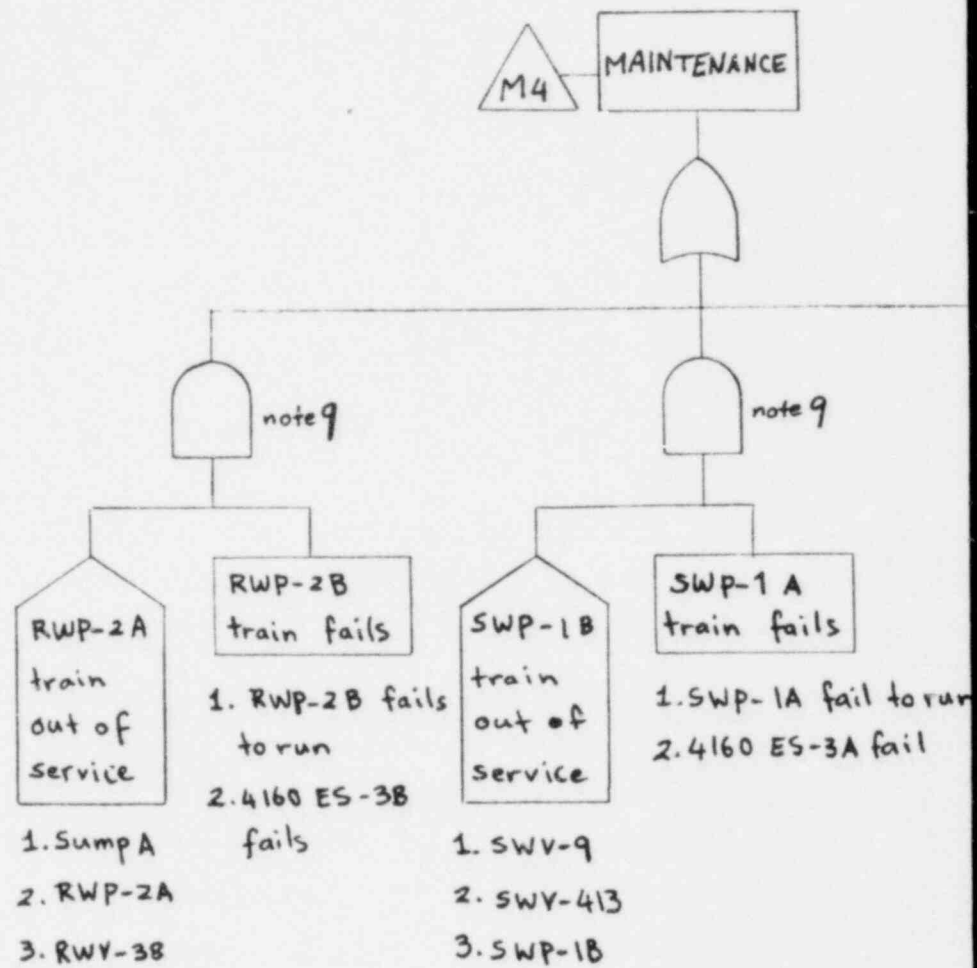
Missile damage to
DM coolers of RCP
for coolers.

- 1. Failure of ES train AB (note 7)
- 2. Failure of valve to close
SWV-79, 80, 81, 82, 83, 84, 85, 86, 109, 110

Missile damage to
piping or fan coolers
containment

- 1. Failure of operator to detect and isolate

Figure E.4 (1/2) Simplified Fault Tree -
NSCCCS SWP-1A, RWP-2A
Operating



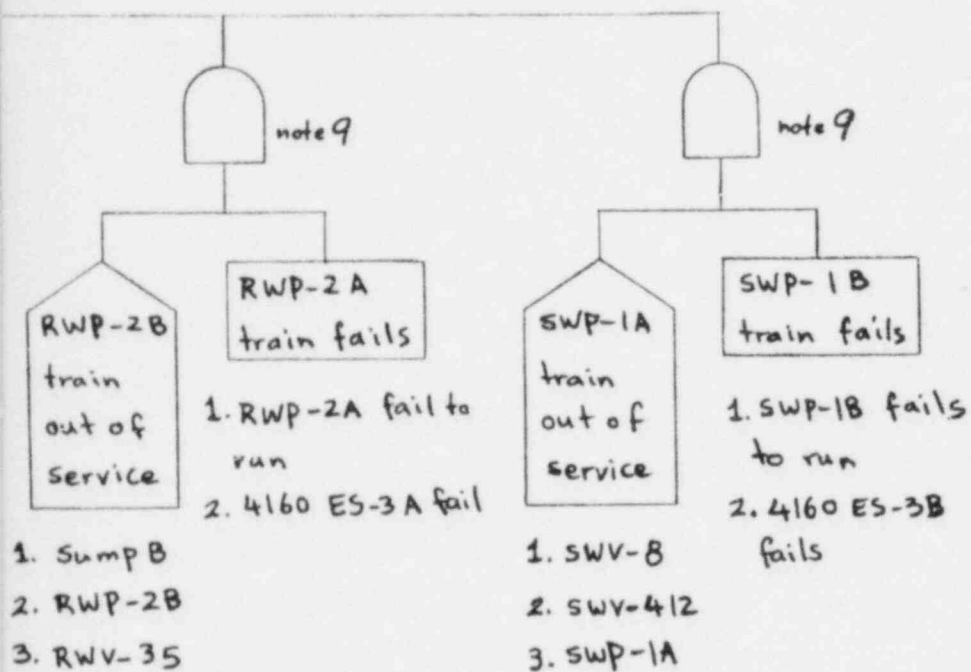


Figure E.4 (2/2) Simplified Fault Tree -
NSCCS: SWP-1A, RWP-2A
Operating

NSCCCS FAILURE

SINGLES

MAINTENANCE

DOUBLES

M5

1. Pipe rupture - NSCCCS
2. Pipe rupture - NS seawater
3. Non-isolable valve rupture - fans
4. Non-isolable valve rupture - NSCCCS
5. Non-isolable valve rupture - seawater
6. Non-isolable expansion joint rupture - seawater
7. Expansion tank SWT-1 rupture

1. RWP-2A fail to run
2. 4160 ES-3A fail

1. RWP-2B fail to start (note 10)
2. RWP-2B fail to run
3. 4160 ES-3B fail
4. ESAS - train B fails (note 4)
5. RWV-35 fails to open (note 2)
6. RWV-21 closed
7. SWV-149 closed } note 1
8. SWV-168 closed

11. SWV-149 closed
12. SWV-168 closed
13. SWV-168 closed
14. SWV-168 closed

1. SWP-1A fail to start
2. SWP-1A fail to run
3. 4160 ES-3A fail

1. SWP-1B fail to start
2. SWP-1B fail to run
3. 4160 ES-3B fail

1. SWV-149 closed
2. SWV-168 closed
3. SWV-168 closed
4. SWV-168 closed
5. SWV-168 closed
6. SWV-168 closed

- (note 4) 4. ESAS train A fail
- (note 3) 5. SWV-8 fail to open
- (note 3) 6. SWV-412 fail to open

4. ESAS train B fail (note 4)
5. SWV-9 fail to open (note 3)
6. SWV-413 fail to open (note 3)

- note 1 {
7. SWV-5 closed
 8. SWV-410 closed
 9. SWV-2 closed
 10. SWV-401 closed

7. SWV-6 closed
 8. SWV-411 closed
 9. SWV-3 closed
 10. SWV-409 closed
- } note 1

1. Mis CRDM motor
1. mis piping contain

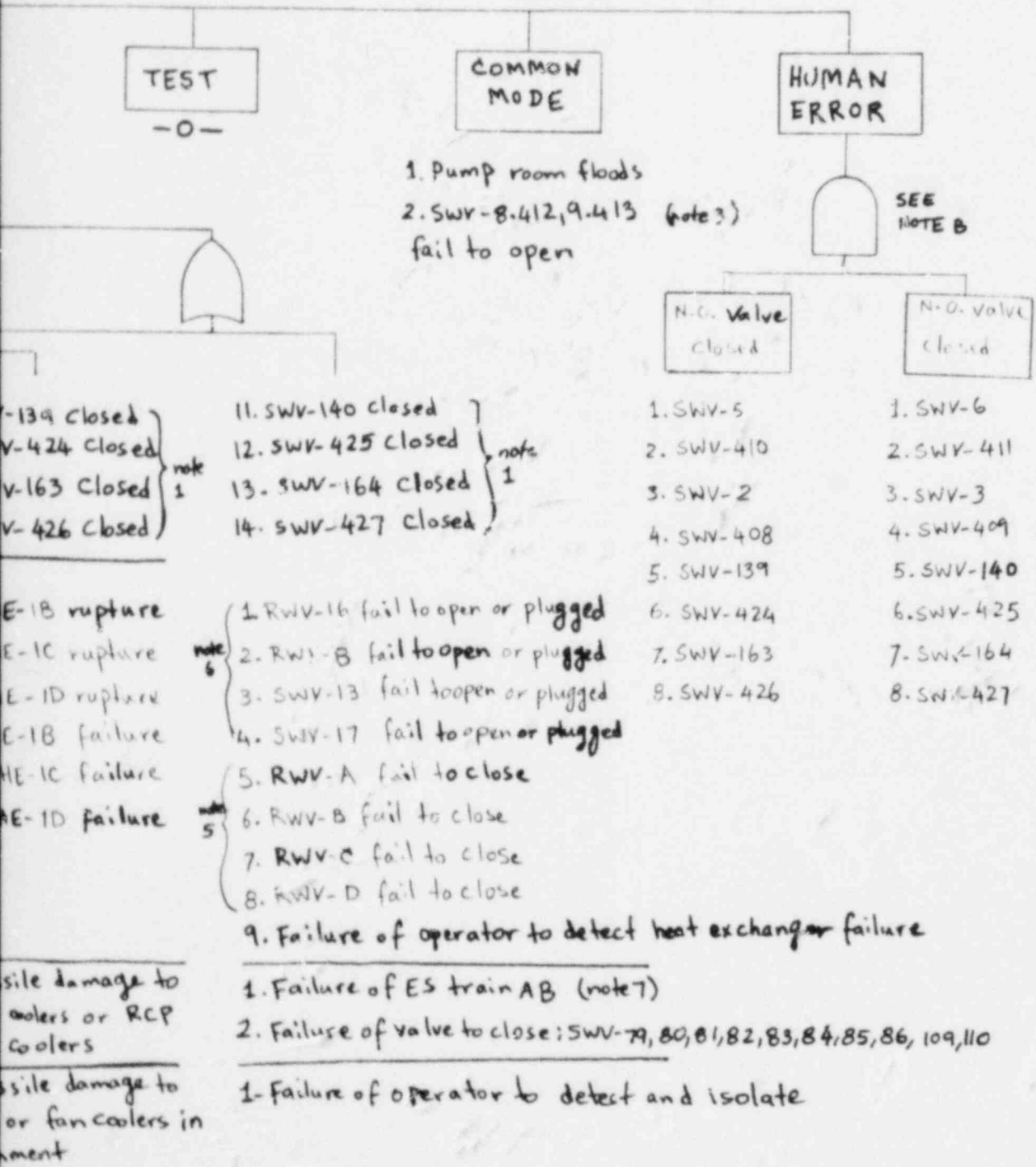
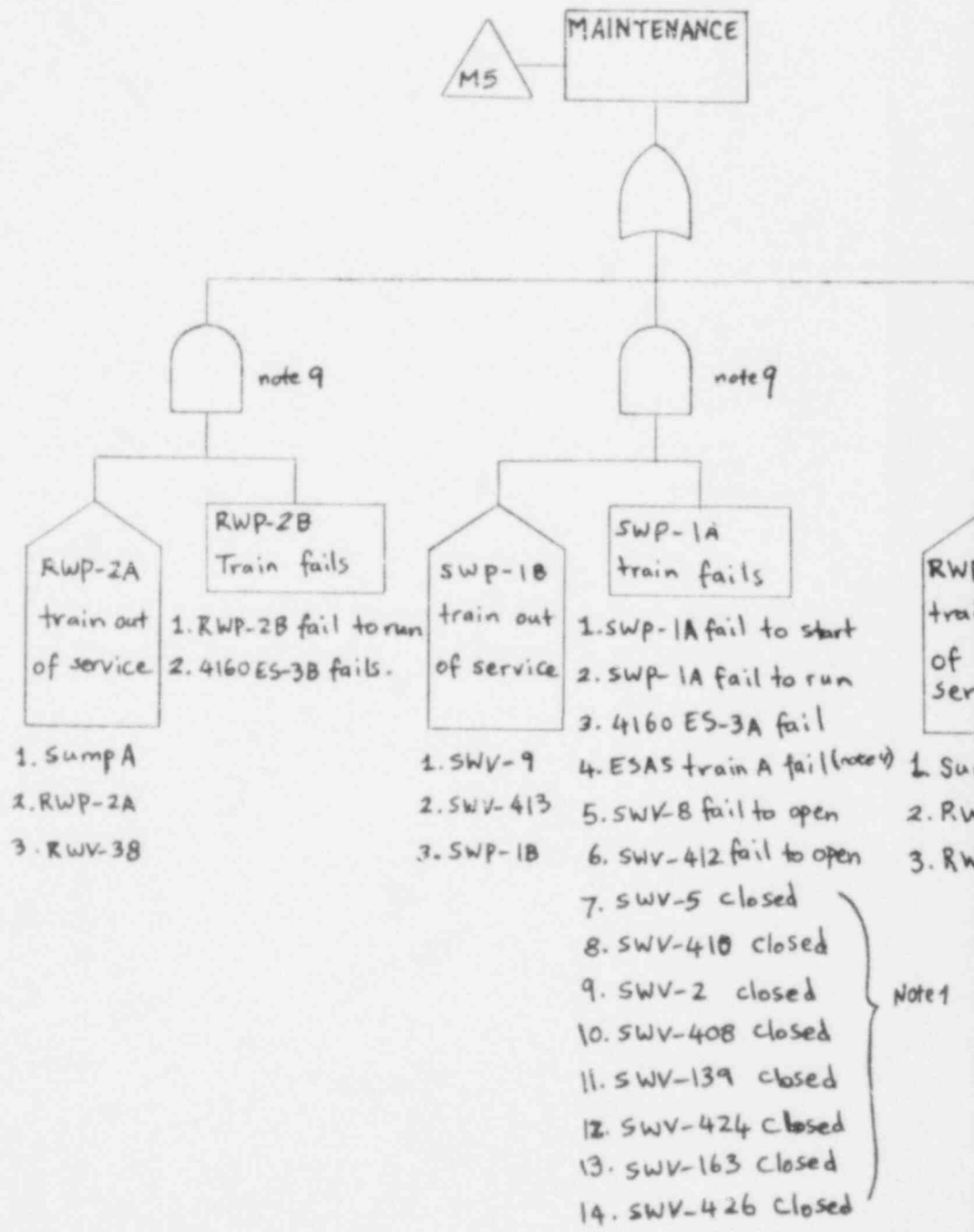


Figure E.5 (1/2) Simplified Fault Tree - NSCCCS; SWP-1C, RWP-2A Operating



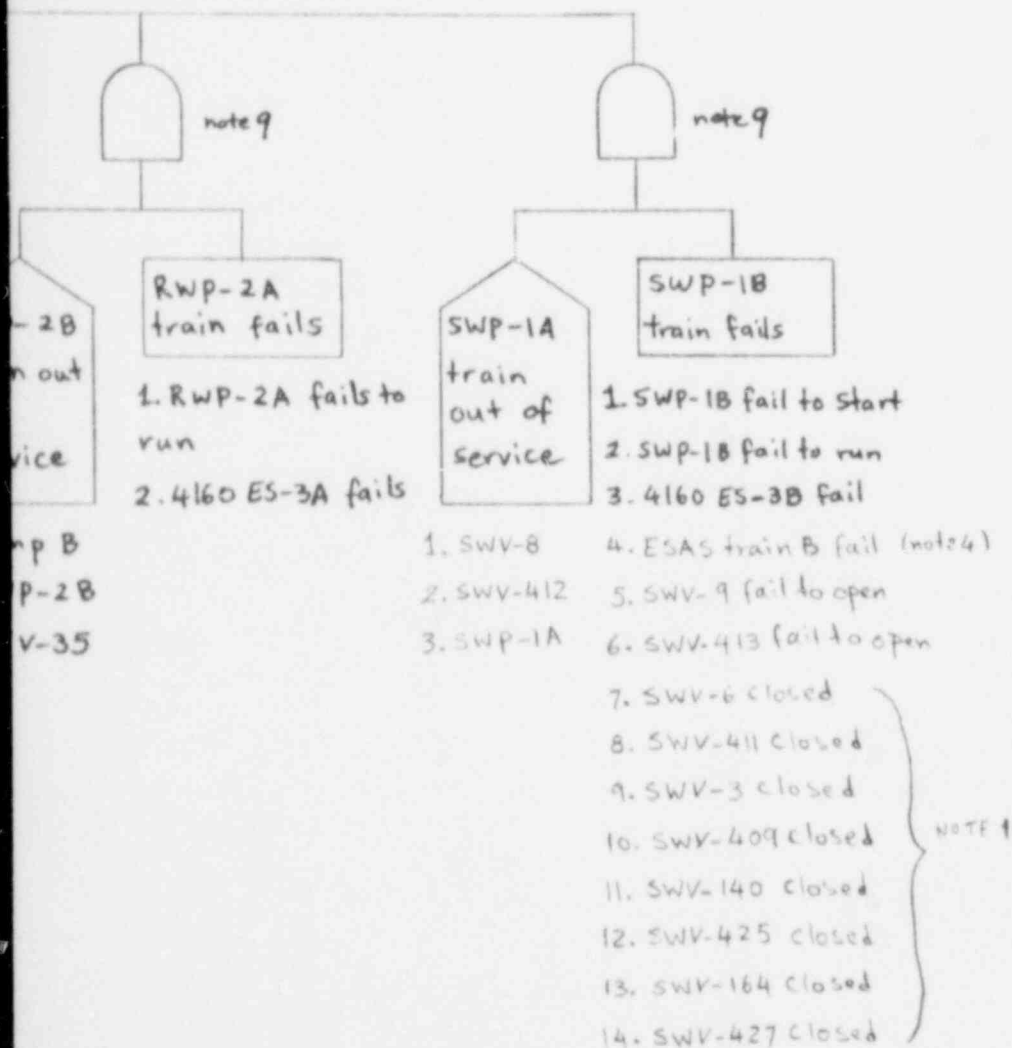


Figure E.5 (2/2) Simplified Fault Tree - NSCCCS; SWP-1C, RWP-2A Operating

NSCCCS
FAILURE



SINGLES

MAINTENANCE

DOUBLES

TEST



- 1. PIPE RUPTURE-NSCCCS
- 2. PIPE RUPTURE-NS-SEAWATER
- 3. NON-ISOLABLE VALVE RUPTURE-FANS
- 4. NON-ISOLABLE VALVE RUPTURE-NSCCCS
- 5. NON-ISOLABLE VALVE RUPTURE-SEAWATER
- 6. NON-ISOLABLE EXPANSION JOINT RUPTURE-SEAWATER
- 7. EXPANSION TANK SWT-1, RUPTURE

- 1. RWP-2A FAIL TO START (note 10)
- 2. RWP-2A FAIL TO RUN
- 3. 4160 ES-3A FAIL
- 4. ESFAS-TRAIN A FAIL (note 4)
- 5. RWV-38-FAIL TO OPEN (note 2)
- 6. RWV-24-CLOSED
- 7. SWV-142-CLOSED } (note 1)
- 8. SWV-160-CLOSED (note 6)

- (note 12) 1. RWP-2B FAIL TO START
- 2. RWP-2B FAIL TO RUN
- 3. 4160 ES-3B FAIL
- (note 4) 4. ESFAS-TRAIN B FAIL
- (note 2) 5. RWV-35-FAIL TO OPEN
- (note 1) { 6. RWV-21-CLOSED
- 7. SWV-149-CLOSED
- 8. SWV-168-CLOSED

- 1. SWP-1A FAIL TO RUN
- 2. 4160 ES-3A FAIL

- 1. SWP-1B FAIL TO RUN
- 2. 4160 ES-3B FAIL

- 1. SWHE-1B RUPTURE
- 2. SWHE-1C RUPTURE
- 3. SWHE-1D RUPTURE
- 4. SWHE-1B FAILURE
- 5. SWHE-1C FAILURE
- 6. SWHE-1D FAILURE

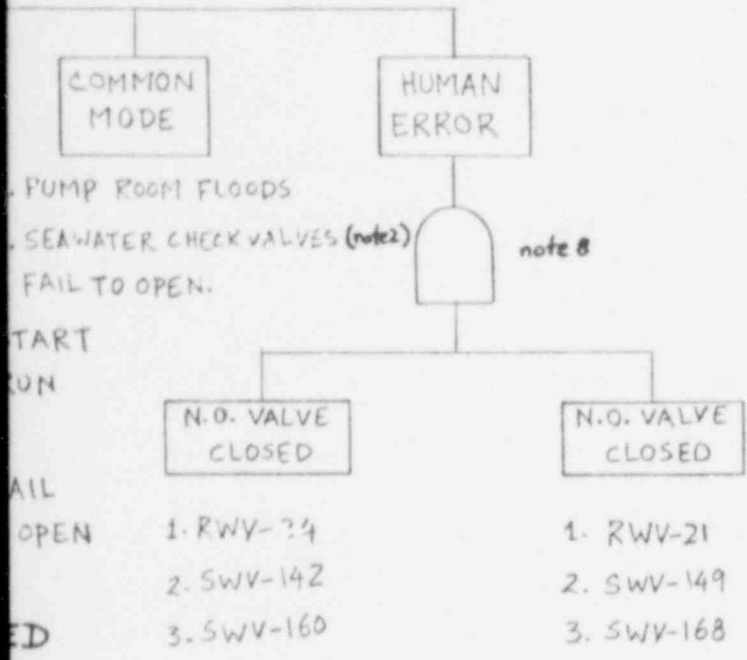
- 1. RWV-16 FAIL TO OPEN
- 2. RWV-8 FAIL TO OPEN
- 3. SWV-13 FAIL TO OPEN
- 4. SWV-17 FAIL TO OPEN
- 5. RWV-A FAIL TO CLOSE
- 6. RWV-B FAIL TO CLOSE
- 7. RWV-C FAIL TO CLOSE
- 8. RWV-D FAIL TO CLOSE
- 9. OPERATOR FAILURE HEAT EXCHANGE

- 1. MISSILE DAMAGE TO CRDM COOLERS OR RCP MOTOR COOLERS

- 1. FAILURE ES TRAIN
- 2. FAILURE OF VALVE SWV-79, 80, 81, 82, 83

- 1. MISSILE DAMAGE TO PIPING OR FAN COOLERS IN CONTAINMENT

- 1. FAILURE OF OPERATOR DETECT AND ISOLATE



OPEN OR PLUGGED }
 OPEN OR PLUGGED } note 6
 OPEN OR PLUGGED }
 OPEN OR PLUGGED }

LOSE }
 LOSE } note 5
 LOSE }
 LOSE }

RE TO DETECT
 R FAILURE

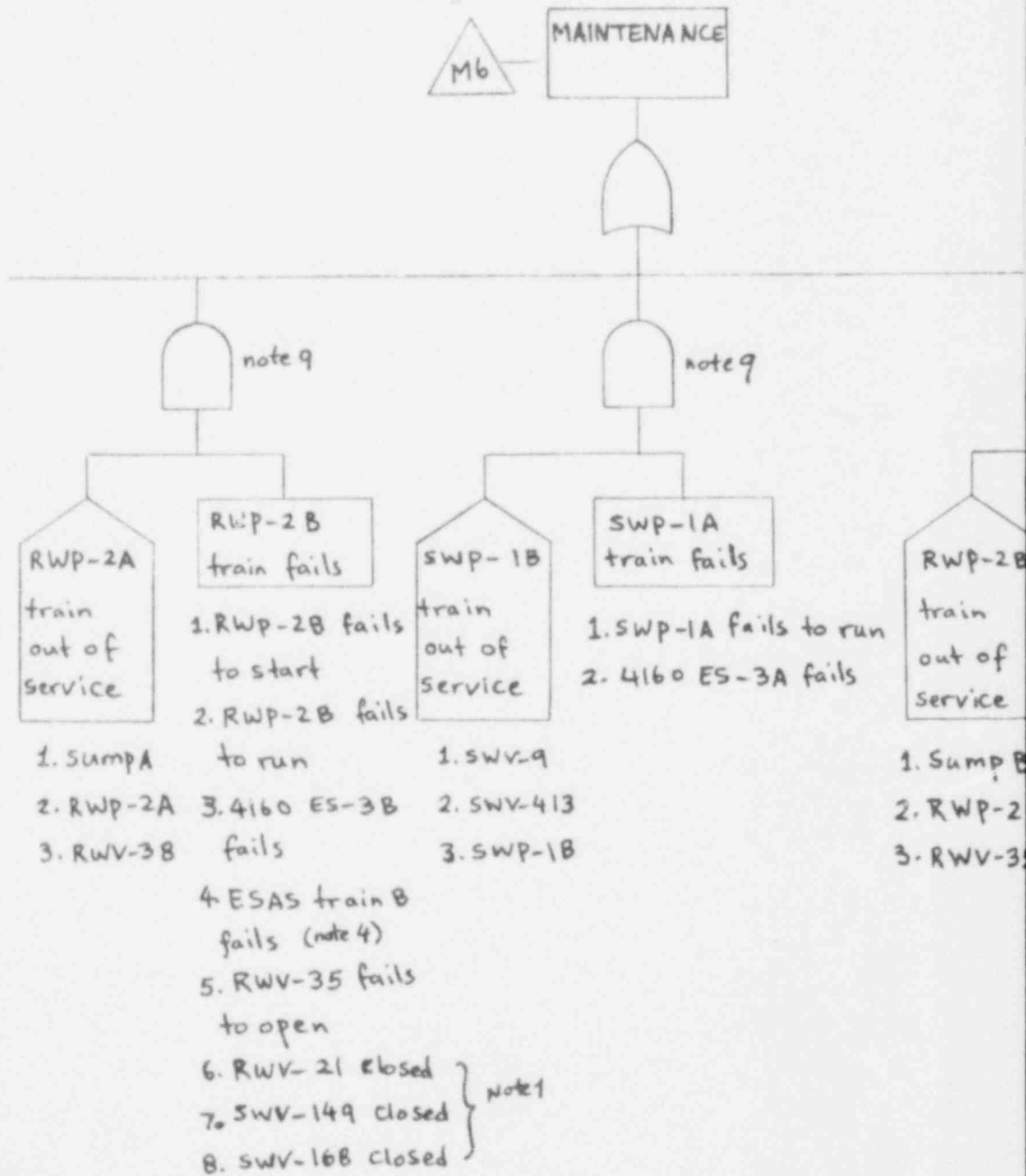
AB (note 7)

TO CLOSE

83, 84, 85, 86, 109, 110

RATOR TO
 ATE

Figure E.6 (1/2) Simplified Fault Tree - NSCCCS; SWP-1A, RWP-1, Operating



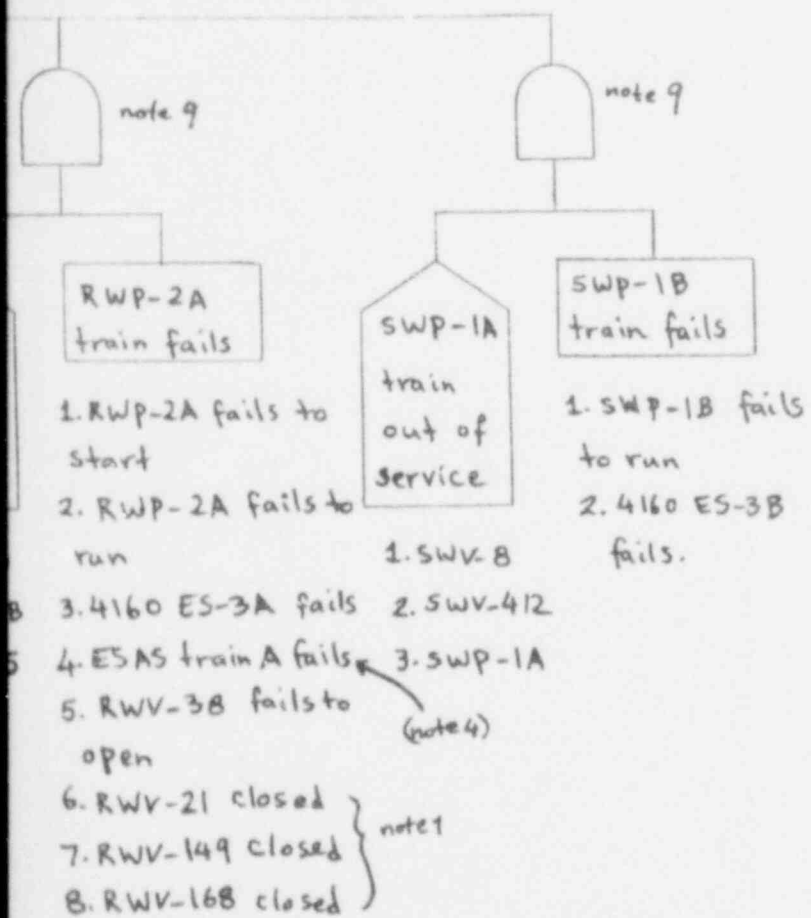


Figure E.6 (2/2) Simplified Fault Tree - NSCCCS; SWP-1A, RWP-1, Operating

Figures E.3 through E.6 Simplified Fault Trees

NOTES

- 1 These valves are normally open. These also appear in the Human Error contribution.
- 2 Both of these valves (RWV-38 and 35) are normally closed check valves in a seawater environment. Marine growth can be expected to occur on the valve during inoperative periods. This will alter the reliability over what can be expected in a freshwater environment. Each pump train is tested once a month on a staggered basis.
- 3 Four identical freshwater check valves, normally closed. Both valves in either pump train must open for success.
- 4 The capability is present to start the pumps manually. Low flow is alarmed in the control room. Pump speed is indicated in the control room.
- 5 The failed heat exchanger must be isolated. Inlet and outlet isolation valves must be closed. These are manual valves. Depending on which heat exchanger failed, the valve combinations are:

<u>1B</u>	<u>1C</u>	<u>1D</u>
SWV-18 RWV-6	SWV-19 RWV-15	SWV-20 RWV-16
SWV-14 RWV-14	SWV-15 RWV-7	SWV-16 RWV-8

Critical isolation time unknown.

- 6 Manual valves - locally operated.
- 7 Manual isolation is possible if detected. Critical isolation time unknown.
- 8 There are no single human errors. They all represent identical valves on redundant pumps.
- 9 Each of these conditions is allowed to exist for 72 hours. Components whose failure causes outage of a pump train are listed below the box.
- 10 Both of these pumps are inactive and located in non-flowing seawater. Each pump is tested once a month. Corrosion and marine growth on the pump internals may create high common mode coupling.

E.3 SYSTEM QUANTIFICATION

E.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The major contributor to the unavailability of the NSCCCS during the injection phase for cases where offsite power is available, is the failure of the NSSWS to remove heat from the NSCCCS. This is due to coupled hardware faults of the two seawater pumps (RWP-2A and -2B) or of the two check valves in the pump discharge (RWV-35 and -38). However, if offsite power is not available the dominant contributor to the system's unavailability is failure of both diesels to start and unavailability of power from fossil units CR-1 and -2. (The unavailability of both fossil units was assessed as 0.56).

The contribution of simultaneous hardware faults in both NSCCCS pump trains is about a factor of two smaller. These hardware faults include manual valves inadvertently left closed. Other contributors, about an order of magnitude smaller, are pump maintenance outages in one train and hardware failures in the other pump train.

The unavailability of the NSCCCS during the recirculation phase is dominated by faults that occurred during the injection phase in one train of either the NSCCCS or NSSWS and are not recovered for recirculation (they may not be recoverable faults) and faults that occur during the recirculation phase in the other train of NSCCCS or NSSWS. However, the NSCCCS unavailability during recirculation is about two orders of magnitude smaller than during injection.

E.3.2 SYSTEM FAULT TREE QUANTIFICATION — INJECTION PHASE

This section presents the quantification of the NSCCCS unavailability for required emergency operation of the NSCCCS during the injection phase of a postulated accident. The quantitative results are presented in table form with attached notes outlining the assumptions. To perform the fault tree quantification, the simplified fault tree representing the normally operating configuration (SWP-1C and RWP-1 in service, Figure E.3) was transformed into a modularized fault tree. Evaluating the system's unavailability for the normally operating configuration is conservative, since at least one emergency pump is required to start in each system (NSCCCS, NSSWS). For all other system operating configurations, at least one emergency pump is already running. Therefore, the relative high probability of failure to start of the emergency pump(s) does not contribute to the system's unavailability.

Table E.2 shows the NSCCCS success requirements, Table E.3 contains the top event definition for the modularized fault tree, and Figure E.7 shows the modularized fault tree for the NSCCCS. The unavailability of each gate is shown on the tree. Table E.4 shows the Boolean equation that represents the fault trees. Table E.5 shows the quantification of each gate by component and failure mode. The attached notes explain the assumptions used in the quantification. Table E.6 presents a summary of the point estimates for each gate and the error factors that were used in the sensitivity analysis.

Table E.2 NSCCCS Injection — System Success Requirements

<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B1, B2, B3, B4 Transient initiators	One pump flow for component cooling during injection.	1,2,3

-
- NOTES: 1. The NSCCCS is required to supply containment cooling water to the containment cooling fans and high pressure system pumps MUP-1B and MUP-1A during injection and recirculation.
2. The NSCCCS is a single loop system but with dual pumps. The ultimate heat sink is the NSSWS, which is a dual loop system.
3. The NSSWS function of providing the ultimate heat sink for the NSCCCS is included in the analysis of the NSCCCS.

Table E.3 NSCCCS Injection — Top Event Definitions

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
N	Failure of the NSCCCS to deliver one pump flow with ultimate heat removal for component cooling during injection	1
NC	Failure of the NSCCCS to deliver one pump flow during injection.	2
NR	Failure of the NSSWS to provide ultimate heat removal during injection.	3

-
- NOTES: 1. The event N includes failures in both NSCCCS and in the NSSWS.
 2. The event NC is defined for convenience of analysis.
 3. The event NR is defined for convenience of analysis.

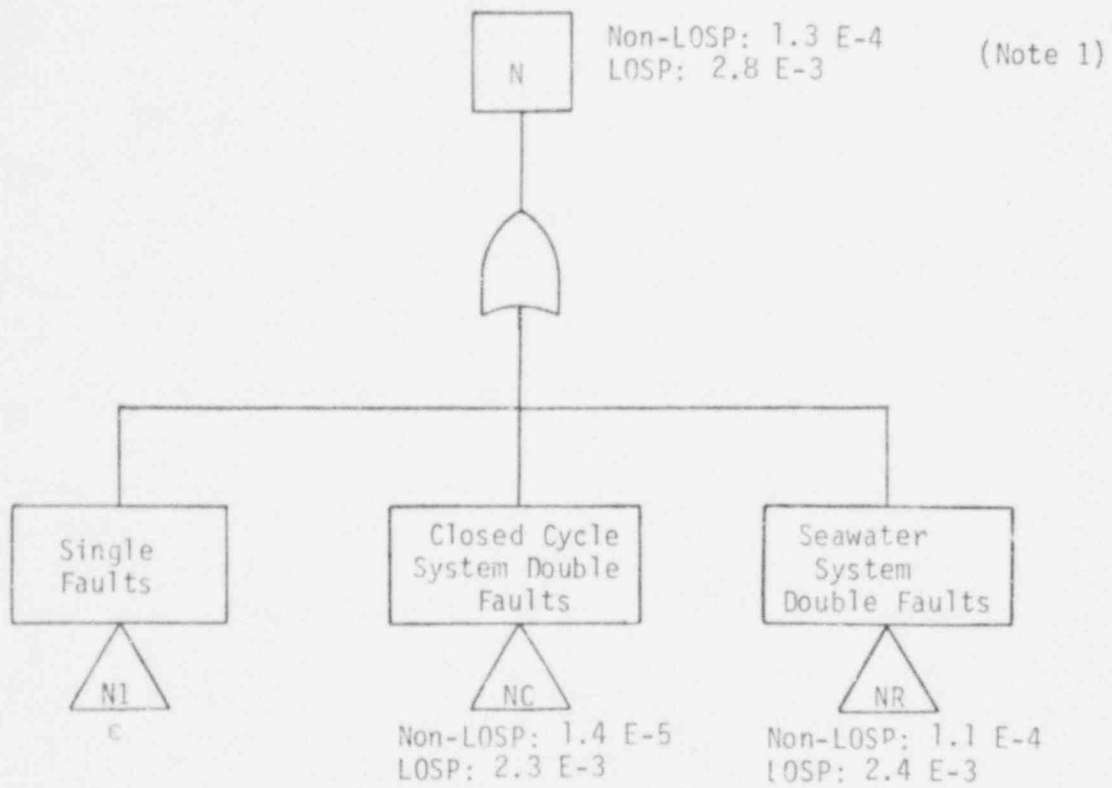


Figure E.7 (1/3) Modularized Fault Tree For Event "N"

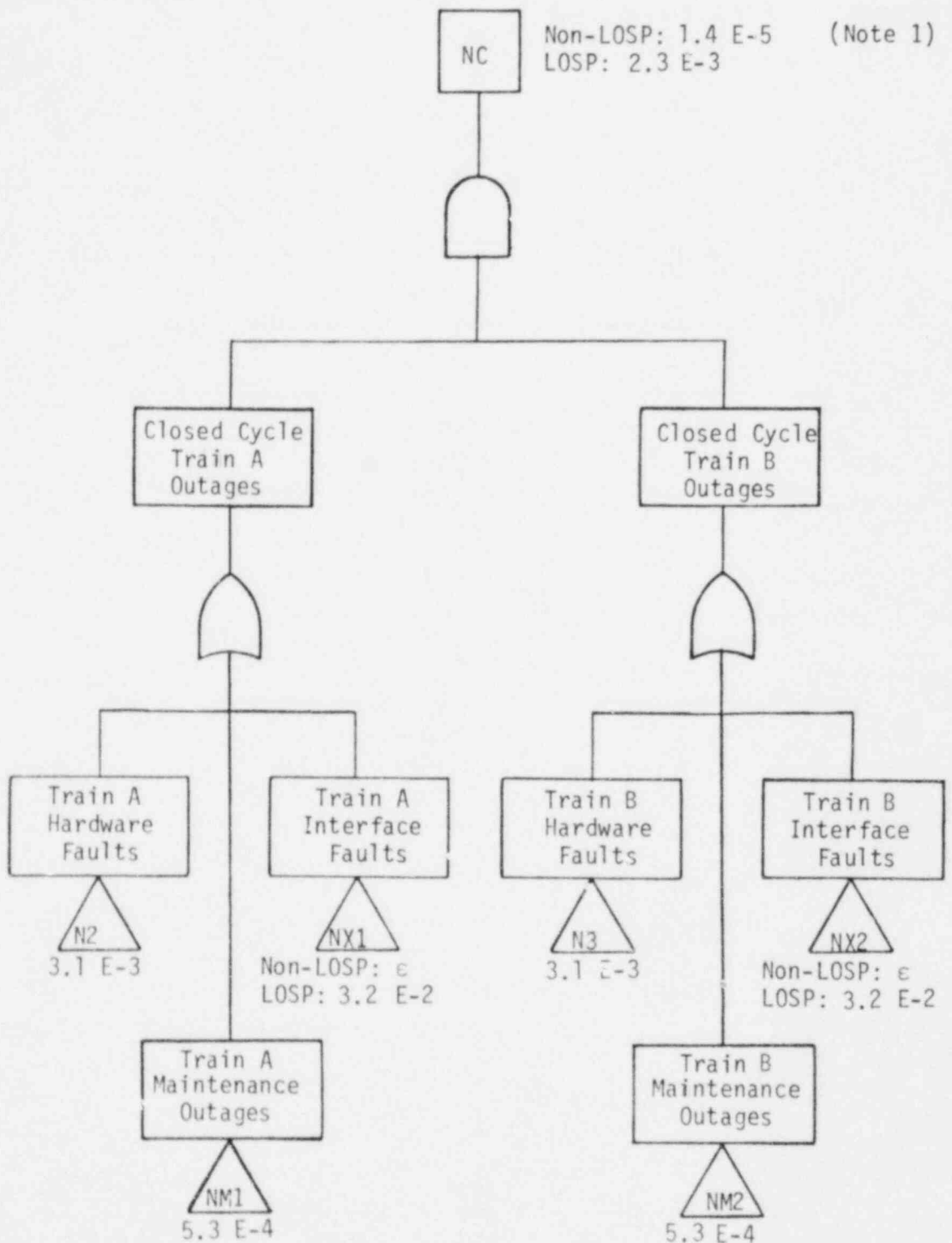


Figure E.7 (2/3) Modularized Fault Tree For Event "NC"

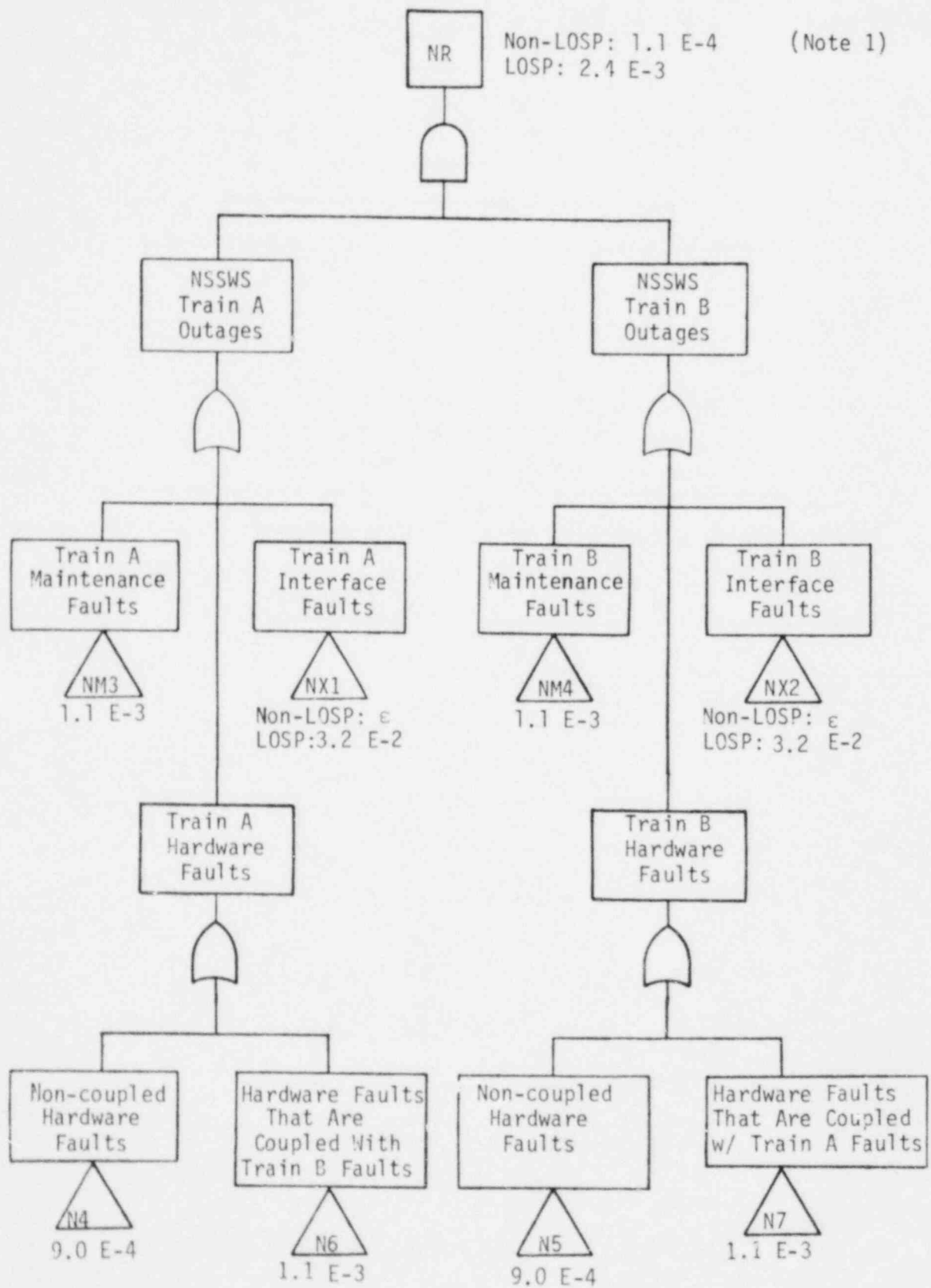


Figure E-7 (3/3) Modularized Fault Tree For Event "NR"

Figure E.7 NSCCCS - Injection

FAULT TREE

NOTES

- 1 These probabilities are based on Boolean reduced equations.

Table E.4 NSCCCS - Injection

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

<u>TOP EVENT</u>	<u>NOTES</u>
$N = N1 + NC + NR$	1
 INTERMEDIATE EVENTS	
$NC = (N2 + NM1 + NX1) \cdot (N3 + NM2 + NX2)$	1
$NR = (N4 + N6 + NM3 + NX1) \cdot (N5 + N7 + NM4 + NX2)$	1
$NX1 = ACA + DCA$ $NX2 = ACB + DCB$	

BOOLEAN EQUATIONS REGROUPED FOR BOOLEAN REDUCTION

TOP EVENT	
$ \begin{aligned} N = & N1 + ACA \cdot (N3 + N5 + N7 + NM2 + NM4) + \\ & + ACB \cdot (N2 + N4 + N6 + NM1 + NM3) + \\ & + ACA \cdot ACB + N2 \cdot (N3 + NM2) + N6 \cdot (N5 + NM4) + \\ & + N4 \cdot (N5 + N7 + NM4) + NM3 \cdot (N5 + N7) + \\ & + N6 \cdot N7 + N3 \cdot NM1 \end{aligned} $	2

Table E.4 NSCCS Injection

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

-
- NOTES: 1. These Boolean equations are not reduced to remove cross maintenance terms that are prohibited by Technical Specifications.
2. These Boolean equations have been reduced to remove cross maintenance terms that are prohibited by Technical Specifications. The DC - dependency is included in ACA and ACB.

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N1		SINGLE FAILURES - VARIOUS PIPE AND VALVE RUPTURES			c			1
N6-N7		COUPLED HARDWARE FAULTS			1.1 E-4	2 ⁺ , 2 ⁻	B	5
	(PWP-2A) x (PWP-2B)	COUPLED SEAWATER PUMP FAILURE	(1.0 E-3) (.1)		1.0 E-4	2 ⁺ , 2 ⁻	B	5
	(BIV-35) x (BIV-38)	COUPLED SEAWATER CHECKVALVE FAILURE	(1.0 E-4) (.1)		1.0 E-5	2 ⁺ , 2 ⁻	B	5
					<u>1.1 E-4</u>			

Table E.5 (1/5) Event "N" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N2		CLOSED CYCLE TRAIN A HARDWARE FAULTS			3.1 E-3	10 ⁺ , 10 ⁻		
	PUMP SWP-1A	FAILS TO START	D		1.0 E-3	3 ⁺ , 3 ⁻		
	PUMP SWP-1A	FAILS TO RUN	3.0 E-5	10	3.0 E-4	10 ⁺ , 10 ⁻		2
	ESFAS-A	NO SIGNAL AND FAILURE TO RECOVER	(2.1 E-4)(0.1)		2.1 E-5			3, 6
	CHECK VALVE SVV-8	FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
	CHECK VALVE SWV-412	FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
	SWV-5	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
	SWV-410	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
	SWV-2	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
	SWV-408	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
	SWV-139	MANUAL VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
	SWV-424	MANUAL VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
	SWV-153	MANUAL VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
SWV-426	MANUAL VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4	
				E=3.1 E-3				
NW1		MAINTENANCE OUTAGES			5.3 E-4			
	PUMP SWP-1A	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
NX1		SYSTEM INTERFACE FAULTS						
ACA		AC TRAIN A FAILS						
		NON LOSP			E			
		LOSP			3.2 E-2			
DCA		DC TRAIN A FAILS						
		NON LOSP			E			
		LOSP			3.2 E-3			
N3		CLOSED CYCLE TRAIN B HARDWARE FAULTS			3.1 E-3	10 ⁺ , 10 ⁻		
	PUMP SWP-1B	FAILS TO START	D		1.0 E-3	3 ⁺ , 3 ⁻		
	PUMP SWP-1B	FAILS TO RUN	3.0 E-5	10	3.0 E-4	10 ⁺ , 10 ⁻		2
	ESFAS-B	NO SIGNAL AND FAILURE TO RECOVER	(2.1 E-4)(0.1)		2.1 E-5			3, 6
	CHECK VALVE SVV-9	FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
	CHECK VALVE SWV-413	FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
	SWV-6	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
	SWV-411	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
SWV-3	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4	

Table E.5 (2/5) Event "NIC" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
	SWV-409	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
	SWV-140	MANUAL VALVES INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
	SWV-425	MANUAL VALVES INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
	SWV-164	MANUAL VALVES INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
	SWV-427	MANUAL VALVES INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
					$\Sigma = 3.1 E-3$			
NM2		MAINTENANCE OUTAGES			5.3 E-4	3 ⁺ , 3 ⁻	M	
	PUMP SWP-1B	OUT FOR MAINTENANCE	02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
NX2		SYSTEM INTERFACE FAULTS						
ACB		AC TRAIN B FAILS						
		NON LOSP			ϵ			
		LOSP			5.2 E-2			
DCB		DC TRAIN B FAILS						
		NON LOSP			ϵ			
		LOSP			3.2 E-3			

Table E.5 (3/5) Event "NC" Quantification

E-42

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N4		NON-COUPLED TRAIN A HARDWARE FAULTS			9.0 E-4	10 ⁺ , 10 ⁻	H	
	PUMP RWP-2A	FAILS TO RUN	3.0 E-5	10	3.0 E-4	10 ⁺ , 10 ⁻		2
	ES/AS-A	NO SIGNAL AND FAILURE TO RECOVER	(2.1E-4)(0.1)		2.1 E-5			3, 6
	RWV-24	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
	SWV-102	MANUAL VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
	SWV-166	MANUAL VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
					<u>Σ=9.0 E-4</u>			
N6		COUPLED TRAIN A HARDWARE FAULTS			1.1 E-3	3 ⁺ , 3 ⁻	S	
	PUMP RWP-2A	FAILS TO START	D		1.0 E-3	3 ⁺ , 3 ⁻	S	
	CHECK VALVE RWV-38	FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻	S	
					<u>Σ=1.1 E-3</u>			
N13		TRAIN A MAINTENANCE OUTAGES			1.1 E-3	3 ⁺ , 3 ⁻		
	PUMP RWP-2A	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
	CHECK VALVE RWV-38	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
					<u>Σ=1.1 E-3</u>			

Table E.5 (4/5) Event "NR" Quantification

Table E.5 (5/5) Event "NR" Quantification (Continued)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N5	PUMP RWP-2B ESFAS-3 SWV-21 SWV-149 SWV-168	NON COUPLED HARDWARE FAULTS IN TRAIN B						
		FAILS TO RUN	3.0 E-5	10	9.0 E-4	10 ⁺ , 10 ⁻	H	2
		NO SIGNAL AND OPERATOR FAILS TO RECOVER	2.1 E-4(0.1)		3.0 E-4	10 ⁺ , 10 ⁻		
		BUTTERFLY VALVE INADVERTENTLY LEFT CLOSED	4.02(1.0 E-2)		2.1 E-5	10 ⁺ , 10 ⁻		3,6
		MANUAL VALVE INADVERTENTLY LEFT CLOSED	4.02(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
N7	PUMP RWP-2B CHECK VALVE SWV-35	MANUAL VALVE INADVERTENTLY LEFT CLOSED	4.02(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
		MANUAL VALVE INADVERTENTLY LEFT CLOSED	4.02(1.0 E-2)		2.0 E-4	10 ⁺ , 10 ⁻	H	4
		COUPLED TRAIN B HARDWARE FAULTS			2.0 E-4 Σ=9.0 E-4	10 ⁺ , 10 ⁻	H	4
N14	PUMP RWP-2B CHECK VALVE RWV-35	FAILS TO START	D		1.1 E-3	3 ⁺ , 3 ⁻	S	
		FAILS TO OPEN	D		1.0 E-3	3 ⁺ , 3 ⁻	S	
		TRAIN B MAINTENANCE OUTAGES			1.0 E-4	3 ⁺ , 3 ⁻	S	
		OUT FOR MAINTENANCE	.02/720	19	Σ=1.1 E-3	3 ⁺ , 3 ⁻	M	
		OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
		OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	

Table E.5 NSCCCS - Injection

QUANTIFICATION TABLES

NOTES

- 1 The NSCCCS is a normally operating system. It was assumed that pipe or valve ruptures would be detected when they occur, and repaired. Therefore, these faults were assessed to be negligibly small.
- 2 The time duration for injection can vary from 0.5 hrs. to 10 hrs., depending on the LOCA size. A fault duration time of 10 hrs. was conservatively chosen for the analysis.
- 3 The failure of ESFAS to actuate single equipment was assessed as 2.1 E-4 (Event ISS1 in ESAS quantification). Although this number is insignificant, it is correct only for the B4 LOCA. It is conservative for the other LOCA cases. Failure to recover was assumed to be 0.1 per act.
- 4 The frequency of maintenance was assumed to be 0.02 acts per month. The probability of leaving a valve in the incorrect position after maintenance was assessed as 1E-2 per maintenance act.
- 5 The failure of these components was assumed coupled since they see the same seawater environment. A coupling coefficient (β factor) of 0.1 was assumed.
- 6 Failure of ESAS to provide actuation signals to both trains is not included because the potential for recovery is high enough to make this contribution negligible.

Table E.6 NSCCCS - Injection Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
N1	ϵ
N2	3.1 E-3
NM1	5.3 E-4
N3	3.1 E-3
NM2	5.3 E-4
N4	9.0 E-4
N6	1.1 E-3
NM3	1.1 E-3
N5	9.0 E-4
N7	1.1 E-3
NM4	1.1 E-3
N6·N7	1.1 E-4
ACA	ϵ^* 3.2 E-2**
ACB	ϵ^* 3.2 E-2**
ACA·ACB	2.3 E-3

*offsite power available

**offsite power not available

This section presents the quantification of the NSCCCS unavailability for required emergency operation during the recirculation phase of a postulated accident. As for the injection phase, modularized fault trees were constructed. Credit was given for recovery of certain failures which occurred during the injection phase, e.g., events N*3 and N*4 in the quantification tables.

Table E.7 shows the NSCCCS success requirements. Table E.8 contains the top event definitions, and Figure E.8 shows the modularized fault tree. The unavailability of each gate is shown on these trees, as well as the top event unavailabilities. Table E.9 shows the Boolean equations that represent the fault tree. Table E.10 shows the quantification of each gate, by component and failure mode. The attached notes explain the assumptions used in the quantification. Table E.11 presents a summary of the point estimates for each gate and the error factors that were used in the sensitivity analysis.

Table E.7 NSCCCS Recirculation — System Success Requirements

<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B1, B2, B3, B4 transient initiators	One pump flow for component cooling during recirculation	1,2,3

-
- NOTES: 1. The NSCCCS is required to supply containment cooling water to the containment cooling fans and high pressure system pumps MUP-1B and MUP-1A during injection and recirculation
2. The NSCCCS is a single loop system but with dual pumps. The ultimate heat sink is the raw water system, which is a dual loop system.
3. The NSSWS function of providing the ultimate heat sink for the NSCCCS is included in the analysis of the NSCCCS.

Table E-8 NSCCCS Recirculation — Top Event Definitions

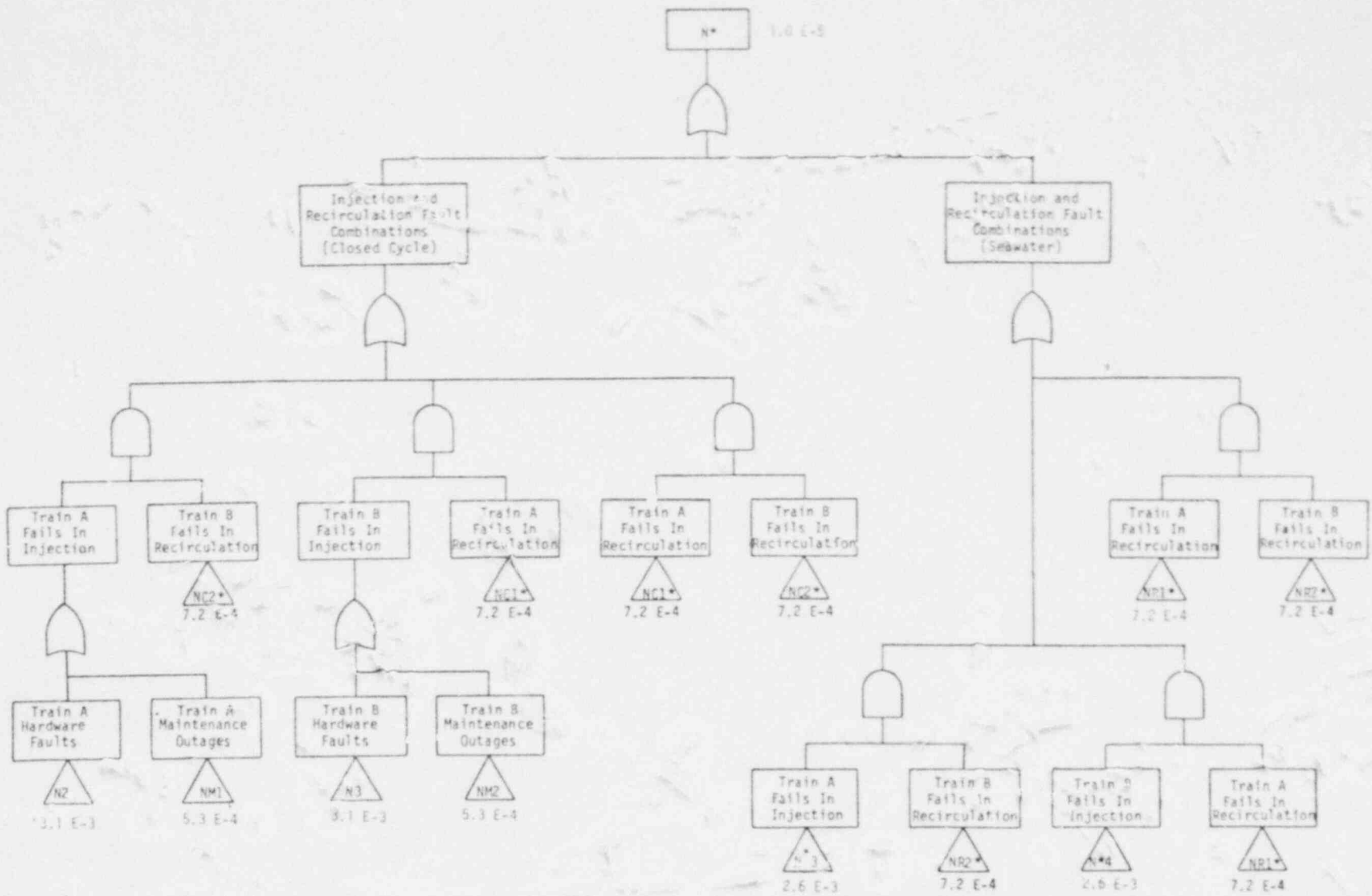
<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
N*	Failure of the NSCCCS to deliver one pump flow with ultimate heat removal for cooling during recirculation.	1
NC1*(NC2*)	Failure of the NSCCCS Train A(B) to deliver pump flow during recirculation.	2
NR1* (NR2*)	Failure of the NSSWS Train A(B) to deliver pump flow during recirculation.	3

NOTES: 1. The event N* includes failures in both the closed cycle portion of the cooling system and in the seawater portion of the system.

2. The event NC1* (NC2*) is defined for convenience of analysis.

3. The event NR1*(NR2*) is defined for convenience of analysis.

Figure E-8 (1/3) Modularized Fault Tree for Event "N"



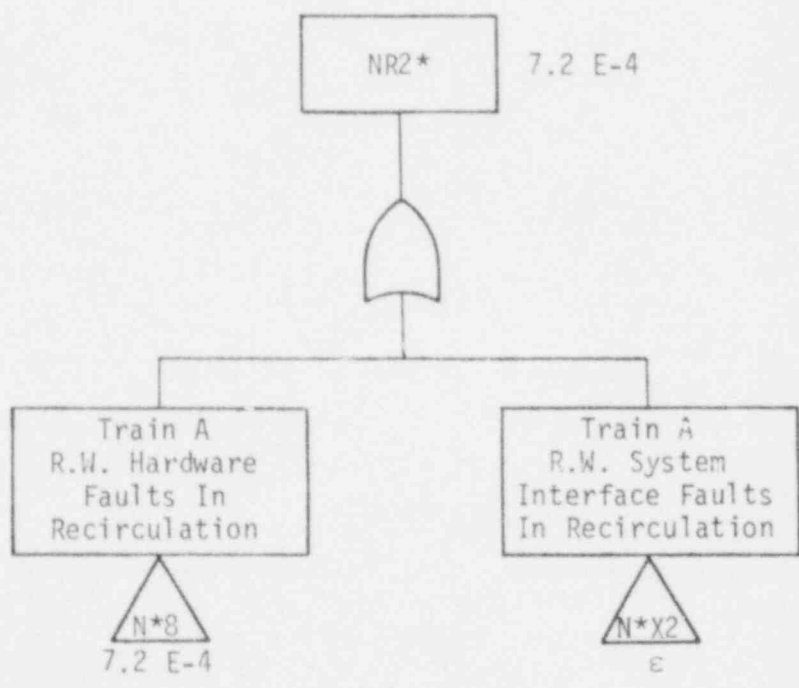
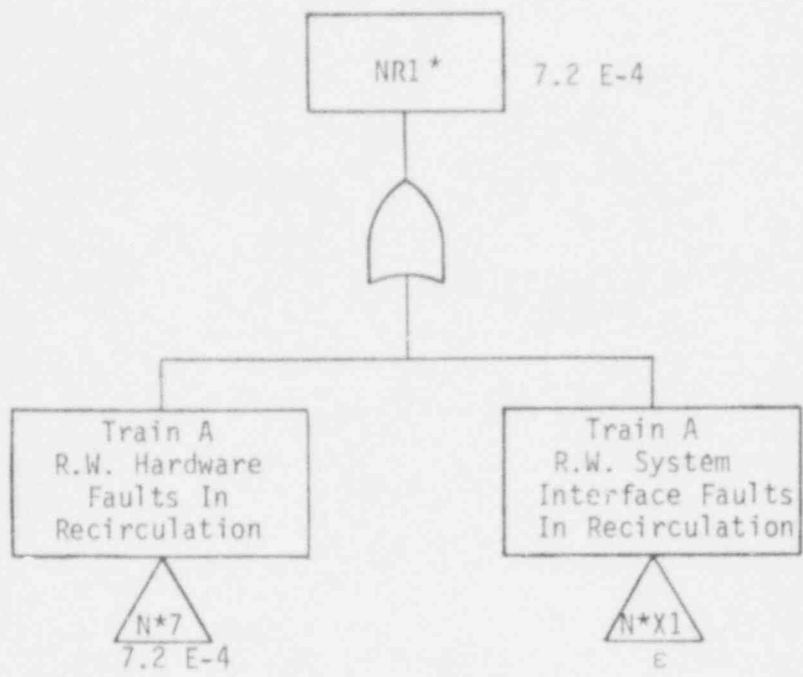


Figure E.8 (2/3) Modularized Fault Tree For Event "NR1*" and "NR2*"

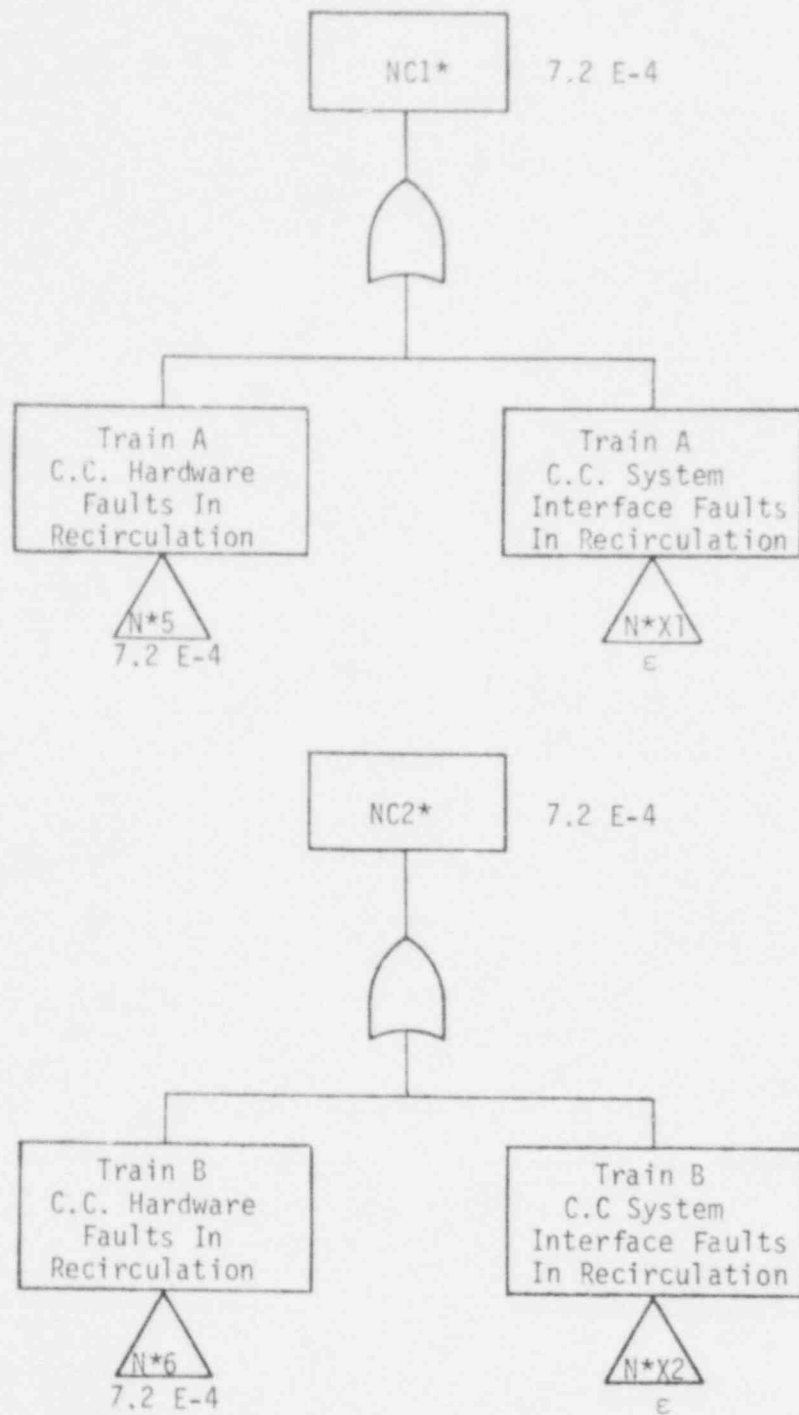


Figure E.8 (3/3) Modularized Fault Tree For Event "NC1*" and "NC2*"

Table E.9 NSCCCS - Recirculation

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENT

NOTES

$$N^* = NC1^* \cdot (N3 + NM2) + NC2^* \cdot (N2 + NM1) + NC1^* \cdot NC2^* + \\ + NR1^* \cdot N^*4 + NR2^* \cdot N^*3 + NR1^* \cdot NR2^*$$

1

$$NC1^* = N^*5 + N^*X1$$

$$NC2^* = N^*6 + N^*X2$$

$$NR1^* = N^*7 + N^*X1$$

$$NR2^* = N^*8 + N^*X2$$

INTERMEDIATE EVENTS

$$N^*X1 = ACA^*$$

$$N^*X2 = ACB^*$$

BOOLEAN EQUATIONS REGROUPED FOR BOOLEAN REDUCTION

TOP EVENT

$$N^* = N^*5 \cdot N^*6 + N^*8 + N^*4 \cdot N^*7 + N^*7 \cdot N^*8 + \\ + ACA^* \cdot ACB^* + ACA^* \cdot (N3 + NM2 + N^*6 + N^*4 + N^*8) + \\ + ACB^* \cdot (N2 + NM1 + N^*5 + N^*3 + N^*7) + \\ + N^*5 \cdot (N3 + NM2) + N^*6 \cdot (N2 + NM1)$$

2

NOTES: 1. This equation has not been reduced.

2. This equation is Boolean reduced.

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N*3		RAW WATER TRAIN A FAILS IN INJECTION AND IS NOT RECOVERED			2.6 E-3	3+, 3-	S	
	PUMP R1P-2A	FAILS TO RUN	3.0 E-5	10	3.0 E-4	10+, 10-		
	ESFAS-A	NO SIGNAL AND FAILURE TO RECOVER	(2.1 E-4)(0.1)		2.1 E-5			
	R1V-24	VALVE CLOSED AND FAILURE TO RECOVER	(2.0 E-4)(.1)		2.0 E-5	10+, 10-	H	1
	SWV-142	VALVE CLOSED AND FAILURE TO RECOVER	(2.0 E-4)(.1)		2.0 E-5	10+, 10-	H	1
	SWV-166	VALVE CLOSED AND FAILURE TO RECOVER	(2.0 E-4)(.1)		2.0 E-5	10+, 10-	H	1
N6		SEE NSCCCS INJECTION QUANTIFICATION TABLES			1.1 E-3	3+, 3-	S	
NM3		SEE NSCCCS INJECTION QUANTIFICATION TABLES			1.1 E-3	3+, 3-	H	
					<u>Σ=2.6 E-3</u>	3+, 3-		

E-53

Table E.10 (1/5) Event "N*3" Quantification

Table E.10 (2/5) Event "N*4" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES	
N*4	PUMP RMP-2B ESFAS-B RMV-21 SMV-149 SMV-168	RAW WATER TRAIN B FAILS IN INJECTION AND IS NOT RECOVERED			2.6 E-3	3 ⁺ , 3 ⁻	S		
		FAILS TO RUN	3.0 E-5	10	3.0 E-4	10 ⁺ , 10 ⁻			
		NO SIGNAL AND OPERATOR FAILS TO RECOVER	(2.1 E-4)(0.1)		2.1 E-5				
		BUTTERFLY VALVE INADVERTENTLY LEFT CLOSED AND FAILURE TO RECOVER	(2.0 E-4)(0.1)		2.0 E-5		10 ⁺ , 10 ⁻	H	1
		MANUAL VALVE INADVERTENTLY LEFT CLOSED AND FAILURE TO RECOVER	(2.0 E-4)(0.1)		2.0 E-5		10 ⁺ , 10 ⁻	H	1
		MANUAL VALVE INADVERTENTLY LEFT CLOSED AND FAILURE TO RECOVER	(2.0 E-4)(0.1)		2.0 E-5		10 ⁺ , 10 ⁻	H	1
N7		SEE NSCCCS INJECTION QUANTIFICATION TABLES			1.1 E-3	3 ⁺ , 3 ⁻	S		
N*4		SEE NSCCCS INJECTION QUANTIFICATION TABLES			1.1 E-3 E=2.6 E-3	3 ⁺ , 3 ⁻ 3 ⁺ , 3 ⁻	M		

Table E.10 (3/5) Events "N2, N3, NM1, NM2" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N2		CLOSED CYCLE NSCCCS TRAIN A INJECTION FAULTS - SEE NSCCCS INJECTION QUANTIFICATION TABLES			3.2 E-3	10 ⁺ , 10 ⁻	H	
NM1		SEE NSCCCS INJECTION QUANTIFICATION TABLES			5.3 E-4	3 ⁺ , 3 ⁻	R	
N3		CLOSED CYCLE NSCCCS TRAIN B INJECTION FAULTS - SEE NSCCCS INJECTION QUANTIFICATION TABLES			3.2 E-3	10 ⁺ , 10 ⁻	H	
NM2		SEE NSCCCS INJECTION QUANTIFICATION TABLES			5.3 E-4	3 ⁺ , 3 ⁻	R	

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N*5	PUMP SWP-1A	CLOSED CYCLE TRAIN A HARDWARE FAULTS DURING RECIRCULATION			7.2 E-4			
		FAILS TO RUN	3.0 E-5	24	7.2 E-4	10 ⁺ , 10 ⁻		
N*X1		CLOSED CYCLE TRAIN A SYSTEM INTERFACE FAULTS DURING RECIRCULATION			e			
ACA*		AC TRAIN A FAILS DURING RECIRCULATION			e			
N*6	PUMP SWP-1B	CLOSED CYCLE TRAIN B HARDWARE FAULTS DURING RECIRCULATION			7.2 E-4			
		FAILS TO RUN	3.0 E-5	24	7.2 E-4	10 ⁺ , 10 ⁻		
N*X2		CLOSED CYCLE TRAIN B SYSTEM INTERFACE FAULTS DURING RECIRCULATION			e			
ACB*		AC TRAIN B FAILS DURING RECIRCULATION			e			

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N*7		RAW WATER TRAIN A HARDWARE FAULTS DURING RECIRCULATION			7.2 E-4			
	PUMP RWP-2A	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10 ⁴ , 10 ⁵		
N*X1		SEE NC1*, NC2*, QUANTIFICATION TABLES			c			
N*8		RAW WATER TRAIN B HARDWARE FAULTS DURING RECIRCULATION			7.2 E-4			
	PUMP RWP-2B	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10 ⁴ , 10 ⁵		
N*X2		SEE NC1*, NC2* QUANTIFICATION TABLES			c			

Table E.10 (5/5) Events "NR1", "NP2*" Quantification

Table E.10 NSCCCS - Recirculation

QUANTIFICATION TABLES

NOTES

- 1 Valves inadvertently closed and fail to recover were assessed as $2.0 \text{ E-}4$ probability of the valve being in the closed position times 0.1 probability of no recovery. See NSCCCS - Injection Quantification Tables.

Table E.11 NSCCCS - Recirculation Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
N*5	7.2 E-4
N*X1	E
ACA*	E
N*6	7.2 E-4
N*X2	E
ACB*	E
N*7	7.2 E-4
N*8	7.2 E-4
N*3	2.6 E-3
N*4	2.6 E-3

APPENDIX F

DECAY HEAT CLOSED CYCLE COOLING SYSTEM (DHCCCS)

F.1 SYSTEM DESCRIPTION AND OPERATION

The purpose of the Decay Heat Closed Cycle Cooling System (DHCCCS) is (1) to remove decay heat from the Low Pressure Heat Removal System and (2) to provide component cooling for bearings and motors in the Low Pressure Heat Removal System, the Containment Spray System, and one train of the High Pressure Injection System. In addition, the DHCCCS provides component cooling for components that are part of the raw seawater (or ultimate heat sink) portion (DHSS) of the DHCCCS. The DHCCCS is required to operate for decay heat removal and component cooling for all accidents or transients that require the Low Pressure Heat Removal System, the Containment Spray System, or the High Pressure Injection System (makeup pump MUP-1C only). Operation may be required during both the injection and recirculation phases of the accident sequence. Operation is also required during normal operation to remove reactor decay heat during shutdown.

F.1.1 SYSTEM DESCRIPTION

The DHCCCS consists of two loops, a closed cycle loop that removes decay heat and component heat, and a once-through system (the raw water, or seawater system) that removes heat from the closed cycle loop and discharges it to the seawater discharge canal. Both the once-through seawater system, and the closed cycle system are doubly redundant, consisting of Trains A and B. Train A of the seawater system removes heat from Train A of the closed cycle system, and Train B of the seawater system removes heat from Train B of the closed cycle system. The trains are independent of each other and each is rated at 100% capacity for decay heat removal and cooling of components they serve. Figures F.1 and F.2 show simplified one-line diagrams of the closed cycle and seawater portions of the DHCCCS, respectively.

The design flow rate in each of the closed cycle trains is 3200 gpm, 3000 of which goes through the respective DHRS heat exchanger. The remaining 200 gpm is used for pump cooling. Maximum heat rejection capability

per loop, under emergency conditions, is 120×10^6 BTU/hr. Under these conditions, the hot leg operates at 140°F and the cold leg at 105°F. The pump develops an 80 foot head. Each loop has its own surge tank which is pressurized to 5-10 psig. This is not necessary for NPSH requirements. Both the source and sink heat exchangers are shell and tube, with the closed cycle water on the shell side of both.

There are no MOV's or automatic valves in the closed cycle portion of the system. Each loop has manual blocking valves for the major components. These are not locked and are locally indicated. The only locked valves in the system are those in the cooling lines to the motors. The pumps in the closed cycle portion of the system are forced air cooled. A fan cooler assembly (AHF-15A or 15B) in each train provides motor cooling. AHF-15A and 15B are cooled by their respective DHCCCS loops. Both the pumps and AHF-15 are powered by the 480V ESMCC's. The pump bearing is self cooled.

The major lines in the closed cycle portion of the system are 12 inch pipes. These supply flow to the heat exchangers. The majority of the flow is directed to the low pressure heat removal heat exchanger. The motor cooling loads are through smaller 2-3 inch lines directed from the main pipe. The flow to the low pressure system heat exchanger is controlled by a two-valve bypass. The flow can be totally shunted from the heat exchanger. The two valves are controlled together by a single circuit. These are regulated to control the cooldown rate after a normal shutdown. During emergency operation, the total flow is directed through the heat exchanger. The position of these valves before ESAS is such that total flow is directed through the heat exchanger.

The seawater portion of the system (DHSS) transports heat from the closed cycle portion to the seawater discharge canal. Each seawater train services its respective closed cycle train. The seawater system is a once-through, open cooling system. Seawater flows by gravity from the intake canal to the seawater sump through 48 inch pipes. The two pumps from the respective seawater trains are installed in separate compartments in the seawater sump to allow the isolation of either compartment for service without disabling both trains.

Each seawater pump takes suction from the seawater sump, pumps water through its respective heat exchanger and into the discharge canal. There are no other cooling loads on the system. The pump motors are cooled by the respective freshwater (closed cycle) cooling train. They are powered by the 4160V ES buses. The bearing is cooled by domestic water supply. If that fails, the demineralized water supply will back-up the domestic water. If both those fail, the seawater will back into the bearing. This provides adequate cooling although it is not desirable for long term cooling because of corrosion considerations.

Each 300 HP RW pump supplies 9700 gpm at a 75 foot head. Inlet discharge piping is 20 inches, but it diffuses to 24 inches before it reaches the heat exchanger. The temperature rise through the heat exchanger is only 6°F. Technical Specifications (T.S.3.4.7.5) prohibit plant power operation if the inlet temperature rises above 105°F.

The seawater trains have no MOV's or remotely operated valves. Each pump has a 20 inch check valve in the discharge. There are no locked valves in the system. Manual valves are locally indicated. Table F.1, reproduced from the Crystal River FSAR, contains design information on specific DHCCS equipment.

F.1.2 DHCCCS SYSTEM OPERATION

The DHCCCS is required to operate when any of the components it serves are in operation. These consist of pumps in the Low Pressure Heat Removal System, Containment Spray System, and High Pressure Injection System pump MUP-1C. The DHCCCS is required during emergency operation for component cooling and decay heat removal, and during normal operation for decay heat removal on reactor shutdown. Operation of the system is initiated either manually, or on the 1500 psi ESAS trip signal.

Normal Operation - This system has no function when the plant is at power. Under normal shutdown, the system removes decay heat from heat exchangers DHHE-1A/1B. The system is normally in a standby state with its valves aligned for emergency service.

Emergency Operation - This system is activated on ES signal. Activation consists of starting RWP-3A/3B and DCP-1A/1B.

Control - Pumps can be manually started or stopped from the control room or locally at the breakers. Valves DCV-18/DCV-178 are manually controlled from the control room (PSA panel).

Testing of the closed cycle pumps does not require reconfiguration of the loop. Testing of each pump is done once a month per SP-340. DCV-18/17 and DCV-178/177 are stroked once a quarter. All valves are checked for proper position once a month per SP-347. Testing of the two loops is alternated on a two-week staggered basis.

Each raw water pump is also tested once a month per SP-340. Check valves RWV-34 and 37 are checked with the pumps. Valves are checked for proper position once a month per SP-347. Testing is on a two-week staggered basis. Maintenance was assumed to be performed only on major components such as pumps and valves.

Table F.1
Component Design Information

Decay Heat Closed Cycle Heat Exchangers

Number	2
Type	Shell and Tube
Duty Btu/h	120 x 10 ⁶ Normal
Sea Cooling Water Flow (tubeside), gpm	9700
Sea Cooling Water Temperature, F	85
Closed Cycle Cooling Water Outlet Temp, F	105 Max
Closed Cycle Cooling Water Flow (shell side), gpm	3200
Design Pressure, Shell/Tube, psig	100/75
Max Design Temperature, Shell/Tube, F	200/140
Tube Material	90/10 Cu-Ni
Shell Material	Carbon Steel, ASTM
Channel Material	2% Nickel Cast Iron
Code/Seismic Class	ASME Section VIII/I

Decay Heat Closed Cycle Cooling Water Pumps

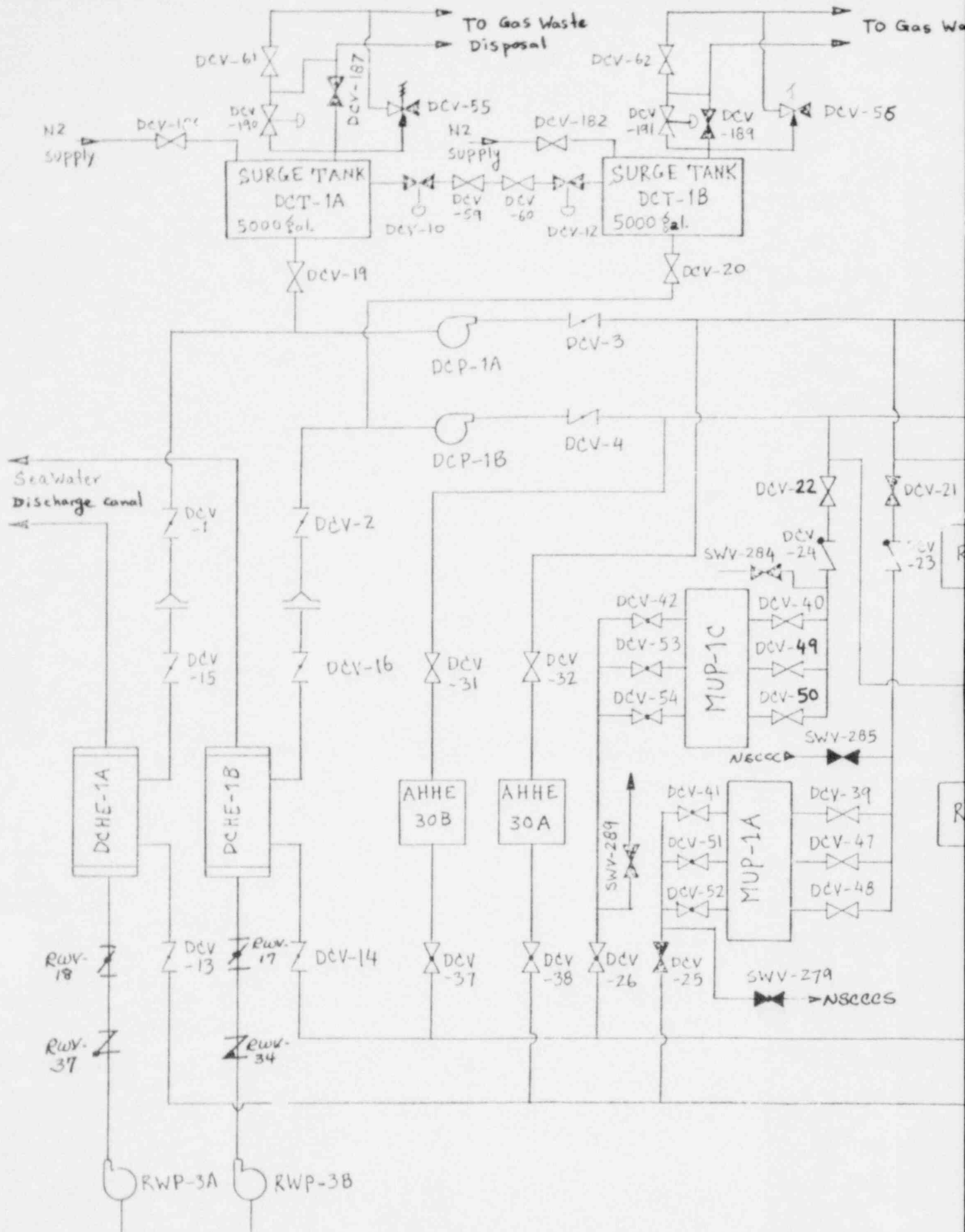
Number	2
Flow, gpm	3200
Design Head, ft	80
Design Pressure, psig	100
Max Design Temperature, F	135
Seismic Class	I

Decay Heat Closed Cycle Surge Tank

Number	2
Capacity, gal.	5000
Design Temperature, F	135
Design Pressure, psig	15
Material	Welded Carbon Steel
Code/Seismic Class	ASME Section VIII/I

Decay Heat Service Seawater Pumps

Number	2
Flow, gpm	9700
Design Head, ft	75
Design Pressure, psig	75
Design Temperature, F	109
Seismic Class	I



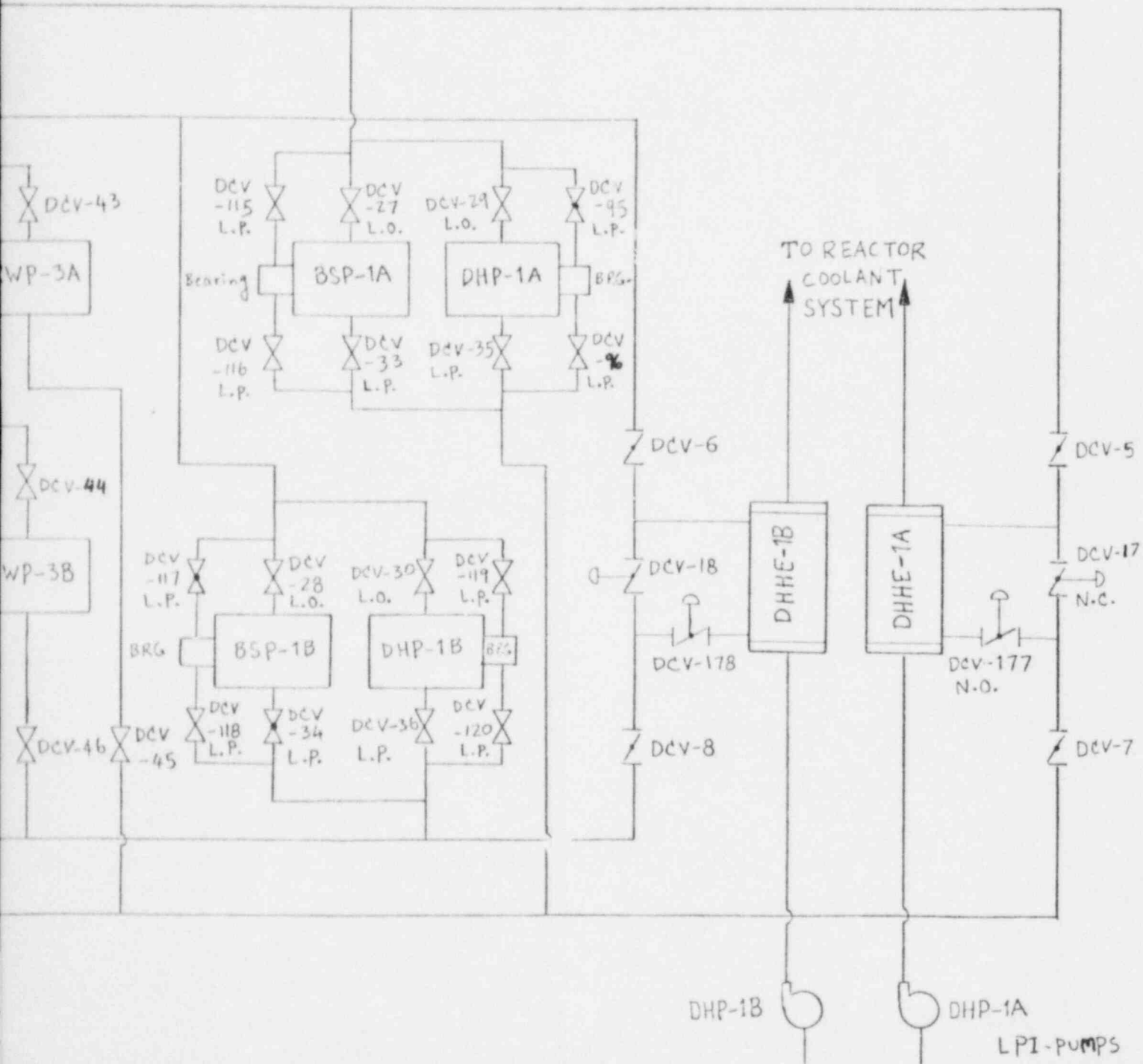


Figure F.1 Decay Heat Closed Cycle Cooling System Schematic Diagram

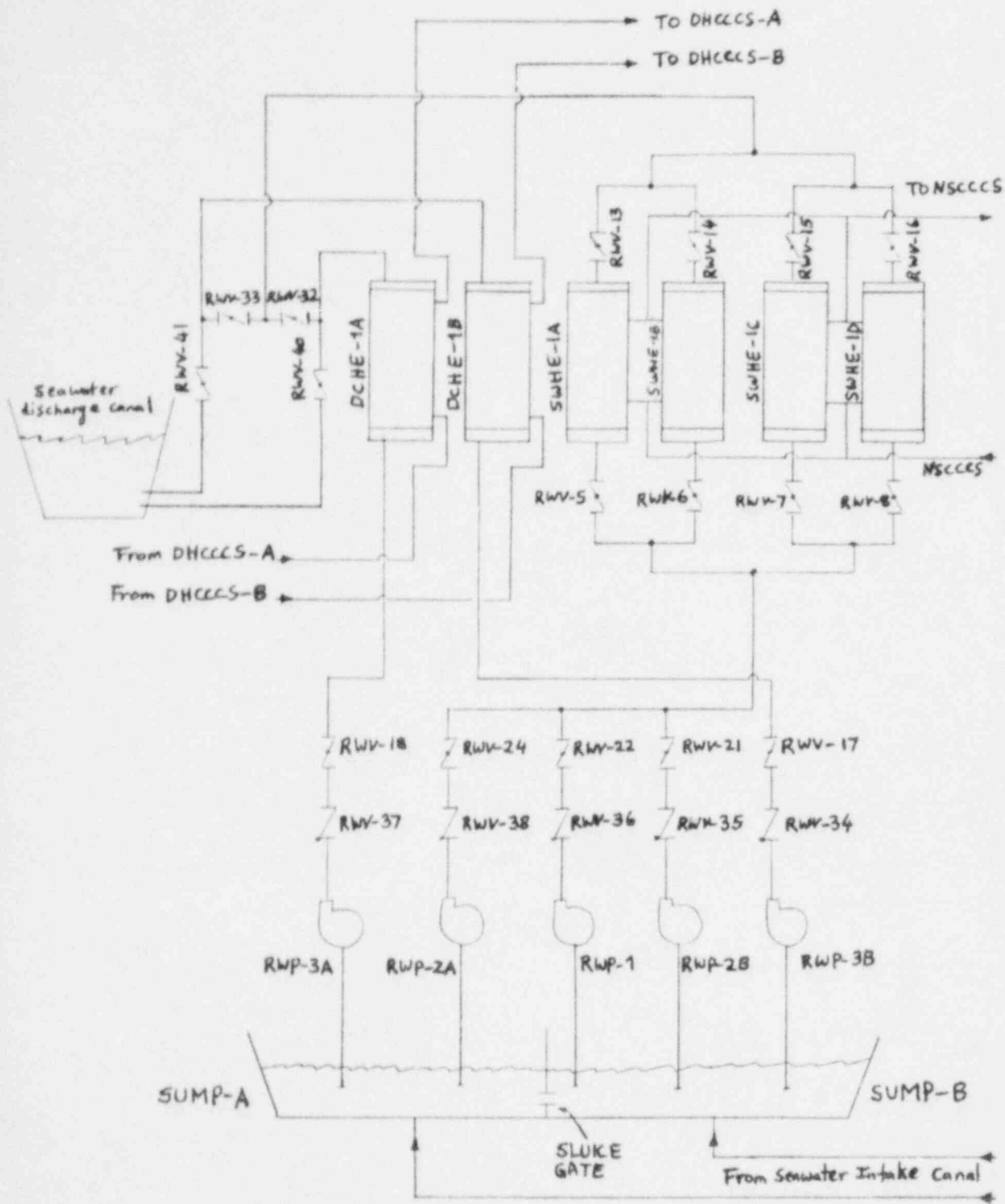


Figure F.2 Decay Heat (Raw) Seawater System Schematic Diagram

F.2 SYSTEM SIMPLIFIED FAULT TREE

Figure F.3 is a simplified fault tree of the closed loop portion of DHCCCS Train A. The tree for failure of Train B is identical except for corresponding component number differences. Failure of flow in DHCCCS-A is a single fault for Train A of the Low Pressure and Containment Spray Systems. Failure of flow in DHCCCS-B will fail the analogous components, and in addition MUP-1C. There are additional faults which can cause cooling failure of components in the Low Pressure and Containment Spray Systems independently of the other components. These faults are primarily mispositioning of valves due to human error.

The major assumptions used to construct the simplified fault tree for DHCCCS-Train A (shown in Figure F.3) are listed below:

- a. Components, lines, and valves that were considered insignificant contributors were omitted from the fault tree.
- b. The DHCCCS is a normally inactive system. There is a probability it will be unavailable on demand due to maintenance, repair, or misposition of valves due to human error. There are no MOV's in the system. The manual block valves associated with each component are locally indicated and are not locked. Positions of valves in the flow path are checked once a month per SP-347. The only locked valves in the system are those on the cooling lines of DHP-1A, BSP-1A, and in the case of Train B, MUP-1C. Test frequencies are listed in the descriptive section. Each train is tested de facto, once every two weeks for three hours when the corresponding Decay Heating (LPI) pump is operated.
- c. It was assumed that if flow to DHHE-1A was blocked, DCP-1A could still operate against the shut-off head, thus supplying bearing and motor cooling to the RWP-3A, BSP-1A, DHP-1A, and in the case of Train B, MUP-1C. Furthermore, it was assumed that failure to provide cooling for the pumps implies failure to provide cooling to DHHE-1A.

- d. The system does not require reconfiguration for testing. It is, therefore, never unavailable due to periodic testing.
- e. The gas pressure in the surge tank is not necessary for system operation. The intent is to prevent air bubbles from accumulating in the high points of the system. However, if the surge tank valve, DCV-19, is inadvertently closed, it was assumed that flow could not be established in the system.
- f. All pumps can be started from the control room or at the breaker.
- g. The Auxiliary Building which contains the closed cycle DHCCCS pumps, also contains the four nuclear service heat exchangers, the two DHCCCS heat exchangers, and three surge tanks. Common causative damage events could result in significant flooding of the room. This is a single fault for both DHCCCS pumps. However, the pump room is large and is equipped with a sump pump.

The major assumptions used to construct the simplified fault tree for the raw seawater portion of DHCCCS- Train A (shown in Figure F.3) are shown below:

- a. Components, lines, and valves which were not considered significant were omitted from the analysis.
- b. Loss of cooling to the bearing of RWP-3A is not considered significant for this study. The bearing pot is supplied by three sources. Cooling is accomplished by circulation of water through the bearing pot. The primary source of water is the domestic water system. The demineralized water system backs up the domestic water supply system. If both of these systems fail, the seawater will back into the bearing. This provides adequate cooling. It is not done on a permanent basis because it is undesirable from a corrosion standpoint.
- c. The raw water loop of DHCCCS is a normally inactive system. There is a probability that it will be unavailable due to maintenance, repair, and mispositioning of valves.

- d. Testing does not cause the system to be unavailable. Testing requires no reconfiguration. Test frequencies are stated in the descriptive section of this report. There are no locked valves in the system.
- e. The pumps can be started from the control room or at the breaker.
- f. Severe flooding of the pump room is a single fault which fails the pumps in both raw water trains.
- g. Pump cavitation was considered unlikely enough to be ignored.
- h. It was assumed the intake canal never goes dry while the plant is operating. T.S.3.4.7.5 limits the bottom of the canal to EL 74 and the minimum water level to EL 81. T.S.4.7.5.1 requires the inlet water temperature and water level to be checked every 24 hours. It was further assumed the seawater sump never goes dry. Either section of the sump may be out of service at any given time for maintenance. There is a 48" pipe which gravity feeds the seawater sump from the intake structure. A separate pipe goes from the intake structure to each sump. A sluice gate also connects the two sumps. The canal is wide enough to preclude blockage by shipwreck. There are large grates on the intake structure which remove trash, seaweed, flotsam and jetsam from the seawater. It was assumed that blockage of these grates to the extent that they block flow is not possible.
- i. OP-404 contains a procedure for the lay-up of the seawater side of DCHE-1A to prevent marine growth. This basically is a gravity drain and flush with domestic water. It involves opening and closing of drain valves, vent valves, and fill valves. Because these lines are very small, discharge rates would be very small if a valve was inadvertently left in the wrong position. For this reason, improper filling procedure was not considered a credible fault.
- j. Due to its nature, the seawater system is exposed to a very corrosive-marine growth environment. Failures of the two seawater pumps were assumed to be coupled, as were failures of the two discharge check valves. Failure (plugging, blockage, marine-encrustation) of equipment in the dormant state was also considered. However, plugging and blockage of equipment while in operation was not considered likely.

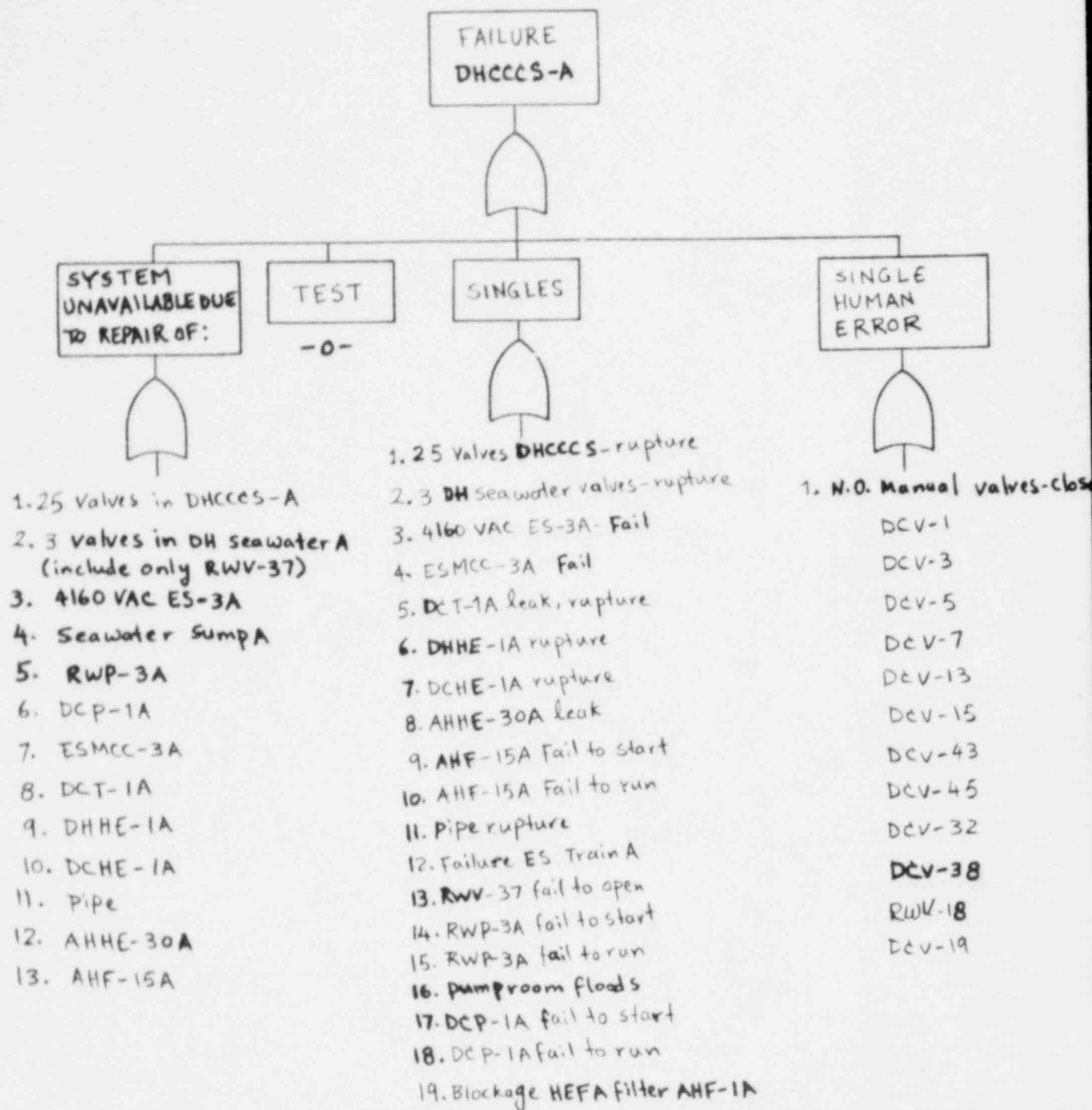


Figure F.3 Simplified Fault Tree - DHCCCS - Train A (including DHSS)

F.3 SYSTEM QUANTIFICATION

F.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The DHCCCS is a double train system with no cross-ties. This configuration allows failure of a single train to fail component cooling to the corresponding single train of several safety systems. Each train is dependent on the availability of AC power (AC power Train A powers DHCCCS Train A equipment and AC power Train B powers DHCCCS Train B equipment).

For cases where offsite power is available, the unavailability of a single train of DHCCCS was assessed to be principally due to single hardware faults, which were dominated by failure of the raw water pump, and to maintenance outages. The unavailability of both trains was assessed to be principally due to coupled raw water pump and check valve failure and maintenance outages coupled with failures on the in-service train.

For cases where offsite power is lost, diesel failures become dominant contributors to both single and double train DHCCCS failure, along with the same contributors described above. The unavailability of a single train of the DHCCCS for the loss-of-offsite power case is about a factor of three higher than the case where offsite power is available.

F.3.2 SYSTEM FAULT TREE QUANTIFICATION - INJECTION PHASE

This section presents the quantification of the DHCCCS unavailability for required emergency operation during the injection phase of a postulated accident. The quantitative results are presented in table form with attached notes outlining the assumptions. To perform the fault tree quantification, the simplified fault tree presented in Section F.3 was rearranged and is presented in this section in modular form.

Two modularized fault trees were constructed for the DHCCCS, one for failure of Train A and the other for failure of Train B. The failure of both trains is the product of these top events. In the new tree the product of two gates that were assumed to be coupled is treated as described in Section 4.1 of the Main Report.

Table F.2 shows the DHCCCS success requirements, Table F.3 contains the top event definitions for the two modularized fault trees, trees, and Figure F.4 shows the modularized fault trees for DHCCCS Trains A and B. The unavailability of each gate is shown on these as well as the top event unavailability. Table F.4 shows the Boolean equation that represents the fault trees. Table F.5, the quantification tables, shows the quantification of each gate, by component and failure mode. The attached notes explain the assumptions used in the quantification. Table F.6 summarizes the point estimates for each gate, and the error factors that were used in the sensitivity analysis.

Table F.2 DHCCCS - System Success Requirements

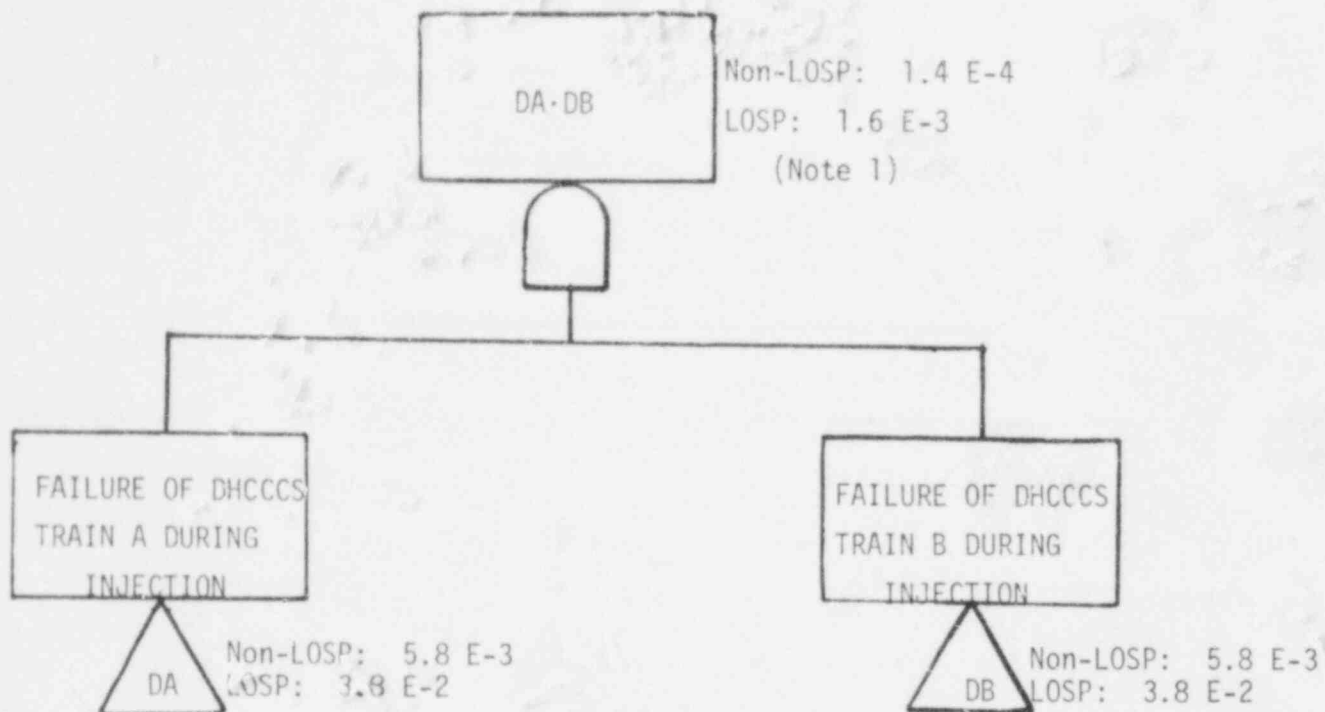
<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B1, B2, B3, B4, transient initiators	Train A delivers one pump flow for component cooling and/or decay heat removal during injection.	1,2
	Train B delivers one pump flow for component cooling and/or decay heat removal during injection.	3

-
- NOTES: 1. The DHCCCS is required for component cooling and/or decay heat removal for all LOCA sizes and transients requiring containment spray success.
2. Train A of the DHCCCS supplies component cooling for containment spray pump BSP-1A, makeup pump MUP-1A, raw seawater pump RWP-3A, decay heat removal pump DHP-1A, and decay heat removal from low pressure Train A.
3. Train B of the DHCCCS supplies component cooling for containment spray pump BSP-1B, makeup pump MUP-1C, raw seawater pump RWP-3B, decay heat removal pump DHP-1B, and decay heat removal from low pressure Train B.

Table F.3 DHCCCS Top Event Definitions

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
DA	Failure of DHCCCS Train A to provide one pump flow with ultimate heat removal for component cooling or decay heat removal during injection.	1
DB	Failure of DHCCCS Train B to provide one pump flow with ultimate heat removal for component cooling or decay heat removal during injection.	1

NOTE: 1. The event DA(DB) includes failures in both the closed cycle cooling system and the raw seawater system.



Note

- 1 Events DA and DB are not independent.

Figure F.4A Modularized Fault Tree for Event "DA·DB"

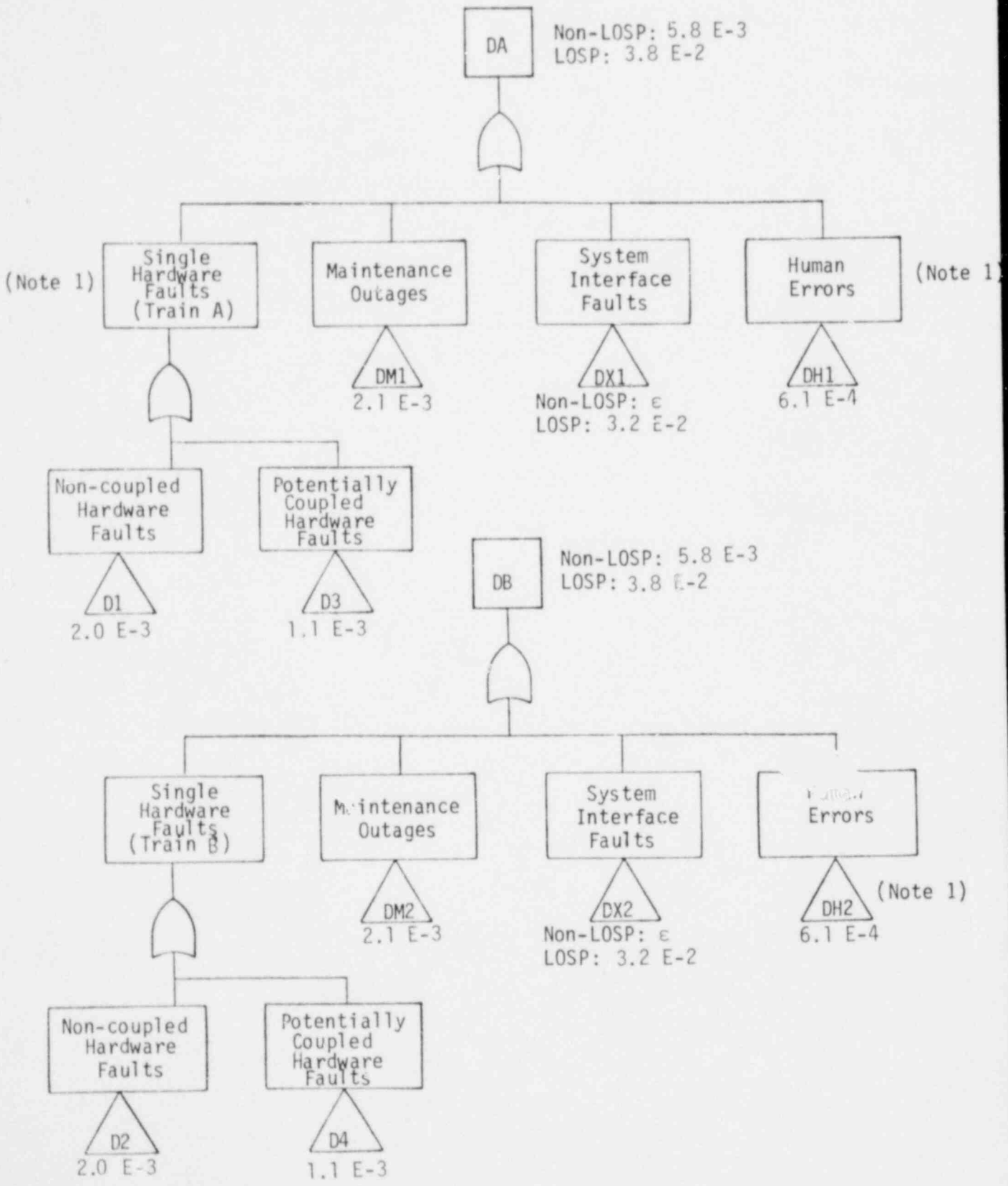


Figure F.4 Modularized Fault Trees for Events "DA" and "DB"

Figure F.4 - DHCCCS - Fault Trees

NOTES

1. Valve faults that would prevent component cooling to specific equipment are included in the fault tree analysis of the system in which the equipment is found.

Table F.4 DHCCCS - Injection

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENT

NOTES

$$DA = D1 + D3 + DM1 + DX1 + DH1$$

$$DB = D2 + D4 + DM2 + DX2 + DH2$$

$$DA \cdot DB = D3 \cdot D4 + (D1 + DX1 + DH1) \cdot (D2 + D4 + DM2 + DX2 + DH2) + D3 \cdot (D2 + DM2 + DX2 + DH2) + DM1 \cdot (D2 + D4 + DX2 + DH2)$$

1,2

INTERMEDIATE EVENTS

$$DX1 = ACA + DCA$$

3

$$DX2 = ACB + DCB$$

3

-
- NOTES: 1. Terms representing maintenance on both legs at the same time are deleted since this is prohibited by Technical Specifications.
2. The term $D3 \cdot D4$ represents component failures that were assumed to be coupled. See Quantification Tables.
3. DC power train failure is explicitly included in the Boolean equations. However, DC power train failure is also included in the failure of the AC trains, and will reduce out.

Table F.5 (1/3) Event "DA" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES																															
D1	25 VALVES DCT-1A DHRE-1A AHHE-3A AHF-15A AHF-15A PIPE ESFAS A PUMP RWP-3A PUMP DCP-1A DCP-1A HEPA FILTER	HARDWARE FAULTS THAT ARE NOT COUPLED WITH TRAIN B FAULTS RUPTURE SURGE TANK RUPTURE LOW PRESSURE SYSTEM HEAT EXCHANGER RUPTURE PUMP COOLING HEAT EXCHANGER RUPTURE PUMP COOLING FAN FAILS TO START FAILS TO RUN RUPTURES (SEVERAL SECTIONS) FAILS TO INITIATE, AND OPERATOR FAILS TO RECOVER FAILS TO RUN FAILS TO START FAILS TO RUN PLUGGED	: 1.0 E-5 (2.1E-4)(.1) 3.0 E-5 D 3.0 E-5	10	2.0 E-3 e e e 3.0 E-4 1.0 E-4 e 2.1 E-5 3.0 E-4 1.0 E-3 3.0 E-4 e 2.0 E-3	3 ⁺ , 3 ⁻ 3 ⁺ , 3 ⁻ 10 ⁺ , 10 ⁻ 3 ⁺ , 3 ⁻		1 2 3,7 4 2																															
									D3	HARDWARE FAULTS THAT ARE COUPLED WITH TRAIN B FAULTS FAILS TO OPEN FAILS TO START	D D		1.1 E-3 1.0 E-4 1.0 E-3 e=1.1 E-3	3 ⁺ , 3 ⁻ 3 ⁺ , 3 ⁻ 3 ⁺ , 3 ⁻	S S S																								
																	DM1	TRAIN A MAINTENANCE OUTAGE OUT FOR MAINTENANCE OUT FOR MAINTENANCE OUT FOR MAINTENANCE FAN OUT FOR MAINTENANCE	.02/720 .02/720 .02/720 .02/720	19 19 19 19	2.1 E-3 5.3 E-4 5.3 E-4 5.3 E-4 5.3 E-4 e=2.1 E-3	3 ⁺ , 3 ⁻ 3 ⁺ , 3 ⁻ 3 ⁺ , 3 ⁻ 3 ⁺ , 3 ⁻ 3 ⁺ , 3 ⁻	M M M M M																
																									DK1 ACA	SYSTEM INTERFACE FAULTS AC TRAIN A NON LOSP LOSP	e 3.2 E-2				6								
																																	DM1 HUMAN	5 OPPORTUNITIES TO LEAVE SINGLE VALVES CLOSED AFTER MAINTENANCE	6.0 E-4	3 ⁺ , 3 ⁻	H	4	

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
D2		HARDWARE FAULTS THAT ARE NOT COUPLED WITH TRAIN A FAULTS			2.0 E-3			
	25 VALVES	RUPTURE			e			
	DCT-1B	RUPTURE			e			
	DHHE-1B	LOW PRESSURE HX-RUPTURE			e			
	AHHE-30B	PUMP COOLING HEAT EXCHANGER			e			
	AHF-15B	PUMP COOLING/FAN FAILS TO START	D		3.0 E-4	3 ⁺ , 3 ⁻		
	AHF-15B	PUMP COOLING/FAN FAILS TO RUN	1.0 E-5	10	1.0 E-4	3 ⁺ , 3 ⁻		2
	PIPE	RUPTURE (SEVERAL SECTIONS)	D		e			
	ESFAS-B	FAILS TO INITIATE AND OPERATOR FAILS TO RECOVER	(2.1E-4)(.1)		2.1 E-5			3,7
	RWP-3B	RAW WATER PUMP FAILS TO RUN	3.0 E-5	10	3.0 E-4	10 ⁺ , 10 ⁻		2
	DCP-1B	PUMP FAILS TO START			1.0 E-3	3 ⁺ , 3 ⁻		
	DCP-1B	PUMP FAILS TO RUN	3.0 E-5	10	3.0 E-4	10 ⁺ , 10 ⁻		2
	HEPA-FILTER	PLUGGED			e			
					$\Sigma=2.0 E-3$			
D4		HARDWARE FAULTS THAT ARE COUPLED WITH TRAIN B FAULTS			1.1 E-3	3 ⁺ , 3 ⁻	S	
	RWV-34	CHECK VALVE/FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻	S	
	PUMP RWP-3B	FAILS TO START	D		1.0 E-3	3 ⁺ , 3 ⁻	S	
					$\Sigma=1.1 E-3$			
D12		TRAIN B MAINTENANCE OUTAGE			2.1 E-3	3 ⁺ , 3 ⁻	M	
	RWV-34	CHECK VALVE OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
	PUMP RWP-3P	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
	PUMP DCP-1B	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
	AHF-15B	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
					$\Sigma=2.1 E-3$			
DX2		SYSTEM INTERFACING FAULTS						
ACB		AC-TRAIN B						E
		NON LOSP			e			
		LOSP			3.2 E-2			
DH2	HUMAN	6 OPPORTUNITIES TO LEAVE SINGLE VALVES CLOSED AFTER MAINTENANCE			6.0 E-4	3 ⁺ , 3 ⁻	H	4

Table F.5 (2/3) Event "DB" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
D3-D4		COUPLED FAILURES OF EQUIPMENT EXPOSED TO SEAWATER ENVIRONMENT			1.1 E-4	1 ⁺ , 10 ⁻		5
	(RWV-34)	COUPLED SEAWATER CHECKVALVE FAILURES	(1.0 E-4)(0.1)		1.0 E-5	2 ⁺ , 2 ⁻	B	
	(RWP-3A) x (PWP-3B)	COUPLED SEAWATER PUMP FAILURES	(1.0 E-3)(0.1)		1.0 E-4	2 ⁺ , 2 ⁻	B	
					<u>1.1 E-4</u>	2 ⁺ , 2 ⁻		

Table F.5 (3/3) Event "D3-D4" (Coupled Failure) Quantification for Failure of Both Trains

Table F.5 DHCCCS - Injection

QUANTIFICATION TABLES

NOTES

- 1 Rupture of any one of 25 separate valves in a single train of the DHCCCS was assessed to fail the system. These valves each see surge tank system pressure. However, rupture of any of the valves would drain the surge tank which is monitored. Therefore, these faults are assessed to be ϵ .
- 2 The DHCCCS is required for all LOCA-sizes and transients. The injection period depends on the LOCA size or transient duration (0.5 to 10 hours). The fault duration time was conservatively chosen for the 10 hour injection period.
- 3 The failure of ESFAS to actuate single equipment was assessed as 2.1 E-4 (Event ISS1 in ESAS quantification). This number is applicable for a B4 LOCA and would be smaller for the other LOCA cases; however, it is an insignificant contributor and was therefore not changed for the larger LOCAs. Failure to recover was assumed to be 0.1 per act.
- 4 Each opportunity to leave a valve open is associated with isolation of active components during maintenance. When more than one valve is involved with the maintenance activity on a single component, they are treated collectively as providing one opportunity for inadvertent closure. The valve combinations for Train A are: DCV-1, -3 and -19 (for DCP-1A); DCV-5 and -7 (for DHHE-1A); DCV-13 and -15 (for DCHE-1A); DCV-43 and -45 (for RWP-3A); DCP-32 and -38 (for AHHE-30A); and RWV-18 (for RWP-3A). Similar combinations apply to Train B. This fault was assessed assuming a human error probability of 1.0 E-2 for leaving closed after maintenance any of the valves associated with one component. The frequency at which this could occur was assumed to be 0.02 times per month. However, because the decay heat system is tested once every 2 weeks, the fault duration time was assessed as 1/2 month. The fault was assessed as 6 opportunities times 0.02 times 1/2 times 1.0 E-2 .
- 5 The seawater check valves and pumps in Trains A and B were assumed coupled with a β -factor of 0.1.
- 6 Only AC power faults are involved, although DC power is required to close breakers that start pumps. DC power train failures are included in the AC fault tree, and would Boolean reduce out of the gate for system interface faults. Therefore, it would not be appropriate to add the AC and DC unavailability to obtain the system interface gate unavailability.

Table F.5 DHCCCS - Injection

QUANTIFICATION TABLES (NOTES) continued

- 7 Failure of ESAS to provide actuation signals to both trains is not included because the potential for recovery is high enough to make this contribution negligible.

Table F.6 DHCCCS - Injection Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
D1	2.0 E-3
D3	1.1 E-3
DM1	2.1 E-3
ACA	ϵ^* 3.2 E-2**
DH1	6.0 E-4
D2	2.0 E-3
D4	1.1 E-3
DM2	2.1 E-3
ACB	ϵ^* 3.2 E-2**
DH2	6.0 E-4
D3·D4	1.1 E-4

*Offsite power available

**Offsite power not available

F.3.3 SYSTEM FAULT TREE QUANTIFICATION - RECIRCULATION PHASE

This section presents the quantification of the DHCCCS unavailability for required emergency operation during the recirculation phase of a postulated accident. As in the injection case, modularized fault trees were constructed for failure of Train A and failure of Train B. Failure of either train during the recirculation phase is predicated on success during the injection phase; if a train fails during injection, it is assumed to be unavailable for recirculation. Thus, only DHCCCS hardware failures that occur during recirculation are assumed to contribute to the top events.

Table F.7 shows the DHCCCS success requirements, Table F.8 contains the top event definitions, and Figure F.5 shows the modularized fault trees for failure of Train A and B, respectively. The unavailability of each gate is shown in these trees, as well as the top event unavailabilities. Table F.9 shows the Boolean equations that represent the fault trees. Table F.10, the quantification table, shows the quantification of each gate, by component and failure mode. The attached notes to this table outline the assumptions used in the quantification. Table F.11 summarizes the point estimates for each gate.

Table F.7 DHCCCS - System Success Requirements - Recirculation

<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B1, B2, B3, B4, transient initiators	Train A delivers one pump flow for component cooling and/or decay heat removal during recirculation.	1,2,4
	Train B delivers one pump flow for component cooling and/or decay heat removal during recirculation.	3,4

-
- NOTES:
1. The DHCCCS is required for component cooling and/or decay heat removal for all LOCA sizes and transients requiring containment spray success.
 2. Train A of the DHCCCS supplies component makeup pump MUP-1A, raw water pump RWP-3A, decay heat removal pump DHP-1A, and decay heat removal from low pressure Train A.
 3. Train B of the DHCCCS supplies component cooling for containment spray pump BSP-1B, makeup pump MUP-1C, raw water pump RWP-3B, decay heat removal pump DHP-1B, and decay heat removal from low pressure Train B.
 4. Recirculation phase is assumed to last for 24 hours after injection phase.

Table F.8 DHCCCS Top Event Definitions - Recirculation

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
DA*	Failure of DHCCCS Train A to provide one pump flow with ultimate heat removal for component cooling or decay heat removal during recirculation.	1,2
DB*	Failure of DHCCCS Train B to provide one pump flow with ultimate heat removal for component cooling or decay heat removal during recirculation.	1,2

NOTES: 1 The event DA*(DB*) includes failures in both the closed cycle cooling system and the raw water system.
 2. Assumes success during injection phase.

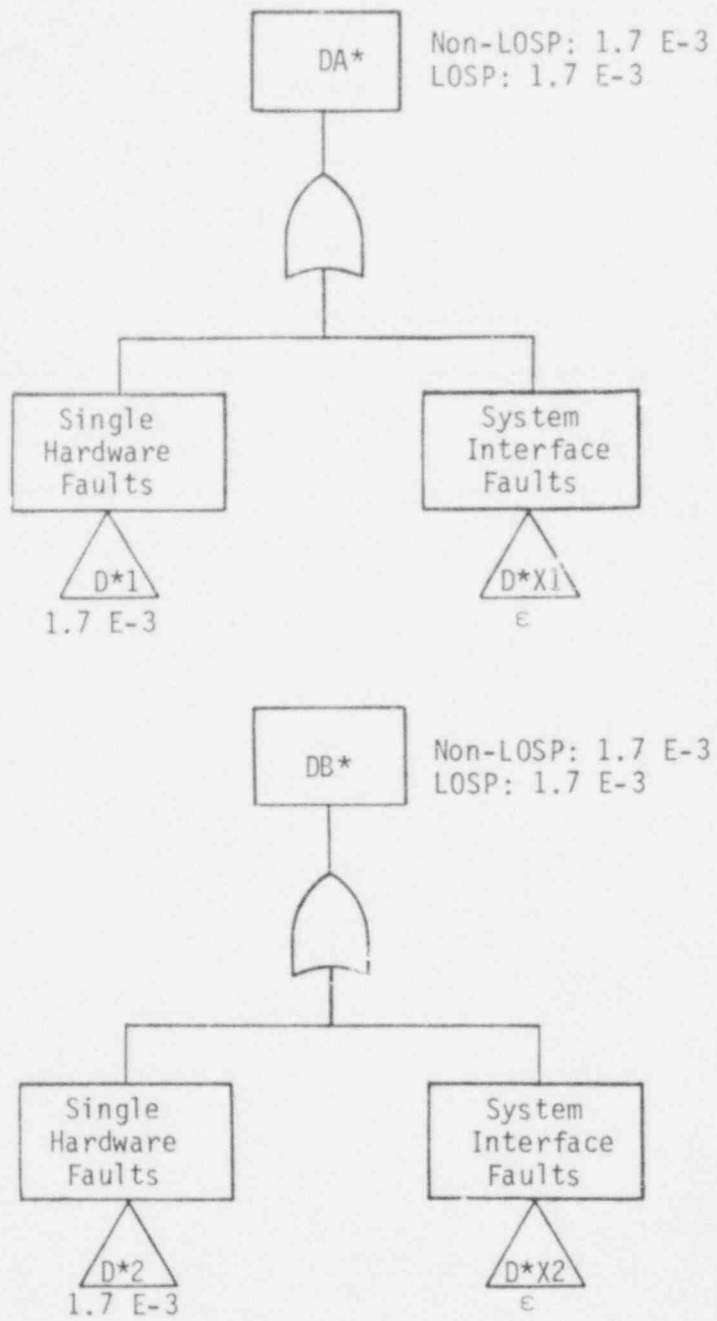


Figure F.5 Modularized Fault Tree for Events "DA*" and "DB*"

Table F.9 DHCCCS - Recirculation

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

NOTES

$$\begin{aligned} DA^* &= D^*1 + D^*X1 \\ DB^* &= D^*2 + D^*X2 \end{aligned}$$

INTERMEDIATE EVENTS

$$\begin{aligned} D^*X1 &= ACA^* \\ D^*X2 &= ACB^* \end{aligned}$$

1

1

NOTES: 1. Offsite power is assumed to be recovered when entering the recirculation phase. The unavailability of AC power with offsite power available was calculated to be negligible compared to other system failure modes.

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
D*1		HARDWARE FAULTS THAT OCCUR DURING RECIRCULATION - TRAIN A			1.7 E-3			
	FAN HAF-15A	FAILS TO RUN	1.0 E-5	24	2.4 E-4	3 ⁺ , 3 ⁻		
	PUMP PWP-3A	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10 ⁺ , 10 ⁻		
	PUMP DCP-1A	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10 ⁺ , 10 ⁻		
					<u>Σ=1.7 E-3</u>			
D*X1		SYSTEM INTERFACE FAULTS			E			
ACA*		AC TRAIN A						
		FAILS DURING RECIRCULATION			E			
		NON LOSP			E			
		LOSP			E			
D*2		HARDWARE FAULTS THAT OCCUR DURING RECIRCULATION - TRAIN B			1.7 E-3			
	FAN AHF-15B	FAILS TO RUN	1.0 E-5	24	2.4 E-4	3 ⁺ , 3 ⁻		
	PUMP R/P-3B	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10 ⁺ , 10 ⁻		
	PUMP DCP-1B	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10 ⁺ , 10 ⁻		
					<u>Σ=1.7 E-3</u>			
D*X2		SYSTEM INTERFACE FAULTS			E			
ACB*		AC TRAIN B						
		FAILS DURING RECIRCULATION			E			
		NON LOSP			E			
		LOSP			E			

Table F.10 Events "DA*" and "DB*" Quantification

Table F.11 DHCCCS - Recirculation Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
D*1	1.7 E-3
D*X1	E
ACA*	E
D*2	1.7 E-3
D*X2	E
ACB*	E

APPENDIX G

HIGH PRESSURE INJECTION AND RECIRCULATION SYSTEM

APPENDIX G HIGH PRESSURE INJECTION AND RECIRCULATION SYSTEM

G.1 SYSTEM DESCRIPTION AND OPERATION

The HP-system is used to provide emergency coolant to the reactor vessel in the event of a small loss of coolant accident where the reactor coolant system (RCS) is not depressurized sufficiently for core flood or for low pressure coolant injection. The High Pressure Injection (HPI) is also used to delay the need for core flood and low pressure coolant injection in the event of intermediate size RCS breaks.

The HP-system is required to operate during both the injection (HPI configuration) and recirculation (HPR-configuration) phases of small LOCAs and transients. It also provides an alternate to the Emergency Feedwater System for core cooling during loss of feedwater transients, when the EFS is not available (referred to as "Feed and Bleed" operation). The HP-system is an operating mode of the makeup and purification system, and consists of a portion of that operating system, with additional standby components.

G.1.1 SYSTEM DESCRIPTION

The HP-system is comprised of the pumps, valves, storage tank and interconnecting piping shown in Figure G.1. Although three pumps and four injection valves are shown, the system is essentially a two-train system because of its interfaces with other systems. These interfaces are summarized as follows:

- (1) Borated Water Storage Tank (BWST) - common to both trains.
- (2) Engineered Safeguards Actuation System (ESAS)
 - ESAS-A - Starts Pumps 1A and 1B
Closes Valves 27, 53, 64
Opens Valves 23, 24, 73
 - ESAS-B - Starts Pump 1C
Closes Valves 64, 257
Opens Valves 25, 26, 58

- (3) AC Power
 - 4160V Bus 3A - Pumps 1A and 1B
 - 4160V Bus 3B - Pump 1C
 - 480V MCC 3A1 - Valves 23, 24, 27, 53, and 73
 - 480V MCC 3B1 - Valves 25, 26, and 257
- (4) DC Power
 - 125VDC A - Pumps 1A and 1B
 - Valve 64
 - 125VDC B - Pump 1C
 - Valve 64
- (5) Nuclear Services Closed Cycle Cooling System (NSCCCS)
 - Cools Pumps 1A and 1B
- (6) Decay Heat Closed Cycle Cooling System (DHCCCS)
 - Cools Pump 1C

The Crystal River HP-system contains the following features:

- Pump 1B can be shifted from Train A to Train B by manually shifting its circuit breaker from its Bus 3A cubicle to its Bus 3B cubicle.
- Valve 64 isolates HPI from the makeup tank. It gets signals to close from both ESAS trains, and it obtains control power from both 125VDC trains.
- Should loss of power occur on 480VAC Train A, injection valves can be switched manually in the control room to Train B; likewise, injection valves 25 and 26 can be switched to Train A upon loss of Train B power. Loss of 480 VAC power on either train should be readily apparent in the control room.
- The cooling water to pumps 1A and 1C can be changed by realignment of valves to the DHCCCS or NSCCCS systems, respectively. Pump 1B is always cooled by NSCCCS. The lineup of cooling water systems with HPI pumps has been changed to that indicated above and does not agree with the Crystal River Final Safety Analysis Report.

Most of the HP-system components are located inside the auxiliary building adjacent to the reactor building. Exceptions are the borated water storage tank which is located outside adjacent to and south of the reactor building and check valves 36, 37, 42, 43, 160, 161, 163, and 164 which are located in the injection lines inside the reactor building. The pumps are located in an auxiliary building room adjacent to and east of the reactor building. These pumps are separated from each other by concrete walls which serve as missile shields.

The following is a summary description of the major components in the HPI system.

BWST

Capacity 420,000 gal.

Pumps

Type Horizontal, Multistage
Centrifugal, Mechanical
Seal

Rated Capacity
@ 2400 psi 300 gpm
Rated Head 5,545 ft.
Motor Size 700 hp
Design Pressure 3000 psig
Design Temp 200⁰F
Speed 6800 rpm

Each pump is equipped with two lube oil pumps (one AC and one DC) and two gear oil pumps (one AC and one DC). Upon loss of an AC pump, or its power source, the DC alternate pump starts automatically. The AC and DC lube and gear oil pumps are aligned to Train A or Train B power sources in concert with their associated HPI pump lineup.

Valves

All valves are Seismic Class I conforming to ASME III requirements.

G.1.2 SYSTEM OPERATION

HPI is initiated automatically by the engineered safeguards actuation system (ESAS) upon 1500 psig decreasing RCS pressure, 500 psig RCS pressure, or 4 psig increasing reactor building pressure. The system can also be started manually. During normal reactor operation the system draws treated water from a makeup tank using one pump (usually 1B) and discharges that water into RCS loop 3A1 (via control valve 31 and block valve 27 as shown in Figure G.1). The system also provides seal water to the RCS pumps. Upon receipt of an ESAS signal the system is realigned so that coolant is drawn from the borated water storage tank (BWST) by three pumps (two pumps if only diesel power is available) and is discharged through four injection lines into the four RCS cold legs, respectively. The makeup tank and the normal makeup and seal water discharge paths are isolated upon HPI.

Once started by the ESAS the operator cannot reconfigure the system without first bypassing those ESAS channels which initiated HPI. This includes such subsequent reconfiguration as valve realignment for recirculation of spilled fluid from the reactor building sump and injection valve throttling to limit pump flow or coolant loss through a RCS break. All of these reconfigurations are required by procedures. Once valves are reconfigured or pumps stopped they are subject to becoming commanded back to the injection mode by subsequent ESAS signals; e.g., by the 4 psig reactor building pressure signal if not also bypassed.

The following summarizes the operational sequence of the HPI:

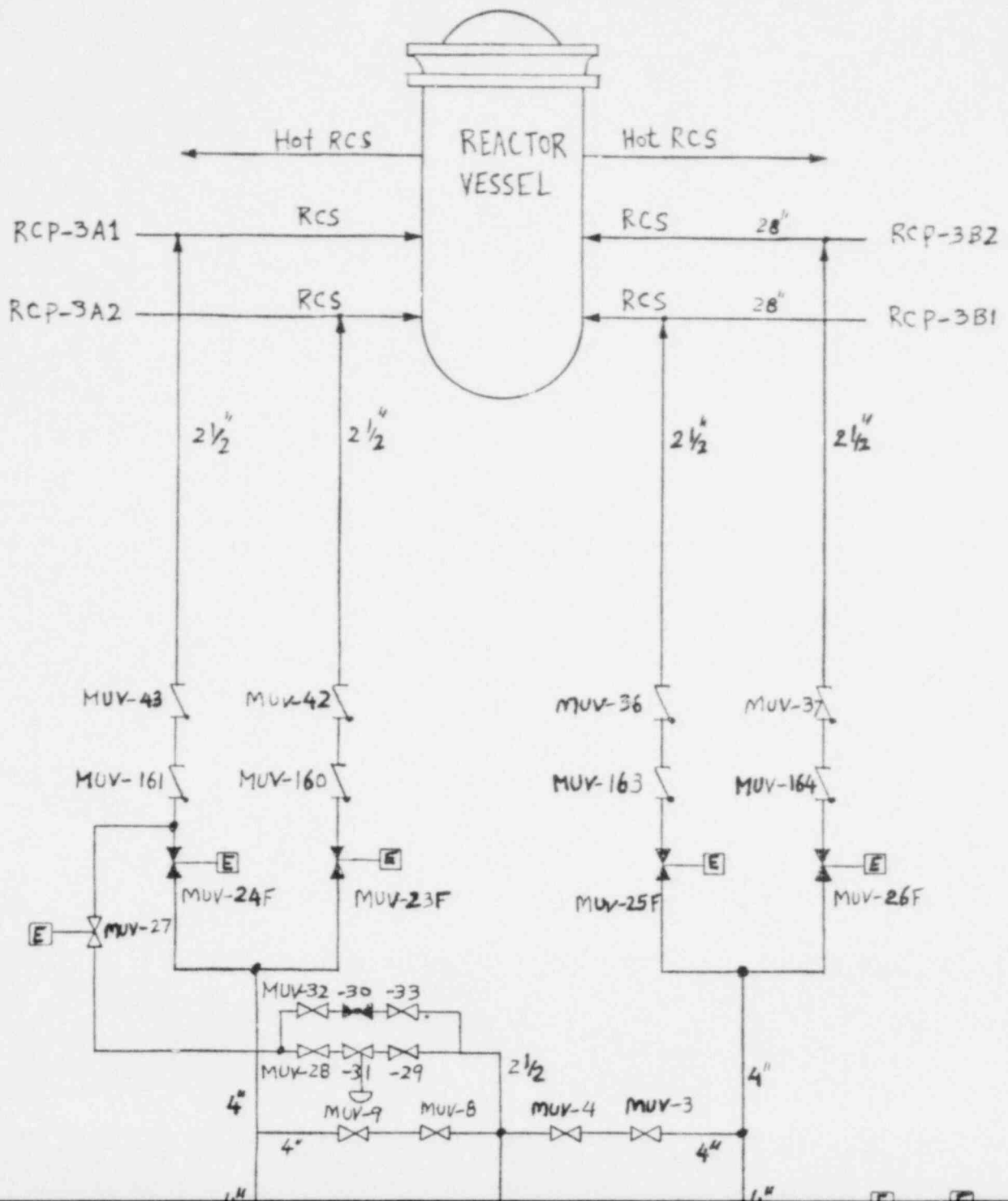
- Pump 1B or 1A normally running with injection via makeup line.
- Figure shows normal valve lineup with either pump 1A or 1B running.
- HPI automatically actuated by ESAS on low RCS pressure (~ 1500 psi).
- Actuation starts all pumps, opens injection valves 23F, 24F, 25F, 26F; opens valve 73, sends open signal to MV 58 (normally open); closes makeup valve 27, closes recirculation valves 257 and 53, closes makeup suction valve 64.

- Some small breaks in the injection line require isolation of the affected line by closing the injection valve. Operator must bypass HPI/ESAS channel to close the valve.
- Procedures (EP-106) call for controlling flow by throttling injection valves. Requires bypassing HPI/ESAS channels A and B.

The HPI pumps are tested by running them alternately for approximately one hour each month. All valves that must respond to an accident are fully or partially stroked once each quarter. Pump and valve tests do not alter the system such that it or its subsystems would be unavailable upon demand.

No maintenance is performed on the system unless a component has failed or the reactor is shut down. Technical specifications require that at least two HPI pumps be operable. If only one pump is operable another pump must be restored within 72 hours, or the plant must be placed in hot standby within six hours. If at hot standby and only one pump is operable, another pump must be restored to operable status within the next seven days, or the plant must be in cold shutdown within 30 hours.

All motor operated valves and pumps can be operated using switches in the control room. Manual valves are locked in position using padlocks.



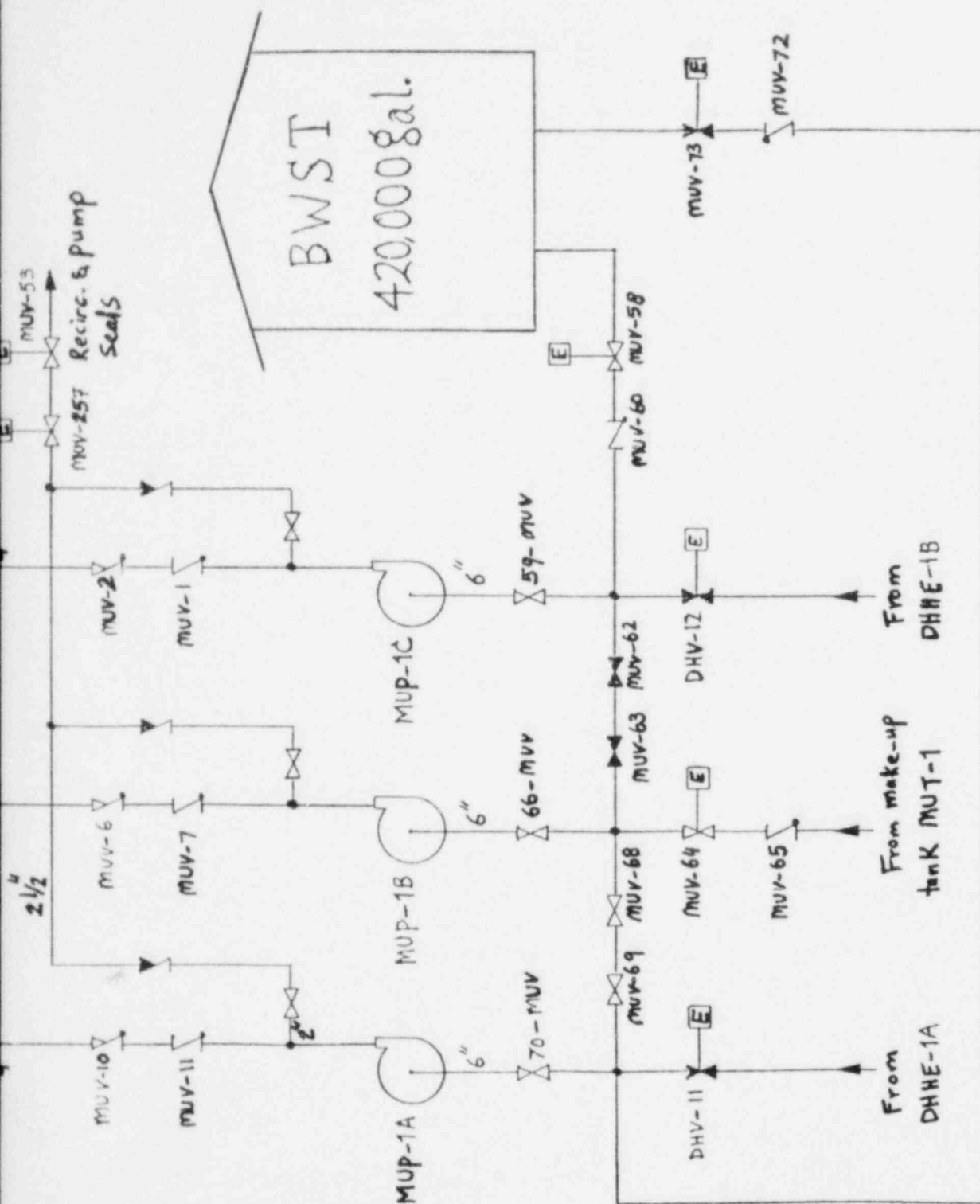


Figure G.1 High Pressure Injection System Schematic Diagram

G.2 SIMPLIFIED FAULT TREE

Two fault trees were developed: one tree for the accident initiating events that require only one-pump flow and another tree for those accident initiators that require two-pump flow. However, the fault tree for the two pump flow case was not evaluated, since:

- Two pump flow is required for ATWS, but ATWS was estimated to be a very low probability event, and ATWS sequences were not evaluated in this study.
- The break size requiring two pump flow (between 0.008 ft² and 0.015 ft²) will result in some core damage if only one pump is operating, but not core melt.*

For these reasons only the fault tree resulting from one pump flow success criteria was evaluated. The simplified form of this fault tree is shown in Figure G.2. The fault tree was developed using information contained in the Crystal River, Unit 3, Final Safety Analysis Report, system drawings (primarily FD-302-661), plant procedures and correspondence, and from plant visits. The simplified form of the fault tree shows only the single passive and active faults and the double active faults. All higher order combinations of component faults were considered to be negligible contributors to system failure probability. Human error events are also shown on the fault tree.

Success/Failure Criteria. One of three HPI pumps is required for all RCS breaks, or for a stuck open power operated relief valve (PORV). Two of three available injection lines were considered successes on the fault tree. One of four injection lines was assumed to be unavailable for injection because of the initiating event. If the break (or initiating event) occurs in the RCS recirculation loop, no credit is given for coolant injection into the broken loop. If the break occurs in the injection line itself (between the block valve and the RCS loop) the block valve must be closed by the operator.

*Telecon 11/16/79 with R. Jones, B&W

Assumptions. Assumptions and ground rules used in the development of the fault tree are as follows:

- (1) Breaks in the RCS which require HPI flow were assumed to be in the cold leg of RCS loop 3B1. Loss of coolant from this loop is somewhat more likely because a stuck open PORV and an open pressurizer spray valve would result in coolant loss from RCS loop 3B1. Failure of valves to open in this injection loop do not appear as faults on the fault tree. The flow requirements for success assume that part of the fluid will be discharged out the break, therefore, success does not depend upon isolation of the break by closing block valve 25.
- (2) HPI injection line breaks were assumed to occur in the line to RCS loop 3B1. It was assumed that a break in any of the four injection lines was equally likely, and therefore the selection would have no bearing on the numerical results. If a break occurs in an injection line it is incumbent on an operator to close the associated block valve; otherwise insufficient coolant will be delivered to the RCS despite the number of operating HPI pumps.
- (3) Isolation of the pump recirculation and RCS pump seal water piping was assumed necessary in order to assure that all flow is injected into the RCS. (Isolation is certainly important from a containment integrity point of view during recirculation. If not isolated, contaminated water would be pumped to the makeup tank and ultimately released to the atmosphere).
- (4) Pump 1B is the pump normally used for RCS coolant makeup. It was acknowledged on the fault tree that this pump might be down for maintenance because of its required long duty cycle (high likelihood of malfunctioning). If pump 1B is down, pump 1A was assumed to be operating as a makeup pump at the time of the accident.

It was assumed that pump 1B is aligned to the Train A services at the time of an accident and that it cannot be changed during the course of an accident. Changeover would require a shifting of pump 1B breaker at the switchgear.

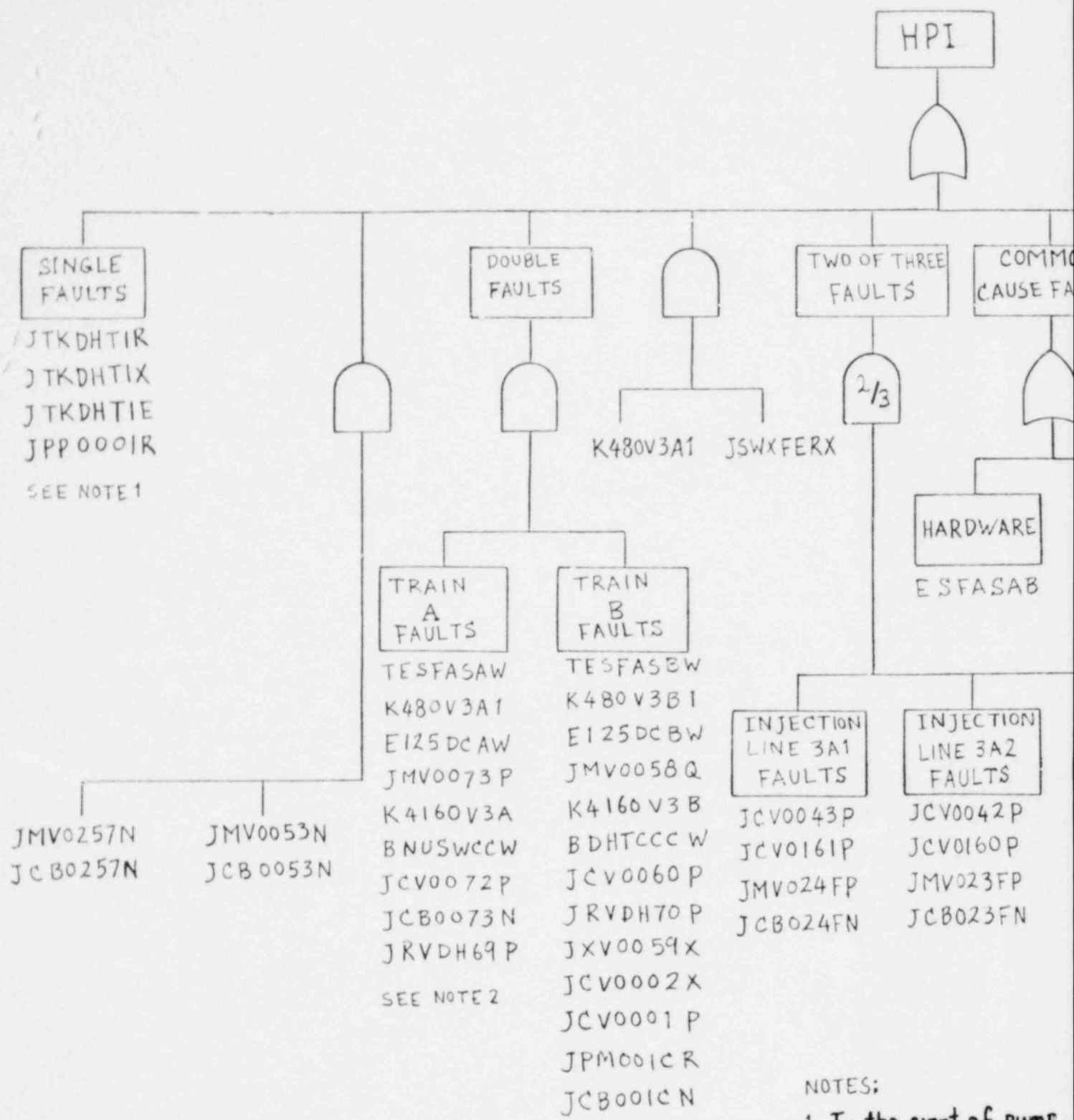
- (5) It was assumed that the system must be started automatically following an accident. This is to say that the operator expects that it will start and if it doesn't start it is too late for the operator to do so. (This is a conservative assumption and may not be a realistic one).

Table G.i (1/2) High Pressure System Fault Summary

SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
JCV0042P	Check Valve 42	Does Not Open
JCV0160P	Check Valve 160	Does Not Open
JMV023FP	Motor Operated Valve 23F	Does Not Open
JMV0073P	Motor Operated Valve 73A	Does Not Open
JCV0072P	Check Valve 72	Does Not Open
JCV0010P	Check Valve 10	Does Not Open
JCV0011P	Check Valve 11	Does Not Open
JPM001AS	Pump 1A	Does Not Start
JPM001AR	Pump 1A	Stops Running
JXV0070X	Manual Valve	Left Closed
JCV0010X	Stop Check Valve	Left Closed
JPM001BQ	Pump 1B	Out of Service
E125BCBW	125VDC Bus B	No Output
JCV0036P	Check Valve 36	Does Not Open
JCV0163P	Check Valve 163	Does Not Open
JMV024FF	Motor Operated Valve 245	Does Not Open
JCV0037P	Check Valve 37P	Does Not Open
JCV0164P	Check Valve 164	Does Not Open
JMV026FP	Motor Operated Valve 26F	Does Not Open
JCV0001P	Check Valve 1	Does Not Open
JCV0002P	Check Valve 2	Does Not Open
JXV0059X	Manual Valve 59	Left Closed
JCV0060P	Check Valve 60	Does Not Open
JMV0058Q	Motor Operated Valve 58	Does Not Remain Open
E125DCAW	125VDC Bus A	No Output
JTKDHT1R	Rank DHT-1 (RWST)	Rupture
JPM001CS	Pump 1C	Does Not Start
JPM001CR	Pump 1C	Stops Running
BNUSWCCW	Nuclear Service Water System	No Cooling Water to Pump 1B
JTKDHT1X	BWST	Not Full
K4160V3A	4160VAC Bus 3A	No Power to Pump 1B
K480V3A1	480VAC Bus 3A1	No Power to Valves
TESFASAW	Engineered Safeguards Actuation System A	No Signal to Start HPI-A
BDHTCCCW	Decay Heat Closed Cycle Cooling	No Cooling to Pump 1C
JTKDHT1E	BWST Output Piping	Plugged
K4160V3B	4160VAC Bus 3B	No Power to Pump 1C

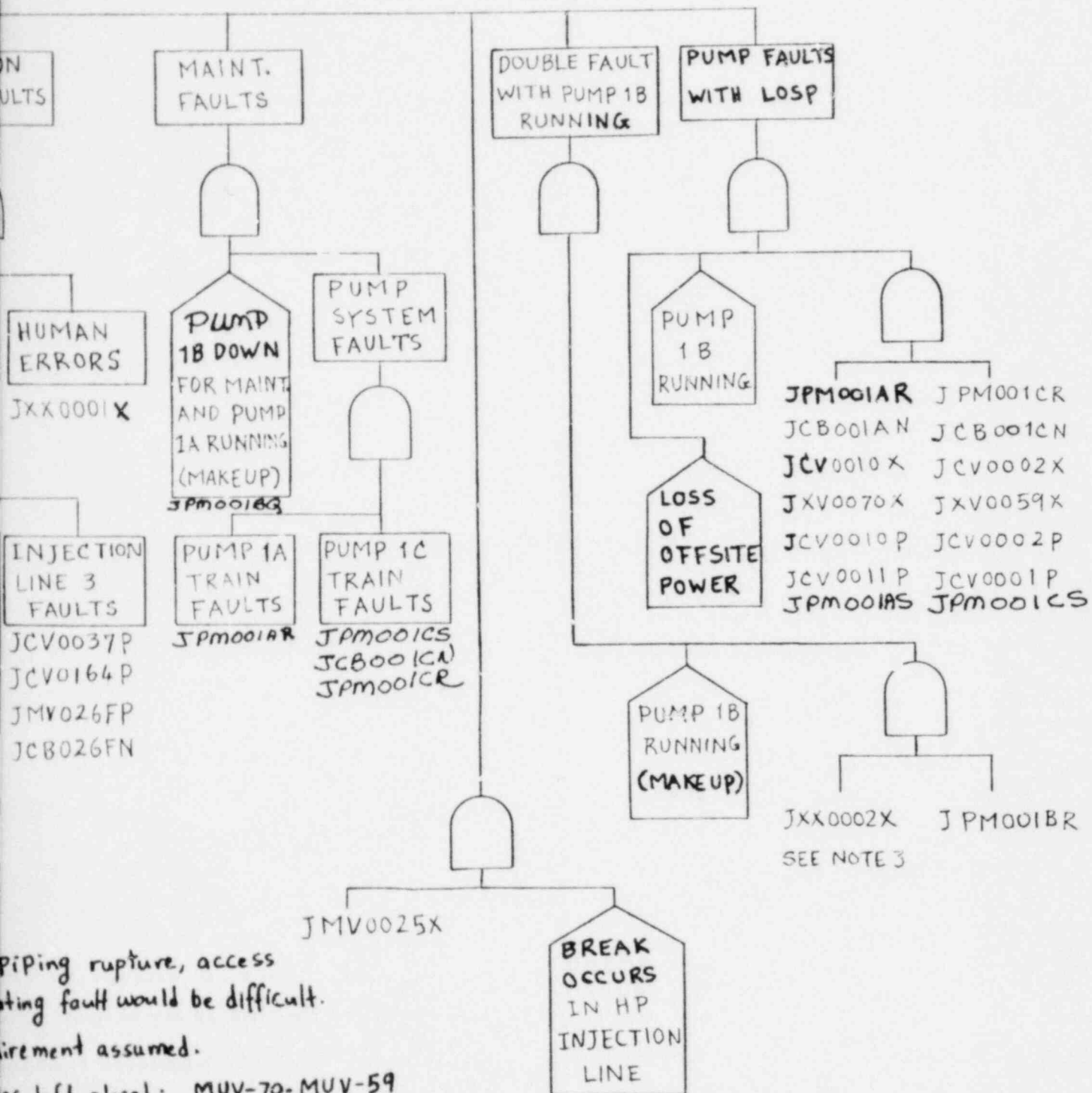
Table G.1 (2/2) High Pressure System Fault Summary

SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
K480V3B1	480VAC Bux 3B1	No Power to Valves
TESFASBW	Engineered Safeguards Actuation System B	No Signals to HPI B
JXX0001X	Operator Error	System Stopped Prematurely
JPP0001R	Any Pipe Between DHT-1 and Injection Valve	Rupture
JXX0002X	Valve 59 (for isolating pumps 1A & 1C)	Left Closed After Maintenance
JMV0025V	Broken Loop Not isolated by Operator	
JSWXFERX	480V Power to Injection Valves 23F and 24 F XFER Switch	Operator Does Not XFER
JCB001AN	Motor Starter for Pump 1A	Does Not Close
JCB001CN	Motor Starter for Pump 1C	Does Not Close
JCB024FN	Motor Starter for Valve 24E	Does Not Close
JCB023FN	Motor Starter for Valve 23F	Does Not Close
JCB026FN	Motor Starter for Valve 26F	Does Not Close
JCB0073N	Motor Starter for Valve 73	Does Not Close
JCB0025N	Motor Starter for Valve 25	Does Not Close
JMV0257N	Pump Recirculation Valve 257	Does Not Close
JCB0257N	Motor Starter for Valve 257	Does Not Close
JMV0053N	Pump Recirculation Valve 53	Does Not Close
JCB0053N	Pump Recirculation Valve 53	Does Not Close
JCV0043P	Check Valve 43	Does Not Open
JCV0161P	Check Valve 161	Does Not Open



NOTES:

1. In the event of pump, to manual valves for isolate
2. Automatic start require
3. Any combination of valve



... piping rupture, access
 ... fault would be difficult.
 ... irement assumed.

- ... es left closed; MUV-70 - MUV-59
- MUV-2 - MUV-10
- MUV-2 - MUV-70
- MUV-10 - MUV-59

Figure G.2 Simplified Fault Tree - High Pressure System (For Fault Summary see Table G.1)

G.3 SYSTEM QUANTIFICATION

G.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The Crystal River HPI system is basically a two pump train system but with the following characteristics that affect the reliability of the system:

- Pump Train A employs two parallel pumps (MUP-1B, MUP-1A), while pump Train B employs a single pump (MUP-1C). One pump on pump Train A is normally operating.
- There is a crossover at the discharge side of the pumps, so that any pump can pump into any of four discharge lines. (Two out of three lines other than the break line are required for success.)
- Components are maintained only after they fail. The only maintenance contribution assessed was that due to failure of MUP-1B.
- Pump and valve testing were assumed not to alter the system unavailability.

System interfaces include AC power, DC power, and component cooling. The NSCCCS provides component cooling for the Train A pumps, while the Train B pump is cooled by the DHCCCS. Train A equipment interfaces with AC power and DC power Train A, while Train B equipment interfaces with AC and DC power Train B.

For the case where off-site power is available, the dominant contributors to HPI system unavailability are operator error. Hardware and other contributions are about an order of magnitude lower than the operator error.

For the loss of offsite power case, various hardware faults (including diesel faults) are of the same order of magnitude as operator error. The system unavailability in this case is about a factor of two higher than in the case where offsite power is available. No one hardware contributor stands out as being dominant; but the aggregate increases the system unavailability by a factor of two.

A separate fault tree was constructed for the case where the HPI is used in the "Feed and Bleed" mode. For this case the dominant failure mode is that the operator will fail to establish feed and bleed, which is about two orders of magnitude higher than the aggregate hardware related faults.

G.3.2 SYSTEM FAULT TREE QUANTIFICATION - INJECTION PHASE

This section presents the quantification of the HPI unavailability for required emergency operation during the injection phase of a postulated accident or transient. The quantitative results are presented in table form with attached notes outlining the assumptions. Modularized fault trees were constructed from the simplified fault tree presented in Section G.2 as an aid to performing the quantification and sensitivity analyses.

Table G.2 shows the HPI success requirements for various transients and LOCA sizes, Table G.3 contains top event definitions for the modularized fault trees, and Figures G.3 through G.8 show the modularized fault trees. The unavailability of each gate is shown on these trees, as well as the unavailability of the top events. Table G.4 shows the Boolean equations that represent the fault trees. Table G.5, the HPI quantification table, shows the quantification of each gate by component and failure mode. The notes for this table explain the assumptions used in the quantification. Table G.6 summarizes the point estimates for each gate.

Table G.2 High Pressure Injection Success Requirements

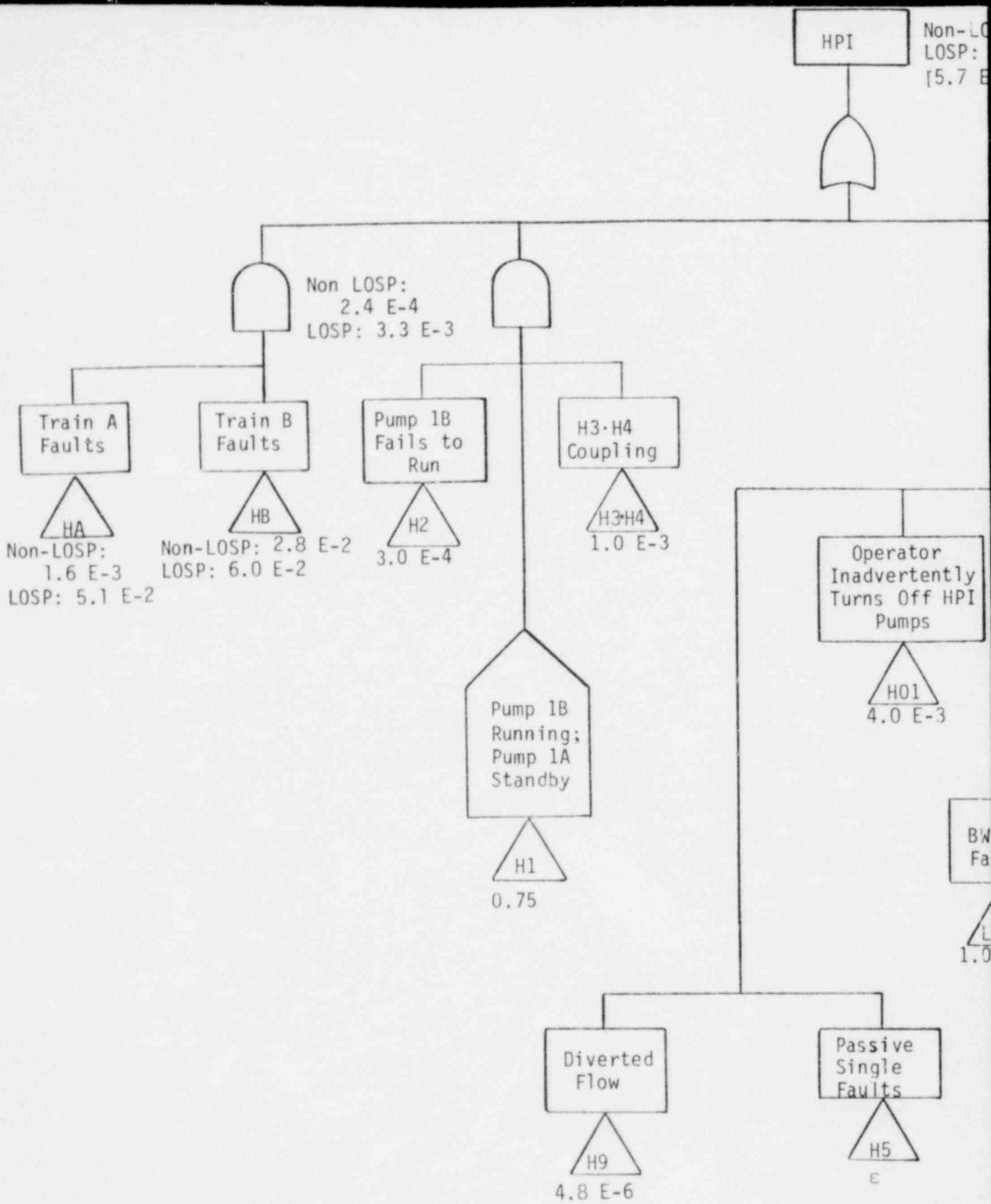
<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B3, B4-LOCA	1/3 pump flow 2/3 injection lines	1 2
Transient induced LOCA	1/3 pump flow 2/3 injection	1 2
Transient with loss of all secondary cooling	1/3 pump flow 2/4 injection lines	1 3

-
- NOTES: 1. The HPI is a two-pump train system, where Train A consists of two parallel pumps (MUP-B, MUP-A) and Train B consists of a single pump (MUP-C)
2. The HPI contains four injection lines, but the injection line feeding into the leg containing the break is assumed to be ineffective for cooling the reactor.
3. All four injection lines are presumed potentially functional in this case.

Table G.3 High Pressure Injection - Top Events

<u>INITIATOR</u>	<u>BOOLEAN REPRESENTATION</u>		
B4, B3-LOCAs; Transient induced LOCAs	HPI	High pressure injection system fails to provide one pump flow via two injection lines to cold legs	1
B4 LOCAs; Transient induced LOCAs.	HA	High pressure injection system Train A fails to provide one pump flow to injection line headers	1,2
	HB	High pressure injection system Train B fails to provide one pump flow to injection line headers	1,2
Transient with loss of all secondary cooling	HPFB	Operator fails to establish feed and bleed operation or high pressure injection system fails to provide one pump flow via two injection lines to cold legs	1
Transient with loss of all secondary cooling	HAF	High pressure injection Train A fails to provide one pump flow to injection line headers for feed and bleed	3
	HBF	High pressure injection Train B fails to provide one pump flow to injection line headers for feed and bleed	3

- NOTES:
1. Requirements for break isolation or manual initiation are reflected in fault trees or Boolean equations for the individual initiators as appropriate.
 2. HA and HB are required for modeling emergency coolant recirculation. Failure modes common to both trains are excluded from the individual train failures.
 3. These events are defined for convenience of analysis, and correspond to events HA and HB, except that some failures in these events are not contained in HAF and HBF.



Note 1: The unavailability in brackets is for the LOCA initiator

- 2: The initiating event for the tree is either a loss of offsite power or a LOCA, but not both simultaneously.

SP: 5.4 E-2
 5.8 E-2
 -2] Note 1

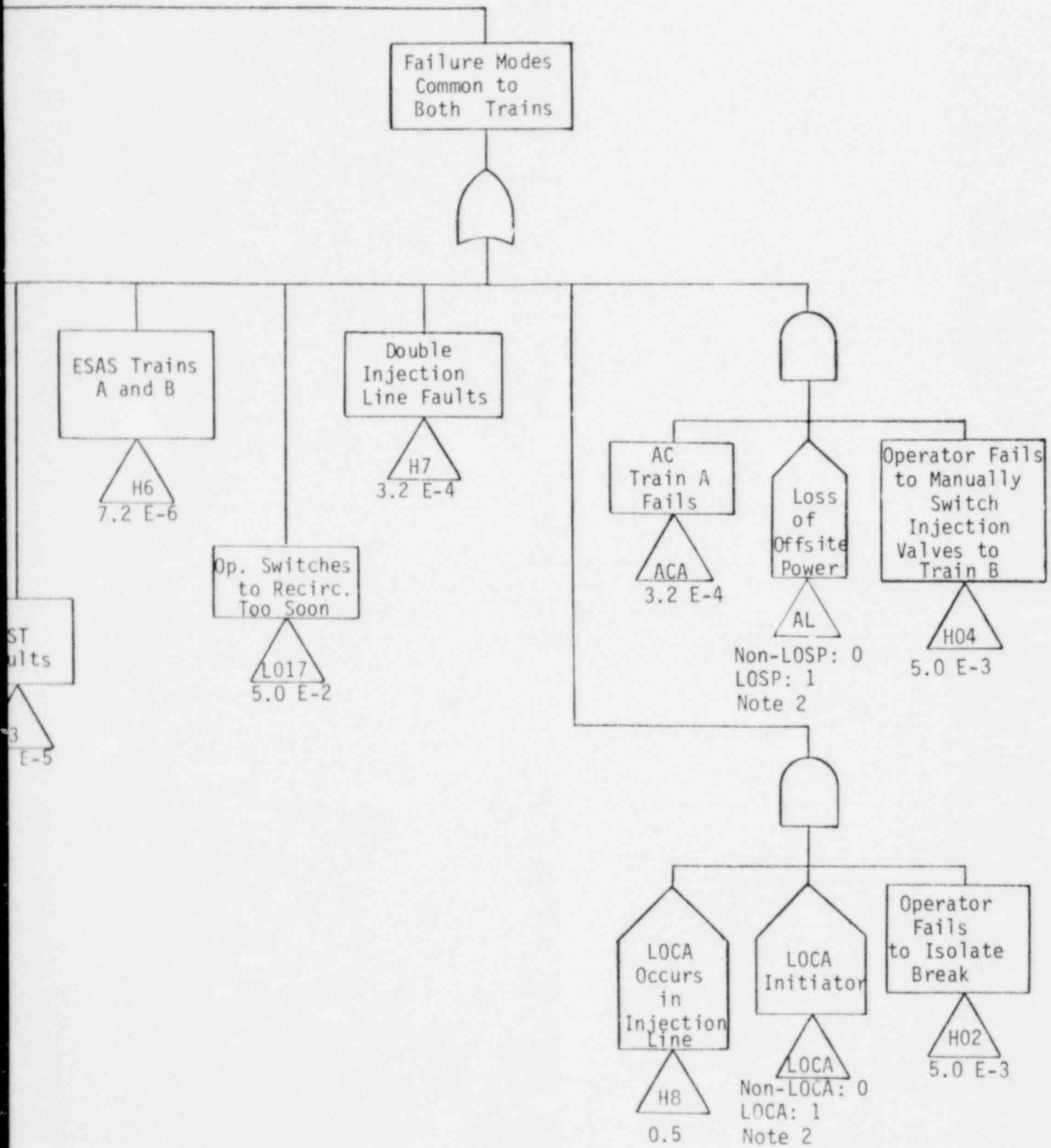


Figure G.3 Modularized Fault Tree for Event "HPI"

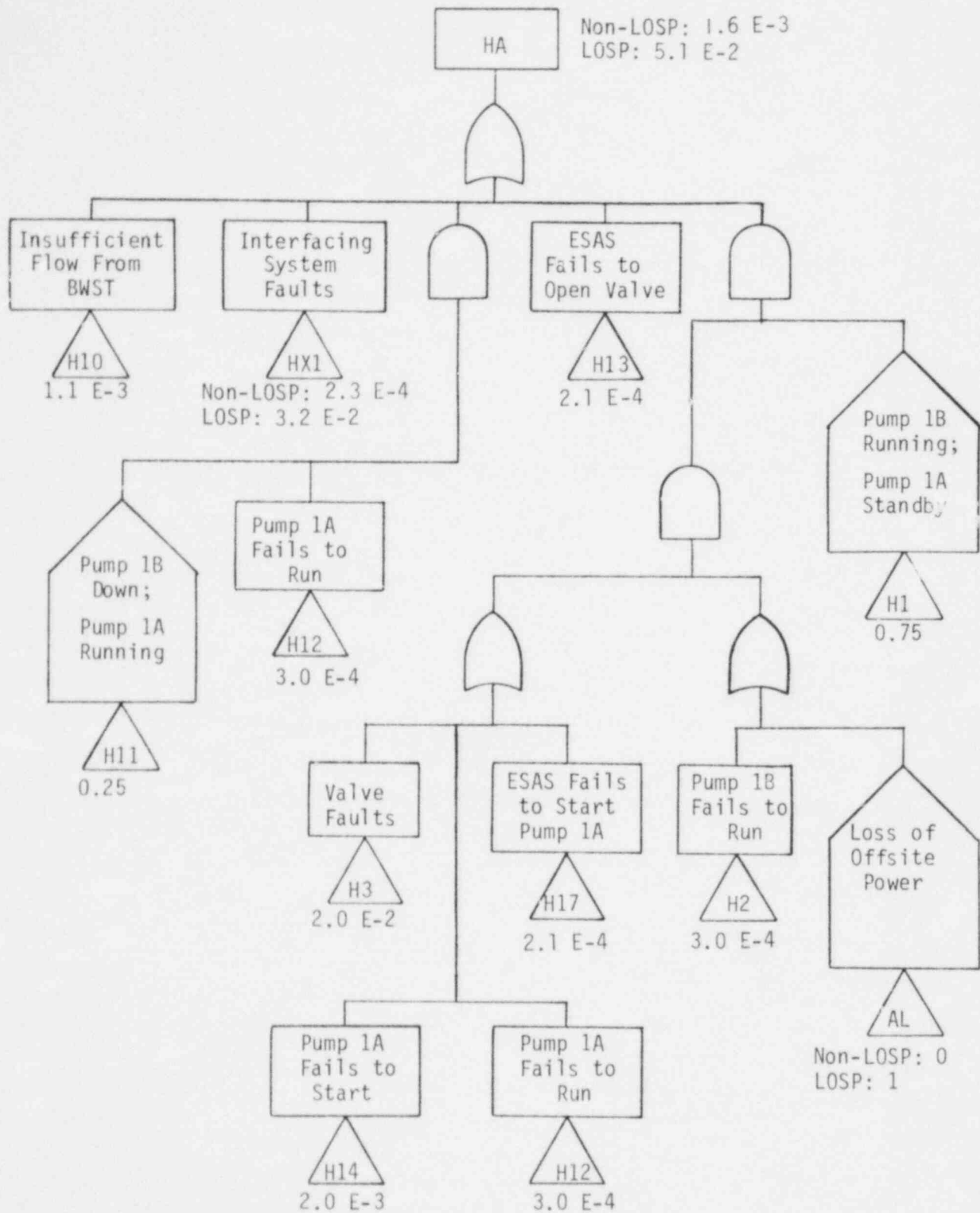


Figure G.4 Modularized Fault Tree for Event "HA"

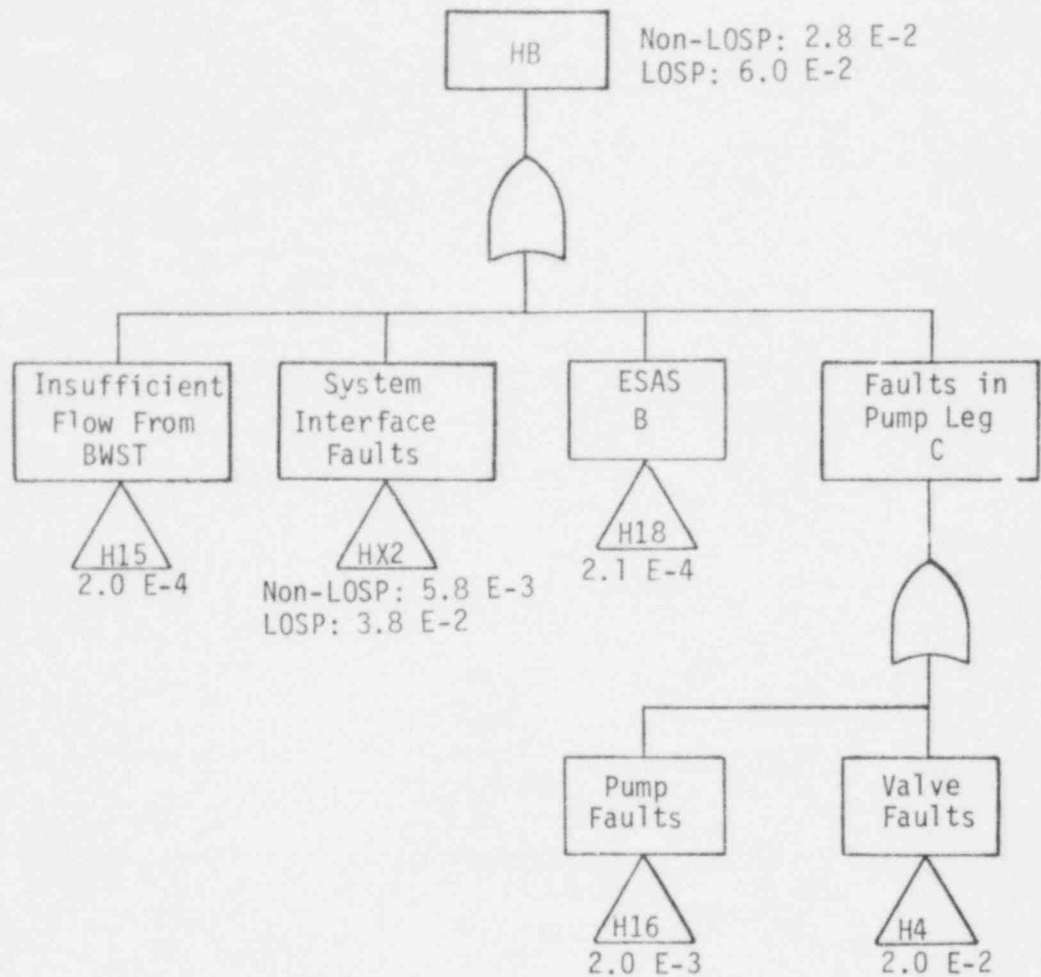


Figure G.5 Modularized Fault Tree for Event "HB"

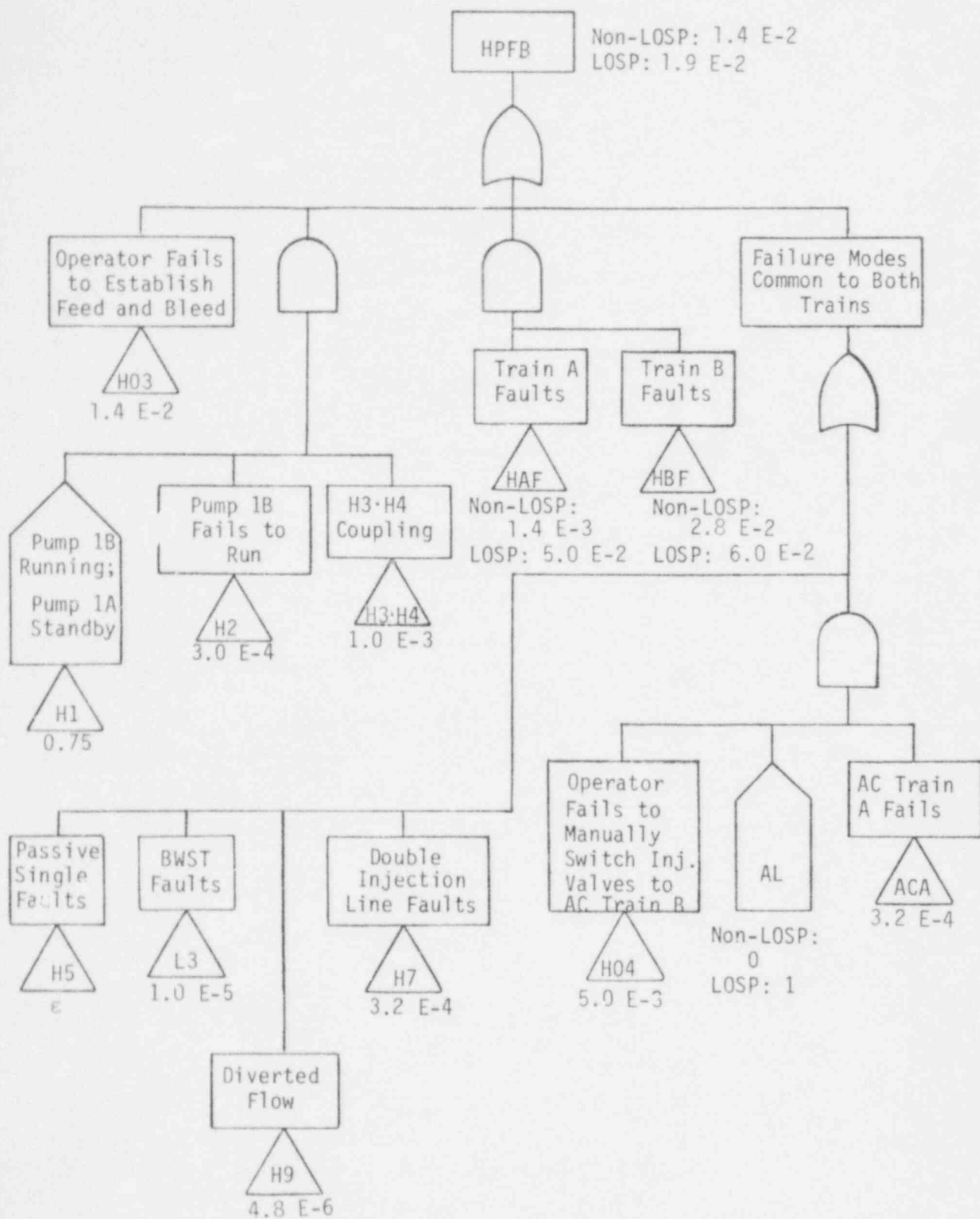


Figure G.6 Modularized Fault Tree for Event "HPFB"

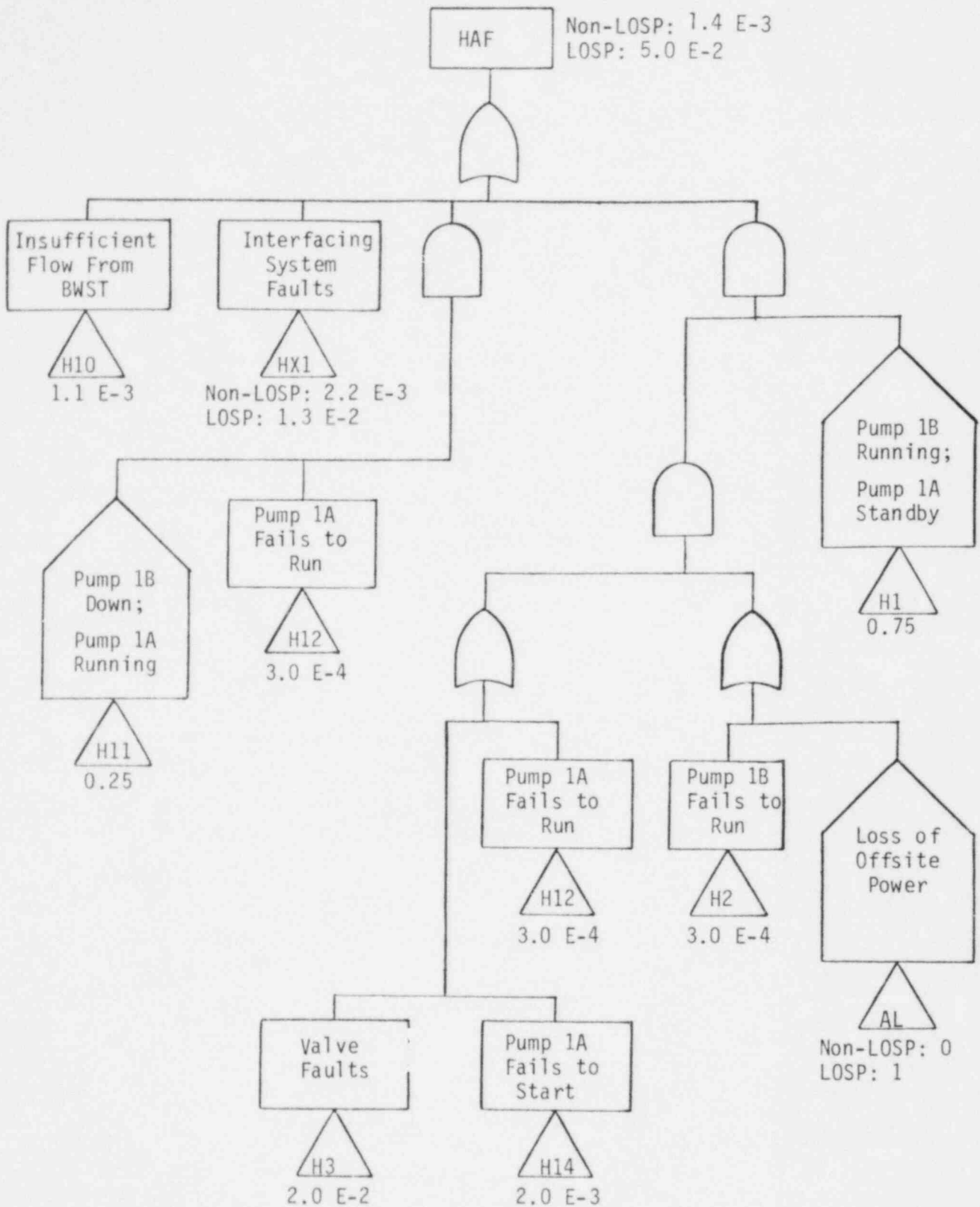


Figure G.7 Modularized Fault Tree for Event "HAF"

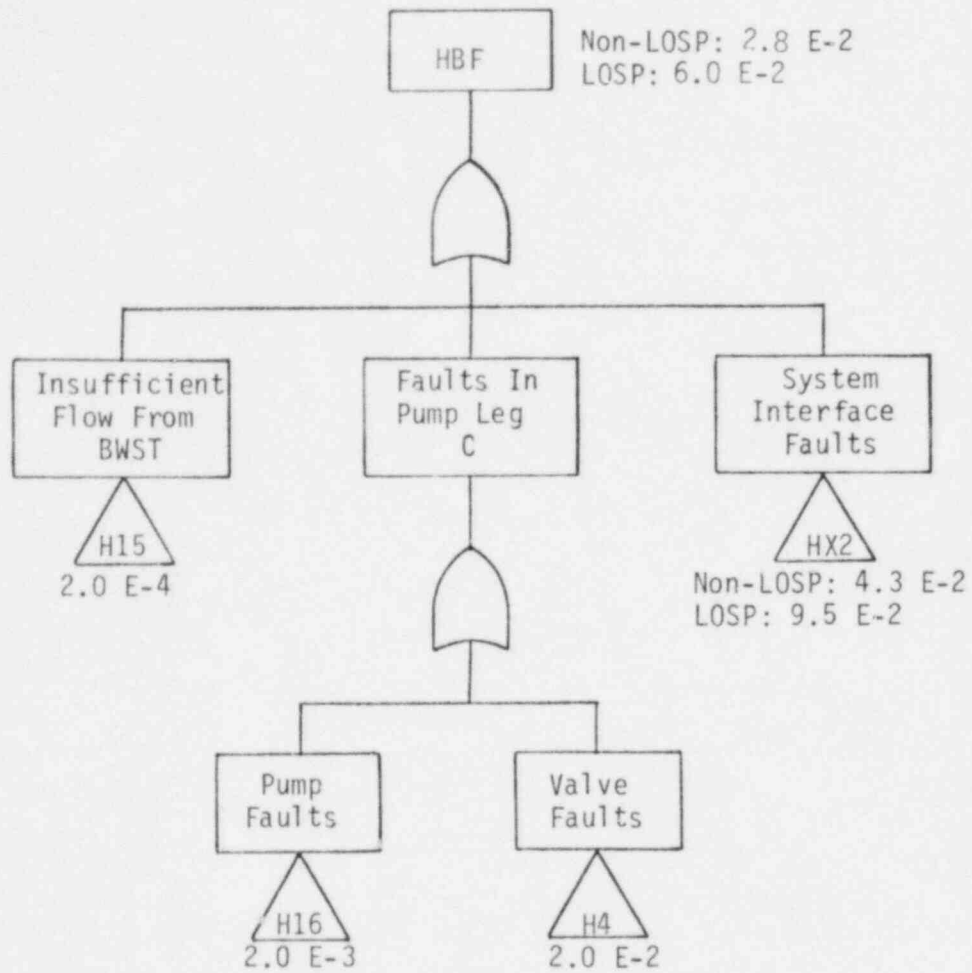


Figure G.8 Modularized Fault Tree for Event "HBF"

Table G.4 (1/2) HPI

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

NOTES

$$HPI = HA \cdot HB + H1 \cdot H2 \cdot (H3 \cdot H4) + H5 + H6 + H7 + H9 + L3 + \\ + L017 + H01 + (H02 \cdot H8) \cdot LOCA + (H04 \cdot ACA) \cdot AL$$

$$HA = HX1 + H10 + H11 \cdot H12 + H13 + H1 \cdot (AL + H2) \cdot (H3 + H12 + H17 + H14)$$

$$HB = HX2 + H4 + H15 + H16 + H18$$

INTERMEDIATE EVENTS

$$HX1 = ACA + DCA + N \quad (1)$$

$$HX2 = ACB + DCB + DB \quad (1)$$

$$HX1 \cdot HX2 = ACA \cdot ACB + ACA \cdot (D2 + D4 + DM2 + DH2) + DB [N1 + N2 (N3 + NM2) + \\ + N6 \cdot (N5 + NM4) + N4 \cdot (N5 + N7 + NM4) + NM3 \cdot (N5 + N7) + N6 \cdot N7 + \\ + N3 \cdot NM1] \quad (1)$$

BOOLEAN EQUATIONS REGROUPEU FOR REDUCTION

TOP EVENT

$$HPI = H5 + H6 + H7 + H9 + L3 + L017 + H01 + H02 \cdot H8 \cdot LOCA + (H04 \cdot ACA) \cdot AL + \\ + HX1 \cdot (H4 + H15 + H16 + H18) + ACA \cdot ACB + \\ + HX2 \cdot \{H10 + H11 \cdot H12 + H13 + H1 \cdot [AL \cdot (H3 + H12 + H17 + H14) + \\ + H2 \cdot (H12 + H17 + H14) + H2 \cdot H3]\} + (H10 + H11 \cdot H12 + H13) \cdot \\ \cdot (H4 + H15 + H16 + H18) + H1 \cdot \{(H4 + H15 + H16 + H18) \cdot \\ \cdot [AL \cdot (H3 + H12 + H17 + H14) + H2 \cdot (H12 + H17 + H14)] + \\ + H2 \cdot H3 \cdot (H15 + H16 + H18) + H2 \cdot (H3 \cdot H4)\} + \\ + ACA \cdot (D2 + D4 + DM2 + DH2) + DB [N1 + N2 \cdot (N3 + NM2) + \\ + N6 \cdot (N5 + NM4) + N4 \cdot (N5 + N7 + NM4) + NM3 \cdot (N5 + N7) + N6 \cdot N7 + N3 \cdot NM1] \quad (1)$$

Table G.4 (2/2) HPI - Feed and Bleed

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

NOTES

$$\text{HPFB} = \text{H5} + \text{H7} + \text{H9} + \text{L3} + \text{H03} + \text{H04} \cdot \text{ACA} \cdot \text{AL} + \text{H1} \cdot \text{H2} \cdot (\text{H3} \cdot \text{H4}) + \text{HAF} \cdot \text{HBF}$$

$$\text{HAF} = \text{H10} + \text{H11} \cdot \text{H12} + \text{HX1} + \text{H1} \cdot (\text{AL} + \text{H2}) \cdot (\text{H3} + \text{H12} + \text{H14})$$

$$\text{HBF} = \text{H4} + \text{H15} + \text{H16} + \text{HX2}$$

INTERMEDIATE EVENTS

$$\text{HX1} = \text{ACA} + \text{DCA} + \text{N} \tag{1}$$

$$\text{HX2} = \text{ACB} + \text{DCB} + \text{DB} \tag{1}$$

$$\begin{aligned} \text{HX1} \cdot \text{HX2} = & \text{ACA} \cdot \text{ACB} + \text{ACA} \cdot (\text{D2} + \text{D4} + \text{DM2} + \text{DH2}) + \text{DB} \left[\text{N1} + \text{N2} \cdot (\text{N3} + \text{NM2}) + \right. \\ & + \text{N6} \cdot (\text{N5} + \text{NM4}) + \text{N4} \cdot (\text{N5} + \text{N7} + \text{NM4}) + \text{NM3} \cdot (\text{N5} + \text{N7}) + \text{N6} \cdot \text{N7} + \\ & \left. \cdot \text{N3} \cdot \text{NM1} \right] \tag{1} \end{aligned}$$

BOOLEAN EQUATIONS REGROUPED FOR REDUCTION

TOP EVENT

$$\begin{aligned} \text{HPFB} = & \text{H5} + \text{H7} + \text{H9} + \text{L3} + \text{H03} + \text{H04} \cdot \text{ACA} \cdot \text{AL} + \text{HX1} \cdot (\text{H4} + \text{H15} + \text{H16}) + \\ & + \text{ACA} \cdot \text{ACB} + \text{HX2} \cdot [\text{H10} + \text{H11} \cdot \text{H12} + \text{H1} \cdot (\text{H2} + \text{AL}) \cdot (\text{H3} + \text{H12} + \text{H14})] + \\ & + (\text{H10} + \text{H11} \cdot \text{H12}) \cdot (\text{H4} + \text{H15} + \text{H16}) + \text{H1} \cdot (\text{H2} + \text{AL}) \cdot [(\text{H15} + \text{H16}) \cdot \\ & \cdot (\text{H3} + \text{H12} + \text{H14}) + \text{H4} \cdot (\text{H12} + \text{H14}) + (\text{H3} \cdot \text{H4})] + \\ & + \text{ACA} \cdot (\text{D2} + \text{D4} + \text{DM2} + \text{DH2}) + \text{DB} \left[\text{N1} + \text{N2} \cdot (\text{N3} + \text{NM2}) + \right. \\ & + \text{N6} \cdot (\text{N5} + \text{NM4}) + \text{N4} \cdot (\text{N5} + \text{N7} + \text{NM4}) + \text{NM3} \cdot (\text{N5} + \text{N7}) + \text{N6} \cdot \text{N7} + \\ & \left. \cdot \text{N3} \cdot \text{NM1} \right] \tag{1} \end{aligned}$$

NOTES: (1) See appropriate system fault tree section for definition of faults whose initial letters are D (DHCCCS) or N (NSCCCS).

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAUL. DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
H10		INSUFFICIENT FLOW FROM BWST TO TRAIN A PUMPS			1.1 E-3			
	VALVE MUV-73	N.C. VALVE FAILS TO OPEN	D		1.0 E-3	3 ⁺ , 3 ⁻		
	CHECK VALVE 72	PLUGGED	D		1.0 E-4			
					$\Sigma=1.1 E-3$			
H3		TRAIN A VALVE FAULTS			2.0 E-2	3 ⁺ , 10 ⁻		
	MANUAL VALVE 70	LEFT CLOSED	D		1.0 E-2	3 ⁺ , 10 ⁻	H	
	STOP CHECK VALVE 10	LEFT CLOSED	D		1.0 E-2	3 ⁺ , 10 ⁻	H	
	CHECK VALVE 11	PLUGGED	D		1.0 E-4	5 ⁺ , 5 ⁻		
					$\Sigma=2.0 E-2$			
H14		TRAIN A PUMP FAULTS			2.0 E-3			
	PUMP MUP-1A	FAILS TO START	D		1.0 E-3	3 ⁺ , 3 ⁻		
	CIRCUIT BKR.	FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
					$\Sigma=2.0 E-3$			
H12	PUMP MUP-1A	PUMP 1A FAILS TO RUN, GIVEN RUNNING AT ONSET OF INCIDENT	3.0 E-5	10	3.0 E-4	10 ⁺ , 10 ⁻		1
H2	PUMP MUP-1B	PUMP-1B FAILS TO RUN, GIVEN RUNNING AT ONSET OF INCIDENT	3.0 E-5	10	3.0 E-4	10 ⁺ , 10 ⁻		1
H15		INSUFFICIENT FLOW FROM BWST TO TRAIN B PUMP			2.0 E-4			
	VALVE MUV-58	N.O. VALVE FAILED CLOSED	D		1.0 E-4	3 ⁺ , 3 ⁻		
	CHECK VALVE 60	PLUGGED	D		1.0 E-4	3 ⁺ , 3 ⁻		
					$\Sigma=2.0 E-4$			
H4		TRAIN B VALVE FAULTS			2.0 E-2	3 ⁺ , 10 ⁻	H	
	MANUAL VALVE 59	LEFT CLOSED	D		1.0 E-2	3 ⁺ , 10 ⁻	H	
	STOP CHECK VALVE 2	LEFT CLOSED	D		1.0 E-2	3 ⁺ , 10 ⁻	H	
	CHECK VALVE 1	PLUGGED	D		1.0 E-4	3 ⁺ , 3 ⁻		
						$\Sigma=2.0 E-2$		

Table G.5 (1/5) Events "HA" and "HB" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
H16	PUMP MUP-1C CIRCUIT BKR.	TRAIN B PUMP FAULTS			2.0 E-3			
		FAILS TO START	D		1.0 E-3	3 ⁺ , 3 ⁻		
		FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
					$\epsilon = 2.0 E-3$			
H1		PUMP 1B RUNNING, PUMP 1A ON STANDBY AT ONSET OF INCIDENT			.75			2
H11		PUMP 1B DOWN, PUMP 1A RUNNING AT ONSET OF INCIDENT			.25			2
AL		INITIATOR IS LOSS OF OFFSITE POWER			1 OR 0			3
H5		PASSIVE SINGLE FAULTS COMMON TO BOTH TRAINS			ϵ			
L3		SINGLE BWST FAILURE*	D		1.0 E-5	2 ⁺ , 2 ⁻	B	4, 5
H8-HO2		OPERATOR FAILS TO ISOLATE BREAK IN INJECTION LINE			2.5 E-3	3 ⁺ , 10 ⁻	0	
H0	INJECTION LINE	BREAK OCCURS IN INJECTION LINE, GIVEN THAT SMALL-SMALL BREAK OCCURS			0.5			6
H02	INJECTION LINE	OPERATOR FAILS TO CLOSE VALVE	D		5.0 E-3	3 ⁺ , 10 ⁻	0	
					$\epsilon = 2.5 E-3$			
H3-H4	MANUAL VALVES 10, 70, 2, 59	2 VALVES LEFT CLOSED IN ANY OF THE COMBINATIONS: 70-59, 2-10, 70-2, 10-59	D		1.0 E-3	10 ⁺ , 10 ⁻	H	7
LOCA		LOCA GATE						
		LOCA			1			
		NON LOCA			0			
H01	OPERATOR	OPERATOR INCORRECTLY TURNS OFF PUMPS AND FAILS TO RECOVER IN TIME TO MITIGATE INCIDENT	D		4.0 E-3	10 ⁺ , 3 ⁻	0	8, 17

Table G.5 (2/5) Events "HA", "HB", and "HPI" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L017	OPERATOR	OPERATOR RECONFIGURES VALVES FOR RE-CIRCULATION TOO SOON AND LOSES SUCTION TO PUMPS	D		5.0 E-2	3 ⁺ , 10 ⁻	0	9,17
H9		DIVERSION OF FLOW VIA FAILURE TO CLOSE MVs 257 AND 53			4.8 E-6			10
	MV 257	FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
	CIRCUIT BKR 257	FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
	ESAS/MV 257	NO ESAS SIGNAL TO CLOSE VALVE (ISSI)	D		2.1 E-4	3 ⁺ , 3 ⁻		11
					<u>E=2.2 E-3</u>			
	MV 53	FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
	CIRCUIT BKR 257	FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
	ESAS/MV 53	NO ESAS SIGNAL TO CLOSE VALVE (ISSI)	D		2.1 E-4			11
					<u>E=2.2 E-3</u>			
H03		OPERATOR FAILS TO ESTABLISH FEED AND BLEED OPERATION	D		1. E-2	3 ⁺ , 10 ⁻	0	12, 17
ACA-H04		INSUFFICIENT AC POWER ON TRAIN A AND OPERATOR FAILS TO SWITCH INJECTION VALVES 23F AND 24F TO TRAIN B			3.2 E-4	3 ⁺ , 10 ⁻	0	13
ACA		AC POWER TRAIN A						
		INSUFFICIENT POWER (LOSP)			3.2 E-2			13
H04	OPERATOR	FAILS TO TRANSFER SWITCH	D		5.0 E-3	3 ⁺ , 10 ⁻	0	
					<u>E=3.2 E-4</u>			
H7		DOUBLE INJECTION LINE FAULTS			3.2 E-4			
	VALVE FAULTS	VALVE FAILURE IN 2 INJECTION LINES (FAILURE OF ANY 2 OF 3 INJECTION LINES)			3.2 E-4	2 ⁺ , 2 ⁻	B	15, 16
		INJECTION LINE A1 FAILURE						
	MV24F	FAILS TO OPEN	D		1.0 E-3	3 ⁺ , 3 ⁻		
	CIRCUIT BKR, 24F	FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
	CHECK VALVE 43	FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		

Table G.5 (3/5) Events "HPI" and "HPFB" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
	CHECK VALVE 161	FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		11
	ESAS/MV 24F	NO ESAS SIGNAL TO OPEN VALVE (ISSI)	D		2.1 E-4			
		INJECTION LINE A2 FAILURE			$\Sigma = 2.4 E-3$			
	MV 23F	FAILS TO OPEN	D		1.0 E-3			
	CIRCUIT BKR. 23F	FAILS TO CLOSE	D		1.0 E-3			
	CHECK VALVE 42	FAILS TO OPEN	D		1.0 E-4			
	CHECK VALVE 160	FAILS TO OPEN	D		1.0 E-4			
	ESAS/MV 23F	NO ESAS SIGNAL TO OPEN VALVE (ISSI)	D		2.1 E-4			11
		INJECTION LINE B2 FAILURE			$\Sigma = 2.4 E-3$			
	MV 26F	FAILS TO OPEN	D		1.0 E-3			
	CIRCUIT BKR. 26F	FAILS TO CLOSE	D		1.0 E-3			
	CHECK VALVE 37	FAILS TO OPEN	D		1.0 E-4			
	CHECK VALVE 164	FAILS TO OPEN	D		1.0 E-4			
	ESAS/MV 26F	NO ESAS SIGNAL TO OPEN VALVE (ISSI)	D		2.1 E-4			11
		INJECTION LINE B2 FAILURE			$\Sigma = 2.4 E-3$			
	MVs 23F, 24F, AND 26F	COUPLED FAILURE TO OPEN OF ANY 2 VALVES			3.0 E-4	2 ⁺ , 2 ⁻		14
H17	ESAS/MUP-1A	NO ESAS SIGNAL TO START PUMP (ISSI)			2.1 E-4			
H13	ESAS/MUV-73	NO ESAS SIGNAL TO OPEN VALVE (ISSI)			2.1 E-4			11
H18	ESAS/MUP-1C	NO ESAS SIGNAL TO START PUMP (ISSI)			2.1 E-4			11
H6		NO SIGNALS FROM ESAS-A AND ESAS-B AND FAILURE TO RECOVER	(7.2 E-4)(0.01)		7.2 E-6			11
ACA		INSUFFICIENT AC POWER - TRAIN A WITH LOSS OF OFFSITE POWER FOR OTHER INITIATORS			3.2 E-2			

Table G.5 (4/5) Events "HPPB", "HAF", "HBF", and "HPI" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ACB		INSUFFICIENT AC POWER - TRAIN B WITH LOSS OF OFFSITE POWER FOR OTHER INITIATORS			3.2 E-2 e			
ACA,ACB		INSUFFICIENT AC POWER ON BOTH TRAINS WITH LOSS OF OFFSITE POWER FOR OTHER INITIATORS			2.3 E-3 e			
DCA		INSUFFICIENT DC POWER - TRAIN A NON LOSP LOSP			e 3.2 E-3			
DCB		INSUFFICIENT DC POWER - TRAIN B NON LOSP LOSP			e 3.2 E-3			
N		NSCCCS FAILURE NON LOSP LOSP			1.3 E-4 2.8 E-3			11
DB		DHCCCS - TRAIN B FAILURE NON LOSP LOSP			5.8 E-3 3.8 E-2			11
		NSCCCS TRAIN B FAULTS						11, 18
		NSCCCS TRAIN A FAULTS						11, 18
		NSCCCS DOUBLE FAULTS						11, 18
		DHCCCS TRAIN B FAULTS						11, 18

Table G.5 (5/5) Events "HPI" and "HPFB" Quantification

Table G.5 (1/2) Quantification - HPI

- NOTES:
1. The 10 hour operation timed assumed for the injection phase is conservative for those small breaks which do not require draws on the BWST by other systems.
 2. Pump 1B is assumed to be out of service for 3 months per year. Technical Specifications do not limit the outage time.
 3. The house is 1 for Loss of Offsite Power transients, 0 for all other initiators.
 4. The BWST water level is monitored continuously and alarmed in the control room.
 5. See Table K.6.
 6. The probability of 0.5. is assumed and applied to LOCA initiators only. An opportunity for this fault would occur at each ESAS signal.
 7. This fault represents a coupled human act. The probability that any one valve would be closed is estimated to be $1E-2$. The probability that any one of the four combinations of two valves would be closed, given that one valve was closed, is estimated to be 0.1.
 8. This fault occurred at TMI. Because of new NRC regulations and increased operator awareness, the likelihood of this fault is assumed to be less now than prior to TMI.
 9. Reconfiguration for recirculation of both the high and low pressure ECCS and the reactor building spray system is considered to be a single act. Hence, the fault L017 also appears in the fault trees for the other systems.
 10. Gate H9 represents double failure of the two sub-gates shown.
 11. See appropriate system fault tree analysis section.
 12. The probability is estimated to be relatively high because (1) the operator would likely be reluctant to carry out the procedure, since in effect it requires that he create a LOCA; the ramifications of doing it unnecessarily would be serious, and (2) the procedure is relatively complex in that it involves numerous actions.

Table G.5 (2/2) Quantification - HPI

- NOTES:
13. The unavailability shown for ACA is for the loss of Offsite Power transient. The unavailability for ACA, and therefore the contribution of the double fault ACA:H04, is negligible in the case of other initiators.
 14. The probability of failure of two valves is $(1E-3)(0.1) = 1E-4$, where 0.1 is the coupling probability assumed. There are three pairs of valves, hence the total fault probability is $3(1E-4) = 3E-4$. (See also note 16.)
 15. The probability estimate for H7 is comprised of contributions for both "independent" failures and coupled failures. The independent failure contribution is estimated as $3(2.4E-3) \cdot (2.4E-3) = 1.7E-5$, where $2.4E-3$ is the failure probability of a single injection line as tabulated. The coupling contribution $3.0E-4$ is listed separately.
 16. No credit is taken for flow through the injection line affected by the initiator.
 17. This human error was evaluated using THERP tree analysis as described in NUREG/CR-1278.
 18. Faults from this system contribute to system interface faults HX1 and HX2. See Boolean equations for HPI system faults for identification of the contributing faults.

Table G.6 (1/2) HPI, HPFB - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
H10	1.1 E-3
H3	2.0 E-2
H14	2.0 E-3
H12	3.0 E-4
H2	3.0 E-4
H15	2.0 E-4
H4	2.0 E-2
H16	2.0 E-3
H1	0.75
H11	0.25
AL	0* 1**
H5	ε
L3	1.0 E-5
H3·H02	2.5 E-3
H8	0.5
H02	5.0 E-3
H3·H4	1.0 E-3
LOCA	0+ 1++
H7	3.2 E-4
ACA·H04	3.2 E-4
ACA	3.2 E-2
H04	5.0 E-3

*Offsite power available +non LOCA
 **Offsite power not available ++LOCA

Table G.6 (2/2) HPI, HPFB - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
H01	4.0 E-3
L017	5.0 E-2
H9	4.9 E-6
H03	1.4 E-2
H17	2.1 E-4
H13	2.1 E-4
H18	2.1 E-4
H6	7.2 E-6
ACA	3.2 E-2
ACB	3.2 E-2
ACA·ACB	2.3 E-3
DCA	ϵ^* 3.2 E-3**
DCB	ϵ^* 3.2 E-3**
N	1.3 E-4* 2.8 E-3**
DB	5.9 E-3* 3.8 E-2**

*Offsite power available

**Offsite power not available

G.3.3 SYSTEM FAULT TREE QUANTIFICATION - RECIRCULATION PHASE

This section presents the quantification of the High Pressure System unavailability for required emergency operation during the recirculation phase of a postulated accident or transient. The quantitative results are presented in table form with attached notes outlining the assumptions. A modularized fault tree was constructed as an aid in performing the quantification and sensitivity analysis.

Table G.7 shows the HPR success requirements for various transients and LOCA sizes, Table G.8 contains top event definitions for the modularized fault trees, and Figures G.9 and G.10 show the modularized fault trees. The unavailability of each gate is shown on this tree, as well as the unavailability of the top event. Table G.9 shows the Boolean equation that represents this fault tree. Table G.10, the HPR quantification table, shows the quantification of each gate by component and failure mode. The notes for this table explain the assumptions used in the quantification. Table G.11 summarizes the point estimates for each gate.

Table G.7 High Pressure Recirculation - Success Requirements

<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B4 LOCA	1/2	1,2,3,4
Transient induced LOCA	1/2	1,2,3,4
Transient with 1 all ry cooling	1/2	5

- NOTES: 1. The event tree structure presumes that high pressure recirculation fails if high pressure injection fails. The high pressure recirculation fault tree analysis is therefore predicated on success of the injection phase.
2. Single train failures in the injection phase are assumed not to be recovered for the recirculation phase (with one exception as indicated in Note 3). This assumption is somewhat conservative in that there may be some chance of recovery for some faults, such as manual valves left in the wrong position; however, even if credit for recovery were given, it would make very little difference in the quantification of HPR.
3. For loss of offsite power transients, single train failures due to failure of a diesel generator are assumed to be recoverable for recirculation, since there is a high probability that offsite power would be recovered (within 5-10 hours).
4. The recirculation phase analysis is based on an operating period of 24 hours following the initiating event.
5. If the "feed and bleed" operation extends into the recirculation phase, one of two trains would be required for success. However, injection failure would be the most likely cause of failure to provide makeup; primarily because of the possibility of operator faults. For this reason, high pressure recirculation was not evaluated for this set of transients.

Table G.6 High Pressure Recirculation - Top Events

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
HPR	High pressure system fails to provide at least one pump flow via two injection lines to cold legs in the recirculation phase, given HPI succeeds and the corresponding low pressure trains provide adequate suction head to the high pressure pumps.	
HA*	High pressure system Train A fails to provide at least one pump flow to injection line headers during recirculation, given success during injection and adequate suction head from the corresponding low pressure pump.	1
HB*	High pressure system Train B fails to provide one pump flow to injection line headers during recirculation, given success during injection and adequate suction head from the corresponding low pressure pump.	1

NOTES: 1. For loss of offsite power transients, injection failures due to diesel failures are assumed to be recovered for recirculation. For events HA* and HB*, diesel failures therefore do not preclude "success during injection" as specified in the top event definitions.

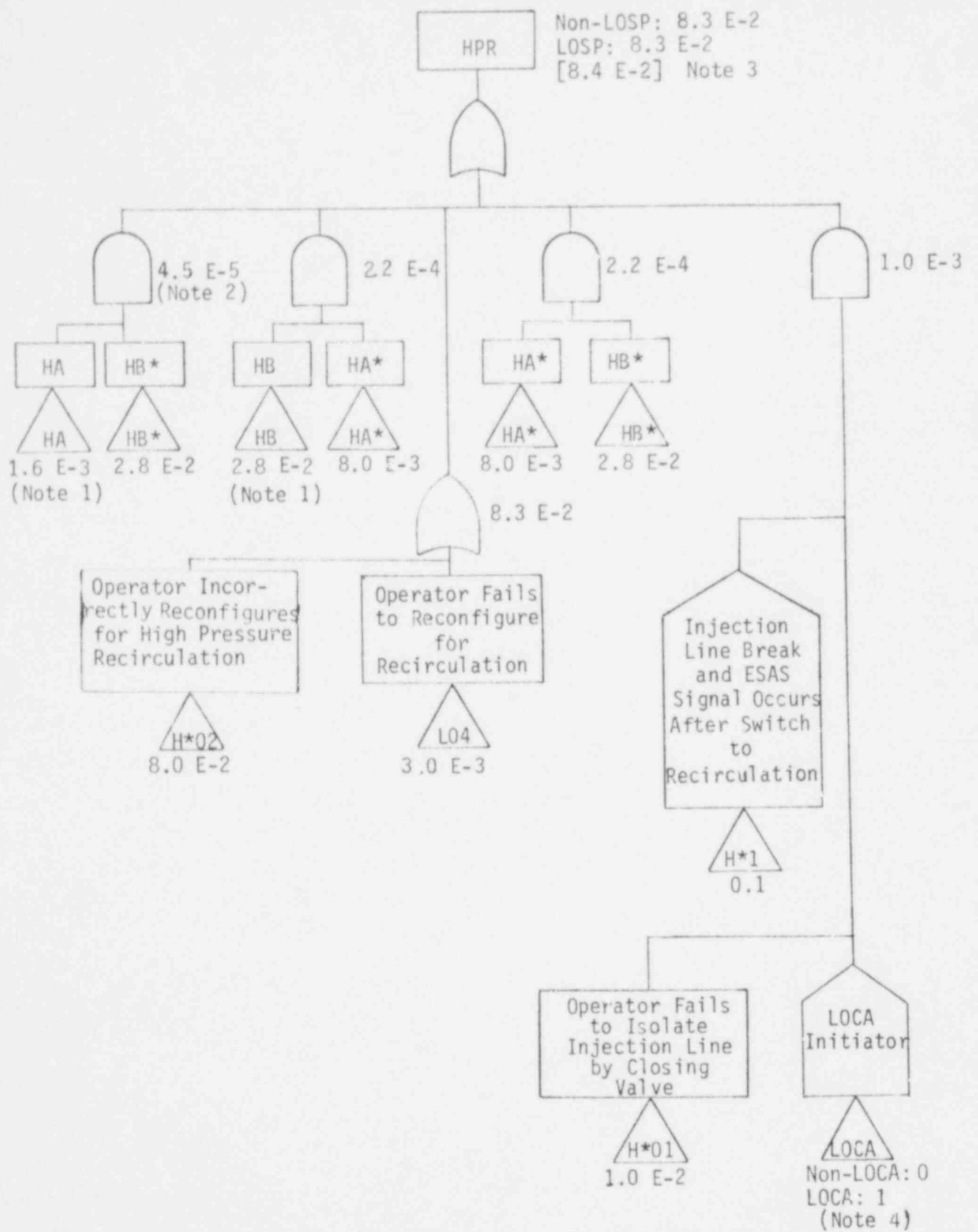


Figure G.9 Modularized Fault Tree Event "HPR"

Figure G.9 HPR Modularized Fault Tree

-
- NOTES:
1. For sequences involving loss of offsite power, offsite power is assumed to be recovered by the recirculation phase, therefore "Non-LOSP" values are used in HPR for HA and HB in all cases. (The injection phase is assumed to last about 10 hours for the B₄ LOCA.) This means that diesel failures do not contribute to system failure in the recirculation phase.
 2. See HPI fault tree quantification tables for HA and HB.
 3. The number in brackets is for the LOCA initiator.
 4. The initiating event assumed for the tree is either a loss of offsite power or a LOCA, but not both simultaneously. A transient induced LOCA is treated as a transient event.

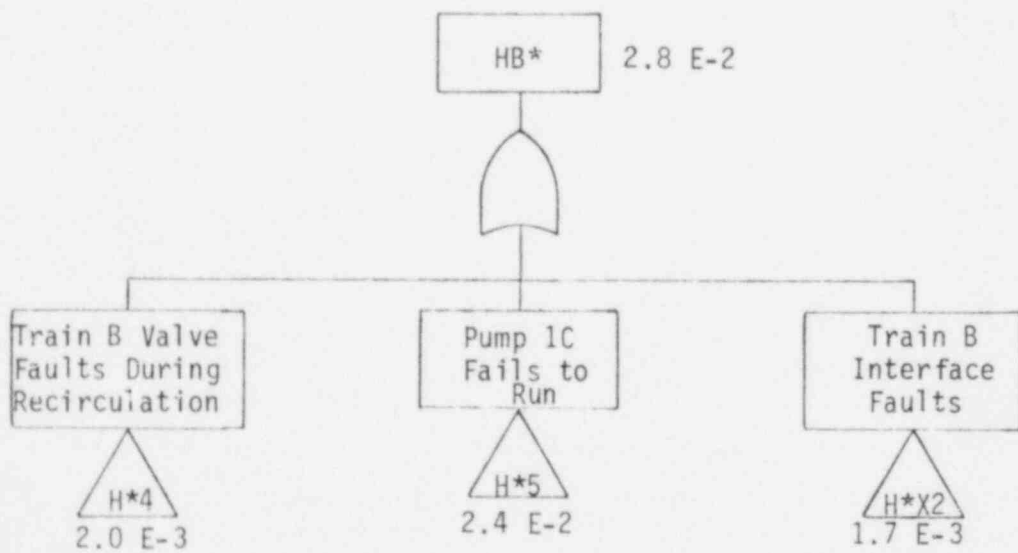
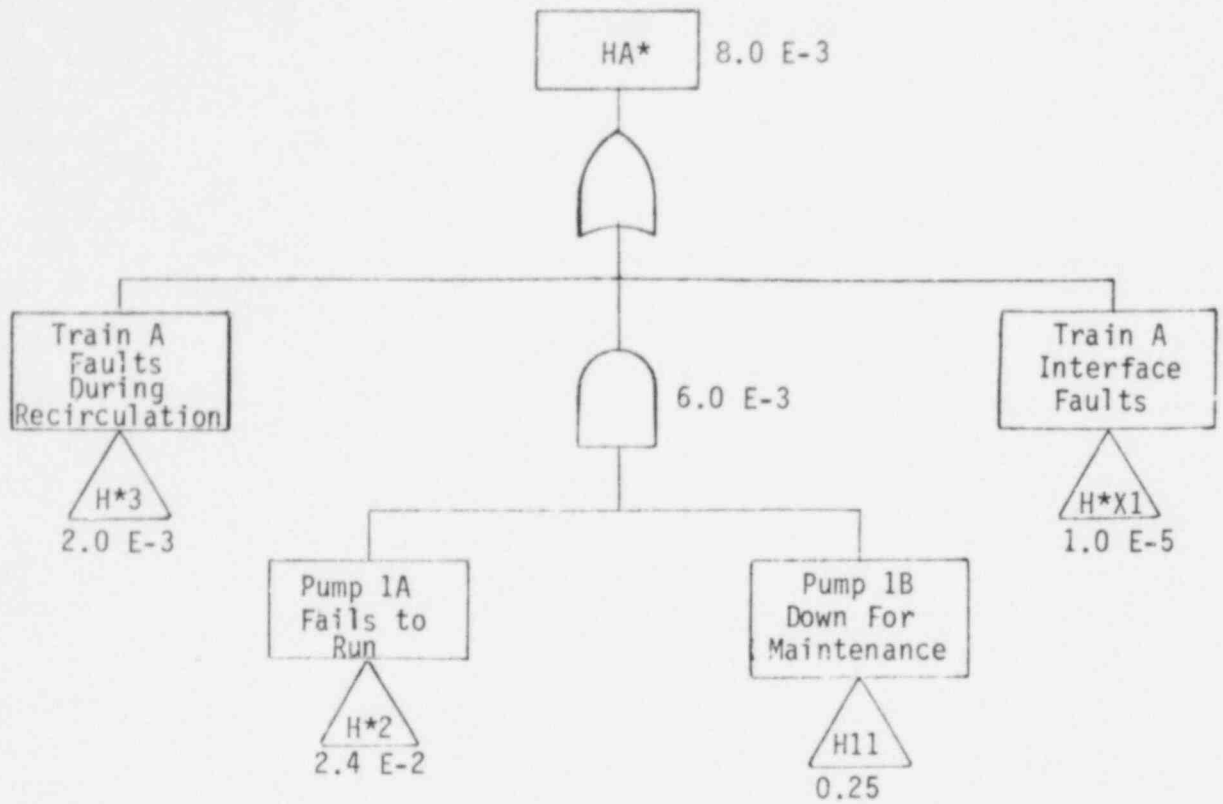


Figure G.10 Modularized Fault Trees for Events "HA*" and "HB*"

Table G.9 HPR

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENT

NOTES

$$HPR = LO4 + (LOCA \cdot H^{*1} \cdot H^{*01}) + HA \cdot HB^{*} + HB \cdot HA^{*} + HA^{*} \cdot HB^{*} + H^{*02}$$

$$HA^{*} = H^{*3} + H^{*2} \cdot H^{11} + H^{*X1}$$

$$HB^{*} = H^{*4} + H^{*5} + H^{*X2}$$

HA = see HPI Boolean equations

HB = " " " "

INTERMEDIATE EVENTS

$$H^{*X1} = ACA^{*} + DCA^{*} + N^{*}$$

1

$$H^{*X2} = ACB^{*} + DCB^{*} + DB^{*}$$

1

NOTES: 1. Offsite power is assessed to be recovered when entering the recirculation phase. The unavailability of AC power with offsite power available was calculated to be negligible compared to other system failure modes.

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
H*3	VALVE DHV 11 CIRCUIT BKR 11	TRAIN A VALVE FAULTS			2.0 E-3			
		FAILS TO OPEN	D		1.0 E-3	3 ⁺ , 3 ⁻		
		FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
					$\Sigma=2.0$ E-3			
H*2		PUMP 1A FAILS TO RUN	1.0 E-3	24	2.4 E-2	1 ⁺ , 30 ⁻	S	5, 1
H*4	VALVE DHV 12 CIRCUIT BKR. 12	TRAIN B VALVE FAULTS			2.0 E-3			
		FAILS TO OPEN	D		1.0 E-3	3 ⁺ , 3 ⁻		
		FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
					$\Sigma=2.0$ E-3			
H*5		PUMP 1C FAILS TO RUN	1.0 E-3	24	2.4 E-2	1 ⁺ , 30 ⁻	S	5, 1
H11		PUMP 1B DOWN, PUMP 1A RUNNING AT ONSET OF INCIDENT			0.25			2
H*X1		TRAIN A INTERFACING SYSTEM FAULTS			1.0 E-5			
DCA*		DC POWER, TRAIN A FAULTS			ϵ			
ACA*		AC POWER, TRAIN A FAULTS			ϵ			
N*		FAILURE OF NUCLEAR SERVICES CLOSED CYCLE COOLING SYSTEM (NSCCCS) DURING RECIRCULATION			1.0 E-5			
H*X2		TRAIN B INTERFACING SYSTEM FAULTS			1.7 E-3			
DCB*		DC POWER, TRAIN B FAULTS			ϵ			
ACB*		AC POWER, TRAIN B FAULTS			ϵ			
DB*		FAILURE OF DECAY HEAT CLOSED CYCLE COOLING SYSTEM (DHCCCS), TRAIN B			1.7 E-3			
HA		SEE HPI FAULT TREE ANALYSIS			1.6 E-3			6
HB		SEE HPI FAULT TREE ANALYSIS			2.8 E-2			6
L04		OPERATOR FAILS TO RECONFIGURE FOR RECIRCULATION	D		3.0 E-3	10 ⁺ , 3 ⁻	0	3
H*02		OPERATOR INCORRECTLY RECONFIGURES FOR HIGH PRESSURE RECIRCULATION	D		8.0 E-2	10 ⁺ , 10 ⁻	0	7

Table G.10 (1/2) Events "HPR", "HA*", and "HB*" Quantification

Table G.10 (2/2) Event "HPR" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
H*1-H*01	INJECTION LINE (H*1)	OPERATOR FAILS TO ISOLATE BREAK IN INJECTION LINE			1.0 E-3	3 ⁺ , 10 ⁻	0	4
		BREAK OCCURS IN INJECTION LINE, GIVEN THAT SMALL BREAK OCCURS. ESPAS SIGNAL OCCURS AFTER RECONFIGURATION FOR RECIRCULATION FAILS TO CLOSE VALVES			0.1			
LOCA	OPERATOR (H*01)	FAILS TO CLOSE VALVE	D		1.0 E-2	3 ⁺ , 10 ⁻	0	
					<u>1.0 E-2</u>			
					<u>=1.0 E-3</u>			
		LOCA GATE			1			
		LOCA			0			
		NON LOCA						

Table G.10 HPR - Quantification Table

NOTES

- 1 The 24 hour run time for pumps during the recirculation phase represents an estimated nominal time after which corrective action could be assumed to mitigate failures that would prevent success during recirculation. This assumption corresponds to a similar assumption made in WASH 1400.
- 2 Pump 1B is assumed to be out of service for 3 months per year. Technical Specifications do not limit the outage time. It was conservatively assumed that the pump is not restored by the time recirculation is required.
- 3 This fault is assumed to be the same fault as a similar operator error that appears in the evaluation of the low head recirculation system.
- 4 The existence of this fault will depend upon whether or not an ESFAS signal (e.g., 500 psi primary pressure) is received after configuration for recirculation. This will depend on LOCA size within the smallest LOCA (B4) category. The assumed probability takes this into account. The fault applies to LOCA initiators only.
- 5 During recirculation, the high pressure pumps are required to pass sump water, which may contain concrete dust and other particulate matter. There is some question concerning the ability of the pumps to operate for extended periods of time in this environment, therefore the pump failure rate for extreme environments was used for the recirculation phase.
- 6 "Non-LOSP" values are used in HPR for HA and HB in all cases. For loss of offsite power transients, injection failures due to diesel failures are assumed to be recovered for recirculation. For events HA* and HB*, diesel failures therefore do not preclude "success during injection" as specified in the top event definitions.
- 7 This human error was evaluated using THERP tree analysis as described in NUREG/CR-1278.

Table G.11 HPR - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
H*3	2.0 E-3
H*2	2.4 E-2
H*4	2.0 E-3
H*5	2.4 E-2
H11	0.25
H*X1	1.0 E-5
DCA*	ε
ACA*	ε
N*	1.0 E-5
H*X2	1.7 E-3
DCB*	ε
ACB*	ε
DB*	1.7 E-3
HA	1.6 E-3
HB	2.8 E-2
L04	3.0 E-3
H*1	0.1
H*01	1.0 E-2
H*02	8.0 E-2
LOCA	0* 1**

*non LOCA
 **LOCA

APPENDIX H
CORE FLOOD SYSTEM (CFS)

H.1 SYSTEM DESCRIPTION AND OPERATION

The core flood system is a passive engineered safeguards system which stores a supply of borated water which will automatically flow into the reactor vessel following a loss-of-coolant accident (LOCA). Although intended primarily to provide rapid core reflooding following a large LOCA, the tank contents will be injected into the reactor vessel any time the reactor coolant pressure drops below 600 psig. The CFS is required to operate only during the injection phase of accidents.

H.1.1 SYSTEM DESCRIPTION

The core flood system is depicted in the simplified schematic, Figure H.1. Each subsystem consists of a core flood tank containing at least 7626 gallons of borated water pressurized by 600 psig nitrogen, and three valves in the injection line path to the reactor vessel (RV). Instrumentation and alarms monitor tank pressure and level, and a relief valve provides overpressure protection. Each injection line path to the RV contains a normally open motor-operated valve (MOV) and two in-line check valves in series.

H.1.2 SYSTEM OPERATION

The core flood system is not dependent on any other system and requires no operator or control action to actuate. Since the core flood tank isolation MOV is normally open, the two check valves serve to prevent the high pressure reactor coolant from entering the core flooding tanks. Under a LOCA condition, these check valves open automatically when the reactor coolant system pressure drops below the 600 psig nitrogen pressure held in the tanks. To ensure that the MOV remains open, limit switches monitor the position of the MOV with annunciation in the main control room. Additionally, the circuit breaker for the MOV motor control center is locked open. During operation, level and pressure are maintained when required by makeup from the High Pressure Injection System and nitrogen supply. Sample lines are provided to verify boron concentration periodically.

The following are general comments on limiting conditions for operation regarding the core flood system. For a more complete description refer to Section 3/4.5 of the Technical Specifications.

Each reactor coolant system core flooding tank must be operable with:

- the isolation valve open,
- a contained borated water volume between 7626 and 8005 gallons of borated water,
- between 2270 and 3500 ppm of boron, and,
- a nitrogen cover-pressure of between 575 and 625 psig.

The Technical Specifications require that if either a core flood tank is inoperable or the MOV closes, restoration must occur within 1 hour or go to a Hot Shutdown condition within the next 12 hours.

Surveillance requirements for the core flood system components include the following:

- Every 8 hours tank level and pressure as well as correct MOV position are verified.
- Every 31 days a sample is taken from the tanks to verify boron concentration.
- Every 31 days it is ensured that no power is available to the valve actuator by verifying the associated breaker is locked open.
- Every 18 months (prior to shutdown for refueling) the core flood "Isolation Valve Closed" alarm is verified to annunciate when the MOV is not fully open. During this same period as plant cooldown continues and reactor coolant pressure drops, the in-line check valves are verified to actuate by observing pressurizer level and core flood tank level.

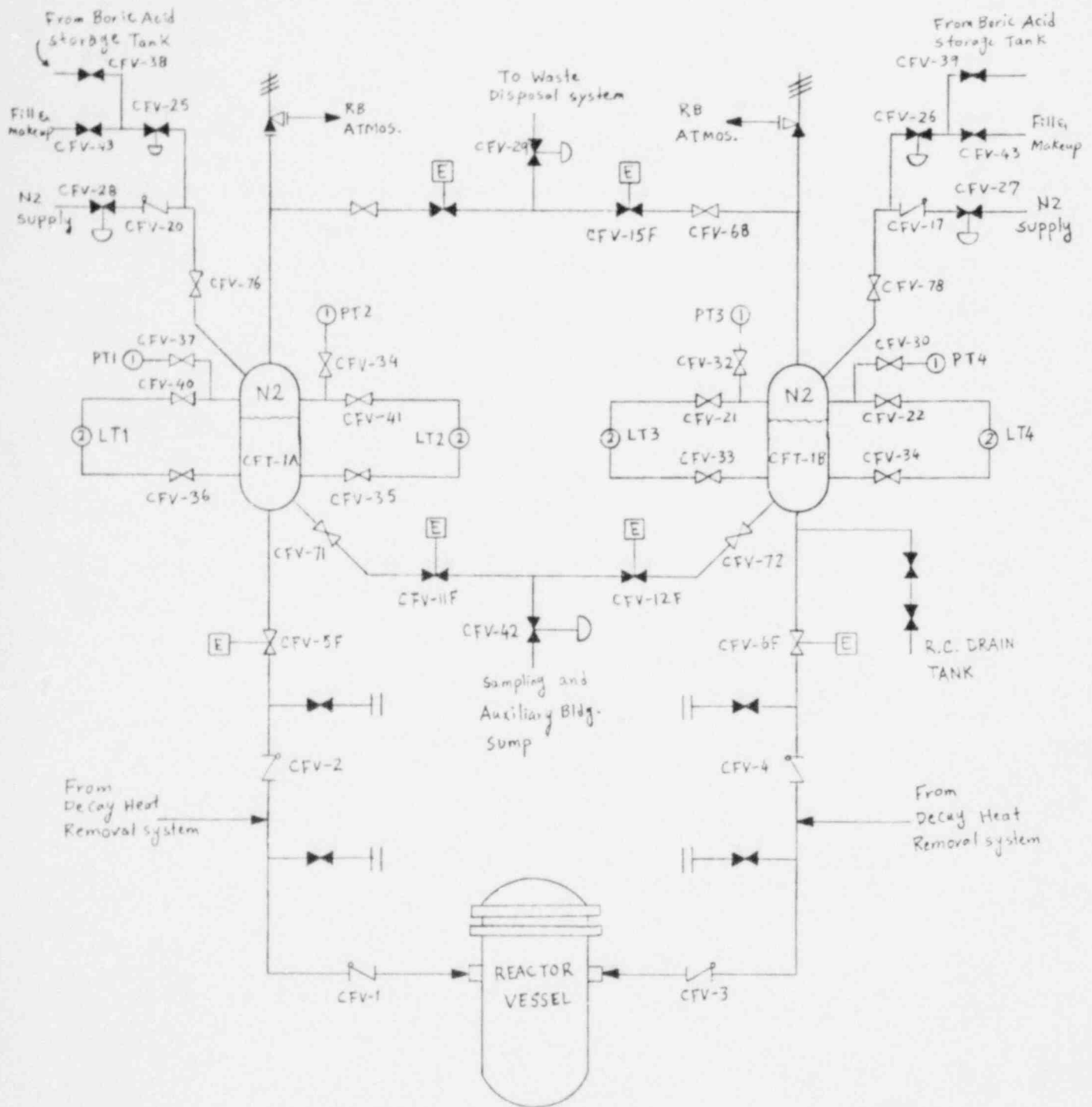


Figure H.1 Core Flood System Schematic Diagram

H.2 SYSTEM SIMPLIFIED FAULT TREE

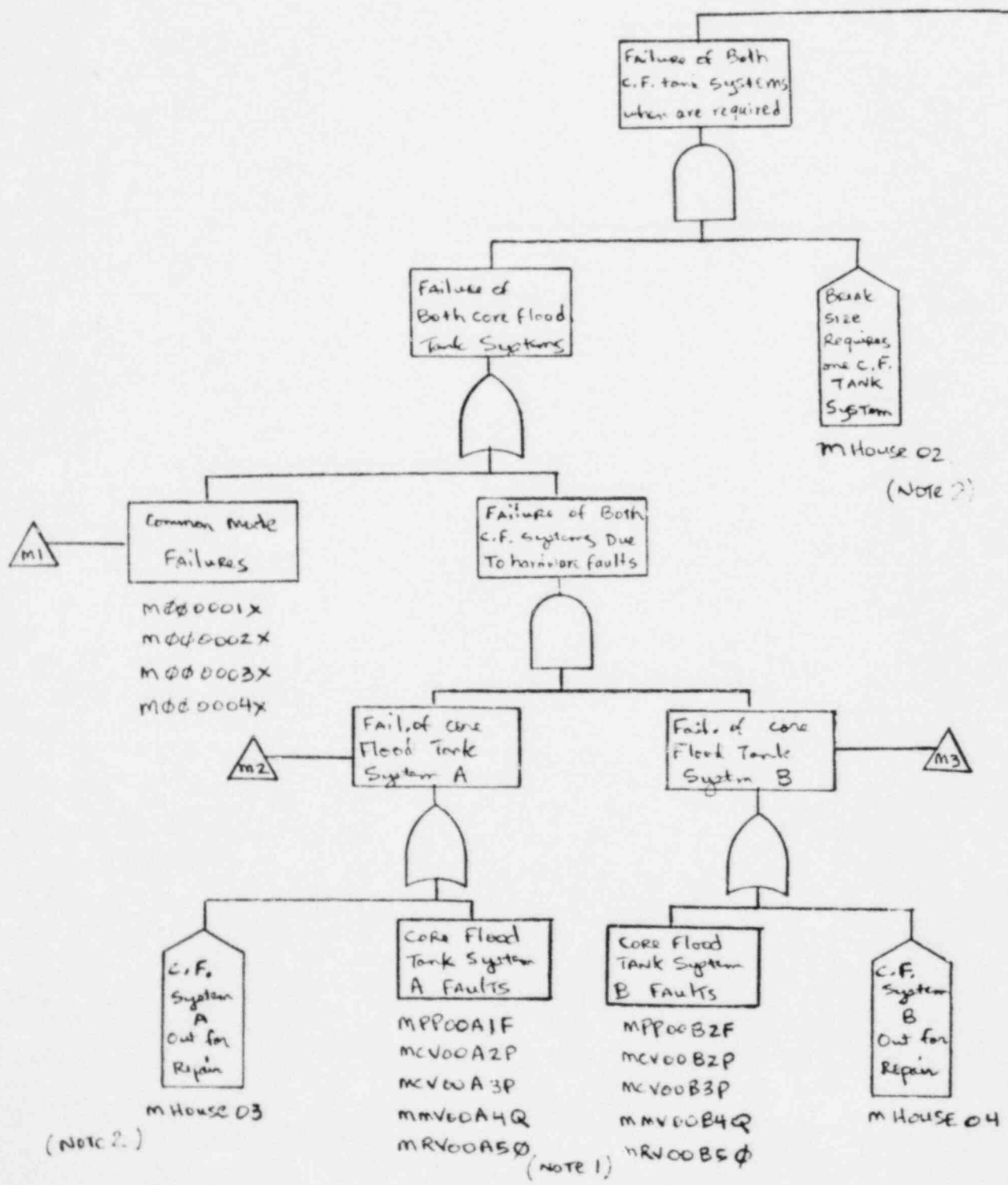
The FSAR Section 14 indicates that both core flood systems are required for a large LOCA. However, the fault tree is drawn with house events in order to be representative whenever one or both systems are required. Loss of one core flood system is represented by single faults associated with pipe ruptures, check valves failing to open, MOV plugging, and inadvertent actuation of the core flood tank relief valve. As noted on the fault tree, inadvertent opening of the relief valve with failure to reset would be immediately detectable by the associated tank level and pressure instrument alarms. Common mode failures were considered for operator error during initial fill and pressurization of the tanks as well as incorrect boron concentration. The first two should be considered unlikely since instrumentation monitors tank level and pressure. However, an additional common mode event was considered for miscalibration of this instrumentation by maintenance personnel which could result in insufficient volume or pressure.

Figure H.2 shows the simplified fault tree for the CFS.

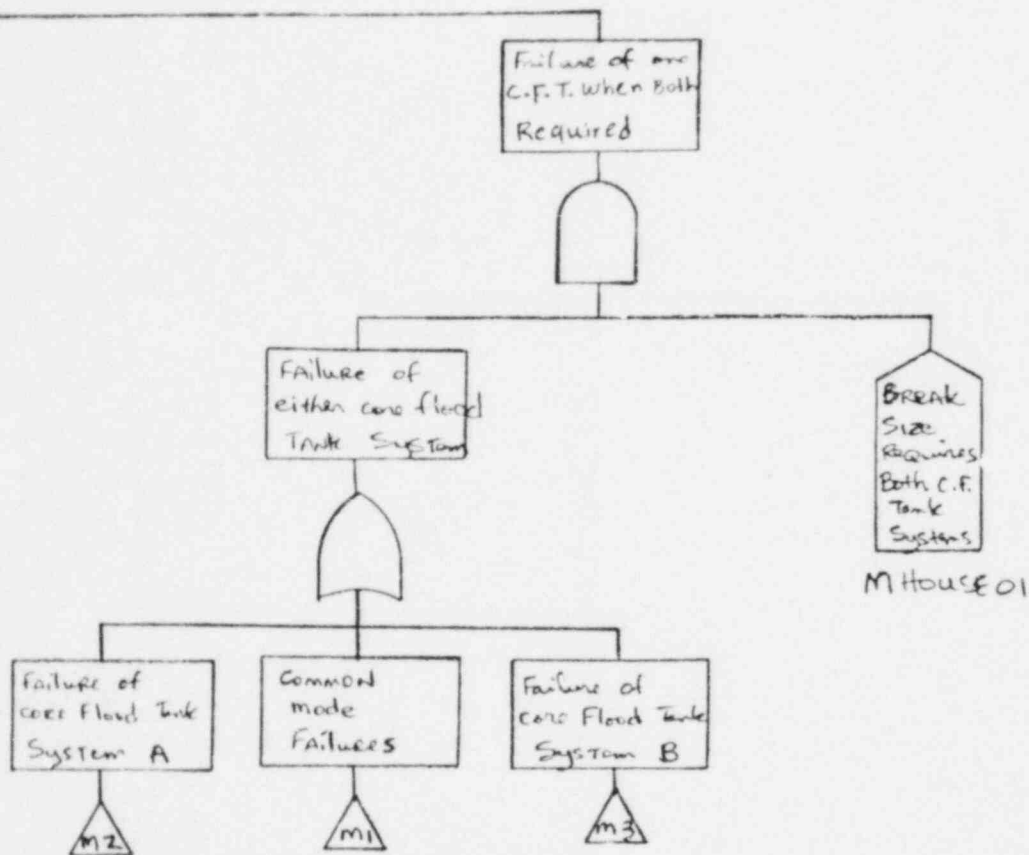
Table H.1 Core Flood System Fault Summary

SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
M000001X	Insufficient BORON concentration in Core Flood Tanks	Operator Error (Omission)
M000002X	Insufficient Water Volume in Core Flood Tanks	Operator Error (Omission)
M000003X	Insufficient Nitrogen Pressure in Core Flood Tanks	Operator Error (Omission)
MP000A1F	Piping Between CFV-1 and RV	Rupture
MCV00A2P	Check Valve CFV-1	Does Not Open
MCV00A3P	Check Valve CFV-2	Does Not Open
MMV00A4Q	Motor Operated Valve CFV-5F	Does Not Remain Open (Plug)
MRV00A5Q	Relief Valve CFV-24F	Does Not Remain Closed
MPP00B1F	Piping Between CFV-3 and RV	Rupture
MCV00B2P	Check Valve CFV-3	Does Not Open
MCV00B3P	Check Valve CFV-4	Does Not Open
MMV00B4A	Motor Operated Valve CFV-6F	Does Not Remain Open (Plug)
MRV00B5Q	Relief Valve CFV-23F	Does Not Remain Closed
M000004X	Miscalibration of Level and Pressure Instrumentation	Operator Error (Commission)

Core systems perform required



Flood
Fails To
ITS
Function



- NOTES:
1. Relief valve opening inadvertently would be immediately detected.
 2. Only M House 01 or 02 will be on at one time. Similarly M House 03 or 04 will not be on concurrently. One system can be out for 1 hr for repair before going to hot shutdown.

Figure H.2 Simplified Fault Tree - Core Flood System (For Fault Summary see table H.1)

H3 SYSTEM QUANTIFICATION

H.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The CFS is a double train system, but the success requirements depend on the size LOCA and operation of other systems (see Table H.2). For accidents where CFS is required, both trains are required to function, except in the case where the break occurs in one of the core flood lines downstream of the check valve; in this case the other core flood train is required to function. Thus, failure of either train will, in general, result in system failure. The system is entirely independent of other system interfaces, as no AC power or component cooling are required. Thus, the system unavailability is dependent only on check valves opening, and a small maintenance outage contribution.

H.3.2 SYSTEM FAULT TREE QUANTIFICATION

This section presents the quantification of the CFS unavailability for required emergency operation. A modularized fault tree was constructed from the simplified fault tree to show CFS unavailability in terms of major gates, each gate consisting of collections of component failures or outages. Table H.2 shows the CFS success requirements, Table H.3 contains the top event definitions for the modularized fault tree, and Figure H.3 shows the modularized fault tree with the unavailability of each gate and the top event. Table H.4 shows the Boolean equation that represents the fault tree. Table H.5, the quantification table, shows the quantification of each gate, and the attached notes explain the assumptions used in the quantification. Table H.6 summarizes the point estimates for each gate.

Table H.2 Core Flood System — Success Requirements

<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B ₄	Not required	
B ₃	Not required	
B ₂	2/2 tanks	1
	0/2 tanks	2
	1/1 tanks	3
B ₁	2/2 tanks	

- NOTES:
1. 2/2 core flood tanks (CFT) are required if only 1/2 LPI trains are operable.
 2. CFT are not required if both LPI trains are operable.
 3. If the break occurs in the core flood line the remaining CFT and the associated LPI train (one one HPI train) are required for success. This case was not analyzed.

Table H.3 Core Flood System — Top Events

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
CA	Failure of core flood tank A to deliver contents to reactor vessel at 600 psi reactor coolant pressure	1
CB	Failure of core flood tank B to deliver contents to reactor vessel at 600 psi reactor coolant pressure	1
CFS	Failure of either core flood tank to deliver contents to reactor vessel at 600 psi reactor coolant pressure.	2

- NOTES: 1. This top event is defined as a convenience to facilitate the quantification of CFS
2. For the cases analyzed either both core flood tanks are required (B_1 -LOCA and B_2 -LOCA where one LPI-train is inoperable) or no core flood tanks are required (B_3 -LOCA with both LPI-trains operating).

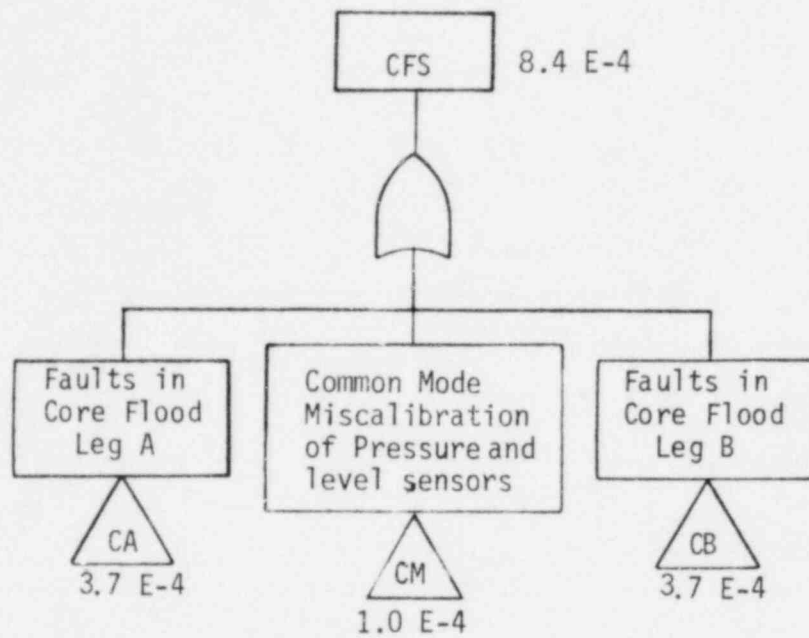


Figure H.3 Modularized Fault Tree for Event "CFS"

Table H.4 Core Flood System

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREE

TOP EVENT

$$CFS = CA + CB + CM$$

Table H.5 Events "CA" and "CB" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
CA	OPERATOR	FAULTS THAT FAIL TRAIN A						1
	OPERATOR	INSUFFICIENT BORON CONCENTRATION						2
	OPERATOR	INSUFFICIENT WATER LEVEL IN CORE FLOOD TANK A	D					2
	CFV-1 CHECK VALVE	INSUFFICIENT NITROGEN PRESSURE IN CORE FLOOD TANK A	D		1.0 E-4	3 ⁺ , 3 ⁻		
	CFV-2 CHECK VALVE	DOES NOT OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
	CFV-5F 10V	DOES NOT REMAIN OPEN (PLUGGED)	D		1.0 E-4	3 ⁺ , 3 ⁻		3
	CFV-24F	DOES NOT REMAIN CLOSED	1.0 E-5	4	4.0 E-5	3 ⁺ , 3 ⁻		4
	MAINTENANCE	TRAIN A MAINTENANCE	.03/720	1	2.8 E-5	3 ⁺ , 3 ⁻		5
					$\Sigma = 3.7 E-4$			
	CB	OPERATOR	FAULTS THAT FAIL TRAIN B					
OPERATOR		INSUFFICIENT BORON CONCENTRATION						2
OPERATOR		INSUFFICIENT WATER LEVEL IN CORE FLOOD TANK B	D					2
OPERATOR		INSUFFICIENT NITROGEN PRESSURE IN CORE FLOOD TANK B	D					
CFV-3 CHECK VALVE		DOES NOT OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
CFV-4 CHECK VALVE		DOES NOT OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
CFV-5F 10V		DOES NOT REMAIN OPEN (PLUGGED)	D		1.0 E-4	3 ⁺ , 3 ⁻		
CFV-23 F		DOES NOT REMAIN CLOSED	1.0 E-5	4	4.0 E-5	3 ⁺ , 3 ⁻		3
MAINTENANCE		TRAIN B MAINTENANCE	.02/720	1	2.8 E-5	3 ⁺ , 3 ⁻		4
OPERATOR		MISCALIBRATION OF TANK B PRESSURE AND LEVEL SENSORS			1.0 E-4	10 ⁺ , 10 ⁻		H

Table H.5 Core Flood System

QUANTIFICATION TABLES

NOTES

- 1 This fault would not fail the core flood tank function of cooling the core in the initial state of the accident since boron concentration is available from the BWST through the low pressure system. This fault was not further developed.
- 2 This parameter is maintained in the control room. Therefore, this fault was assumed to be a low probability event.
- 3 Tank pressure and level are verified every 8 hours via SP-300. Therefore, the fault duration time is 1/2 of 8 (=4) hours.
- 4 One CFT is allowed out of service for 1 hour before requirement to go to hot shutdown. Maintenance contribution was assessed assuming a frequency of 0.02 acts/month times 1/720 hr likelihood that the accident would occur during the outage.

Table H.6 Core Flood System - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
CA	3.7 E-4
CB	3.7 E-4
CM	1.0 E-4

APPENDIX K

LOW PRESSURE INJECTION AND RECIRCULATION SYSTEM

APPENDIX K. LOW PRESSURE INJECTION AND RECIRCULATION SYSTEM

K.1 SYSTEM DESCRIPTION AND OPERATION

Low pressure injection and recirculation, is an emergency function of the Decay Heat Removal System (DHRS). The Decay Heat Removal System (DHRS) provides both residual heat removal and emergency core cooling functions. This analysis deals only with failure of the emergency functions of the Decay Heat Removal System. Because the DHRS provides both low pressure coolant injection (LPI) and low pressure coolant recirculation (LPR), a separate fault tree analysis was performed for each mode of emergency operation.

The DHRS is utilized to provide low-pressure emergency core cooling (ECC) in the event of a large LOCA. Water, for the injection phase of ECC, called low pressure injection (LPI), is obtained from the BWST and injected directly into the reactor vessel. The LPR is also used to provide suction head to the high pressure pumps, when the High Pressure System is required during recirculation.

K.1.1 SYSTEM DESCRIPTION

The DHRS consists of two essentially identical trains. For ease of description, each train is separated into the following three parts: 1) pump discharge, 2) pumps and associated equipment, and 3) pump suction.

The pump discharge of each DHRS train has, as its main functional path, a separate discharge line directly into the reactor vessel through a check valve. A portion of this flow path into the vessel is shared with a core flood tank. DHRS pump discharge can also be directed to the borated water storage tank through an eight inch return line shared by both trains. Finally, DHRS flow is supplied to the suction side of the makeup pumps by each train through a remote manually operated valve for cases where the High Pressure System is required during recirculation.

The pump section of each train consists of a decay heat pump, a decay heat removal heat exchanger, and a flow control throttle valve. A minimum flow return line is provided for each pump. However, the pumps cannot operate with minimum flow for more than 15 hours without risking pump damage.

Pump suction for the DHRS can be supplied from three sources:

1) the borated water storage tank (BWST), 2) the reactor building sump, and 3) the reactor coolant system. Each train has an independent line from the BWST and RB sump while sharing a return line from the RCS. The suction lines for each DHRS train also supply suction to a reactor building spray system and the BWST portion of the suction line (BWST side of valves DHV-34 and 35) is also shared with the makeup pump suction header.

Figure K.1 shows the LPI system valve alignment in the injection mode. The LPI system is essentially a two train redundant system. Successful operation requires flow from one operating pump (DHP-1A or 1B) be supplied to the reactor vessel. Each single stage centrifugal pump can deliver 3000 gpm at 350 foot head. The decay heat removal heat exchangers (DHHE-1A and 1B) are not required for heat removal during the injection phase.

The pumps and motor operated valves are supplied with power from the emergency AC power system. In addition, pump control power is from the emergency DC power supply. The pumps require cooling which is provided by the Decay Heat Closed Cycle Cooling System (DHCCCS). The DHCCCS, analyzed separately with the results in Section II.F, consists of two independent redundant trains, each train providing cooling to only one DHRS pump.

The BWST is the only source of water for LPI. This tank also supplies water for reactor building spray injection and high pressure injection. As illustrated in Figure K.1, each DHRS suction line supplies a spray pump and a line to the makeup pump suction header.

Figure K.2 shows the DHRS in the LPR configuration. As can be seen, LPR utilizes the same equipment as LPI with the exception of the pump suction source. Successful LPR requires the delivery of water from the reactor building sump to the reactor vessel by at least one DHRS train.

The LPR system also supplies water for two additional systems during the recirculation phase. If reactor coolant system pressure remains above the effective discharge pressure of the DHRS pumps, the makeup pumps can be used in the high pressure recirculation (HPR) mode. During HPR operation, makeup pump suction must be supplied by the DHRS pumps through DHV-11 or 12.

During the recirculation mode, reactor building heat removal is performed by the fan coolers, sprays and decay heat removal heat exchangers. The specific combinations of equipment required for successful heat removal are addressed in Section 3.0. However, the LPR system does play a role in heat removal by circulating reactor building sump water through the decay heat exchangers for heat removal.

K.1.2 SYSTEM OPERATION

Should a LOCA occur, the DHRS LPI mode is actuated by the ESAS signal which starts both pumps and sends confirmatory open signals to the normally open discharge valves on the pump discharge lines to the reactor vessel. The pumps receive a start signal when reactor coolant system pressure is less than 1500 psig and the normally open valves receive an ESAS signal to open when RCS is less than 500 psig. Although normally open, the BWST discharge valves on the suction side of the LPI pumps also receive an ESAS signal to open when RCS is less than 500 psig. The LPI system is also automatically actuated when the reactor building pressure is rising above 4 psig. Operator action is not required for actuation or operation of the DHRS in the LPI mode.

The BWST water must be recirculated once a week. This is accomplished by utilizing a DHRS pump and the DHRS return line to the BWST. This test is required to recirculate the equivalent of two volumes of the 420,000 gallon BWST which is estimated to take three hours. During this test, the LPI flow path to the reactor vessel from one DHRS pump is disabled. The test is alternated every week between LPI trains such that each LPI pump is operated for three hours once every 14 days. The technical specifications require that the reactor be shut down to hot standby if the BWST is found to be not operable and is not restored within one hour. The BWST is checked once a week for volume, boron concentration, and temperature. The temperature test frequency is increased to once a day when the ambient air temperature is less than 40⁰F.

In addition to BWST circulation, additional checks on DHRS valve position and status are performed. Automatic actuation of pumps and valves is tested once every 18 months during refueling and the system is operated in its DHRS mode during shutdown. Should a DHRS train be found inoperable during power operation, technical specifications require it be restored within 72 hours or the plant be put in the hot shutdown mode.

When the BWST water level reaches the 'low level' (3' 9"), the emergency coolant recirculation phase is initiated and continued as long as necessary. To initiate this phase of operation, the DHRS pump suction is manually switched from the BWST to the reactor building sump. This is accomplished by first opening the RB sump valves DHV-43 and 42 when the BWST low level alarm is activated and after these two valves are verified open, the BWST outlet valves to LPI are closed.

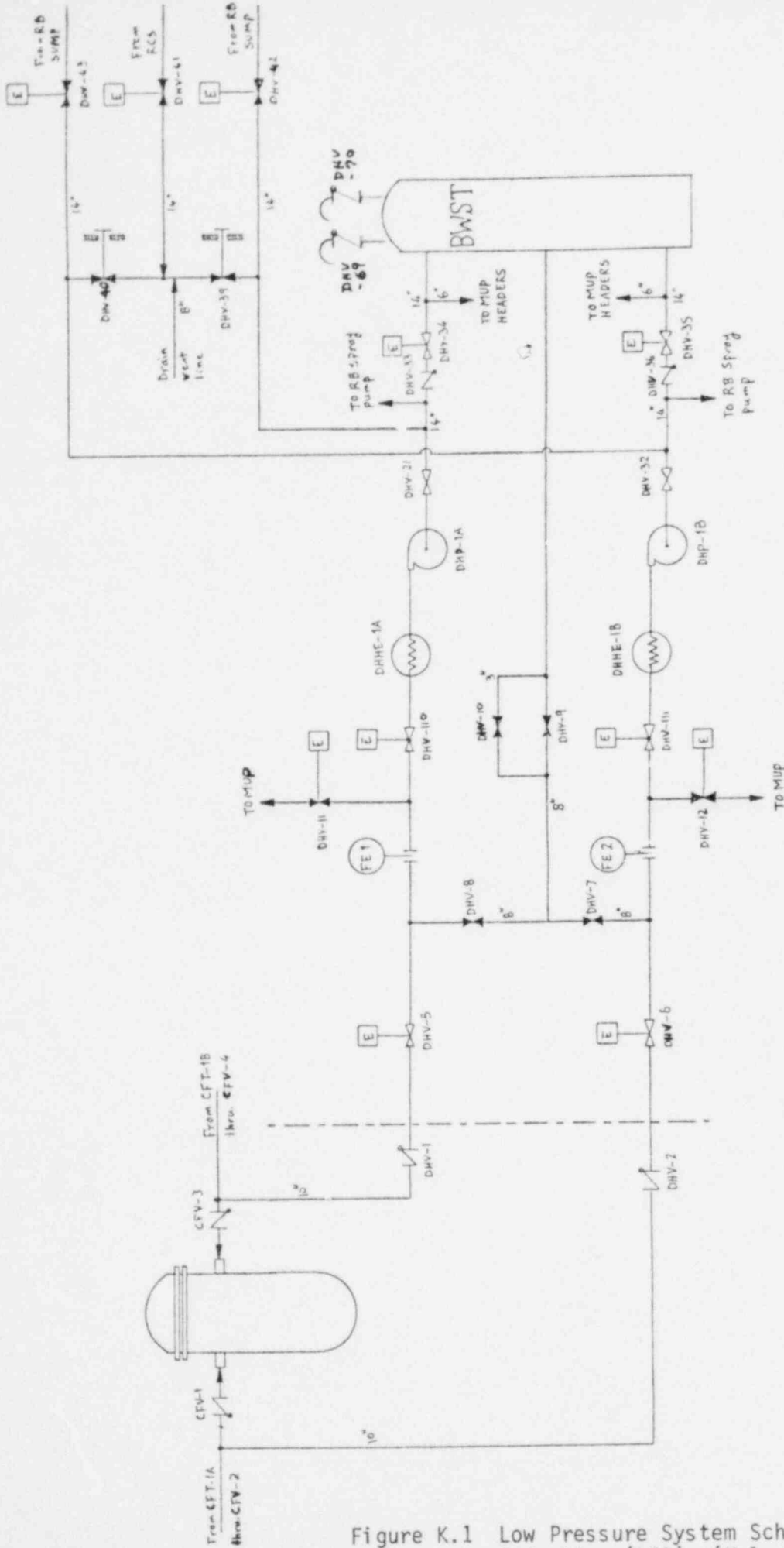


Figure K.1 Low Pressure System Schematic Diagram - Injection (LPI) (Valve Alignment in the Injection Mode)
K-6

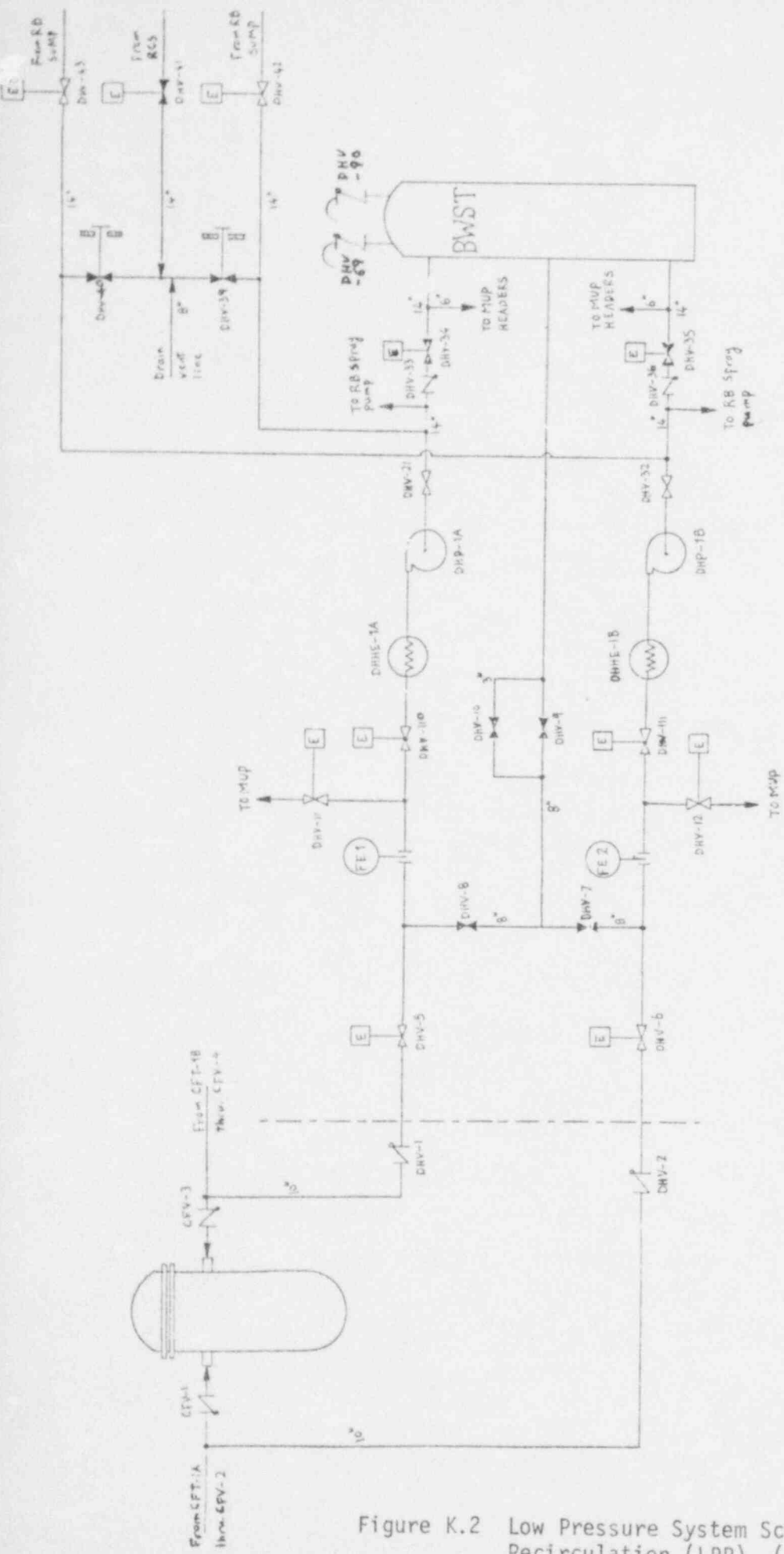


Figure K.2 Low Pressure System Schematic Diagram - Recirculation (LPR). (Valve Alignment in the Recirculation Mode)

K.2 SYSTEM SIMPLIFIED FAULT TREES

K.2.1 LPI FAULT TREE

Failure of the LPI system to supply sufficient water to the reactor vessel after a large LOCA was postulated as the top event for the simplified LPI fault tree, Figure K.3. This event implies that water from both LPI trains is not available to the reactor vessel either at the start of emergency core coolant injection or sometime during the injection phase.

The LPI system shares two ten inch lines into the reactor vessel with the core flood tanks, with one LPI train and one core flood tank (CFT) per vessel penetration. A LOCA in this line on the vessel side of CFV-1 or 3 (see Figure K.1) would also result in the failure of one CFT and one LPI train. This event was not included in the fault tree of LPI. But should it occur, the probability of failure of LPI would be the single train failure probability.

An LPI (DHRS) pump is operated once a week for BWST recirculation. During this test, either DHV-7 and 9 or DHV-8 and 9 are opened depending upon whether pump DHP-1B or 1A, respectively, is being operated. Because two valves are opened for a single pump test, failure to close both valves is postulated as a single fault event. Also, the flow path to the reactor vessel is disabled for one LPI train for the duration of this test which is estimated to require three hours.

Switching to the recirculation mode too early could also fail LPI due to insufficient NPSH in the reactor building sump. This has been identified as a plausible failure mode.

K.2.2 LPR FAULT TREE

Successful LPR operation requires the delivery of flow from one operating DHRS train. The LPR fault tree was developed for failure to supply sufficient flow from both DHRS trains when required, Figure K.4. The LPR fault tree was based upon LPI success which implies at least one operating DHRS train when LPR is required (low-level BWST alarm).

Some faults which could result in failure of one LPI train are recoverable for successful LPR. Recoverable faults are generally failures of automatic signals and mispositioned valves on the pump discharge which do not result in pump failure. The LPR fault tree includes these faults combined with the failure of the operators to recover.

Failure to properly switch to recirculation is critical. Mispositioning of either sump suction (DHV-42 and 43) or BWST outlet (DHV-34 and 35) valves could result in cavitation of LPR pumps and spray pumps. For the fault tree analysis, it is assumed that mispositioning of the valves will fail LPR and sprays in the following combinations:

<u>Valve(s)</u>	<u>Misoperation</u>	<u>Failed Subsystem</u>
DHV-42 and 43	Closed	LPR and Spray-Both
DHV-34 and 35	Open	LPR and Spray-Both
DHV-42	Closed	LPR and Spray-'A'
DHV-34	Open	LPR and Spray-'A'
DHV-43	Closed	LPR and Spray-'B'
DHV-35	Open	LPR and Spray-'B'

Procedure OP-404 requires that one LPR subsystem be shut down within 24 hours after the accident and additional lines from the reactor coolant system to the DHRS be opened to avoid boron precipitation. Many of the LPR components are subject to misoperation during implementation of this procedure. These items are motor operated valves DHV-5, 6, 110, 111, 42, 43, 34, and 35; locally operated manual valves DHV-8, 9, 10, and 7; and pumps DHP-1A and 1B. Misoperation of this equipment could result in failure of a single LPR subsystem or both. The specific combinations of LPR failures are included in the fault tree.

Faults associated with the suction side of the DHRS pumps are assumed to fail the pumps and necessitate pump repair for recovery. During LPR, faults on the discharge side of the pumps require only repair or reconfiguration of the faulted component or item for LPR recovery. For faults that were assessed to be recoverable see the quantification tables.

Table K.1 Simplified Fault Tree - Fault Summary (Train A (B))

SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
LMVDHV5(6)P	DHV-5(6) (N.C.)	Fails to Open
LCBDHV5(6)N	DHV-5(6) Circuit Breaker	Fails Open
LXVTESTX	DHV-8(7) and -9	Open After Test
LCNV110(111)Q	DHV-110(111) Auto Controller	Closes Valve
LPMDH3A(B)R	DHP-1A(B)	Fails to Short
LPMDH3A(B)S	DHP-1A(B)	Fails to Run
LCBPU3A(B)O	Motor Contactor	Inadvertent Trip
LXVDH21(32)X	Manual Valve DHV-21(32)	Inadvertently Closed
LCBPU3A(B)N	Motor Contactor	Does Not Close
MCVOOB2(1)P	Check Valve CFV-3(-1)	Fails to Open
MCVOOB2(1)E	Check Valve CFV-31(-1)	Plugged
LCVDHV1(2)P	DHV-1(-2)	Fails to Open
LCVDHV1(2)E	DHV-1(-2)	Plugged
LPMDHP-1A(B)	Pump DHP-1A(B)	Fails
LCVDH33(36)P	Check Valve DHV-33(-36)	Plugged
JTKDHT1X	BWST	Leak
JTKDHT1R	BWST	Rupture
JTKDHT1E	BWST	Plug
JRVDH69P JRVDH70P	DHV 69 and DHV 70 (Coupled)	Fails to Open

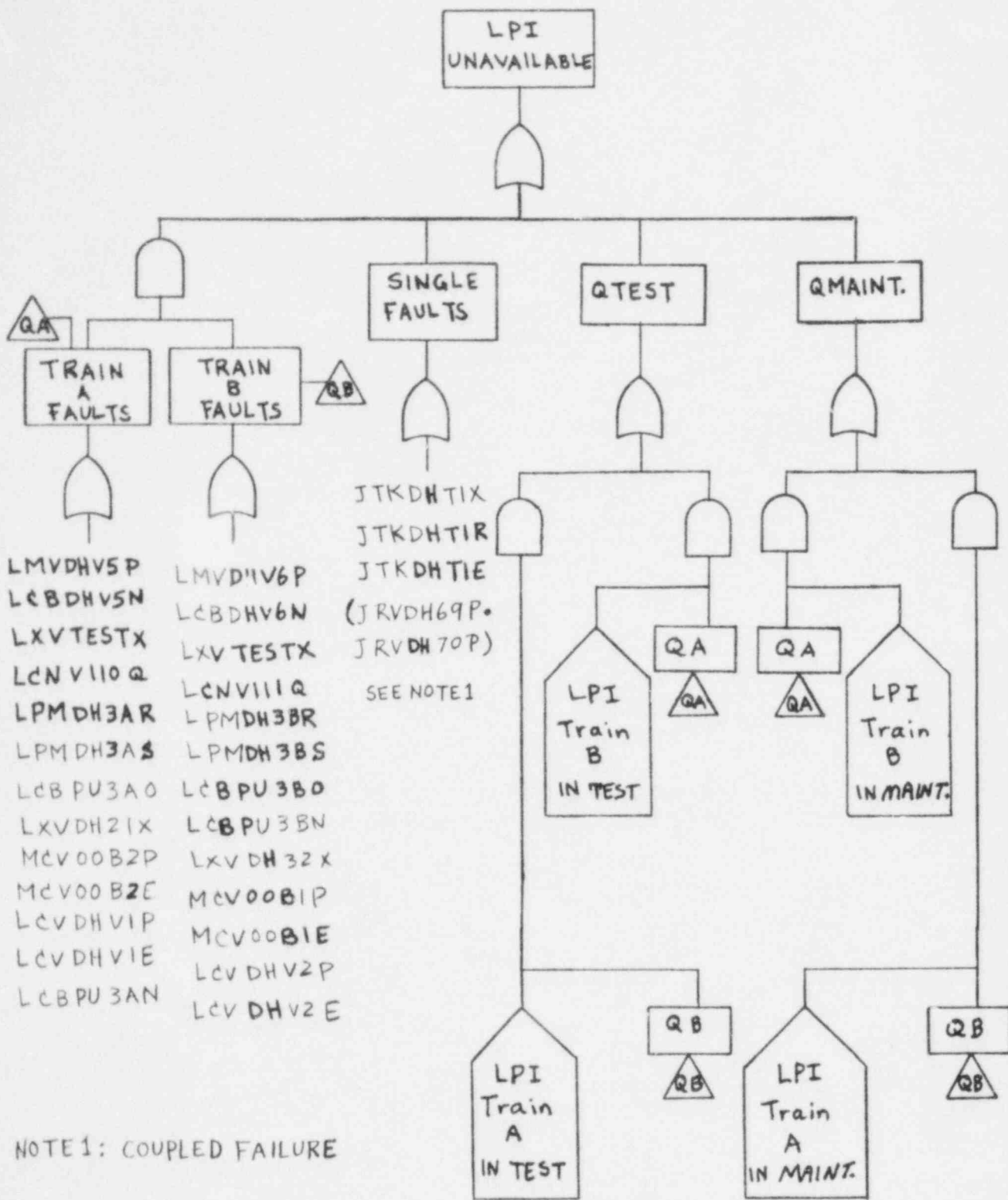


Figure K.3 Simplified Fault Tree - LPI (for the fault summary see Table K.1)

LPR UNAVAILABILITY

COMMON MODE FAULTS

- DHV-70K 8 AND DHV-9 LEFT OPEN
- SUCTION VALVE FAULT COMBINATIONS (SEE SECTION K.2.2)

LPI TRAIN A AND LPR TRAIN B FAILS

LPI TRAIN A FAULTS NOT RECOVERED FOR LPR

NON-RECOVERABLE LPI TRAIN A FAULTS

- LMVDHV5P
- LCBDHV5N
- LPMDHP1A
- LPMDH3AS
- LCBPUSAN
- MCV00B2P
- LCVDHV1P
- LCVDH33P
- LXVDH21X

RECOVERABLE LPI TRAIN A FAULTS

- LPI TRAIN A IN TEST
- LKV TEST X
- DHV-5 DOES NOT RECEIVE ESAS
- NO POWER ON MCC 3-A1
- DHP-1A DOES NOT RECEIVE ESAS
- DPPP-5A FUSE TO OPEN

TRAIN B FAULTS

- DHV-42 FAILS TO OPEN
- OPERATOR DOES NOT OPEN DHV-42
- DHP-1A FAILS TO CONTINUE TO RUN
- DHV-110 PLUGGED
- DHV-5 FAILS CLOSED
- NO POWER ON MCC-3A1
- OPERATOR CLOSES DHV-5 INADVERTANTLY
- OPERATOR TURNS OFF DHP-1A INADVERTANTLY
- DHV-34 DOES NOT CLOSE
- OPERATOR DOES NOT CLOSE DHV-34

LPR TRAIN A FAULTS

QAR

LPR TRAIN B FAULTS

QBR

- DHV-43 FAILS TO OPEN
- OPERATOR DOES NOT OPEN DHV-43
- DHP-1B FAILS TO CONTINUE TO RUN
- DHV-111 PLUGGED
- DHV-6 FAILS CLOSED
- NO POWER ON MCC 3B-1
- OPERATOR CLOSES DHV-6 INADVERTANTLY
- OPERATOR TURNS OFF DHP-1B INADVERTANTLY
- DHV-35 DOES NOT CLOSE
- OPERATOR DOES NOT CLOSE DHV-35

LPI TRAIN B AND LPR TRAIN A FAILS

TRAIN A FAULTS

TRAIN B MAINTENANCE OUTAGE

- LMVDHV6P
- LCBDHV6N
- LPMDHP1B
- LPMDH3B5
- LCBPUSBN
- MCV00B1P
- LCVDHV2P
- LCV36P
- LXVDH32X

LPI TRAIN B FAULTS NOT RECOVERED FOR LPR

NON-RECOVERABLE LPI TRAIN B FAULTS

- LPI TRAIN B IN TEST
- LKV TEST X
- DHV-6 DOES NOT RECEIVE ESAS
- NO POWER ON MCC 3-B1
- DHP-1B DOES NOT RECEIVE ESAS
- DPPP-5B FUSE IS OPEN

RECOVERABLE LPI TRAIN B FAULTS

Figure K.4 Simplified Fault Tree - LPR (For Fault Summary see Table K.1)

K.3 SYSTEM QUANTIFICATION

K.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The low pressure decay heat removal system is a two train system with a crossover that is normally valved closed. The crossover can be opened by opening manual valves, if sufficient time is available. The system is required to perform several functions, depending on the LOCA size. For the smallest LOCA, the system is required to provide suction head to the high pressure pumps during the recirculation phase. For the larger size LOCA's, the system is required to inject and recirculate cooling water directly into the reactor vessel. The low pressure system requires AC power, DC power and the DHCCCS for component cooling and decay heat removal.

For the case where offsite power is available, the LPI system unavailability is due to operator error and double failures in the low pressure trains. The operator error contribution is about a factor of two higher than the hardware contribution. This case only is applicable for the larger LOCA sizes (B_1 , B_2 , B_3), since it was assumed that offsite power would be available in these cases. For the smallest LOCA size (B_4) the low pressure system is not required until recirculation.

During recirculation the low pressure system is required to provide suction head to the high pressure pumps for the B_4 LOCA case. In this mode of operation, the primary contributors to low pressure system failure are operator errors. Maintenance outages also contribute to the unavailability in this case. For the larger size LOCA's, the primary contributors are also operator errors, which are about an order of magnitude larger than hardware faults.

K.3.2 SYSTEM FAULT TREE QUANTIFICATION - INJECTION PHASE

Five modularized fault trees were constructed to quantify LPI unavailability. The top level tree shows LPI unavailability in terms of the unavailability of LPI Train A, Train B, and single faults that fail LPI. Modularized fault trees of LPI Trains A and B were constructed. For convenience of quantification, fault trees of each LPI leg to the crossover were also constructed. These fault trees apply to LOCA sizes B_1 , B_2 and B_3 . For the B_4 LOCA, the Low Pressure System supplies suction head to the high head pumps during the recirculation phase. Therefore, component start failures for the low head system are contained in the LPR analysis for this size LOCA.

Table K.2 shows the success criteria for LPI for the various LOCA sizes (B_1 , B_2 , B_3). Table K.3 shows the top event definitions for the modularized fault trees. Figures K.5 through K.7 presents the modularized fault trees. The notes to the fault trees are in Table K.4. The unavailability of each gate is shown on these trees, as well as the unavailability of the top events. Table K.5 shows the Boolean equations that represent each of these trees. Table K.6, the fault tree quantification table, shows the quantification of each gate in terms of component failure modes. The assumptions used in the quantification are described in the notes for this table. Table K.7 shows the point estimate for each gate.

Table K.2 Low Pressure Injection - Success Requirements

<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B ₄ LOCA and Transient induced LOCA	1/2	1
B ₃ LOCA	1/2	2
B ₂ LOCA	2/2 or 1/2 with both core flood tanks operating	2, 3
B ₁ LOCA	1/2 with both core flood tanks operating	2, 3

NOTES: 1. For these initiators, the Low Pressure System is actually not required until the High Pressure System is reconfigured for recirculation. The system function is more appropriately referred to as Low Head Initiation; its purpose is to boost suction pressure to the high pressure pumps. The Low Head System for the B₄-LOCA is analyzed together with B₄ - recirculation LHR. See Low Pressure Recirculation analysis.

2. For this initiator, the successful low pressure train need not correspond to a successful high pressure train.

3. Core Flood Tanks are analyzed separately.

Table K.3 Low Pressure Injection - Top Events

BOOLEAN
REPRESENTATION

NOTES

B₁, B₂, B₃ - LOCAs

LPA	Failure of low pressure Train A to provide flow to reactor vessel.	1
LPB	Failure of low pressure Train B to provide flow to reactor vessel.	
LPI	Failure of Low Pressure System to provide at least one pump flow to reactor vessel.	
LA	Low Pressure Train A failures from BWST to crossover.	
LB	Low Pressure Train B failures from BWST to crossover.	

Note: 1. The low pressure injection system is not required during the injection phase for B₄-LOCA. Faults occurring during the injection phase are included in LHR, LHA, and LHB. See quantification of the Low Pressure System during recirculation for B₄-LOCA.

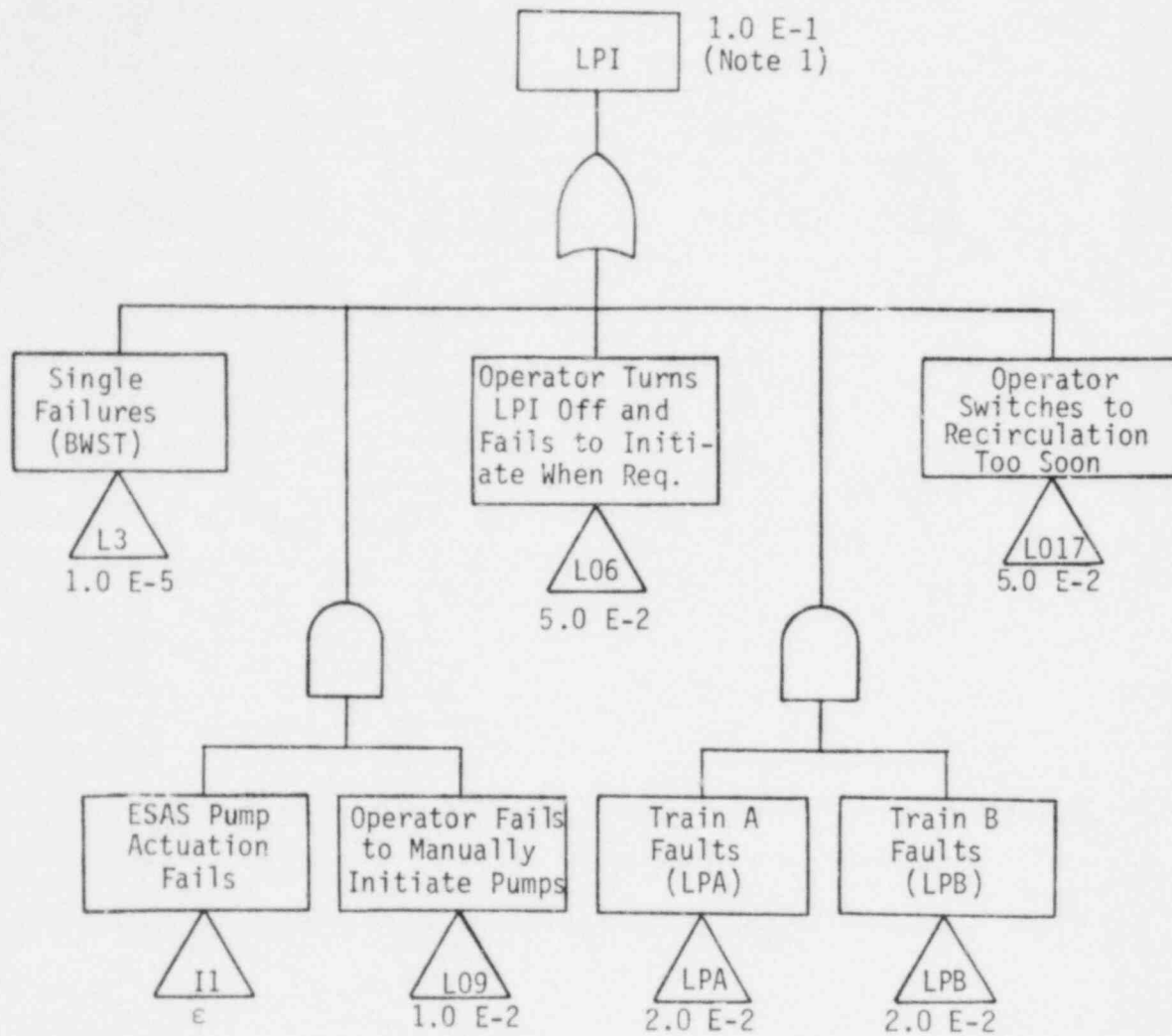


Figure K.5 Modularized Fault Tree for Event "LFI" (B_1 , B_2 , B_3 LOCAs)

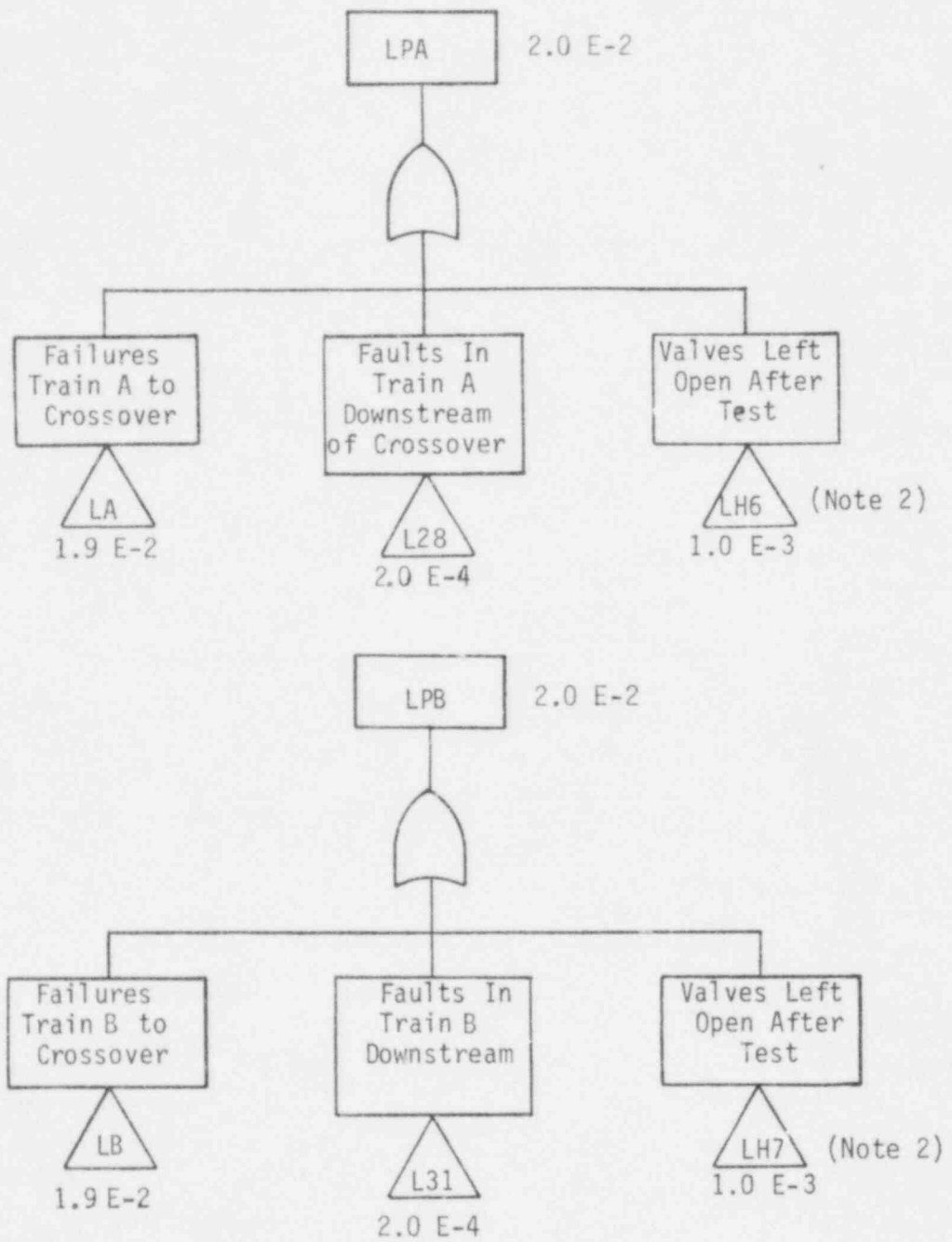


Figure K.6 Modularized Fault Trees for Events "LPA" and "LPB" (B₁, B₂, B₃ LOCAs)

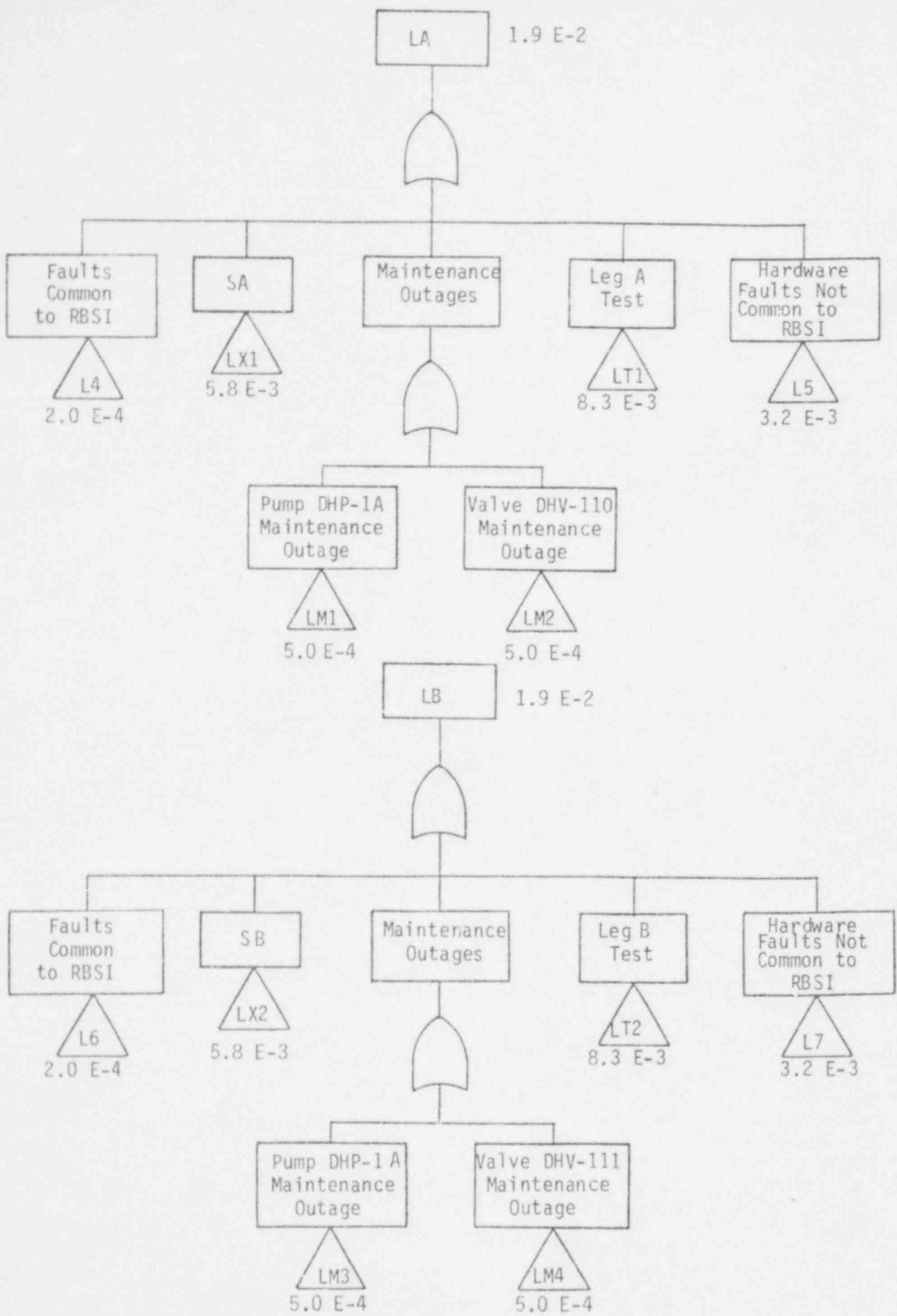


Figure K.7 Modularized Fault Trees for Events "LA" and "LB"
 (B_1, B_2, B_3 LOCAs)

Table K.4 Low Pressure Injection (B₃, B₂, B₁-LOCAs)

FAULT TREES

(LPA, LPB, LPI)

NOTES

- 1 LPA, LPB, and LPI are failure of the low pressure injection system during emergency core cooling initiation.
- 2 Operator fails to close DHV-8,9 which fails Train A of LPI. Operator fails to close DHV-7,9 which fails Train B of LPI. These acts were assessed as a triple common mode human fault that fails both trains of LPI

Table K.5 Low Pressure Injection (B_1, B_2, B_3 -LOCAs)

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

NOTES

$$LPI = L3 + L06 + I1 \cdot L09 + L017 + LPA \cdot LPB$$

$$LPA = L28 + LH6 + LA$$

2

$$LPB = L31 + LH7 + L3$$

2

INTERMEDIATE EVENTS

$$LA = L4 + L5 + LT1 + LM1 + LM2 + LX1$$

2

$$LB = L6 + L7 + LT2 + LM3 + LM4 + LX2$$

2

$$LX1 = ACA + DCA + DA$$

$$LX2 = ACB + DCB + DB$$

BOOLEAN EQUATIONS REGROUPED FOR REDUCTION

TOP EVENTS

$$\begin{aligned} LPI = & L3 + L06 + I1 \cdot L09 + L017 + (L4 \cdot L6) + (L5 \cdot L7) + (ACA \cdot ACB) + \\ & + DA \cdot DB + (L28 \cdot L31) + (LH6 \cdot LH7) + L4 \cdot L7 + L5 \cdot L6 + \\ & + ACA \cdot (L6 + L7 + LT2 + LM3 + LM4 + DB) + (L4 + L5) \cdot (LT2 + LM3 + LM4) + \\ & + ACB \cdot (L4 + L5 + LT1 + LM1 + LM2 + DA) + (L6 + L7) \cdot (LT1 + LM1 + LM2) + \\ & + DA \cdot (L6 + L7 + LT2 + LM3 + LM4) + DB \cdot (L4 + L5 + LT1 + LM1 + LM2) + \\ & + LA \cdot (L31 + LH7) + LB \cdot (L28 + LH6) \end{aligned} \quad (1,2,3,4)$$

$$LA = L4 + L5 + LT1 + LM1 + LM2 + LX1$$

$$LB = L6 + L7 + LT2 + LM3 + LM4 + LX2$$

Table K.5 Boolean Equations (LOCAs B_1 , B_2 , B_3)

NOTES

- 1 The event LH6-LH7 was evaluated as a triple common mode human error of leaving valves DHV-7, DHV-8, DHV-9 in the wrong position (open) after test.
- 2 The terms LPA-LPB and LA-LB contain hardware components that were assumed to have coupled failure modes. See quantification tables.
- 3 It was assumed that no recovery is possible for legs in test when the low pressure injection system is required for the injection phase.
- 4 Terms representing simultaneous outages in both legs are omitted since they are prohibited by Technical Specifications.

K-23

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L3		SINGLE FAILURES	D		1.0 E-5	2 ⁺ , 2 ⁻	B	
	BWST	LEAKS			e			1
	BWST	RUPTURE			e			1
	BWST	PLUG			e			1
	BWST	TWO REDUNDANT VACUUM BREAKERS FAIL TO OPEN	D	(1.E-4)(0.1)	1.0 E-5 =1.0 E-5	2 ⁺ , 2 ⁻	B	2
L06	OPERATOR	TURNS LPI OFF AND FAILS TO INITIATE	D		5.0 E-2	3 ⁺ , 10 ⁻	O	12, 20
L09	OPERATOR	FAILS TO MANUALLY INITIATE PUMPS	D		1.0 E-2	3 ⁺ , 10 ⁻	O	11
I1	ESAS(ILB3-ILB3)	FAILS TO ACTUATE BOTH PUMPS			e			
L017	OPERATOR	SWITCHES TO RECIRCULATION TOO SOON	D		5.0 E-2	3 ⁺ , 10 ⁻	O	20
L4-L6		EVENT INCLUDING COUPLED VALVE FAILURES DHV-33, DHV-34, DHV-35, DHV-36			1.0 E-5	2 ⁺ , 2 ⁻	B	3
L5-L7		EVENT INCLUDING COUPLED PUMP FAILURES DHP-1A, DHP-1B			1.0 E-5	2 ⁺ , 2 ⁻	B	4
DA-DB		EVENT INCLUDING COUPLED FAILURES IN BOTH TRAINS OF DHCCCS. SEE DHCCCS FAULT TREE QUANTIFICATION TABLE						
L28-L31		EVENT INCLUDING COUPLED CHECK VALVE FAILURES CFV-1, CFV-3			2.0 E-5	2 ⁺ , 2 ⁻	B	5
LH6-LH7	HUMAN	COMMON MODE HUMAN FAILURE OF LEAVING VALVES DHV-7, 8, 9 IN OPEN POSITION AFTER TEST (SEE TABLE K.6)			1.0 E-5	3 ⁺ , 3 ⁻	H	6

Table K.6 (1/4) Event "LPI" Quantification

Table K.6 (2/4) Events "LPA" and "LPB" Quantification (Note 9)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L26		FAULTS IN TRAIN A DOWNSTREAM OF CROSSOVER			2.0 E-4			
	CHECK VALVE DHV-1	FAILS TO OPEN	D		1.0 E-4	3+, 3-		
	CHECK VALVE CFV-3	FAILS TO OPEN	D		1.0 E-4 Σ = 2.0 E-4	3+, 3-		10
LH6	HUMAN	VALVES DHV-5, DHV-9 LEFT OPEN AFTER TEST	D		1.0 E-3	3+, 3-	H	13
L31		FAULTS IN TRAIN B DOWNSTREAM OF CROSSOVER			2.0 E-4			
	CHECK VALVE DHV-2	FAILS TO OPEN	D		1.0 E-4	3+, 3-		
	CHECK VALVE CFV-1	FAILS TO OPEN	D		1.0 E-4 Σ = 2.0 E-4	3+, 3-		10
LH7	HUMAN	VALVE DHV-7, DHV-9 LEFT OPEN AFTER TEST	D		1.0 E-3	3+, 3-	H	13

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L4	DHV-34	FAULTS COMMON TO REACTOR BUILDING SPRAY INJECTION			2.0 E-4			
		VALVE PLUGGED	D		1.0 E-4	3 ⁺ , 3 ⁻		
	CHECK VALVE DHV-33	FAILS TO OPEN (PLUGGED)	D		1.0 E-4 Σ=2.0 E-4	3 ⁺ , 3 ⁻		
L5	HARDWARE FAULTS NOT COMMON TO REACTOR BUILDING SPRAY INJECTION				3.2 E-3	3 ⁺ , 3 ⁻ 3 ⁺ , 3 ⁻	H H	
	DHP-1A	PUMP FAILS TO START	D		1.0 E-3	3 ⁺ , 3 ⁻		
	DHP-1A CIRCUIT BREAKERS	CIRCUIT BREAKER FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
	DPDP-5A FUSE 13	OPEN	1.0 E-6	160	1.7 E-4	3 ⁺ , 3 ⁻		15
	DHV-21	MANUAL VALVE LEFT CLOSED	D		1.0 E-3 Σ=3.2 E-3	3 ⁺ , 3 ⁻	H	16
L71	DHP-1A	OUT OF SERVICE	.02/720	10	5.0 E-4	3 ⁺ , 3 ⁻	H	
L72	DHV-110	OUT OF SERVICE	.02/720	18	5.0 E-4	3 ⁺ , 3 ⁻	M	
LT1		LEG A IN TEST	2/720	3	8.3 E-3			17
LX1		SYSTEM INTERFACE FAULTS			5.8 E-3			
ACA		AC TRAIN A INSUFFICIENT POWER NON LOSS OF OFFSITE POWER			c			18, 19
DCA		DC TRAIN A INSUFFICIENT POWER NON LOSS OF OFFSITE POWER			c			
DA		DHCCS INSUFFICIENT COOLING NON LOSS OF OFFSITE POWER			5.8 E-3 Σ=5.8 E-3			7 8

K-25

Table K.6 (3/4) Event "LA" Quantification (Note 14)

Table K.6 (4/4) Event "LB" Quantification (Note 14)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES	
L6	DHW-55	FAULTS COMMON TO REACTOR BUILDING SPRAY INJECTION VALVE PLUGGED	D		2.0 E-4	3+, 3-			
					1.0 E-4				
L7	CHECK VALVE DHW-56	FAILS TO OPEN (PLUGGED)	D		1.0 E-4	3+, 3-			
					≈ 2.0 E-4				
	DHP-1B DHP-1B CIRCUIT BREAKER	HARDWARE FAULTS NOT COMMON TO REACTOR BUILDING SPRAY INJECTION FAILS TO START	D	D		3.2 E-3	3+, 3-	H	
						1.0 E-3			
						1.0 E-3			
IPDB-5B FUSE 1J	FAILS TO CLOSE	D	D		1.7 E-4	3+, 3-		15	
DHW-32	MANUAL VALVE LEFT CLOSED	D	D	168	1.0 E-3	3+, 3-		16	
LM3	DHP-1B	OUT OF SERVICE	.02/720	18	5.0 E-4	3+, 3-			
LM4	DHW-111	OUT OF SERVICE	.02/720	18	5.0 E-4	3+, 3-			
L12		LEG B IN TEST	2/720	3	8.3 E-3	3+, 3-		17	
LX2	ACB	SYSTEM INTERFACE FAULTS AC TRAIN B INSUFFICIENT POWER NON LOSP			5.8 E-3				
DCB		DC TRAIN B INSUFFICIENT POWER NON LOSP			5.8 E-3				
TB		DHCSS INSUFFICIENT COOLING NON LOSP			5.8 E-3			7	

Table K.6 (1/2) Fault Tree Quantification (B_1 , B_2 , B_3 -LOCAs)

NOTES

- 1 BWST level is monitored, so these faults could not exist for any appreciable length of time before discovery and corrective action. Therefore, they were assessed as negligible contributors (ϵ).
- 2 This fault was assessed as a hardware common mode failure of 2 vacuum breakers failing to open when required. A failure probability of $1.0 \text{ E-}4$ (check valve demand failure rate) was used as the single vacuum breaker failure mode. A coupling coefficient (β -factor) of 0.1 was used as the conditional probability of failure of the second given failure of the first.
- 3 The event L4-L6 was evaluated assuming coupled failure between valves DHV-33, 34, 35, and 36. A coupling coefficient (conditional probability of failure of one valve, given failure of the other valve, or β -factor) of 0.1 was assumed.
- 4 The event L5-L7 was evaluated assuming coupled failures between pumps DHP-1A and DHP-1B. A coupling coefficient (conditional probability of failure of one pump, given failure of the other pump, or β -factor) of 0.1 was assumed.
- 5 The event L28-L31 was evaluated assuming coupled failures between check valves CFV-1 and CFV-3. These component failures were assumed to be coupled because they see the same pressure differential. A coupling coefficient (conditional probability of failure of one check valve, given failure of the other, or β -factor) of 0.1 was assumed.
- 6 This common error was assessed as $1.0 \text{ E-}3$ (frequency) for leaving 1 pair of valves in incorrect position after test with an additional frequency of $1.0 \text{ E-}2$ for leaving the third valve in incorrect position. The two acts were assumed to be independent.
- 7 See DC-power quantification tables.
- 8 The event DA contains event ACA.

Table K.6 (2/2) Fault Tree Quantification (B_1 , B_2 , B_3 -LOCAs) (Cont.)

NOTES

- 9 LPA (LPB) includes only those faults that fail Train A(B) of LPI to the reactor vessel.
- 10 Check valve CFV-3(1) failure assumed coupled with check valve CFV-1(3) failure; see event L28-L31 in LPI quantification table.
- 11 If ESAS actuation of pump DHP-1H(B) fails, operator can recover by manually initiating. A frequency of $1.0 \text{ E-}2$ was assumed to be the probability of failure to recover.
- 12 Operator terminates LPI. When LPI is required at a later time, initiation is manual.
- 13 Common mode human error of leaving two manual valves in wrong position after test. Assessed as $1.0 \text{ E-}2$ for the basic fault and a coupling coefficient of 0.1.
- 14 Only faults upstream of crossover contribute to LA or LB.
- 15 Fault duration time is 1/2 of 2 weeks, since fuse is tested bi-weekly via pump tests.
- 16 This fault represents the human error of leaving the valve closed following pump maintenance. The unavailability is estimated as follows: (0.02 maintenance acts per month) X ($1.0 \text{ E-}2$ per act) X (360/720 months fault duration).
- 17 Each leg is operated for about 3 hours every two weeks to recirculate BWST water.
- 18 See appropriate fault tree analysis.
- 19 For loss of offsite power transients, this fault is assumed to be recovered, even if the diesel fails, by the time the system is required.
- 20 This human error was evaluated using THERP tree analysis as described in NUREG/CR-1278.

Table K.7 (1/2) LPI - Quantification Summary (B₁, B₂, B₃ LOCAs)

BOOLEAN VARIABLE	POINT ESTIMATES
L3	1.0 E-5
L06	5.0 E-2
L09	1.0 E-2
I1	ε
L017	5.0 E-2
L4·L6	1.0 E-5
L5·L7	1.0 E-4
L28·L31	2.0 E-5
LH6·LH7	1.0 E-5
L28	2.0 E-4
LH6	1.0 E-3
L31	2.0 E-4
LH7	1.0 E-3
L4	2.0 E-4
L5	3.2 E-3
LM1	5.0 E-4
LM2	5.0 E-4
LT1	8.3 E-3
ACA	ε* 3.2 E-2**
DCA	ε* 3.2 E-3**
DA	5.8 E-3* 3.8 E-2**
L6	2.0 E-4

Table K.7 (2/2) LPI - Quantification Summary (B₁, B₂, B₃ LOCAs)

BOOLEAN VARIABLE	POINT ESTIMATES
L7	3.2 E-3
LM3	5.0 E-4
LM4	5.0 E-4
LT2	8.3 E-3
ACB	ε*
	3.2 E-2**
DCB	ε*
	3.2 E-3
DB	5.8 E-3*
	3.8 E-2**

*Offsite power available
 **Offsite power not available

K.3.3 SYSTEM FAULT TREE QUANTIFICATION - RECIRCULATION PHASE

Modularized fault trees for Low Pressure System failure during the recirculation phase were developed for the four LOCA size accident initiators. For the smallest LOCA size (B_4) the Low Pressure System is not required until the recirculation phase. At recirculation this system is required to boost the suction head of the high pressure pumps. Modularized fault trees were constructed for failure to provide suction head to each of the high pressure pumps, and failure to provide suction head to either of the high head pumps. For the other LOCA sizes, the LPR is required to inject water into the reactor vessel and remove heat during the recirculation phase. Four modularized fault trees were constructed for failure of this function, corresponding to failure of combinations of each train in injection and recirculation leading to failure of both trains.

Table K.8 shows the success criteria for each LOCA size, Table K.9 shows the top event definitions for each of the modularized fault trees, and Figures K.8 through K.14 show the modularized fault trees. The unavailability or unreliability of each gate is shown on these trees, as well as the unreliability of the top events. Tables K.10 and K.11 show the Boolean equations that represent the fault trees. Table K.12, the fault tree quantification tables, show the quantification of each gate in terms of component failure modes. The notes for this table explain the assumptions that were made in the quantification. Tables K.13 and K.14 show the point estimates of each gate.

Table K.8 Low Pressure Recirculation - Success Requirements

<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B ₄ LOCA and Transient induced LOCA	1/2 trains with associated high pressure train	1,2,3
B ₃ LOCA	1/2	4,5,6
B ₂ LOCA	1/2	4,5,6
B ₁ LOCA	1/2	4,5,6

Table K.8 Low Pressure Recirculation - Success Requirements

NOTES

- 1 For the B₄-LOCA failures of pumps and valves to change state (e.g., alignment to low head injection) which would ordinarily be included in the analysis of low head injection, are included in low head recirculation. This is because the low pressure system is not required until the recirculation phase.
- 2 The low pressure trains are required to boost the suction head of the high pressure trains. The associated trains of the low pressure and high pressure systems are required to provide a flow path between the pump and the reactor vessel. The associated DHCCCS-trains are also required to provide component cooling and decay heat removal.
- 3 A possible second success path is 1/2 high pressure recirculation trains with associated low pressure train with 1/3 fan coolers operating. However, this success path implies that component cooling is provided by the DHCCCS and only the decay heat removal function of the DHCCCS is unavailable. Such a failure mode for the DHCCCS is considered to be very unlikely. Therefore, only the first success criterion was used in the analysis.
- 4 The success path is 1/2 low pressure recirculation trains with associated DHCCCS-trains for component cooling and decay heat removal. The alternate success path of 1/2 LPR-trains with 1/3 fan coolers was not considered for the reasons given in Note 2.
- 5 For this initiator, the successful low pressure train need not correspond to a successful high pressure train.
- 6 Assumes system success in the injection phase.

Table K.9 Low Pressure Recirculation - Top Events

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
B ₄ - LOCA		
LHA	Failure of low pressure system to provide flow to suction of high pressure Train A during recirculation	1
LHB	Failure of low pressure system to provide flow to suction of high pressure Train B during recirculation.	1
LHR	Failure of low pressure system to provide flow to suction of at least one high pressure train during recirculation.	1
OTHER LOCAs (B ₁ , B ₂ , B ₃)		
LPR	Failure of low pressure system to provide at least one pump flow to reactor vessel during recirculation.	2
LRR	Failure of both low pressure system trains to provide flow to the reactor vessel during recirculation.	2
LIR	Failure of low pressure system Train A during injection and of Train B during recirculation to provide flow to reactor vessel.	2
LRI	Failure of low pressure system Train B during injection and of Train A during recirculation to provide flow to reactor vessel.	2

- NOTES: 1. This event includes failure of the pumps to start, and failure of the valves to align for injection.
2. This event assumes success or recovery during the injection phase.

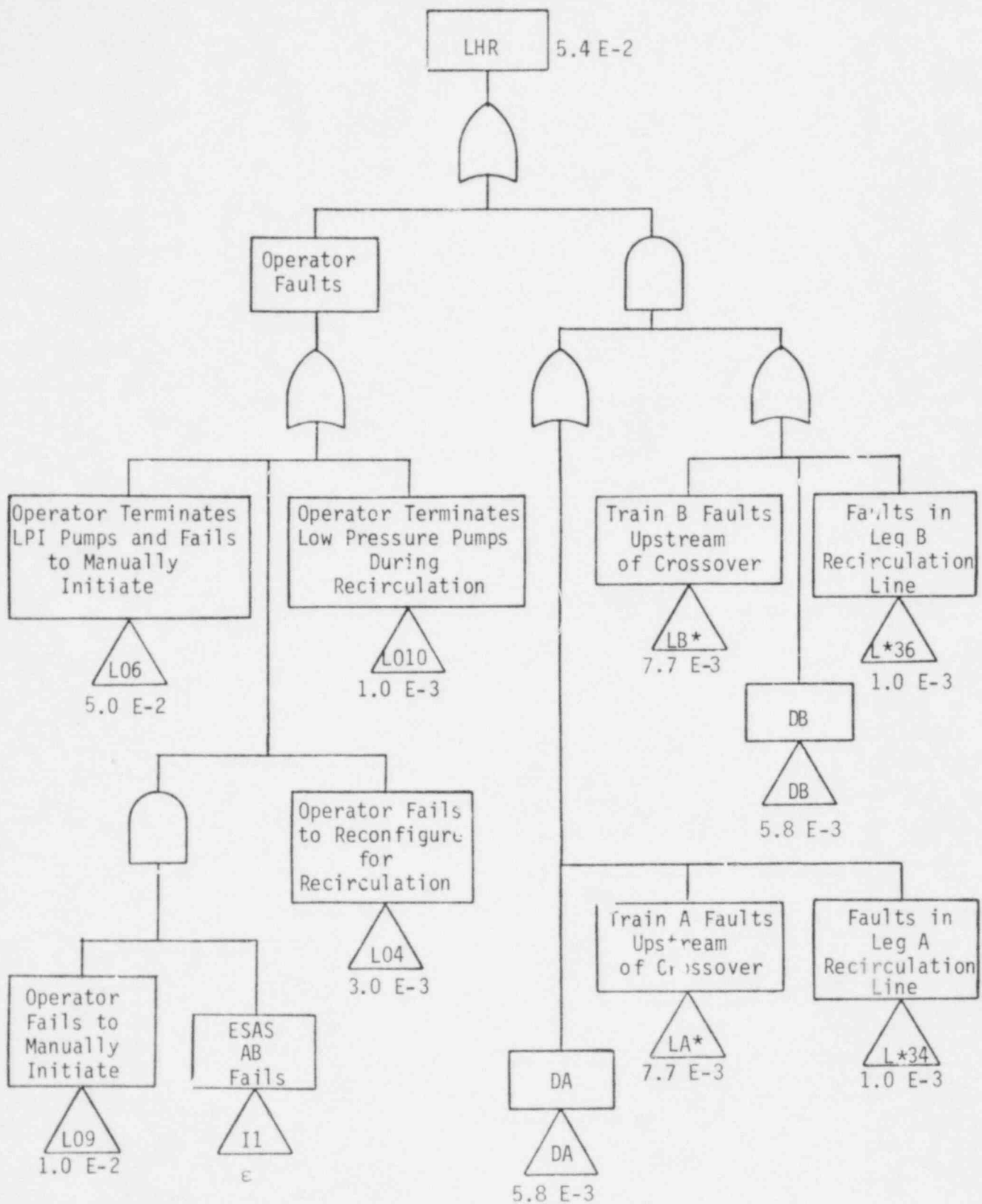


Figure K.8 Modularized Fault Tree for Event "LHR" (B₄ LOCA)

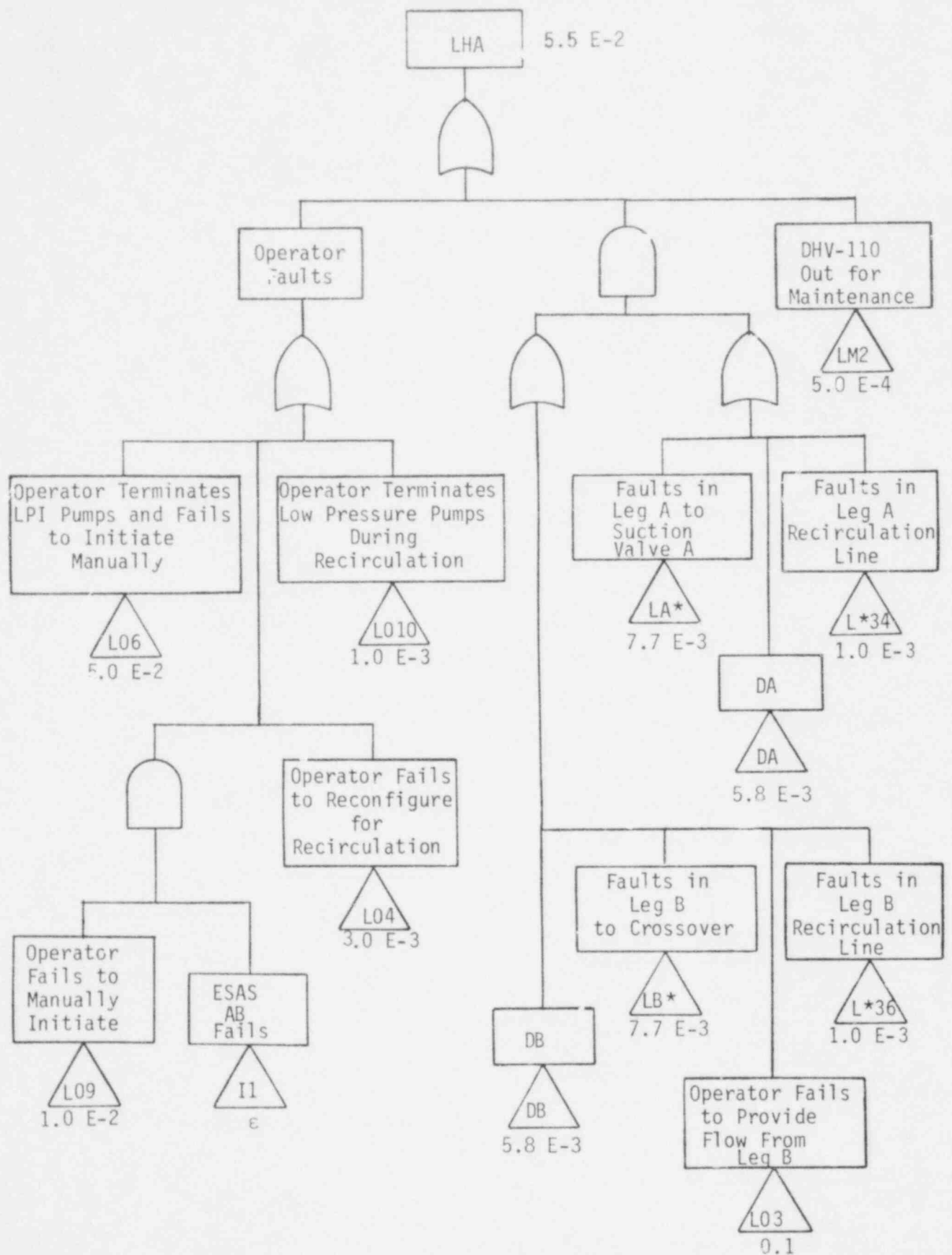


Figure K.9 Modularized Fault Tree for Event "LHA" (B₄ LOCA)

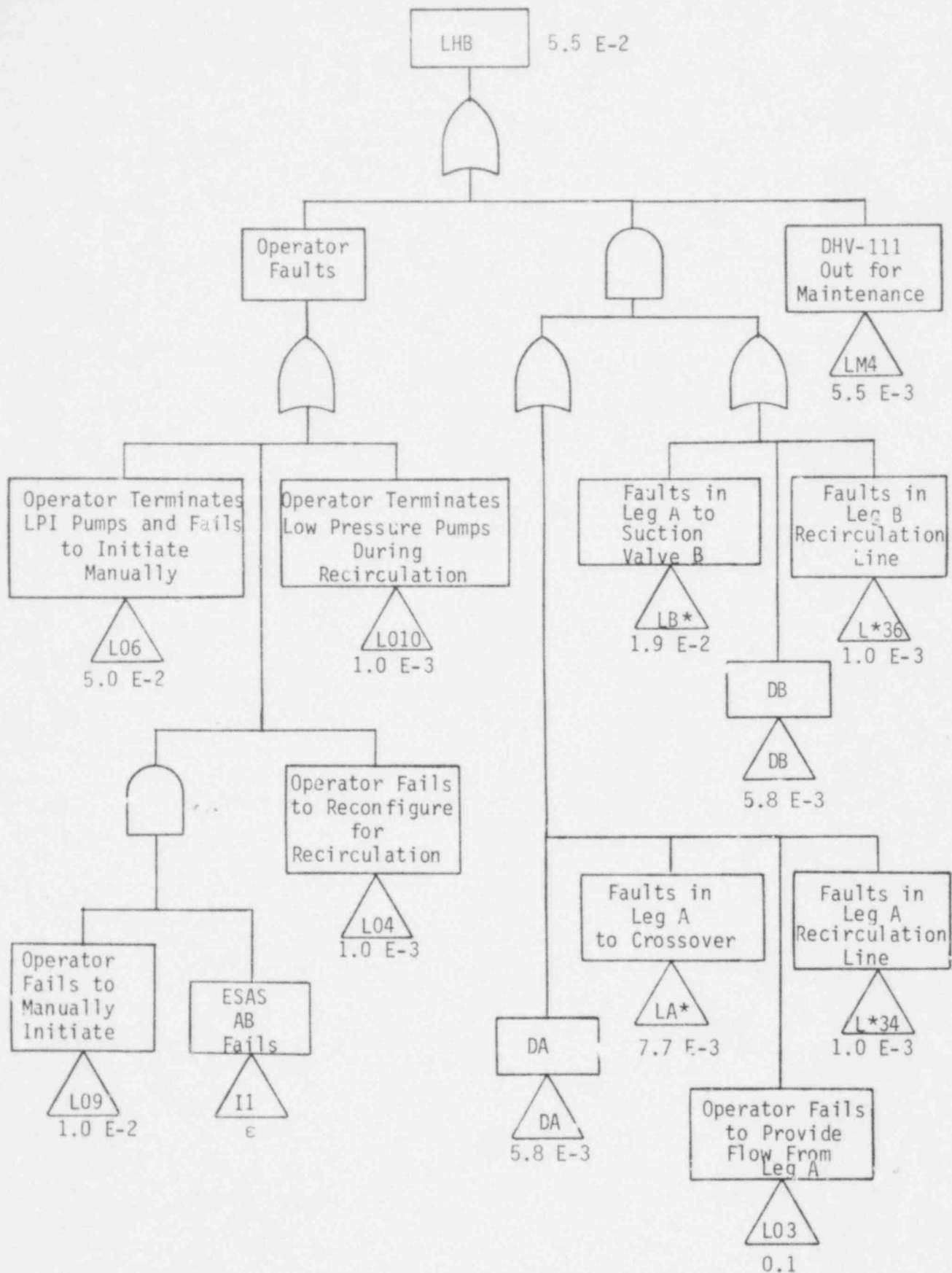


Figure K.10 Modularized Fault Tree for Event "LHB" (P₄ LOCA)

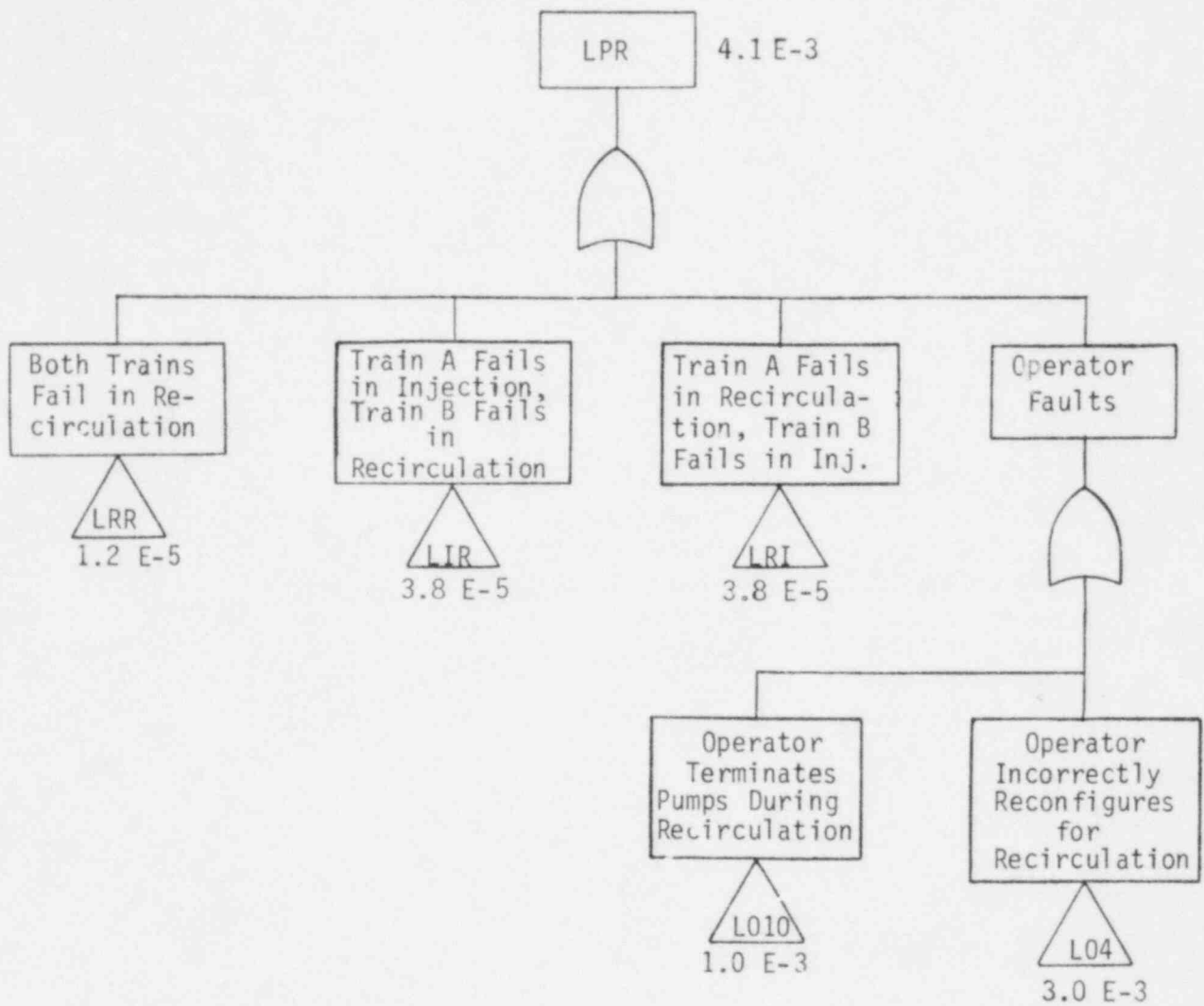


Figure K.11 Modularized Fault Tree for Event "LPR" (B_1 , B_2 , B_3 LOCAs)

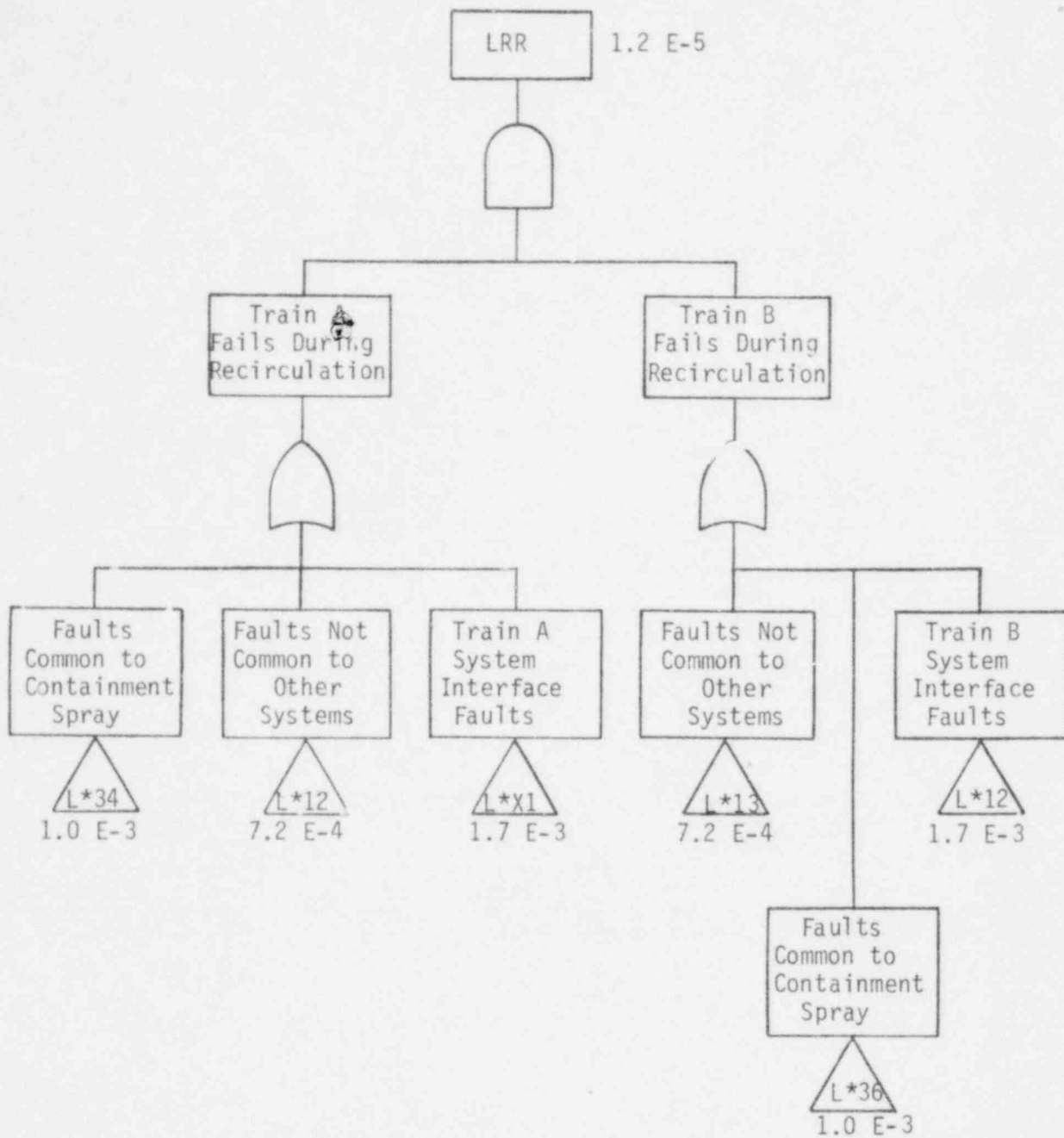


Figure K.12 Modularized Fault Tree for Event "LRR" (B₁, B₂, B₃ LOCAs)

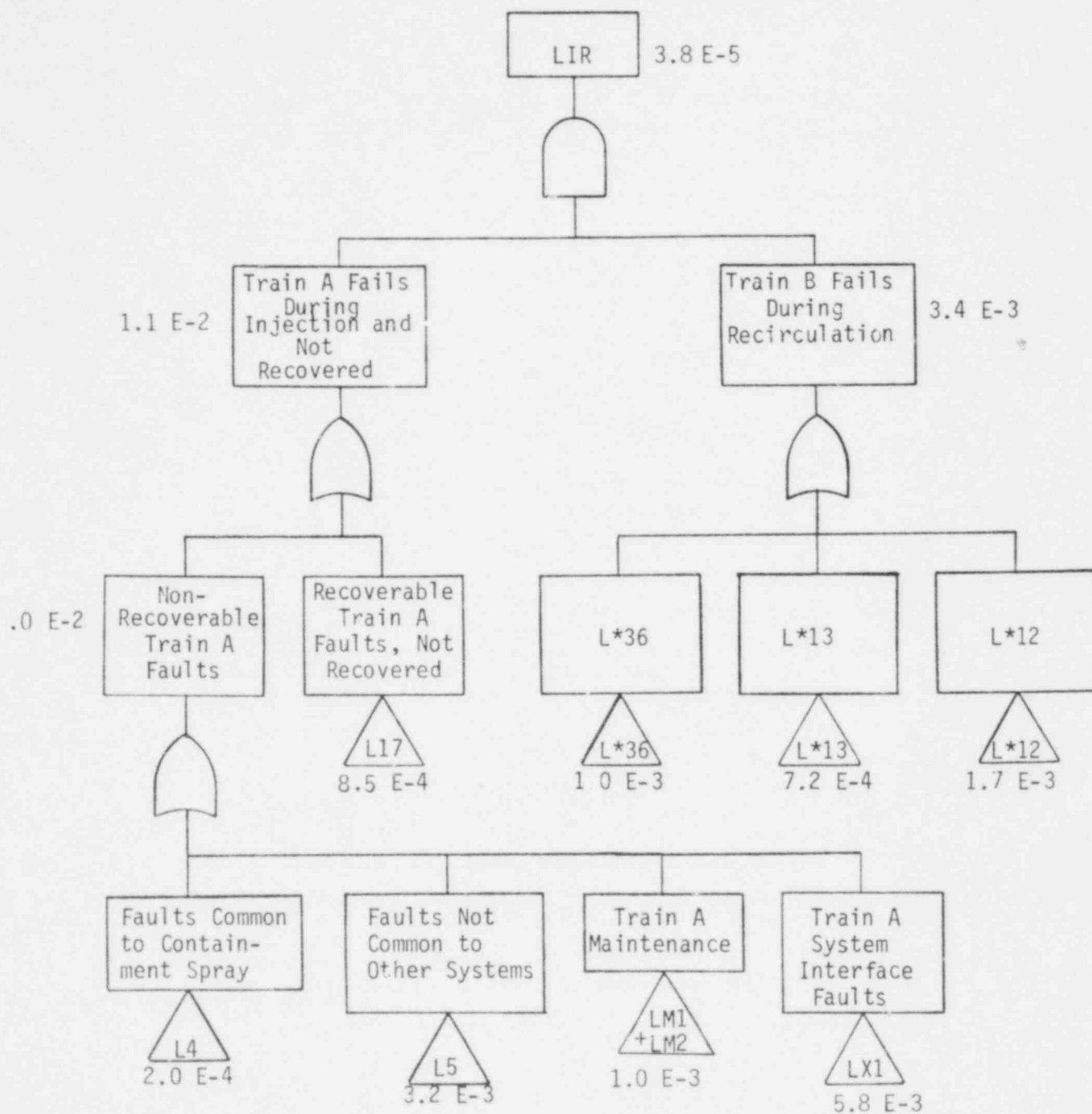


Figure K.13 Modularized Fault Tree for Event "LIR" (B_1 , B_2 , B_3 LOCAs)

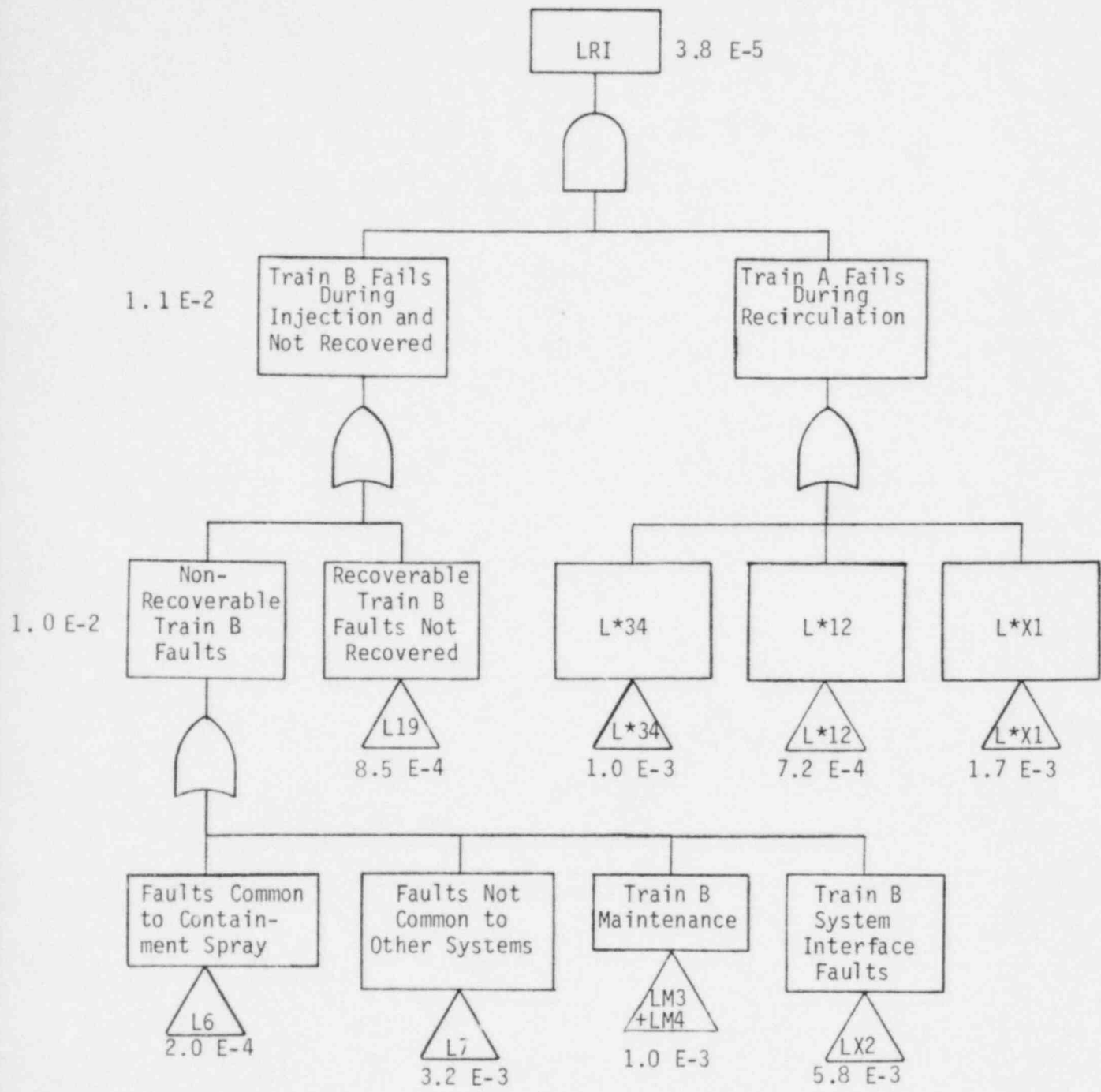


Figure K.14 Modularized Fault Tree for Event "LRI" (B_1, B_2, B_3 LOCAs)

Table K.10 Low Pressure Recirculation (B₄-LOCA)

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

<u>TOP EVENTS</u>	<u>NOTES</u>
$LHR = L04 + L06 + L010 + I1 \cdot L09 + (L*34 + LA* + DA) \cdot (L*36 + LB* + DB)$	(1)
$LHA = LM2 + L06 + L010 + L04 + I1 \cdot L09 + (L*34 + LA* + DA) \cdot (L*36 + LB* + DB + L03)$ $= LHR + LM2 + L03 \cdot (L*34 + LA* + DA)$	(1)
$LHB = LM4 + L06 + L010 + L04 + I1 \cdot L09 + (L*36 + LB* + DB) \cdot (L*34 + LA* + DA + L03)$ $= LHR + LM4 + L03 \cdot (L*36 + LB* + DB)$	(1)

INTERMEDIATE EVENTS

$$LA* = L4 + LM1 + LM2 + LT1 \cdot L011 + L14 + L*X1$$

$$LB* = L6 + LM3 + LM4 + LT2 \cdot L012 + L15 + L*X2$$

$$L*X1 = ACA* + DCA* + DA*$$

$$L*X2 = ACB* + DCB* + DB*$$

BOOLEAN EQUATIONS REGROUPED FOR REDUCTION

TOP EVENT

$$LHR = L04 + L06 + L010 + I1 \cdot L09 + (L4 \cdot L6) + (L14 \cdot L15) + (DA \cdot DB) + D*1 \cdot D*2 + L6 \cdot L*34 + L4 \cdot L*36 + L*34 \cdot L*36 + DA \cdot (L*36 + L6 + LM3 + LM4 + LT2 \cdot L012 + L15 + D*2) + DB \cdot (L*34 + L4 + LM1 + LM2 + LT1 \cdot L011 + L14 + D*1) + D*1 \cdot (L*36 + L6 + LM3 + LM4 + LT2 \cdot L012 + L15) + D*2 \cdot (L*34 + L4 + LM1 + LM2 + LT1 \cdot L011 + L14) + L14 \cdot (L*36 + L6 + LM3 + LM4 + LT2 \cdot L012) + L15 \cdot (L*34 + L4 + LM1 + LM2 + LT1 \cdot L011) + (L*34 + L4) \cdot (LM3 + LM4 + LT2 \cdot L012) + (L*36 + L6) \cdot (LM1 + LM2 + LT1 \cdot L011)$$

(2,3)

Table K.10 Low Pressure Recirculation (B_4 -LOCA)

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

NOTES

- 1 These equations are not fully reduced since LM2 appears in LA* and LM4 appears in LB*. The term LM2·LM3 represents simultaneous maintenance outages in both legs, and are omitted since they are prohibited by Technical Specifications.
- 2 Terms representing simultaneous outages in both legs are omitted since they are prohibited by Technical Specifications.
- 3 For quantification, events L4·L6 and L14·L15 are assumed to be coupled. (See Fault Tree Quantification Tables.)

Table K.11 Low Pressure Recirculation (B_1, B_2, B_3 -LOCAs)

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

$$LPR = L04 + L010 + LRR + LIR + LRI$$

$$LRR = (L*12 + L*34 + L*X1) \cdot (L*36 + L*13 + L*X2)$$

$$LIR = (L*13 + L*36 + L*X2) \cdot (L4 + L5 + L17 + LM1 + LM2 + LX1)$$

$$LRI = (L*12 + L*34 + L*X1) \cdot (L6 + L7 + L19 + LM3 + LM4 + LX2)$$

INTERMEDIATE EVENTS

$$LX1 = ACA + DCA + DA$$

$$LX2 = ACB + DCB + DB$$

$$L*X1 = ACA* + DCA* + DA*$$

$$L*X2 = ACB* + DCB* + DB*$$

BOOLEAN EQUATIONS REGROUPED FOR REDUCTION

TOP EVENTS

$$LPR = L04 + L010 + LRR + LIR + LRI$$

$$LRR = (ACA* \cdot ACB*) + (DA* \cdot DB*) + ACA* \cdot DB* + ACB* \cdot DA* + \\ + (L*13 + L*36) \cdot (ACA* + DA*) + (L*12 + L*34) \cdot (ACB* + DB*) + \\ + (L*12 + L*34) \cdot (L*13 + L*36)$$

$$LIR = (ACB* + DB*) \cdot (ACA + DA) + \\ + (LM1 + LM2) \cdot (L*13 + L*36 + ACB* + DB*) \\ + (L4 + L5 + L17) \cdot (L*13 + L*36 + ACB* + DB*) + \\ + (ACA + DA) \cdot (L*13 + L*36) \\ = (ACA* + DA*) \cdot (ACB + DB) + \\ + (LM3 + LM4) \cdot (L*12 + L*34 + ACA* + DA*) + \\ + (L6 + L7 + L19) \cdot (L*12 + L*34 + ACA* + DA*) + \\ + (ACB + DB) \cdot (L*12 + L*34)$$

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
LA* LB*		SEE QUANTIFICATION TABLE						
L03	OPERATOR	FAILS TO OPEN VALVES DHV-7 AND DHV-8 TO PROVIDE FLOW FROM LEG B(4) TO HIGH PRESSURE TRAIN A (B), GIVEN FAILURE OF LEG A (B)			0.1	5 ⁺ , 5 ⁻	0	10
L04	OPERATOR	FAILS TO RECONFIGURE FOR RECIRCULATION	D		3.0 E-3	10 ⁺ , 10 ⁻	0	14
L06	OPERATOR	TURNS LPI OFF AND FAILS TO INITIATE	D		5.0 E-2	3 ⁺ , 10 ⁻	0	
I1	ESAS/LB3-ILB3	FAILS TO ACTUATE BOTH PUMPS						
L09	OPERATOR	FAILS TO MANUALLY INITIATE PUMPS	D		1.0 E-2	3 ⁺ , 10 ⁻	0	
L010	OPERATOR	INADVERTENTLY TERMINATES LOW PRESSURE RECIRCULATION	D		1.0 E-3	10 ⁺ , 10 ⁻	0	15
L*2	DHV-110	MAINTENANCE OUTAGE	.02/720	18	5.0 E-4	3 ⁺ , 3 ⁻	M	11
L*4	DHV-111	MAINTENANCE OUTAGE	.02/720	18	5.0 E-4	3 ⁺ , 3 ⁻	M	11
L*34		FAULTS IN LEG A RECIRCULATION LINE			1.0 E-3			
	DHV-42	FAILS TO OPEN	D		1.0 E-3	3 ⁺ , 3 ⁻		
	DHV-42 SWITCH	FAILS TO TRANSFER	D		1.0 E-5	3 ⁺ , 3 ⁻		
	DHV-42	PLUGGED	3.0 E-7	24	7.2 E-6	3 ⁺ , 3 ⁻		
					$\Sigma=1.0 E-3$			
L*36		FAULTS IN LEG B RECIRCULATION LINE			1.0 E-3			
	DHV-43	FAILS TO OPEN	D		1.0 E-3	3 ⁺ , 3 ⁻		
	DHV-43 SWITCH	FAILS TO TRANSFER	D		1.0 E-5	3 ⁺ , 3 ⁻		
	DHV-43	PLUGGED	3.0 E-7	24	7.2 E-6	3 ⁺ , 3 ⁻		
					$\Sigma=1.0 E-3$			
L4 L6		EVENT INCLUDING COUPLED VALVE FAILURES DHV-34 AND DHV-35			1.0 E-5	2 ⁺ , 2 ⁻	B	12
L14 L15		EVENT INCLUDING COUPLED PUMP FAILURES DHP-1A AND DHP-1B			1.0 E-4	2 ⁺ , 2 ⁻	B	13
DA	DHCCCS A TRAIN	INSUFFICIENT COOLING			5.8 E-3			
DB	DHCCCS B TRAIN	INSUFFICIENT COOLING			5.8 E-3			
DA-DB	DHCCCS A&B TRAINS	INSUFFICIENT COOLING			1.4 E-4			

Table K.12 (1/9) Events "LHA" and "LHB" Quantification

K-45

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L4		FAULTS COMMON TO REACTOR BUILDING SPRAY INJECTION			2.0 E-4			
	MOV DHV-34	VALVE PLUGGED	D		1.0 E-4	3 ⁺ , 3 ⁻		17
	DHV-33	CHECK VALVE FAILS TO OPEN (PLUGGED)	D		1.0 E-4	3 ⁺ , 3 ⁻		17
					<u>2.0 E-4</u>			
L14		FAULTS NOT COMMON TO REACTOR BUILDING SPRAY INJECTION			3.7 E-3			
	DHP-1A	PUMP FAILS TO START	D		1.0 E-3	3 ⁺ , 3 ⁻		
	DHP-1A	PUMP FAILS TO RUN FOR 24 HRS	3.0 E-5	24	7.2 E-4	10 ⁺ , 10 ⁻		
	CIRCUIT BKR DHP-1A	FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
	DHV-21	MANUAL VALVE LEFT CLOSED	D		1.0 E-3		H	3
	DPDP-5A FUSE IO	OPEN AND FAILURE TO RECOVER	(0.1)(1.E-6)	168	1.7 E-5	3 ⁺ , 3 ⁻		2, 9
					<u>3.7 E-3</u>			
LM1	DHP-1A	OUT FOR MAINTENANCE	.02/720	18	5.0 E-4	3 ⁺ , 3 ⁻	M	
LM2	DHV-110	OUT FOR MAINTENANCE	.02/720	18	5.0 E-4	3 ⁺ , 3 ⁻	M	
LT1+011		LEG A IN TEST AND FAILURE TO RECOVER			8.3 E-4	3 ⁺ , 3 ⁻	H	
LT1		LEG A IN TEST	2/720	3	8.3 E-3			4
L011		OPERATOR FAILS TO RECOVER FROM TEST BY CLOSING DHV-8 AND DHV-9			3.1	3 ⁺ , 3 ⁻		5
					<u>8.3 E-4</u>			
L*X1		TRAIN A SYSTEM INTERFACE FAULT			1.7 E-3			
ACA*	AC TRAIN A	INSUFFICIENT POWER			c			6, 7
DCA*	DC TRAIN A	INSUFFICIENT POWER			c			8
DA*	DHCCCS A TRAIN	INSUFFICIENT COOLING			1.7 E-3			

Table K.12 (2/9) Events "LA*" Quantification (See Note 1)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L6	DHV-35	FAULTS COMMON TO REACTOR BUILDING SPRAY INJECTION			2.0 E-4			
		VALVE PLUGGED	D		1.0 E-4	3 ⁺ , 3 ⁻		17
	CHECK VALVE DHV-36	FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		17
					$\pi=2.0 E-4$			
L15		HARDWARE FAULTS NOT COMMON TO REACTOR BUILDING SPRAY INJECTION			3.7 E-3			
	DHP-1B	PUMP FAILS TO START	D		1.0 E-3	3 ⁺ , 3 ⁻		
	DHP-1B	PUMP FAILS TO RUN FOR 24 HRS	3.0 E-5	24	7.2 E-4	10 ⁺ , 10 ⁻		
	DHP-1B CIRCUIT BREAKER	FAILS TO CLOSE	D		1.0 E-3			
	DHV-32	MANUAL VALVE LEFT CLOSED	D		1.0 E-3		H	3
	DPDP-5B FUSE 10	FAILS OPEN	1.0 E-6	168	1.7 E-4	3 ⁺ , 3 ⁻		2
	OPERATOR	FAILS TO RECOVER			0.1			
					$\pi=1.7 E-3$			
					$\pi=3.7 E-3$			
LM3	DHP-1B	OUT OF SERVICE	.02/720	18	5.0 E-4	3 ⁺ , 3 ⁻	M	
LM4	DHV-111	OUT OF SERVICE	.02/720	18	5.0 E-4	3 ⁺ , 3 ⁻	M	
LT24.012		LEG 6 IN TEST AND FAILURE TO RECOVER			3.3 E-4	5 ⁺ , 3 ⁻	H	
LT2		LEG B IN TEST	2/720	3	6.7 E-3			4
LJ12		OPERATOR FAILS TO RECOVER FROM TEST BY CLOSING DHV-7 OR DHV-9			0.1	3 ⁺ , 3 ⁻		5
					$\pi=8.3 E-4$			
L*X2		INTERFACING SYSTEM FAULTS			1.7 E-3			
ACB*		AC TRAIN B						6, 7
		INSUFFICIENT POWER						
BCC*		DC TRAIN B						8
		INSUFFICIENT POWER						
DB*		DHCCCS-B						
		INSUFFICIENT COOLING			1.7 E-3			

K-47

Table K.12 (3/9) Event "LB*" Quantification (See Note 1)

Table K.12 (4/9) Event "LPR" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L04	OPERATOR	FAILS TO RECONFIGURE FOR RECIRCULATION	D		3.0 E-3	10 ⁺ , 10 ⁻	0	14
L010	OPERATOR	INADVERTENTLY TERMINATES LOW PRESSURE RECIRCULATION	D		1.0 E-3	10 ⁺ , 10 ⁻	0	15

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L*12		SINGLE HARDWARE FAULTS THAT ARE NOT COMMON TO OTHER SYSTEMS (TRAIN A)			7.2 E-4			
	PUMP DHP-1A	FAILS TO CONTINUE TO RUN	3.0 E-5	24	7.2 E-4			
L*13		SINGLE HARDWARE FAULTS THAT ARE NOT COMMON TO OTHER SYSTEMS (TRAIN B)			7.2 E-4			
	PUMP DHP-1B	FAILS TO CONTINUE TO RUN	3.0 E-5	24	7.2 E-4			
L*34		FAULTS IN TRAIN A COMMON TO CONTAINMENT SPRAY			1.0 E-3			
	MOV DHV-42	NC VALVE FAILS TO OPEN	D		1.0 E-3			
	DHV-42 SWITCH	FAILS TO TRANSFER	D		1.0 E-5			
	DHV-42	PLUGGED	3.0 E-7	24	7.2 E-6			
					$\Sigma=1.0 E-3$			
L*36		FAULTS IN TRAIN B COMMON TO CONTAINMENT SPRAY			1.0 E-3			
	MOV DHV-43	NC VALVE FAILS TO OPEN	D		1.0 E-3			
	DHV-43 SWITCH	FAILS TO TRANSFER	D		1.0 E-5			
	DHV-43	PLUGGED	3.0 E-7		7.2 E-6			
					$\Sigma=1.0 E-3$			
L*X1		TRAIN A SYSTEM INTERFACE FAULTS			1.7 E-3			
ACA*		AC TRAIN A						
		INSUFFICIENT POWER			e			
DCA*		DC TRAIN A						
		INSUFFICIENT POWER			e			
DA*		DHCCCS-A						
		INSUFFICIENT COOLING			1.7 E-3			
L*X2		TRAIN B SYSTEM INTERFACE FAULTS			1.7 E-3			
ACB*		AC TRAIN B						
		INSUFFICIENT POWER			e			
DCB*		DC TRAIN B						
		INSUFFICIENT POWER			e			
DB*		DHCCCS-B						
		INSUFFICIENT COOLING			1.7 E-3			

K-49

Table K.12 (5/9) Event "LRR" Quantification

Table K.12 (6/9) Event "LIR" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L*06		FAULTS IN TRAIN B COMMON TO CONTAINMENT SPRAY (SEE LRR TABLE)			1.0 E-3			
L*13		SINGLE HARDWARE FAULTS NOT COMMON TO OTHER SYSTEMS (SEE LRR TABLE)			7.2 E-4			
L*X2		TRAIN B SYSTEM INTERFACE FAULTS (SEE LRR TABLE)			1.7 E-3			
L4		FAULTS COMMON TO CONTAINMENT SPRAY (SEE LA TABLE)			2.0 E-4			
L5		FAULTS NOT COMMON TO OTHER SYSTEMS (SEE LA TABLE)			3.2 E-3	3 ⁺ , 3 ⁻	H	
L11		DHP-1A OUT FOR MAINTENANCE (SEE LA TABLE)			5.0 E-4	3 ⁺ , 3 ⁻	M	
L12		DHV-110 OUT FOR MAINTENANCE (SEE LA TABLE)			5.0 E-4	3 ⁺ , 3 ⁻	M	
LX1		SYSTEM INTERFACE FAULTS: ONLY DHCCCS TRAIN A, NON LOSP (SEE LA TABLE)			5.8 E-3			16
L17		RECOVERABLE TRAIN A FAULTS NOT RECOVERED			8.5 E-4	3 ⁺ , 3 ⁻	0	
L2 L013		DHV-5 DOES NOT RECEIVE ESAS AND OPERATOR DOES NOT RECOVER			e			
L2 L013		DHV-5 DOES NOT RECEIVE ESFAS (ILB3)	D		e			
L013		OPERATOR FAILS TO RECOVER			0.1	3 ⁺ , 3 ⁻	0	
					$\pi=e$			
LT1 L014		LEG A IN TEST AND OPERATOR DOES NOT RECOVER			8.3 E-4			
LT1 L014		LEG A IN TEST		3	8.3 E-3			
L014		OPERATOR FAILS TO RECOVER			0.1	3 ⁺ , 3 ⁻	0	
					$\pi=8.3 E-4$			
L1 L015		DHP-1A DOES NOT RECEIVE ESFAS			e			
L1 L015		PUMP DHP-1A DOES NOT RECEIVE ESFAS (ILB3)	D		e			
L015		OPERATOR FAILS TO RECOVER			0.1	3 ⁺ , 3 ⁻	0	
					$\pi=e$			

K-50

Table K.12 (7/9) Event "LIR" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	ENS	NOTES
L21 L016		NO POWER FROM DPDP-5A FUSE 10 AND OPERATOR DOES NOT RECOVER	1.0 E-6	168	1.7 E-5			
L21 L016		NO POWER FROM DPDP-5A FUSE 10 BLOWN OPERATOR DOES NOT RECOVER	D		0.1 = 1.7 E-5	3+, 3-	0	
					t=8.5 E-4			

K-52

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L*34		FAULTS IN TRAIN A COMMON TO CONTAINMENT SPRAY (SEE LRR TABLE)			1.0 E-3			
L*12		TRAIN A FAULTS NOT COMMON TO OTHER SYSTEMS (SEE LRR TABLE)			7.2 E-4			
L*X1		TRAIN A SYSTEM INTERFACE FAULTS (SEE LRR TABLE)			1.7 E-3			
L6		FAULT COMMON TO CONTAINMENT SPRAY (SEE LB TABLE)			2.0 E-4			
L7		FAULTS NOT COMMON TO OTHER SYSTEMS (SEE LB TABLE)			3.2 E-3	3 ⁺ , 3 ⁻	H	
LN3		DHP-1B OUT FOR MAINTENANCE (SEE LB TABLE)			5.0 E-4	3 ⁺ , 3 ⁻	M	
LN4		DHV-111 OUT FOR MAINTENANCE (SEE LB TABLE)			5.0 E-4	3 ⁺ , 3 ⁻	M	
LX2		SYSTEM INTERFACE FAULTS: DB, NON LOSP ONLY (SEE LB TABLE)			5.8 E-3			16
L19		RECOVERABLE TRAIN B FAULTS NOT RECOVERED			8.5 E-4	3 ⁺ , 3 ⁻	0	
L2* L013		DHV-6 DOES NOT RECEIVE ESFAS AND OPERATOR DOES NOT RECOVER			ϵ			
L2 L013		DHV-6 DOES NOT RECEIVE ESFAS (ILB3) OPERATOR FAILS TO RECOVER	D		ϵ 0.1	3 ⁺ , 3 ⁻	0	
LT2* L014		LEB B IN TEST AND OPERATOR DOES NOT RECOVER			$\pi = \epsilon$			
LT2 L014		LEG B IN TEST OPERATOR FAILS TO RECOVER		3	8.9 E-4 8.9 E-3 0.1	3 ⁺ , 3 ⁻	0	
LT2* L015		DHP-1B DOES NOT RECEIVE ESFAS			$\pi = 8.9 E-4$			
L1 L015		PUMP DHP-1B DOES NOT RECEIVE ESFAS (ILB3) OPERATOR FAILS TO RECOVER	D		ϵ ϵ 0.1	3 ⁺ , 3 ⁻	0	
					$\pi = \epsilon$			

Table K.12 (8/9) Event "LRI" Quantification

Table K.12 (3/9) Event "LRI" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L23 L016		NO POWER FROM DPDP-5B FUSE 10 AND OPERATOR DOES NOT RECOVER	D		1.7 E-5			
L23 L016		NO POWER FROM DPDP-5B FUSE 10 BLOWN OPERATOR DOES NOT RECOVER	D		1.7 E-4			
					0.1		3 ⁺ , 3 ⁻	0
					$\pi=1.7 \text{ E-5}$			
					$\Sigma=6.9 \text{ E-4}$			

Table K.12 (1/2) Fault Tree Quantification Tables

NOTES

- 1 Only faults upstream of crossover contribute to LA* or LB*.
- 2 Fault duration time is 1/2 of 2 weeks, since fuse is tested bi-weekly via pump tests.
- 3 This fault represents the human error of leaving the valve closed following pump maintenance. The unavailability is estimated as follows: (0.22 maintenance acts per month) X (1.0 E-2 per act) X (360/720 months fault duration).
- 4 Each leg is operated for about 3 hours every two weeks to recirculate BWST water.
- 5 The probability of 0.1 is assumed. Recovery involves closing manual valves, but several hours or more would be available before the system is required.
- 6 See appropriate fault tree analysis.
- 7 For loss of offsite power transients, this fault is assumed to be recovered, even if the diesel fails, by the time the system is required.
- 8 DA* includes all faults in DA except failure of the diesel in the case of loss of offsite power transients. Similarly for DB*.
- 9 The probability of 0.1 is assumed. Recovery involves identifying the open fuse and replacing it, but several hours or more would be available before the system is required.
- 10 This fault involves failure to provide an alternative flow path by reconfiguring valves DHV-7 and DHV-8. Procedures do not require this operation, but it is an obvious alternative and sufficient time is available to perform the act.
- 11 LM2 also appears in LA*; LM4 also appears in LB*. The indicated valve is isolated when it is out of service for maintenance, and it is conservatively assumed that the valve bonnet has been removed. Under these conditions, neither leg could provide adequate flow, even if the crossover valves were open.

Table K.12 (2/2) Fault Tree Quantification Tables

NOTES

- 12 The event L4-L6 was evaluated assuming coupled failures between valves DHV-34 and DHV-35. A coupling coefficient (conditional probability of failure of both valves, given failure of one valve, or β factor) of 0.1 was assumed.
- 13 The event L14-L15 was evaluated assuming coupled failures between pumps DHP-1A and DHP-1B. A coupling coefficient (conditional probability of failure of both pumps, given failure of one pump or β factor) of 0.1 was assumed.
- 14 This fault might occur in several different ways:
- (a) The operator fails to open the recirculation valves DHV-42 and DHV-43.
 - (b) Operator opens recirculation valves, but fails to close the injection line suction valves DHV-34 and DHV-35 (this may not fail the system).
 - (c) Operator closes the injection line valves before opening the recirculation valves, and the time between these acts is sufficiently large to fail the pumps.
- 15 This fault was included since the operator is required by procedure to terminate operation of the low pressure pumps when they are activated by ESFAS during the injection phase.
- 16 For the events LX1 and LX2, the non loss of the offsite power numbers for DHCCCS Trains A and B are used, since it is assumed that offsite power is restored by the recirculation phase.
- 17 It is assumed that if the suction line from the BWST is plugged (or the MOV closed) when the LP pump is turned on, it will cavitate and eventually fail. This fault may occur when the pump is automatically actuated by an ESAS signal or when the operator starts the pump prior to reconfiguring the suction lineup to the sump for LPR.

Table K.13 (1/2) Low Pressure Recirculation Quantification Summary (B₄ LOCA)

BOOLEAN VARIABLE	POINT ESTIMATES
L4	2.0 E-4
L14	3.7 E-3
LM1	5.0 E-4
LM2	5.0 E-4
LT1·L011	8.3 E-4
LT1	8.3 E-3
L011	0.1
L*X1	1.7 E-3
ACA*	ε
DCA*	ε
DA*	1.7 E-3
L6	2.0 E-4
LM3	5.0 E-4
LM4	5.0 E-4
LT2·L012	8.3 E-4
LT2	8.3 E-3
L012	0.1
L15	3.7 E-3
L*X2	1.7 E-3
ACB*	ε
DCE*	ε
DB*	1.7 E-3
LA*	7.7 E-3
LB*	7.7 E-3
L03	0.1
L04	3.0 E-3

Table K.13 (2/2) Low Pressure Recirculation - Quantification Summary (B₄ LOCA)

BOOLEAN VARIABLE	POINT ESTIMATES
L06	5.0 E-2
I1	ε
L09	1.0 E-2
L010	1.0 E-3
LM2	5.0 E-4
LM4	5.0 E-4
L*34	1.0 E-3
L*36	1.0 E-3
L4·L6	1.0 E-5
L14·L15	1.0 E-4
L17	8.5 E-4
L19	8.5 E-4

Table K.14 Low Pressure Recirculation - Quantification Summary
(B₁, B₂, B₃ LOCAs)

BOOLEAN VARIABLE	POINT ESTIMATES
L04	3.0 E-3
L010	1.0 E-3
L*12	7.2 E-4
L*13	7.2 E-4
L*34	1.0 E-3
L*36	1.0 E-3
L*X1	1.7 E-3
ACA*	ε
DCA*	ε
DA*	1.7 E-3
L*X2	1.7 E-3
ACB*	ε
DCB*	ε
DB*	1.7 E-3
L4	2.0 E-4
L5	3.2 E-3
LM1	5.0 E-4
LM2	5.0 E-4
LX1	5.8 E-3
L17	8.5 E-4
L6	2.0 E-4
L7	3.2 E-3
LM3	5.0 E-4
LM4	5.0 E-4
LX2	5.8 E-3
L19	8.5 E-4

APPENDIX L

REACTOR BUILDING EMERGENCY COOLING SYSTEM (RBECS)*

*The RBECS is the emergency operating mode of the Reactor Building Cooling System (RBCS).

APPENDIX L REACTOR BUILDING EMERGENCY COOLING SYSTEM (RBECS)

L.1 SYSTEM DESCRIPTION AND OPERATION

Two redundant and diverse cooling systems are provided to cool the Reactor Building (RB) atmosphere during post accident time periods. RB cooling is necessary in order to prevent overpressurization and potential subsequent failure. The Reactor Building Emergency Cooling System (RBECS) is the first source of heat removal. The Reactor Building Spray System (RBSS) in conjunction with the Decay Heat Removal System (DHRS) provide a redundant heat removal capability. A simplified schematic is shown in Figure L.1.

The RBECS consists of three fan/cooler assemblies. This system is independent and diverse from the spray system. The RBECS simply circulates containment air through the coolers. During emergency service, the heat load from the fan coolers is diverted to the Nuclear Services Closed Cycle Cooling System (NSCCCS).

L.1.1 SYSTEM DESCRIPTION

The RBECS is comprised of three large fan assemblies. A schematic diagram of the fan system is shown in Figure L.1. Each assembly consists of an air to water heat exchanger, a fan, fan motor, a roughing filter to act as a demister, and associated ducting. The ducting inlets are distributed throughout the upper containment. There is one common ducting system for all three fans. Two of the fans are located at EL 95 (bottom of the reactor building) and the third at EL 119. The air from the lower fans is discharged into the reactor building at EL 102. The air from the upper fan is discharged into the reactor building at EL 135.

Power for the fans is supplied by the 480V ESMCC's, one fan being on each of the 3A, 3B and AB centers. This way, failure of either 480V train will only fail one fan. Each fan has two motor coils, a high speed coil for normal operation and a low speed coil for emergency operation. Two fans operate during normal plant operation. Back pressure dampers in the ducting restrict airflow to the inactive fan assembly.

The cooling water flow to all three cooler assemblies is provided by the industrial cooling system during normal plant operation. During emergency operation the fan cooling water supply is switched to the NSCCCS to accommodate the increased heat load.

The lines to and from the individual coolers penetrate the containment. Each line has a containment isolation valve. Manual block valves are provided on either side of the isolation valves. Differential flow meters are provided on each side of the cooler to detect leaks in the cooler assembly. The differential flow meters are displayed and annunciated in the control room. The fan is the only other instrumented component in the system. Annunciated in the control room are the high speed coil trip, low air flow, and fan assembly vibration. The fan motor bearing temperature is computer alarmed. Major component data are listed in Table L.1.

L.1.2 SYSTEM OPERATION

Cooling water flows through all three coolers continuously, regardless of the status of the fan. The water flow is 530 gpm/air handling unit. The cooling water outlet temperature of 85°F is raised by 8°F. During normal operation the heat load per fan assembly is 2×10^6 BTU/hr. The post-LOCA saturated condition of the containment atmosphere raises the heat load to 80×10^6 BTU/hr per fan assembly. In order to accommodate this emergency heat load, the fan coils are switched over to the NSCCCS. The cooling water flow rate increases to 1700 gpm/assembly, the inlet temperature rises to 105°F. The emergency mode of the fans is activated by the ESAS when the reactor building pressure reaches 4 psig.

The configuration changes necessary on an ESAS are summarized below:

- (1) The high speed coil on the fan is de-energized and the low speed coil is energized. This is to compensate for the increased pumping requirements of the fans in the saturated containment atmosphere.
- (2) The third fan is activated. During normal operation, only two fans are operating. The third is activated to provide redundancy. Airflow through the inactivated cooler is restricted by a set of back pressure, gravity flow dampers. These are expected to open automatically when the fan starts.
- (3) The heat load is switched from the industrial cooler to the NSCCCS. This is necessary because of the larger heat loads in the emergency mode as opposed to the normal mode of operation. The inlet and outlet valves (SWV-354 and 353) are opened to connect the fans to the NSCCCS. Inlet and outlet valves from the industrial cooler (SWV-151, 152, 355) are closed.

No requirement for valve alignment checks exists because the fans are a normally operating system. Each fan is required to be demonstrated operable monthly on a staggered test basis (SP-344). The fan has to be operated for 15 minutes and a coolant flow of 500 gpm must be verified. SWV-353 and 354 are stroked once a quarter. Technical Specification 3.6.2.3 requires that two fans be available for normal plant operation. Normal plant operation with only one fan available is limited to 72 hours.

Table L.1 (1/2) Reactor Building Cooling Unit Performance and Equipment Data
 (Capacities are on a per air handling unit basis.)

Performance Data	Duty	
	Emergency	Normal
No. Installed	3	3
Type Coil	Finned Tube	Finned Tube
Design Heat Load, Btu/h	80×10^6	2.15×10^6
Fan Capacity, cfm	54,000	108,000
Reactor Building Atmosphere Inlet Conditions		
Temperature, F	281	110
Steam Partial Pressure, psia	49.99	---
Air Partial Pressure, psia	18.31	---
Total Pressure, psia	68.30	Atmospheric
Cooling Water Flow, gpm	1,780	530
Cooling Water Inlet Temperature, F	105	85
Cooling Water Outlet Temperature, F	183	93.1

Equipment Construction Data

Item	Description
Coil Tubes	5/8 in. OD seamless copper with 0.049 in. wall
Coil Fins	0.008 in. thick copper spaced 8.5 per inch
Coil Header	Schedule 40 steel pipe
Plenum Casing	1/4 in. steel plate
Fan Casing	1/4 in. steel plate
Motor	Pipe ventilated--air to water heat exchanger
Casing Material	ASTM A-36

Table L.1 (2/2) Reactor Building Cooling Unit Performance and Equipment Data
 (Capacities are on a per air handling unit basis.)

Summary of Requirements for
 Reactor Building Fan Cooling Units

Item	Acceptance Standard
Cooling Coils	
Tubes and Fins Hydrostatic Test	ASTM Material Specification ASME Section VIII
Demisters	ASTM Material Specification
Casing and Miscellaneous Parts Painting	ASME Material Specification SSPCS SP-1063T
Piping	
Fabrication, Welding, and Inspection	USAS B31.1
Seismic Requirements	Seismic Class I
Motors	NEMA MG-1, ANSI C50.2 and 50.20, IEEE

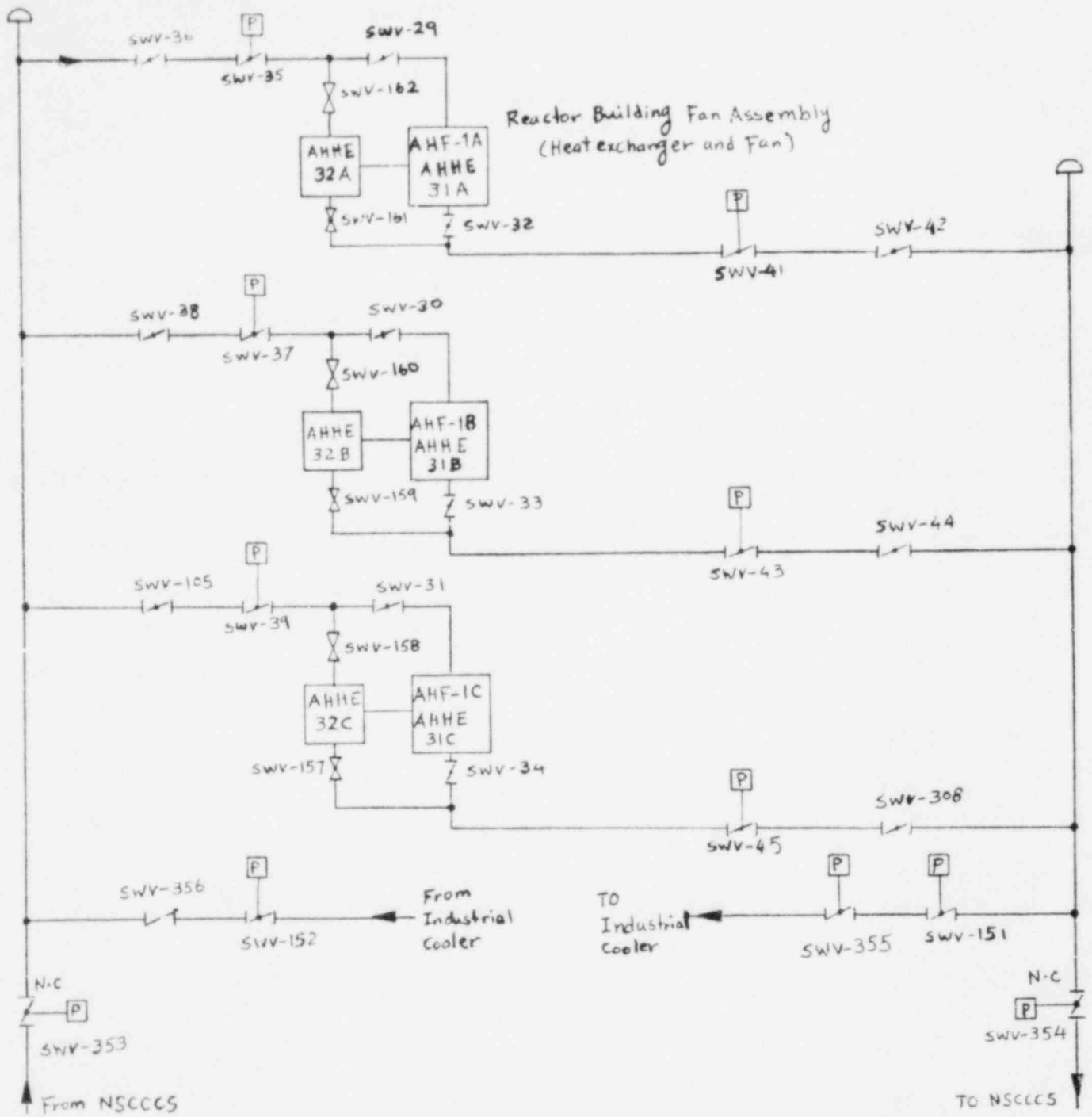


Figure L.1 Reactor Building Emergency Cooling System Schematic Diagram

L.2 SYSTEM SIMPLIFIED FAULT TREE

The detailed fault tree, initially drawn for the RBECS, was simplified in a series of intermediate steps. The simplified fault tree is shown in Figure L.2.

The top event for the fault tree is defined as:

Failure of all fans - failure of at least one fan cooler to operate at rated emergency conditions.

MAJOR ASSUMPTIONS

The major assumptions used to construct the detailed fault tree are listed below:

1. Technical Specification 3.6.2.3 allows operation with only one operable fan for 72 hours. This situation is accounted for in the fault tree.
2. The fans are normally operating and can therefore be expected to have the correct valve alignment at ESAS initiation. However, since one fan is inactive during normal plant operation, there is a possibility it will not have correct valve alignment. Each assembly is required (T.S. 4.6.2.3) to be tested and flow verified, once a month. Each cooler is flow monitored in the control room. Valve mispositions were only listed for the inactive cooler assembly.
3. If the high speed coil is not de-energized, the fan motor will overheat and burn out.
4. Missile damage was assumed possible to the ducting and piping which would fail the fan cooling system, although unlikely.
5. SWV-353 and SWV-354 are stroked once a month, per SP-351.
6. The fan motors and bearings are self-cooled.
7. Airflow across the inactive cooler is zero. Full NSCCCS flow continues through the cooler. Back-pressure gravity dampers starve the airflow. They should open when the fan motor starts.

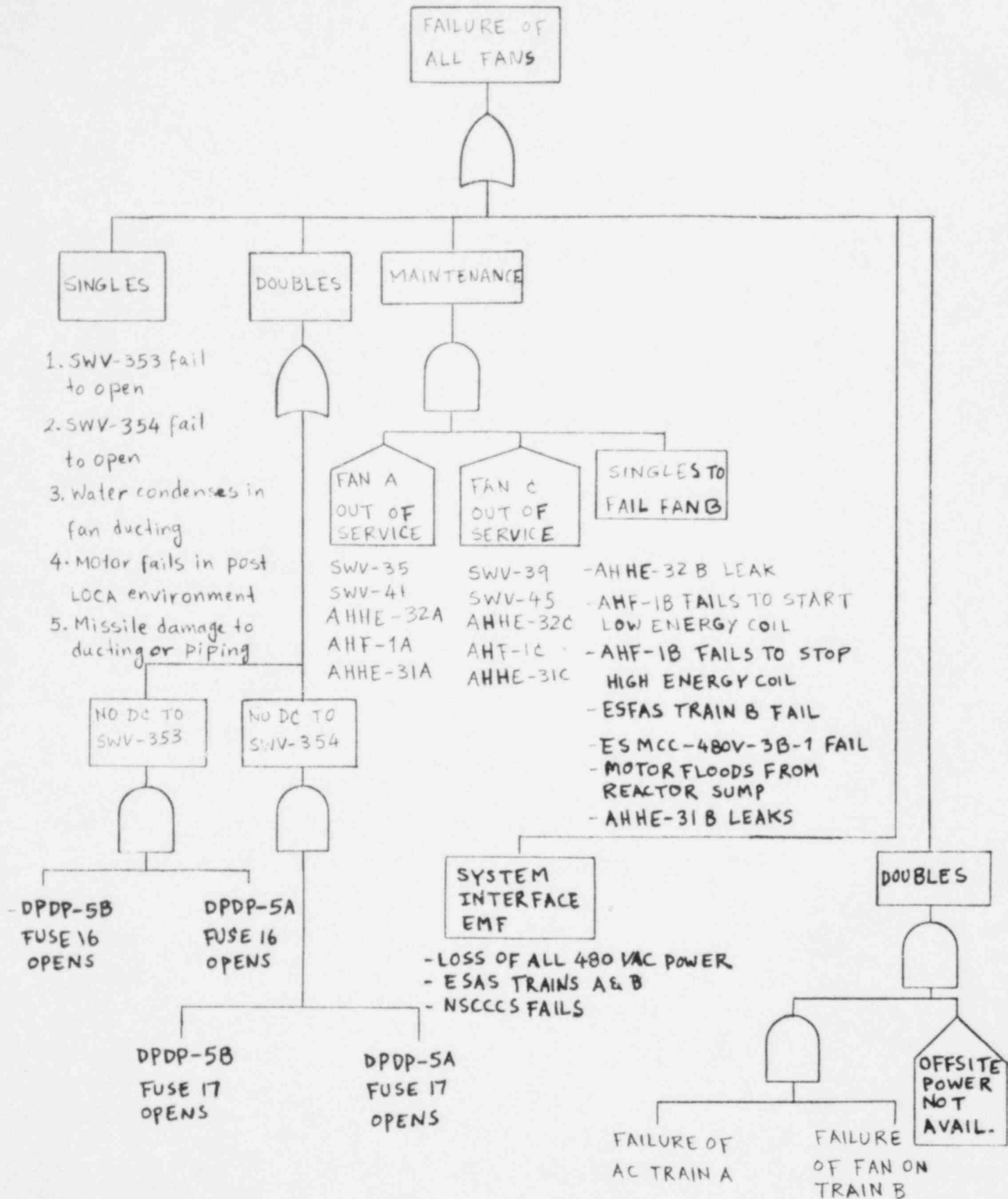


Figure L.2 Simplified Fault Tree - RBECs

L.3 SYSTEM QUANTIFICATION

L.3.1 SYSTEM RELIABILITY CHARACTERISTICS

For cases where offsite power is available the main contributor to the unavailability of the RBECS during the injection phase is failure to admit cooling to the fans from the NSCCCS. Cooling water from the NSCCCS is admitted to the fan coolers when the air-operated valves SWV-353 and -354 receive an ESAS signal. However, if offsite power is not available the dominant contributor to the system's unavailability is failure of both diesels to start and power from both units CR-1 and -2 is not available (the unavailability of both fossil units was assessed as 0.36).

About a factor of two smaller is the probability that the NSSWS does not remove heat from the NSCCCS. Failure of both seawater pumps (RWP-2A and 2B) to start or failure of the check valves in the pump discharge to open are the main contributors. The remainder of the failures responsible for the unavailability of RBECS are at least one order of magnitude smaller than the above. They are mainly hardware failures in the NSCCCS. The unavailability of the RBECS during the recirculation phase is dominated by the failure of all fans to run. Failure of all fans to run was assessed as a strongly coupled failure since the three fans operate in the same severe post-LOCA containment atmosphere. The unavailability of RBECS is about the same for both post-accident phases.

L.3.2 SYSTEM FAULT TREE QUANTIFICATION - INJECTION PHASE*

This section presents the quantification of the RBECS unavailability for emergency operation during the injection phase of a postulated accident. The quantitative results are presented in table form with attached notes outlining the assumptions. To perform the fault tree quantification the simplified fault tree presented in Section L.2 was transformed into a modularized fault tree.

Table L.2 shows the RBECS success requirements. Table L.3 contains the top event definitions for the modularized fault tree. The unavailability of each gate is shown on the tree, Figure L.3. Table L.4 shows the Boolean equations that represent the fault tree. Table L.5 shows the quantification of each gate by component and failure mode. Table L.6 summarizes the point estimates for each gate.

*The RBECS is analyzed in terms of its fan cooler availability. Therefore, the RBECS is referred to as "fan coolers" in this and the following section.

Table L.2 Fan Coolers - Injection

SUCCESS REQUIREMENTS

INITIATOR

TRAINS

NOTES

B₁, B₂, B₃, B₄

1/3 fans

Table L.3 Fan Coolers - Injection

TOP EVENT DEFINITION

BOOLEAN
REPRESENTATION

TOP EVENT

NOTES

FCI

Failure of fan cooler system to provide at least 1/3 fan cooling to containment during injection phase.

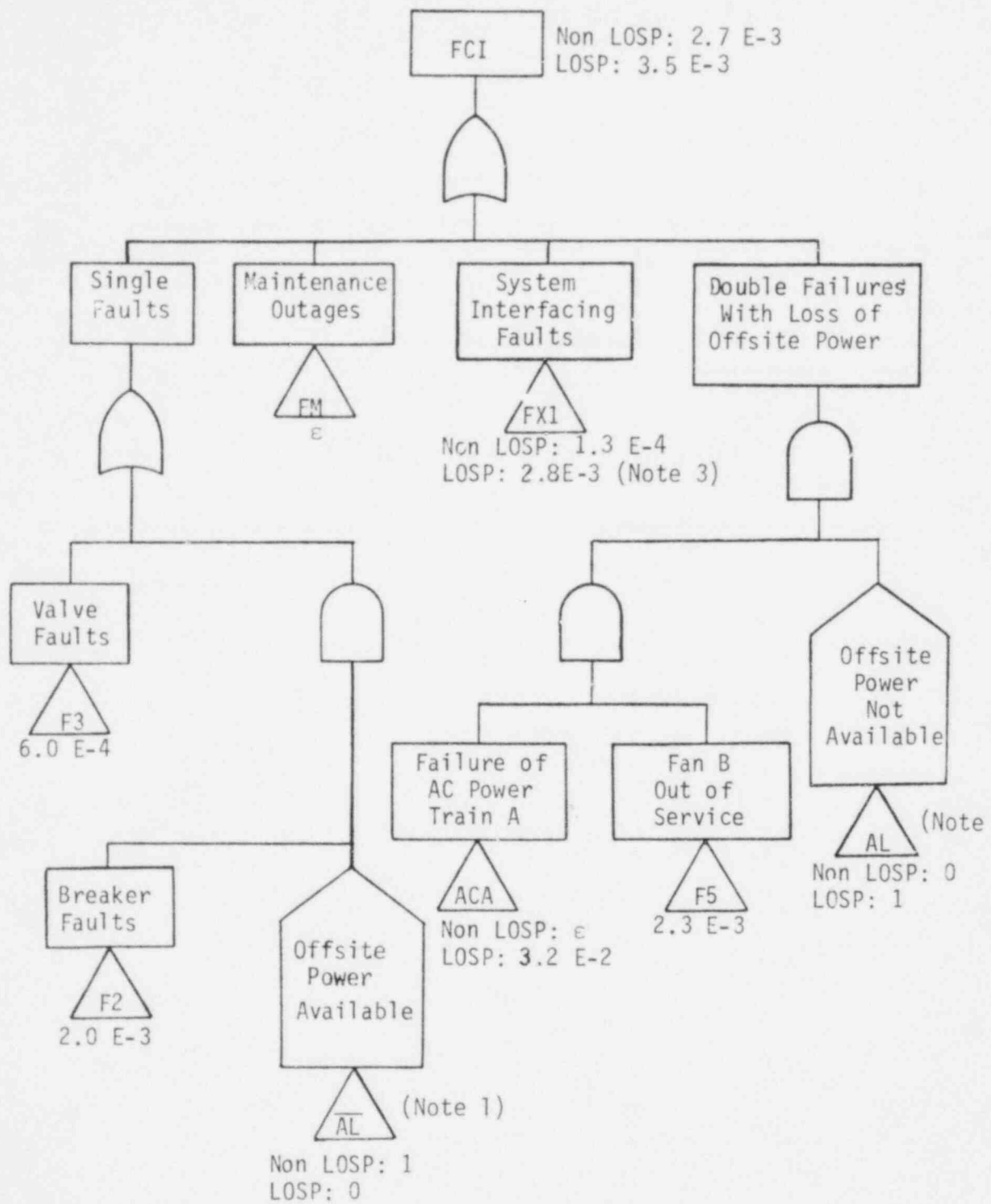


Figure L.3 Modularized Fault Tree for Event "FCI"

Figure L.3 Fan Coolers - Injection

FAULT TREE

NOTES

- 1 For cases where offsite power is available, house \overline{AL} is one; for cases where offsite power is not available house \overline{AL} is zero.
- 2 AL is the complement of house \overline{AL} . For cases where offsite power is available, house AL is zero; for cases where offsite power is not available house AL is one.
- 3 This value was obtained from a Boolean reduced form of $N + ACA \cdot ACB + DCA \cdot DCB$.

Table L.4 Fan Coolers - Injection

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREE

TOP EVENT

NOTES

$$FCI = \overline{AL} \cdot F2 + F3 + FX1 + AL \cdot ACA \cdot F5 + FM$$

(1,2)

BOOLEAN EQUATION WITH TERMS REGROUPED FOR SEQUENCE ANALYSIS

$$FCI = F4 + FX1 + AL \cdot ACA \cdot F5$$

$$F4 = \overline{AL} \cdot F2 + F3 + FM$$

$$FX1 = N + ACA \cdot ACB + DCA \cdot DCB$$

-
- NOTES:
1. Maintenance outage contributions are negligible for this system since it was assumed that only very rarely would 2 fans be out for maintenance.
 2. Fans A and C are powered from AC - Train A, while fan B is powered from AC - Train B. Therefore, loss of AC - Train A and fan B out of service is a double failure to FCI. The opposite case involves triple failures and therefore is not shown on the fault tree.

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
$\bar{A}L$		HOUSE FOR AVAILABILITY OF OFFSITE POWER			1, 0			1
		NON LOSP			1			
		LOSP			0			
F2		CIRCUIT BREAKER FAULTS			2.0 E-3			
	CIRCUIT BKR SWV-353	FAILS TO TRANSFER	D		1.0 E-3	3 ⁺ , 3 ⁻		
	CIRCUIT BKR SWV-354	FAILS TO TRANSFER	D		1.0 E-3	3 ⁺ , 3 ⁻		
					$\Sigma=2.0 E-3$			
F3		VALVE FAULTS						
	PNEUMATIC VALVE SWV-353	FAILS TO OPEN	D		3.0 E-4	3 ⁺ , 3 ⁻		
	PNEUMATIC VALVE SWV-354	FAILS TO OPEN	D		3.0 E-4	3 ⁺ , 3 ⁻		
					$\Sigma=6.0 E-4$			
FN		MAINTENANCE OUTAGES			ϵ			2
FX1		SYSTEM INTERFACING FAULTS						
		NON LOSP			1.3 E-4			3
		LOSP			2.8 E-3			
ACA-ACB		AC POWER FAILS						
		NON LOSP			ϵ			
		LOSP			2.3 E-3			
H		HSCCCS FAILS TO PROVIDE COOLING (SEE QUANTIFICATION TABLES FOR N)						
		NON LOSP			1.3 E-4			
		LOSP			2.8 E-3			
$\bar{A}L$		COMPLEMENT OF $\bar{A}L$			0, 1			
		NON LOSP			0			
		LOSP			1			

Table L.5 (1/2) Event "FCI" Quantification

Table L.5 (2/2) Event "FCI" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ACA		AC TRAIN A FAILS						
		NON LOSP			c			
		LOSP			3.2 E-2			
F5		FAN B OUT OF SERVICE			2.3 E-3			
	FAN AHF-1B	FAILS TO START	D		3.0 E-4	3 ⁺ , 3 ⁻		
	CIRCUIT BKR. AHF-1B(HI)	F. ILS TO TRANSFER	D		1.0 E-3	3 ⁺ , 3 ⁻		
	CIRCUIT BKR. AHF-1B(LO)	FAILS TO TRANSFER	D		1.0 E-3	3 ⁺ , 3 ⁻		
					<u>1.0 E-3</u>			
					=2.3 E-3			

Table L.5 Fan Coolers - Injection

QUANTIFICATION TABLES

NOTES

- 1 For offsite power available, house has a value of one; for offsite power not available, house has a value of zero. On loss of offsite power air operated valves configure to open position without requiring breaker operation.
- 2 Maintenance outages were assumed to not contribute since it was assumed that only rarely would two fans be in maintenance at the same time.
- 3 After Boolean reduction, $FX1 = N$.

Table L.6 RBECS - Injection Phase Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
$\bar{A}L$	1* 0**
F2	2.0 E-3
F3	6.0 E-4
FM	ϵ
AL	0* 1**
F5	2.3 E-3
ACA	ϵ^* 3.2 E-2**
ACA·ACB	ϵ^* 2.3 E-3**

*Offsite power available
 **Offsite power not available

L.3.3 SYSTEM FAULT TREE QUANTIFICATION - RECIRCULATION PHASE

This section presents the quantification of the RBECS unavailability for emergency operation during the recirculation phase of a postulated accident. As for the injection phase, a modularized fault tree was constructed.

Table L.7 shows the RBECS success requirements. Table L.8 contains the top event definitions for the modularized tree, and Figure L.4 shows the modularized fault tree. The unavailability of each gate is shown on the tree. Table L.9 shows the Boolean equations that represent the fault tree. Table L.10 shows the quantification of each gate by component and failure mode. Table L.11 summarizes the point estimates for each gate.

Table L.7 Fan Coolers - Recirculation

SUCCESS REQUIREMENTS

INITIATOR

B₁, B₂, B₃, B₄

TRAINS

1/3 Fans

NOTES

Table L.8 Fan Coolers - Recirculation

TOP EVENT DEFINITION

BOOLEAN
REPRESENTATION

TOP EVENT

NOTES

FCR

Failure of fan cooler system to provide at least 1/3 fan cooling to containment during recirculation phase

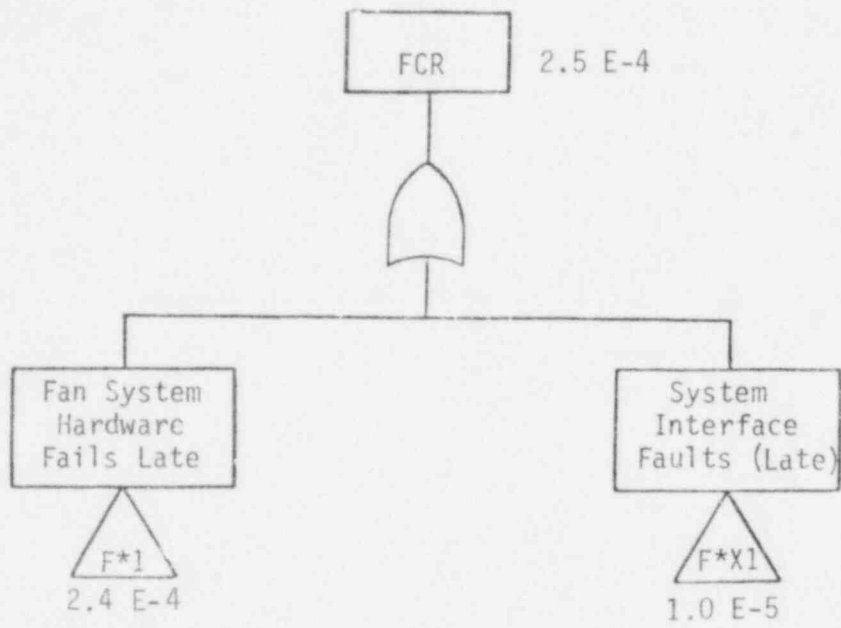


Figure L.4 Modularized Fault Tree for Event "FCR"

Table L.9 Fan Coolers - Recirculation

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREE

TOP EVENT

NOTES

$$FCR = F^*1 + F^*X1$$

INTERMEDIATE EVENTS

$$F^*X1 = N^* + ACA^* \cdot ACB^*$$

(1)

NOTES: 1. Offsite power is assumed to be recovered when entering the recirculation phase. The unavailability of AC power with offsite power available was calculated to be negligible compared to other system failure modes.

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
F*1	8 FXAS	FAN SYSTEM HARDWARE FAILS LATE FAILS IN POST-LOCA ENVIRONMENT	(1.0 E-4)(0.1)	2	2.4 E-4 2.4 E-4	2*, 2-	B	1
F*XI		INTERFACING SYSTEM FAULTS						
N*		MOCCS FAILS DURING RECIRCULATION (SEE QUANTIFICATION TABLE FOR "N")			1.0 E-5			
ACA* ACB*		AC POWER FAILS DURING RECIRCULATION						

Table L.10 Event "FCR" Quantification

Table L.10 Fan Coolers - Recirculation

QUANTIFICATION TABLES

NOTES

- 1 This fault was assessed assuming that failure of a:1
3 fans in the post-LOCA environment would be coupled.
A failure rate of 1.0 E-4/hr. was used as the basic failure rate
(intermediate between the normal and extreme environment failure
rates given in WASH-1400).

Table L.11 RBECS - Recirculation Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
F*1	2.4 E-4
ACA*·ACB*	E

APPENDIX M

REACTOR BUILDING SPRAY SYSTEM (RBSS)

M.1 SYSTEM DESCRIPTION AND OPERATION

The Reactor Building Spray System is designed to furnish reactor building atmosphere cooling to reduce the building pressure after LOCA. In addition, the sprays reduce the fission product iodine inventory from the containment atmosphere. The pressure reduction function of the sprays serves as a back-up to the reactor building emergency cooling system (RBECS, Appendix L). The RBSS is an engineered safety feature and performs no normal operating function.

M.1.1 SYSTEM DESCRIPTION

The RBSS, Figure M.1, is a once-through, two train system, taking suction from the low pressure injection system suction header and discharging into the containment atmosphere. Each of the two independent trains is rated at 100% pressure reduction and iodine removal capacity and consists of a pump, a spray header, associated piping, valves, instrumentation, and controls.

The spray pumps are powered from 4160V ES busses. Cooling to pump BSP-1A and BSP-1B is provided by Trains A and B, respectively, of the Decay Heat Closed Cycle Cooling System (DHCCCS, see Appendix F). The water source for the sprays during the injection phase is the BWST and during the recirculation phase the reactor building sump. The low pressure injection and recirculation system suction header configuration is described in Appendix K. Old connections for addition of sodium thio-sulfate to the spray water exist between check valve BSV-1 and spray pump BSP-1A in Train A and between BSV-8 and BSP-1B in Train B (see Figure M.1). However, the sodium thio-sulfate admission valves BSV-99 and 100 are locked closed (according to procedure OP-405) and the tanks are drained.

Each spray pump can discharge 1500 gpm at the rated head of 450 ft into the containment atmosphere through spray nozzles. There are 192 nozzles located on nine spray rings, evenly divided between both spray trains (4 spray rings for Train A, 5 spray rings for Train B). Each nozzle discharges 15.2 gpm at 40 psi pressure differential across the nozzle.

All motor operated valves are powered by the 480V ES MCC's.

M.1.2 SYSTEM OPERATION

The valves in the spray lines are opened by an ESAS signal if the containment pressure rises above 4 psig. The spray pumps are started by ESAS when the containment pressure reaches 30 psig. This is assumed to occur after a large LOCA. A small LOCA may not raise the containment pressure enough to actuate the sprays. However, if the sprays are needed, they can be actuated manually.

Upon low-level alarm in the BWST, the operator must start the recirculation phase by opening the sump valves and closing the BWST outlet valves (see also Appendix K). The operator is then required to throttle the spray flow to 1200 gpm by means of valve BSV-3 (BSV-4 in Train B). This flow rate corresponds to the NPSH of 22.5 feet available from the sump (a flow rate of 1500 gpm requires a NPSH of 24.8 feet).

High and low flows are alarmed in the control room. The alarm set points are automatically transferred to the lower recirculation values when the suction is reconfigured to the sump. The spray pumps are alarmed for high motor and pump bearing temperature, and for high motor starter temperature.

The spray pumps are tested on a staggered basis once a month. Testing is governed by procedure SP-340. During the test, water from the BWST is recirculated by opening valves BSV-28 and BSV-5 or BSV-6, depending on which pump is tested. All valves in the spray flow path are stroked once a quarter. Pump testing verifies position of BSV-17 and -16 and operability of BSV-1 and -8.

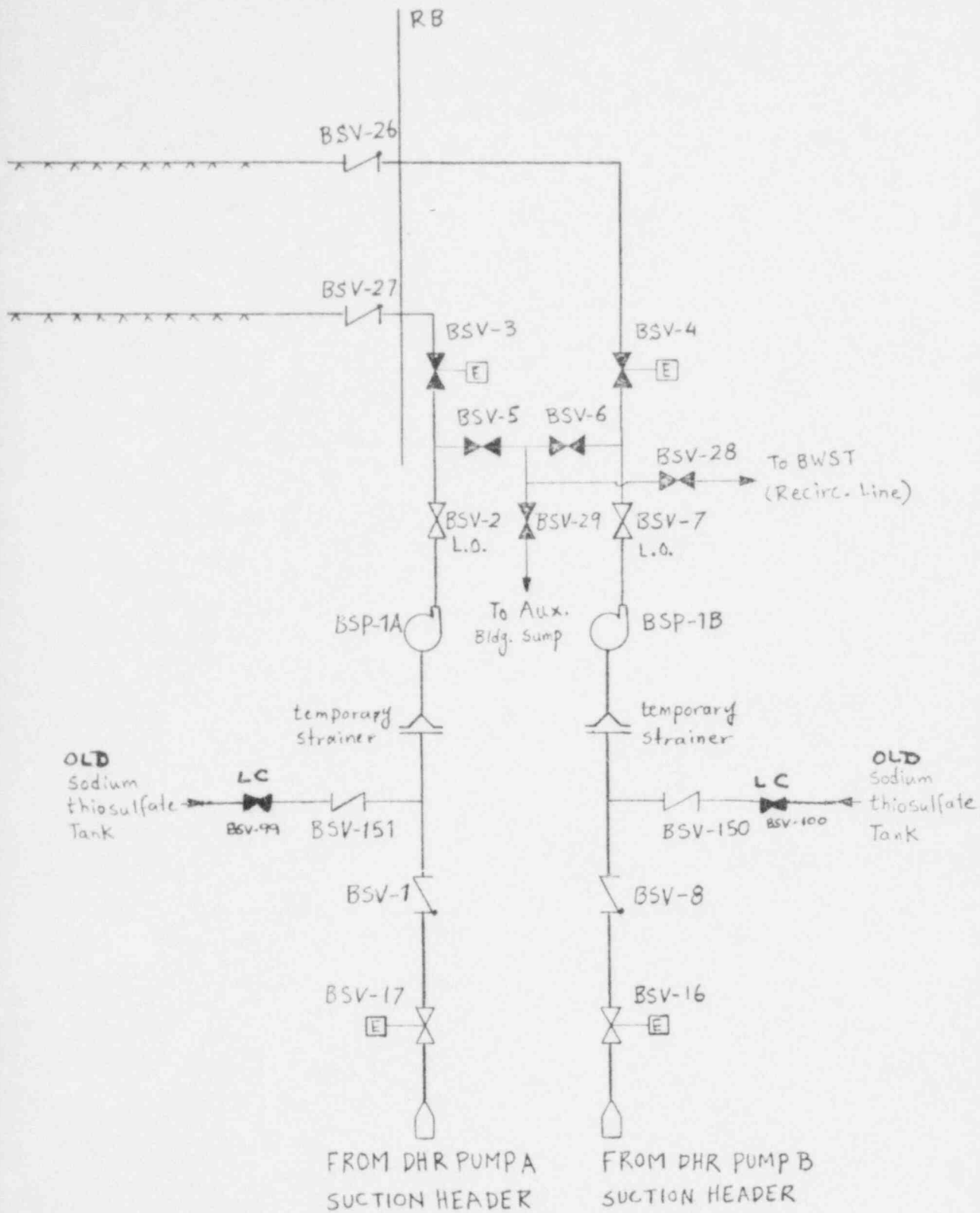


Figure M.1 Reactor Building Spray System Schematic Diagram

M.2 SIMPLIFIED FAULT TREE

A detailed fault tree was originally drawn for failure of the Reactor Building Spray System Train A. The tree included the injection and the recirculation phase. The fault tree for Train B is identical, except for corresponding component number differences.

The detailed tree then was simplified and separated into two trees, one for the injection phase and one for the recirculation phase.

The top events are defined as:

Failure of Both Sprays, Injection - failure of at least one spray train to deliver rated flow at the rated head to its respective spray nozzles while taking suction from the BWST, Figure M.2.

Failure of Both Sprays, Recirculation - failure to successfully reconfigure at least one spray train or failure to deliver rated flow at the rated head to the train's spray nozzles for 24 hours, while taking suction from the containment sump, Figure M.3.

Failure of the sprays will also fail the function of iodine removal from the containment atmosphere.

MAJOR ASSUMPTIONS

The assumptions used to construct the detailed fault tree for the RBSS are listed below:

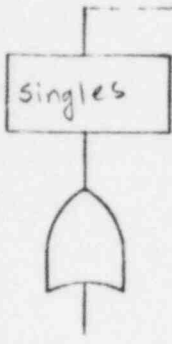
- (1) The spray system is a normally inactive system and therefore may be unavailable on demand due to maintenance, test, or improper configuration of valves. BSV-3 and 17 are motor operated valves. BSV-2 is locked open (SP-381). The valves on the cooling lines to the pumps DCV-115, 116, 27, and 33 are locked open (SP-381). BSV-2 is a manual blocking valve, locally indicated. BSV-3 and 17 are indicated in the control room.
- (2) Technical Specification 3.6.2.1 requires two spray trains to be operable. If only one is operable, the plant must be shut down in 72 hours. Plant procedure SP-347 requires valves in the flow path to be checked for position every month. Plant procedures also require the pump to be started once a month and BSV-3 and 17 stroked once a quarter. The two spray trains are tested on an alternating basis, i.e., one every two weeks. The pump is tested by opening valves BSV-28 and BSV-5 (BSV-28 and BSV-6 for BSP-1B). Flow is diverted to the BWST.

- (3) It was assumed that if cooling is lost to BSP-1A, the pump will fail immediately. This is a conservative assumption. The motor and the bearing both require cooling. All faults for the cooling function can be classified as either those which prevent flow or those which prevent heat rejection from the DHCCCS. If faults occur which prevent flow to the motor or bearing, the water in the motor or bearing will quickly heat up and in very short order the motor will short or the bearing will seize. This is particularly true in the recirculation phase where the pumped water is hotter than the motor coolant. If faults occur which prevent heat rejection from the DHCCCS, but allow flow to the pump cooler, the pump may run for some time before it fails. This is particularly true for the injection phase, when there is no heat removal from DHHE-1A. The thermal inertia of the DHCCCS may be sufficient to allow continued operation of the spray pump.
- (4) The spray nozzles cannot become plugged while they are inactive.
- (5) The operator must reduce the system flow rate from 1500 gpm to 1200 gpm by throttling BSV-3 shortly after switchover to recirculation to prevent cavitation. The NPSH required to provide a flow rate of 1500 gpm is 24.8 feet. When operating in the recirculation mode, the NPSH available to the BS pumps is only 22.5 feet. If the operator switches to recirculation based on sump height and not BWST level, and premises the switchover on DH pump NPSH requirements, the BS pumps may cavitate even if the flow rate is reduced to 1200 gpm. Cavitation was assumed to cause pump failure. Although the sprays have two independent loops, throttling of BSV-3 and BSV-4 will be done simultaneously. They are considered to be a single operator action. "Failure to throttle the valve correctly" includes:
- throttling too much to starve flow,
 - throttling too little to cause cavitation,
 - not throttling at all.

Switching on sump level rather than on BWST level is a fault because the sump may not contain sufficient water (NPSH) to prevent pump cavitation and subsequent failure of the pumps.

- (6) Upon changing from the injection phase to the recirculation phase, the entire spray system will experience a thermal shock. The BWST water is about 70°F while the reactor building sump water is about 280°F. The amount of mixing between the two streams during reconfiguration is not known. The FSAR and personnel contacts at B&W claim the spray pumps have been designed and qualified for this transient. The pump is also qualified at the higher temperature.
- (7) Components, lines, and valves that were considered to be insignificant were omitted from the fault tree.

FAILURE
BOTH S
INJECT



1. BWST rupture
2. Pump room floods
3. Both BWST breaks fail to open
4. Recirculation reconfiguration too soon.

COMMON MODE
HARDWARE



1. BSP-1A/1B fail to start
2. BSP-1A/1B fail to run
3. BSV-3/4 fail to open
4. BSV-1/8 fail to open
5. BSV-26/27 fail to open
6. DHV-36/33 fail to open
7. DCP-1A/1B fail to start
8. DCP-1A/1B fail to run
9. AHF-15B/15A fail to start
10. AHF-15B/15A fail to run
11. RWP-3A/3B fail to start
12. RWP-3A/3B fail to run
13. RWV-37/34 fail to open
14. Blockage HEPA filter AHF 15A/15B
15. Spray strainer line A/B



1. DHCCCS A-fail
2. 4160 ES-3A fail
3. ESAS train A fail
4. BSP-1A fail to start
5. BSP-1A fail to run
6. BSV-27 fail to open
7. BSV-3 fail to open
8. BSV-1 fail to open
9. DHV-33 fail to open
10. DCV-115
11. DCV-27
12. DCV-116
13. DCV-33
14. BSV-2
15. Spray strainer
16. DHV-34 plugged

N.O. manual
valve closed

DOUBLES



1. DHCCCS-B fail
2. 4160 ES-3B fail
3. ES Train B fail
4. BSP-1B fail to start
5. BSP-1B fail to run
6. BSV-26 fail to open
7. BSV-4 fail to open
8. BSV-8 fail to open
9. DHV-36 fail to open
10. DCV-117
11. DCV-118
12. DCV-28
13. DCV-34
14. BSV-27
15. spray line strainer
16. DHV-35 plugged

NOTES: 1. N.O. valves left closed
2. Each event should be considered only in combination with the event across from

E OF
RAYS
ON

1

part
un
pen
pen
pen

er, blocked
ed

it.

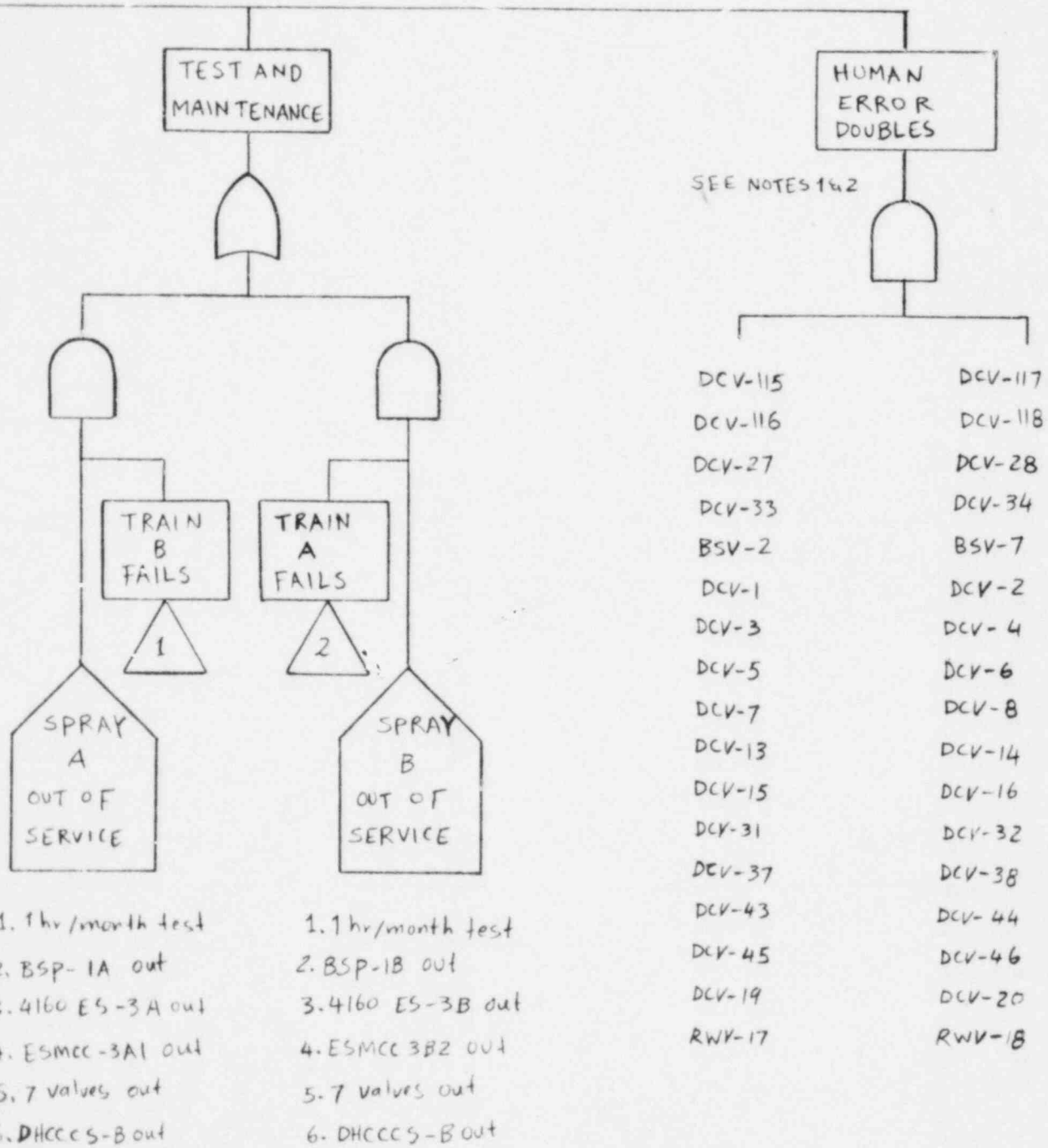


Figure M.2 Simplified Fault Tree - RBSS (Injection)

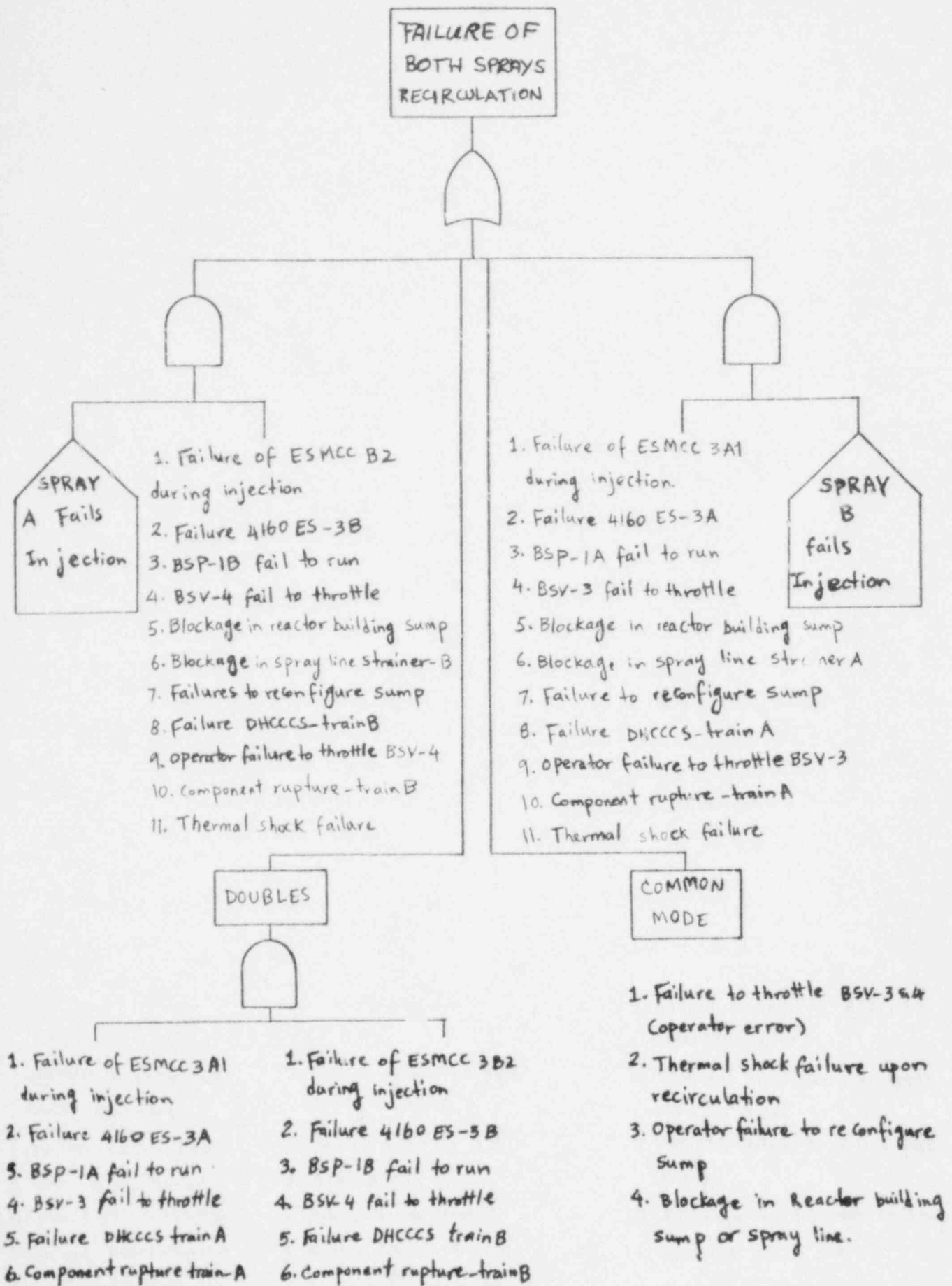


Figure M.3 Simplified Fault Tree - RBSS (Recirculation)

M.3 SYSTEM QUANTIFICATION

M.3.1 SYSTEM RELIABILITY CHARACTERISTICS

For cases where offsite power is available the major contributors to the unavailability of the RBSS during the injection phase are operator errors. For large LOCAs (B1, B2) the dominant contributor is that the operator reconfigures for recirculation too soon. For small LOCAs (B3, B4) an additional operator error of the same order of magnitude can occur: failure to manually initiate the sprays when required.

In the case that offsite power is not available, the failure of both diesels to start and unavailability of power from fossil units CR-1 and -2 (the unavailability of both fossil units was assessed as 0.36) is about an order of magnitude smaller than the probability of the first two operator errors described.

The unavailability of the RBSS during the recirculation phase is dominated by two operator errors. The first is that the operator fails to reconfigure the suction to the reactor building sump for recirculation. The second dominant contribution is that the operator fails to throttle the spray valves to prevent pump cavitation. About two orders of magnitude smaller are the contributions of nonrecoverable hardware faults during the injection phase (or a maintenance outage) in one train combined with hardware faults that occur during the recirculation phase in the other train. These failures include the DHCCCS that supplies pump cooling.

M.3.2 SYSTEM FAULT TREE QUANTIFICATION - INJECTION PHASE

This section presents the quantification of the RBSI^{*} unavailability for required emergency operation of the RBSS during the injection phase of a postulated accident. The quantitative results are presented in table form with attached notes outlining the assumptions. To perform the fault tree quantification, the simplified fault tree was transformed into a modularized fault tree.

Table M.1 shows the RBSS success requirements, Table M.2 contains the top event definition for the modularized fault tree, and Figures M.4 through M.7 show the modularized fault trees for the RBSI. The unavailability of each gate is shown on the tree. Table M.3 shows the Boolean equations that represent the fault trees. Table M.4 shows the quantification of each gate by component and failure mode. The attached notes explain the assumptions used in the quantification. Table M.5 presents a summary of the point estimates for each gate.

*RBSI; Reactor Building Spray System - Injection Phase.

Table M.1 Containment Spray Injection

SUCCESS REQUIREMENTS

<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B1, B2, B3, B4	1/2 Trains	1,2,3

-
- NOTES: 1 Success definition is the same for all LOCA sizes.
- 2 The time into the accident sequence when containment spray (CS) will be required is dependent on the size of the LOCA. However, it was assumed that CS would be required during the injection phase for all LOCA sizes
- 3 The containment spray system is used both for containment atmosphere heat removal and post accident radioactivity removal.

Table M.2 Containment Spray Injection - Top Events

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
CSA	Failure of containment spray Train A to provide containment atmosphere cooling.	
CSB	Failure of containment spray Train B to provide containment atmosphere cooling.	
CSI	Failure of both containment spray trains to provide containment atmosphere cooling.	

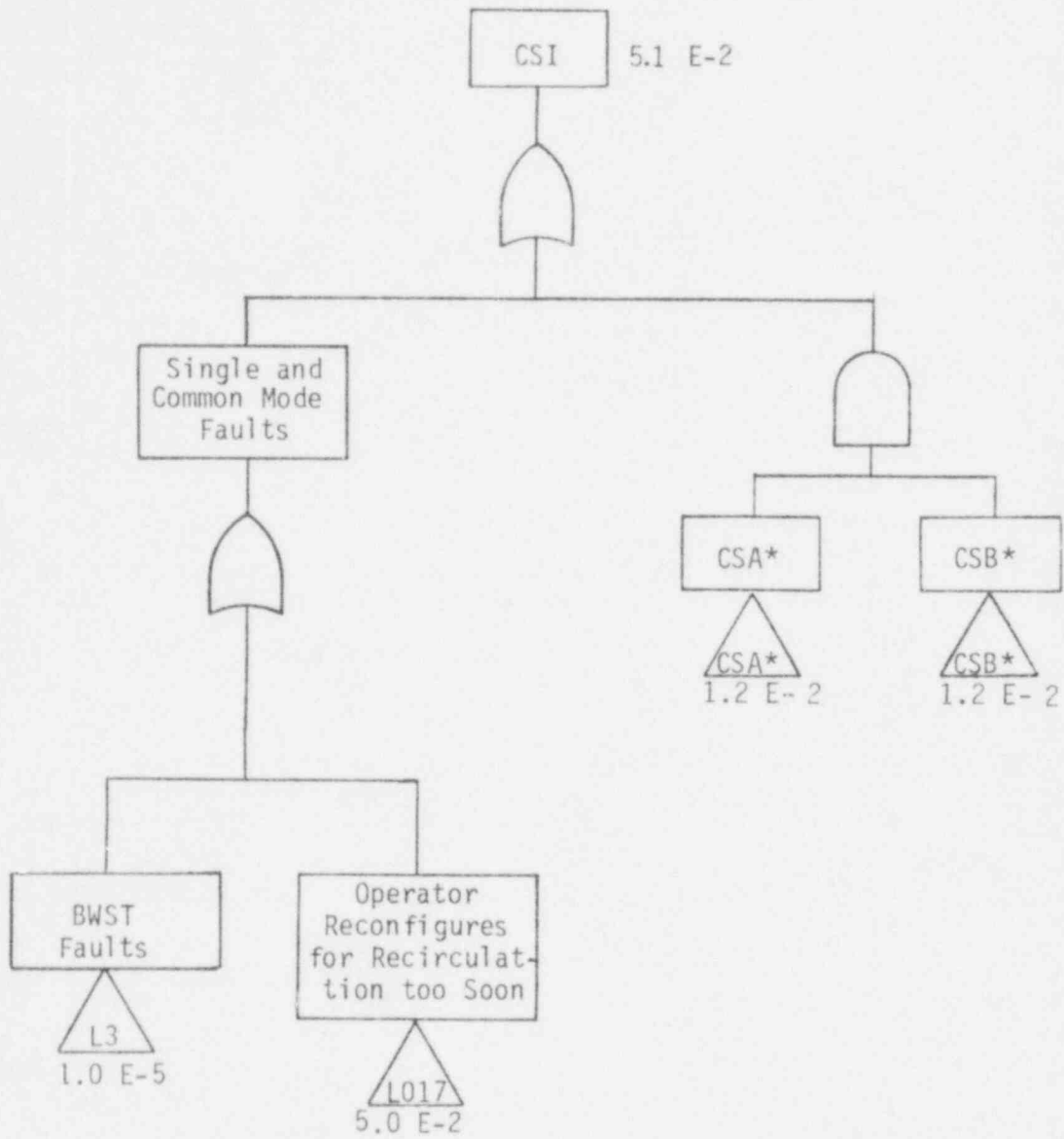


Figure M.4 Modularized Fault Tree for Event "CSI"; B₁ and B₂-LOCA

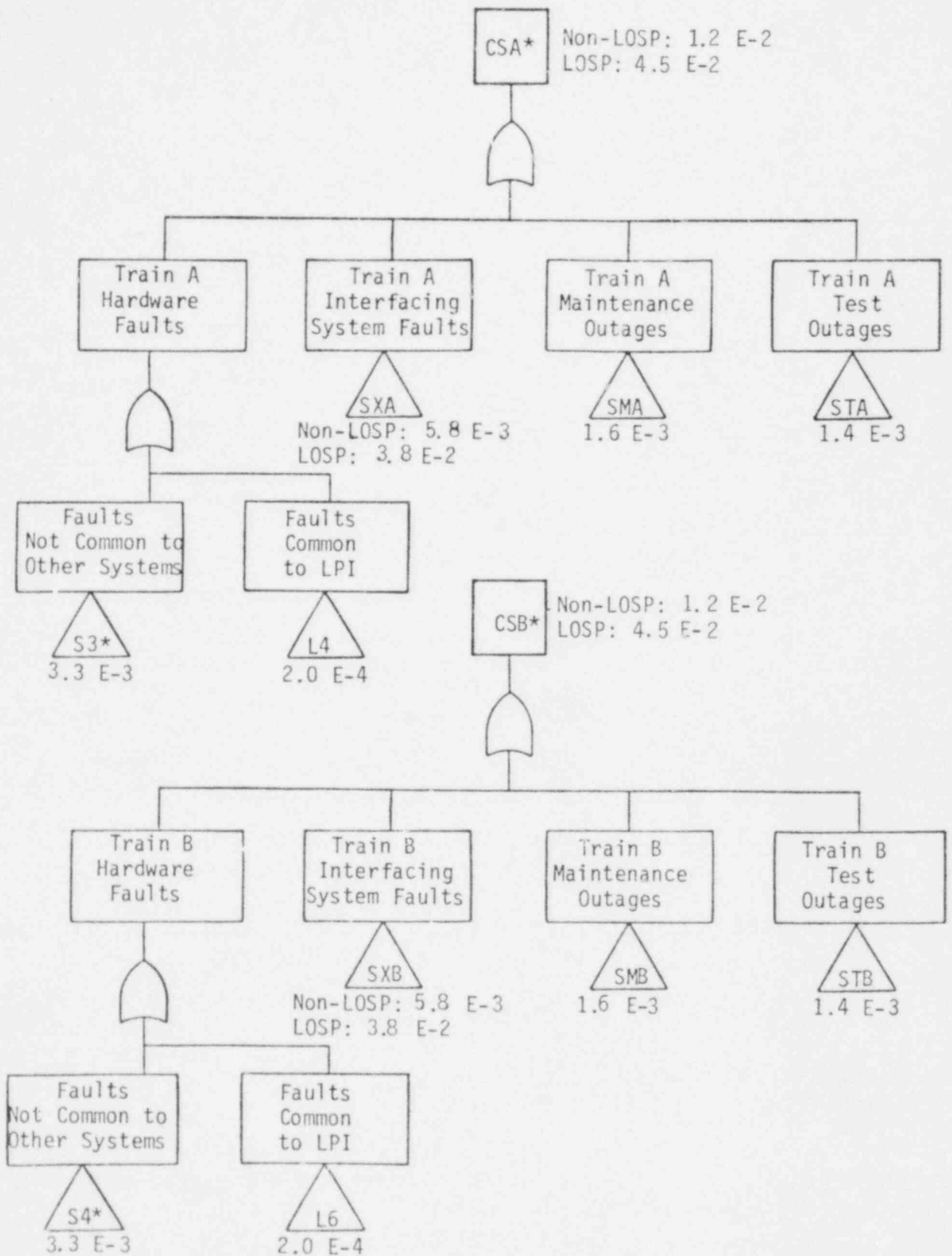
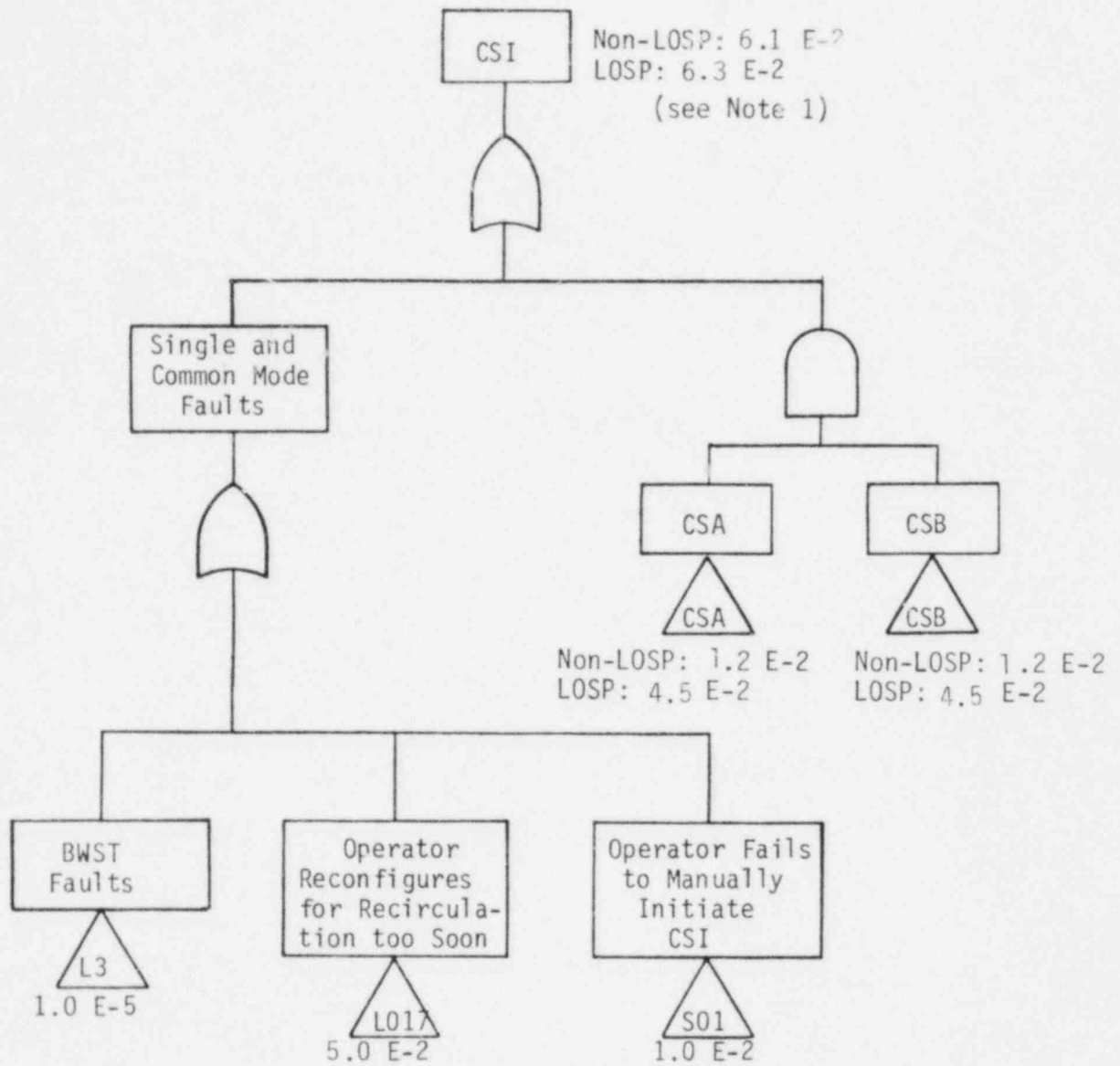


Figure M.5 Modularized Fault Trees for Events "CSA*" and "CSB*" (B₁ and B₂ LOCAs)



NOTE 1. The Non-LOSP probability applies to both the B₃ and B₄ LOCA cases. The LOSP probability applies only to the transient-induced B₄ LOCA.

Figure M.6 Modularized Fault Tree for Event "CSI"; B₃ and B₄-LOCA

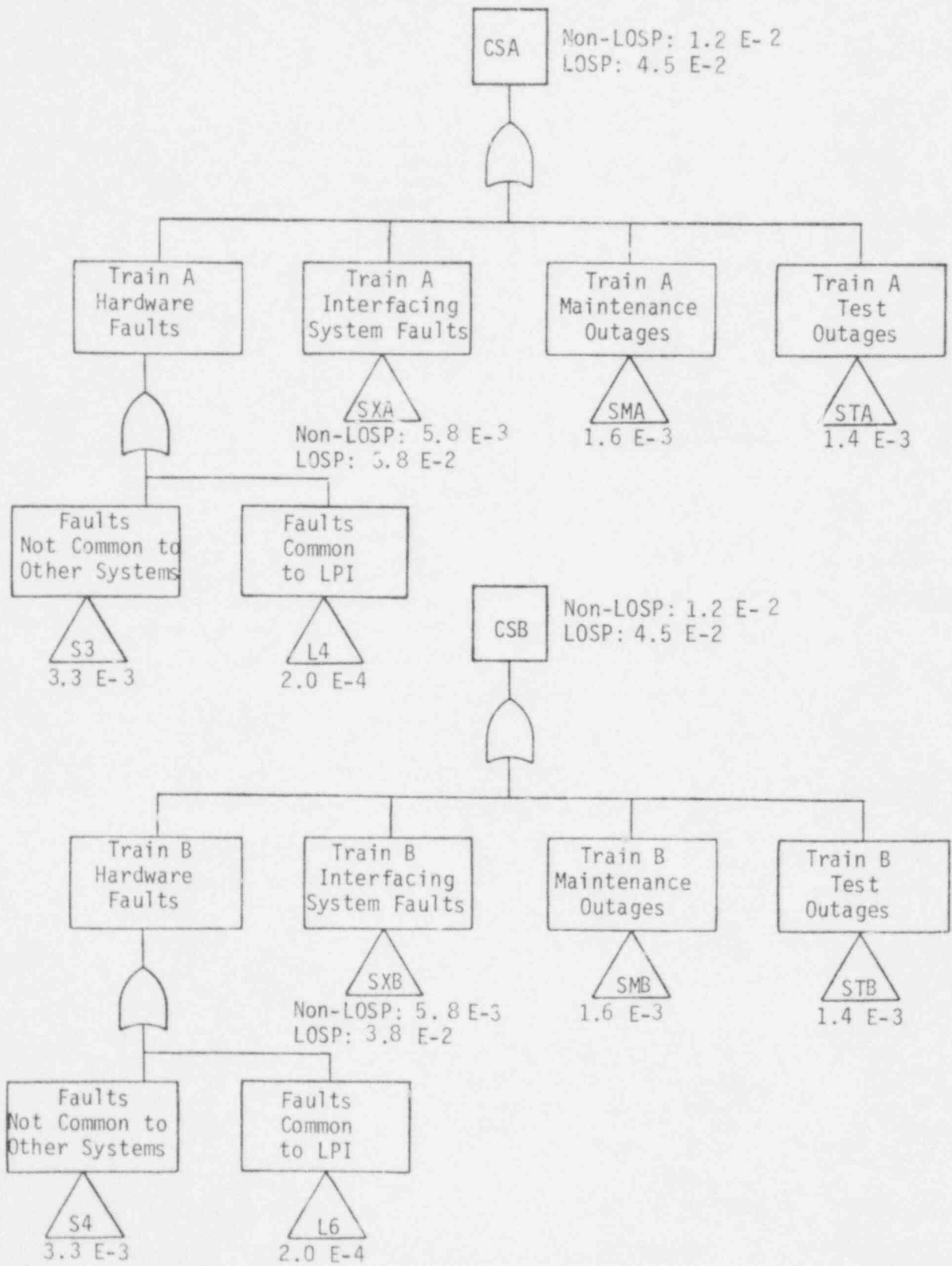


Figure M.7 Modularized Fault Trees for Events "CSA" and "CSB";
(B₃ and B₄ LOCAs)

Table M.3 (1/2) Containment Spray Injection

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

NOTES

B3, B4 - LOCAs

$$CSI3 = CSI4 = S01 + L017 + L3 + CSA \cdot CSB \quad 1$$

B1, B2 - LOCAs

$$CS11 = CS12 = L017 + L3 + CSA^* \cdot CSB^* \quad 1$$

INTERMEDIATE EVENTS

$$CSA = L4 + S3 + SXA + SMA + STA$$

$$CSB = L6 + S4 + SXB + SMB + STB$$

$$SXA = DA + ACA \quad 2$$

$$SXB = DB + ACB \quad 2$$

$$CSA^* = L4 + S3^* + SXA + SMA + STA$$

$$CSB^* = L6 + S4^* + SXB + SMB + STB$$

- NOTES: 1. Terms representing simultaneous outages in both legs are to be omitted since they are prohibited by Technical Specifications.
2. For offsite power available only DA and DB, respectively, contribute quantitatively. For loss of offsite power initiator ACA and ACB will be contained in DA and DB, respectively, and require a further Boolean reduction; see fault tree analysis of the DHCCCS. DC-contribution contained in ACA and ACB.

Table M.3 (2/2) Containment Spray Injection (Cont.)

BOOLEAN EQUATIONS REGROUPED FOR REDUCTION

B3, B4 - LOCAs

$$\begin{aligned}
 \text{CSI3} = \text{CSI4} = & \text{S01} + \text{L017} + \text{L3} + (\text{S3} \cdot \text{S4}) + (\text{L4} \cdot \text{L6}) + (\text{ACA} \cdot \text{ACB}) + \\
 & + \text{ACA} \cdot (\text{DB} + \text{S4} + \text{L6} + \text{SMB} + \text{STB}) + \text{ACB} \cdot (\text{DA} + \text{S3} + \text{L4} + \text{SMA} + \text{STA}) + \\
 & + (\text{DA} \cdot \text{DB}) + \text{DA} \cdot (\text{S4} + \text{L6} + \text{SMB} + \text{STB}) + \text{DB} \cdot (\text{S3} + \text{L4} + \text{SMA} + \text{STA}) + \\
 & + \text{S3} \cdot (\text{L6} + \text{SMB} + \text{STB}) + \text{S4} \cdot (\text{L4} + \text{SMA} + \text{STA}) + \text{L4} \cdot (\text{SMB} + \text{STB}) + \\
 & + \text{L6} \cdot (\text{SMA} + \text{STA})
 \end{aligned}$$

B1, B2 - LOCAs

$$\begin{aligned}
 \text{CSI1} = \text{CSI2} = & \text{L017} + \text{L3} + (\text{S3}^* \cdot \text{S4}^*) + (\text{L4} \cdot \text{L6}) + (\text{ACA} \cdot \text{ACB}) + \text{ACA} \cdot \\
 & \cdot (\text{DB} + \text{S4}^* + \text{L6} + \text{SMB} + \text{STB}) + \text{ACB} \cdot (\text{DA} + \text{S3}^* + \text{L4} + \text{SMA} + \text{STA}) + \\
 & + (\text{DA} \cdot \text{DB}) + \text{DA} \cdot (\text{S4}^* + \text{L6} + \text{SMB} + \text{STB}) + \text{DB} \cdot (\text{S3}^* + \text{L4} + \text{SMA} + \text{STA}) + \\
 & + \text{S3}^* \cdot (\text{L6} + \text{SMB} + \text{STB}) + \text{S4}^* \cdot (\text{L4} + \text{SMA} + \text{STA}) + \text{L4} \cdot (\text{SMB} + \text{STB}) + \\
 & + \text{L6} \cdot (\text{SMA} + \text{STA})
 \end{aligned}$$

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L3		BWST FAULTS			1.0 E-5			6, 7
LD17	OPERATOR	SWITCHES TO RECIRCULATION TOO SOON			5.0 E-2	3 ⁺ , 10 ⁻	0	6, 7
S3, S4*		PRODUCT INCLUDING COUPLED PUMP AND CHECK VALVE FAILURE			2.6 E-4	2 ⁺ , 2 ⁻	8	9

Table M.4 (1/10) Event "CSI" Quantification; B₁ and B₂ LOCAS

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S3*		TRAIN A HARDWARE FAULTS NOT COMMON TO OTHER SYSTEMS			3.3 E-3			10
	PUMP BSP-1A	FAILS TO START	D		1.0 E-3	3 ⁺ , 3 ⁻		
	PUMP BSP-1A	FAILS TO RUN	3.0 E-5	0.5	1.5 E-5	10 ⁺ , 10 ⁻		
	CHECK VALVE BSV-27	FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
	MOV BSV-3	FAILS TO OPEN	D		1.0 E-3	3 ⁺ , 3 ⁻		
	CHECK VALVE BSV-1	FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
	MOV BSV-17	FAILS TO REMAIN OPEN (PLUGGED)	D		1.0 E-4	3 ⁺ , 3 ⁻		
	SPRAY STRAINER	NOT REMOVED			c			
	VALVE DCV-115	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
	VALVE DCV-27	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
	VALVE DCV-116	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
	VALVE DCV-33	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
	VALVE BSV-2	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
					$\Sigma=3.3 E-3$			
	ILS SO2	ESAS TRAIN A FAILS AND OPERATOR FAILS TO RECOVER						
	ILS SO2	ESAS TRAIN A FAILS	D		1.1 E-4			
		OPERATOR FAILS TO RECOVER	D		1.0 E-2			
					$\Sigma=1.1 E-6$			
L4 SXA		TRAIN A HARDWARE FAULTS COMMON TO LPI			$\Sigma=3.3 E-3$			
		TRAIN A INTERFACING SYSTEM FAULTS			2.0 E-4			2
		NON LOSP			5.8 E-3			
		LOSP			3.8 E-2			
DA		DHCCS TRAIN A FAULTS (INSUFFICIENT COOLING)						
		NON LOSP			5.8 E-3			3
		LOSP			3.8 E-2			

Table M.4 (2/10) Event "CSA*" Quantification; B₁ and B₂ LOCAS

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ACA		AC TRAIN A (INSUFFICIENT POWER) NON LOSP LOSP			e 3.2 E-2			4
DCA		DC TRAIN A (INSUFFICIENT POWER) NON LOSP LOSP			e 3.2 E-3			5
STA		TRAIN A MAINTENANCE OUTAGES			1.6 E-3	3 ⁺ , 3 ⁻	H	
	PUMP BSP-1A	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	H	
	MOV BSV-3	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	H	
	MOV BSV-17	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	H	
					<u>Σ=1.6 E-3</u>			
STA		TRAIN A TEST OUTAGE	1/720	1	1.4 E-3		T	

Table M.4 (3/10) Event "CSA*" Quantification; B₁ and B₂ LOCAS

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S4*		TRAIN B HARDWARE FAULTS NOT COMMON TO OTHER SYSTEMS			3.3 E-3			10
	PUMP B5P-13	FAILS TO START	D		1.0 E-3	3 ⁺ , 3 ⁻		
	PUMP B5P-13	FAILS TO RUN	3.0 E-5	0.5	1.5 E-5	10 ⁺ , 10 ⁻		
	CHECK VALVE B5V-26	FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
	MOV B5V-4	FAILS TO OPEN	D		1.0 E-3	3 ⁺ , 3 ⁻		
	CHECK VALVE B5V-8	FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
	MOV B5V-16	FAILS TO REMAIN OPEN (PLUGGED)	D		1.0 E-4	3 ⁺ , 3 ⁻		
	SPRAY STRAINER	BLOCKED OR PLUGGED			c			
	VALVE DCV-117	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
	VALVE DCV-118	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
	VALVE DCV-20	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
	VALVE DCV-34	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
	VALVE B5V-7	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
					$\Sigma=3.3 E-3$			
ILS S02		ESFAS TRAIN B FAILS AND OPERATOR FAILS TO RECOVER						
	ILS	ESFAS TRAIN B FAILS	D		1.1 E-4			
	S02	OPERATOR FAILS TO RECOVER	D		1.0 E-2			
					$\pi=1.1 E-6$			
					$\Sigma=3.3 E-3$			
L6 SXB		TRAIN B HARDWARE FAULTS COMMON TO LPI			2.0 E-4			
		TRAIN B INTERFACING SYSTEM FAULTS NON LOSP			5.8 E-3			2
		LOSP			3.8 E-2			
DB		DHCCCS-B (INSUFFICIENT COOLING)						
		NON LOSP			5.8 E-3			
		LOSP			3.8 E-2			
ACB		AC TRAIN B (INSUFFICIENT POWER)						
		NON LOSP			c			
		LOSP			3.2 E-2			4

Table M.4 (4/10) Event "CSB*" Quantification; B₁ and B₂ LOCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
DCB		DC TRAIN B (INSUFFICIENT POWER)						
		NON LOSP			ϵ			
		LOSP			3.2 E-3			5
STB		TRAIN B MAINTENANCE OUTAGES			1.6 E-3	3 ⁺ , 3 ⁻	N	
	PUMP BSP-1B	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
	MOV BSV-4	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	N	
	MOV BSV-1G	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	N	
					$\Sigma=1.6 E-3$			
STB		TRAIN B TEST OUTAGE	1/720	1	1.4 E-3		T	

Table M.4 (5/10) Event "CSB*" Quantification; B₁ and B₂ LOCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L3		BYST FAULTS			1.0 E-5			6, 7
L017	OPERATOR	SWITCHES TO RECIRCULATION TOO SOON			5.0 E-2	3 ⁺ , 10 ⁻	0	6, 7
S01	OPERATOR	FAILS TO MANUALLY INITIATE CSI			1.0 E-2	3 ⁺ , 10 ⁻	0	8
S3- S4		PRODUCT INCLUDING COUPLED PUMP AND CHECK VALVE FAILURE			2.6 E-4	2 ⁺ , 2 ⁻	B	9

Table M.4 (6/10) Event "CSI" Quantification; B₃ and B₄ LOCAs

Table M.4 (7/10) Event "CSA" Quantification; B₃ and B₄ LOCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (PER YEAR)	MULTIPLICITY (DURATION/HR)	UNAVAILABILITY OR PROBABILITY	SEVERITY	NOTES
SF	TRAIN A HARDWARE FAULTS NOT COMMON TO OTHER SYSTEMS						
	PUMP BSV-14	FAILS TO START			3.3 E-3		11
	PUMP BSV-14	FAILS TO RUN	3.0 E-5	0.5	1.0 E-3		
	CHECK VALVE BSV-27	FAILS TO OPEN	D		1.0 E-4		
	MOV BSV-3	FAILS TO OPEN	D		1.0 E-3		
	CHECK VALVE BSV-1	FAILS TO OPEN	D		1.0 E-4		
	MOV BSV-17	FAILS TO REMAIN OPEN (PLUGGED)	D		1.0 E-4		
	SPRAY STRAINER	BLOCKED OR PLUGGED					
	VALVE DCV-115	LEFT CLOSED AFTER MAINTENANCE	(.02)	1.0 E-2	2.0 E-4		1
	VALVE DCV-27	LEFT CLOSED AFTER MAINTENANCE	(.02)	1.0 E-2	2.0 E-4		1
VALVE DCV-116	LEFT CLOSED AFTER MAINTENANCE	(.02)	1.0 E-2	2.0 E-4		1	
VALVE DCV-33	LEFT CLOSED AFTER MAINTENANCE	(.02)	1.0 E-2	2.0 E-4		1	
VALVE BSV-2	LEFT CLOSED AFTER MAINTENANCE	(.02)	1.0 E-2	2.0 E-4		1	
					3.3 E-3		
L4	TRAIN A HARDWARE FAULTS COMMON TO LPI						
SXA	TRAIN A INTERFACING SYSTEM FAULTS						
		NON LOSP			2.0 E-4		2
		LOSP			5.8 E-3		
DA	DHLCCS TRAIN A FAULTS (INSUFFICIENT COOLING)						
		NON LOSP			3.8 E-2		
		LOSP			5.8 E-3		3
ACA	AC TRAIN A (INSUFFICIENT POWER)						
		NON LOSP			e		4
		LOSP			3.2 E-2		
DCA	DC TRAIN A (INSUFFICIENT POWER)						
		NON LOSP			e		5
		LOSP			3.2 E-3		

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
SPA		TRAIN A MAINTENANCE OUTAGES			1.6 E-3	3 ⁺ , 3 ⁻	M	
	PUMP DSP-1A	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
	MOV DSV-3	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
	MOV DSV-17	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
					<u>1.6 E-3</u>			
STA		TRAIN A TEST OUTAGE	1/720	1	1.4 E-3		T	

Table M.4 (8/10) Event "CSA" Quantification; B3 and B4 LDCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S4		TRAIN B HARDWARE FAULTS NOT COMMON TO OTHER SYSTEMS			3.3 E-3			11
	PUMP DSP-1B	FAILS TO START	0		1.0 E-3	5 ⁺ , 5 ⁻		
	PUMP DSP-1B	FAILS TO RUN	3.0 E-5	0.5	1.5 E-5	10 ⁺ , 10 ⁻		
	CHECK VALVE BSV-2G	FAILS TO OPEN	0		1.0 E-4	5 ⁺ , 5 ⁻		
	MOV BSV-4	FAILS TO OPEN	0		1.0 E-3	5 ⁺ , 5 ⁻		
	CHECK VALVE BSV-8	FAILS TO OPEN	0		1.0 E-4	5 ⁺ , 5 ⁻		
	MOV BSV-1G	FAILS TO REMAIN OPEN (PLUGGED)	0		1.0 E-4	5 ⁺ , 5 ⁻		
	SPRAY	BLOCKED OR PLUGGED						
	VALVE DCV-117	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
	VALVE DCV-118	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
	VALVE DCV-28	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
	VALVE DCV-24	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
	VALVE BSV-7	LEFT CLOSED AFTER MAINTENANCE	(.02) 1.0 E-2		2.0 E-4	10 ⁺ , 10 ⁻	H	1
					<u>Σ=3.3 E-3</u>			
L6		TRAIN B HARDWARE FAULTS COMMON TO LPI			2.0 E-4			2
SXB		TRAIN B INTERFACING SYSTEM FAULTS						
		NON LOSP			5.8 E-3			
		LOSP			3.8 E-2			
DB		DHCCCS-B - INSUFFICIENT COOLING						
		NON LOSP			5.8 E-3			
		LOSP			3.8 E-2			3
ACB		AC TRAIN B - INSUFFICIENT POWER						
		NON LOSP			ε			
		LOSP			3.2 E-2			4
DCB		DC TRAIN B - INSUFFICIENT POWER						
		NON LOSP			ε			
		LOSP			3.2 E-3			5

Table M.4 (9/10) Event "CSB" Quantification; B3 and B4 LOCAs

Table M.4 (10/10) Event "CSB" Quantification; B₃ and B₄ LOCAs

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S33		TRAIN 3 MAINTENANCE OUTAGES						
	PUP BSP-13	OUT FOR MAINTENANCE	.02/720	19	1.6 E-3	3 ⁺ , 3 ⁻	II	
	MOV DSV-4	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	M	
	MOV DSV-1C	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3 ⁺ , 3 ⁻	II	
S18					$\frac{5.3}{6} = 1.6 \text{ E-3}$	3 ⁺ , 3 ⁻	II	
		TRAIN B TEST OUTAGE	1/720	1	1.4 E-3		T	

Table M.4 Containment Spray Injection

QUANTIFICATION TABLES

NOTES

- 1 This valve is closed in order to perform maintenance. Failure to reopen after maintenance would fail the train. The failure probability was assessed as (0.02) maintenance acts/month times a human error rate of (1.0 E-2). Recovery would occur on monthly CSI tests.
- 2 For assessment of these faults see LPI fault tree analysis, gate L4 (L6).
- 3 See DHCCCS fault tree analysis. For loss of offsite power case AC train A(B) is included as a fault in DA(DB).
- 4 See AC-power fault tree analysis.
- 5 See DC-power fault tree analysis
- 6 See low pressure injection fault tree.
- 7 This fault common to low pressure injection system.
- 8 For this size LOCA, procedures require balancing HPI flow which in turn requires defeating the ESFAS-signal. Therefore, spray initiation is manual if the system is required.
- 9 Check valve failures BSV-26 and BSV-27 and pumps BSP-1A and BSP-1B were assumed coupled with a β -factor of 0.1.
- 10 This event applies to B₁-and B₂-LOCAs only.
- 11 This event applies to B₃-and B₄-LOCAs only.

Table M.5 RBSI - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
S3	3.3 E-3
L4	2.0 E-4
DA	5.8 E-3* 3.8 E-2**
SMA	1.6 E-3
STA	1.4 E-3
S4	3.3 E-3
L6	2.0 E-4
DB	5.8 E-3* 3.8 E-2**
SMB	1.6 E-3
STB	1.4 E-3
S3·S4	2.6 E-4
L3	1.0 E-5
L017	5.0 E-2
S01	1.0 E-2
S3*	3.3 E-3
S4*	3.3 E-3
S3*·S4*	2.6 E-4
ACA	ϵ^* 3.2 E-2**
ACB	ϵ^* 3.2 E-2**
DCA	ϵ^* 3.2 E-3**
DCB	ϵ^* 3.2 E-3**

*Offsite power available

**Offsite power not available

M.3.3 SYSTEM FAULT TREE QUANTIFICATION - RECIRCULATION PHASE

This section presents the quantification of the RBSR* unavailability for required emergency operation of the RBSS during the recirculation phase of a postulated accident. The quantitative results are presented in table form with attached notes outlining the assumptions. To perform the fault tree quantification, the simplified fault tree was transformed into a modularized fault tree.

Table M.6 shows the RBSS success requirements. Table M.7 contains the top event definition for the modularized fault tree, and Figures M.8 through M.12 show the modularized fault trees for the RBSR. The unavailability of each gate is shown on the tree. Table M.8 shows the Boolean equations that represent the fault trees. Table M.9 shows the quantification of each gate by component and failure mode. The attached notes explain the assumptions used in the quantification. Table M.10 presents a summary of the point estimates for each gate.

* RBSR: Reactor Building Spray System - Recirculation Phase

Table M.6 Containment Spray Recirculation

SUCCESS REQUIREMENTS

<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B1, B2, B3, B4	1/2 trains	1,2,3

-
- NOTES: 1. Success definition is the same for all LOCA sizes.
2. The time into the accident sequence when containment spray (CS) will be required is dependent on the size of the LOCA. However, it was assumed that CS would be required during the recirculation phase for all LOCA sizes.
3. The containment spray system is used both for containment atmosphere heat removal and post accident radioactivity removal.

Table M.7 Containment Spray Recirculation

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
CSR	Failure of both containment spray trains to provide containment atmosphere cooling during recirculation.	
CSA**	Failure of containment spray Train A to provide containment atmosphere cooling during injection.	
CSB**	Failure of containment spray Train B to provide containment atmosphere cooling during injection.	
CRA	Failure of containment spray Train A to provide containment atmosphere cooling during recirculation.	
CRB	Failure of containment spray Train B to provide containment atmosphere cooling during recirculation.	

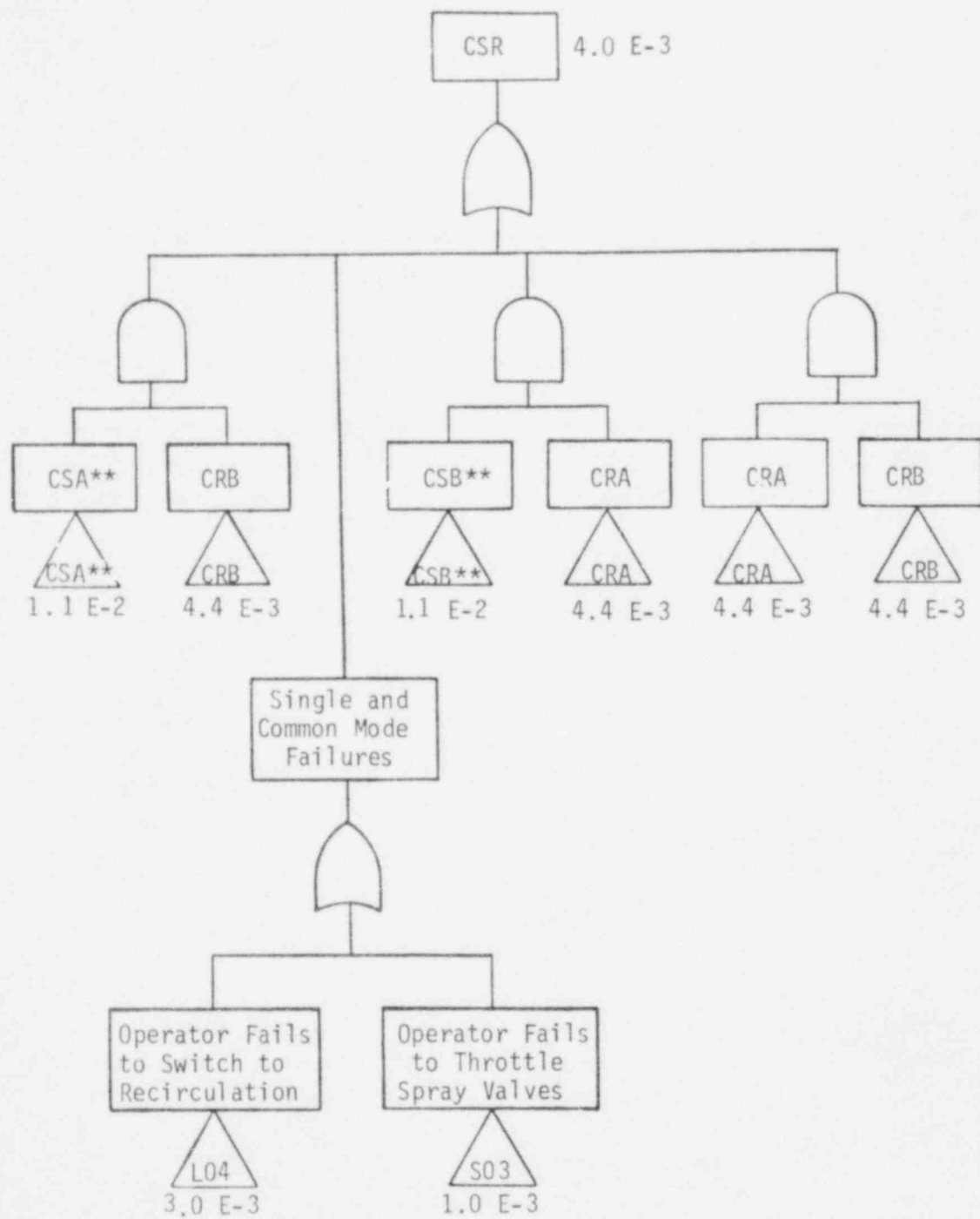


Figure M.8 Modularized Fault Tree for Event "CSR"

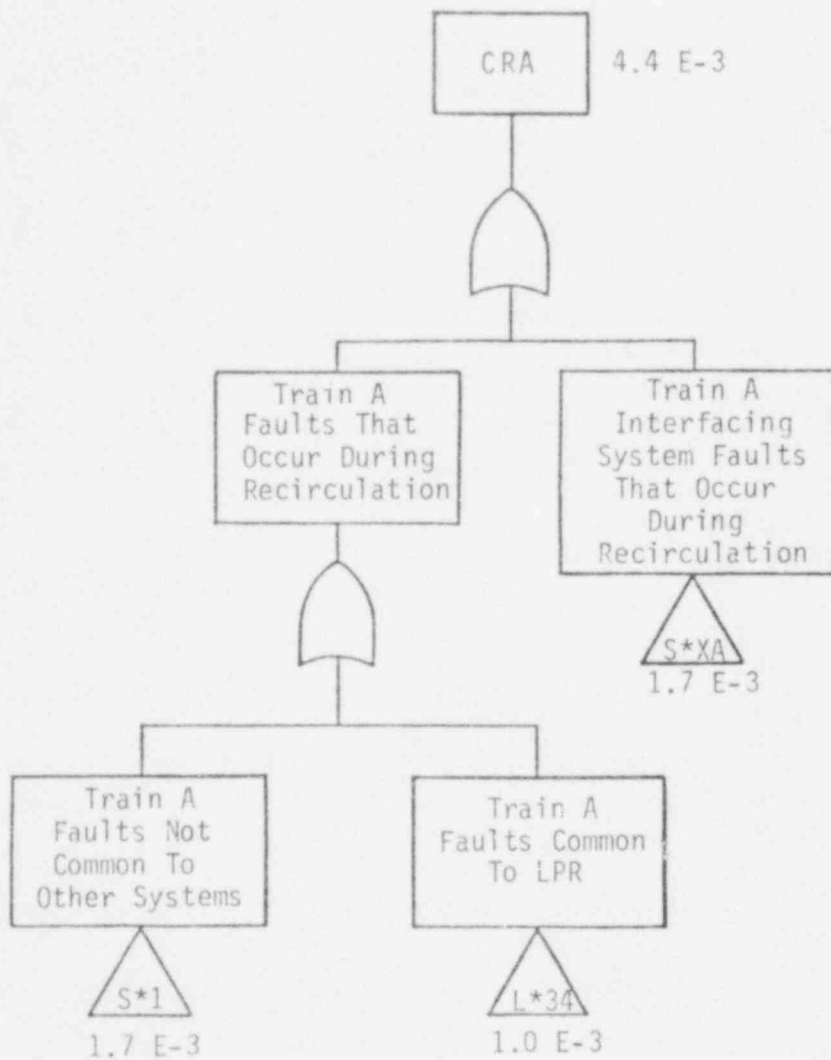


Figure M.9 Modularized Fault Tree for Event "CRA"

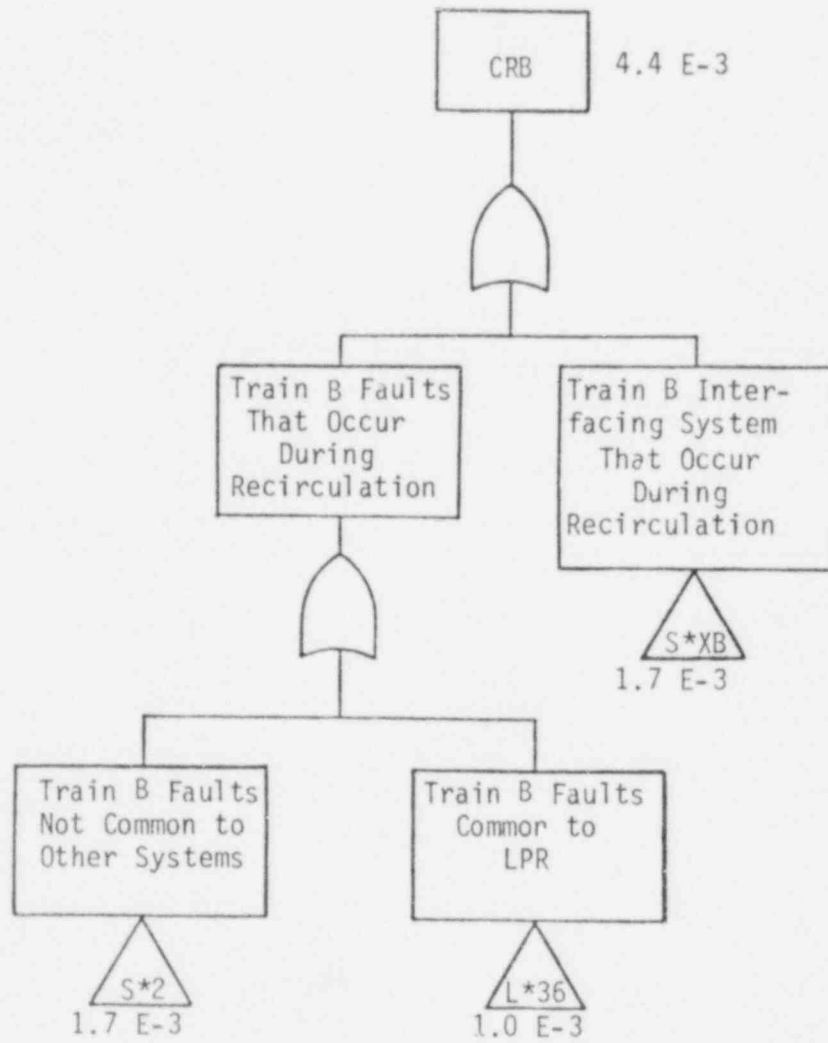


Figure M.10 Modularized Fault Tree for Event "CRB"

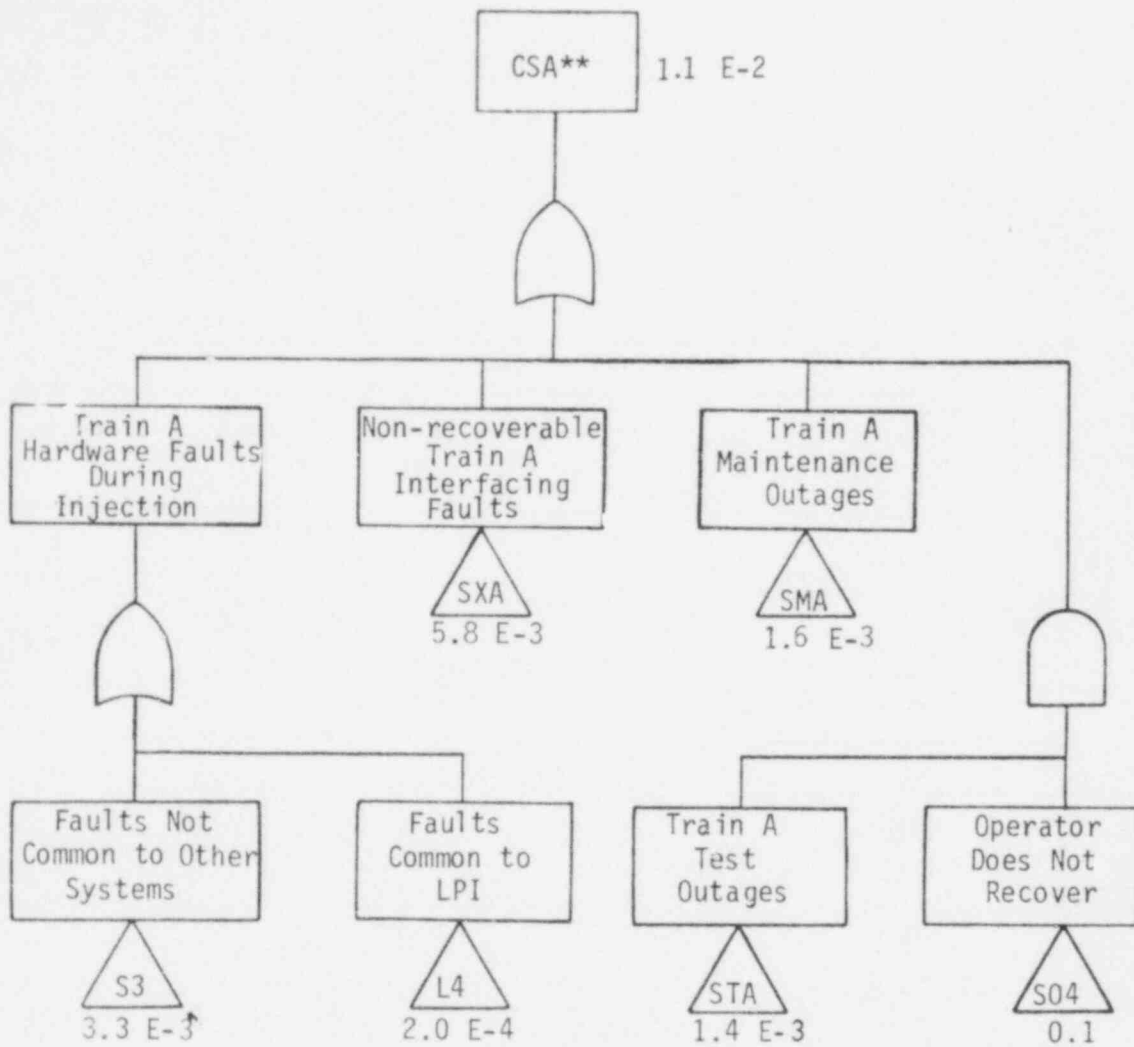


Figure M.11 Modularized Fault Tree for Event "CSA**"

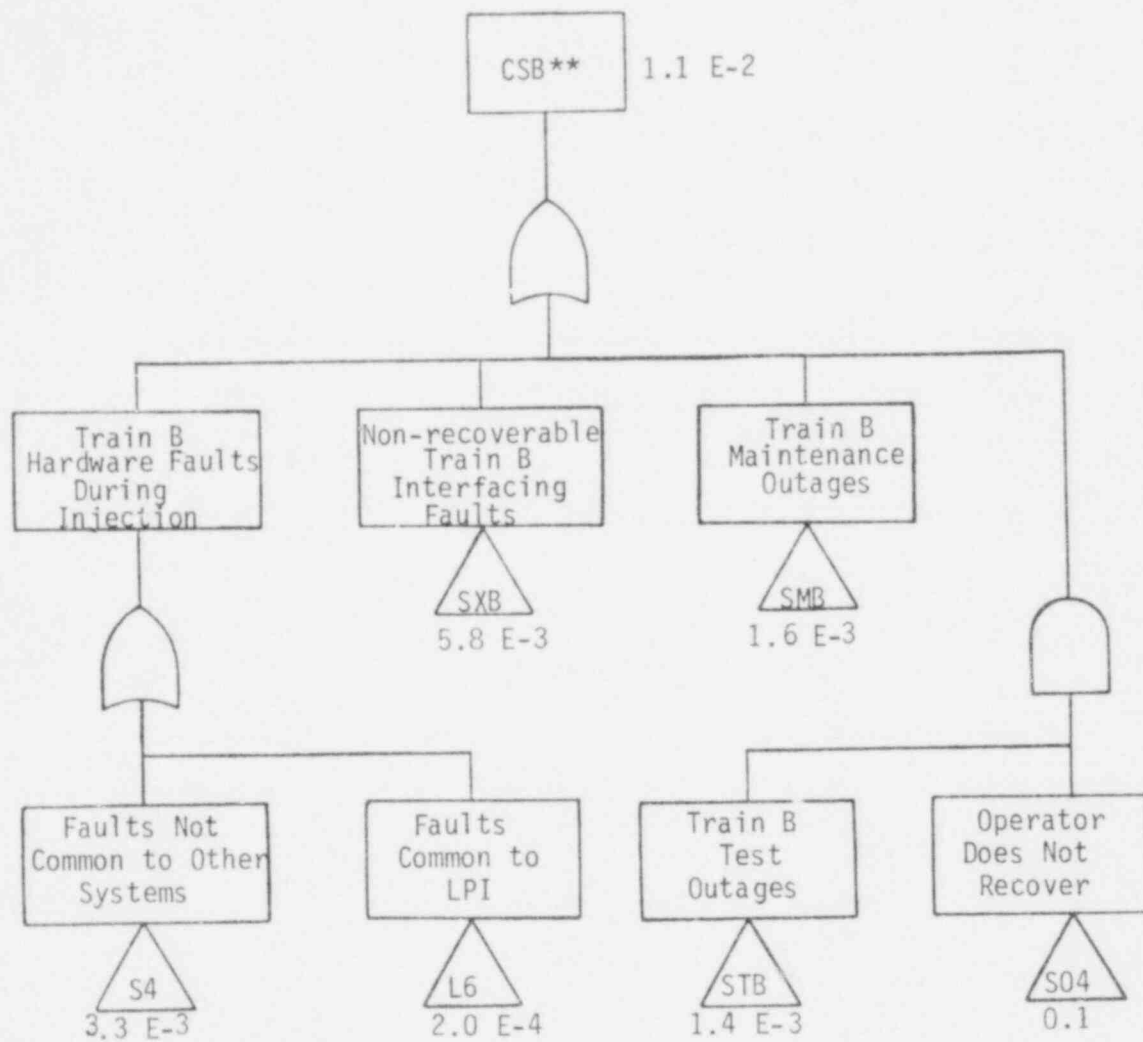


Figure M. 12 Modularized Fault Tree for Event "CSB**"

Table M.8 Containment Spray Recirculation

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

NOTES

$$CSR = L04 + S03 + CRB \cdot CSA^{**} + CRA \cdot CSB^{**} + CRA \cdot CRB$$

$$CSA^{**} = S3 + L4 + SXA + SMA + STA \cdot S04$$

$$CSB^{**} = S4 + L6 + SXB + SMB + STB \cdot S04$$

INTERMEDIATE EVENTS

$$CRA = S^*1 + S^*XA + L^*34$$

$$CRB = S^*2 + S^*XB + L^*36$$

$$S^*XA = DA^* + ACA^*$$

$$S^*XB = DB^* + ACB^*$$

1

1

NOTES: 1. Offsite power is assumed to be recovered when entering the recirculation phase. The unavailability of AC power with offsite power available was calculated to be negligible compared to other system failure modes.

Table M.9 (1/5) Event "CSR" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
LD4	OPERATOR	FAILS TO SWITCH TO RECIRCULATION	D		3.0 E-3	10 ⁺ , 10 ⁻		4
S93	OPERATOR	FAILS TO THROTTLE SPRAY VALVES	D		1.0 E-3	10 ⁺ , 10 ⁻		5

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S*1		TRAIN A FAULTS THAT OCCUR DURING RECIRCULATION			1.7 E-3			
	PUMP BSP-1A	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10 ⁺ , 10 ⁻		
	VALVE BSV-3	FAILS TO THROTTLE	D		1.0 E-3	3 ⁺ , 3 ⁻		
	R.B. SUMP STRAINER	BLOCKED PLUGGED			e e			
					$\Sigma=1.7 E-3$			
S*XA		SYSTEM INTERFACING FAULTS THAT OCCUR DURING RECIRCULATION			1.7 E-3			
	DA*	DHCCS TRAIN A FAILS DURING RECIRCULATION			1.7 E-3			2, 3
	ACA*	AC POWER TRAIN A FAILS DURING RECIRCULATION			e			
	DCA*	DC POWER TRAIN A FAILS DURING RECIRCULATION			e			
L*34		TRAIN A FAULTS COMMON TO LPR			1.0 E-3			4

Table M.9 (2/5) Event "CRA" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S*2		TRAIN B FAULTS THAT OCCUR DURING RECIRCULATION			1.7 E-3			
	PUMP BSP-1B	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10 ⁺ , 10 ⁻		
	VALVE BSV-4	FAILS TO THROTTLE	D		1.0 E-3	3 ⁺ , 3 ⁻		
	R.B. SUMP	BLOCKED			e			
	STRAINER	PLUGGED			e			
					$\Sigma=1.7 E-3$			
S*XB		SYSTEM INTERFACING FAULTS THAT OCCUR DURING RECIRCULATION			1.7 E-3			
	DB*	DHCCS TRAIN B FAILS DURING RECIRCULATION			1.7 E-3			2, 3
	ACB*	AC POWER TRAIN A FAILS DURING RECIRCULATION			e			
	DCB*	DC POWER TRAIN B FAILS DURING RECIRCULATION			e			
L*36		TRAIN B FAULTS COMMON TO LPR			1.0 E-3			4

Table M.9 (3/5) Event "CRB" Quantification

M-45

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S3		TRAIN A FAULTS NOT COMMON TO OTHER SYSTEMS			3.3 E-3			1
L4		TRAIN A FAULTS COMMON TO LOW PRESSURE SYSTEM			2.0 E-4			1
SXA		TRAIN A SYSTEM INTERFACING FAULTS						1.6
	DA	DHCCCS TRAIN A FAILS NON LOSP			4.3 E-2			
	ACA	AC POWER TRAIN A FAILS NON LOSP			e			
	DCA	DC POWER TRAIN A FAILS NON LOSP			e			
SMA		TRAIN A MAINTENANCE OUTAGE			1.6 E-3	3 ⁺ , 3 ⁻	11	1
STA-S04		TRAIN A IN TEST AND NOT RECOVERED FOR RECIRCULATION			1.4 E-4			
	STA	TRAIN A IN TEST			1.4 E-3			
	S04	OPERATOR FAILS TO RECOVER			0.1	3 ⁺ , 10 ⁻	0	
					$\pi=1.4 E-4$			

Table M.9 (4/5) Event "CSA**" Quantification

M-46

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
S4		TRAIN B FAULTS NOT COMMON TO OTHER SYSTEMS			1.3 E-2			1
L6		TRAIN B FAULTS COMMON TO LOW PRESSURE SYSTEM			2.0 E-4			1
SXB		TRAIN B SYSTEM INTERFACING FAULTS						1.6
	DB	DHCCCS TRAIN B FAILS NON LOSP			4.3 E-2			
	ACB	AC POWER TRAIN B FAILS			ϵ			
	DCB	DC POWER TRAIN B FAILS			ϵ			
SMB		TRAIN A MAINTENANCE OUTAGE			1.6 E-3	3 ⁺ , 3 ⁻	M	1
STB. SQ4		TRAIN B IN TEST AND NOT RECOVERED FOR RECIRCULATION			1.4 E-4			1
	STB	TRAIN B IN TEST			1.4 E-3			
	SQ4	OPERATOR FAILS TO RECOVER			0.1	3 ⁺ , 10 ⁻	0	
					$\approx 1.4 E-4$			

Table M.9 (5/5) Event "CSB**" Quantification

Table M.9 Containment Spray Recirculation

QUANTIFICATION TABLES

NOTES

- 1 For definition see CSI fault tree analysis.
- 2 Failure of DHCCCS Train A(B) during recirculation phase implies success during injection phase.
- 3 For loss of offsite power initiator failure of DA(DB) due to diesel failure is assumed to be recovered for the recirculation phase.
- 4 See LPR fault tree analysis.
- 5 Operator is required to throttle valves BSV-3 and 4 to prevent pump cavitation. This was assessed as $1.0 \text{ E-}3$ rather than the usual value of $1.0 \text{ E-}2$ for operator faults because procedures are clear and fault is alarmed. Inclusion of this fault in the analysis may be conservative because it is not certain that throttling these valves is required to prevent cavitation.
- 6 In CSA** and CSB** for LOSP, the events SXA and SXB exclude diesel failures because offsite power is assumed to be recovered by the recirculation phase.

Table M.10 RBSR - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
S3	3.3 E-3
L4	2.0 E-4
DA	5.8 E-3
SMA	1.6 E-3
STA·S04	1.4 E-4
S4	3.3 E-3
L6	2.0 E-4
DB	5.8 E-3*
SMB	1.6 E-3
STB·S04	1.4 E-4
S*1	1.7 E-3
DA*	1.7 E-3
L*34	1.0 E-3
S*2	1.7 E-3
DB*	1.7 E-3
L*36	1.0 E-3
S04	1.0 E-1
L04	3.0 E-3
S03	1.0 E-3

APPENDIX N

REACTOR BUILDING ISOLATION SYSTEM (RBIS)

N.1 SYSTEM DESCRIPTION AND OPERATION

The purpose of the reactor building isolation system (or containment isolation system, CIS) is to insure that no path exists between the containment atmosphere and the outside environment. However, emergency system piping penetrating the containment must remain open (e.g., Emergency Core Cooling Systems, Containment Sprays, and Containment Cooling Fan System). The largest penetrations to be closed are the 48-inch reactor building purge supply and exhaust ducts.

In this analysis only the closure of the purge isolation valves was treated. All smaller penetrations and liquid flow paths were not analyzed since their contribution to offsite dose consequences would be comparatively small.

N.1.1 SYSTEM DESCRIPTION

The majority of the reactor building isolation system is passive. Most containment isolation valves are locked closed or normally closed. The valves which are not locked closed receive a signal to close from the ESAS when a pressure greater than 4 psi is detected within the containment. Only two containment penetrations are normally open. The 48-inch reactor building purge supply and purge exhaust ducts are frequently open while the reactor is at power. Two valves, one pneumatic, one motor operated, are in each line on opposite sides of the containment wall. The pneumatic valve is held open by instrument air. If air pressure or control power to the valve operator is lost, the valve will automatically close. The motor operated valve must be driven closed.

The valve operators on the 48-inch butterfly valves located outside of the reactor building are of the spring return air cylinder type with the spring driving the valve closed. Each pneumatic valve is controlled with two 3 way solenoid valves, either capable of permitting the valve to close in two seconds maximum time. These valves on the exterior of the reactor building are in areas totally protected from damage by missiles or pipe and equipment rupture.

The valve operators on the valves located on the inside of the reactor building are electric motor driven with a totally enclosed, non-ventilated type motor and gear drive. The valves close in five seconds maximum time. Both internal and external valves are capable of satisfactory performance in the post-accident ambient.

The system has interfaces with the ESAS reactor building isolation and cooling circuits, radiation detection circuits and 480VAC from ES MCC 3A1, unit 8A. The ESAS and high radiation signal affect both pneumatic and motor operated valves, while only the motor operated valves have an interface with the 480V AC power.

The following critical design requirements were applied to the four 48-inch purge isolation valves:

a. Exterior valves:

- Must be capable of closing against a differential pressure of 55 psig.
- Must close fully in 2 seconds.
- When closed, the valve must seal bubble-tight, that is, no air bubbles appear in a pool of water, with 63.3 psig air pressure applied across the closed face.

b. Interior Valves:

- Must be capable of closing against a differential pressure of 55 psig.
- Must close fully in 5 seconds.
- When closed, the valve must seal bubble-tight under the same conditions as above.

N.1.2 SYSTEM OPERATION

The reactor building isolation system is actuated by either the Engineered Safeguard Actuation System (ESAS), or by manual action. High radiation in the reactor purge line will close the purge valves. Upon receipt of the ESAS signal (Reactor Building Isolation and Cooling, RBIC) all system valves which are not manually operated (and locked closed) are commanded closed.

The ESAS will generate a closure signal to the valves when a reactor building pressure exceeding 4 psi is detected. A second signal, generated from a high radiation detector in the reactor building purge exhaust line, will also allow valve closure. Manual actuation from the control room is a third method for closing the valves.

It should be noted that for small LOCAs, (B4), only manual operations or operation by the radiation detection circuits is possible.

The radiation detection circuit is a single train system containing no redundancy.

N.2 SYSTEM SIMPLIFIED FAULT TREE

A detailed fault tree for the RBIS was constructed to model the failure to isolate the outside environment from containment atmosphere.

The top event was defined as:

Containment Isolation Fails - failure of
one or both of the containment purge
lines to isolate.

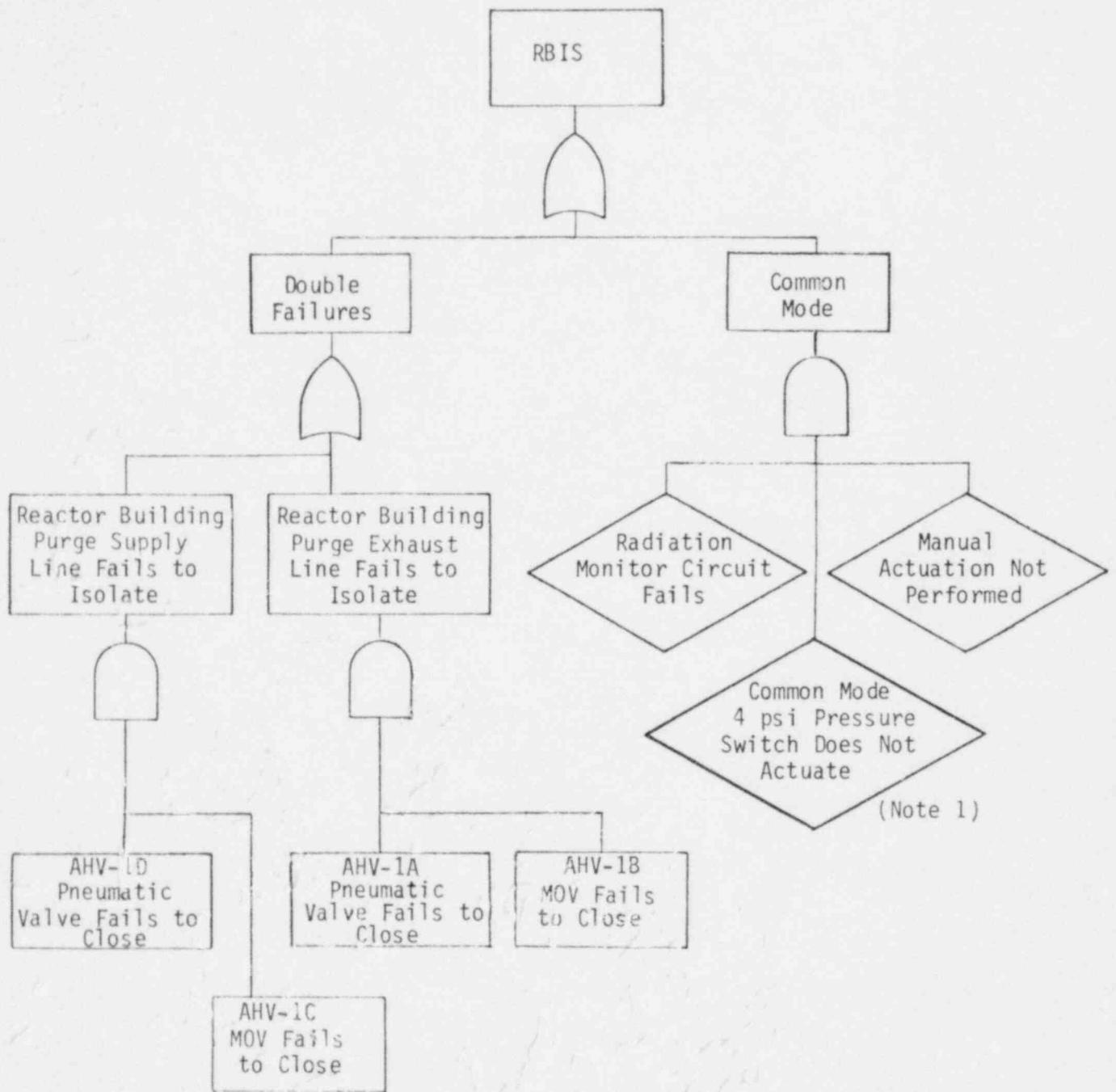
The simplified fault tree shown in Figure N.1 was constructed from the detailed tree. The simplified tree shows only the single passive and active faults and double active faults. All higher order combinations of component faults were considered to be negligible contributors to system failure probability. Human error events are also shown on the fault tree.

MAJOR ASSUMPTIONS

The major assumptions used to construct the detailed fault tree are listed below:

- (1) Penetrations less than 4 inches in diameter are not considered since flow rates having a significant effect on consequences would not be realized.
- (2) Liquid flow paths and paths into liquid systems were not analyzed.
- (3) Leak rate test penetrations were not analyzed due to the double passive failures required for a breach of containment isolation.
- (4) The penetrations which dominate the containment leakage event are the 48-inch reactor building purge supply and exhaust lines.
- (5) The containment purge supply and exhaust lines are frequently open during power operation. In this analysis the isolation valves are considered to be always open.

- (6) A small LOCA, (B4), does not generate enough pressure within the containment to generate a trip (4 psig) signal from the ESAS. Therefore, only a high radiation trip or a manual actuation signal is available during a small LOCA.
- (7) High radiation in the purge exhaust line was assumed to be present for all LOCA sizes.



NOTES: 1. From ESAS Fault Tree

Figure N.1 Simplified Fault Tree Reactor Building Isolation System

N.3 SYSTEM QUANTIFICATION

N.3.1 SYSTEM RELIABILITY CHARACTERISTICS

For large LOCAs (B1, B2, B3) the failure to isolate the containment is determined by the failure of at least one isolation valve to close in the purge supply and in the purge exhaust line.

For small LOCAs (B4) the dominant contributor is failure to initiate containment isolation by a high radiation signal and the operator fails to manually isolate the containment. Other contributors are several orders of magnitude smaller.

N.3.2 SYSTEM FAULT TREE QUANTIFICATION

This section presents the quantification of the RBIS failure to isolate the containment after a LOCA. Two modularized fault trees, using the simplified fault tree in Figure N.1, were constructed to accommodate different LOCA sizes. One modularized tree represents large LOCAs (B1,B2,B3) and the second represents small LOCAs (B4). The distinction is necessary since the 4 psig reactor building pressure was assumed not to be reached after a small LOCA. Therefore, only an operator action will initiate containment isolation; high radiation in the purge line will close the purge valves.

Table N.1 shows the RBIS success requirement. Table N.2 contains the top event definitions for the modularized fault tree. The modularized trees are shown in Figures N.2 and N.3. On the trees, the unavailability of each gate is shown. Table N.3 shows the Boolean equations that represent the fault trees and Table N.4 shows the quantification of each gate by component and failure mode. The point estimates for each gate are summarized in Table N.5.

Table N.1 Reactor Building Isolation System

SUCCESS REQUIREMENTS

<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
B1,B2,B3,B4	1/2, taken twice (at least one of two valves in each line must close)	1

NOTES

- 1 Both the reactor building purge supply and exhaust lines must be closed within a specified time.

Table N.2 Reactor Building Isolation System

TOP EVENT DEFINITIONS

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
CIS	Containment Isolation fails	1
CIS*	Containment Isolation fails	2

NOTES

- 1 CIS applies to large LOCAs (B1,B2,B3)
- 2 CIS* applies to small LCCAs (B4)

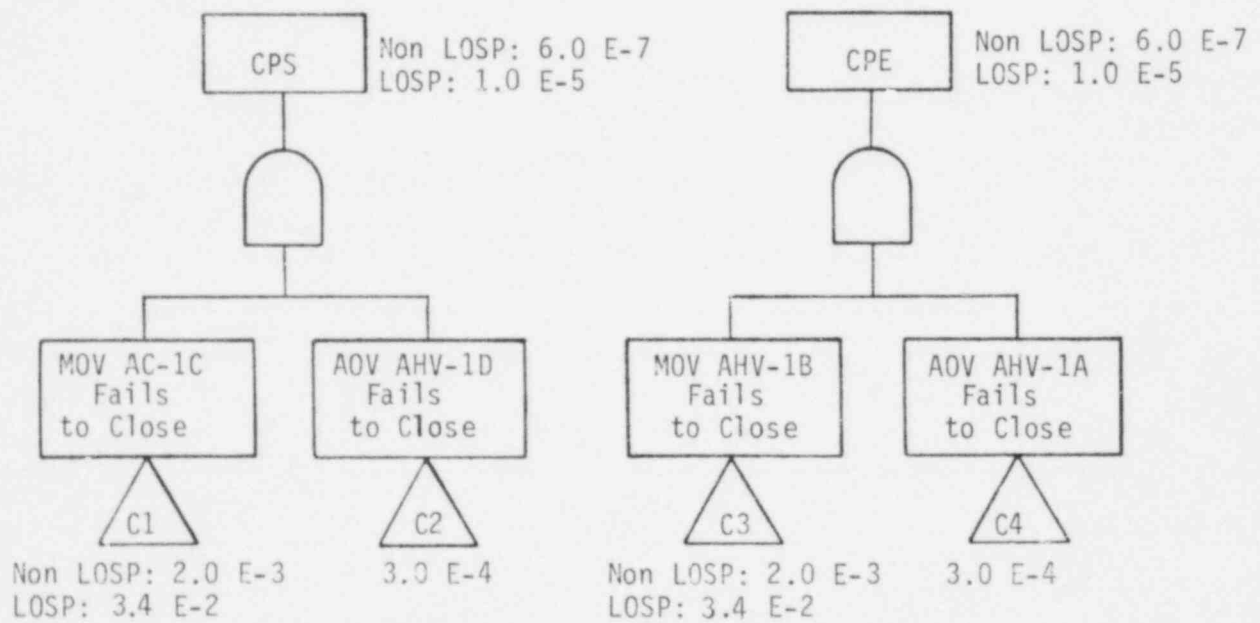
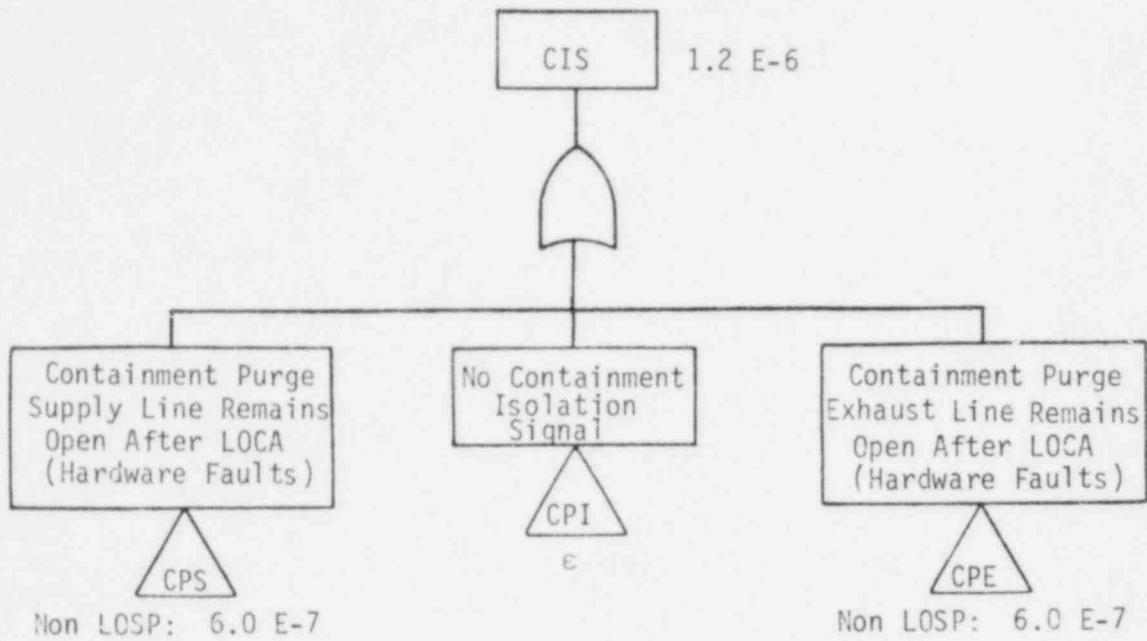


Figure N.2 (1/2) Modularized Fault Tree for Events "CIS", "CPS", and "CPE" (B₁, B₂, B₃ LOCAs)

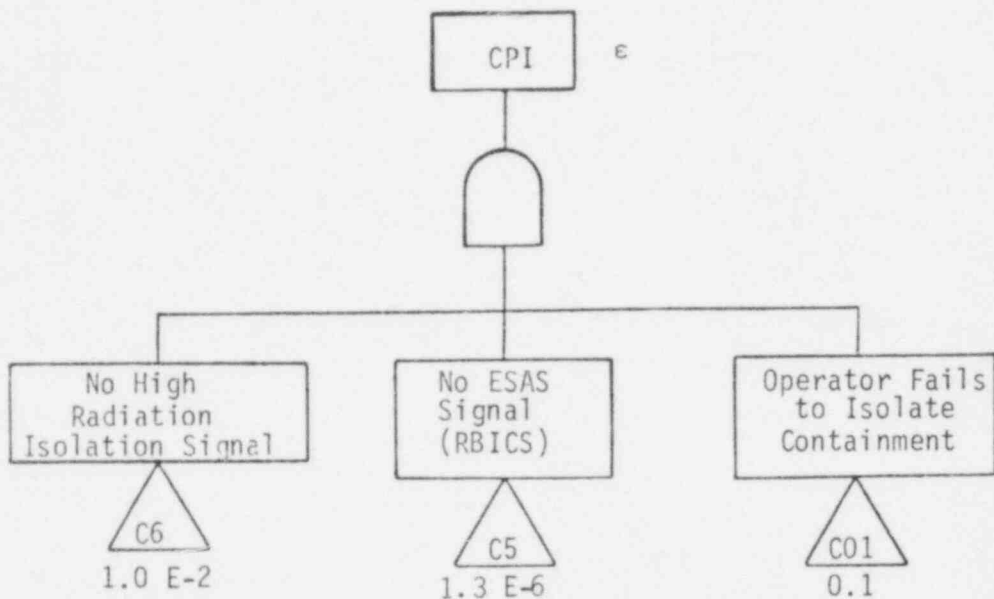


Figure N.2 (2/2) Modularized Fault Tree for Event "CPI"
 (B₁, B₂, B₃ LOCAs)

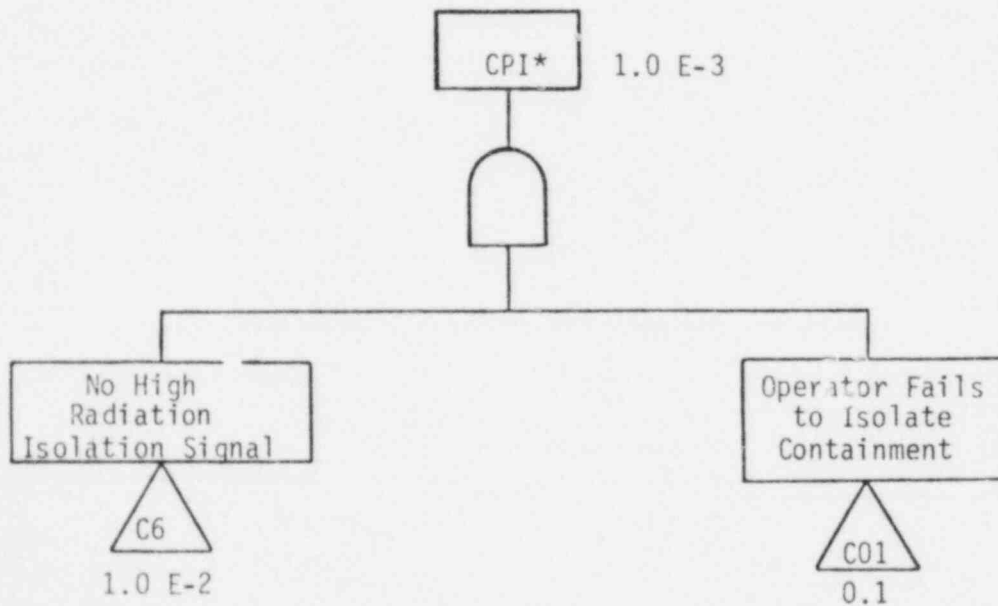
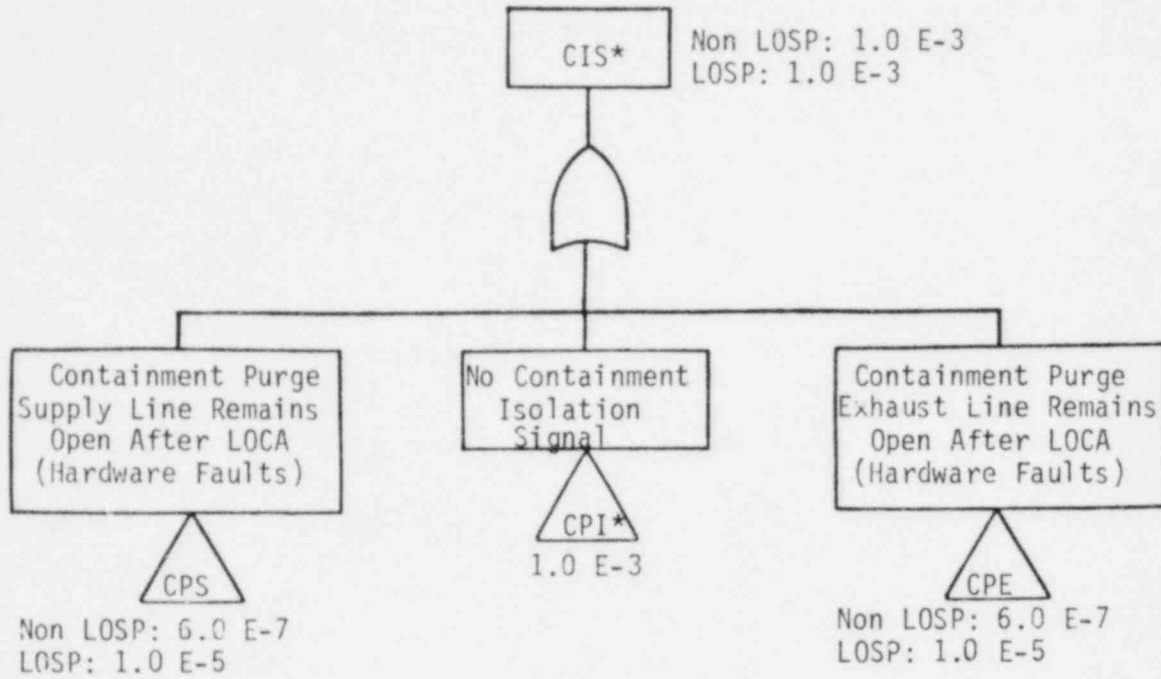


Figure N.3 (1/1) Modularized Fault Tree for Event "CIS*" and "CPI*" (B₄ LOCA)

Table N.3 Reactor Building Isolation System

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREE

TOP EVENT

NOTES

B1,B2,B3 - LOCAs:

$$CIS = CPS + CPE + CPI$$

B4 - LOCAs:

$$CIS^* = CPS + CPE + CPI^*$$

INTERMEDIATE EVENTS

B1,B2,B3 - LOCAs:

$$CPI = C6 \cdot C5 \cdot C01$$

B4 - LOCAs:

$$CPI^* = C6 \cdot C01$$

a11 LOCAs:

$$CPS = C1 \cdot C2$$

$$CPE = C3 \cdot C4$$

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
CPS		CONTAINMENT PURGE SUPPLY LINE REMAINS OPEN AFTER LOCA (HARDWARE FAULTS)			6.0 E-7* 1.0 E-5**			
C1		MOTOR OPERATED VALVE AHV-1C FAILS TO CLOSE			2.0 E-3* 3.4 E-2**			
	MOV AHV-1C	FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
	CIRCUIT BKR	FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
		AC-TRAIN A FAILS (ACA)						
		NON LOSP						
		LOSP			3.2 E-2			
					$\Sigma=2.0 E-3^*$			
					$\Sigma=3.4 E-2^{**}$			
C2		AIR OPERATED VALVE AHV-1D FAILS TO CLOSE			3.0 E-4			
	AOV AHV-1D	FAILS TO CLOSE	D		3.0 E-4			
					$\Sigma=6.0 E-7^*$			
					$\Sigma=1.0 E-5^{**}$			

*NON LOSP

**LOSP

Table N.4 (1/4) Event "CPS" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
CPE		CONTAINMENT PURGE EXHAUST LINE REMAINS OPEN AFTER LOCA (HARDWARE FAULTS)			6.0 E-7* 1.0 E-5**			
C3		MOTOR OPERATED VALVE AHV-1B FAILS TO CLOSE			2.0 E-3* 3.4 E-2**			
	MOV AHV-1B	FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
	CIRCUIT BKR	FAILS TO CLOSE	D		1.0 E-3	3 ⁺ , 3 ⁻		
		AC-TRAIN A FAILS (ACB)						
		NON LOSP			e			
		LOSP			3.2 E-2			
					$\Sigma=2.0 E-3^*$			
					$\Sigma=3.4 E-2^{**}$			
C4		AIR OPERATED VALVE AHV-1A FAILS TO CLOSE			3.0 E-4			
	ACV AHV-1A	FAILS TO CLOSE	D		3.0 E-4			
					$\pi=6.0 E-7^*$			
					$\pi=1.0 E-5^{**}$			

Table N.4 (2/4) Event "CPE" Quantification

*NON LOSP

**LOSP

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
CPI		NO CONTAINMENT ISOLATION SIGNAL			1.3 E-9			
C5	ESAS (ILB4)	NO REACTOR BUILDING ISOLATION AND COOLING SYSTEM (RBICS) ISOLATION SIGNAL (SEE ESAS)			1.3 E-6			
C6	RADIATION MONITOR COMPARATOR	NO HIGH RADIATION SIGNAL			1.0 E-2			
		FAILS			1.0 E-4	3 ⁺ , 3 ⁻		
		OPERATOR MISCALIBRATES	D		1.0 E-2	3 ⁺ , 3 ⁻		
					<u>E=1.0 E-2</u>			
C01		OPERATOR FAILS TO ISOLATE CONTAINMENT WHEN REQUIRED	D		0.1	3 ⁺ , 10 ⁻	0	
					<u>*=1.3 E-9</u>			

Table N.4 (3/4) Event "CPI" Quantification

Table N.4 (4/4) Event "CPI*" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
CPI*		NO CONTAINMENT ISOLATION SIGNAL			1.0 E-3			
C6		SEE CPI QUANTIFICATION TABLE			1.0 E-2			
C01		SEE CPI QUANTIFICATION TABLE			0.1 r=1.0 E-3			

Table N.5 RBIS - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
C1	2.0 E-3* 3.4 E-2**
C2	3.0 E-4
C3	2.0 E-3* 3.4 E-2**
C4	3.0 E-4
C5	1.3 E-6
C6	1.0 E-2
C01	0.1

*Offsite power available
 **Offsite power not available

APPENDIX P

EMERGENCY FEEDWATER SYSTEM (EFS)

APPENDIX P EMERGENCY FEEDWATER SYSTEM (EFS)

P.1 SYSTEM DESCRIPTION AND OPERATION

The purpose of the Crystal River Emergency Feedwater System (EFS) is to backup the Main Feedwater System (MFS) in removing post shutdown decay heat from the reactor coolant system via the steam generators. During normal shutdowns the MFS is throttled down to a level capable of removing decay heat and the EFS is not utilized. However, if the plant shutdown is caused by a loss of the MFS or if the MFS is lost subsequent to the plant shutdown, then the EFS is put into operation. It is important to note that only in the B&W PWR design is it possible for the MFS to throttle down and remain on line for all shutdowns except those caused by failures in the MFS. Other PWR designs trip the MFS whenever the turbine trips before the reactor, placing the "auxiliary" feedwater system (their backup system) into operation in the majority of shutdowns. This explains why the backup feedwater system at Crystal River is labeled emergency rather than auxiliary.

P.1.1 SYSTEM DESCRIPTION

A diagram of the Crystal River Unit 3 EFS is presented in Figure P.1. The system consists of two interconnected trains, each capable of supplying emergency feedwater to either or both steam generators under automatic or manual initiation and control.

WATER SOURCES

The primary water source for both trains of the Crystal River EFS is the Condensate Storage tank, CDT-1. Water is provided to the pumps through six-inch branch lines which are fed from CDT-1 by a common eight-inch line. Each six-inch branch line contains a normally open AC-powered valve and the common eight-inch line contains a locked-open manual valve.

A reserve of 150,000 gallons is maintained within the tank and is verified by control room indication of level, control room annunciation on low level, and Technical Specification requirements.

An alternate, non-seismic qualified source of water is available for EFS use from the main condenser hotwell. Water is provided to the pumps through eight-inch branch lines which are fed from the hotwell by a common eight-inch line. Each eight-inch branch line contains a normally-closed DC-powered valve and the common eight-inch line contains a normally-open manual valve. The DC-powered valves are interlocked such that they can be opened only if at least one of the two DC-powered vacuum breaker valves is open.

PUMPS AND DISCHARGE CROSS-TIES

The pumps in both trains are Ingersoll-Rand centrifugal horizontal split multi-stage type and are each rated at 740 gpm with a design recirculation flow rate of 20 gpm. Thus each pump is capable of delivering 720 gpm against maximum OTSG pressure to the discharge piping supplying both steam generators.

The Train A pump (EFP-2) is turbine-driven, capable of receiving motive steam from either OTSG or from the auxiliary steam supply from fossil-powered Units 1 and 2. The Train B pump (EFP-1) is motor-driven, powered from diesel-backed ES bus 3A.

The pumps are interconnected at their discharge by separate cross-ties, each containing a normally open DC-powered valve and a check valve. In addition, there is another cross-tie containing two normally closed manual valves.

FLOW CONTROL VALVES

The flow of emergency feedwater to steam generator A (B) is controlled by pneumatic valve FWV-40 (FWV-39). During automatic EFS initiation and control, this valve is under control of the Integrated Control System (ICS) via electric to pneumatic converters. Control for this valve, including manual control, will be described in greater detail in the Instrument and Control section.

Valve FWV-40 (FWV-39) functions both as the emergency feedwater flow control valve and as the startup feedwater flow control valve. During low power operation, flow from the main feedwater pump passes through FWV-41 (FWV-42), is controlled by FWV-40 (FWV-39), and returns to the main feedwater header through FWV-36 (FWV-33); FWV-35 (FWV-34) is closed to prevent this flow from entering the emergency feedwater nozzles.

STEAM SUPPLY FOR EFP-2

Steam for the turbine-driven pump (EFP-2) is extracted immediately downstream of both steam generators. This steam must pass through a normally-open DC-operated stop-check valve (MSV-55 or 56), a check valve (MSV-186 or 187), and a normally closed DC-operated stop valve (ASV-5). Initiation of the turbine-driven pump is accomplished by opening this stop valve. Initiation signals are described in the Instrument and Control section.

In addition, an alternate source of steam is available from fossil-powered Units 1 and 2 which connect immediately upstream of ASV-5. Lineup of this source requires local, manual operation of valves at Unit 3.

OTHER SYSTEM FEATURES

The primary components for EFS operation following a loss of the main feedwater system are described above. There are additional system features, however, which affect overall system performance. These features are described below:

Steam Line Rupture Matrix: This feature is a redundant Class IE logic matrix that senses low steam generator pressure and isolates the generator with low pressure by closing main steam isolation valves, main feedwater isolation valves and emergency feedwater isolation valves FWV-35, 36, and 162 for SG-A or FWV-33, 34, and 161 for SG-B.

Remote Manual Bypass Valves: A Remote-manual, normally open, DC powered bypass valve is provided in each EFS supply line to the steam generators (FWV-162 for SG-A and FWV-161 for SG-B). These valves provide a back-up means of controlling EFS flow should the ICS-controlled valves (FWV-40, 39) fail for any reason. They are pre-throttled to provide approximately 550 gpm to each steam generator at design pressure.

VALVE INDICATIONS AND OPERABILITY

All AC- and DC-powered valves fail "as is" on the loss of electric power. All such valves shown in Figure P.1 are controllable from the control room and their position is indicated in the control room. Power for the indication and control of these valves is derived from the power source for the respective valve motors. Only four valves (EFV-4 and 8 for SG-A and EFV-3 and 7 for SG-B) are AC-powered (non-vital) and they are normally open.

The pneumatic flow control valves (FWV-40, 39) will fail "as is" on loss of supply air pressure. An air lock is provided that senses low air pressure and de-energizes a solenoid valve to lock the existing air pressures across the control valve piston. An air reservoir is provided for each valve which allows remote-manual opening of the control valve when normal supply air is lost. This is accomplished using DC-powered solenoid valves to direct air from the reservoir to the underside of the control valve piston while venting the top of the piston. Loss of power to the electric/pneumatic converters will result in the valves assuming a position of approximately half-open.

In addition to the backup air supply, further reliability is achieved by the provision of remote-manual DC-powered valves (FWV-162, 161).

SYSTEM INTERFACES

Cooling Systems

Cooling water for the EFS pumps is required for successful operation of the EFS. At the time the analysis was performed, both pumps were cooled

by water provided by the Nuclear Services Closed Cycle Cooling System (NSCCCS), which thus creates an undesirable AC-power dependency for this system. Florida Power Corp. had recognized this dependency and proposed to eliminate it by modifying the pump cooling design to make both pumps self cooled.* For this reason, the analysis herein assumes the EFS pumps are self-cooled.

The pumps are separated by a missile wall and are located in the intermediate building. The intermediate building is cooled by two 100% air fan subsystems. The main steam lines also run through this building at an elevation above the pumps. Missile protection is provided by internal building structure but the pumps and steam lines are in air communication.

Lubricating System

Lubricating oil for the EFS pumps is an integral system powered by the pump shaft, and requires no electrical input.

Electric Power Systems

Simplified diagrams showing power distribution for the EFS are shown in Figures P.2 through P.4. The motor-driven emergency feedwater pump (EFP-1) AC power interface is shown in Figure P.2. EFS automatic start control circuit power dependencies are shown in Figure P.3. It can be noted from Figure P.5 that DC power is required to close the breaker for the motor-driven pump. DC-powered EFS valves are powered as shown in Figure P.3. AC-powered valves (EPV-3, 4, 7, and 8) are not diesel backed and are powered as shown in Figure P.4; these valves are normally open and fail "as is" on loss of power. Flow paths from each pump to both steam generators are available without any valve repositioning.

*FPC has indicated that both the turbine-driven and electric-driven pumps will be modified. It is noted, however, that only the modification to the turbine-driven pump will cause a significant improvement in predicted system reliability.

In the event of loss of main feedwater induced by loss of offsite power, the motor-driven EFS pump (EFP-1) will not start automatically; it must be manually loaded on the diesel. Loss of offsite power will also result in a loss of normal air supplies but backup is available as previously described. The follow up action in the plant operating procedure for loss of offsite power requires manual loading of air compressors on the diesels.

In the event of a total loss of AC power (offsite and diesels), the EFS flow will be initiated through the DC-powered steam supply valve and the turbine driven pump.

INSTRUMENTATION AND CONTROL

Initiation Logic

A simplified diagram of EFS initiation is shown in Figure P.5. This diagram is functional in nature and does not represent actual hardware. The actual logic is contained in relay racks and the individual component controllers. Automatic initiation will occur whenever one of two conditions exists: loss of both main feedwater pumps or low level in both steam generators. The non-redundant single train logic in the relay cabinets de-energizes a relay to initiate the EFS. A loss of the vital 120VAC source powering these cabinets will also cause initiation. The automatic initiation will open ASV-5 and MSV-55 (MSV-55 and 56 are normally open) to start the turbine-driven pump. The initiation signal also causes the circuit breaker to start the motor-driven pump provided the two interlocks described below are satisfied. Once a pump is started, EFS flow will exist since the flowpaths, including the discharge cross-connects, are normally open.

In addition, the motor-driven pump is interlocked to prevent automatic start unless offsite power is available on the ES bus and one of the suction valves (EFV-2 or 3) is open.

A key-operated bypass is provided to prevent inadvertent initiation of the EFS when the main feedwater pumps are secured during normal startups and shutdowns. This bypass feature does not have automatic removal but it is under administrative control. Initiation on low steam generator level is provided as a backup means of ensuring EFS initiation and this actuation feature is not bypassed.

Flow Control

Normal control of EFS flow is achieved with flow control valves FWV-39 and 40. The ICS senses the loss of main feed pumps or low level in the steam generators and opens the EFS Block Valves (FWV-34 and 35) and closes the Main Feedwater Connections (FWV-33 and 36). This directs EFS flow through FWV-39 and 40 to the upper nozzles in the steam generators.

FWV-39 and 40 are pneumatic-operated valves and are normally controlled by the ICS via electric/pneumatic converters. The ICS adjusts these valves to attain and maintain one of two steam generator level set-points, depending on reactor coolant pump (RCP) status. If the RCP's are running, the low level is maintained. If the RCP's are off, the high set-point is maintained in order to promote natural circulation in the reactor coolant system. A loss of the ICS control signal will result in the valve failing to a position approximately 50% open. On loss of supply air pressure, the valve will fail "as is", which, depending on SG level at the time of failure, could be the closed position.*

In addition to the backup provisions for FWV-39 and 40, DC-powered bypass valves (FWV-161 and FWV-162) are provided. These valves are pre-throttled to allow a flow rate of approximately 550 gpm to each steam generator, to ensure flow is established should FWV-34, 35, 39, or 40 fail. Once EFS initiation occurs, the operator will verify proper operation of the normal flow control path and then close FWV-161 and 162. Failure to close these valves could result in a rapid cool down transient.

*However, each valve has associated with it an air accumulator allowing for 2-3 full valve strokes.

Instrumentation

The availability of several important instrument indicators in the control room for three specific incident initiators is tabulated below:

<u>Indication</u>	<u>Loss of MFW</u>	<u>Loss of MFW Due to Loss of Offsite Power</u>	<u>Loss of All AC Power</u>
CDT-1 level	Yes	No	No
CDT-1 level alarms	Yes	Yes	Yes
EFW flow	Yes	Yes	Yes
Valve positions	Yes	Yes*	Yes*
OTSG level	Yes	Yes	Yes
OTSG level alarms	Yes	Yes	Yes

*for all except AC-powered valves ESW-3, 4, 7, 8

Steam Line Rupture Matrix

Operation of the EFS can be affected by the steam line rupture matrix (SLRM).

The SLRM detects low steam pressure in either steam generator and will isolate a generator if a low pressure condition exists; low pressure must be detected by two pressure switches, one set at 725 psig, the other at 600 psig (see Figure P.6). The isolation signal will cause closure of the main steam isolation valves, main feedwater isolation valves, and emergency feedwater isolation valves for the affected steam generator.

The SLRM is a safety-grade system provided with battery-backed power and coincidence logic in the actuation circuitry. Inadvertent actuation of the SLRM could cause isolation of one steam generator.

OPERATOR ACTIONS

For a loss of MFW, no operator action is required to establish EFS flow. The operator will verify proper flow control and adjust FWV-161 and 162 as required. Certain failures (e.g., mispositioned valves, pump fail to auto start, etc.) have the potential of being corrected from the control room.

The only significant differences for a loss of MFW induced by loss of offsite power are as follows:

- a. The motor-driven pump must be manually loaded onto the ES bus (from the control room).
- b. Failure involving AC-powered valves EFW-3, 4, 7, or 8 would require local manual correction since they are not attached to an emergency bus.

In the event of total loss of AC power, the turbine-driven pump would start automatically and all the DC-powered valves would be operable from the control room.

Testing

The ability of either of the two pumps to deliver a minimum of 550 gpm to either steam generator with the reactor at power is verified every eighteen months (Procedure PT-123). The ability of both pumps to start automatically upon receiving the actuation signals is verified during hot shutdown every eighteen months (Procedure PT-122). Both procedures verify that the EFS can be controlled independent of the ICS. Additional automatic actuation is also verified during cold shutdown at which time automatic valve actuations by the ICS are tested (Procedure SP-416).

EFS valves are cycled once each quarter. After cycling they are verified to be in the correct position by two independent valve lineup checks. Valves with position indication in the control room are verified to be in the correct position daily. A monthly operability check of each pump is performed using the normal recirculation flow paths (Procedures SP-349 and SP-350). These checks, made on a staggered schedule for the two pumps, confirm the pumps capability to produce the required pump discharge pressure. These checks require closure of the associated stop-check valve (EFV-7 or EFV-8). Following the tests, proper valve lineup is ensured by two independent checks.

Maintenance

Maintenance acts which require isolation of one component in the EFS occur about every quarter. The EFS has 14 active components (AOV's, MOV's, pumps) capable of being isolated without violating technical specifications (e.g., isolation of EFV-3, EFV-4, MSV-55, MSV-56, FWV-39, or FWV-40 would violate technical specifications). Isolation is achieved by closing the appropriate upstream and downstream valves from the component under maintenance.

Technical Specification Limitations

The limiting condition for operation of the EFS requires that two independent emergency feedwater pumps and associated flow paths be operable with:

- a. One emergency feedwater pump capable of being powered from an operable emergency bus.
- b. One emergency feedwater pump capable of being powered from an operable steam supply system.

If one emergency feedwater system becomes inoperable, it must be restored to an operable condition within 72 hours or the plant must be placed in hot shutdown within the next 12 hours.

The technical specifications also require the availability of 150,000 gallons of water in the condensate storage tank (CDT-1) for EFS use.

P.1.2 SYSTEM OPERATION

The simplified schematic of the EFS presented in Figure P.1 shows that the EFS is a two train system with a steam driven turbine pump train and an electric pump train. The pump trains draw water from either the condensate storage tank (preferred) or from the condenser hot-wells and deliver to the steam generators. Either pump can feed either steam generator through interties at the pumps' discharge. Steam required to operate the turbine pump is extracted from either steam generator upstream of the four main steam isolation stop valves.

Both pump trains are started automatically following all loss of MFW events which do not involve offsite power. The pumps may also be started manually from the control room. For loss of offsite power cases, the turbine pump train starts automatically but the electric pump is started manually from the control room. Successful operation of the EFS requires full flow from one pump to the secondary side of either steam generator and discharge of the generated steam to either the condenser or atmosphere. It is also required that either forced or natural circulation be maintained on the primary side of the steam generator receiving the EFS cooling. If this is not established, the decay heat produced by the reactor will not be transmitted to the secondary side of the steam generators.

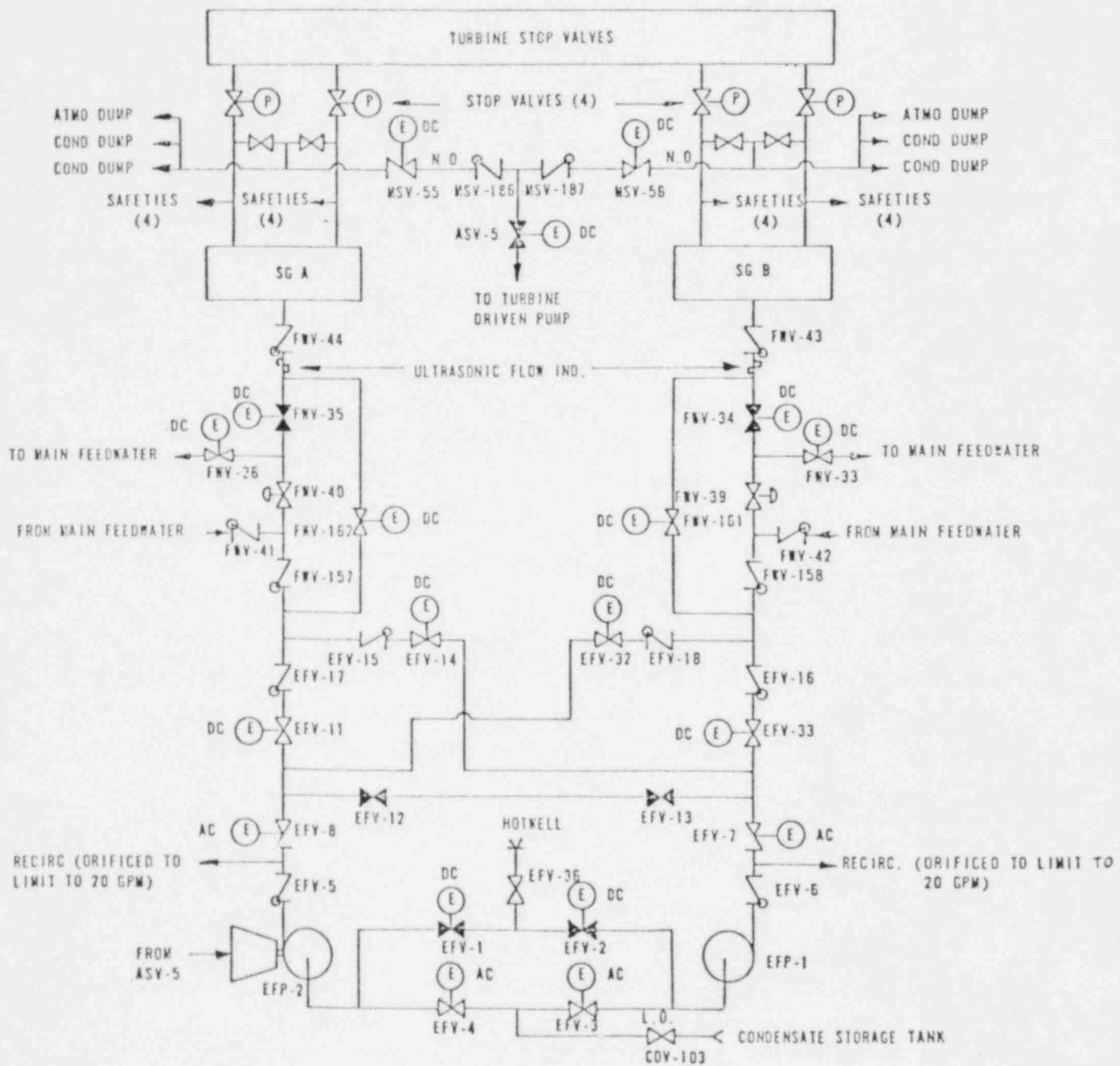
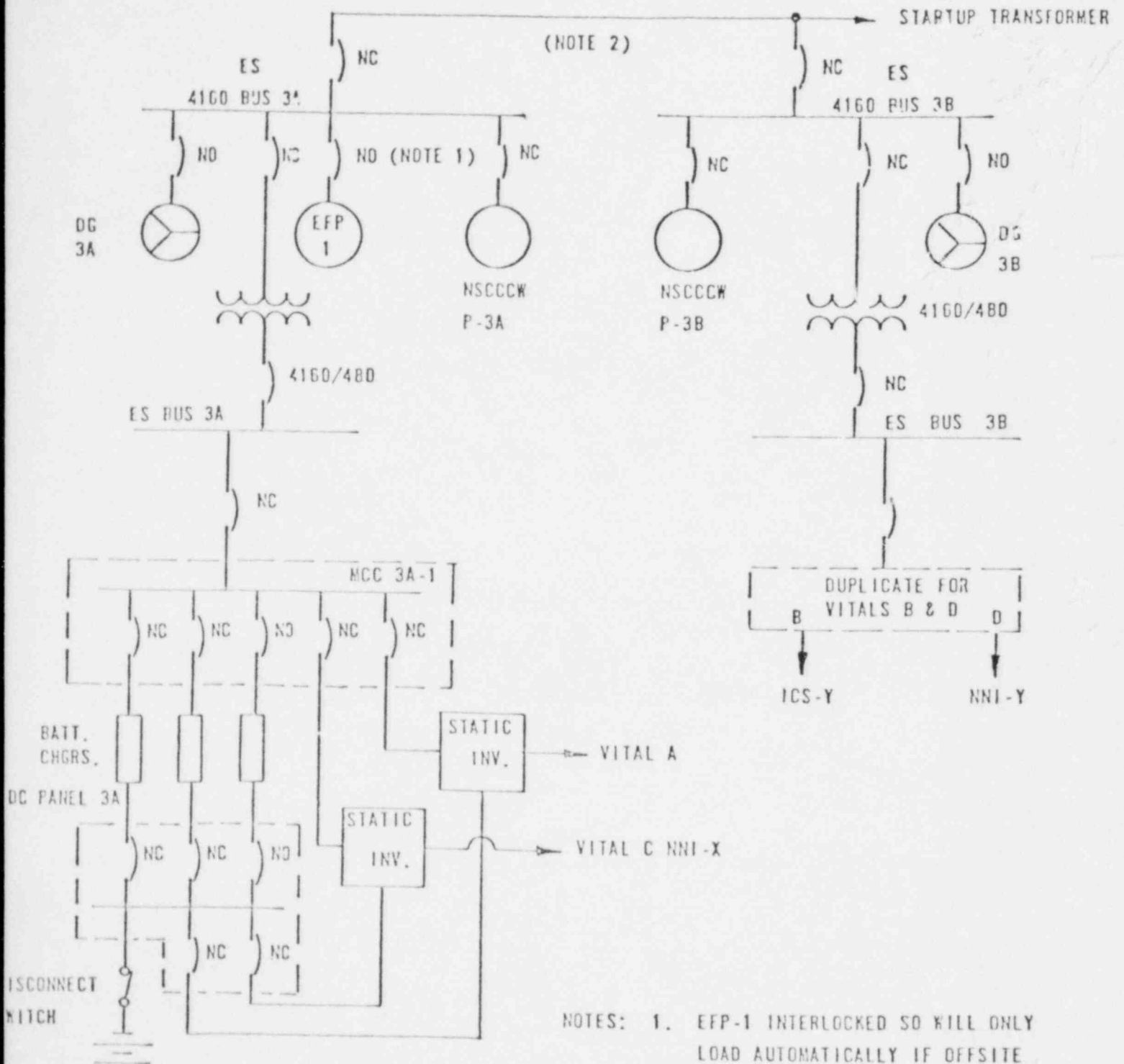


Figure P.1 Emergency Feedwater System Schematic Diagram



- NOTES: 1. EFP-1 INTERLOCKED SO WILL ONLY LOAD AUTOMATICALLY IF OFFSITE POWER ON BUS 3A.
2. TWO ALTERNATE SOURCES AVAILABLE MANUALLY; UNIT 1/2 STARTUP XFMR WITHIN MINUTES AND UNIT 3 AUX. XFMR WITHIN EIGHT HOURS.

Figure P.2 Simplified Power Source Diagram
 P-13

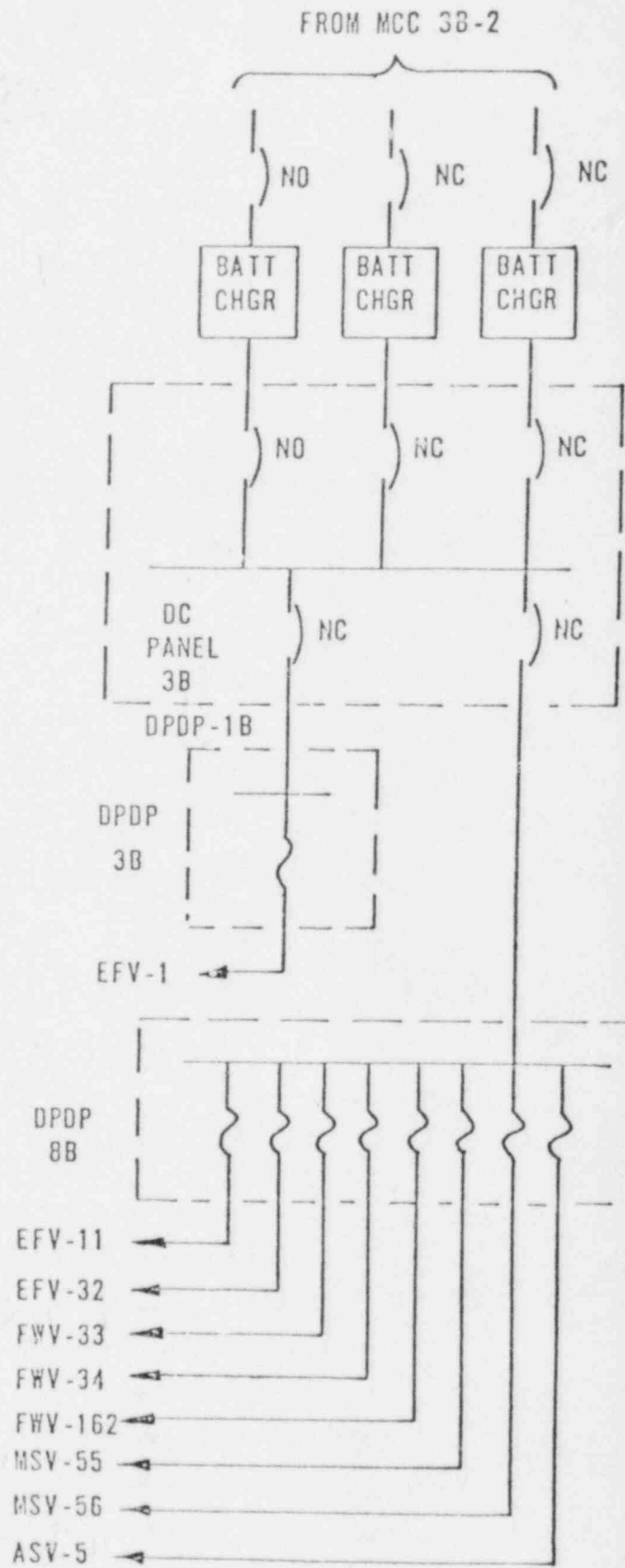
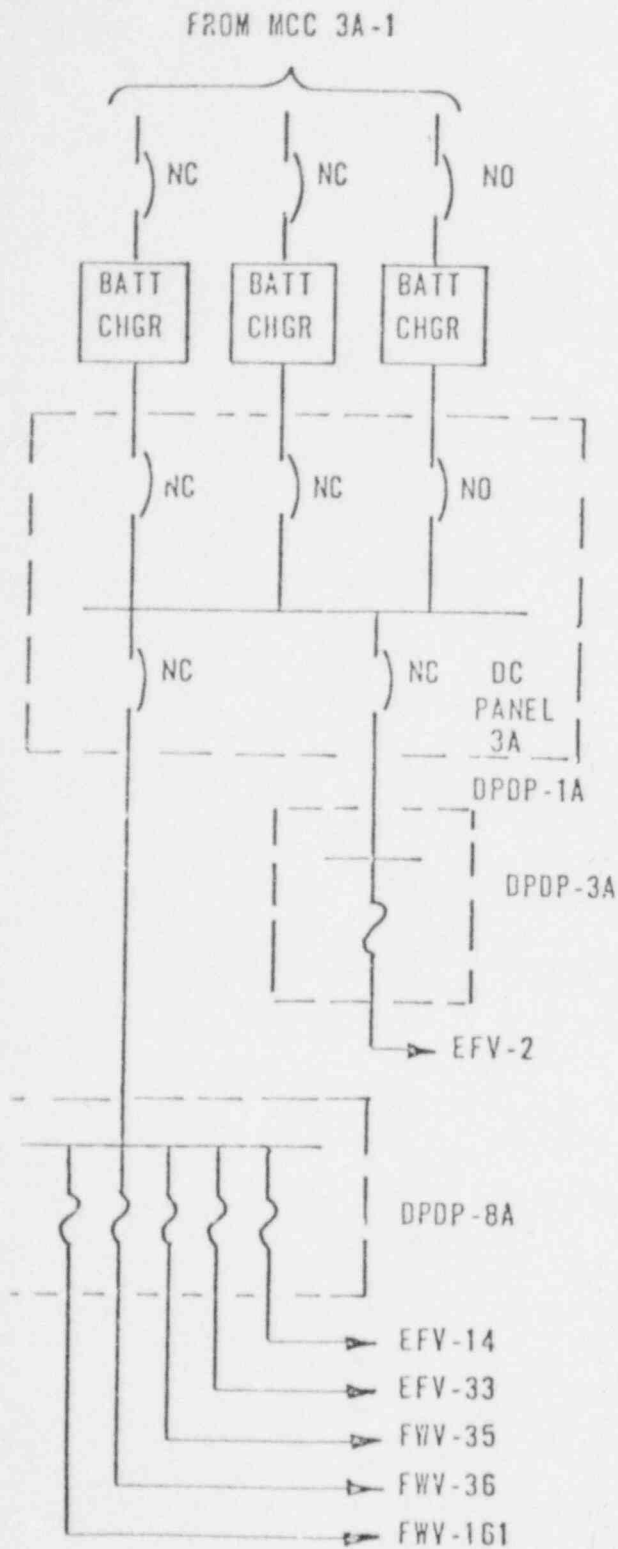


Figure P.3 Simplified Power Source Diagram
DC Loads

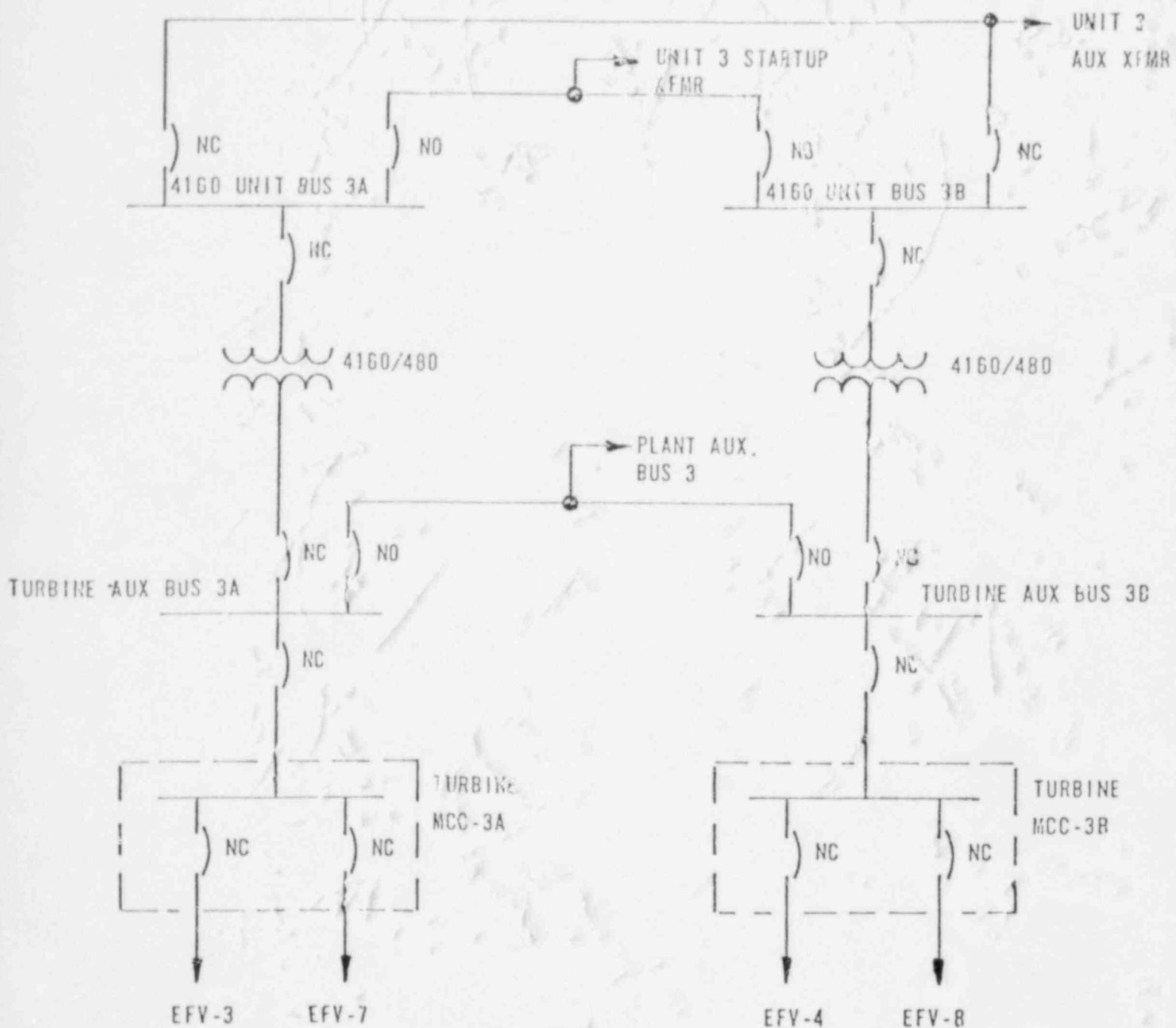


Figure P.4 Simplified Power Source Diagram
AC Valves

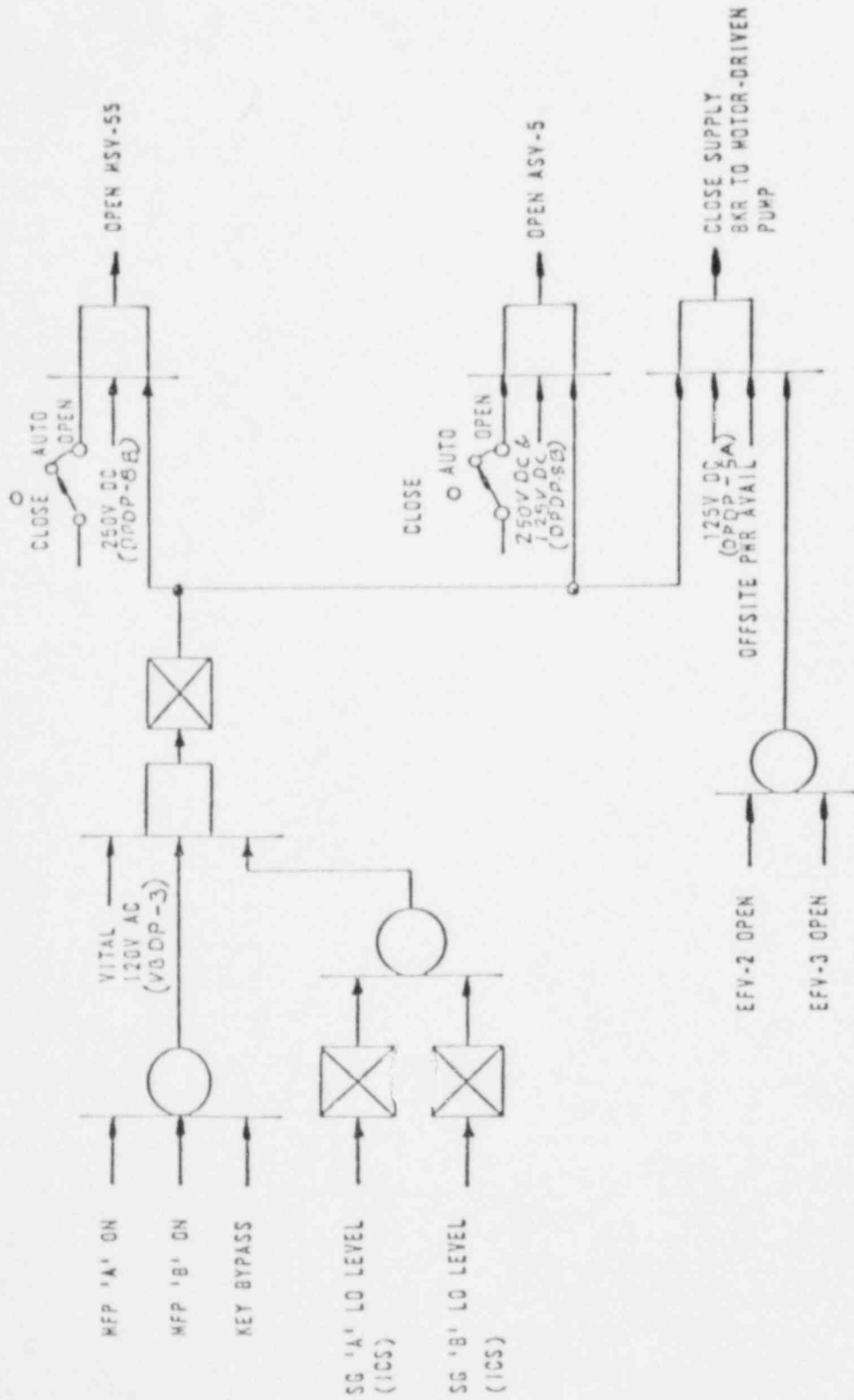


Figure P.5 Pump Start Logic

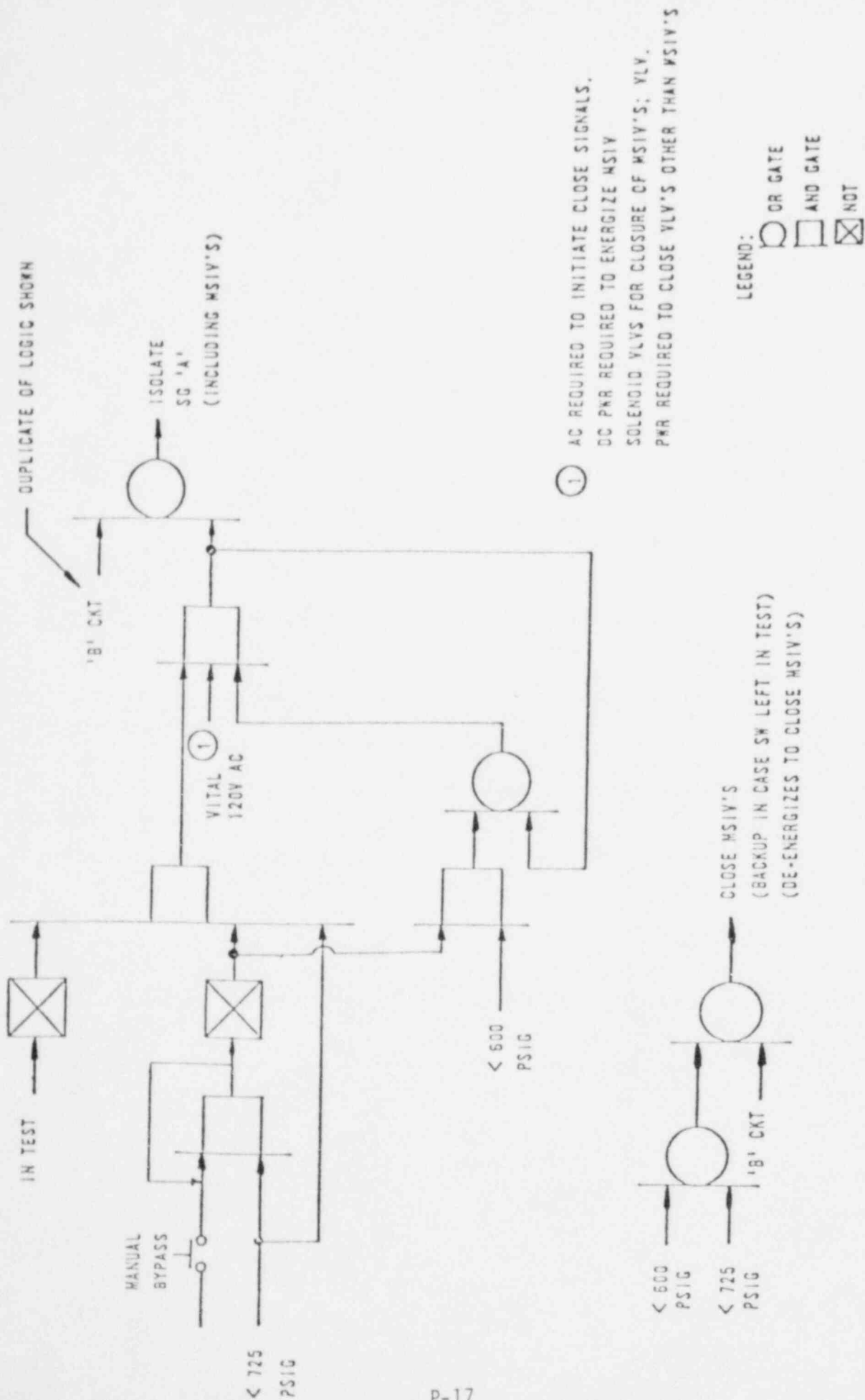


Figure P.6 SLRM Logic ("A" Circuit Shown)

P.2 SYSTEM SIMPLIFIED FAULT TREE

The top event representing the failure definition is "EFS Fails to Remove Reactor Coolant System Decay Heat Via One of Two Steam Generators". EFS failure therefore occurs if both pump trains do not provide adequate flow (550 gpm initially) to the secondary side of either steam generator. The simplified EFS fault tree is presented in Figure P.7.

MAJOR ASSUMPTIONS

The assumptions made during the development of the EFS simplified fault tree include:

1. Component outages due to maintenance are considered on active components only.
2. Component outages due to test are generally negligible. All active valves are cycled quarterly and the test duration is short enough to cause a negligible outage. However, during monthly tests of the pumps, valves EFV-7 and EFV-8 are closed for a much longer period and the test outage was therefore considered.
3. No common mode coupling was assumed between valves which have open and closed status indication in the control room. All of these valves undergo a status check by the operators at least once per shift. Common mode coupling was considered between certain groups of manual valves however.
4. Although separate control circuits are provided within the ICS to control the flow of EFS to either of the steam generators, the ICS was assumed to consist of only a single control device with signals to both EFS trains. This approach was taken due to the complexity of the ICS and the time limitations imposed on this study.
5. Credit was given for an alternate water source from the hotwell should suction be lost from the condensate storage tank (see also quantification tables).

6. Although an alternate source of steam is available to the turbine-driven pump from fossil-powered Units 1 and 2, this was not considered in the analysis. Use of this steam requires operation of manual valves in Unit 3.
7. Intermediate building cooling is not important to the operation of the EFS pumps since the large building would probably heat up relatively slowly if cooling was lost. Also, the electric pump motor windings are forced air cooled through a NSCCCS heat exchanger which is independent from the intermediate building cooling system.

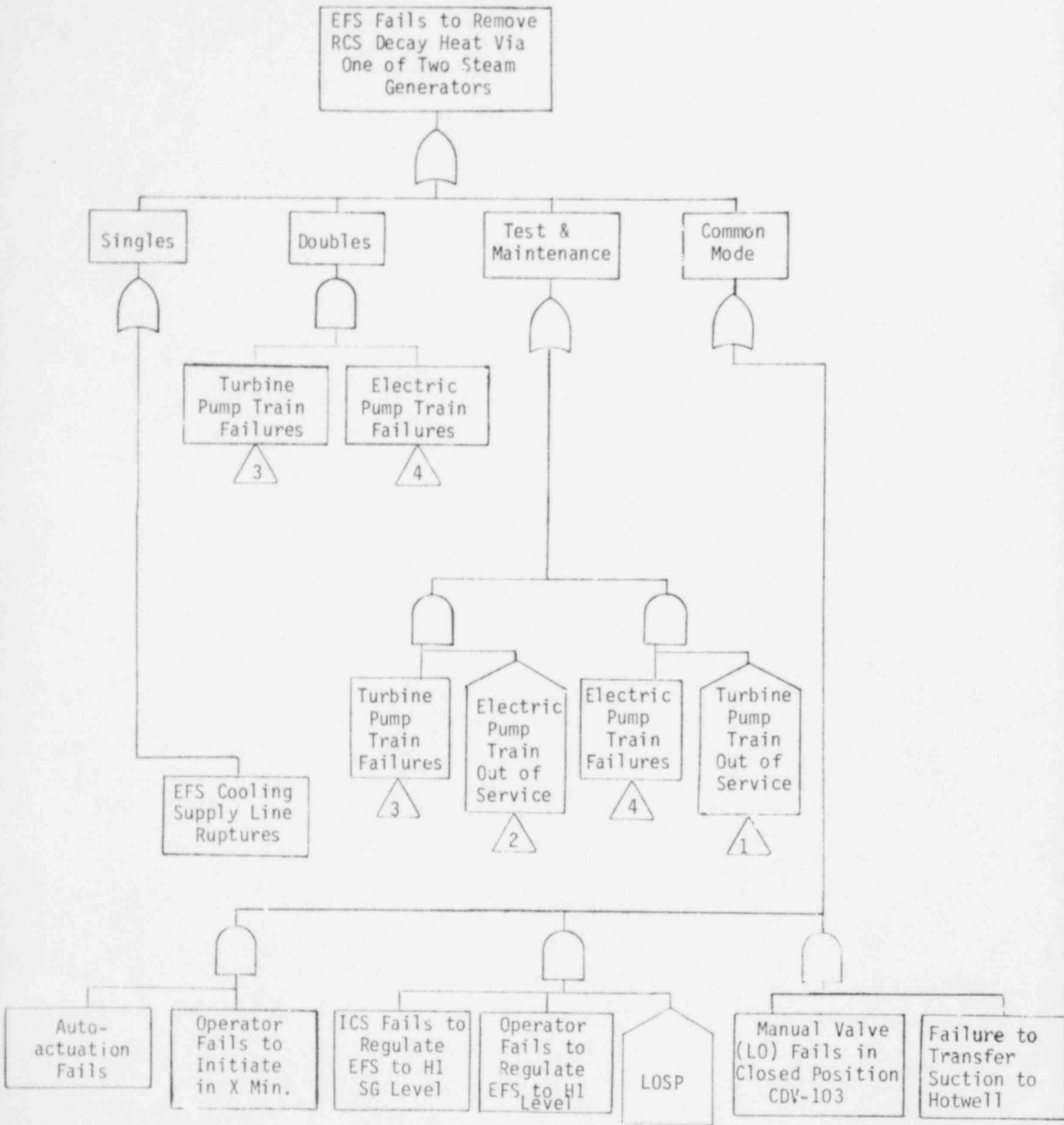


Figure P.7 (1/3) Simplified Fault Tree - Emergency Feedwater System

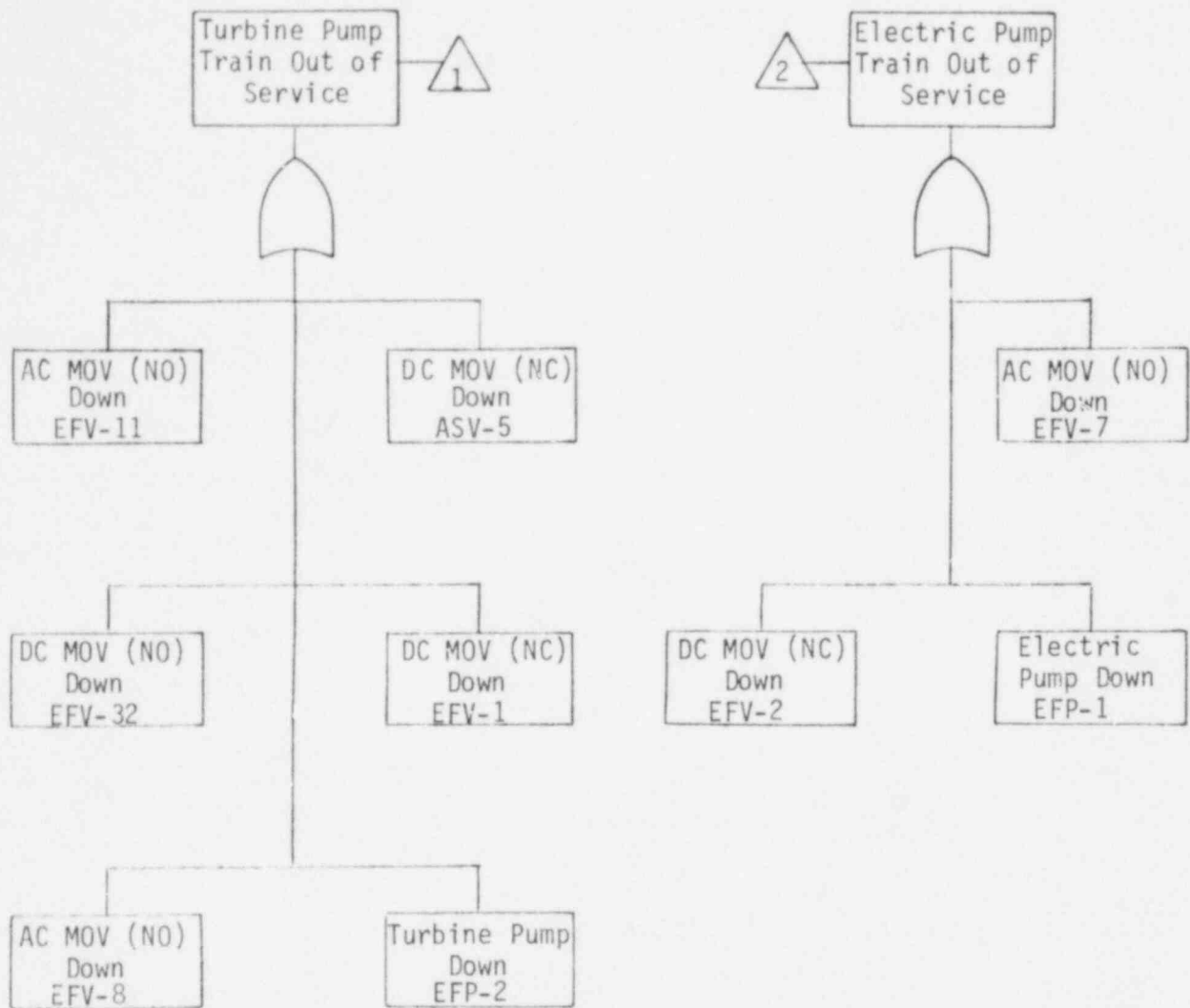


Figure P.7 (2/3) Simplified Fault Tree - Emergency Feedwater System

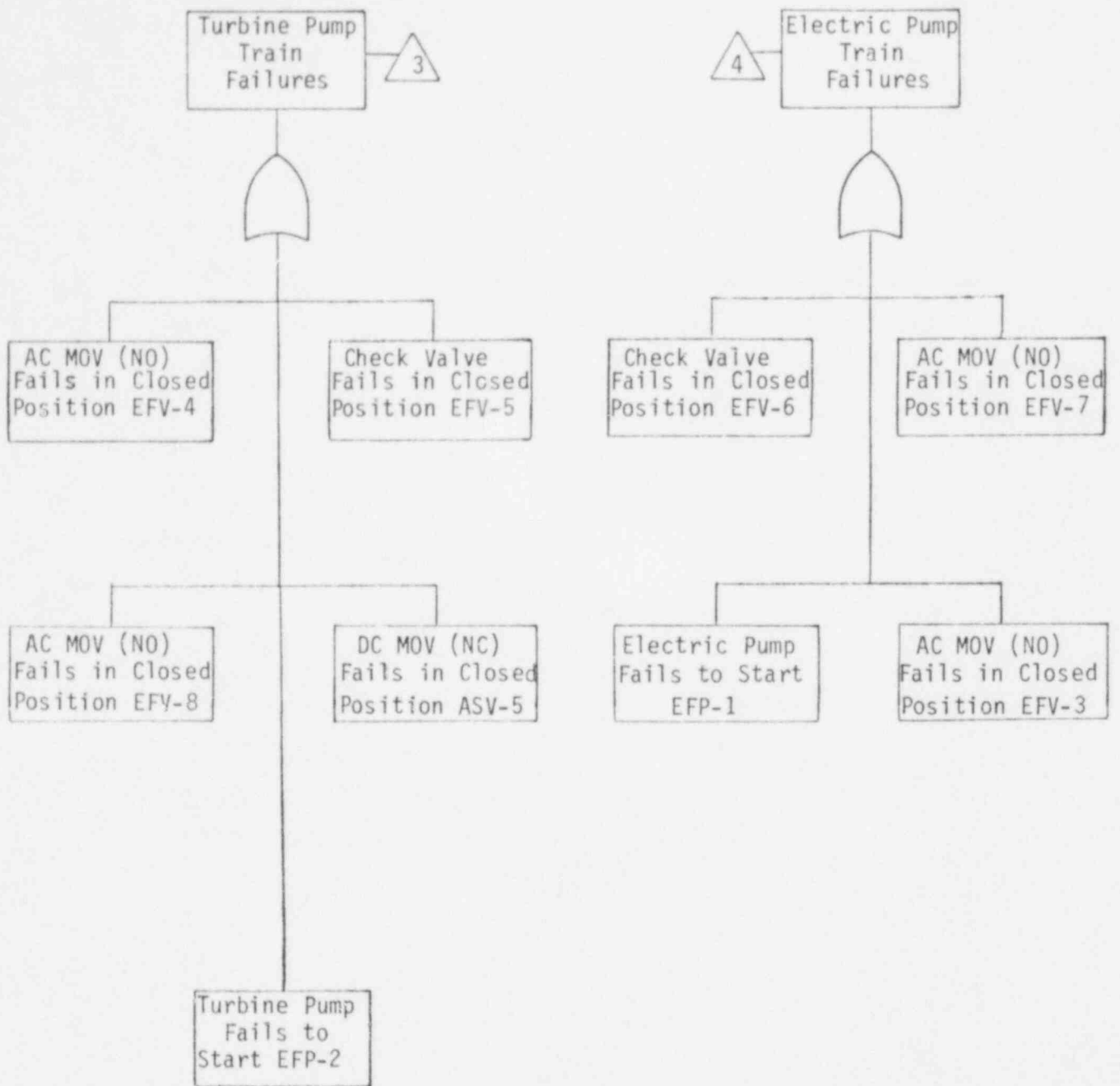


Figure P.7 (3/3) Simplified Fault Tree - Emergency Feedwater System

P.3 SYSTEM QUANTIFICATION

P.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The Crystal River EFS is basically a two train system with system success defined as successful operation of one of the two trains. Motive power diversity is achieved by employing a turbine-driven pump in Train A and a motor-driven pump in Train B. The turbine-driven pump is self-cooled so system operation is not dependent on AC power. However, DC power is required to open the turbine-driven pump steam admission valve (DC Train B).

For cases where off-site power is available, the unavailability of the EFS was assessed to be principally due to maintenance outages, combinations of hardware failures on both Train A and Train B (double failure), and operator error. Each of these factors is responsible for approximately equal contributions to total system unavailability. For cases where off-site power is lost, the principal contributors to system unavailability are double hardware failures and maintenance outages, which are about an order of magnitude larger than in the non-LOSP case. These contributions are larger here primarily because of the large diesel failure rate, which raises the unavailability of Train B (the motor-driven pump train). Thus, the double failure combinations are dominated by diesel failure and failure of the turbine-driven pump. Turbine-driven pump failure rates were assumed to be about an order-of-magnitude higher than motor-driven pump failure rates - see fault tree quantification tables, and notes for additional details.

P.3.2 SYSTEM FAULT TREE QUANTIFICATION

Two modularized fault trees were constructed for the EFS, one for the case where offsite power is available, and one for the LOSP case.

Table P.1 shows the EFS success requirements with attached notes. Table P.2 contains the top event definitions for the two modularized fault trees. Figures P.8 and P.9 show the two EFS fault trees in terms of the major gates. A point estimate unavailability is shown on these trees for each gate and for the system. Table P.3 shows the Boolean equations that represent the EFS fault trees. Table P.4 shows the quantification of each gate, by component and failure mode for the two fault trees. The attached notes explain the assumptions used in the quantification. Table P.5 summarizes the point estimates for each gate.

Table P.1 EFS - System Success Requirements

<u>INITIATOR</u>	<u>TRAINS</u>	<u>NOTES</u>
T ₂ - T _{2A}	1/2	1
T _{2A}	1/2	2

-
- NOTES: 1. This group of initiators involves loss of main feedwater by any means other than loss of offsite power. A separate tree is developed for this set of initiators, although the success requirements are the same as for the loss of offsite power case.
2. This initiator is loss of main feedwater due to loss of off-site power. A separate tree is developed for this initiator.

Table P.2 EFS Top Event Definition

<u>BOOLEAN REPRESENTATION</u>	<u>TOP EVENT</u>	<u>NOTES</u>
EF1	Failure of EFS to provide at least 1/2 pump flow to at least 1/2 OTSGs given offsite power is available.	---
EF2	Failure of EFS to provide at least 1/2 pump flow to at least 1/2 OTSGs given offsite power is not available.	---

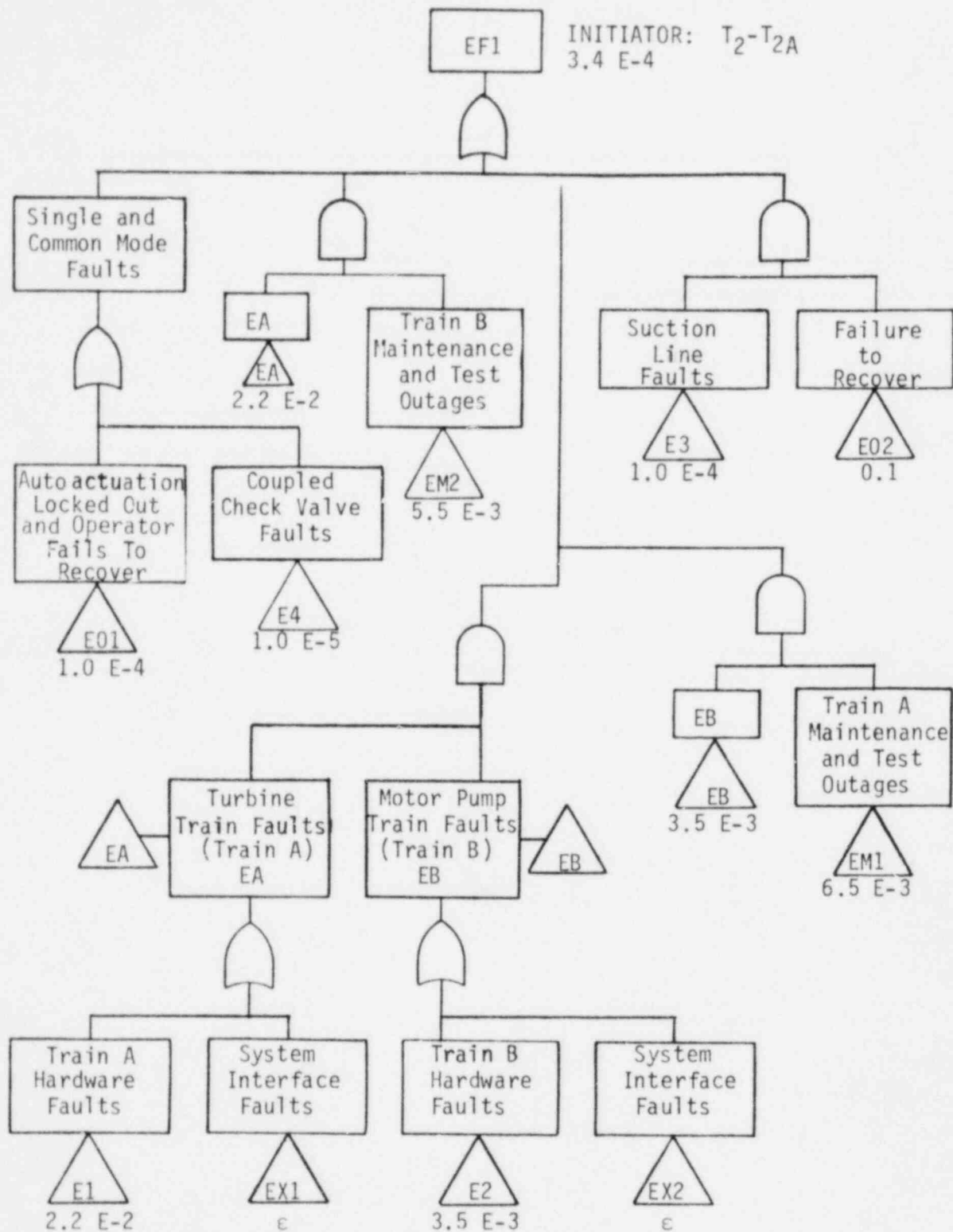
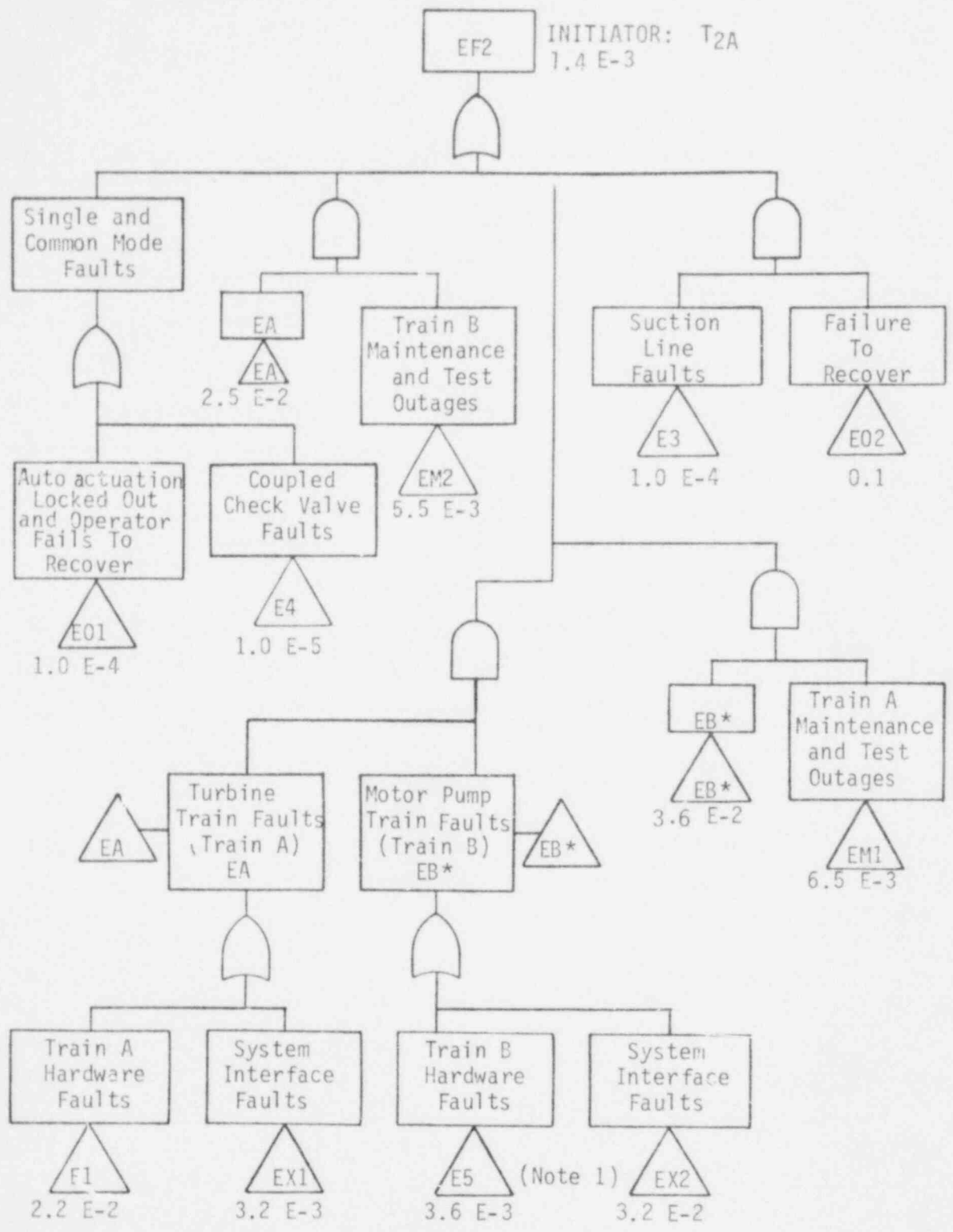


Figure P.8 Modularized Fault Tree for Event "EF1" (Offsite Power Available)



Note 1: Gate E 5 differs from Gate E 2 in that it includes operator faults not contained in Gate E 2

Figure P.9 Modularized Fault Tree for Event "EF2" (Offsite Power Not Available)

Table P.3 Emergency Feedwater System

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

$$EF1 = E01 + E4 + EA \cdot EB + EA \cdot EM2 + EB \cdot EM1 + E3 \cdot E02$$

$$EF2 = E01 + E4 + EA \cdot EB^* + EA \cdot EM2 + EB^* \cdot EM1 + E3 \cdot E02$$

INTERMEDIATE EVENTS

$$EA = E1 + EX1$$

$$EB = E2 + EX2$$

$$EB^* = E5 + EX2$$

$$EX1 = DCB$$

$$EX2 = ACA + DCA$$

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
E01		AUTO ACTUATION LOCKED OUT AND OPERATOR FAILS TO RECOVER			1.0 E-4	10 ⁺ , 10 ⁻	0	12
E03	OPERATOR	LOCKS OUT AUTO ACTUATION	D		1.0 E-3	10 ⁺ , 10 ⁻	0	
E04	OPERATOR	FAILS TO RECOVER	D		0.1	10 ⁺ , 10 ⁻	0	
					$\Sigma=1.0 E-4$			
E4		COUPLED CHECKVALVE FAULTS (FWV-43, 44)	1.0 E-4(0.1)		1.0 E-5	2 ⁺ , 2 ⁻	B	
EA		TURBINE TRAIN FAULTS (TRAIN A)						
E1		TRAIN A HARDWARE FAULTS			2.2 E-2	3 ⁺ , 3 ⁻	S	
	MOV EFV-4	INADVERTENTLY CLOSED	D		3.0 E-6	10 ⁺ , 10 ⁻		1
	MOV EFV-4	PLUGGED	D		1.0 E-4	3 ⁺ , 3 ⁻		
	MOV EFV-8	INADVERTENTLY CLOSED	D		3.0 E-4	10 ⁺ , 10 ⁻		2
	MOV EFV-8	PLUGGED	D		1.0 E-4	3 ⁺ , 3 ⁻		
	EFV-5	CHECKVALVE FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
	ASV-5	FAILS CLOSED	D		1.0 E-3			
	ASV-5	AUTO ACTUATION LOCKED OUT AND OPERATOR FAILS TO RECOVER	D		1.0 E-4	3 ⁺ , 10 ⁻		3, 12
	CTRL. CIRCUIT	FAILS TO TRANSFER (RELAY FAILS TO ENERGIZE)	D		1.0 E-4	3 ⁺ , 3 ⁻		
	EFP-2	TURBINE PUMP FAILS TO START	D		2.0 E-2	3 ⁺ , 3 ⁻	S	4
	EFP-2	TURBINE PUMP FAILS TO RUN FOR 24 HRS	3.0 E-5/HR	24	7.2 E-4	10 ⁺ , 10 ⁻		5
					$\Sigma=2.2 E-2$			
EX1		SYSTEM INTERFACE FAULTS (NON LOSP)			c			
DCB	DC E8B	DC POWER TRAIN B FAILS						
		NON LOSP			c			
EB		MOTOR PUMP TRAIN FAULTS (TRAIN B)						
E2		TRAIN B HARDWARE FAULTS			3.5 E-3	2.4 ⁺ , 1.5 ⁻	0	
	MOV EFV-3	INADVERTENTLY CLOSED	D		3.0 E-6	10 ⁺ , 10 ⁻	0	1
	MOV EFV-3	PLUGGED	D		1.0 E-4	3 ⁺ , 3 ⁻		
	MOV EFV-7	INADVERTENTLY CLOSED	D		3.0 E-4	10 ⁺ , 10 ⁻	0	2
	MOV EFV-7	PLUGGED	D		1.0 E-4	3 ⁺ , 3 ⁻		
	EFV-6	CHECK VALVE FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
	EFP-1	MOTOR PUMP FAILS TO START	D		1.0 E-3	3 ⁺ , 3 ⁻		
	EFP-1	MOTOR PUMP FAILS TO RUN FOR 24 HRS	3.0 E-5	24	7.2 E-4	10 ⁺ , 10 ⁻		
	CTRL. CIRCUIT	FAILS TO ACTUATE (RELAY)	D		1.0 E-4	3 ⁺ , 3 ⁻		
	EFP-1 BRK.	FAILS TO TRANSFER	D		1.0 E-3	3 ⁺ , 3 ⁻		
	AUTO. ACT.	AUTO-ACTUATION LOCKED OUT AND OPERATOR FAILS TO RECOVER	D		1.0 E-4	3 ⁺ , 10 ⁻	0	6, 12
					$\Sigma=3.5 E-3$			

Table P.4 (1/4) Event "EF1" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
EX2	DCA DC ESA	SYSTEM INTERFACE FAULTS (NON LOSP)			ε			
		DC POWER TRAIN A FAILS NON LOSP			ε			
ACA		AC TRAIN A FAILS NON LOSP			ε			
		LOSP			3.2 E-2			
EI11		TRAIN A MAINTENANCE AND TEST OUTAGES			6.5 E-3	3+, 3-	M	7, 8
	MOV EFV-11	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3+, 3-	M	10
	MOV EFV-32	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3+, 3-	M	10
	MOV ASV-5	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3+, 3-	M	10
	MOV EFV-8	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3+, 3-	M	10
	EFP-2	OUT FOR MAINTENANCE	.1/720	19	2.6 E-3	3+, 3-	M	8
					Σ=6.5 E-3			
EI12		TRAIN B MAINTENANCE AND TEST OUTAGES			5.5 E-3	3+, 3-	M	7, 8
	MOV EFV-14	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3+, 3-	M	10
	MOV EFV-33	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3+, 3-	M	10
	MOV EFV-7	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3+, 3-	M	10
	EFP-1	OUT FOR MAINTENANCE	.1/720	19	2.6 E-3	3+, 3-	M	8
					Σ=5.5 E-3			
E3	CDV-103	SUCTION LINE FAULTS VALVE PLUGGED	D		1.0 E-5	2+, 2-	0	
E02	OPERATOR	FAILS TO RECOVER	D		1.0 E-4	3+, 3-		
					0.1	2+, 2-	0	9
					Σ=1.0 E-5			

Table P.4 (2/4) Event "E11" Quantification

Table P.4 (3/4) Event "EF2" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE (HR ⁻¹)	FAULT DURATION (HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
E01		AUTO-ACTUATION LOCKED OUT AND OPERATOR FAILS TO RECOVER			1.0 E-4	10 ⁺ , 10 ⁻	0	12
E03	OPERATOR	LOCKS OUT AUTO-ACTUATION	D		1.0 E-3	10 ⁺ , 10 ⁻	0	
E04	OPERATOR	FAILS TO RECOVER	D		0.1	3 ⁺ , 10 ⁻	0	
					$\pi=1.0$ E-4			
E4		COUPLED CHECKVALVE FAULTS (FNV-43, 44) (1.0 E-4X0.1X)			1.0 E-5	2 ⁺ , 2 ⁻	B	
E4		TURBINE TRAIN FAULTS (TRAIN A)						
E1		TRAIN A HARDWARE FAULTS						
	MOV EFV-4	INADVERTENTLY CLOSED	D		2.2 E-2	3 ⁺ , 3 ⁻	S	1
	MOV EFV-4	PLUGGED	D		3.0 E-6	10 ⁺ , 10 ⁻		
	MOV EFV-8	INADVERTENTLY CLOSED	D		1.0 E-4			2
	MOV EFV-3	PLUGGED	D		3.0 E-4	10 ⁺ , 10 ⁻¹		
	EFV-5	CHECKVALVE FAILS TO OPEN	D		1.0 E-4			
	ASV-2	FAILS CLOSED	D		1.0 E-3			
	ASV-5	AUTO-ACTUATION LOCKED OUT AND OPERATOR FAILS TO RECOVER	D		1.0 E-4	3 ⁺ , 10 ⁻		3, 12
	CTRL. CIRCUIT	FAILS TO TRANSFER (RELAY FAILS TO ENERGIZE)	D		1.0 E-4	3 ⁺ , 3 ⁻		
	EFP-2	TURBINE PUMP FAILS TO START	D		2.0 E-2	3 ⁺ , 3 ⁻	S	4
	EFP-2	TURBINE PUMP FAILS TO RUN FOR 24 HRS	3.0 E-5/HR	24	7.2 E-4	10 ⁺ , 10 ⁻		5
					$\pi=2.2$ E-2			
E1		SYSTEM INTERFACE FAULTS (LOSP)			3.2 E-3			
	DC E2B	DC POWER TRAIN B FAILS						
		LOSP			3.2 E-3			
E1		MOTOR PUMP TRAIN FAULTS (TRAIN B)						
E5		TRAIN B HARDWARE FAULTS						
	MOV EFV-3	INADVERTENTLY CLOSED	D		3.6 E-5	2 ⁺ , 1.2 ⁻	0	
	MOV EFV-3	PLUGGED	D		3.0 E-6	10 ⁺ , 10 ⁻		1
	MOV EFV-7	INADVERTENTLY CLOSED	D		1.0 E-4	3 ⁺ , 3 ⁻		
	MOV EFV-7	PLUGGED	D		3.0 E-4	10 ⁺ , 10 ⁻		2
	EFV-6	CHECKVALVE FAILS TO OPEN	D		1.0 E-4	3 ⁺ , 3 ⁻		
	EFP-1	MOTOR PUMP FAILS TO START	D		1.0 E-4	3 ⁺ , 3 ⁻		
	EFP-1	MOTOR PUMP FAILS TO RUN FOR 24 HRS	3.0 E-5/HR	24	7.2 E-4	10 ⁺ , 10 ⁻		
	CTRL. CIRCUIT	FAILS TO ACTUATE (RELAY)	D		1.0 E-4	3 ⁺ , 3 ⁻		
	EFP-1 BKK.	FAILS TO TRANSFER	D		1.0 E-3	3 ⁺ , 3 ⁻		
	OPERATOR	FAILS TO LOAD ELECTRIC PUMP ON AC BUS (TRAIN A)	D		1.0 E-4	10 ⁺ , 10 ⁻		11

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR ⁻¹)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
EX2		SYSTEM INTERFACE FAULTS (LOSP)			3.2 E-3			
DCA	DC ESA	DC POWER TRAIN A FAILS						
		LOSP			3.2 E-3			
ACA	AC TRAIN A	AC TRAIN A FAILS						
		NON LOSP						
		LOSP			2.2 E-2			
EM1		TRAIN A MAINTENANCE AND TEST OUTAGES			6.5 E-3	3 ⁺ , 3 ⁻	N	7, 8
	MOV EFV-11	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3 ⁺ , 3 ⁻	N	10
	MOV EFV-32	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3 ⁺ , 3 ⁻	N	10
	MOV ASV-5	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3 ⁺ , 3 ⁻	N	10
	MOV EFV-8	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3 ⁺ , 3 ⁻	N	10
	EFP-2	OUT FOR MAINTENANCE	.1/720	19	2.6 E-3	3 ⁺ , 3 ⁻	N	8
					$\Sigma=6.5 E-3$			
EM2		TRAIN B MAINTENANCE AND TEST OUTAGES			5.5 E-3	3 ⁺ , 3 ⁻	N	7, 8
	MOV EFV-14	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3 ⁺ , 3 ⁻	N	10
	MOV EFV-33	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3 ⁺ , 3 ⁻	N	10
	MOV EFV-8	OUT FOR MAINTENANCE	.1/720	7	9.7 E-4	3 ⁺ , 3 ⁻	N	10
	EFP-1	OUT FOR MAINTENANCE	.1/720	19	2.6 E-3	3 ⁺ , 3 ⁻	N	8
					$\Sigma=5.5 E-3$			
E3-E02		SUCTION LINE FAULTS			1.0 E-5	2 ⁺ , 2 ⁻	0	
E3	CDV-103	VALVE PLUGGED	D		1.0 E-4	3 ⁺ , 3 ⁻		
E02	OPERATOR	FAILS TO RECOVER	D		0.1	2 ⁺ , 2 ⁻	0	9
					$\Sigma=1.0 E-5$			

Table P.4 (4/4) Event "EF2" Quantification

Table P.4 Emergency Feedwater System

QUANTIFICATION TABLES

NOTES

- 1 This fault was assessed as an inadvertent act of commission (1.0 E-3/year) since the valve is not closed by any procedure. The valve is checked once per shift. Therefore, the fault exposure time is 8 hours. The fault is therefore assessed as $(1.0 \text{ E-3})(8/8760)=1.0 \text{ E-6}$.
- 2 This valve is closed on monthly test. The basic act of leaving the valve closed was assessed as 1.0 E-2/month. The valve is checked every 8 hours; so the fault duration time is 8 hours. Therefore, the fault was assessed as $(1.0 \text{ E-2})(8/720)=1.1 \text{ E-4}$.
- 3 The basic fault of leaving auto actuation of steam admission valve ASV-5 locked out was assessed as 1E-3. An additional probability of the operator failing to recover of 0.1 was assumed. The total fault was assessed as 1.E-4. The fault probability could be lower because the auto actuation is verified to be in AUTO once every shift.
- 4 The demand probability for the turbine fails to start was obtained from NUREG/CR-1205 (Reference P-1) which contains a summary of B&W turbine pump failure rates.
- 5 The turbine pump failure rate was obtained from Appendix III of WASH-1400 since Reference P-1 did not contain data for turbine failure to run.
- 6 This is a similar fault to that described in Note 3, except that the electric-driven pump auto actuation is locked out.
- 7 Test outages were assessed to not contribute to system unavailability since valves EFV-3,4,7, and 8 open automatically on receipt of an actuation signal.
- 8 Maintenance outages were assessed by assuming one train outage every 2 months. This outage was converted to a component outage frequency of 0.1/month. Average maintenance outage times of 7 hours for valves and 19 hours for pumps were assumed.
- 9 The operator could recover here by transferring suction from the condensate storage tank to the hotwell. DC valves EFV-1 and EFV-2 would have to open to supply their respective train.
- 10 It was assumed that valve maintenance would require isolation of the valve being maintained by closing valves on either side of the maintained valve.

Table P.4 Emergency Feedwater System (con't)

QUANTIFICATION TABLES

NOTES

- 11 Operator is required to load motor pump EFP-1 on to AC bus (Train A) after D.G. A starts, this fault was assessed as $1.E-3$ with 10% chance that he would recover.
- 12 Auto-actuation faults in E1 and E2 and the fault E01 are separate events. The former two are associated with individual trains, while the latter refers to the entire system. The fault probabilities indicated are probably very conservative since auto-actuation is verified once each shift and is monitored in the control room.

References

- P-1 "Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants, January 1, 1972 to April 30, 1978," prepared by W. H. Sullivan and J. P. Poloski, EG&E Idaho, Inc., for the U.S. Nuclear Regulatory Commission, (EG&E Report No. EGG-EA-5044) NUREG/CR-1205, January 1980.

Table P.5 EFS - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
E01	1.0 E-4
E03	1.0 E-3
E04	0.1
E4	1.0 E-5
E1	2.2 E-2
DCB	ϵ^* 3.2 E-3**
E2	3.5 E-3
DCA	ϵ^* 3.2 E-3**
ACA	ϵ^* 3.2 E-2**
EM1	6.5 E-3
EM2	5.5 E-3
E3	1.0 E-4
E02	0.1
E5	3.6 E-3

*Offsite power available

**Offsite power not available

Distribution:

USNRC Distribution Contractor (CDSI) (155)
7300 Pearl Street
Bethesda, Maryland 20014
130 Copies for AN
25 Copies for NTIS

Author selected distribution - 25 Copies
(List available from author.)

4400 A. W. Snyder
4410 D. J. McCloskey
4412 J. W. Hickman (3)
4412 D. D. Carlson
4412 W. R. Cramond
4412 D. D. Drayer
4412 F. T. Harper
4412 S. W. Hatch
4412 A. M. Kolaczowski
4412 G. J. Kolb
4412 A. C. Payne
4412 R. G. Spulak
4412 T. A. Wheeler
4413 N. R. Ortiz
4414 G. B. Varnado
4415 D. J. McCloskey, Actg.
4416 L. D. Chapman
3141 L. J. Erickson (5)
3151 W. L. Garner (3)
8214 M. A. Pound

120555078877 2 AN
US NRC
ADM DIV OF TIDC
POLICY & PUBLICATIONS MGT BR
PDR NUREG COPY
LA 212
WASHINGTON DC 20555