

Docket No. 50-259

DEC 23 1982

Mr. Hugh G. Parris
Manager of Power
Tennessee Valley Authority
500A Chestnut Street, Tower II
Chattanooga, Tennessee 37401

Dear Mr. Parris:

SUBJECT: INTERIM RELIABILITY EVALUATION PROGRAM (IREP) STUDY OF BROWNS
FERRY NUCLEAR PLANT, UNIT 1

We have received from our contractor, EG&G - Idaho the results of its IREP analysis of Browns Ferry Unit 1. The results are presented in NUREG/CR-2802, which consists of four volumes; the main report and three appendixes. The main report provides a summary of the engineering insights acquired in doing the study and a discussion regarding the accident sequences that dominate the risks of Browns Ferry, Unit 1. It also describes the study methods and their limitations, the Browns Ferry plant and its systems, the identification of accidents, the contributors to those accidents, and the estimating of accident occurrence probabilities. Appendix A provides supporting material for the identification of accidents and the development of logic models, or event trees, that describe the Browns Ferry accidents. Appendix B provides a description of Browns Ferry, Unit 1, plant systems and the failure evaluation of those systems as they apply to accidents at Browns Ferry. Appendix C generally describes the methods used to estimate accident sequence frequency values. A copy of the main report and appendixes is enclosed.

We understand you are nearing completion of your own IREP Study. We would appreciate you reviewing the enclosed reports and provide us any comments you may have on the results of the EG&G IREP study and your current position with respect to the conclusions of the report. We would appreciate a response within the next three months. Upon completion of our review of your response, we plan to prepare and issue a Safety Evaluation. If you have any questions or would like to discuss this with our staff, please contact Dick Clark, the Browns Ferry project manager (301-492-7162).

8301030305 821223
PDR ADOCK 05000259
P PDR

OFFICE ▶						
SURNAME ▶						
DATE ▶						

The reporting and/or recordkeeping requirements contained in this letter affect fewer than ten respondents; therefore, OMB clearance is not required under P. L. 96-511.

Sincerely,

ORIGINAL SIGNED BY

Domenic B. Vassallo, Chief
Operating Reactors
Division of Licensing

Enclosures: As stated

cc: See next page

Distribution:

- Docket File
- NRC PDR
- Local PDR
- ORB Rdg
- D. Eisenhut
- D. Clark
- S. Norris
- OELD
- E. L. Jordan
- NSIC
- J. M. Taylor
- ARCS 10
- Gray File
- MWilliams, DL
- RBernero, D/DRA, RES
- JAMurphy, DRA/RES
- MLErnst, AD/TECH/DST
- AThadani, RRAB/DST

without ENCLOSURES

M. Williams as noted

OFFICE	ORB#2:DL	DL:ORB#2	M. Williams	DL:ORB#2		
SURNAME	S.Norris	D.Clark:pr	M. Williams	D.Vassallo		
DATE	12/3/82	12/03/82	12/6/82	12/16/82		

cc:

W/o enclosures

H. S. Sanger, Jr., Esquire
General Counsel
Tennessee Valley Authority
400 Commerce Avenue
E 11B 33C
Knoxville, Tennessee 37902

Mr. Charles R. Christopher
Chairman, Limestone County Commission
P. O. Box 188
Athens, Alabama 35611

Ira L. Myers, M. D.
State Health Officer
State Department of Public Health
State Office Building
Montgomery, Alabama 36104

Mr. Oliver Havens
U. S. Nuclear Regulatory Commission
Reactor Training Center
Osborne Office Center, Suite 200
Chattanooga, Tennessee 37411

W/enclosures

Mr. Ron Rogers
Tennessee Valley Authority
400 Chestnut Street, Tower II
Chattanooga, Tennessee 37401

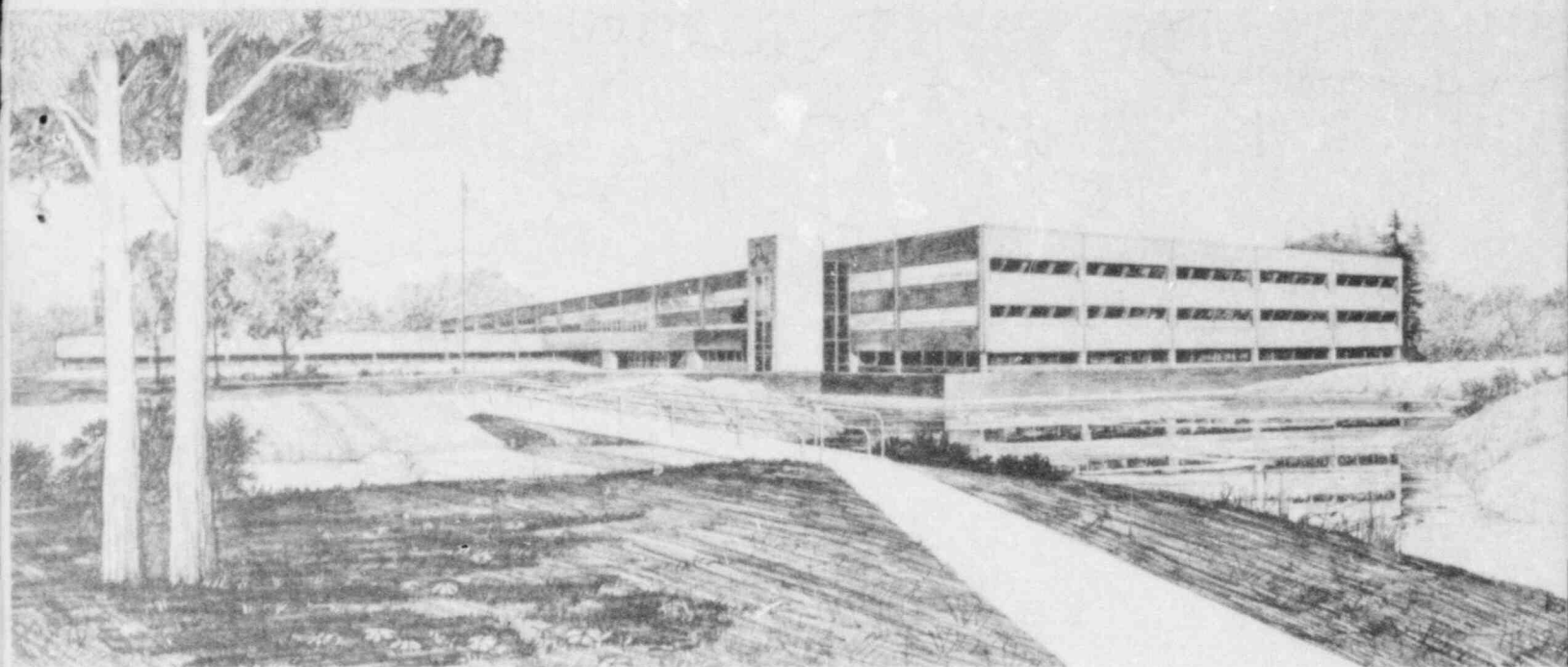
Mr. H. N. Culver
249A HBD
400 Commerce Avenue
Tennessee Valley Authority
Knoxville, Tennessee 37902

Resident Inspector
U. S. Nuclear Regulatory Commission
Route 2 Box 311
Athens, Alabama 35611

George Jones
Tennessee Valley Authority
P. O. Box 2000
Decatur, Alabama 35602

Mr. Robert Christie
Tennessee Valley Authority
W10D 190C-K
400 West Summit Hill Avenue
Knoxville, Tennessee 37902

James P. O'Reilly
Regional Administrator, Region II
U.S. Nuclear Regulatory Commission
101 Marietta Street, Suite 3100
Atlanta, Georgia 30303



U.S. Department of Energy

Idaho Operations Office • Idaho National Engineering Laboratory

Interim Reliability Evaluation Program: Analysis of the Browns Ferry, Unit 1, Nuclear Plant

Main Report

EG&G Idaho, Inc.

Energy Incorporated, Seattle Office

S. E. Mays
J. P. Poloski
W. H. Sullivan
J. E. Trainer

R. C. Bertucio
T. J. Leahy

July 1982

Prepared for the
U.S. Nuclear Regulatory Commission
Under Sandia National Laboratories
Purchase Order No. 62-7776

8209270137

 **EG&G** Idaho

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, nor 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

**INTERIM RELIABILITY EVALUATION PROGRAM:
ANALYSIS OF THE BROWNS FERRY,
UNIT 1, NUCLEAR PLANT**

MAIN REPORT

EG&G Idaho, inc.

S. E. Mays
J. P. Poloski
W. H. Sullivan
J. E. Trainer

Energy Incorporated, Seattle Office

R. C. Bertucio
T. J. Leahy

Published July 1982

EG&G Idaho, Inc.
Idaho Falls, Idaho 83415

Prepared for the
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
Under Sandia National Laboratories
Purchase Order No. 62-7776
FIN No. A1241

ABSTRACT

A probabilistic risk assessment (PRA) was made of the Browns Ferry, Unit 1, nuclear plant as part of the Nuclear Regulatory Commission's Interim Reliability Evaluation Program (IREP). Specific goals of the study were to identify the dominant contributors to core melt, develop a foundation for more extensive use of PRA methods, expand the cadre of experienced PRA practitioners, and apply procedures for extension of IREP analyses to other domestic light water reactors.

Event tree and fault tree analyses were used to estimate the frequency of accident sequences initiated by transients and loss of coolant accidents. External events such as floods, fires, earthquakes, and sabotage were beyond the scope of this study and were, therefore, excluded. From these sequences, the dominant contributors to probable core melt frequency were chosen. Uncertainty and sensitivity analyses were performed on these sequences to better understand the limitations associated with the estimated sequence frequencies. Dominant sequences were grouped according to common containment failure modes and corresponding release categories on the basis of comparison with analyses of similar designs rather than on the basis of detailed plant-specific calculations.

Each of eight dominant sequences for Browns Ferry, Unit 1, were initiated by postulated plant transients. Six of the eight sequences involved failure of the long-term decay heat removal functions of the residual heat removal system. These sequences account for 73% of the sum of the dominant sequence frequencies. The other two sequences involved an anticipated transient without a (subsequent) scram and account for 27% of the sum of the dominant sequence frequencies.

While no LOCA-initiated sequences were dominant contributors to the frequency of core melt accidents, two of the eight dominant sequences involved transient-induced stuck-open relief valve scenarios.

The results show that the single most important factor in reducing the risk of a core melt accident at Browns Ferry, Unit 1, is providing reliable long-term decay heat removal capability; the next most important factor would be providing more reliable means to ensure that the reactor can be rapidly shut down and maintained subcritical.

SUMMARY

Probabilistic risk assessment (PRA) techniques offer important analytical tools for the safety evaluation of nuclear power plants. Toward this end, the Three Mile Island Action Plan¹ identifies the Interim Reliability Evaluation Program (IREP) as a high priority effort to apply PRA techniques in the measurement of public health and safety risk of nuclear power plants. Because of plant-to-plant differences in design and operation, it is desirable to apply these techniques to other reactor plants in addition to those already studied.

The purpose of the current program, then, is to apply PRA techniques to several plants. Specific goals include:

1. Identify accident sequences that dominate the contribution to core melt.
2. Develop a foundation of information for additional and more extensive application of PRA techniques.
3. Expand the cadre of experienced PRA practitioners.
4. Develop procedures for the uniform application of PRA techniques to other domestic light water reactors.

EG&G Idaho, Inc., was contracted by Sandia National Laboratories to perform the IREP assessment of the Browns Ferry Nuclear Plant, Unit 1 (BF1). Analytical support was furnished by Energy Inc., Seattle office. Battelle-Columbus Laboratories provided analyses for grouping the dominant sequences according to release categories.

The BF1 IREP team identified and estimated the frequency of potential core melt sequences caused by loss of coolant accidents (LOCAs) and transients. The dominant sequences were identified and release categories similar to those defined in WASH-1400 were assigned to each of these sequences. In the course of the analysis, many engineering insights important to risk were identified. This section of the report summarizes those insights and the dominant sequence evaluation.

Engineering Insights

The single most important engineering insight relating to risk is the dependence of BF1 on the residual heat removal (RHR) system for long-term decay heat removal. For the majority of the accident initiators, the power conversion system (PCS) is unavailable. Therefore, only the RHR system in either the torus cooling or the shutdown cooling mode is available to remove decay heat from the reactor.

Six of the eight dominant sequences identified involve failure of the torus cooling and shutdown cooling modes of the RHR system. These sequences account for approximately 73% of the sum of the dominant sequence frequencies. Therefore, no significant reduction in core melt frequency can be achieved without reducing the unavailability of the RHR system or providing an alternate means of long-term decay heat removal. Thus, the RHR system is the most risk-critical system at BF1.

Of the three dominant sequences involving a loss of offsite power, failure of the emergency equipment cooling water (EECW) system accounts for approximately 40% of the initial core melt frequency value. While consideration of potential recovery actions makes EECW system failure a nonsignificant contributor to the final frequency of these sequences, it would seem feasible that the system could be designed and operated in such a way that the dependence on operator recovery actions is minimized.

The rupture disks on the exhaust lines of the reactor core isolation cooling (RCIC) and high pressure coolant injection (HPCI) systems affect the unavailability of these systems. These devices are intended to

be last-resort safety devices to prevent a rupture of the turbines or turbine exhaust lines. Premature failure of these rupture disks leads to isolation of the system when no such isolation is required. Therefore, rupture disk failures contribute significantly to RCIC and HPCI system unavailabilities.

Scheduled testing and maintenance accounts for approximately 25% of the HPCI system unavailability. That is, one fourth of the probability of the HPCI system being unavailable when required is due to the operators making the system unavailable in order to test or maintain the system. This value seems to be high in light of scheduled testing and maintenance contributions of other systems. This indicates that a close examination of the scheduled testing and maintenance requirements may be needed to ensure that the benefit of frequent testing is balanced against the unavailability caused by that testing.

Dominant Sequences

Eight dominant sequences were identified for BF1. Table S-1 lists these sequences along with the sequence frequencies, calculated error factors and containment failure mode frequencies. Each error factor represents an upper 95% sequence frequency bound divided by the corresponding frequency point estimate. The containment failure modes are identical to those of WASH-1400. For these particular sequences, the release categories are $\alpha - 1$, $\gamma' - 2$, and $\gamma - 3$, where the Numbers 1, 2, and 3, refer to the WASH-1400 release categories.

Table S-1. Dominant sequences versus containment failure modes

Sequence	Frequency	Error Factor	Containment Failure Mode Frequencies ^a		
			α	γ'	γ
T _U R _B R _A	9.7×10^{-5}	8.7	9.7×10^{-9}	1.9×10^{-5}	7.8×10^{-5}
T _U B	5.1×10^{-5}	5.0	5.1×10^{-9}	1.0×10^{-5}	4.1×10^{-5}
T _P R _B R _A	2.8×10^{-5}	2.8	2.8×10^{-9}	5.6×10^{-6}	2.2×10^{-5}
T _K R _B R _A	9.3×10^{-6}	9.0	9.3×10^{-8}	1.9×10^{-6}	7.4×10^{-6}
T _U Q _R B _R A	4.1×10^{-6}	15.3	4.1×10^{-10}	8.2×10^{-7}	3.3×10^{-6}
T _A BM	3.7×10^{-6}	4.6	3.7×10^{-10}	7.4×10^{-7}	3.0×10^{-6}
T _P K _R B _R A	1.6×10^{-6}	2.8	1.6×10^{-8}	3.2×10^{-7}	1.3×10^{-6}
T _P Q _R B _R A	1.2×10^{-6}	4.7	1.2×10^{-10}	2.4×10^{-7}	9.6×10^{-7}
Final	2.0×10^{-4}	5.6	1.3×10^{-7}	3.9×10^{-5}	1.7×10^{-4}

a. Probabilities of containment failure modes:

α (in-vessel steam explosion)	=	0.01 for LOCAs
α (in-vessel steam explosion)	=	0.0001 for transients
γ (release through annulus)	=	0.8
γ' (direct release to atmosphere)	=	0.2.

Several of the dominant sequences have similar phenomenology and system responses and will be grouped together in this discussion. Each is discussed individually in the main report and Appendix C.

Transients with DHR Failure

Three sequences, $T_{UR_B}R_A$, $TKR_B R_A$, and $T_{UQR_B}R_A$, involve transient initiators with subsequent failure of the torus cooling and shutdown cooling modes of the RHR system. In each case, a transient is followed by a reactor scram and successful overpressure protection. In one case, $TKR_B R_A$, a relief valve fails to reseat causing steam to be discharged from the reactor to the torus. In each case, one of the high pressure injection systems (RCIC or HPCI) operates to maintain reactor water level. However, failure of the RHR system to remove the decay heat being transferred from the reactor to the torus eventually results in an inability to pump the torus water back to the reactor due to excessive torus water temperatures. Core uncovering and core melt ensues.

The dominant contributors to the unavailability of torus cooling and shutdown cooling modes of RHR are control circuit faults associated with motor-operated valves. In particular, minimum-flow bypass valve faults contribute approximately 18% to the total system unavailability of 7.6×10^{-5} . Figure S-1 is a sequence evaluation diagram illustrating RHR failure for these sequences.

Since the high pressure systems can operate for several hours before the torus water temperature becomes excessive, there are recovery actions available to the operator. One potential recovery action is to use the PCS to remove decay heat from the reactor. Since some transient initiators may preclude use of the PCS and since PCS recoverability is not easily quantifiable, no credit was taken for PCS recovery in the final sequence frequency. However, control circuit faults were considered to be recoverable in this time frame. The operator could manually operate the valves or bypass/repair the control circuits. Inclusion of recovery potential reduced the unavailability of the torus cooling and shutdown cooling modes from 7.6×10^{-5} to 5.7×10^{-5} . This value was used to calculate the final sequence frequency of Table S-1.

Loss of Offsite Power with DHR Failure

Three sequences, $T_{PR_B}R_A$, $T_{PKR_B}R_A$, and $T_{PQR_B}R_A$, involve a loss of offsite power and subsequent failure of the torus cooling and shutdown cooling modes of the RHR system. The phenomenology of these three sequences is identical to the three described in the previous section. The differences between these sequences and the previous sequences are in the initiator frequency and effect of the initiator on system unavailabilities.

The dominant contributors to the unavailability of torus cooling and shutdown cooling can be separated into two parts: EECW-related faults and non-EECW-related faults. Failure of the EECW system will eventually cause failure of all the emergency diesel generators, thereby precluding use of the RHR system. The non-EECW faults are primarily combinations of diesel generator faults which of themselves disable the RHR system. The unavailability of torus cooling and shutdown cooling is the sum of these two values ($2.0 \times 10^{-2} + 2.9 \times 10^{-2} = 4.9 \times 10^{-2}$). Figure S-2 is a sequence evaluation diagram describing RHR failure for these sequences.

As before, the high pressure systems can operate for several hours before the torus water overheats. This allows time for the operators to take recovery actions. Among the recovery actions available is restoration of offsite power. WASH-1400² data suggest that offsite power can be restored 97% of the time before the torus water overheats. For the other 3% of the time, the operators could manually start additional pumps to serve the EECW function before total diesel power failure occurred. The operators could also isolate nonessential EECW loads so that fewer than three of four pumps would be needed to serve the vital loads. Taking these factors into account reduces the unavailability of torus cooling and shutdown cooling from 4.9×10^{-2} to 9.4×10^{-4} . This value was used to calculate the final sequence frequency of Table S-1.

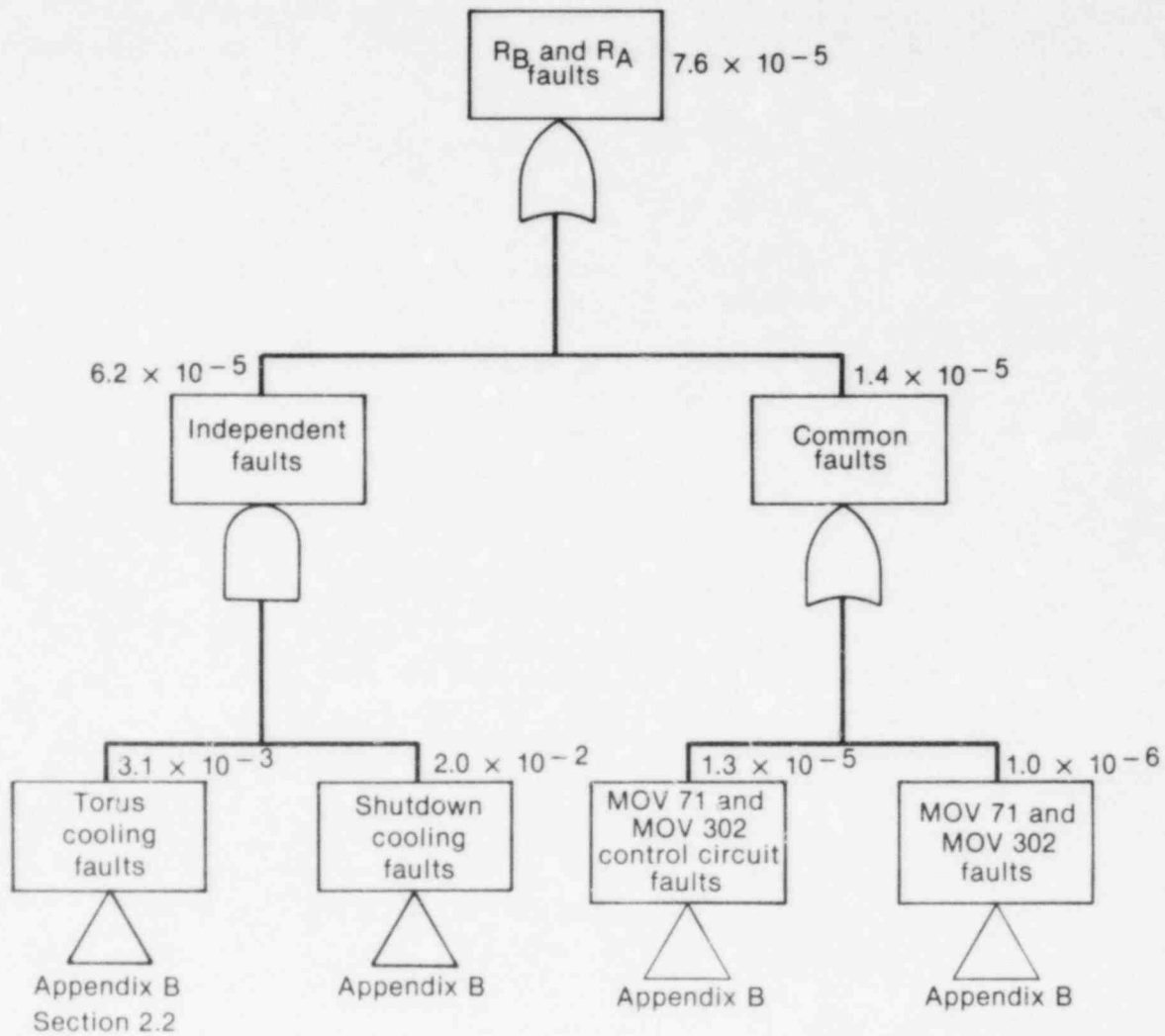


Figure S-1. Residual heat removal failure for transient sequences with normal power available.

Transients with Failure to Scram

Two sequences, T_{UB} and T_{ABM} , involve failure of the control rod drive system to insert enough rods to make the reactor subcritical. For the first sequence, T_{UB} , a transient that disables the PCS is followed by a failure to scram. The resulting power level causes the relief valves to lift and dump steam to the torus. This coolant loss rate is greater than the high pressure system makeup rate. Therefore, core uncover and core melt occurs. For the second case, T_{ABM} , the PCS is available. However, the turbine bypass valves cannot pass more than 30% rated steam flow. Without successful recirculation pump trip reactor power may remain significantly higher than 30%. Therefore, the relief valves open to dump steam to the torus. This causes depletion of the water in the condensate storage tank (CST) and a trip of the feed pumps. Main steam isolation valve closure follows and this sequence is then identical to T_{UB} .

The value for failure to scram (3.0×10^{-5}) was taken from Reference 3. The complexities of precisely modeling how many rods in which patterns must fail to insert in order to remain critical was considered to be beyond the scope of this analysis.

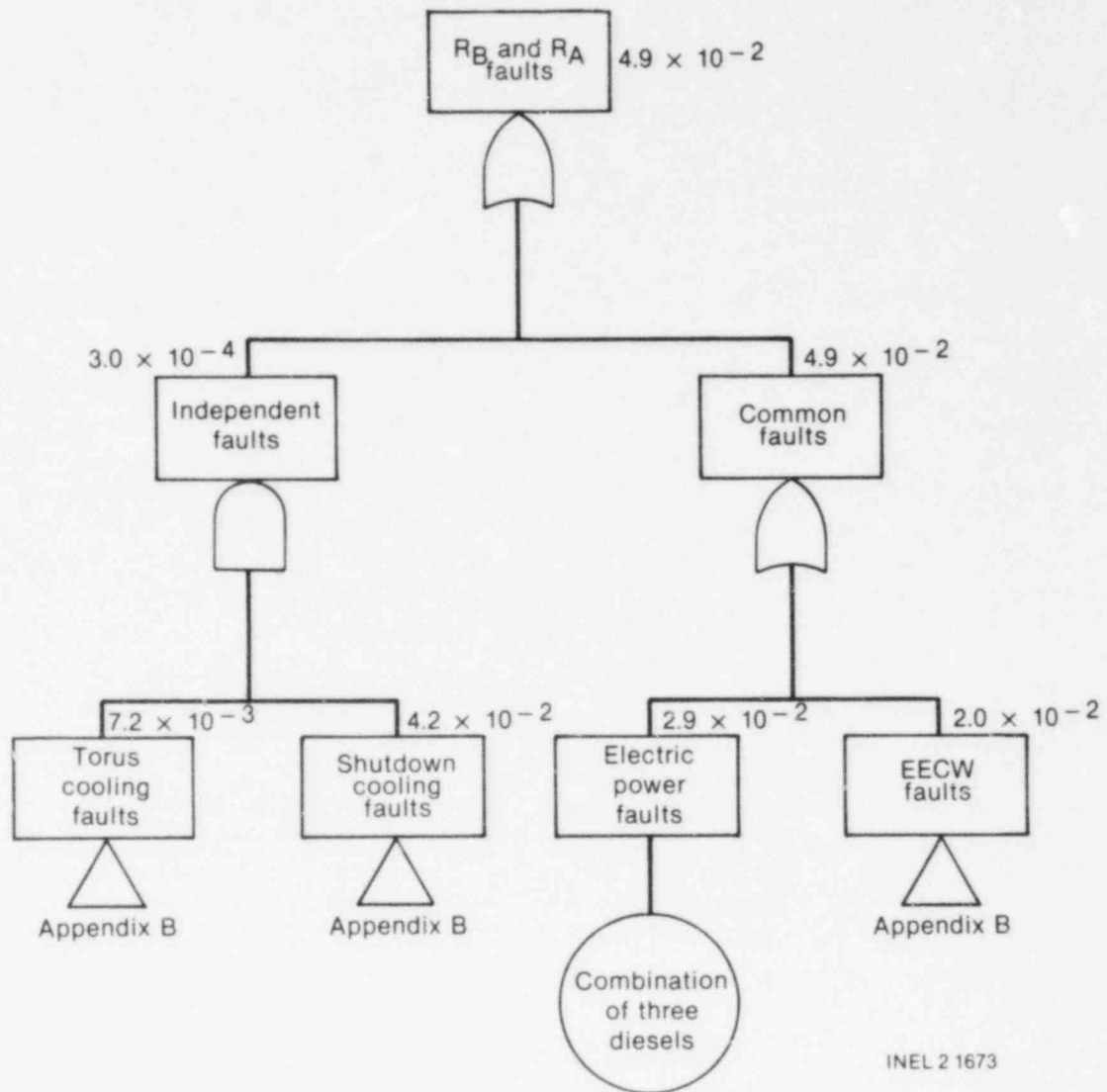


Figure S-2. Residual heat removal failure given a loss of offsite power.

The lack of adequate models to determine plant thermodynamics under the failure to scram conditions previously described, along with the rapid development of events in such a scenario, resulted in the decision to exclude operator recovery actions for these sequences. Therefore, no credit for operator recovery is taken in calculating the final sequence frequency of Table S-1.

Conclusion

The single most important factor in reducing the risk of a core melt accident at BF1 is providing reliable long-term decay heat removal capability; the next most important factor would be providing more reliable means to ensure that the reactor can be rapidly shut down and maintained subcritical. The analysis suggests that no significant reduction in the core melt frequency can be achieved without making improvements in these two areas.

FOREWORD

This report describes a risk study of the Browns Ferry, Unit 1, nuclear plant. The study is one of four such studies sponsored by the NRC Office of Research, Division of Risk Assessment, as part of its Interim Reliability Evaluation Program (IREP), Phase II. Other studies include evaluations of Arkansas One, Unit 1, by Sandia National Laboratories; Calvert Cliffs, Unit 1, by Science Applications, Inc.; and Millstone, Unit 1, by Science Applications, Inc. EG&G Idaho, Inc. was assisted by Energy Inc., Seattle, in its evaluation of the Browns Ferry, Unit 1, plant. Battelle-Columbus Laboratories provided information regarding the fission product releases that result from risk-significant accident scenarios. Sandia National Laboratories has overall project management responsibility for the IREP studies. It also has responsibility for the development of uniform probabilistic risk assessment procedures for use on future studies by the nuclear industry.

This report is contained in four volumes: a main report and three appendixes. The main report provides a summary of the engineering insights acquired in doing the study and a discussion regarding the accident sequences that dominate the risks of Browns Ferry, Unit 1. It also describes the study methods and their limitations, the Browns Ferry plant and its systems, the identification of accidents, the contributors to those accidents, and the estimating of accident occurrence probabilities. Appendix A provides supporting material for the identification of accidents and the development of logic models, or event trees, that describe the Browns Ferry accidents. Appendix B provides a description of Browns Ferry, Unit 1, plant systems and the failure evaluation of those systems as they apply to accidents at Browns Ferry. Appendix C generally describes the methods used to estimate accident sequence frequency values.

Numerous acronyms are used in the study report. For each volume of the report, these acronyms are defined in a listing immediately following the table of contents.

ACKNOWLEDGMENTS

The authors wish to express their thanks to several individuals who have made important contributions to this study report: Joe Murphy of the Nuclear Regulatory Commission, Dave Carlson of Sandia National Laboratories, and Jonathan Young of Energy Inc. for their technical comments as the study progressed; Cindy Gentillon for her assistance in incorporating review comments into the final report; Paul Adye for his technical editing of the final report; Kim Culbertson for her typing of the several drafts and final text of this report; Pat Virgil for proofreading the copy; and Debi Iverson for her typesetting and final layout of the report.

CONTENTS

ABSTRACT	ii
SUMMARY	iii
FOREWORD	viii
ACKNOWLEDGMENTS	ix
NOMENCLATURE	xiv
1. INTRODUCTION	1
2. IREP METHODOLOGY	3
2.1 Information Base	3
2.2 Methodology	4
3. PLANT DESIGN	8
3.1 General	8
3.2 Accident Mitigation Functions	8
3.3 Front-Line and Support Systems	10
4. INITIATING EVENTS	13
4.1 Introduction	13
4.2 Identification of Potential Core-Related Initiating Events	13
4.3 Initiating Event/Mitigating System Dependencies	18
5. ACCIDENT SEQUENCE DELINEATION	22
5.1 Introduction	22
5.2 LOCA Functional Event Trees	22
5.3 Transient Functional Event Trees	34
6. SYSTEMS ANALYSIS	40
6.1 Front-Line Systems Description	42
6.2 Support Systems Description	62
7. ACCIDENT SEQUENCE QUANTIFICATION	76
7.1 General Approach	76

7.2	Data Sources.....	76
7.3	System Unavailabilities.....	76
7.4	Sequence Frequencies.....	76
7.5	Candidate Dominant Accident Sequences.....	77
7.6	Example Calculation.....	77
8.	RESULTS.....	81
8.1	General.....	81
8.2	Dominant Sequences.....	81
8.3	Containment Response and Release Categories.....	85
8.4	Engineering Insights.....	88
8.5	Uncertainty Analysis.....	93
8.6	Sensitivity Analysis.....	94
8.7	Limitations of the IREP Methodology and Uses of the Models.....	95
8.8	Application of Results.....	96
	REFERENCES.....	99

APPENDIXES

(Each appendix is published as a separate volume)

APPENDIX A—EVENT TREES

APPENDIX B—SYSTEM DESCRIPTIONS AND FAULT TREES

APPENDIX C—SEQUENCE QUANTIFICATION

FIGURES

S-1.	Residual heat removal failure for transient sequences with normal power available.....	vi
S-2.	Residual heat removal failure given a loss of offsite power.....	vii
1.	IREP methodology.....	5
2.	Emergency core cooling systems.....	9
3.	Core standby cooling systems performance capability bar chart.....	14
4.	LOCA functional event tree—break inside containment.....	23
5.	LOCA functional event tree—break outside containment.....	24

6.	LOCA systemic event tree for large liquid break, suction-side of recirculation pumps (L _S)	27
7.	LOCA systemic event tree for large liquid break, discharge-side of recirculation pumps (L _D)	28
8.	LOCA systemic event tree for large steam break (L _V)	29
9.	LOCA systemic event tree for intermediate liquid break (I _L)	30
10.	LOCA systemic event tree for intermediate steam break (I _V)	31
11.	LOCA systemic event tree for small liquid-line or steam-line break (S)	32
12.	Transient functional event tree	35
13.	Transient systemic event tree where PCS is unavailable (T _U)	38
14.	Transient systemic event tree where PCS is available (T _A)	39
15.	RHR/RHRSW/EECW interplant power dependencies	43
16.	RCIC system	44
17.	RHR system, Loop 1	46
18.	HPCI system	48
19.	Automatic depressurization system	51
20.	Core spray system	52
21.	Vapor suppression part of the primary containment	54
22.	CRDH system	56
23.	Scram discharge volume equipment	57
24.	Main steam system	58
25.	Condensate and feedwater system	59
26.	RPT circuit	61
27.	EPS diagram showing AC and DC systems	63
28.	RHRSW system	65
29.	RHRSW/EECW system power dependencies	66
30.	EECW system	68
31.	Keep-full system	70
32.	CCW system	71

33.	Simplified RCW system diagram.....	73
34.	RPS Channel A.....	74
35.	Transient systemic event tree for PCS unavailable.....	78
36.	Core melt sequence frequencies versus initiators (recovery actions not considered).....	89
37.	Core melt sequence frequencies versus failed function (recovery actions not considered).....	91

TABLES

S-1.	Dominant sequences versus containment failure modes.....	iv
1.	Information sources for IREP.....	3
2.	Front-line systems for LOCA and transient functions.....	11
3.	Front-line versus support systems.....	12
4.	LOCA mitigation success criteria.....	15
5.	LOCA pipe rupture frequencies.....	16
6.	Transient initiator groupings and frequencies.....	18
7.	Transient mitigation success criteria.....	19
8.	LOCA initiator effects on mitigating systems.....	20
9.	Front-line and support system list.....	40
10.	RHR operational mode success criteria.....	47
11.	Transients where the PCS is unavailable.....	79
12.	Candidate dominant sequences.....	81
13.	Dominant sequences.....	82
14.	Dominant sequences versus containment failure modes.....	86
15.	Dominant sequence uncertainties.....	93

NOMENCLATURE

\bar{A}	The complement of A (a success event if A is a failure event). (\bar{A} may also be used to mean "unavailability.")
A	Alarm
AC	Alternating current
ACC	Accumulator
ADS	Automatic depressurization system
AH	Alarm-high
AO	Air operator
APRM	Average power range monitor
AT	Anticipated transient
ATWS	Anticipated transient without scram
BF1	Browns Ferry, Unit 1, nuclear plant
BI	Break isolation
BWR	Boiling water reactor
CAD	Containment atmosphere dilution
CCW	Condenser circulating water
CD	Complete dependence
CE	Conductivity element
CIS	Containment isolation system
Clg	Cooling
COND	Main condenser
CR-3	Crystal River, Unit 3, nuclear plant IREP study
CRD	Control rod drive
CRDH	Control rod drive hydraulic
CRDHS	Control rod drive hydraulic system
CRW	Clean rad waste
CS	Core spray
CS&T	Condensate storage and transfer
CSCS	Core standby cooling system
CSS	Core spray system
CST	Condensate storage tank
CV	Control valve
D	Demand
DC	Direct current
DEP	Depressurization
DG	Diesel generator
DHR	Decay heat removal
Diff	Different
DPI	Differential pressure indicator
DPIS	Differential pressure indicating switch
DPS	Differential pressure switch
DPT	Differential pressure transmitter
EAC	Equipment area cooling
ECCS	Emergency core cooling system
ECI	Emergency coolant injection
EECW	Emergency equipment cooling water
EHC	Electro-hydraulic control
EMI	Electrical Maintenance Instruction

EOI	Equipment Operating Instructions
EPRI	Electric Power Research Institute
EPS	Electrical power system
ESFAS	Engineered safety features actuation system
F(•)	Frequency of initiator in parentheses
FCV	Flow control valve
FE	Flow element
FI	Flow indicator
FIC	Flow indicating controller
FLS	Front-line system
FMEA	Failure mode effects analysis
FR	Flow recorder
FS	Flow switch
FSAR	Final Safety Analysis Report
FT	Flow transmitter
FWC	Feedwater control
FWCS	Feedwater control system
G	Green
GOI	General Operating Instructions
H	High
H/L	High/low
HCU	Hydraulic control unit
HCV	Hand control valve
HEP	Human error probability
HPCI	High pressure coolant injection
HPCS	High pressure core spray
HPI	High pressure injection
HS	Handswitch
HSS	High speed stop
HVAC	Heating, ventilation, and airconditioning
HX	Heat exchanger
I&C	Instrumentation and control
I&E	Inspection and enforcement
IMI	Instrument Maintenance Instruction
INJ	Injection
IREP	Interim Reliability Evaluation Program
IRM	Intermediate range monitor
L	Low
LA	Level alarm
LD	Low dependence
LER	Licensee Event Report
LIC	Level indicating controller
LIS	Level indicating switch
LL	Low-low
LOCA	Loss of coolant accident
LOSP	Loss of offsite power
LPCI	Low pressure coolant injection
LPI	Low pressure injection
LS	Limit switch
LSS	Low speed stop
LT	Level transmitter

M	Motor (operated valve)
MCR	Main control room
MD	Moderate dependence
MGU	Master governor unit
MMG	Motor generator
MMI	Mechanical Maintenance Instruction
MO	Motor operated
MOV	Motor-operated valve
MSC	Manual speed control
MSI	Main steam isolation
MSIV	Main steam isolation valve
MSL	Main steam line
NA; N/A	Not applicable
NC	Normally closed
NMS	Neutron monitoring system
NO	Normally open
OI	Operating Instructions
OL	Overload
OP	Overpressure protection
OP(C)	Overpressure protection (relief valves closed)
OP(O)	Overpressure protection (relief valves open)
PA	Pressure alarm
PB	Pipe break
PCIS	Primary containment isolation system
PCS	Power conversion system
PCV	Pressure control valve
PG	IREP Procedure Guide
PI	Pressure indicator
PORV	Power-operated relief valve
PRA	Probabilistic risk assessment
PS	Pressure switch
PSCWT	Pressure suppression chamber water transfer
PT	Pressure transmitter
PWR	Pressurized water reactor
Q(•)	Unavailability of system in parentheses
QA	Quality assurance
R	Red
RBCCW	Reactor building component cooling water
RBEDT	Reactor building equipment drain tank
RCB	Reactor coolant boundary
RCIC	Reactor core isolation cooling
RCS	Reactor coolant system
RCW	Raw cooling water
RCWS	Raw cooling water system
Recirc	Recirculation
RFP	Reactor feed pump
RFPT	Reactor feed pump turbine
RFWPT	Reactor feedwater pump turbine
RHR	Residual heat removal
RHRWS	Residual heat removal service water

RMOV Reactor motor-operated valve
 RMS Remote manual switch
 RPS Reactor protection system
 RPT Recirculation pump trip
 RS Reactor subcriticality; reactor shutdown; reactor scram
 RV(C) Relief valve (closed)
 RV(O) Relief valve (open)
 RWCU Reactor water cleanup
 RX Reactor

S/D Shutdown
 S/RV Safety relief valve
 S/V Safety valve
 SBCS Standby coolant supply
 SBTG Standby gas treatment
 SCI Short-term containment integrity
 SD-BD Shutdown board
 SDV Scram discharge volume
 SIV Scram instrument volume
 SJAE Steam jet air ejector
 SLCS Standby liquid control system
 SORV Stuck-open relief valve
 SRM Source range monitor

TA Temperature alarm
 TCV Turbine control valve
 TD Time delay
 TDC Time delay contact
 TDPU Time delay pickup
 TE Temperature element
 TIP Traversing in-core probe
 TMI Three Mile Island
 TR Temperature recorder
 Trans Transient
 TS Technical Specifications; torque switch
 TVA Tennessee Valley Authority

UV Undervoltage

V Volts
 VB Vacuum breaker
 VO Valve open
 VS Vapor suppression
 VSS Vapor suppression system
 VWI Vessel water inventory

ε An insignificant quantity, generally less than 10^{-8}

INTERIM RELIABILITY EVALUATION PROGRAM: ANALYSIS OF THE BROWNS FERRY, UNIT 1, NUCLEAR PLANT

MAIN REPORT

1. INTRODUCTION

Probabilistic risk assessment (PRA) techniques offer important analytical tools for the safety evaluation of nuclear power plants. Application of such techniques to commercial nuclear plants has (a) provided useful information on accident sequences, (b) identified many strengths and weaknesses in the design and operation of the plants, (c) provided insights into the importance of accident contributors, and (d) provided rough estimates of the likelihood of serious accidents. Recent evidence tends to suggest that plant-to-plant differences in design and operation may give rise to significant differences in both the likelihood and the event-sequence of accidents. Therefore, the application of PRA techniques to many reactor plants appears to be desirable.

The need for PRA application is reflected in the Three Mile Island Action Plan,¹ which identifies the Interim Reliability Evaluation Program (IREP) as a high priority effort. The IREP is intended to apply PRA techniques to several nuclear power plants and then to develop procedures for the consistent analysis of other plants. The IREP has the following specific objectives:

1. Identify those accident sequences that are the principal risks to public health and safety.
2. Develop a foundation of information for subsequent, more intensive, application of PRA techniques on the subject plants.
3. Expand the cadre of experienced practitioners of risk assessment methods within the NRC and the nuclear power industry.
4. Develop procedures for codifying the use of these techniques to other domestic light water reactor plants.

Phase I of the IREP study was a reliability analysis of the Crystal River, Unit 3, facility.⁴ Using methodological insights gained from the Crystal River study, the Phase II IREP studies were initiated in September 1980 to analyze four plants:

1. Browns Ferry, Unit 1 (BF1), by a team from EG&G Idaho, Inc., and Energy Incorporated.
2. Arkansas Nuclear One, Unit 1, by a team from Sandia National Laboratories, Science Applications, Inc. (SAI), and Arkansas Power and Light Company.
3. Calvert Cliffs, Unit 1, by a team from SAI, Evaluation Associates, and NRC.
4. Millstone, Unit 1, by a team from SAI, Northeast Utilities, and NRC.

The principal analysts responsible for conducting the Browns Ferry risk assessment were Steve Mays, Walt Sullivan, John Poloski, and Jack Trainer of EG&G Idaho, Inc., Bob Bertucio and Tim Leahy of the Seattle Office of Energy Incorporated, provided analytical support to assist EG&G Idaho in the early

phases of the study. Utility support from Tennessee Valley Authority (TVA) was coordinated by Mark Linn with assistance from Terry Tyler, Henry Jones, and Tom Barkalow. Unlike other IREP teams who had a full-time participant from the utility, the Browns Ferry team relied on telephone calls, mail, and occasional meetings with TVA personnel for information exchange. The TVA support included documentation of plant design, analyses beyond those found in the Final Safety Analysis Report (FSAR), and verification of system operating characteristics.

Responsibility for overall technical management of the study rested with Sandia National Laboratories. Periodic reviews to assure the quality of the product were conducted by Sandia and NRC personnel not involved directly with the work of any one team, with the assistance of Energy Incorporated.

This report is one of a series of four reporting the results of these Phase II studies. Separate reports will be issued regarding procedures for conducting future analyses of the same scope and breadth as these four studies, and detailing the technical and methodological insights and nuclear safety perspectives gained from this activity.

The reader is cautioned that while it is our opinion that these studies represent the state-of-the-art within their scope, they are incomplete. External events (earthquakes, fires, etc.) are not included, and the assignment of accident sequences to release categories was performed in a subjective manner with limited plant-specific calculations. Thus, this portion of the study relied heavily on analyses performed previously on similar facilities. Other limitations are discussed in detail in Section 8.7. While accident sequence and release category frequencies were quantified, they are of value primarily in comparative analyses, and the absolute values determined should not be used without a clear appreciation of their inherent uncertainties. The principal product obtained is the integrated engineering logic presented in the plant and system models and the insights into plant features contributing significantly to risk—not the specific values computed for accident frequencies.

The main body of this report is essentially a condensation of the more detailed information supplied by the three appendixes. A general discussion of the methodology used to conduct the risk assessment is provided in Section 2. Section 3 describes the general design of the plant including a brief discussion of the systems that perform the functions to mitigate the effects of loss of coolant accidents (LOCAs) and transient events at BF1. Section 4 defines the accident initiating events that were considered for BF1 and how their associated frequencies were estimated. Section 5 presents the event trees that display the functional relationships between systems designed to respond to a potential accident initiator. Event trees were provided for the various LOCA and transient initiator groupings; a discussion of each is also given in Section 5. A more detailed description of the various plant systems (and their associated support systems) that affect the mitigation of a LOCA or transient is provided in Section 6. The assumptions that went into the construction of fault tree models, as well as the insights gained from each of these models, is provided for each system. The methodology for accomplishing the quantification of the accident sequences displayed by the event trees is discussed briefly in Section 7. An example calculation for a representative event tree sequence is also given in this section. The selection of the final dominant accident sequences is provided in the results, Section 8. Each of the dominant sequences is discussed on an individual basis. More detail supporting each of the sections can be found in the appendixes. The appendixes are organized as follows:

Appendix A—Event Trees. Applicable to Sections 2, 3, 4, and 5 of main report.

Appendix B—System Descriptions and Fault Trees. Applicable to Sections 2, 3, and 6 of the main report.

Appendix C—Sequence Quantification. Applicable to Sections 2, 5, 7, and 8 of the main report.

2. IREP METHODOLOGY

To provide guidance for the IREP analyses and to assist in consistency among the four IREP teams, procedures⁵ for conducting the analysis were developed. The four teams generally followed the same approach. Even though these procedures had never been used in their entirety, and it was recognized that some flexibility in approach would be necessary.

2.1 Information Base

The IREP analyses represent an integrated plant systems analysis. Detailed analyses were performed on those systems required to respond to a variety of initiating events and on those systems supporting the responding systems. The analysis included unavailabilities during test and maintenance activities, human errors that could arise in restoring the systems to operability following test and maintenance and in response to accident situations, and a thorough investigation of support system faults that could affect operations of more than one front-line system.

To perform the analysis, considerable, and occasionally very detailed, information was obtained from the plant. The sources of information used in the analysis are listed in Table 1.

Table 1. Information sources for IREP

Final Safety Analysis Report (FSAR)
System description and plant drawings
Other analyses of the plant or a similar plant
Modified WASH-1400 (Reference 2) data base
EPRI NP-801 (Reference 7)
Licensee event reports for the plant and similar plants
System performance documentation
Electrical one-line drawings
Control and actuation circuitry drawings
Test and maintenance procedures
Emergency procedures
Plant logs
NUREG/CR-1278 (Reference 8)
Plant visits
Discussions with and review by plant personnel

The final FSAR⁶ and plant system descriptions and drawings provided the basic information base for the analysis. This was supplemented by information contained in other studies of the plants (where available).

To identify initiating events and initiating event frequencies, EPRI NP-801,⁷ was used as the basic source. Additional insights were obtained through reviewing licensee event reports for the plant and for plants of similar design. To identify the systems needed to respond to an accident and their success criteria, the FSAR was used. In some instances, documentation from the plant or vendor was obtained suggesting and supporting the use of less stringent success criteria.

To construct the fault tree models, detailed drawings were obtained, particularly for electrical systems and control and actuation circuitry. Test, maintenance, and emergency procedures were reviewed to identify potential human errors to be included in the plant models.

Data for quantifying the fault trees were a mixture of generic and plant-specific data. Basic hardware failure rate data were obtained from a modified WASH-1400 data base assembled by NRC personnel participating in IREP. For particular components, plant-specific data obtained from plant logs were used. Plant-specific test and maintenance frequencies obtained from plant logs were used in the analysis. Data for human error rates were obtained from NUREG/CR-1278.⁸

In addition to the above documentation, the utility personnel participating in the study served as contacts with the plant to obtain more information when needed. Each team visited their plant to view particular equipment and to discuss questions with plant personnel. The IREP team prepared periodic letter reports that the utilities reviewed to ensure the accuracy of information.

2.2 Methodology

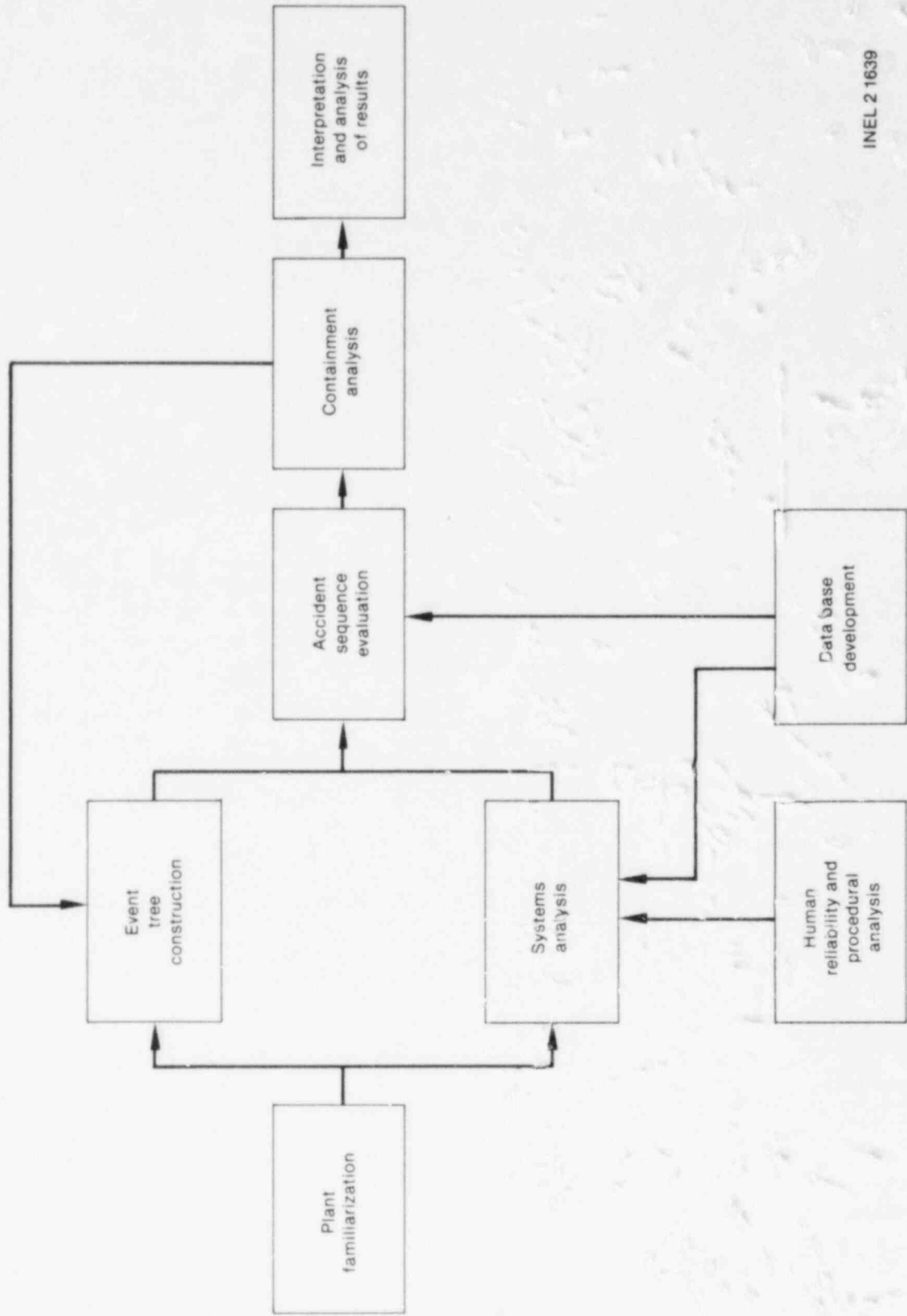
The IREP analyses consisted of eight tasks:

1. Plant familiarization.
2. Event tree construction.
3. Systems analysis.
4. Human reliability and procedural analysis.
5. Data base development.
6. Accident sequence evaluation.
7. Containment analysis.
8. Interpretation and analysis of results.

The relationships between these tasks are illustrated in Figure 1. Each is discussed briefly below.

2.2.1 Plant Familiarization. The initial task of the analysis was to become familiar with the plant. This was done by identifying those functions that must be performed to prevent core melt or to mitigate its consequences. By reviewing the FSAR and other documentation, the systems that perform these functions, termed "front-line systems," were identified.

Initiating events for consideration in the analysis were determined from EPRI NP-801 and licensee event reports. These were grouped such that all initiating events requiring the same systems to respond were



INEL 2 1639

Figure 1. IRIS methodology.

placed in the same group. LOCAs were generally grouped into three or four groups. This grouping was by size of LOCA since mitigating requirements generally depend on the size of the break. Transients fell into three to six groups. The grouping often reflected equipment lost as a result of the initiating event.

For each initiating event grouping, the criteria for successful system operation to mitigate the accident were determined. This information was usually found in the FSAR. Utility and vendor calculations sometimes indicated that the FSAR criteria were too conservative. Where appropriate documentation existed, the IREP teams used the more realistic criterion.

A final task during plant familiarization was to identify system dependencies. Systems that support the front-line systems were identified; dependencies among various support systems were also noted.

Upon completion of plant familiarization, the following information was available:

1. The necessary functions to prevent core melt or to mitigate its consequence.
2. The systems that perform these functions (i.e., front-line systems).
3. The initiating events included in the analysis and grouped according to mitigating requirements.
4. The systems required to respond to each initiating event group and the criteria for system success.
5. Dependencies between front-line and support systems and among support systems.

Completion of this task set the groundwork for construction of the models used in the study. The systems to be analyzed were identified, and the number of and headings for event trees were defined.

2.2.2 Event Tree Construction. The accident sequences to be analyzed in IREP were delineated by event trees. Functional event trees were constructed to clarify functional dependencies. From these and information developed in the plant familiarization activity, systemic event trees were constructed. Sequences delineated on the systemic trees were analyzed in the study.

Separate systemic event trees were constructed for each initiating event group. Each event tree has a different structure since the initiating events were grouped according to mitigating requirements. Different mitigating requirements result in different tree structure. Headings for the event trees correspond to the systems responding to the initiating event. Only front-line systems appear on the trees. System dependencies and dependencies arising from phenomenological aspects of the accident are reflected in the tree structure.

2.2.3 Systems Analysis. Fault tree models were constructed for each front-line system. Support system fault trees were constructed to further model the particular interfaces with the front-line systems. The fault tree modeling approach used in this analysis is discussed in Section 6. Top events for the front-line system fault trees correspond to the success criteria defined in the plant familiarization task. The fault trees were developed to the component level. Component faults that affected only the particular component were grouped as "local faults." Faults that could affect multiple components, generally those faults associated with support systems, were further developed. The level of detail in the fault trees generally corresponds to the detail of available data.

In addition to hardware faults, the fault trees include unavailability due to test and maintenance, human errors associated with failing to restore components to their operable state following test and maintenance, and human errors associated with accident responses. Human reliability analysis is discussed in the next section.

The detailed development contained in the system fault trees facilitated identification of hardware, test and maintenance, and human error faults that could cause multiple component failures. These three classes of common mode failures were explicitly modeled in the fault trees. Other potential common mode failures, such as environmental conditions or manufacturing defects, were not considered in the study.

2.2.4 Human Reliability and Procedural Analysis. Test, maintenance, and emergency procedures were reviewed to determine potential human errors. Human errors associated with failing to restore the system to its operable state following test and maintenance were included explicitly in the fault trees. Potential operator errors in response to an accident were included in a limited way. The emergency procedures expected to be used in response to each accident sequence were reviewed to identify actions expected to be performed. Incorrect performance or omission of the actions were postulated and included in the model. The investigation, however, was limited to those actions expected to be performed, rather than postulating all actions an operator might take.

2.2.5 Data Base Development. A modified WASH-1400 data base was used for quantification of hardware faults. In some instances, plant-specific data were used instead. Test and maintenance intervals and durations were obtained, where possible, from discussions with plant personnel and from reviewing plant logs. Estimated upper values were chosen for human error rates for initial calculations. For those human errors that appeared in potentially dominant accident sequences, detailed analyses were performed with the assistance of human-factors specialists. This approach to human error quantification permitted more efficient use of limited human-factors expertise.

2.2.6 Accident Sequence Evaluation. For each accident sequence, an initial frequency was calculated. This was performed by logically combining the initiating event and the system successes and failures to develop combinations of failures that could result in the accident sequence. Frequencies assigned to the initiating events and probabilities assigned to each failure were combined to produce a frequency for each sequence.

The evaluation process was an iterative one. Initial calculations used generic data and upper bound human error rates. From these initial calculations, a collection of potentially dominant accident sequences was chosen. These were chosen based on a certain frequency below which none of the sequences were expected to contribute significantly.

The potentially dominant sequences were examined more closely to ensure that the probabilities chosen were as accurate as they could be and to develop better human error rate estimates. The potential for recovery actions that would terminate the sequence was evaluated in a gross manner. More refined calculations resulted in a list of dominant accident sequences.

2.2.7 Containment Analysis. Each potential dominant accident sequence was evaluated by Battelle-Columbus Laboratories to determine the expected mechanism of containment failure and the associated probability of failure, and to characterize the potential radioactive release. This analysis was quite limited in nature, relying primarily on insights developed from similar analyses in the past, but was supplemented by further calculations where necessary.

2.2.8 Interpretation and Analysis of Results. The dominant accident sequences in terms of risk (the highest probability sequences in the most severe release categories) were examined to develop engineering insights from the analysis. Those plant features contributing most significantly to risk were identified; these results constitute the principal results of the study. Limited uncertainty and sensitivity analyses were performed to ascertain a rough estimate of uncertainty in results and to identify those assumptions which, if changed, could significantly alter the results.

3. PLANT DESIGN

3.1 General

BF1 is a General Electric designed boiling water reactor (BWR) of the BWR-4 product line, with a Mark I (drywell and torus) containment. The TVA owns and operates the unit, which is located with two essentially identical units along the Tennessee River near Decatur, Alabama. Unit 1 began operating in August 1974 and has a rated power of 3293 MW thermal (1100 MW electric). The primary differences in the reactor systems of this plant compared with earlier BWR plant designs include:

1. Variable speed recirculation pumps that discharge into jet pumps arranged around the periphery of the reactor vessel.
2. An integrated core standby cooling system (CSCS) including high pressure coolant injection (HPCI), low pressure core spray, automatic depressurization (ADS), and residual heat removal (RHR) systems.
3. An integrated RHR system providing low pressure coolant injection (LPCI), shutdown cooling, and containment cooling modes of operation.
4. A reactor core isolation cooling (RCIC) system instead of an isolation condenser for mitigating transients where the reactor is isolated from the main condenser.
5. LPCI loop selection logic has been disabled and the LPCI discharge header cross-connect valve closed.

The containment design features include:

1. A drywell enclosing the reactor coolant system.
2. A wetwell (or torus) connected to the drywell and designed to provide energy suppression in the event of a LOCA and to provide a source of water for injection into the reactor.
3. A reactor building surrounding the drywell and torus that houses the CSCS and provides a second barrier between the reactor and the plant environment.

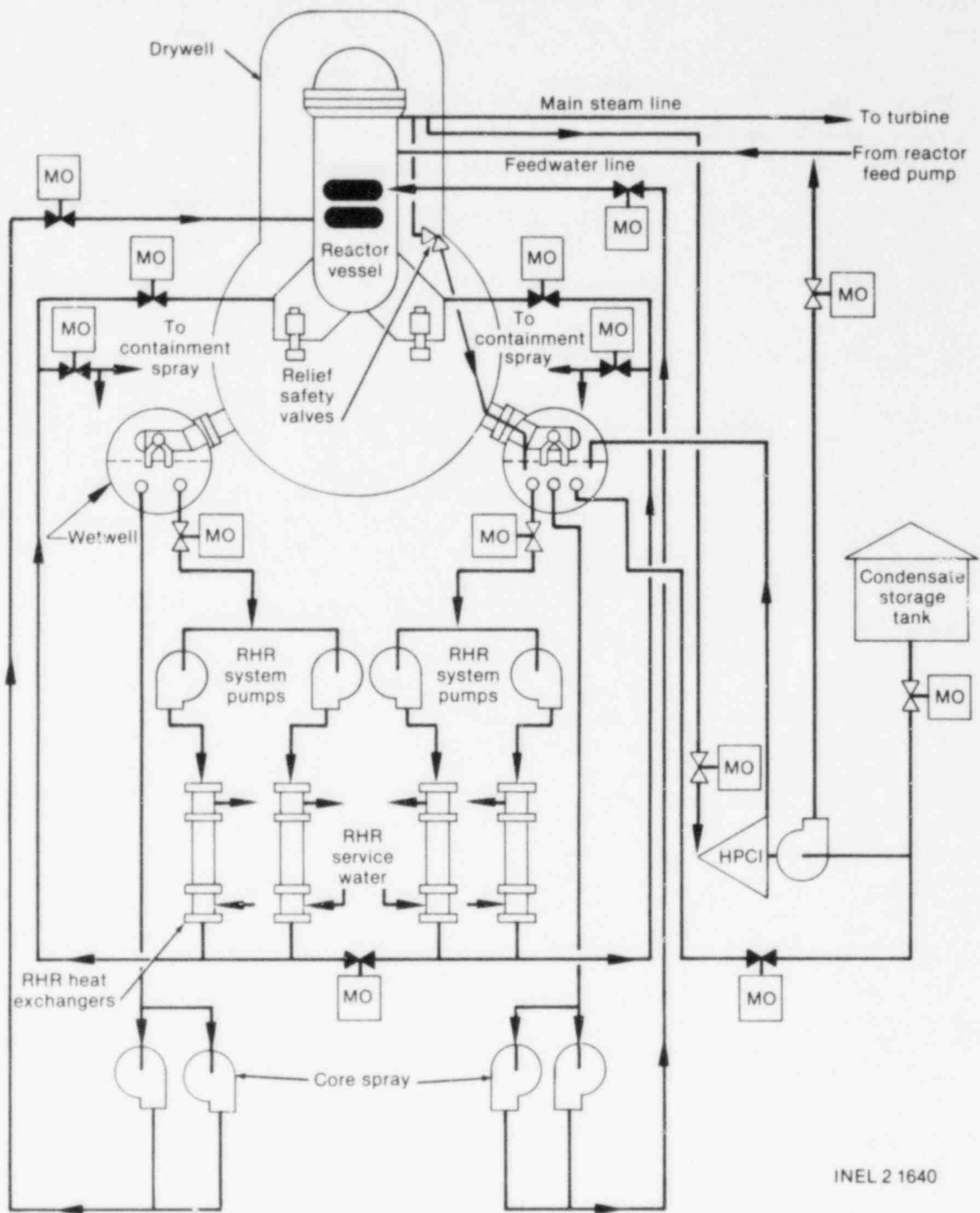
Figure 2 provides a simplified diagram of the safety-related design features.

3.2 Accident Mitigation Functions

The plant functions necessary to prevent core melt and mitigate radiological consequences of accidents fall into two groups. One group is the functions necessary to mitigate a loss of coolant accident (LOCA) while the other group is the functions necessary to mitigate a transient. The following sections generally describe the functions and the systems that perform these functions. More detailed function and system descriptions will be found in Sections 4 and 6, respectively.

3.2.1 LOCA Mitigators. There are four functions required to mitigate the effects of a LOCA. These are reactor subcriticality, short-term containment integrity (SCI), emergency coolant injection (ECI), and decay heat removal (DHR).

Reactor subcriticality is necessary to stop the fission chain reaction so that the heat generated in the core is reduced. This action limits the thermodynamic conditions that the remaining functions must mitigate. The control rod drive (CRD) system performs this function.



INEL 2 1640

Figure 2. Emergency core cooling systems.

SCI is necessary to ensure that any radioactivity released from the reactor coolant system boundary is not allowed to escape into the atmosphere. This is accomplished by ensuring that the pressure rise in the containment is limited to less than the containment design pressure. The vapor suppression system performs this function.

ECI ensures that the water lost from the reactor due to the LOCA is replaced. This action keeps the core covered and provides heat transfer from the fuel rods to prevent melting. The HPCI system provides high pressure injection while the core spray and LPCI systems provide low pressure injection. The ADS depressurizes the reactor so that the low pressure systems can operate.

DHR is the method by which heat from fission product decay is removed from the reactor to the ultimate heat sink, the Tennessee River. The RHR system provides this function in either shutdown cooling or torus cooling modes.

3.2.2 Transient Mitigators. There are four functions required to mitigate the effects of a transient. For purposes of this analysis, a transient is any event that challenges the reactor protection system (RPS) to initiate a reactor scram. The transient mitigating functions are reactor subcriticality, overpressure protection, vessel water inventory (VWI), and DHR.

The reactor subcriticality function for transient initiators is identical to that for LOCA initiators, except that successful reactor subcriticality can also be achieved if the power conversion system (PCS) remains available following the initiator and both recirculation pumps trip. It is recognized that in this latter case the reactor is not actually subcritical. However, the resulting power level after successful recirculation pump trip is such that the capacity of the PCS is adequate to remove the heat being generated. In this case, as long as the PCS is available, the core will be cooled. If PCS becomes unavailable, it is assumed the core will melt.

The overpressure protection function is required to ensure two actions. First, the relief valves must open to maintain reactor pressure below the emergency stress limits. Otherwise, some part of the reactor coolant boundary may rupture. Second, all the relief valves involved in this pressure limiting action must reclose after pressure falls below the relief valve setpoint to prevent an uncontrolled release of reactor coolant inventory.

The VWI function is analogous to the ECI function for LOCA initiators. The HPCI or RCIC system can provide high pressure coolant injection. For some transients, the PCS can also provide both the VWI and DHR functions. If the PCS is not available, isolation of the main condenser from the reactor vessel with the main steam isolation valves is necessary for successful VWI. Manual depressurization of the reactor vessel using the relief valves permits any of the low pressure systems, [i.e., core spray, LPCI, condensate system, or standby coolant supply (SBCS) system] to provide injection.

The DHR function for transients is the same as that described previously for LOCAs except for the case when PCS can provide long-term decay heat removal.

3.3 Front-Line and Support Systems

Front-line systems are those that directly perform the functions for mitigating the effects of a LOCA or transients. Support systems are those systems that effect LOCA or transient mitigation by way of their effect on the front-line systems. Table 2 lists the front-line systems for each mitigating function mentioned in Section 3.2. Table 3 lists both the front-line and support systems and their interdependencies.

Table 2. Front-line systems for LOCA and transient functions

LOCA Functions	Systems	Transient Functions	Systems
RS ^a	CRDHS	RS ^a	CRDHS, RPT
SCI	VS ^b	OP ^c	Relief valves
ECl	High pressure systems: HPCI	VWI	Main steam isolation: MSIVs
	Low pressure systems: ADS CS ^d LPCI		High pressure systems: HPCI RCIC PCS
DHR	RHR		Low pressure systems: Manual depressurization CS ^a LPCI Condensate SBCS
		DHR	RHR, PCS

- a. RS = reactor subcriticality
- b. VS = vapor suppression
- c. OP = overpressure protection
- d. CS = core spray.

Table 3. Front-line systems versus support systems

Front-Line Systems ^a	Support Systems									
	AC Power	DC Power	EAC ^b	EECW	RHRSW	RCW	Circulation Water	RPS	Keep-Full System	Operator
RCIC	—	X	—	—	—	—	—	—	—	—
RHR (shutdown cooling)	X	X	X	X	X	X	—	—	X	EOI-74
RHR (LPCI)	X	X	—	—	—	—	—	—	X	—
RHR (torus cooling)	X	X	X	X	X	X	—	—	X	EOI-74
RPT	—	X	—	—	—	—	—	X	—	—
HPCI	—	X	—	—	—	—	—	—	—	—
ADS	—	X	—	—	—	—	—	—	—	—
Core spray	X	X	—	—	—	—	—	—	X	—
SBCS	X	X	—	—	X	—	—	—	—	EOI-74
PCS	X	X	—	—	—	X	X	—	—	EOI-1,2,3
CRD	X	X	—	—	—	—	—	X	—	EOI-85
Relief valves	—	X	—	—	—	—	—	—	—	—
Vapor suppression	—	—	—	—	—	—	—	—	—	—
MSI	X	X	—	—	—	—	—	—	—	—

a. The front-line systems are given a one-letter name on the systemic event trees (see Table A-12).

b. Equipment area cooling.

4. INITIATING EVENTS

4.1 Introduction

Accident-sequence definition is one of the major steps of a risk assessment. It consists of defining a list of potential accident-initiating events and developing event trees to define the accident sequences that could result from these initiating events. Event tree development is discussed in Section 5 of this report.

4.2 Identification of Potential Core-Related Initiating Events

As a starting point for the risk assessment, potential initiating events that could lead to the release of significant amounts of radioactivity to the environment had to be identified. The initiating event list developed here is for core-related accidents with the plant at or near full power. Significant fuel pin damage can only take place if, as the result of greatly increased fuel temperatures, the fuel melts (or at least the cladding melts, which could, in turn, cause the fuel to collapse).

In order for the fuel or cladding to melt, an imbalance must occur between the heat generated in the core and the heat removed from the core. Thus, potential accidents that could not cause this imbalance are excluded from consideration of being core-related risks. There are two ways of creating a heat imbalance in the fuel: inadequate heat removal for the designed amount of heat generated (either at power or after shutdown) or excessive power generation due to failure to scram.

4.2.1 Inadequate Heat Removal. Heat removal during normal power operation is accomplished by the PCS, which consists primarily of the main steam, condensate, and feedwater systems. For inadequate heat removal to occur during power operation, this normal heat flow system must be disrupted by transients or LOCAs that disable the PCS, or by LOCAs that result in loss of reactor vessel coolant inventory. Transients can cause the PCS to be unavailable either directly by failing PCS systems or indirectly by isolation of the main condenser from the reactor by events that result in closure of the main steam isolation valves (MSIVs). Similarly, LOCAs cause the MSIVs to close upon low reactor vessel level.

Heat removal during shutdown (i.e., decay heat removal) can be accomplished by the normal heat flow system (i.e., by PCS) if available or by the RHR system. Inadequate decay heat removal would occur if both of these heat flow systems were disabled.

4.2.2 Failure to Scram. The second possible means of creating a heat imbalance in the fuel is for the reactor power to be greater than the capacity to remove heat. The transient initiators used in this analysis are defined as malfunctions or failures in the mechanical/electrical systems that result in a demand for trip of the control rods (scram) and removal of heat from the reactor core. Actions such as scrams as part of a planned shutdown or transients that do not result in a challenge to the reactor RPS to initiate a scram were not considered.

The transient and accident mitigating systems are designed to operate only with the reactor subcritical (i.e., with the reactor only producing decay heat). Only the PCS system is capable of removing significant heat from the reactor while maintaining reactor water level. Therefore, for all initiators where the PCS system is unavailable and the reactor is not made subcritical, it was assumed that the mitigating systems will not be able to keep the core covered and core damage will occur. For those initiators where the PCS is not disabled by the transient and insufficient rods do insert, the PCS can still remove the reactor heat and maintain water level provided recirculation pump trip (RPT) is successful. RPT is necessary to ensure that the resultant power level is within the capacity of the bypass valves to relieve steam to the condenser.

4.2.3 Initiating Event List. As discussed above, three major initiating event categories were defined: (a) LOCAs, (b) transients that disable PCS, and (c) transients that do not affect PCS.

LOCA Initiators—Initially, breaches of the reactor coolant boundary that lead to LOCAs inside and outside of containment were considered. However, it was determined that a rupture in an interfacing system that results in a LOCA outside primary containment always requires at least two valve failures. The probability of such an occurrence coupled with the probability of the rupture and subsequent emergency core cooling system (ECCS) failure is several orders of magnitude less than for ruptures inside containment. The rationale for exclusion of interfacing system LOCAs is provided in Section 5. Therefore only breaks inside the primary containment were considered for this analysis.

Break size ranges were developed based on system mitigation requirements. The ranges of break sizes for steam and liquid breaks were defined from the CSCS performance capability bar chart, Figure 6.3-1 of the Browns Ferry FSAR. This figure is shown as Figure 3. In general, the CSCS that are required for the various break ranges are indicated; specific CSCS performance is delineated in Table 4. The frequencies of pipe rupture as an initiating event for these various LOCA sizes are listed in Table 5.

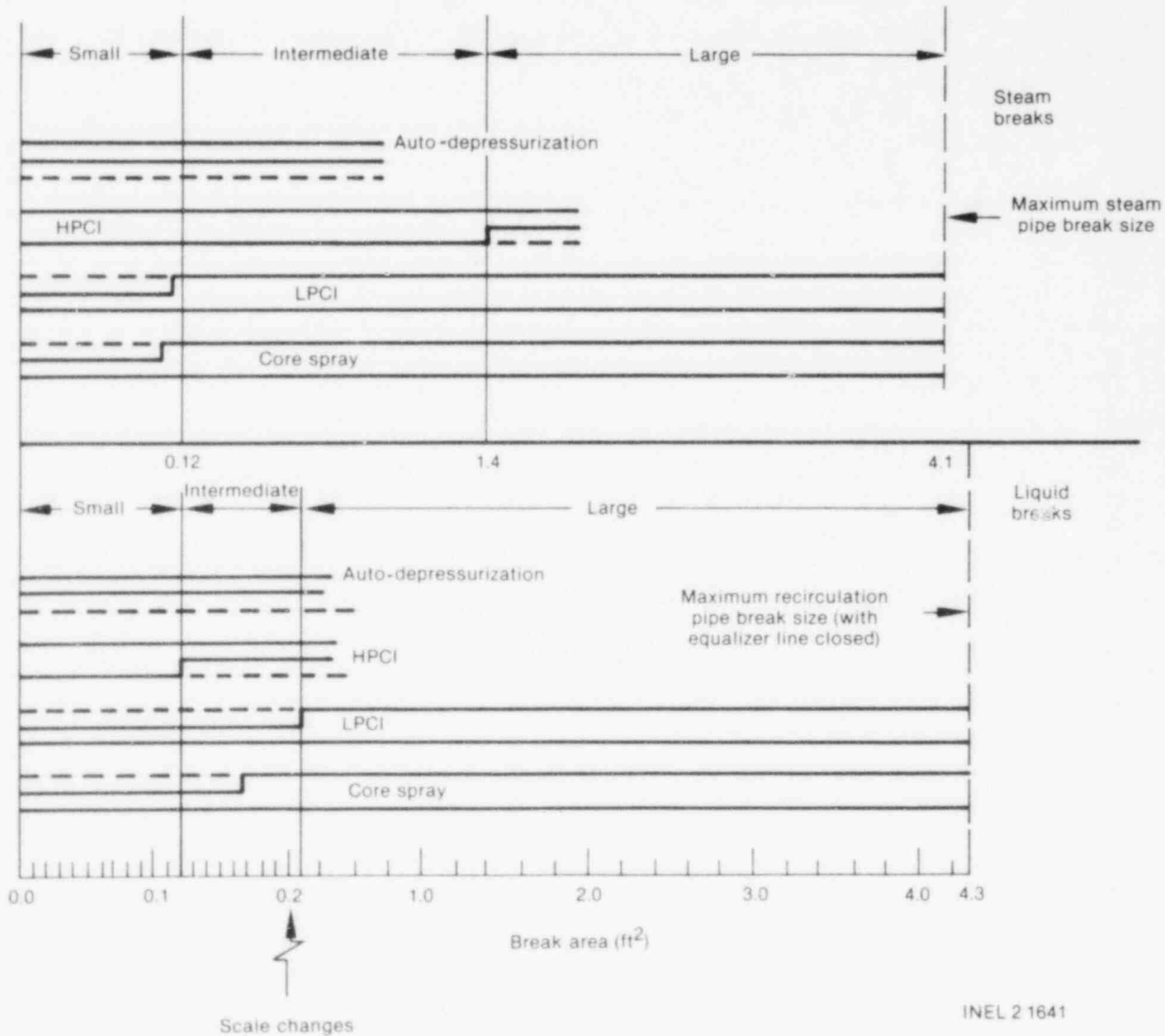


Figure 3. Core standby cooling systems performance capability bar chart.

Table 4. LOCA mitigation success criteria

Reactor Subcriticality	Short-Term Containment Integrity	Emergency Coolant Injection	Decay Heat Removal
Large Break—Liquid Line—0.3 to 4.3 ft ² —Suction			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	Two core spray loops and two of four LPCI pumps	Two of four RHR pumps with associated heat exchangers in torus cooling mode
or		or	
No more than five adjacent rods not fully inserted		Four of four LPCI pumps	or
		or	One of four RHR pumps with associated heat exchangers in shutdown cooling mode
		One of two core spray loops and two of four LPCI pumps (one LPCI pump per injection loop)	
Large Break—Liquid Line—0.3 to 4.3 ft ² —Discharge			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	Two core spray loops	Two of four RHR pumps with associated heat exchangers in torus cooling mode
or		or	
No more than five adjacent rods not fully inserted		One of two core spray loops and one of two LPCI pumps on unaffected side	or
			One of four RHR pumps with associated heat exchangers in shutdown cooling mode
Large Break—Steam Line—1.4 to 4.1 ft ²			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	Two core spray loops	Two of four RHR pumps with associated heat exchangers in torus cooling mode
or		or	
No more than five adjacent rods not fully inserted		Four of four LPCI pumps	or
		or	One of four RHR pumps with associated heat exchangers in shutdown cooling mode
		One of two core spray loops and one of four LPCI pumps	
Intermediate Break—Liquid Line—0.12 to 0.3 ft ²			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	One of one HPCI pump	Two of four RHR pumps with associated heat exchangers in torus cooling mode
or		or	
No more than five adjacent rods not fully inserted		Four of six ADS relief valves	or
		and	One of four RHR pumps with associated heat exchangers in shutdown cooling mode
		One of four LPCI pumps	
		or	
		One of two core spray loops	

Table 4. (continued)

Reactor Subcriticality	Short-Term Containment Integrity	Emergency Coolant Injection	Decay Heat Removal
Intermediate Break—Steam Line—0.12 to 1.4 ft ²			
No more than 30 rods scattered throughout the core not fully inserted!	Adequate suppression pool level and no bypass leakage from drywell to wetwell	One of one HPCI pump or One of four LPCI pumps or One of two core spray loops	Two of four RHR pumps with associated heat exchangers in torus cooling mode or One of four RHR pumps with associated heat exchangers in shutdown cooling mode
or			
No more than five adjacent rods not fully inserted			
Small Break—Liquid or Steam—Up to 0.12 ft ²			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	One of one HPCI pump or Four of six ADS relief valves and one of four LPCI pumps or Four of six ADS relief valves and one of two core spray loops	Two of four RHR pumps with associated heat exchangers in torus cooling mode or One of four RHR pumps with associated heat exchangers in shutdown cooling mode
or			
No more than five adjacent rods not fully inserted			

Table 5. LOCA pipe rupture frequencies

Type	Size	Location	Frequency (per reactor-Year)
Liquid	Large	Suction side Discharge side	9.9 x 10 ⁻⁶ 3.9 x 10 ⁻⁵
Steam	Large	—	5.2 x 10 ⁻⁵
Liquid	Intermediate	—	9.0 x 10 ⁻⁵
Steam	Intermediate	—	2.1 x 10 ⁻⁴
Liquid or steam	Small	—	1.0 x 10 ⁻³

Initiating event frequencies for the various liquid and steam LOCA break sizes were generally derived by multiplying the probability for a given break size times the relative frequency the break occurs in a specific portion of that size piping. One basic assumption was that, within a given break range category, (e.g., intermediate piping, 2 to 6 in.), the rupture was equally likely to occur in any of the piping, whether it be for liquids or steam. The probability for a given break size was taken from Table III 6-9 of WASH-1400. The BFI plant piping isometrics for the systems that comprise the primary pressure boundary were examined to determine the relative probability the break occurs in a specific portion of the piping. Section 2.1 of Appendix A provides an example calculation for LOCA initiator frequency.

Transient-induced LOCAs were treated as a special category of LOCA initiators. Failure of a sufficient number of safety relief valves to open following a transient initiating event was assumed to result in a primary system pressure boundary rupture. Failure of these valves to reclose after opening or failure of isolation valves in the main steam lines to close (when PCS is not available) will also result in a LOCA initiator. As discussed in Section 3 of Appendix A, both failure of a sufficient number of safety relief valves to open and failure of the MSIVs to close were determined to be insignificant compared to other LOCA initiator frequencies. However, the LOCA initiator due to a stuck-open-relief-valve (SORV) is the most likely of all LOCA initiators and is similar to an intermediate steam-break. Section 3 of Appendix A addresses these particular LOCA initiators.

These initiating event designators and their associated frequencies are shown in Table C-10 of Appendix C.

Transient Initiators—The initial set of transient initiators identified for this analysis were those listed in EPRI NP-801. Table A-5 of Appendix A defines this list of transient initiators. Section 14, "Plant Safety Analysis," of the Browns Ferry FSAR indicated those transients that result in thermal-hydraulic, flux, pressure, or similar reactor parameters to challenge the RPS to initiate a scram.

The Licensee Event Reports (LERs)⁹ submitted by Browns Ferry were examined to determine if there existed events not identified in EPRI NP-801. No other additional events were identified from this set of LERs. Each of the transient initiators were further examined along with various electric power bus and cooling water system failures to identify transient initiators effects on front-line system availability. This analysis is described in Section 4.3.2. The set of transient initiators were then examined and grouped according to common mitigating requirements. Only the availability of the PCS varied and, hence, initiating events were grouped according to their effect on PCS availability. Seven of the 37 EPRI NP-801 events were classified as transient initiators that resulted in PCS being unavailable for mitigation of the transient.

Of the remaining 30 events, 8 were identified as having no effect on PCS availability and 22 were considered not applicable for this study. Reasons for exclusion of these events are briefly summarized in Table A-6 of Appendix A.

One final consideration to the transient event was given in the case of the loss of offsite power (LOSP) event. This LOSP event was originally grouped as a PCS unavailable transient initiator. However, due to the dependency of other mitigation systems on this event, this particular event was treated separately in the transient event tree analysis.

The frequency of the transient initiators was estimated using the techniques discussed in EPRI NP-801. An example of these methods is illustrated in Section 2 of Appendix A. Table 6 lists the frequency of these transient initiators. The transient frequencies were estimated using two methods. The first method used strictly the plant-specific data found in EPRI NP-801. The second method was to obtain all pertinent BWR experience from EPRI NP-801 and to calculate the frequency based on the BWR data set. For this analysis, the plant-specific data were used in the transient event tree quantification.

The transient mitigation success criteria are given in Table 7.

Table 6. Transient initiator groupings and frequencies

		Frequencies (events/year)	
		<u>BF1</u>	<u>BWRs</u>
Group 1—Transients that cause PCS to be unavailable			
a.	MSIV closure	0.58	0.24
b.	Loss of normal condenser vacuum	0.56	0.41
c.	Pressure regulator fails open	0.	0.25
d.	Loss of feedwater flow	0.51	0.17
e.	Loss of offsite power	0.03	0.11
f.	Loss of auxiliary power	0.	0.03
g.	Increased feedwater flow at power	0.05	0.18
Totals		1.73	1.39
Group 2—Transients that do not cause PCS to be unavailable			
a.	Electric load rejection	1.02	0.74
b.	Electric load rejection with bypass failure	0.	0.
c.	Turbine trip	0.58	0.77
d.	Turbine trip with bypass failure	0.	0.
e.	Inadvertent closure of one MSIV	0.	0.10
f.	Pressure regulator fails closed	0.	0.11
g.	Bypass/control valve fails causing pressure increase	0.05	0.25
h.	Recirculation control fails causing increased flow	0.03	0.10
Totals		1.68	2.07

4.3 Initiating Event/Mitigating System Dependencies

In addition to identifying the initiating events, it is important to determine what effect the initiator may have on those systems designed to respond to the accident. In some cases, the initiating event may originate in a mitigating system. The resulting accident sequence could be significant since the normal level of redundancy in mitigating systems has been degraded.

The following sections discuss the LOCA and transient initiator effects on mitigating systems.

4.3.1 LOCA Initiator Effects on Mitigating Systems. Some of the LOCA initiators have the potential to render LOCA mitigation systems partially or completely inoperable. For example, a break on the discharge piping of a recirculation loop renders one loop of LPCI inoperable. To account for this possibility in the sequence calculations, the following procedure was used.

If a LOCA initiator could disable a mitigating system, the length of piping for the mitigating system susceptible to that LOCA was calculated using TVA supplied isometric drawings. Then, the total length of piping susceptible to that initiator was calculated. Table 8 provides a list of the systems and the percentage of their piping susceptible to a particular LOCA initiator. It was assumed that for a particular break size,

Table 7. Transient mitigation success criteria

Anticipated Transient	Reactor Shutdown		Overpressure Protection			Vessel Water Inventory			DHR	
	CRD	RPT	OP(O) ^a	OP(C) ^b	PCS	MSI	HPCI	DEP	INJ	RHR
Transients where PCS is available	No more than 30 rods fail to insert	Both recirculation pump strip ^b	NA	All relief valves reclose ^c	Condenser available and Feed system providing makeup	MSIVs shut ^d or Turbine valves ^d and bypass valves shut	HPCI or RCIC	Manual operation of at least four relief valves	One LPCI pump or One core spray loop or One booster and one condensate pump or One RHRSW pump in SBCS mode	Two RHR pumps and two heat exchangers in torus cooling mode or One RHR pump and one heat exchanger in shutdown cooling mode
Transients where PCS is unavailable	No more than 30 rods fail to insert or No more than five adjacent rods fail to insert		Direct scram 2 of 13 valves Flux scram 7 of 13 valves Pressure scram 10 of 13 valves	All relief valves reclose	NA	MSIVs shut or Turbine valves and bypass valves shut	HPCI or RCIC	Manual operation of at least four relief valves	One LPCI pump or One core spray loop or One booster and one condensate pump ^e or One RHRSW pump in SBCS mode	Two RHR pumps and two heat exchangers in torus cooling mode or One RHR pump and one heat exchanger in shutdown cooling mode

a. Relief valves open OP(O) and reclose OP(C).

b. If both recirculation pumps trip and PCS remains available, the resulting power level is such that the capacity of the bypass valves is adequate to remove the heat being generated.

c. Even though relief valve action is not required some relief valves will open.

d. MSI only necessary if PCS fails.

e. Although PCS is unavailable, the condensate system may still be operable.

Table 8. LOCA initiator effects on mitigating systems

LOCA Type	Mitigating Systems Lost	Piping Susceptible to LOCA (%)	Remarks
Large break on discharge of recirculation loops	One LPCI loop and one shutdown cooling discharge path	NA	Both are lost due to break location
Large break on suction of recirculation loops	All of shutdown cooling or None	55 (suction of recirculation Loop A) 45 (suction of recirculation Loop B)	Suction for both shutdown cooling loops comes from recirculation Loop A
Large steam	None	—	—
Intermediate steam	HPCI or One core spray loop or None	23.2 (HPCI) 3.8 (core spray) 73.0 (other piping)	Majority of piping susceptible to LOCA does not affect mitigating systems
Intermediate liquid	One LPCI loop and one shutdown cooling discharge path or All shutdown cooling or None	78.2 (discharge of Loop A or B) 11.2 (suction of recirculation Loop A) 10.6 (suction of recirculation Loop B)	—
Small liquid or steam	HPCI or One core spray loop or One LPCI loop and one shutdown cooling discharge path	16.3 (HPCI) 1.3 (core spray) 23.3 (recirculation discharge)	Assumes small break can occur in larger piping and renders mitigating systems unavailable as in large break cases
Steam	One core spray loop or One LPCI loop and one shutdown cooling discharge path	1.3 (core spray) 23.3 (recirculation discharge)	
Liquid	One LPCI loop and one shutdown cooling discharge path or All shutdown cooling or None	23.3 (recirculation discharge) 3.4 (suction of recirculation Loop A) 55.7 (other piping)	

the LOCA was equally likely to occur at any point on the piping susceptible to the LOCA. The unavailability of the mitigating systems was calculated considering the effect of the initiator. Therefore, the sequence frequency is the sum of two terms. The first term is the product of the probability of a break occurring in a location that affects the mitigating systems and the unavailabilities of those systems. The second term is the product of the probability of the break occurring in a location that does not affect the mitigating systems and the unavailability of those systems under that condition. Section 2.3.4 of Appendix C provides an example of this method.

4.3.2 Transient Initiator Effects on Mitigating Systems

Introduction—Transient initiators are identified in Section 4.2 and are grouped according to their effect on the PCS availability. However, it was necessary to examine these events further in order to determine if these could originate in mitigating systems or affect front-line systems other than the PCS.

Procedure—The goal of the transient initiator analysis was to identify those plant failures at a component or system level that could impact mitigating systems availability. The identification of transient initiator effects was done by a three part process as described below:

Task 1. Consequence Evaluation of Electrical Failures—Failure of each plant electrical bus was postulated. Equipment powered by the bus was tracked and the effect of its failure on the plant was identified.

Task 2. Consequence Evaluation of Cooling System Failures—Failure of each cooling system was postulated. Loads cooled by the system were tracked and the effect of their loss on the plant was identified.

Task 3. Causal Analysis of Transient Categories—Causal-type failure analysis was performed on the 15 transient categories. The BFI study identified 15 transient initiator categories. These were selected from EPRI NP-801. The causal analysis is similar to fault tree analysis in that events that can lead to occurrence of some undesired initiating event category are logically depicted.

Conclusions—The ultimate purpose of this effort was to identify possible dependencies in the core damage sequences not readily apparent from prior analysis. The results of Tasks 1 and 2 above are presented in tabular form in Tables A-7 to A-10 of Appendix A; Task 3 results are represented by causal failure diagrams in Figures A-1 to A-7 of Appendix A. A discussion of these results can be found in Section 2 of Appendix A. From these tables and charts the following conclusions can be drawn:

1. The only significant power failure that results in a scram and causes loss of a front-line system (i.e., the PCS) is a LOSP event.
2. Equipment cooling system failures were not considered to be significant transient initiators because of the allowable time for the operator to recover, e.g., to initiate alternate cooling systems.
3. The events in front-line or support systems that can initiate a transient category do not degrade the ability of the plant to respond to the accident. As can be seen by Figures A-1 to A-7 of Appendix A, the only initiating event failures identified that originate in mitigating systems were double failures in the electrical power system (EPS), e.g., failures in 250 V DC powered instrumentation and control (I&C) buses or 120 V AC RPS buses.
4. Failure of HPCI and RCIC upon loss of 250 V DC nonclass 1E power is possible but relatively improbable.

5. ACCIDENT SEQUENCE DELINEATION

5.1 Introduction

In general, the initiators listed previously in Tables 5 and 6 for LOCAs and transients, respectively, alone do not lead directly to fuel damage and release of radioactivity to the environment, but must be combined with other system failures. Event trees are used to display the functional relationships between systems designed to respond to a potential accident initiator.

5.2 LOCA Functional Event Trees

The LOCA functional event trees are shown in Figures 4 and 5. The purpose of these trees is to show the functions necessary to successfully terminate a LOCA sequence at BFI. A LOCA outside of the containment requires different functions for accident mitigation than the functions required for a break inside containment. This distinction made it necessary to construct two separate functional event trees for this plant.

5.2.1 LOCA Functional Event Tree—Breaks Inside Containment. If a LOCA occurs inside the primary containment boundary, there are three basic functions required for accident mitigation. These functions are successful reactor shutdown, containment integrity, and core cooling. For this plant, it is necessary to consider core cooling during two different phases of the accident. These phases are the immediate core protection or coolant injection/reflood phase of the accident and the long-term protection or decay heat removal phase of the accident. Consequently, core cooling is considered in two different places on the functional event tree. This, in effect, gives a total of four functions to be considered on the functional event tree for breaks inside containment. These functions together with the initiating event are depicted as event tree headings on the functional event tree shown in Figure 4.

Function Descriptions—In the following paragraphs, each function and its relationship to other functions will be described. The LOCA, or pipe break, is the initiating event for the accident sequences depicted in the functional event tree.

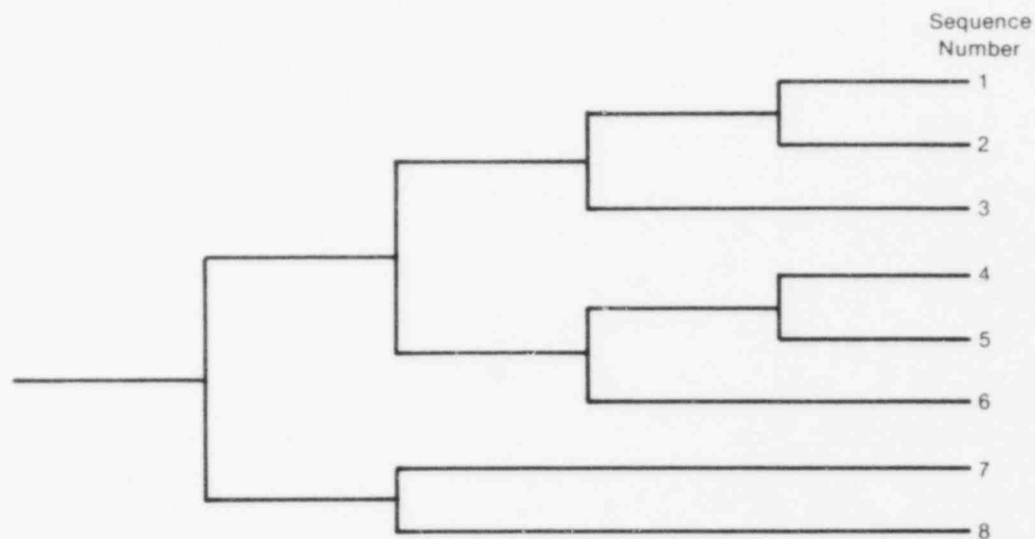
Reactor Subcriticality—If a LOCA inside the containment takes place, it is necessary to immediately stop significant power or heat generation due to the sustained fission process within the reactor. This is accomplished by rapid insertion of the control rods into the core. This is the purpose of the reactor subcriticality function. It was assumed that when reactor subcriticality is unsuccessful, the accident-mitigating functions will not successfully cool the core, the core will melt and, as a result, the containment will be breached and radioactivity will be released to the plant environment.

Upon successful completion of reactor shutdown, it immediately becomes necessary to confine the coolant inventory lost from the break to the inside of the primary containment boundary and to replace the coolant inventory that has been and is being lost out of the break.

Short-Term Containment Integrity—Successful containment of the coolant inventory lost from the break will prevent radioactive products contained or entrained in the coolant from being released into the environment. However, since BWRs characteristically contain large volumes of hot coolant, the release of this coolant into the containment atmosphere will rapidly pressurize the containment. If this pressurization is not reduced or limited by some overpressure protection system, it is assumed that the containment will rapidly overpressurize and rupture. The purpose of the SCI function is to provide this immediate containment protection during the coolant injection phase of the LOCA.

Functioning of the SCI has a direct side benefit. The physical scrubbing of the coolant by the torus water while the coolant is being forced through the torus water results in some of the radioactive particulates entrained in the coolant being transferred to the torus water. This, in effect, removes radioactivity from

PB	RS	SCI	ECI	DHR
LOCA	Reactor Subcriticality	Short-term Containment Integrity	Emergency Coolant Injection	Decay Heat Removal



X = Function failure

R S	S C I	E C I	D H R	Remarks
				Core cooled
			X	Slow melt
		X	N/A	Melt
	X			Core cooled
	X		X	Slow melt
	X	X	N/A	Melt
X		N/A	N/A	Melt
X	X	N/A	N/A	Melt

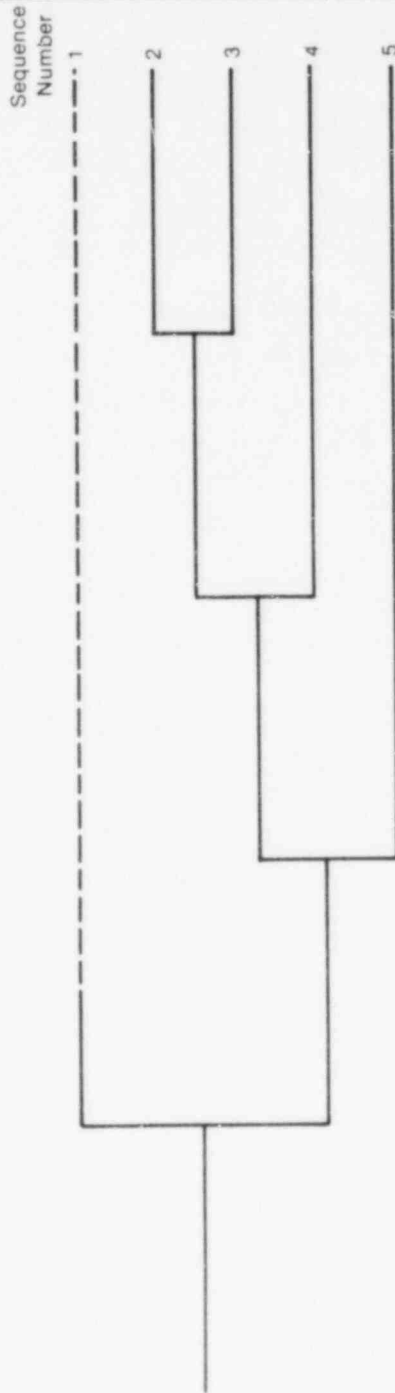
INEL 2 1642

Figure 4. LOCA functional event tree—break inside containment.

PB	BI	RS	ECI	DHR
LOCA	Break Isolation	Reactor Subcriticality	Emergency Coolant Injection	Decay Heat Removal

X = Function failure

B	R	E	D	Remarks
I	S	C	H	
		I	R	
				Transient sequence
X				Core cooled
X			X	Slow melt
X		X	N/A	Melt
X	X	N/A	N/A	Melt



INEL 2 1643

Figure 5. LOCA functional event tree—break outside containment.

the coolant, which results in less radioactivity buildup in the containment atmosphere. If the containment is subsequently breached such that the containment atmosphere is released to the environment, the resulting release will not be as severely radioactive as a release associated with the direct discharge of coolant to the environment.

Should the SCI function fail and the containment rupture, radioactivity will be released to the environment. However, the physical failure of the containment does not necessarily preclude other functions from being performed if the rupture occurs above the water line of the torus. As long as torus water is available, coolant injection can succeed, regardless of the state of the containment. Therefore, the event tree still shows branches for other accident-mitigating functions even though the SCI function has failed.

Since SCI is immediately activated by the physical processes of the LOCA, it is shown on the event tree prior to the remaining accident-mitigating functions. In other words, this function should precede the remaining functions by some finite time, and chronological ordering of the functions will place SCI before the remaining functions.

Emergency Coolant Injection—Even though the reactor is shut down, a significant amount of heat will still be generated in the fuel rods by the decay of the fission products contained within the fuel rods. This decay heat must be removed or the fuel rods will melt. Consequently, it is necessary to replace the coolant lost through the break or the core will be uncovered, the heat removal capability will be lost, and the core will melt.

The injection of relatively cool water into the core at a rate that is greater than the loss of coolant through the break is the purpose of the ECI function. There are two sources of injection water for the ECI function, the condensate storage tank (CST) and the torus. Only a limited amount of coolant (approximately 135,000 gallons) is available in the CST, requiring an eventual transfer of suction from the CST to the torus for those systems initially aligned to the CST. Consequently, as the torus water is injected into the core by the injection systems, the core is cooled, and a closed loop is formed by the injection pumps, the core, and the torus. This loop forms a recirculation flow path for the water and ensures a continuous source of water for injection. Thus, successful performance of this function will reflood the core and provide initial cooling of the core subsequent to the LOCA. Should ECI fail, it is assumed that the melt scenario discussed above will take place and the core will melt.

Upon successful completion of SCI and ECI, it becomes necessary to remove the decay heat from the torus water so that long-term core cooling can be maintained.

Decay Heat Removal—In the injection phase of the accident, discussed above, heat is continually being transferred from the core to the torus. The torus water is then pumped back into the core. This cycle will continually add heat to the torus and will ultimately cause loss of recirculation capability due to loss of net positive suction head to the pumps. The purpose of the DHR function is to remove this heat directly from the torus or prevent further heat buildup in the torus by removing the heat directly from the reactor coolant circulating around the core. These two modes of the RHR system are known as the torus cooling mode and the shutdown cooling mode, respectively. Success of the DHR function by either mode provides long-term core cooling and protection of the containment from overpressurization.

Heat is removed from the torus by the RHR heat exchangers installed in the discharge paths of the RHR pumps. River water is pumped through one side of these heat exchangers while the torus water passes through the other side. The heat in the torus water is transferred to the river water and the torus water is cooled.

Heat is removed from the reactor coolant circulating around the core in much the same way as it is removed from the torus. The RHR pumps are aligned to take a suction from recirculation Loop A and discharge back into one of the recirculation discharge loops via the RHR heat exchangers. Again, the decay heat is transferred to the river water. Of course, if the break is located on the suction side of recirculation Loop A, this method of decay heat removal will not be available.

Should DHR fail, it is assumed that the core will melt and the containment will fail due to the inability to continue pumping water from the torus back to the reactor.

Sequence Descriptions—The following paragraphs discuss the sequences shown in the LOCA functional event tree for breaks inside containment as depicted in Figure 4.

Sequence 1 (no failures)—Sequence 1 is the LOCA sequence with all functions working as expected. In this sequence, the core is cooled and no radioactivity is released to the environment.

Sequence 2 (DHR failure)—In Sequence 2, the DHR function is unavailable after successful performance of the other functions. In this case, decay heat cannot be removed and, eventually, the core will melt, the containment will be breached, and radioactivity will be released to the atmosphere.

Sequence 3 (ECI failure)—In Sequence 3, ECI fails, which causes a relatively rapid core melt and, thus, precludes the success of the DHR function.

Sequence 4 (SCI failure)—As discussed earlier, the failure of SCI does not necessarily preclude the success of the ECI or DHR functions. This is depicted in Sequence 4. In this sequence, the core is cooled even though the containment has been breached by the failure of SCI. The resulting radioactivity release will not be as severe as a release following core melt because, in this sequence, the core is still cooled.

Sequence 5 (SCI and DHR failure)—Sequence 5 results when both SCI and DHR fail. In this case, the containment is breached by the loss of the SCI function and the core eventually melts because the DHR function fails.

Sequence 6 (SCI and ECI failure)—Sequence 6 results when SCI and ECI both fail. Since the core cannot be cooled and the containment has already failed, core melt will occur and radioactivity will be released to the environment. No sequence branch is necessary for DHR because the core has melted before this function can mitigate the accident.

Sequence 7 (no mitigating functions)—As discussed earlier, when the reactor cannot be shut down following a LOCA, it is assumed that the accident mitigating functions will not successfully cool the core, the core will rapidly melt and, as a result, the containment will be breached. In this case, a branch is still shown for the SCI function because, if this function is successful, fission products entrained in the coolant will be scrubbed by the torus water, and the resultant radioactivity release will not be as severe as when the SCI fails to function at all. Sequence 7 depicts a failure of the reactor to shut down with subsequent success of the SCI function.

It should be noted that even with SCI function success, the containment will eventually rupture due to the core melt. But the consequences of the resulting release may be different from those resulting from Sequence 8.

Sequence 8 (scram and SCI failure)—Sequence 8 results when reactor subcriticality fails and SCI fails. In this case, the core melts rapidly and the containment is breached with resultant release of radioactivity to the environment. ECI and DHR will not mitigate the accident.

The LOCA systemic event trees are presented in Figures 6 through 11. The purpose of these trees is to show the interrelationships among the various systems that perform the functions previously discussed. Specific system success criteria are provided in Tables A-2 and A-3 of Appendix A.

5.2.2 LOCA Functional Event Tree—Breaks Outside Containment. If a LOCA occurs outside of the primary containment boundary, there are only two basic functions available for mitigating the LOCA once it is determined that the break cannot be isolated. These functions are successful reactor shutdown and core cooling. Containment overpressure protection will not be necessary because all heat, noncondensable gases, and radioactivity will be transmitted outside of the containment by the break. Core cooling is

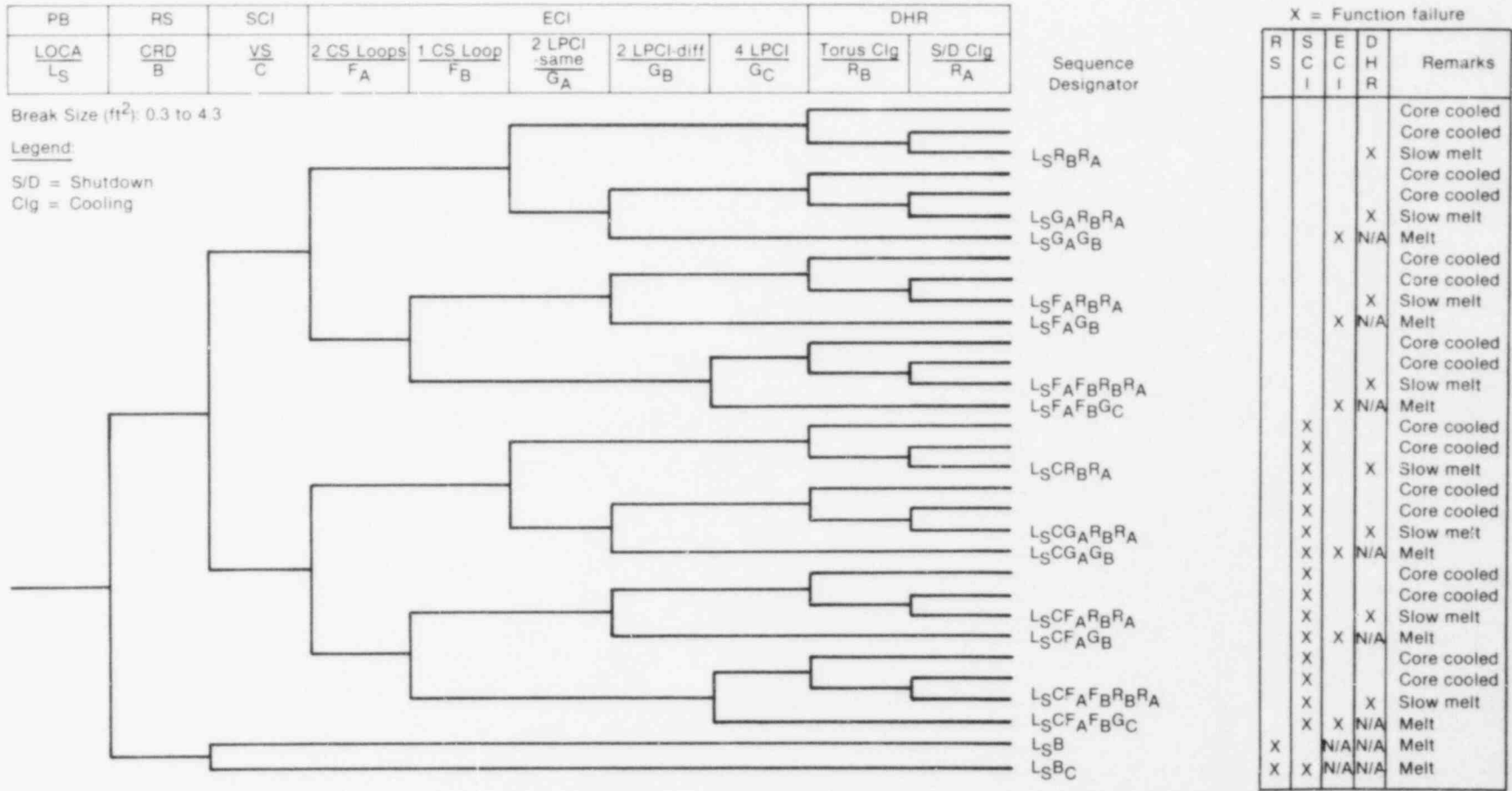
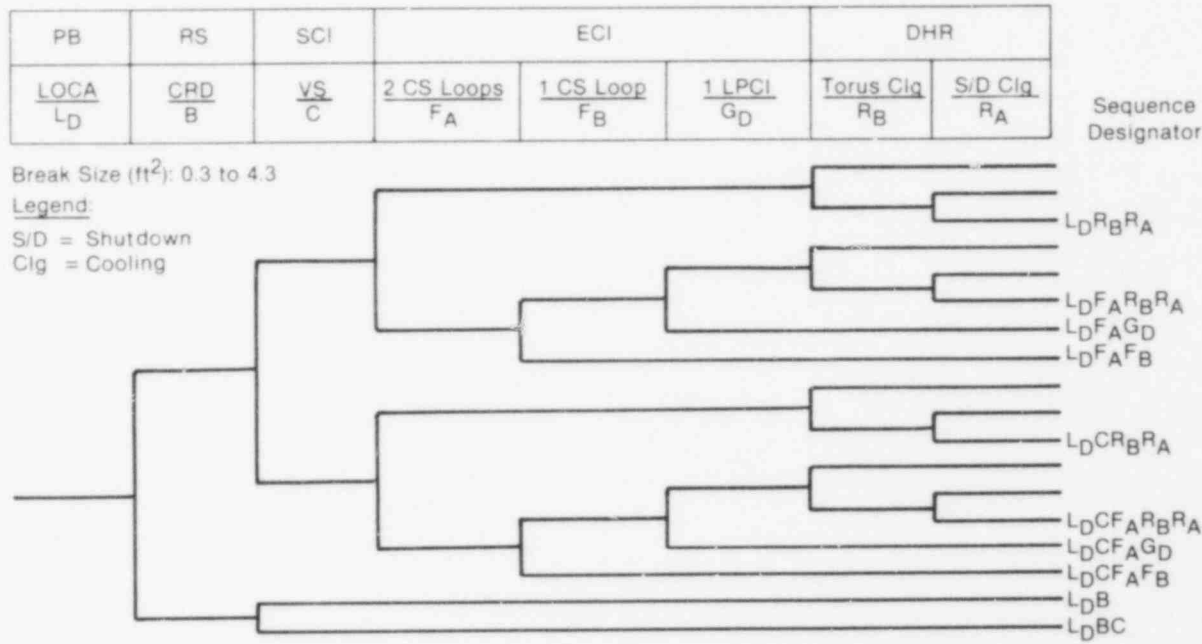


Figure 6. LCCA systemic event tree for large liquid break, suction-side of recirculation pumps (L_S).

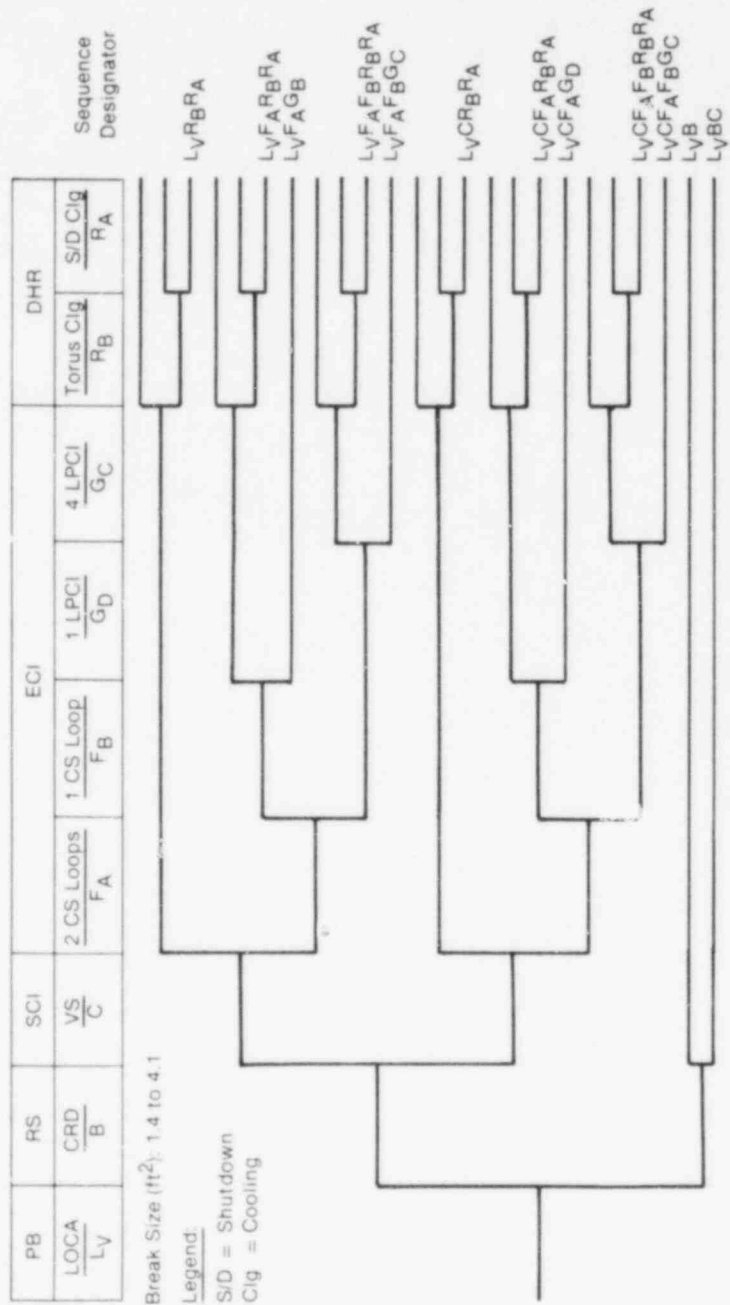


X = Function failure

R	S	E	D	Remarks
S	C	C	H	
	I	I	R	
				Core cooled
			X	Core cooled
				Slow melt
				Core cooled
				Core cooled
			X	Slow melt
		X	N/A	Melt
		X	N/A	Melt
X				Core cooled
X				Core cooled
X			X	Slow melt
X				Core cooled
X			X	Slow melt
X	X		N/A	Melt
X	X		N/A	Melt
X		N/A	N/A	Melt
X	X	N/A	N/A	Melt

INEL 2 1632

Figure 7. LOCA systemic event tree for large liquid break, discharge-side of recirculation pumps (L_D).

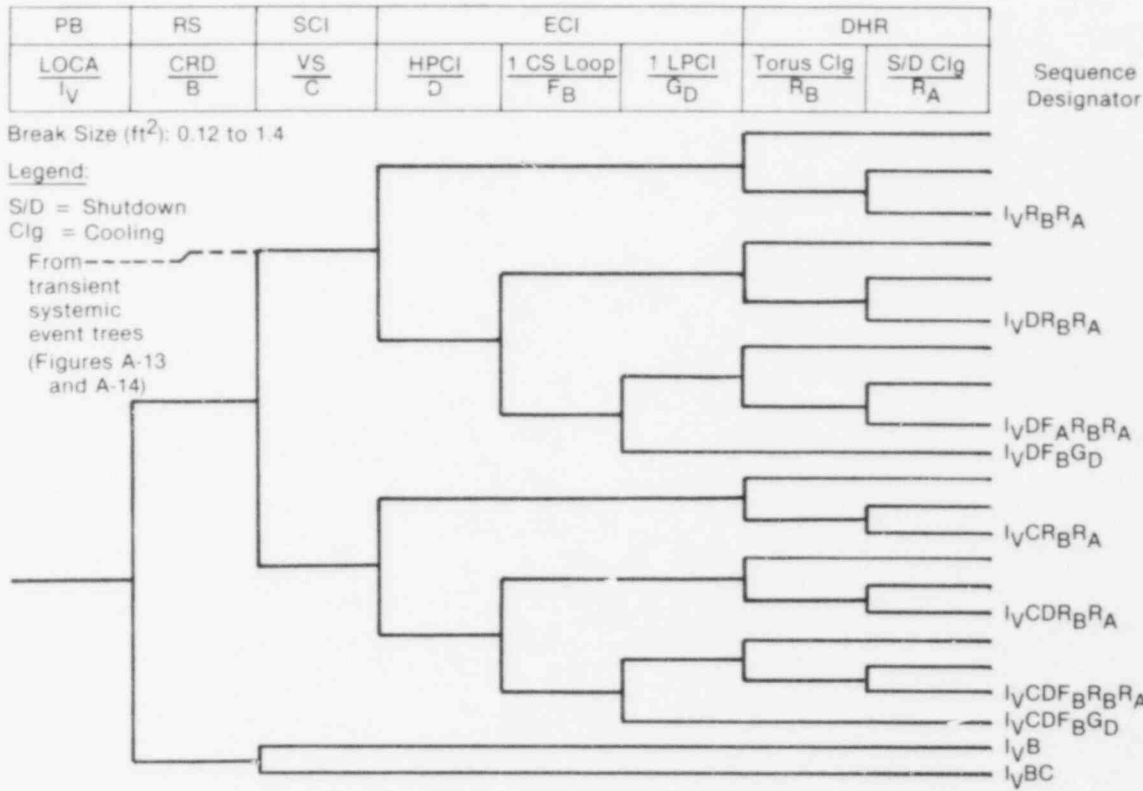


X = Function failure

R S I	S C I	E C I	D H R	Remarks
				Core cooled
			X	Core cooled
			X	Slow melt
		X	N/A	Core cooled
		X	N/A	Slow melt
		X	N/A	Melt
			X	Core cooled
			X	Core cooled
		X	N/A	Slow melt
		X	N/A	Melt
X	X			Core cooled
X	X			Core cooled
X	X		X	Slow melt
X	X		X	Core cooled
X	X		X	Core cooled
X	X		X	Slow melt
X	X		N/A	Melt
X	X		X	Core cooled
X	X		X	Core cooled
X	X		N/A	Slow melt
X	X		N/A	Melt
X	X		X	Core cooled
X	X		X	Core cooled
X	X		N/A	Slow melt
X	X		N/A	Melt
X	X		N/A	Melt

INEL 2 1633

Figure 8. LOCA systemic event tree for large steam break (Lv).



X = Function failure

R	S	E	D	Remarks
S	C	C	H	
I	I	I	R	
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
				Core cooled
			X	Slow melt
		X	N/A	Melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X	X	N/A	Melt
X		N/A	N/A	Melt
X	X	N/A	N/A	Melt

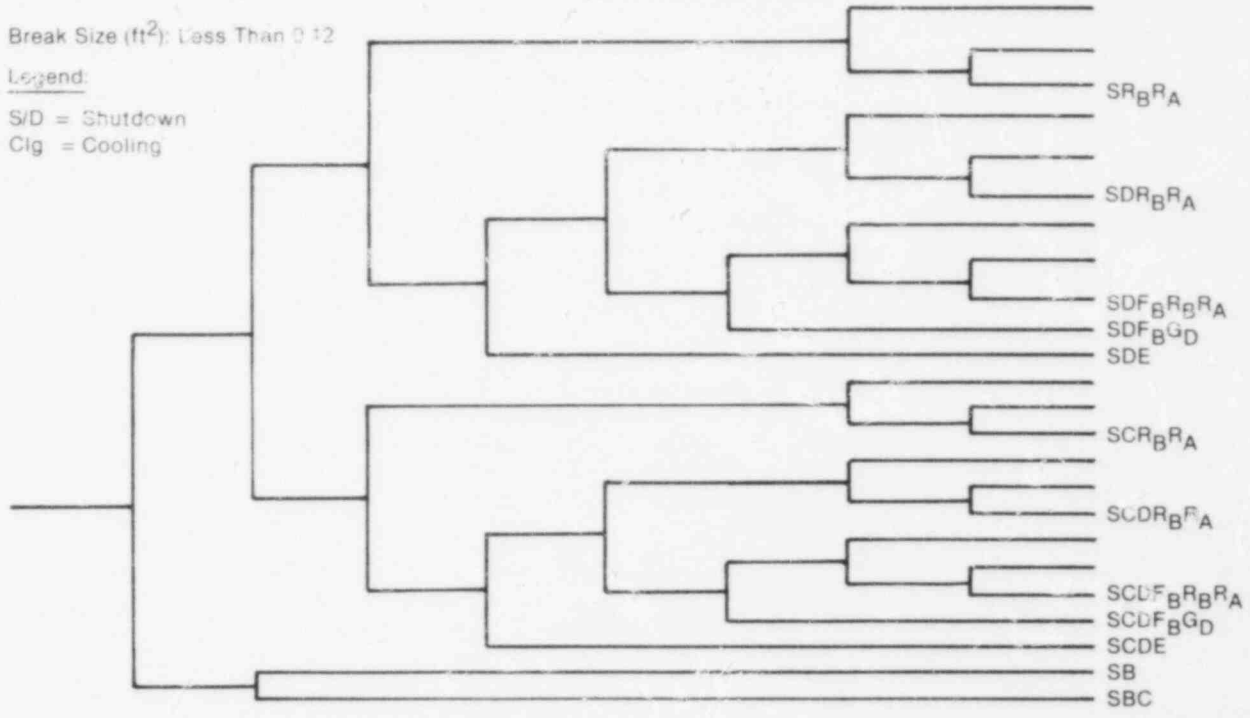
INEL 2 1635

Figure 10. LOCA systemic event tree for intermediate steam break (I_V).

PB	RS	SCI	ECI			DHR	
$\frac{LOCA}{S}$	$\frac{CRD}{B}$	$\frac{VS}{C}$	$\frac{HPCI}{D}$	$\frac{ADS}{E}$	$\frac{1 \text{ CS Loop}}{F_B}$	$\frac{1 \text{ LPCI}}{G_D}$	$\frac{\text{Torus Clg}}{R_B}$ $\frac{\text{S/D Clg}}{R_A}$

Break Size (ft²): Less Than 0.12

Legend:
S/D = Shutdown
Clg = Cooling



X = Function failure

R	S	E	D	Remarks
S	C	C	H	
I	I	I	R	
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
				Core cooled
			X	Slow melt
		X		N/A Melt
		X		N/A Melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X	X		N/A Melt
	X	X		N/A Melt
X			N/A	N/A Melt
X	X		N/A	N/A Melt

32

Figure 11. LOCA systemic event tree for small liquid-line or steam-line break (S).

still needed during the injection and long-term decay heat removal phases. This results in only three functions to be considered on the functional event tree for breaks outside containment. These functions, along with the initiating event and break isolation, are depicted as event tree headings in the functional event tree shown in Figure 5.

Function Descriptions—In order for a break outside the containment to become a LOCA, the break must be incapable of being isolated. Otherwise, the accident becomes a transient in which the break is isolated and, depending on break location, the PCS may or may not be available for mitigation of the transient. The second heading on the event tree, break isolation, reflects whether or not the break is isolated.

Reactor Subcriticality and Emergency Coolant Injection—The reactor subcriticality and ECI functions are identical to the corresponding functions discussed for the LOCA functional event tree for breaks inside containment.

Decay Heat Removal—If a break occurs outside of the containment, the coolant emitted from the break does not enter the torus as it does when the break occurs inside the containment. Thus, no closed loop is formed to return coolant to the core from the torus. Thus, the DHR function is different from that discussed earlier for a break inside containment.

For the break inside containment, the DHR function basically involves cooling of the torus water. Since a break outside the containment will eventually lead to loss of torus water, it will be necessary to replenish the torus water for successful long-term cooling of the core.

It should be noted that, in this case, the DHR function appears to be a continuous form of injection rather than torus recirculation. This is in effect, the case. Failure of the DHR function will eventually lead to core melt.

Frequencies of LOCA Outside Containment—Initially breaches of the reactor coolant boundary that lead to LOCAs inside and outside of containment were considered. However, it was determined that a rupture in an interfacing system that results in a LOCA outside primary containment always requires at least two valve failures. The probability of the rupture and subsequent failure to isolate is several orders of magnitude less than for ruptures inside containment. Similarly, for low pressure systems connected to the reactor coolant boundary but not normally operating when the reactor is at pressure, at least two valve failures must occur for the low pressure system to rupture due to exceeding its design pressure. Therefore, only breaks inside the primary containment were considered for this analysis. The rationale for exclusion of the break outside containment initiators is provided in the following sections.

Large Breaks—A large liquid break on the suction side of the reactor coolant recirculation pump cannot normally occur outside containment since there are two normally closed flow control valves (FCV-74-48 and 47) on either side of the containment penetration.

A large liquid break on the discharge side of recirculation pumps in the RHR injection piping would require failure of the testable check valve (CV-74-54). From Section 2 of Appendix A, the frequency for a large pipe rupture was 1×10^{-4} per reactor-year (Table III 6-9 of WASH-1400). Section XI of the ASME Boiler and Pressure Vessel Code,¹⁰ provides that the test frequency for check valves is at least once every 3 months. Failure frequency of a check valve in the severe internal leak mode is 3×10^{-7} per hour. The resultant unavailability based on a 3 month testing interval is 3×10^{-4} . Thus, the failure frequency for a large break LOCA in the RHR injection piping outside the primary containment is $(1 \times 10^{-4}) (3 \times 10^{-4}) = 3 \times 10^{-8}$ per reactor-year which is insignificant compared to a large discharge break inside containment (3.9×10^{-5}).

Large steam breaks were also insignificant. Section 2.13 of Appendix B shows a failure probability of 1.1×10^{-7} for failure of both MSIVs to close in a given steam line. A large steam break could also occur in the core spray, HPCI, or feedwater piping outside containment. For this failure to occur and not be

isolatable would require failure of a check valve and would be similar to the large liquid break frequency shown previously, 3×10^{-8} . This value is insignificant compared to the frequency of 5.2×10^{-5} for the large steam break inside containment.

Intermediate Breaks—The only intermediate size liquid break piping that interfaces with the primary coolant pressure boundary is that of the reactor water cleanup system. For a break to occur outside containment in the reactor water cleanup piping and not be isolatable would require the failure of an electric motor-operated valve to close (e.g., FCV-69-1), given the intermediate break. The valve failure rate is 1×10^{-3} per demand. The intermediate break frequency is 3×10^{-4} per year. This results in a relative initiator frequency of $(3 \times 10^{-4})(1 \times 10^{-3}) = 3 \times 10^{-7}$, compared with a frequency of 9×10^{-5} for an intermediate break inside containment. In addition, hand control valve (HCV-69-500) can be utilized to isolate the break.

An intermediate size steam break could occur outside containment in the RCIC or feedwater piping. For this break to occur and not be isolatable would require failure of a check valve (CV-3-572) to close, given the intermediate break. In this case, the valve failure rate is 1×10^{-4} per demand. This results in a relative initiator frequency of $(3 \times 10^{-4})(1 \times 10^{-4}) = 3 \times 10^{-8}$, compared with 2.1×10^{-4} for an intermediate steam break inside containment. In addition, hand control valve (HCV-3-66) can be utilized to isolate the break.

Although intermediate size breaks can occur on larger size piping, the frequency of these breaks and failure to isolate the large line is likewise insignificant.

Small Breaks—No small liquid or steam breaks were identified that interface with the primary coolant pressure boundary under the guidelines of NPRDS¹¹ for excluding lines 1-1/4-in. diameter or less. Although small size breaks could occur on large or intermediate piping, the break frequency and probability of failure to isolate makes these events insignificant compared to small breaks inside containment.

5.3 Transient Functional Event Trees

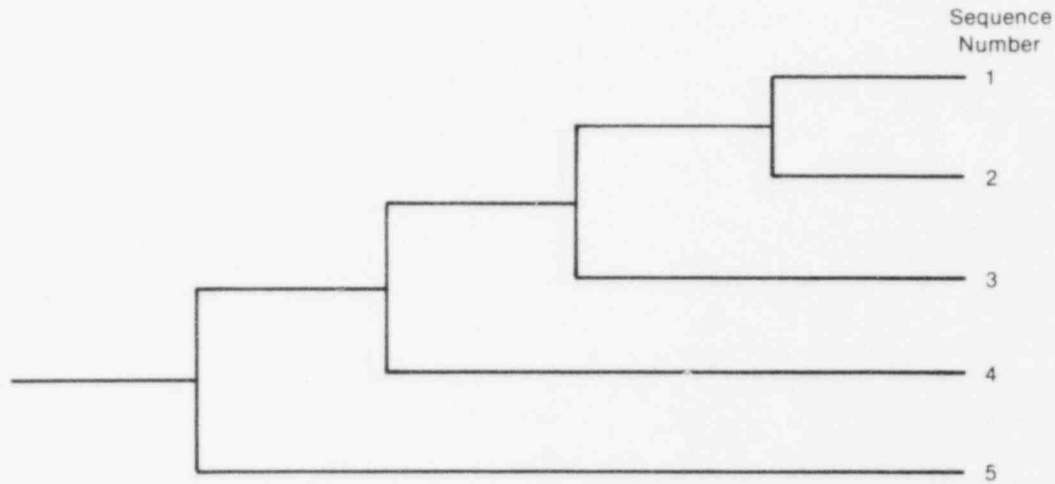
For purposes of this analysis, a transient is any event that causes thermal-hydraulic, flux, pressure, or similar reactor parameters to challenge the RPS to initiate a scram. Actions, such as a scram, as part of a planned shutdown or transients that do not directly result in a challenge to the RPS were not considered. The transient functional event tree is shown as Figure 12.

5.3.1 Function Descriptions

Reactor Subcriticality—The control rods should insert upon receipt of a scram signal caused by the transient. It is necessary for the control rods to insert in order to ensure that the reactor power level after the transient is low enough to allow the transient mitigating systems to function. Failure to insert a sufficient number of rods to achieve subcriticality after a transient with the PCS unavailable will result in a core melt. However, if both reactor coolant recirculation pumps trip and the PCS remains available, the resulting power level is such that the capacity of the bypass valves is adequate to remove the heat being generated.

Overpressure Protection—Following a loss of the PCS as a heat sink for the reactor, reactor pressure will increase sharply due to the decay heat generated by the core. It is necessary for a sufficient number of relief valves to open to limit this pressure rise in order to prevent exceeding reactor design pressure limits. It is also necessary that any relief valves which open in response to this pressure rise reclose when the pressure has dropped below the setpoint of the relief valves. Thus, there are two different ways the overpressure protection function can fail. One involves allowing pressure to get high enough to cause a break somewhere in the system, while the other involves a LOCA due to failure of a relief valve to reclose when necessary.

AT	RS	OP	VW:	DHR
Transient	Reactor Subcriticality	Overpressure Protection	Vessel Water Inventory	Decay Heat Removal



X = Function failure

R S	O P	V W I	D H R	Remarks
				Core cooled
			X	Slow melt
		X	N/A	Melt
	X	N/A	N/A	LOCA sequence
X	N/A	N/A	N/A	Melt

INEL 2 1644

Figure 12. Transient functional event tree.

Failure of a sufficient number of relief valves to open was an insignificant LOCA initiator as discussed in Section 2.5 of Appendix B. Failure of the safety relief valves to reclose was the most likely of the LOCA initiators. This initiator is similar to an intermediate steam break and was treated by transferring to the appropriate LOCA systemic event tree.

Vessel Water Inventory—The PCS (if it remains available) can provide both the VWI and DHR functions by removing steam from the reactor, condensing the steam, and returning the water to the reactor via the feed pumps.

If the main condenser becomes unavailable as a heat sink, it is necessary to isolate the reactor from the remainder of the PCS in order to prevent a loss of VWI at a rate greater than the capability of the mitigating systems to replace the water. Failure to isolate could result in a LOCA outside the containment. However, both MSIVs in a given line must fail to close for this condition to occur.

Once the reactor is subcritical, a substantial amount of residual heat and fission product decay heat will still be produced in the reactor. This heat will cause vessel pressure to rise and will result in either manual or automatic operation of the relief valves to reduce pressure in the reactor vessel, as discussed above. When the relief valves open to depressurize the vessel, the vessel inventory decreases because the steam passing through the valves is directed to the torus. Therefore, there are systems that must operate to inject water into the vessel to replace the lost inventory. If the systems capable of injecting water into the reactor do not maintain adequate VWI, a core melt results.

Decay Heat Removal—Even though replacement of VWI will cool the core, the torus will heat up as a result of open relief valves. Therefore, a means of directly cooling the core to prevent opening of relief valves or a means of removing heat from the torus must be established. Failure to remove heat from the core or the torus could result in containment overpressure, and ultimately, core damage.

5.3.2 Sequence Descriptions. The following paragraphs discuss the sequences shown in the transient functional event tree as depicted in Figure 12.

Sequence 1 (no failures)—Sequence 1 represents the normal course of events where all functions are successful and the core remains covered and cooled.

Sequence 2 (DHR failure)—After successfully accomplishing the reactor subcriticality, overpressure protection, and VWI functions, the DHR function fails. With long-term decay heat removal capability lost, the reactor begins to heat up. This heat is transferred by relief valve action to the torus and causes the torus water to heat up. Eventually, the torus water becomes too hot to be pumped back into the reactor to replace the steam lost through the relief valves. Therefore, core uncover occurs, and core melt and containment failure result.

Sequence 3 (VWI failure)—After the reactor subcriticality and overpressure protection functions succeed, the systems designed to maintain vessel water level fail. This causes the core to uncover, that results in a core melt. This sequence is more severe than Sequence 2 since core melt occurs sooner (when the reactor is generating more decay heat).

Sequence 4 (overpressure protection failure)—After a successful reactor shutdown, either an insufficient number of relief valves fail to open to limit the pressure rise or one or more of the relief valves fail to close when reactor pressure drops below the relief valve setpoint. Either of these conditions results in a LOCA inside containment.

Sequence 5 (reactor subcriticality failure)—After the transient initiating event, the CRD system does not function to bring the reactor to a subcritical condition. If the PCS is unavailable, the relief valves will continue to open and dump steam to the torus. The systems available to replace this lost inventory are not designed to replace the inventory as fast as the reactor is losing it. Consequently, the core will uncover and a rapid core melt will occur. Even if the PCS remains available following the initiator, failure of the reactor

recirculation pumps to trip will result in power level beyond the capability of the bypass valves to remove steam to the condenser. The feed pumps will eventually trip due to decreased inventory in the condensate storage tank (CST) caused by steam being dumped in the torus instead of returned to the condenser. The core uncovers and core melt occurs. This sequence, like Sequence 3, is more severe than other core melt sequences of this event tree due to the rapid core uncover and the high reactor power level at the time of uncover.

The transient systemic event trees are presented in Figures 13 and 14. The purpose of these trees is to show the interrelationships among the various systems that perform the functions previously discussed. Specific system success criteria are provided in Table A-3 of Appendix A.

AT		RS		OP		VWI				DHR		Remarks					
AT	RS	CRD	RV(O)	RV(C)	MSI	HPI	DEP	COND	1 CS Loop	LPI	1 LPCI		SBCS	Torus Clg	RHR	S/D Clg	R _A
Trans	T _U	B	J	K	N	Q	D	V	W	F	G	X	R _B				

R S		O P		V W		D H		Remarks
R S	O P	V W	I	D H	R			
X								Core cooled
				X				Core cooled
					X			Slow melt
						X		Core cooled
							X	Core cooled
							X	Slow melt
							X	Core cooled
							X	Core cooled
							X	Slow melt
							X	Core cooled
							X	Core cooled
							X	Slow melt
							X	Core cooled
							X	Core cooled
							X	Slow melt
							X	Melt
							X	Melt
							X	LOCA initiator
		X					N/A	LOCA initiator
		X					N/A	LOCA initiator
		X					N/A	LOCA initiator
X							N/A	Melt

X = Function failure

INFI 2 1637

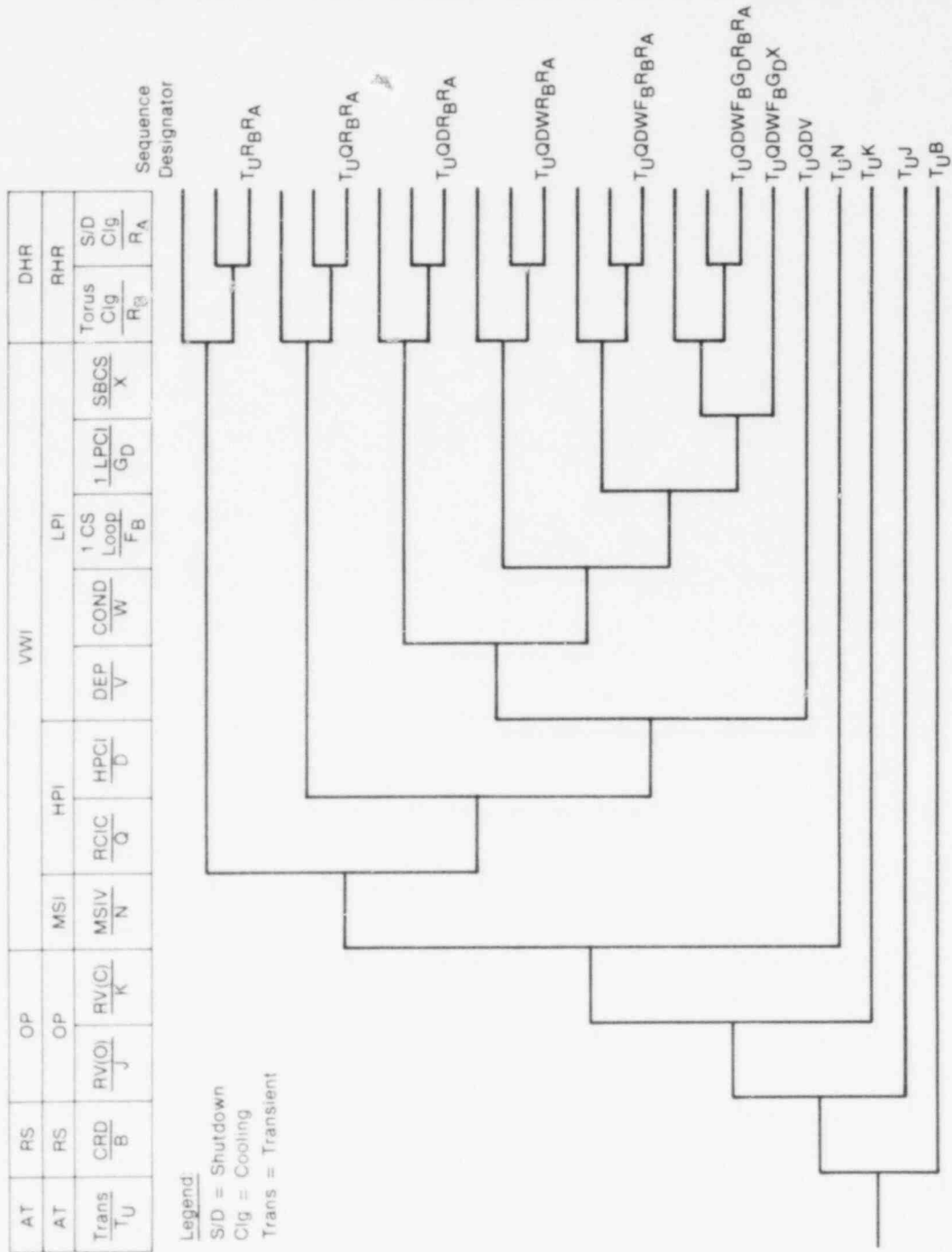
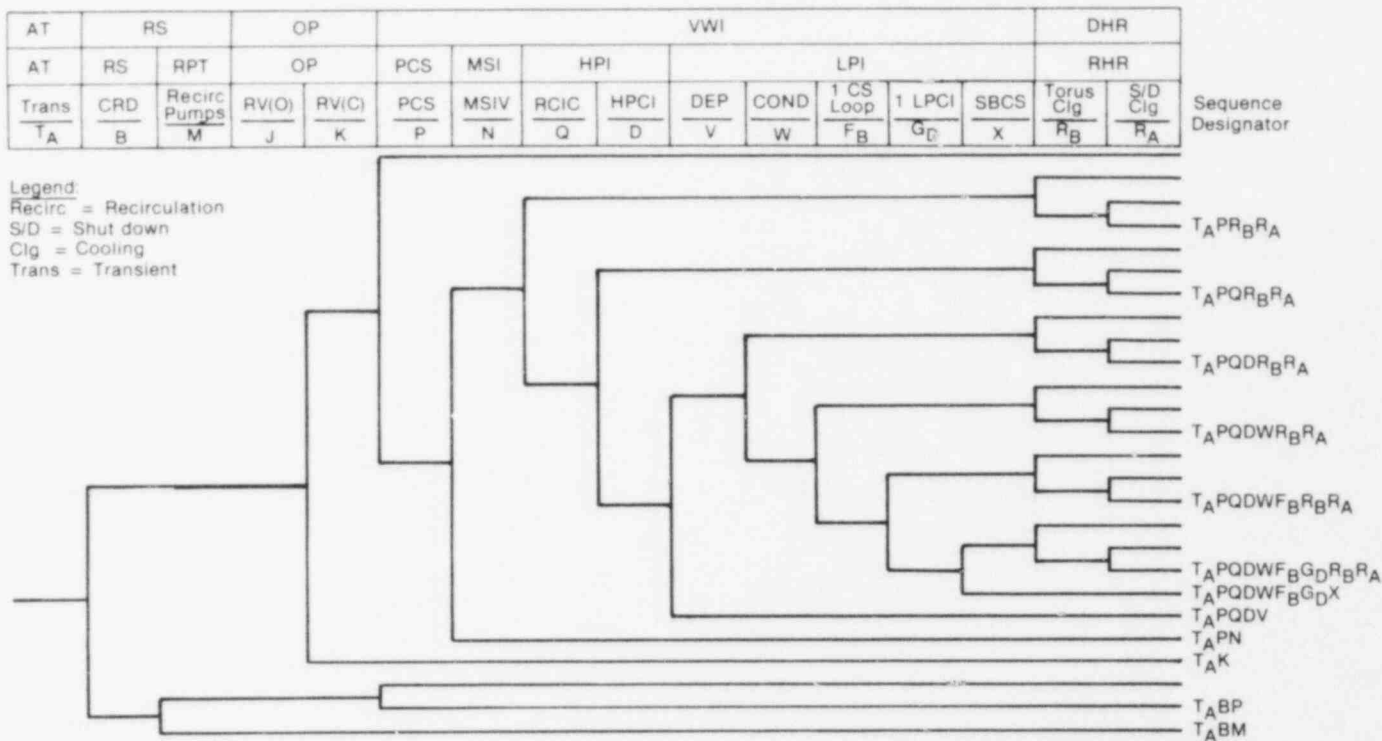


Figure 13. Transient systemic event tree where PCS is unavailable (T_U).



X = Function failure

R	O	V	D	Remarks
S	P	W	H	
		I	R	
				Core cooled
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
				Core cooled
			X	Slow melt
	X	N/A	N/A	Melt
	X	N/A	N/A	Melt
	X	N/A	N/A	LOCA initiator
	X	N/A	N/A	LOCA initiator
X	N/A	N/A	N/A	Core cooled
X	N/A	X	N/A	Melt
X	N/A	N/A	N/A	Melt

Figure 14. Transient systemic event tree where PCS is available (T_A).

6. SYSTEMS ANALYSIS

The systems affecting mitigation of a transient or LOCA fall into two categories. Front-line systems are those systems that directly affect the mitigation of a transient or LOCA, while support systems affect mitigation of a transient or LOCA only by their effect on front-line systems. Table 9 lists the front-line and support systems for BFI.

Table 9. Front-line and support system list

Front-Line Systems
Reactor core isolation cooling (RCIC)
Residual heat removal (RHR)
High pressure coolant injection (HPCI)
Automatic depressurization system (ADS) and safety relief valves
Core spray
Vapor suppression
Control rod drive (CRD)
Power conversion (PCS)
Standby coolant supply (SBCS)
Recirculation pump trip (RPT)
Main steam isolation (MSI)

Support Systems
AC power and DC power
RHR service water (RHRSW)
Emergency equipment cooling water (EECW)
Keep-full system
Condenser circulating water (CCW)
Raw cooling water (RCW)
Reactor protection system (RPS)
Equipment area cooling (EAC)

Based on the success criteria specified by the event tree analyses, fault trees were constructed and quantified for each front-line and support system, with the exception of the PCS, CRD system, RPS, keep-full system, and condenser circulating water system. For the first three systems listed, experience data from U.S. power reactor operating plants or values from WASH-1400 (BF1 is functionally identical to the Peach Bottom Plant analyzed in WASH-1400), or similar NRC-sponsored studies, such as NUREG-0460, were utilized. The latter two systems were determined to be insignificant contributors to front-line system unavailabilities, as is discussed in this section.

The success criteria from the event tree analyses define the top event for each fault tree. Construction of fault trees followed the guidelines of the abbreviated fault tree approach,¹² and the parent tree/daughter tree concept as presented in the IREP procedures guide. The parent tree was constructed first and represented the logic associated with the top event down to the subsystem, pipe segment, or similar level without specifically identifying the components involved. The daughter trees then expanded the inputs to the parent trees down to the component level. These daughter trees were generally divided into two parts: local faults (faults of components in that system) and interfacing faults (faults associated with operators or support systems). The interfacing faults identified locations where transfers were made to other fault trees. The local faults were then listed using tabulation OR gates. Each fault event in the tabulation OR gate is described by an eight-character code. This eight-character event naming code is described in Attachment A to Appendix B. Fault tree construction also conformed to the following guidelines:

1. System faults that could also be LOCA or transient initiators are explicitly included.
2. Passive failures are excluded except for single failures that fail an entire system or are either LOCA or transient initiators.
3. Flow diversions are explicitly included for fluid delivery systems if the diversion can cause the system to fail to meet its success criteria and the probability of the diversion is comparable to other system faults.
4. Spurious control faults are excluded unless the component would receive additional signals to change state during the course of a LOCA or transient.
5. Operator errors of commission are excluded for components not specifically identified in procedures as requiring operator manipulation.
6. Operator action to "back up" automatic actions are excluded from the fault trees and discussed under recovery operations.
7. Valve (or other component) mispositioning prior to a LOCA or transient is excluded if valve position indication is available in the control room and is monitored once every shift or if the mispositioned valve receives an automatic signal to return to the proper state after a LOCA or transient.

Browns Ferry is a three-unit nuclear station. The three units are not independent and, in fact, share many systems between the units. The front-line and support systems for Unit 1 that are shared with other units are as follows:

- Residual heat removal system
- Electric power system (AC and DC)
- Residual heat removal service water system
- Emergency equipment cooling water system

- Raw cooling water system
- Power conversion system
- Control rod drive hydraulic system.

Although the study was intended to address only Unit 1, the large number of shared systems between units made it necessary to address the effects of certain failures (e.g., loss of offsite power) on a plant-wide basis. Figure 15 illustrates some of these interunit and intersystem dependencies.

As a general rule, only those portions of shared systems dedicated to Unit 1 were modeled. In other words, no credit was taken for cross-connects to other units. There are of course exceptions. These are detailed in Section 1.2 of Appendix B.

6.1 Front-Line Systems Description

This section provides an overall description of the front-line systems. System description, assumptions, interfaces, and fault trees are discussed in more detail in Appendix B of this report.

6.1.1 Reactor Core Isolation Cooling System. The purpose of the RCIC system is to provide a source of high pressure coolant makeup water to the reactor vessel in case of a loss of feedwater flow transient. The RCIC system is also used to maintain the reactor in a hot standby condition.

For events other than pipe breaks, the RCIC system has a makeup capacity sufficient to prevent the reactor vessel water level from decreasing to the level where the core is uncovered. This is accomplished without the assistance of an ECCS.

RCIC system operation is designed to be completely independent of AC power. Only DC power from the plant batteries and steam extracted from the reactor vessel are necessary for startup and operation of the system.

Description—The RCIC system consists of a steam turbine assembly that drives a constant-flow pump and includes the associated piping, valves, controls, and instrumentation. Figure 16 is a simplified diagram of the system.

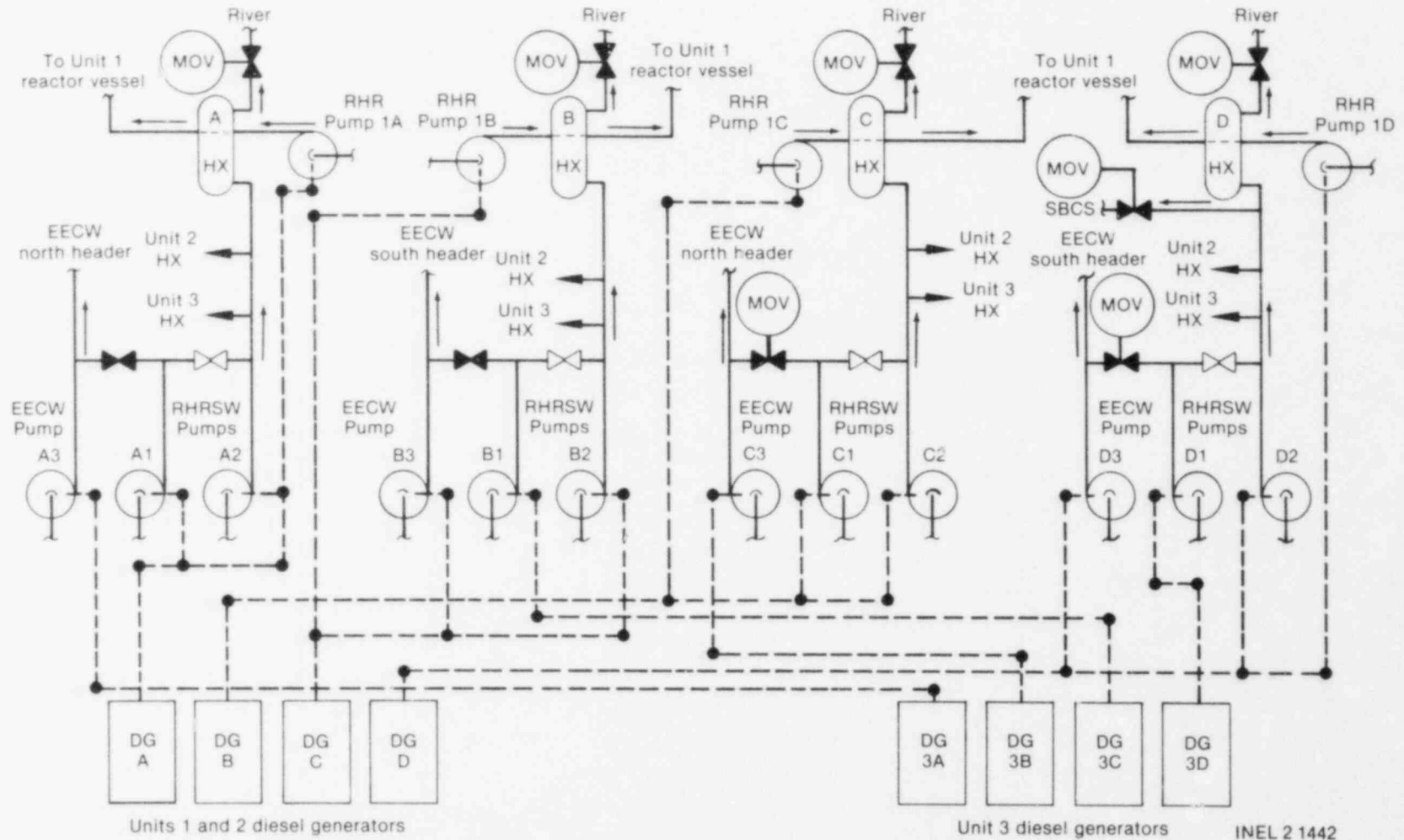
The RCIC turbine is driven by steam that is generated in the reactor vessel. The steam is extracted from main steam Line C upstream of the MSIV. The turbine exhaust is directed to the suppression pool. The turbine-driven pump is provided with two sources of water for injection into the reactor vessel. Demineralized water from the CST is used normally but water from the suppression pool is also available.

The RCIC system controls automatically start the system and bring it to the design flow rate of 600 gpm within 30 sec after receipt of a reactor vessel low-low water level signal. The system is designed to deliver the design flow rate to the core at reactor vessel pressures ranging from 1120 psig down to 150 psig. The RCIC system automatically stops when a high water level in the reactor vessel is signaled, when steam supply pressure drops below 50 psig, or when other system parameters generate a trip signal.

Application—The RCIC system appears only in the transient event trees. Its design basis is to provide makeup coolant to the reactor following a closure of all MSIVs. Therefore, the system is not capable of providing makeup coolant to the reactor during LOCAs.

Assumptions—There were no major assumptions that significantly affected RCIC system unavailability.

Insights—Failure of the first of two rupture disks is the dominant contributor to RCIC unavailability. This failure accounts for approximately 50% of the RCIC unavailability. The purpose of the rupture disks



INEL 2 1442

Figure 15. RHR/RHR/SW/EECW interplant power dependencies.

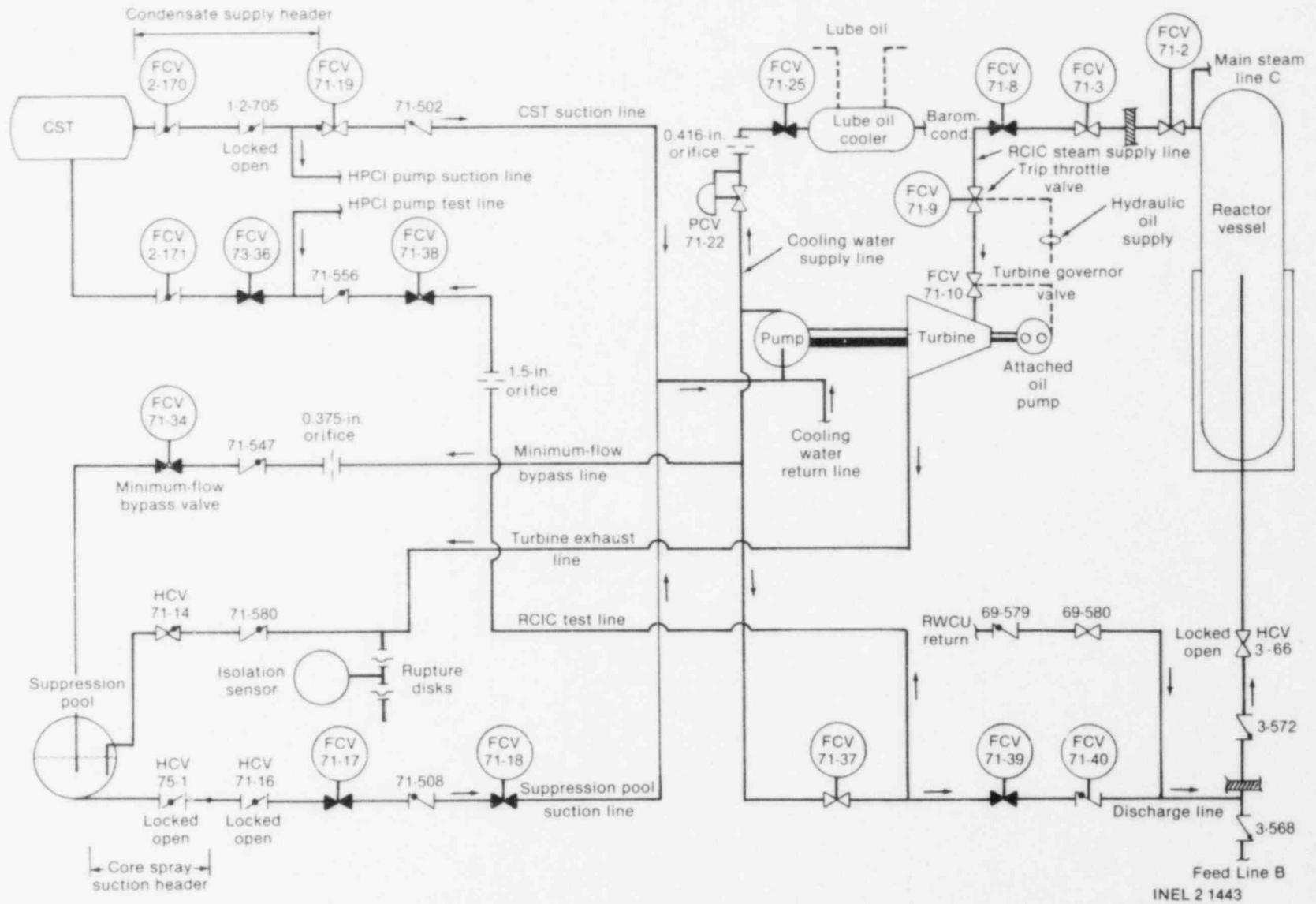


Figure 16. RCIC system.

is to prevent a turbine exhaust line blockage from damaging the turbine. In theory, the rupture disks should only be challenged by a double fault such as the discharge check valve failing to open and the high exhaust pressure trip failing to shut the turbine steam inlet. In practice, the cyclic heating load on the rupture disks leads to fatigue failure. A pressure switch between the first and second disk senses this failure and isolates the turbine. This is unnecessary if the second rupture disk is still intact. Therefore, failure of the first rupture disk leads to turbine isolation even though there is no exhaust line blockage and the second rupture disk is still functional. A factor of two reduction in RCIC unavailability could be achieved by modifying the sensors/circuitry to isolate RCIC on failure of the second rupture disk and only alarm on failure of the first disk.

6.1.2 Residual Heat Removal System. The RHR system provides water at low pressure to the reactor to restore and maintain water level following a LOCA. It also provides a means of removing the residual heat of the reactor after shutdown either by directly cooling the reactor water or by cooling of the torus water.

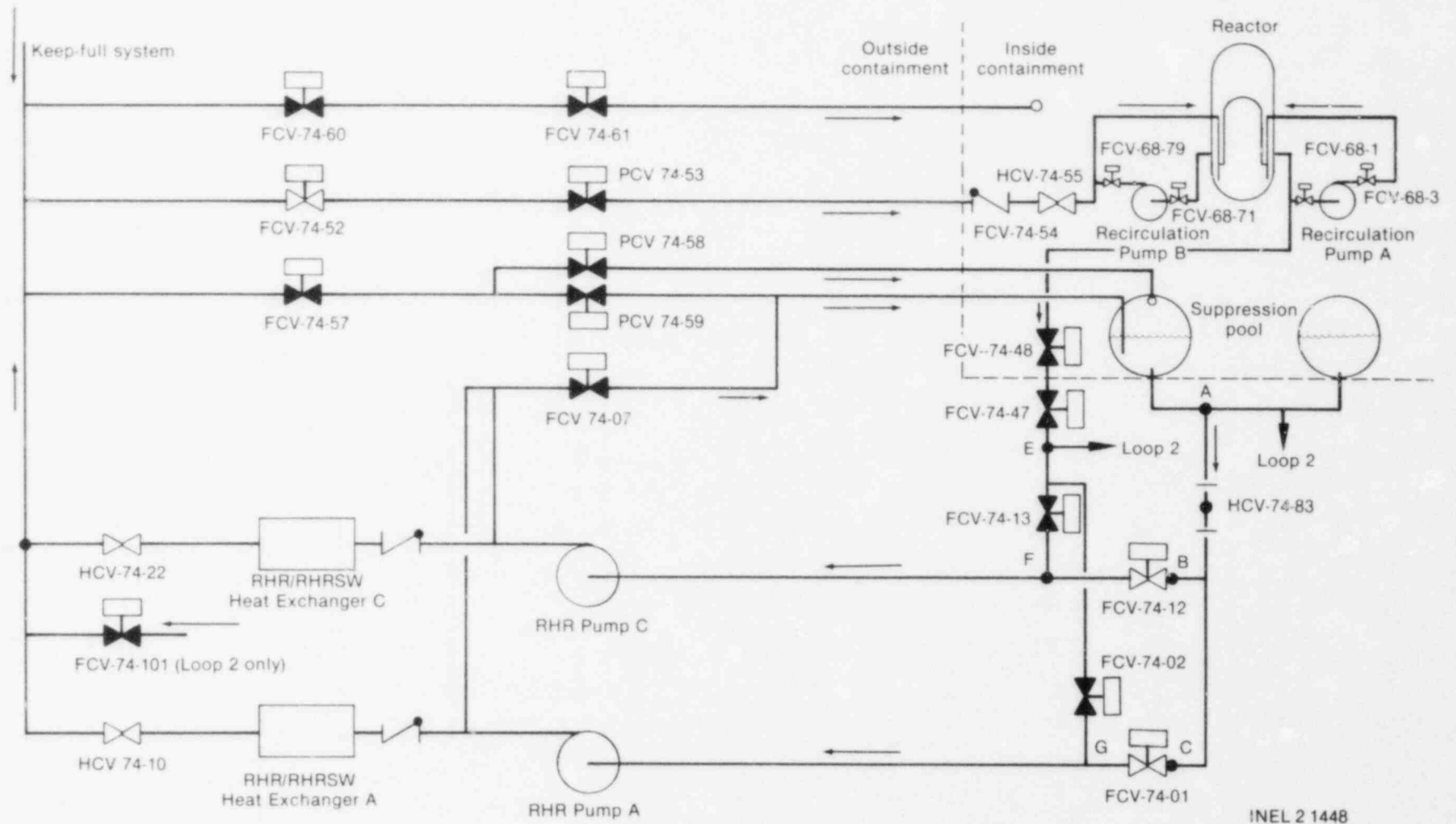
Description—The RHR system consists of two loops. Each loop has a suction line, two pump and heat exchanger combinations, and a discharge line. The loops take suction on the suppression pool (torus) or the reactor recirculation Loop A. Each loop discharges to the reactor, containment sprays, or torus cooling headers, depending on the mode of RHR operation. The LPCI mode takes water from the torus and pumps it into the reactor recirculation discharge piping. Shutdown cooling takes water from recirculation Loop A, cools it in the heat exchanger, and returns it to the reactor via the same discharge path as the LPCI modes. In the torus cooling mode, water is taken from the torus and cooled in the heat exchangers. The torus cooling discharge path is either to the torus spray header or torus test return line. SBCS uses the RHR service water (RHRSW) system to inject river water into the reactor via the same discharge path as LPCI (on Loop 2 only). Figure 17 shows a simplified drawing of Loop 1 of the RHR system. The RHR system drawing shows all the major components included in the fault trees. The valves are shown in their normal positions with the suction aligned to the torus. Loop 1 is shown in the drawing; Loop 2 is similar.

There are four modes of RHR operation modeled in the fault trees. These are the LPCI mode, shutdown cooling mode, torus cooling mode, and SBCS mode. The LPCI mode is automatically initiated upon receipt of a low level signal or a high drywell pressure signal coincident with low reactor pressure signal. All other modes of RHR operation are manually initiated. The logic circuitry provides reactor pressure interlocks to prevent system overpressurization during shutdown cooling and provides signals to open and close the minimum-flow bypass valves for each loop.

There are six system interfaces with the RHR system. These systems are AC and DC power, logic initiation circuitry, keep-full system, emergency equipment cooling water (EECW), raw cooling water, and RHRSW system. There are multiple combinations of AC and DC power necessary to operate the RHR system depending on which mode of RHR is in use. The logic circuitry provides automatic initiation signals and protective interlocks to prevent overpressurization of the RHR system whenever the raw cooling water system cannot. The EECW system provides room cooling and pump seal cooling for the RHR system. The keep-full system ensures that the discharge piping of each RHR loop is filled with water. This prevents water hammer damage when the pumps start. The RHR service water system provides cooling to the RHR heat exchangers for the shutdown cooling, torus cooling, and containment spray modes of RHR operation.

Application—The RHR system appears in every event tree in one or more modes. Table 10 summarizes the success criteria for each mode of RHR operation and lists which event tree applies to each mode.

Assumptions—Failure of the minimum-flow bypass valves to close when required can allow 10% of rated flow to be diverted from the desired path. This analysis assumes this causes failure of that loop since no analyses are available to show that 90% of rated flow is sufficient. Also, if the LOCA initiator is a break on a recirculation loop discharge side, this analysis assumes that the RHR loop which discharges to that loop is likewise failed due to flow diversion.



INEL 2 1448

Figure 17. RHR system, Loop 1.

Table 10. RHR operational mode success criteria

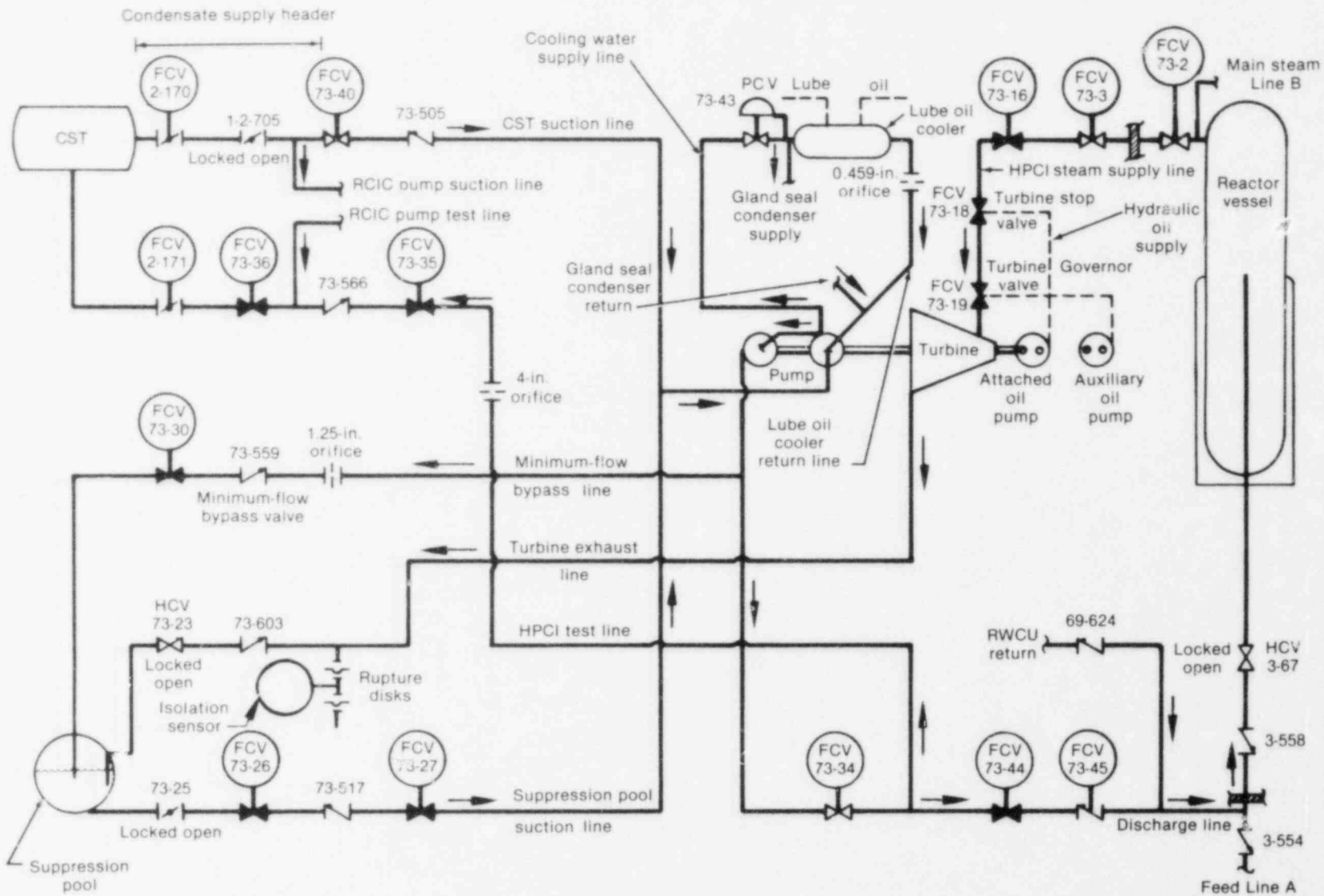
Designation	Success Criteria	Applicable Event Trees
G _A	Two LPCI pumps in the same loop deliver rated flow to the core	Large suction break
G _B	Two LPCI pumps in different loops deliver rated flow to the core	Large suction break
G _C	Four LPCI pumps deliver rated flow to the core	Large suction break; large steam break
G _D	One LPCI pump delivers rated flow to the core	Large discharge break; large steam break; intermediate breaks; small breaks; transients
R _A	One pump and heat exchanger circulating reactor coolant	All
R _B	Two pumps and heat exchangers circulating torus water	All
R _S	One RHRSW pump delivering rated flow to reactor through RHR Loop 2	Transients

Insights—Other than the main condenser, the RHR system is the only system capable of transferring reactor decay heat to the river. Therefore, for LOCA initiators and transients where PCS is not available, it is the only system available to remove decay heat. This fact makes the RHR system the limiting factor affecting core melt frequency. No matter what actions are taken to improve the reliability of other systems, the core melt frequency can never be made less than the frequency of core melt sequences where RHR fails. Furthermore, this analysis has shown that core melt sequences resulting from RHR failures constitute over 70% of the frequency of the total dominant sequences even after recovery is considered. Therefore, the RHR system must be considered to be the most risk critical system at BF1.

6.1.3 High Pressure Coolant Injection System. The HPCI system is one of the ECCS at BF1. The primary purpose of the HPCI system is to provide a supply of cooling water to reflood the reactor core in the event of a LOCA that does not result in depressurization of the reactor vessel. The HPCI system is designed to provide this function unassisted for all liquid breaks less than 0.12 ft² in area (or approximately 5 in. in diameter) or all steam breaks that are less than 1.4 ft² (or approximately 16 in. in diameter). The HPCI system can also be used to provide makeup water to the reactor during periods when the reactor is at or near normal operating pressure and is isolated from normal makeup sources.

Description—HPCI system operation is designed to be completely independent of AC power. Only DC power from the plant batteries and steam extracted from the reactor vessel are necessary for startup and operation of the system. The HPCI system consists of a steam turbine assembly that drives a constant-flow pump and includes the associated piping, valves, controls, and instrumentation. Figure 18 is a simplified diagram of the system.

The HPCI turbine is driven by steam that is generated in the reactor vessel. The steam is extracted from main steam Line B upstream of the MSIVs. The turbine exhaust is directed to the suppression pool. The turbine-driven pump, which actually consists of main pump and booster pump driven by the HPCI turbine



48

INEL 2 1479

Figure 18. HPCI system.

through a speed reducer, is provided with two sources of water for injection into the reactor vessel. Initially, demineralized water from the CST is used. This provides reactor-grade water to the reactor vessel for the case where the need for HPCI is rapidly satisfied. After the water in the CST is depleted, the CST low level signal will automatically shift suction to the suppression pool.

The HPCI system is designed to start and inject water into the reactor vessel without operator action. However, the system can be operated manually. When reactor vessel level decreases to 476.5 in. above vessel zero or when drywell pressure increases to 2 psig, the HPCI logic circuitry sends an initiation signal to various HPCI components to start the system. The turbine control system will maintain turbine speed to provide constant-flow to the reactor vessel until a turbine trip signal or an isolation signal shuts the system down.

Application—The HPCI system appears in the event trees for intermediate and small breaks and all transients. It does not appear in event trees for large breaks since depressurization will occur too fast for the HPCI system to be useful.

Assumptions—A major assumption associated with the HPCI system is that suction transfer from the CST to the torus is required for LOCAs but not for transients. The minimum level of the CST is based on having sufficient volume to replace inventory lost due to decay heat for 8 hours. For LOCAs, the rate of inventory loss is much higher and therefore requires the transfer.

Insights—The rupture disk arrangement for the HPCI system is almost identical to that of the RCIC system. Depending on whether the initiator is a LOCA or transient, rupture disk failure accounts for about 31 and 45%, respectively, of the HPCI unavailability. For the same reasons mentioned in Section 6.1.1, this contribution could be eliminated by modification of the sensors and circuitry.

Routine scheduled tests and maintenance account for over 25% of the HPCI system unavailability for LOCA sequences (about 14% for transients). The purpose of routine testing is to verify operability and limit unavailability by discovering faults as soon as practical for standby systems. Since the testing itself accounts for one quarter of the unavailability, it would be desirable to review the testing duration and frequency to determine if a more optimum schedule can be arranged that will reduce the testing contribution to unavailability without causing component unavailabilities to significantly increase.

6.1.4 Automatic Depressurization System and Relief Valves. The reactor and the steam system are protected from overpressure by 13 relief valves. The 13 valves are distributed among the four main steam lines and located upstream of the main steam isolation valves. Each valve discharges to the suppression pool. The relief valves are designed to maintain primary system pressure below the emergency stress limit of 1350 psig at all times. ADS is provided to reduce reactor pressure whenever the high pressure makeup systems are unable to maintain reactor water level. This allows the core spray system or the LPCI system to maintain water level. The ADS is used in an intermediate or small break LOCA if the HPCI system fails. The depressurization is accomplished through automatic opening of 6 of the 13 safety relief valves to vent steam to the suppression pool.

Description—BF1 has 13 identical Target Rock two-stage safety relief valves. When operating in the overpressure relief mode, the valves are operated by the self-contained pilot valve. The valves are set as follows:

- Five valves at 1105 psig
- Four valves at 1115 psig
- Four valves at 1125 psig.

At their rated setpoints, the 13 valves provide a total relief capacity of 74% of rated steam flow.

ADS uses 6 of the 13 relief valves. The ADS itself is nothing more than the instrumentation and control required to automatically open the six valves. Each valve relieves approximately 800,000 lb/hr at 1000 psi. ADS activation of a relief valve involves energizing a solenoid, which allows compressed air from the drywell control air system to pressurize a pneumatic actuator which in turn opens the relief valve. The valve will remain open until closed by the operator. All ADS valves are equipped with an accumulator on the air line. A simplified diagram of ADS is shown in Figure 19. Depressurization will occur if three conditions exist:

- Reactor water level at Level 1 (-143 in.)
- High drywell pressure (+2 psig)
- Sufficient LPCI or core spray pumps are operating to ensure that makeup water is available after depressurization.

All relief valves can be manually activated from the control room. This serves as a backup to ADS should depressurization be required and the activation logic fails.

Successful ADS requires that four of the six valves open when required to depressurize the reactor. Successful overpressurization protection depends upon the availability of the bypass valves and the signal causing the reactor scram. If the bypass valves are available, no relief valves are required. If the bypass valves are unavailable, then the number of valves varies as shown below:

- Direct scram 2 of 13
- Flux scram 7 of 13
- Pressure scram 10 of 13.

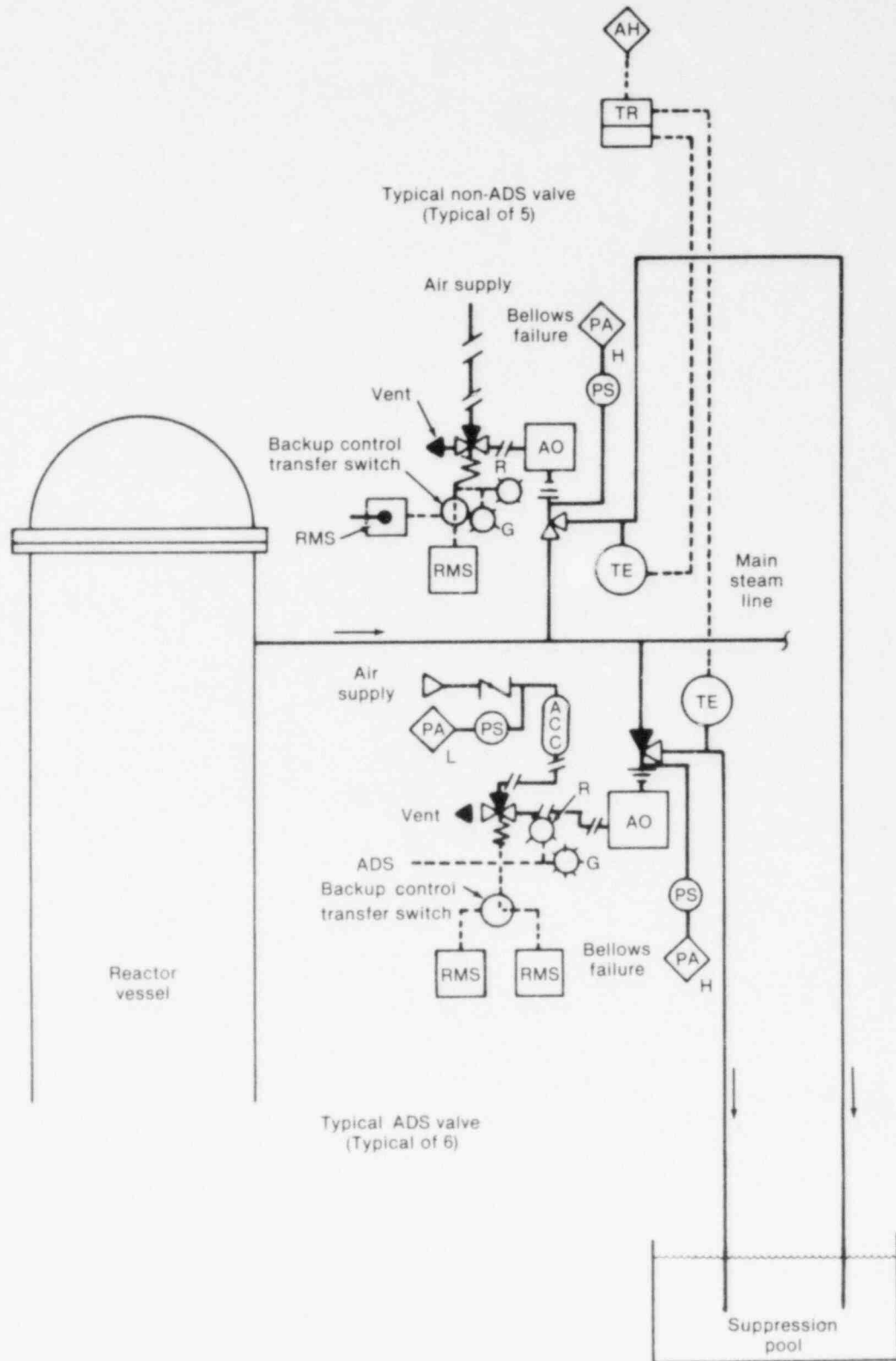
Insights—Since the ADS logic requires both a low level signal and a high drywell pressure signal, ADS will not actuate during transients if HPCI and RCIC fail because no high drywell signal is present. Therefore, the operator must manually depressurize the reactor vessel. Removal of the high drywell signal input would not increase the system unavailability and would allow ADS to automatically function for transients where HPCI and RCIC fail. This would significantly increase depressurization reliability (approximately two orders of magnitude).

6.1.5 Core Spray System. The core spray system along with its control and instrumentation is one of several ECCSs used to inject coolant onto the reactor core following LOCA (pipe break) or a transient. The core spray system is designed to prevent excessive fuel cladding temperature for a pipe break of up to 4.0 ft² by spraying water onto the reactor core.

Description—The core spray system consists of four pumps divided into two parallel systems, which are identical and are physically and electrically independent. Each system contains two AC motor-driven centrifugal pumps, a core spray sparger, and interconnecting pipes and valves.

The pumps in each loop are connected in parallel. Both pumps in a loop must operate since, with only one pump operating in a loop, the core spray system will not deliver the required flow to those fuel assemblies located near the vertical centerline of the core. The arrangement of the core spray system is shown in Figure 20.

The controls and instrumentation for the core spray system include the sensors, relays, wiring, and valve-operating mechanisms used to start, test, and operate the system. Logic control power for each of the core spray loops comes from separate 250 V DC buses. The signals used to initiate the core spray system are:



INEL 2 1487

Figure 19. Automatic depressurization system.

1. Low-low-low reactor water level (470 in.).
2. High drywell pressure (+2 psig) concurrent with low reactor vessel pressure (less than or equal to 450 psig).

These signals seal in and have to be manually reset when the initiating condition has cleared. No operator action is necessary for proper core spray system operation.

Application—The core spray appears on every event tree in one of two modes. One mode requires that both loops deliver rated flow to the spray spargers above the core. The other mode requires only one of the two loops to function.

Assumptions—As with the RHR system, the minimum-flow bypass valves for each loop must shut to ensure that flow is not diverted from the injection path. Failure to close these valves is assumed to fail that loop even though a significant portion of rated flow is not diverted. Likewise, if the LOCA initiator is a break on one of the core spray discharge lines, that loop is considered to be failed.

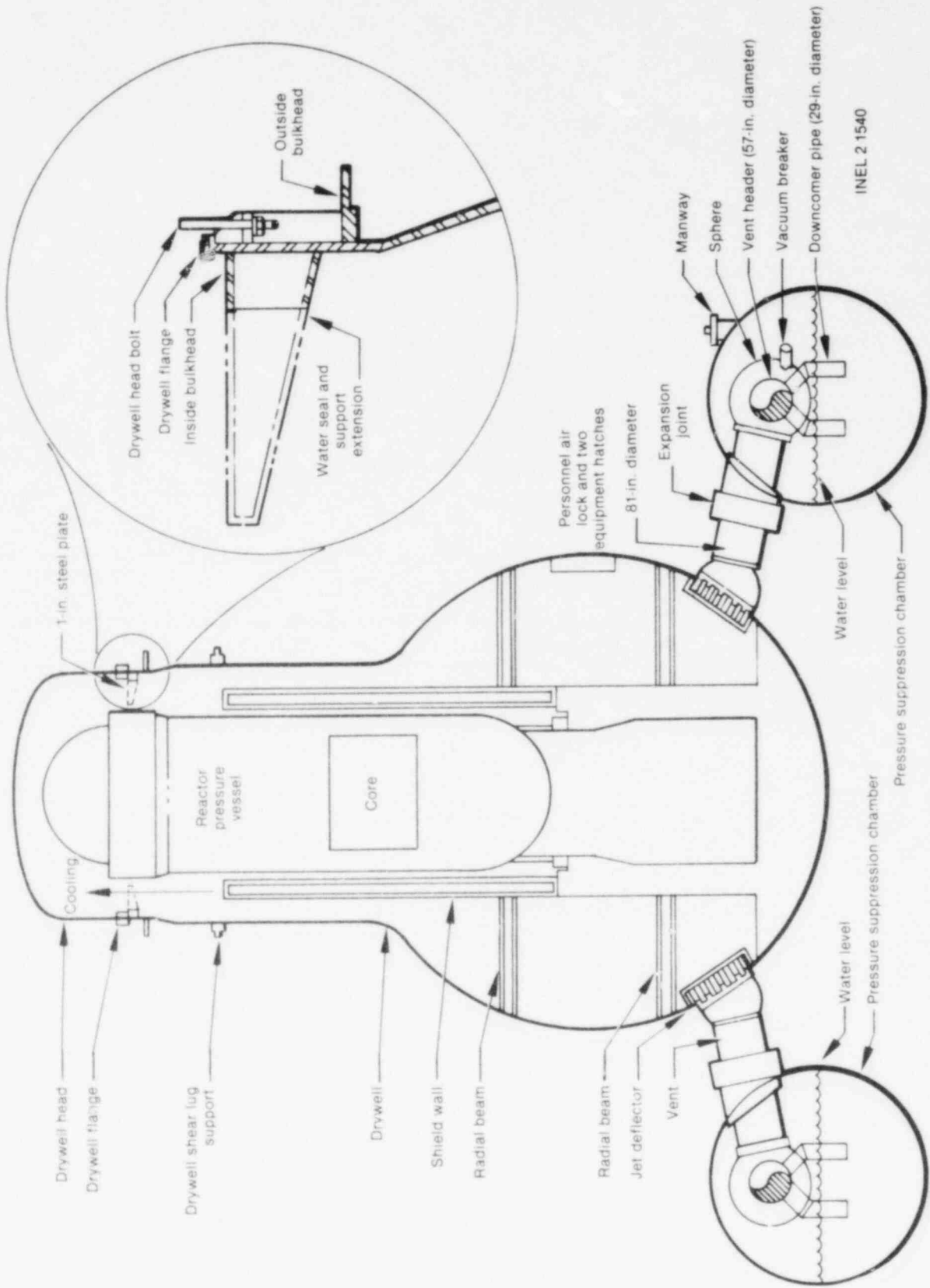
Insights—The design basis for the core spray system is to provide core cooling by spraying water on the fuel elements following a large break. As noted earlier, both pumps in a loop must operate to provide the required spray. However, the core spray system can also provide inventory makeup capabilities during transients. In this case, the spray effect is not the crucial feature but flow rate is. However, the initiation circuitry is set up such that if one pump in a loop does not have power, the other pump is prevented from starting even if it has power available. This appears to be an unnecessary increase in the unavailability of the loop especially when flow rate, not spray effectiveness, is the desired feature.

6.1.6 Vapor Suppression System. The vapor suppression system is designed to direct the LOCA effluents to the pressure suppression chamber to prevent containment overpressurization following a pipe rupture in the drywell. The suppression chamber receives this flow, condensing the steam portion and leaving the noncondensable gases and fission products. The suppression chamber-to-drywell vacuum breakers limit the pressure differential between the drywell and suppression chamber.

Description—Figure 21 represents the basic configuration of the vapor suppression system as part of the primary containment. Large vent pipes form a connection between the drywell and the pressure chamber. A total of eight circular vent pipes are provided, each having a diameter of 6.75 ft. The pressure suppression chamber is a steel pressure vessel in the shape of a torus located below and encircling the drywell. It contains approximately 135,000 ft³ of water as a maximum and has a net air volume above the water pool of approximately 119,000 ft³. The eight drywell vents are connected to a 4-ft, 9-in. diameter vent header in the form of a torus, which is contained within the airspace of the suppression chamber. Projecting downward from the header are 96 downcomer pipes (24-in. diameter) terminating approximately 4 ft below the surface of the water. Vacuum breakers (18-in. diameter) discharge from the suppression chamber into the drywell to equalize the pressure differential and to prevent a backflow of water from the suppression pool into the vent header system. Success criteria for the vapor suppression system is defined as adequate suppression pool level and no bypass leakage from drywell to wetwell.

Application—The vapor suppression system appears on all of the LOCA event trees. Since the system is designed to respond only when there is a breach in the primary coolant boundary into the drywell, it will not be found on the transient trees.

Assumptions—It is conservatively assumed that any of the faults identified (i.e., pipe ruptures or any vacuum breaker failed open) would result in failure of the vapor suppression to perform its function following a LOCA of any size. Faults of wetwell water level being too high, too low, or too hot are assumed to be insignificant contributors to vapor suppression failure due to instrumentation redundancy and frequency of operator observance of this instrumentation.



INEL 2 1540

Figure 21. Vapor suppression part of the primary containment.

6.1.7 Control Rod Drive System. The CRD system is designed to supply and control hydraulic pressure and flow to the CRD mechanisms. Water is supplied to the hydraulic control units (HCUs). Each HCU controls the flow to and from an individual drive. Water that is discharged from the drives during a scram flows through the HCUs to the scram discharge volume. During normal operation rod positioning, this discharge flows through its HCU and exhaust header to the reactor vessel.

Description—A simplified schematic of the CRD hydraulic system is shown as Figure 22. This figure shows one of the 185 HCUs and scram valve arrangements, which is typical of all the units. During a reactor scram, the scram inlet valves and scram discharge valves open, allowing water from the CRD hydraulic system to flow into the drives, thereby inserting the control rods. Operation of the scram inlet valves and the scram discharge valves is controlled by the scram pilot valves. The pilot valves are operated by signals received from the RPS. Two scram pilot valves for each HCU control both the scram inlet valve and scram discharge valve for that HCU. The scram inlet and discharge valves are designed to open on loss of air pressure. The pilot valves are normally energized and are aligned to provide air pressure to the scram inlet and discharge valves, thus keeping them closed. Upon loss of electrical signal, the pilot valve inlet ports are closed and the exhaust ports are opened, which depressurizes the scram inlet and discharge valves. This opens the valves, inserts the rods, and trips the reactor. The scram accumulators store sufficient energy to insert a rod during scram independently of any other energy source. Each accumulator is a water volume stored under nitrogen pressure.

The scram discharge volume, which is provided by the instrument volume and the scram discharge headers, is designed to contain water from all the drives during a scram. During normal plant operation, the volume is empty with both its drain valve and its two vent valves open. These valves close upon receipt of a scram signal. During a scram, the scram discharge volume is partly filled with water, which is discharged from above the drive pistons. An isometric view of the scram discharge volume equipment is included as Figure 23.

The success criteria for the CRD system requires that no more than 30 distributed or 5 adjacent rods fail to insert. The 30 rods are considered conservative for maintaining the reactor subcritical. The 5 rods are to prevent a localized criticality.

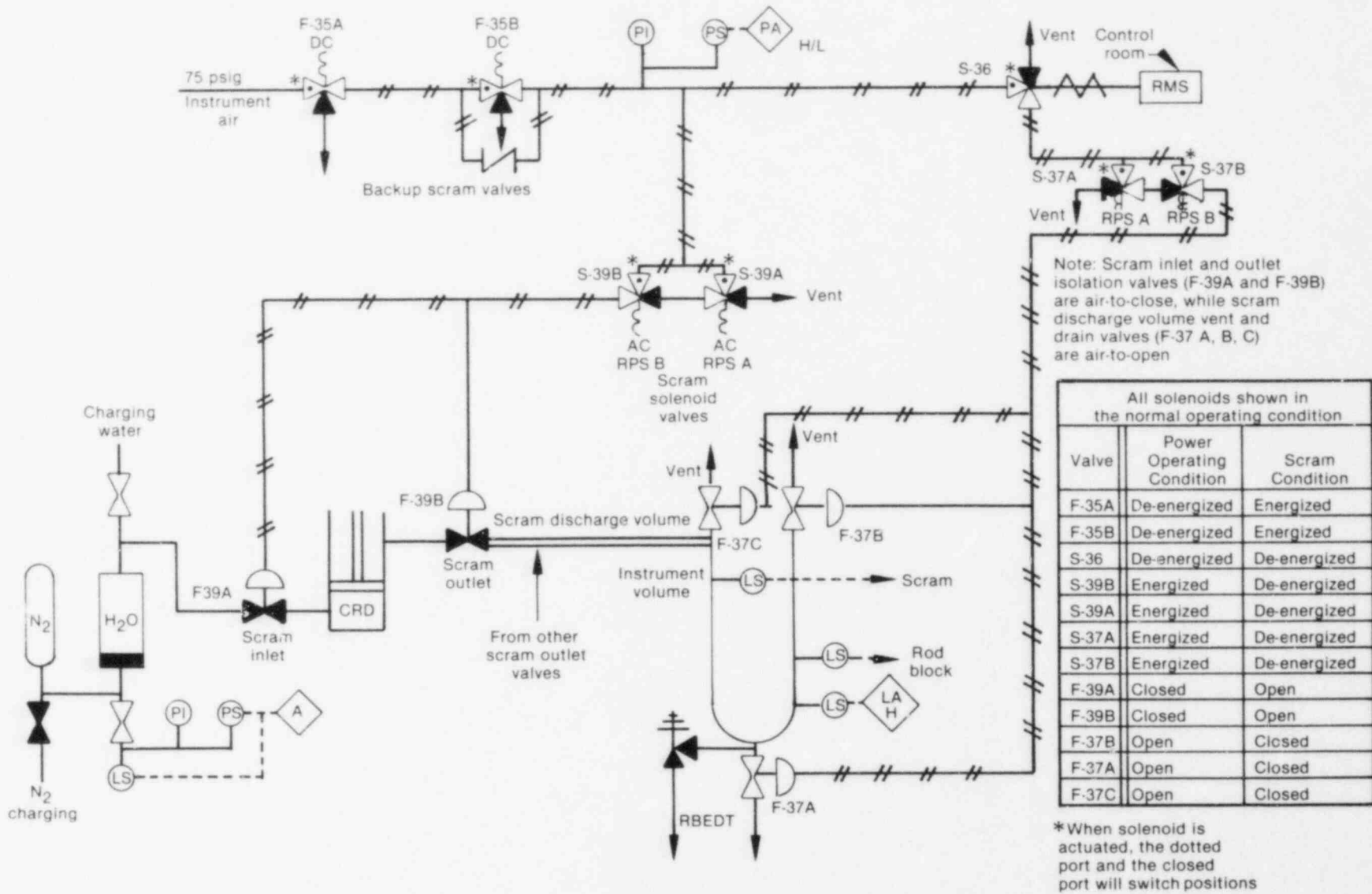
Applications—The CRD system appears on every event tree. The system is required for reactor subcriticality in the event of a LOCA or transient.

Assumptions—As noted previously in Section 6, the unavailability for the CRD system for this analysis was taken from NUREG-0460. The complexity of determining “how many rods in what patterns fail to insert by how much and by what means” was considered beyond the scope of this analysis.

6.1.8 Power Conversion System. The PCS provides a means of bringing the reactor to a stable shut-down condition following a transient event that does not preclude PCS availability. The PCS can provide both the VWI and DHR functions by removing steam from the reactor, condensing the steam, and returning the water to the reactor via the condensate and feedwater systems. Successful PCS operation requires that the condenser is available and the feed system is providing makeup water to the reactor vessel.

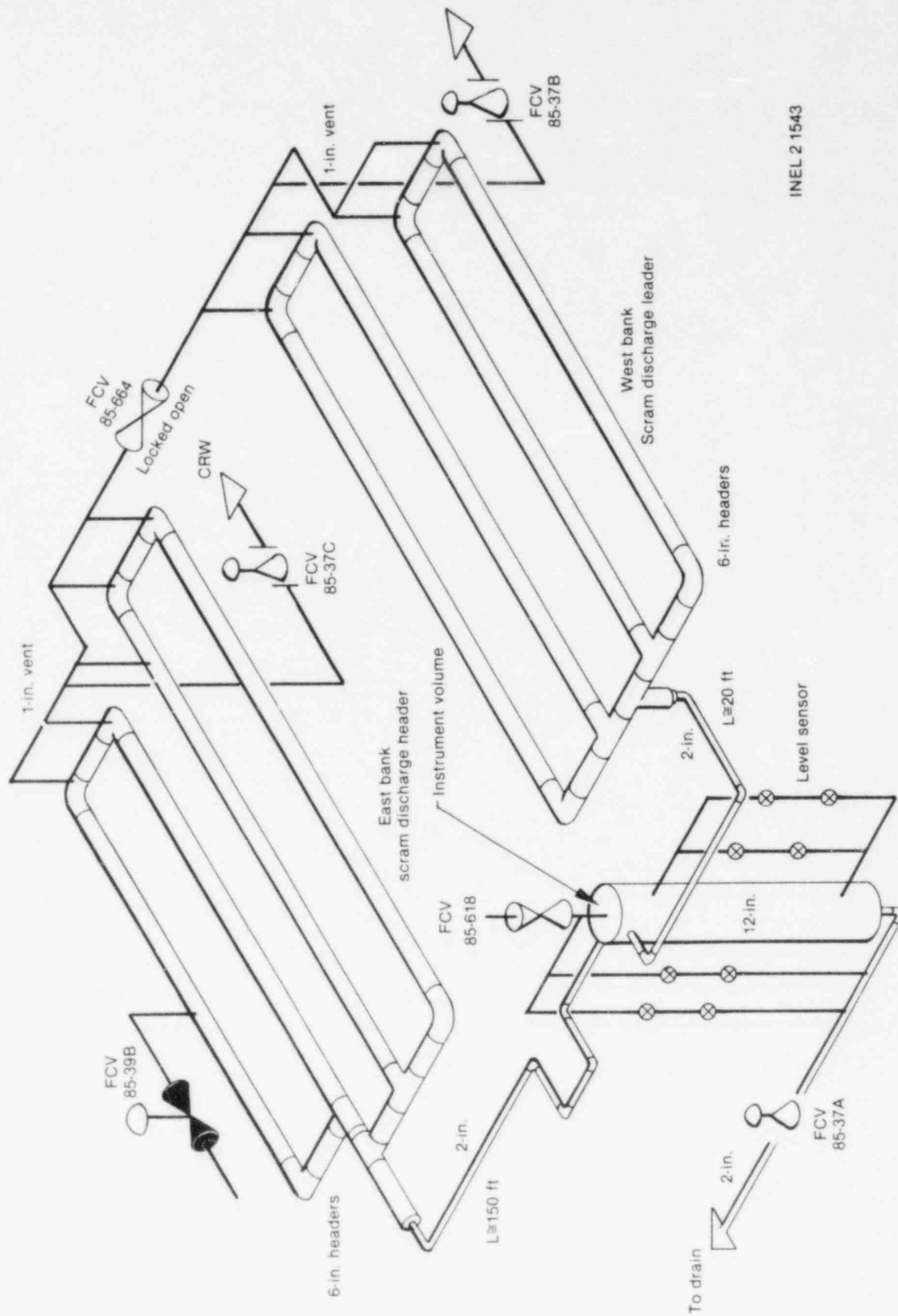
Description—The PCS consists primarily of the main steam, condensate, and feedwater systems. Simplified flow diagrams for these systems are provided by Figures 24 and 25.

During normal operation, steam from the reactor flows directly to the main turbine generator via the main steam lines. Condensed extraction steam is cascaded through the feedwater heaters to the main condenser where it is deaerated and collected in the condenser hotwell along with condensed steam from the turbine exhaust and miscellaneous drains from the turbine cycle. Condensate pumps, taking suction from the hotwell, pump the condensate through the air ejector condensers, gland exhaust condensers, and filter/demineralizers to the condensate booster pumps, which increase the condensate pressure and discharge through the low-pressure heaters to the reactor feed pump suctions. The reactor feed pumps discharge through the high-pressure heaters to the reactor.



INEL 2 1542

Figure 22. CRDH system.



INEL 2 1543

Figure 23. Scram discharge volume equipment.

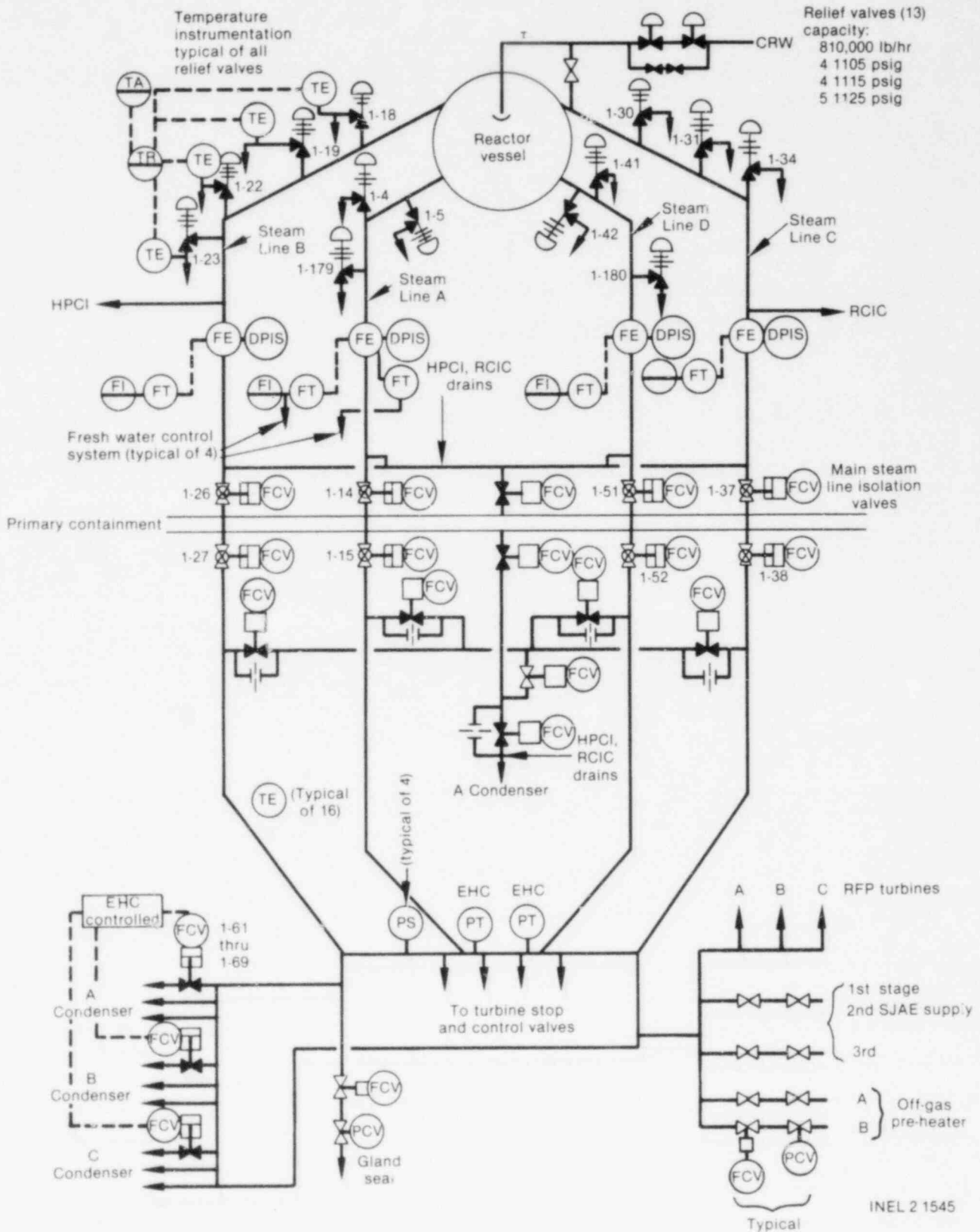


Figure 24. Main steam system.

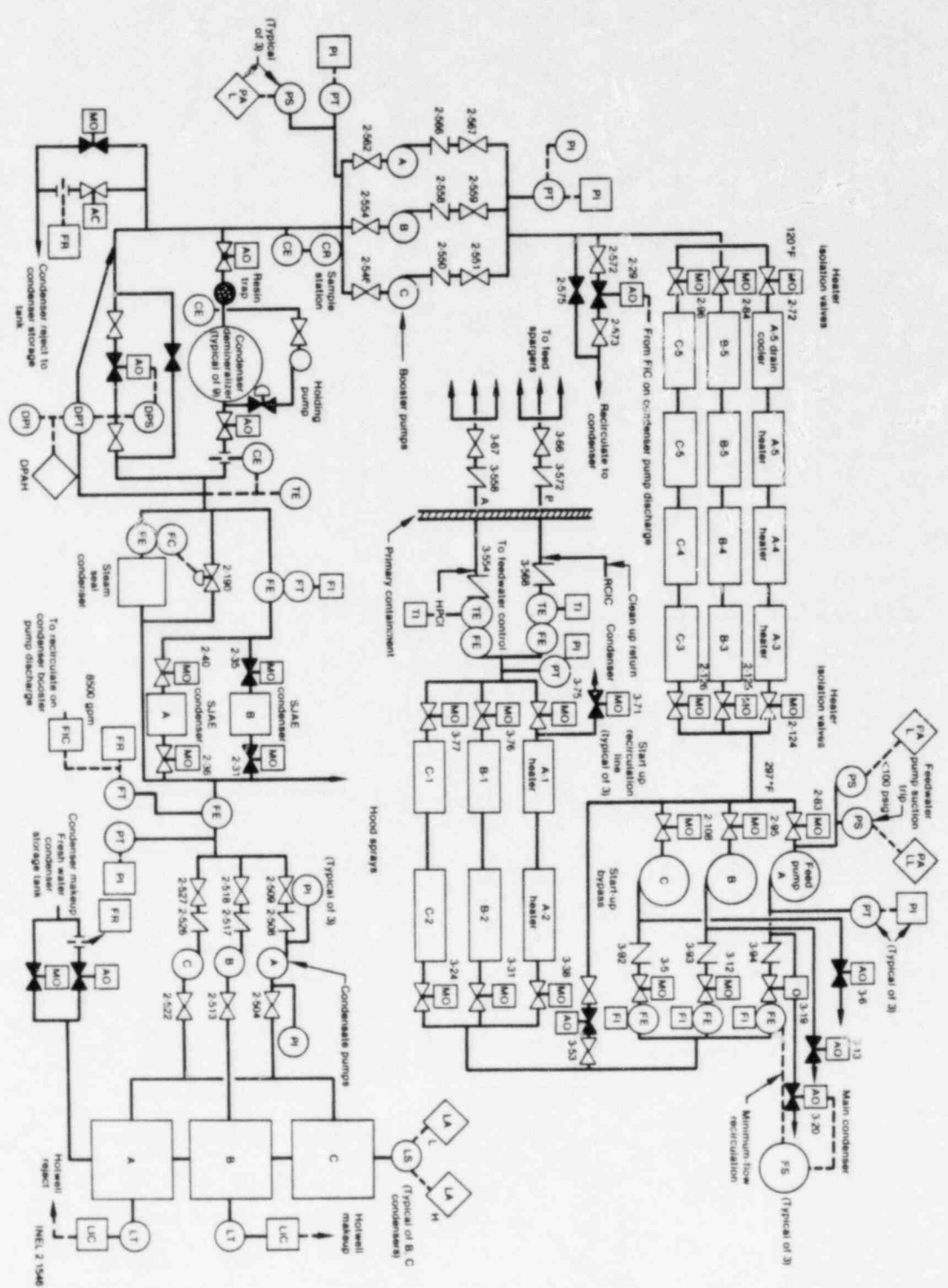


Figure 25. Condensate and feedwater system.

Under abnormal conditions requiring an emergency shutdown from power, the following action occurs if the PCS is not rendered unavailable by the initiating event. The main turbine is tripped, and is isolated from the main steam system by the turbine stop valves and turbine control valves. There are nine turbine bypass valves that open to take steam from ahead of the turbine stop valves and discharge to the condenser. The bypass valves are sized to pass up to 30% of maximum turbine design flow. The condensed steam drops to the lower section of the condenser, called the condenser hotwell. The operator manually trips all but one of the operating condensate pumps taking suction from the condenser hotwell. The condensate discharge passes through filter/demineralizers to the suction header for the condensate booster pumps. The operator manually trips all but one of the operating condensate booster pumps. The remaining condensate booster pump discharges through a series of heaters to raise the condensate water temperature.

The feedwater system is actually an extension of the condensate system, which (a) receives water from the condensate system at booster pump discharge pressure, (b) increases the pressure via a steam-driven reactor feed pump, and (c) feeds the reactor through the high pressure heaters, which further raise the temperature of the feedwater. The feedwater flow is combined into a 30-in. mixing header and then is divided into two 24-in. lines to feed the reactor through the feed sparger rings. The operator trips all but one of the operating reactor feedwater pumps.

Application—The PCS appears only on the event tree for transients where PCS is available. The PCS acts as a heat sink for reactor decay heat following a transient where reactor subcriticality is achieved. If subcriticality is not achieved but the recirculation pumps are tripped, the PCS has adequate heat removal capacity to remove the heat being generated at the resulting reactor power level.

Assumptions—As noted previously in Section 6, the unavailability for PCS used in this analysis was based on experience data from U.S. power reactor operating plants.

6.1.9 Standby Coolant Supply System. The SBCS system is a special mode of alignment of the RHRSW system to the RHR system to provide a standby source of coolant to the reactor. The D supply header of the RHRSW system contains piping and valves that cross-connect the RHRSW system with the RHR system. The purpose of this cross-tie is to inject RHRSW into the reactor vessel or containment, via the RHR piping, for final flooding if all other sources of coolant are expended. This mode of coolant injection to the reactor is included in the description of the RHRSW system (Section 6.2.2).

6.1.10 Recirculation Pump Trip System. During abnormal conditions that lead to sharp increases in reactor system pressure, the RPT system ensures a rapid trip of the recirculation pumps. This action reduces the flow through the core allowing for more void formation and a corresponding reduction in reactor power.

Description—The RPT system consists of the control circuits for the recirculation pump motor generator breakers and portions of the RPS that actuate the trip. The 250 V DC system provides power to the RPT control circuitry. The circuit requires power to function. Figure 26 is a simplified diagram of a RPT circuit.

Application—The RPT function only appears on the transient event tree where PCS is available. For the case where the reactor subcriticality systems fail to shut down the reactor, successful RPT ensures that the resulting reactor power level is within the capacity of the PCS to remove the heat and maintain reactor coolant inventory. Failure of the RPT would allow power levels to remain too high for the PCS to accomplish these tasks and a core melt would eventually occur.

6.1.11 Main Steam Isolation System. The purpose of the main steam isolation (MSI) system is to isolate the reactor from the main condenser when the PCS is unavailable to maintain reactor water level.

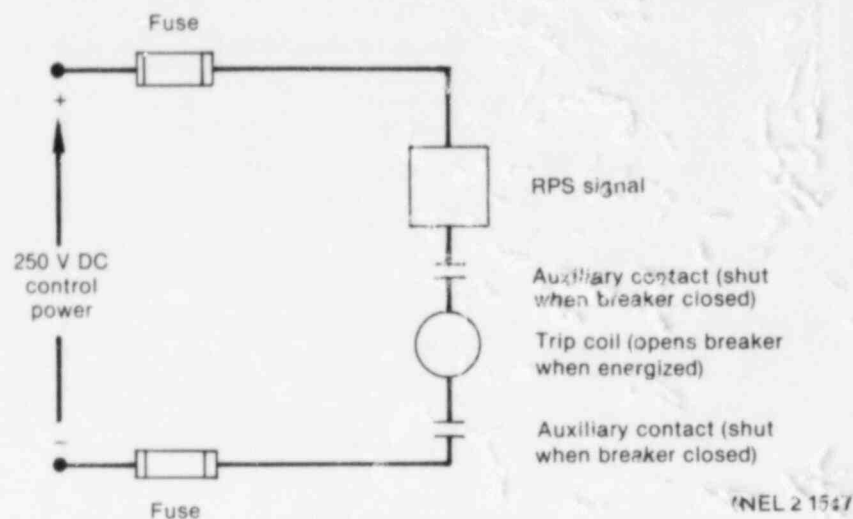


Figure 26. RPT circuit.

Description—There are eight MSIVs, two in each of the four main steam lines leading to the common manifold in the turbine building. From the common manifold, there are four lines leading to the main turbine, each having a turbine stop valve and turbine control valve. There are three bypass valves, arranged in parallel, that can dump steam directly to the main condenser. Figure 16 presented a simplified drawing of the main steam system.

The MSIVs are closed automatically if the reactor water level reaches the low level setpoint. The valves are air-operated to open and spring loaded to shut upon loss of air to the valves. The low level initiation circuitry deenergizes an AC and DC solenoid valve, which causes the air supply to the valve to rapidly bleed off. This action causes the valves to close. The valves may also be closed from the control room by the operator.

The turbine stop valves, control valves, and bypass valves receive their control signals from the pressure regulator via the electro-hydraulic control system. Under normal conditions these valves open and close to maintain a constant pressure at the common manifold. Following a scram, the turbine stop valves and control valves receive signals to shut, while the bypass valves open as necessary to maintain the pressure at the common manifold below a preset pressure. As long as pressure in the manifold remains below this value, the bypass valves will remain shut. The operator may manually open or shut the bypass valves from the control room.

MSI failure is defined as the inability to isolate the reactor from the main condenser when reactor water level is low. This will occur if any two MSIVs in the same steam line fail to close and the turbine stop, control, and bypass valves fail to close.

Application—The MSI function appears on the transient event trees. It is necessary to isolate the reactor whenever the PCS is unavailable in order for the other mitigating systems to be able to function properly.

Assumptions—In quantifying the MSI fault tree, no credit was taken for operation of the turbine stop, control, or bypass valves. These valves are controlled by the pressure regulator and the electro-hydraulic control system. Neither of these systems were modeled in this analysis. Instead, it is conservatively assumed that the added redundancy of these valves provides no additional isolation protection.

6.2 Support Systems Description

This section provides an overall description of the support systems. The systems and fault trees appear in more detail in Appendix B of this report.

6.2.1 Electrical Power System. The Browns Ferry electric distribution system is a complex arrangement of switches, transformers, generators, batteries, and other devices needed to provide power to the various pumps, valves, and control circuits. In general, the system consists of two parts: an AC and DC distribution system (Figure 27). The AC system consists of two parts, those buses powered only by offsite power and those buses powered by either offsite power or emergency onsite diesel generators.

Description—The AC system consists of a distribution system powered by offsite power and a distribution system powered by either offsite power or emergency onsite diesel generators. Figure 27 shows those AC system buses directly associated with Unit 1 that receive power from offsite power or the diesel generators. Breakers shown in solid black (filled in) are normally closed.

Each 4160 V shutdown board has two offsite power supplies. Automatic transfer from one to the other offsite supply occurs if one is lost. If both offsite sources are lost, the diesel generator for that bus receives an automatic start signal. When the diesel is successfully started, the output breaker will automatically close to supply power to the shutdown board if there is no offsite supply. Supplying a shutdown board from its corresponding Unit 3 shutdown board (and vice versa) is a manual operation.

The 480 V shutdown boards each receive power from a normal and alternate transformer powered by the 4160 V shutdown boards. Transfer from one power source to the other is a manual operation.

Each 480 V RMOV (reactor motor-operated valve) board has two power sources. RMOV Boards 1D and 1E have AC-to-DC motor generators providing power from the 480 V shutdown boards. RMOV Boards 1D and 1E automatically transfer from one power supply to the other on undervoltage. Transfers for RMOV Boards 1A, 1B, and 1C are manual operations.

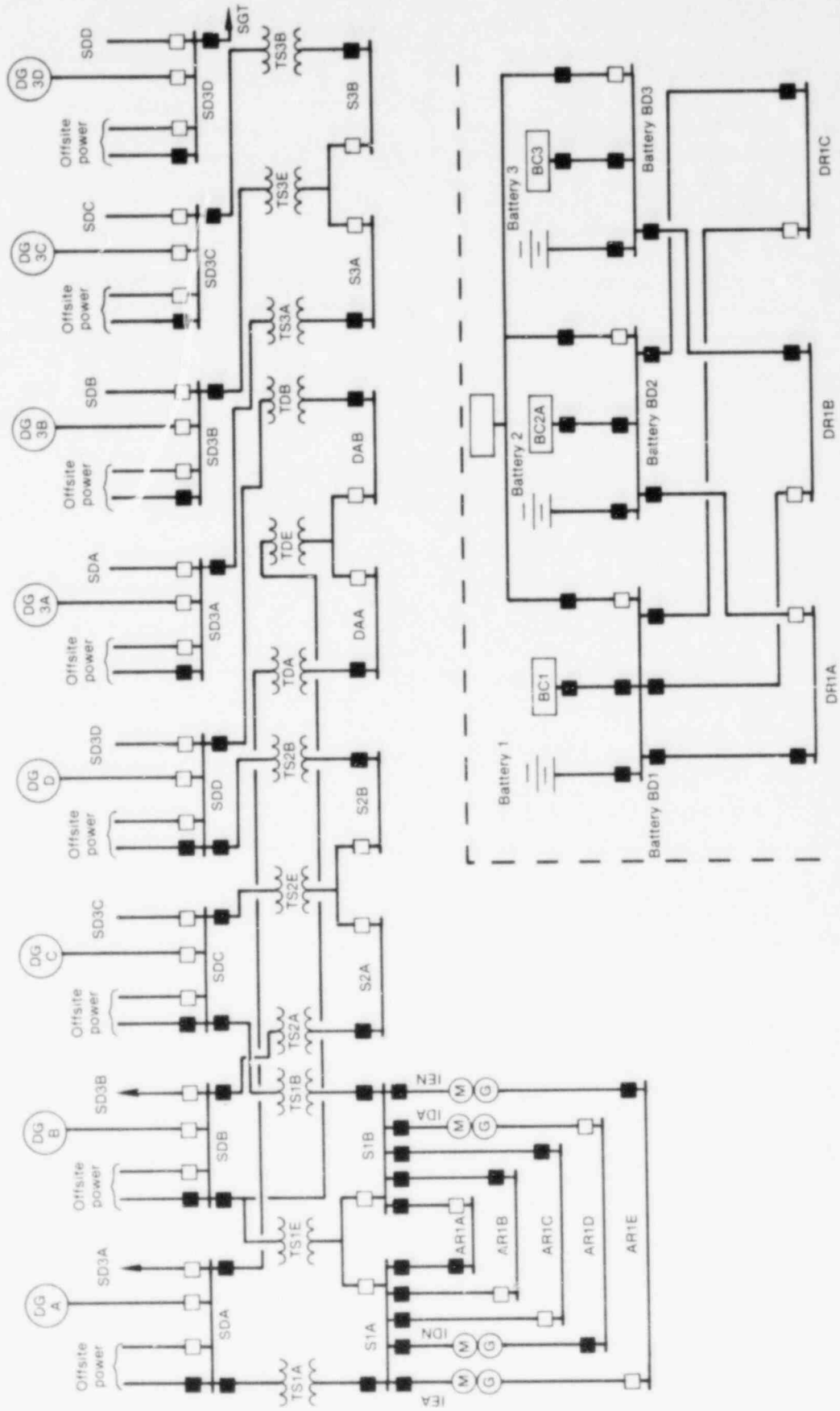
There are four DC systems at Browns Ferry. The 48 and 24 V DC systems do not directly supply any of the loads necessary for accident or transient mitigation. Figure 27 also shows the 250 V DC system as it applies to accident and transient mitigation loads. Breakers shown in solid black (filled in) are normally closed. Each battery board is supplied by a battery and a normal and alternate battery charger. The alternate charger for each board is shared by all three battery boards. Each battery charger has two sources of AC power. Each DC RMOV board receives power from one of two of the battery boards. All transfers of power supplies in this system are manual operations. The 125 V DC system consists of the batteries and chargers associated with starting and controlling the diesel generators. Each diesel has its own 125 V DC system, which is independent of the other diesels' 125 V DC system.

Application—A fault tree exists for each interface between the EPS and a front-line system. Thus, there are many EPS fault trees. Every system except vapor suppression and overpressure protection (relief valves) has an EPS interface.

Assumptions—EPS buses powered only by offsite power were not modeled. Instead the house event HOUSELOP was used to describe the unavailability for these buses. Thus, when HOUSELOP is "on" that bus fails. Otherwise, the value for frequency of loss of offsite power (LOSP) was used for those bus unavailabilities, which, represents the dominant contributor to bus failure.

Normally open or closed breakers not required to change state do not appear in the fault trees.

Since each diesel generator's support systems are unique to that diesel except for EECW cooling, the support systems are not explicitly shown except for the EECW cooling. This includes starting air, lube oil, fuel oil, and others.



INEL 2 1552

Figure 27. EPS diagram showing AC and DC systems.

6.2.2 Residual Heat Removal Service Water System. The primary purpose of the RHRSW system is to provide an assured heat sink for long-term heat removal when the normal means of heat removal through the main condensers is not available or cannot be used. A second purpose of the RHRSW system is to provide an assured supply of water for the EECW system. This system supplies cooling water for various auxiliary systems and for items of equipment that support shutdown operations. The EECW system is discussed in a separate section of this report. Finally, the RHRSW system-to-RHR system cross-connection provides added long-term redundancy to other emergency core cooling and containment cooling methods.

Description—The RHRSW system, as considered in this analysis, consists of eight service water pumps, four service water headers, four service water heat exchangers and the associated piping, valves, controls, and instrumentation. Figure 28 is a simplified composite diagram of the system. Since the system consists of four nearly symmetric trains, a composite diagram more simply illustrates the system. Figure 29 shows the electrical power dependencies for this system. There are eight service water pumps associated with the RHRSW system. Four pairs of pumps are connected to the four RHRSW headers. Each pair is designed to supply only one header according to the following configuration:

<u>Pump Pair</u>	<u>Header</u>
A1, A2	A
B1, B2	B
C1, C2	C
D1, D2	D

As Figure 29 shows, each pump pair supplies only one supply header and, in turn, each supply header supplies only one Unit 1 RHR heat exchanger. Each service water pump has the capacity to supply 100% of the cooling water required by one RHR heat exchanger. No cross-connections exist between the service water supply headers but there is a cross-connection to the EECW system on each train. Control of the RHRSW system is entirely manual.

The D supply header contains piping and valves that cross-connect the RHRSW system with the RHR system. Although it is only used as a last resort, this cross-connection provides a method of injecting river water directly into the reactor vessel or primary containment via the RHRSW system and the RHR piping. In the highly unlikely event that all other sources of injection water were unavailable, this source could be used to keep the reactor core covered and the containment cooled. When the RHRSW system is cross-connected to the RHR system in this manner the resulting configuration is referred to as the SBCS. Control of SBCS is also manual.

Application—Since the RHRSW system provides cooling to the shutdown cooling and torus cooling modes of the RHR system, it contributes to every event tree through its effect on RHR unavailability. The SBCS mode appears only on the transient trees.

Assumptions—The four RHRSW pumps dedicated to the EECW headers are considered unavailable for use in the RHRSW cooling system. Since three of four EECW pumps are required when that system operates, it is likely that no spare pump will be available anyway.

Insights—The procedure for establishing SBCS flow to the reactor requires operation of RHRSW and RHR system valves such that the cross-connect valves are opened before the RHRSW heat exchanger discharge valve is shut. This allows a flow path from either the reactor or torus (depending on the RHR mode line up) directly to the river until the operator closes the heat exchanger discharge valve. Operator failure to close the valve or valve failure would allow the torus (or reactor water) to drain to the river. Since after a LOCA or transient this water may be contaminated, the consequences of such a discharge could be serious. Installing a check valve in the cross-connect line and changing the procedure to require shutting the heat exchanger discharge valve first would reduce the likelihood of this sequence.

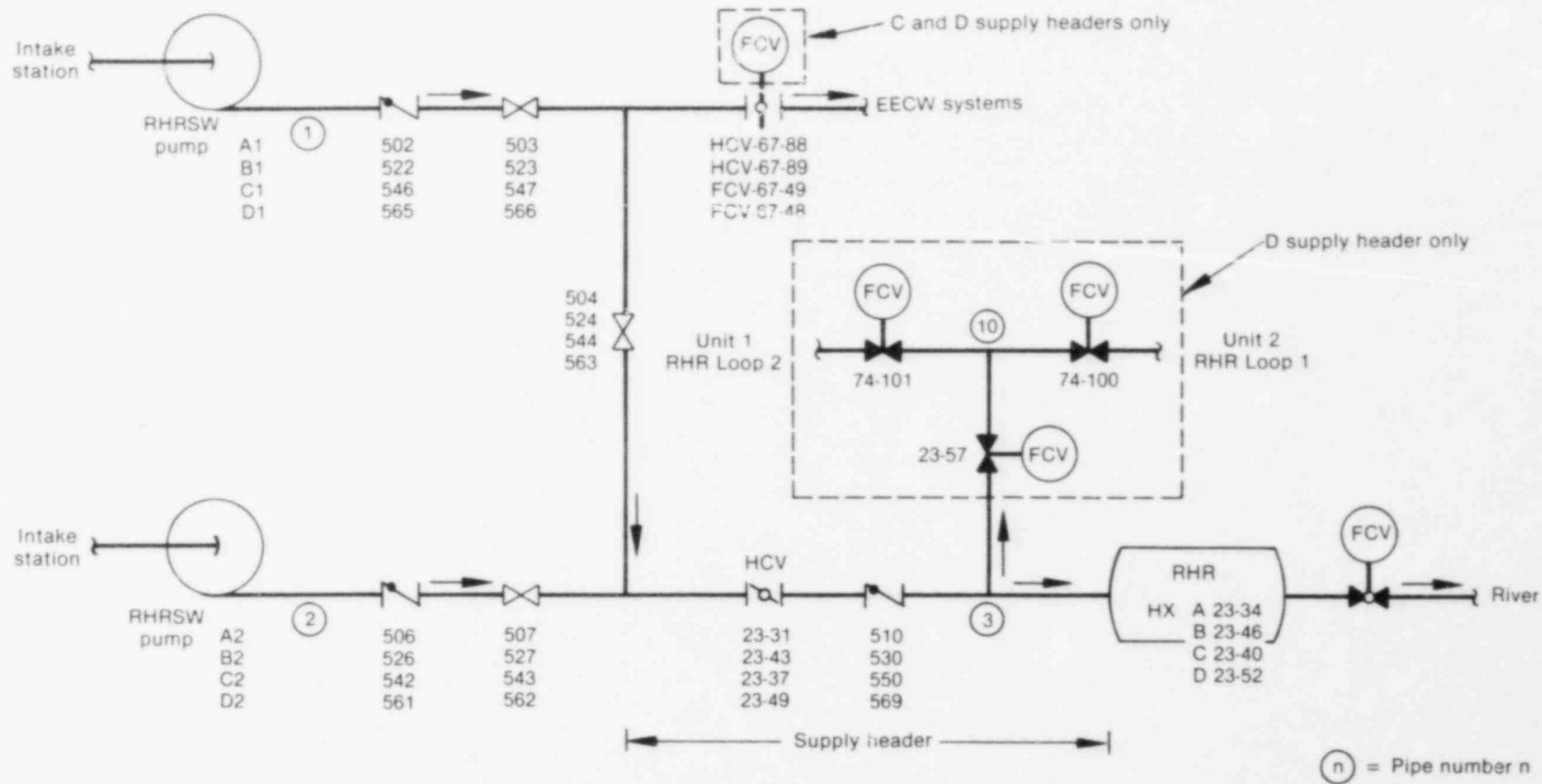


Figure 28. RHRSW system.

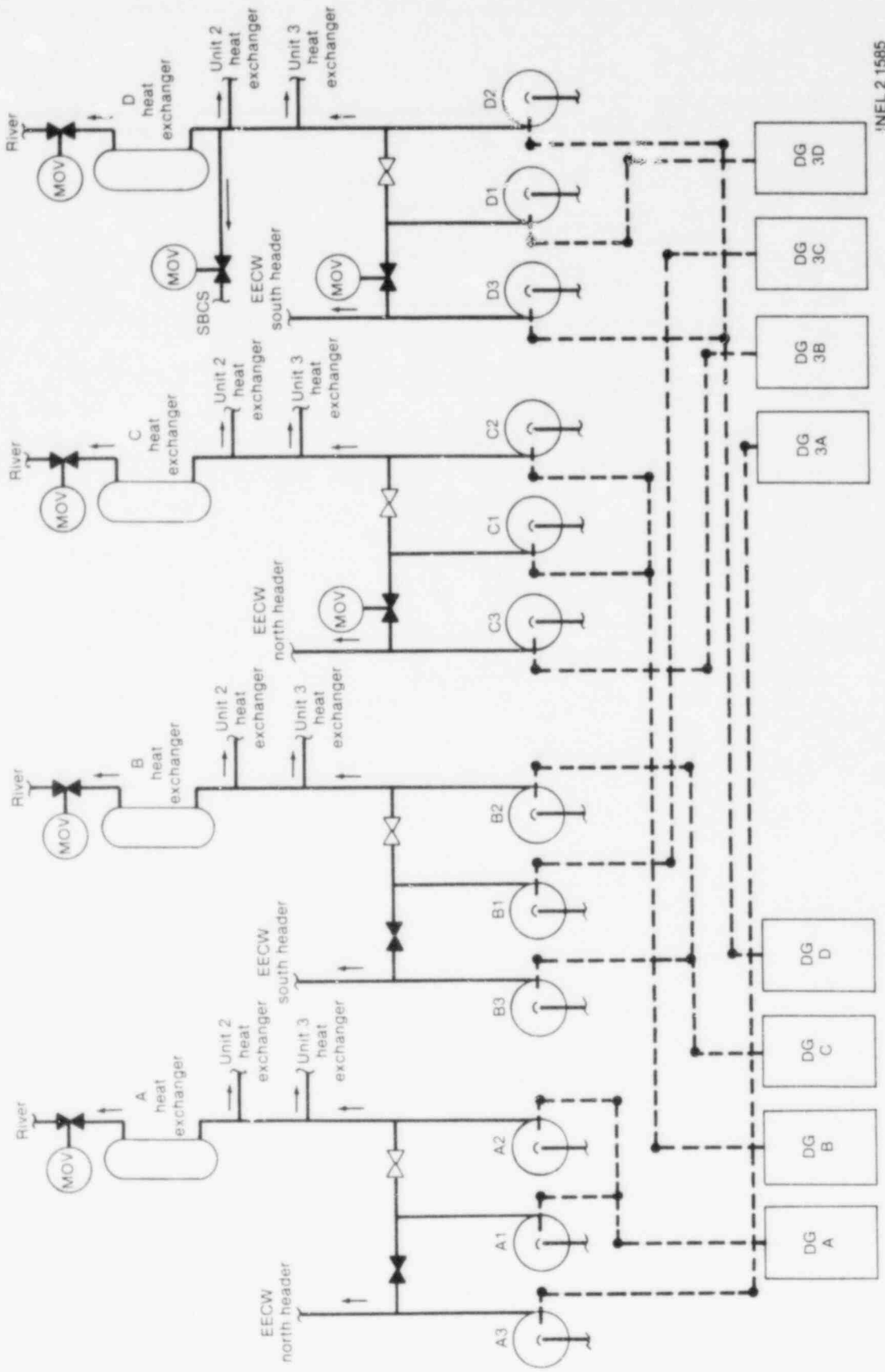


Figure 29. RHRSW/EECW system power dependencies.

6.2.3 Emergency Equipment Cooling Water System. The purpose of the EECW system is to supply cooling water to safety-related components in the core spray, RHR, and diesel generator systems. The EECW system performs this function by supplying water from the intake station to heat exchangers in the previously mentioned safety systems. This cooling water then flows through the heat exchangers and discharges back to Wheeler Reservoir through yard drainage.

Description—A simplified diagram of the EECW system is provided by Figure 30. The EECW system is a Class 1 safety-related system that serves all three of the Browns Ferry nuclear units. Either of two independent piping headers (north and south headers) can supply the safety-related cooling loads. The EECW system uses 4 of the 12 RHRSW pumps to supply the two EECW headers (two pumps per header) according to the following configuration:

<u>Header</u>	<u>Pump Pair</u>
North	A3, C3
South	B3, D3

The remaining eight pumps serve the RHRSW system. Four of these eight pumps may be valved into the EECW system if needed; however, the RHRSW is considered to be a separate support system and is treated independently from the EECW system in Section 6.2.2.

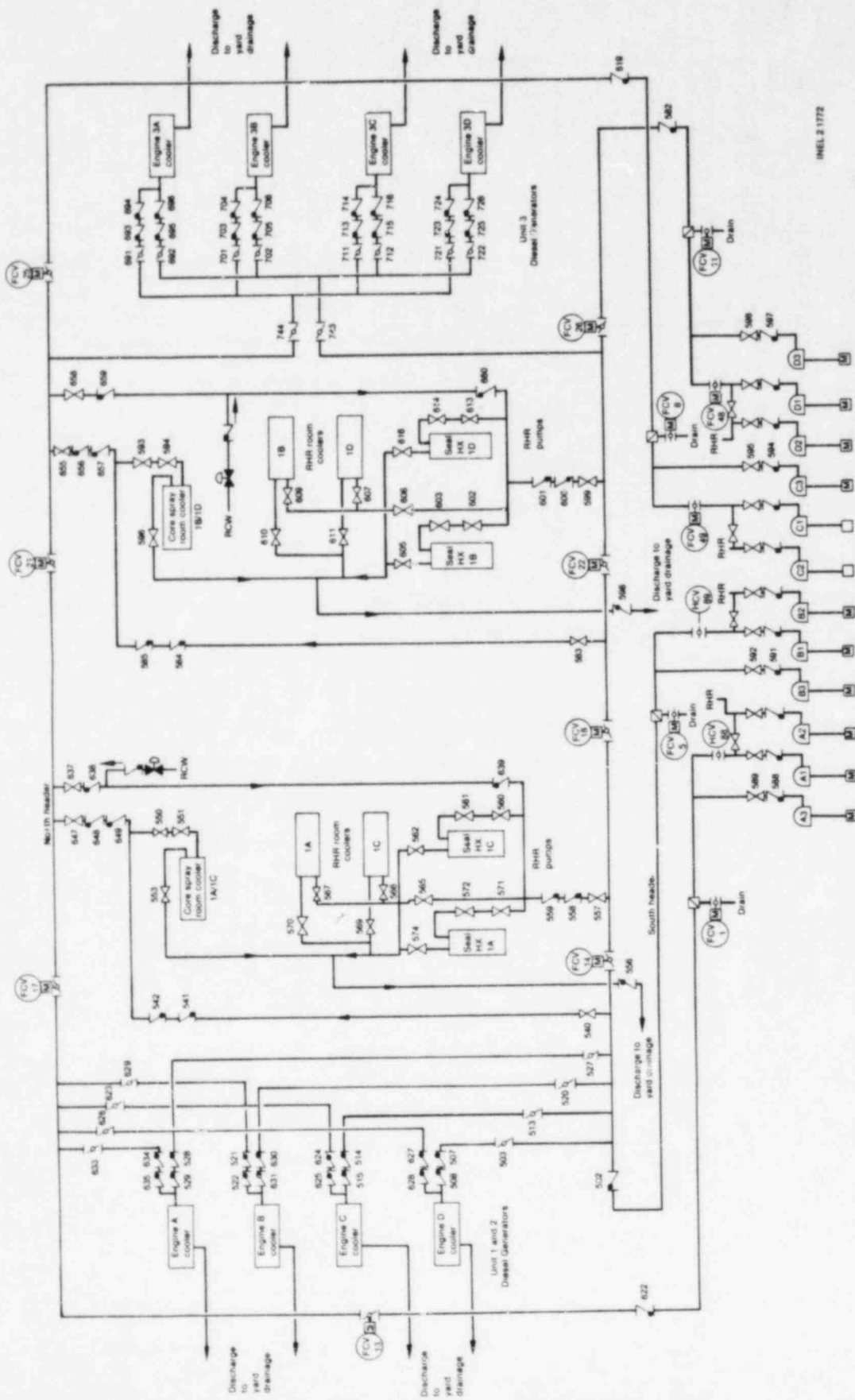
Under worst-case conditions such as exist following a LOSP transient, maximum design flow rates are required at all three units resulting in total station flow requirement of 9900 gpm. Since each pump is designed to deliver approximately 4500 gpm, three of four pumps assigned to EECW are necessary to supply the EECW system design requirements.

The EECW system is normally in standby readiness with the A3, B3, C3, and D3 RHRSW pumps aligned to EECW service. The RHRSW pumps aligned to EECW will automatically start on:

1. Low RCW header pressure.
2. Any time a diesel generator or core spray pump is started:
 - a. The two RHRSW pumps (B3 and D3) aligned to EECW and powered from shutdown boards in Units 1 and 2 will start automatically in less than 30 sec after starting of a diesel generator or core spray pump in Unit 1 or 2.
 - b. The two RHRSW pumps (A3 and C3) aligned to EECW and powered from shutdown boards in Unit 3 will start automatically in less than 30 sec after starting of a diesel generator or core spray pump in Unit 3.
3. ECCS initiation signals of high drywell pressure (+2 psig) or low-low reactor vessel water level (-143.5 in.) in any unit (part of the core spray initiation logic).

Application—The EECW system contributes to every event tree through its contribution to RHR system seal coolers and room coolers necessary for shutdown cooling or torus cooling. When offsite power is available, this contribution is small since the raw cooling water system is normally used to supply these loads. Under LOSP conditions, raw cooling water is unavailable and the EECW system failure contributes not only to RHR failure but also to every AC powered system through its contribution to the loss of diesel generator engine cooling.

Insights—Under LOSP conditions, the EECW system becomes a major contributor to core melt frequencies due to its effect on the unavailability of diesel generators and, therefore, all AC power. The EECW system in this case represents a common mode failure mechanism for AC power since all eight diesel generators receive cooling from EECW. Several steps could be taken to mitigate its effects. Sectionalizing



INEL 2 1772

Figure 30. EECW system.

the headers would allow the operators to keep some generators running if EECW flow was degraded instead of the "all or none" situation. Aligning more RHRSW pumps to the EECW mode would also help. It seems reasonable that the EECW system which requires automatic starting and running should have more pumps dedicated to its headers than the manually initiated RHRSW headers which would normally be operated later in the transient or LOCA sequence. This is especially true since the success criteria for the EECW system are much more restrictive in required equipment and time available to recover from failure than for the RHRSW system.

6.2.4 Keep-Full System. The function of the keep-full system is to keep full of water the core spray system Loops 1 and 2 and the RHR system Loops 1 and 2. The critical section of piping in both systems (i.e., the piping that must remain full of water) is the section from the core spray/RHR pumps discharge check valves to the normally closed core spray/RHR injection valves. Keeping this section of piping full of water will ensure that no piping damage will result from water hammer upon core spray or RHR system initiation.

Description—The keep-full system consists of two pumps, a head tank, and various valves and piping. Figure 31 is a simplified diagram of the keep-full system. The head tank pumps water from the torus via the core spray pump suction line and maintains head tank water level while pressurizing the system to greater than 48 psig. The pumps automatically cycle on high and low head tank levels. The system head tank has a capacity of 3090 gallons. When the system pumps are not running, the water level in the head tank maintains a static head of greater than 48 psig on the system by virtue of head tank elevation above the system. This ensures that the associated core spray and RHR system piping is full and pressurized at all times that the keep-full system valves are aligned to supply water to the associated core spray and RHR loops.

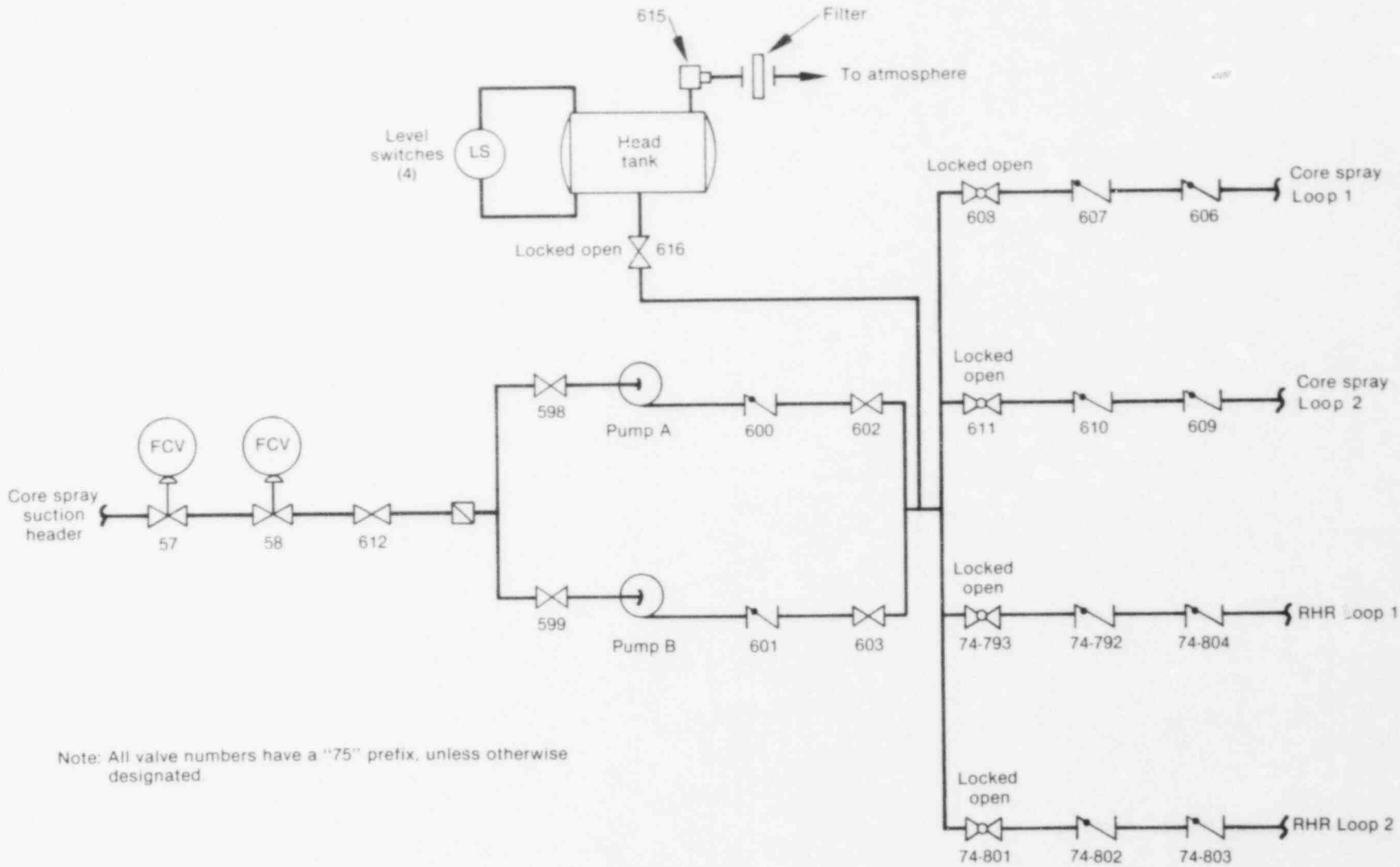
Application—The keep-full system will be required to operate if gross leakage develops in the core spray/RHR loops: (a) as a result of component rupture or operator error, or (b) if an operator intentionally drains a loop, in which case the associated keep-full system supply line should be isolated. In the former case, the rupture or operator error causes loop failure regardless of the status of the keep-full system. In order to intentionally drain a loop, the operator must violate a number of procedures and ignore several indications and alarms in order to cause failure of the keep-full system. This operator action is incorporated in the test and maintenance contribution to the failure rates of the core spray and RHR systems. Since faults in the keep-full system will not disable the RHR or core spray system unless a fault in the RHR or core spray systems has already disabled them, it is unnecessary to model keep-full system faults.

6.2.5 Condenser Circulating Water System. The condenser circulating water (CCW) system is designed to provide an efficient means of rejecting waste heat by providing flow to the condensers that condense steam formed during the power generation cycle or following plant shutdown.

Description—The CCW system is designed to provide a flow of 630,000 gpm to the condenser during open cycle operation and 30,000 gpm to the auxiliaries of each unit. The system consists of three pumps per unit, each with a capacity of 220,000 gpm at a design head pressure of 32.5 ft. The full power requirements of each generating unit are satisfied by that unit's respective group of three CCW pumps. A simplified diagram of the CCW system is shown in Figure 32.

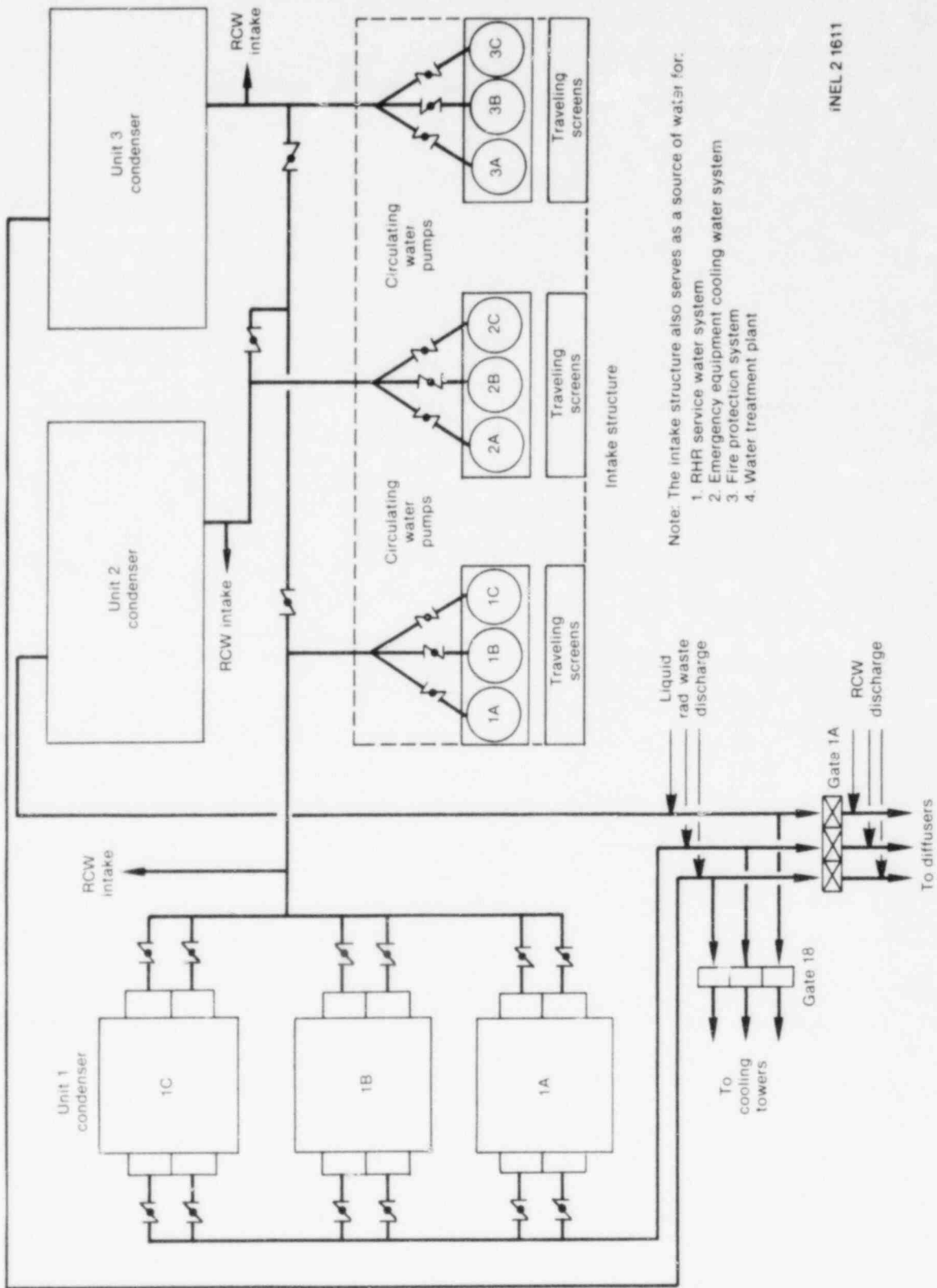
Each of the three pump discharge lines are equipped with a 96-in. diameter motor operated butterfly valve. The three discharge lines are brought together into a single culvert, whose cross section varies throughout its length from an 18.5 ft in diameter circle to a 14.5 ft square. The CCW is carried to the condenser via this culvert. The condenser discharge passes to the discharge culvert and on to either the warm water channel, the cooling towers, or the discharge diffusers.

The Unit 1 condenser is actually composed of three condensing units (1A, 1B, and 1C). Each condenser unit is served by two inlet lines and two discharge lines. Each inlet and discharge line is equipped with a motor-driven flow control valve. The CCW system is normally operating during plant operation; all valves are normally open and all pumps are normally running.



Note: All valve numbers have a "75" prefix, unless otherwise designated.

Figure 31. Keep-full system.



Note: The intake structure also serves as a source of water for:

1. RHR service water system
2. Emergency equipment cooling water system
3. Fire protection system
4. Water treatment plant

INEL 2 1611

Figure 32. CCW system.

Application—The CCW system operates during normal power operation. For this reason, CCW is not required to change state in response to the LOCA or transient condition nor are components of the system required to change state or position. During normal power operation, three CCW pumps serve Unit 1. Following scram, only one CCW pump is required to condense shutdown steam. A fault tree model of the CCW system was not constructed since the CCW system is in operation during normal power operation and the operational requirements in terms of CCW pump availability are less stringent following scram than they are during power operation, and since CCW may be obtained from Units 2 or 3.

6.2.6 Raw Cooling Water System. The raw cooling water system (RCWS) furnishes cooling water to various nonsafety-related in-plant cooling loads during normal operations. The purpose of the RCWS, as it relates to this analysis, is to remove heat from the RHR pump seals and room coolers under shutdown conditions other than LOSP conditions. The RCWS is not a safety-related system nor does it interface with any safety-related systems other than this interconnection with the RHR pump seals and room coolers. The purpose of this interconnection is to obviate the need for operation of the EECW system during normal shutdown.

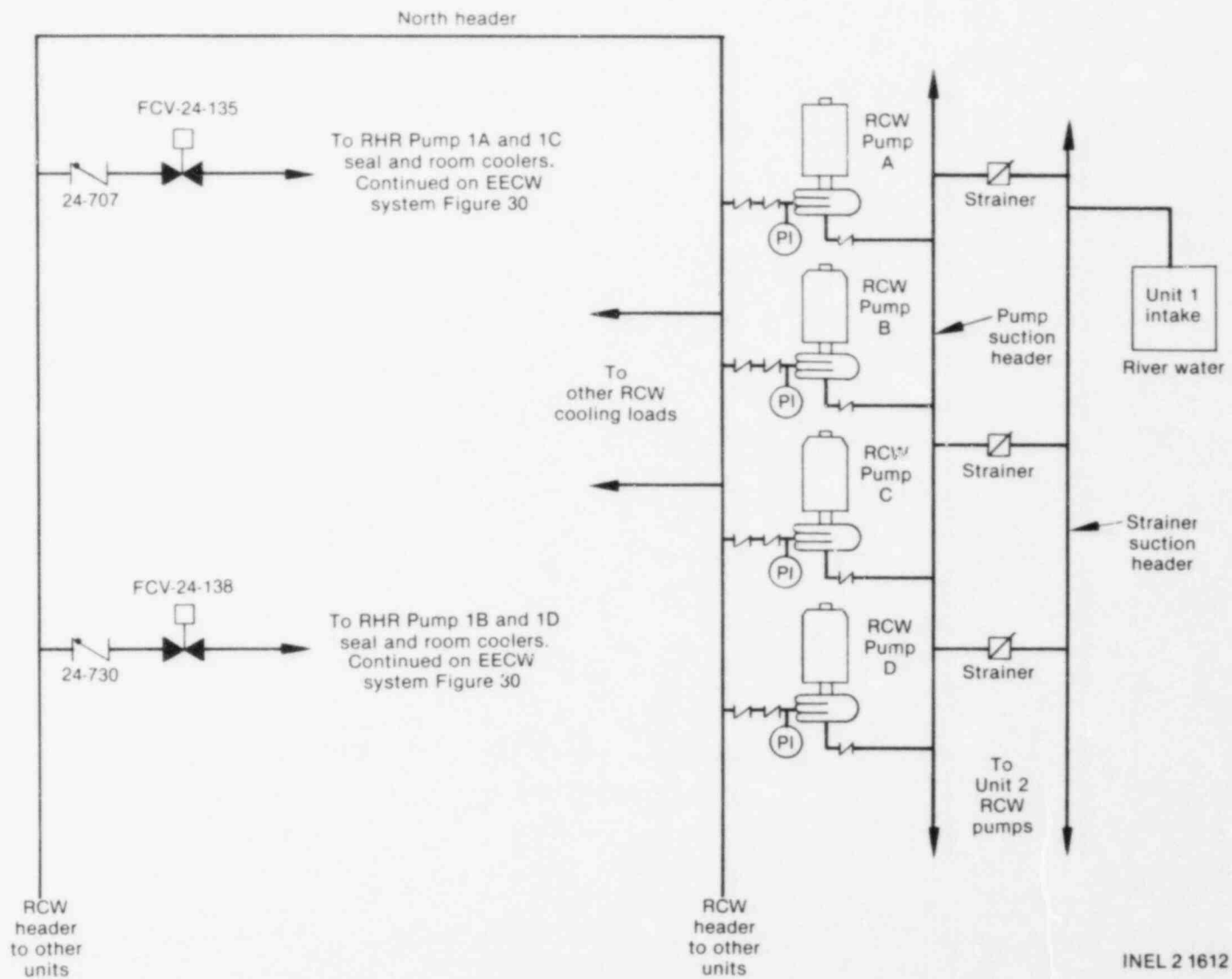
Description—The three-unit Browns Ferry plant has 11 main raw cooling water pumps of which two are spares. Units 1 and 2 are supplied by six raw cooling water (RCW) pumps with one common spare. Suction headers for Units 1 and 2 are interconnected. All of the RCW pumps discharge into a common (three unit) cooling header system. Three pumps are required for each unit during normal operations. Upon normal unit shutdown, there is still a need by that unit for at least one RCW pump for miscellaneous cooling services. The RCWS pumps are supplied 4160 V power from the nonsafety-related unit buses. Under LOSP conditions, the D spare pump can be manually connected to the Units 1 and 2 4160 V shutdown Board A bus supplied by diesel Generator A. However, no credit is taken for this manual connection for the LOSP transient. In the event the pressure in the RCW header that supplies the RHR cooling loads decreases to a preset value, pressure switches sense the drop and start the EECW pumps. Figure 33 is a simplified drawing of the RCWS.

Application—The RCWS can provide room and seal cooling for the long-term DHR functions of the RHR system during all LOCAs and transients where offsite power is not lost. For LOCA sequences, the EECW system automatically starts but the RCWS is also available. Therefore, for all sequences except the LOSP sequences, failure of room and seal cooling to the RHR system requires failure of both the RCWS and the EECW system.

6.2.7 Reactor Protection System Description. The RPS monitors key plant parameters in order to protect against conditions that could damage the fuel or reactor pressure boundary integrity. The RPS automatically initiates a reactor scram to preserve cladding integrity, protect the reactor coolant pressure boundary, minimize the energy that must be absorbed following a LOCA, and prevent subsequent recriticality.

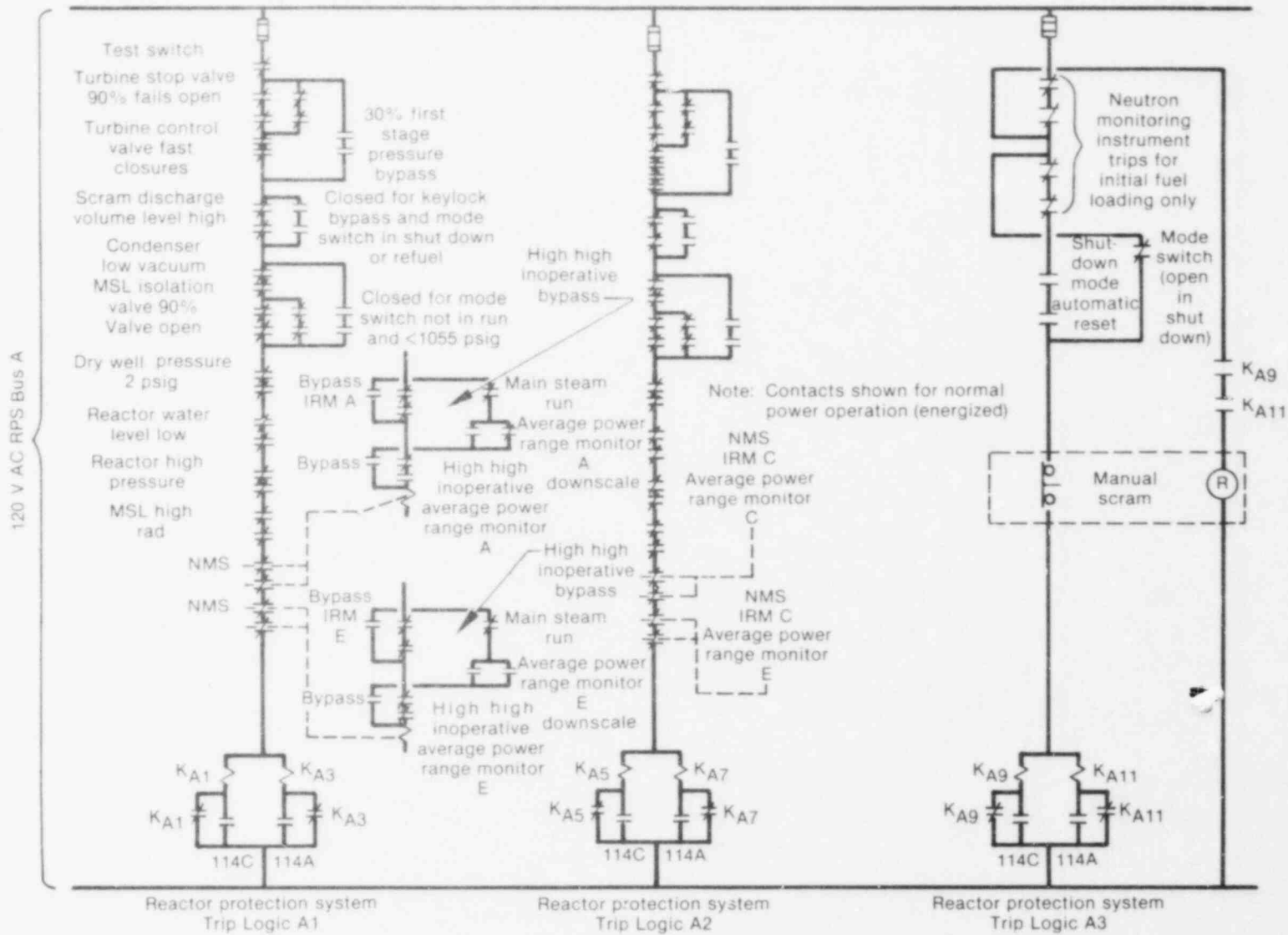
Description—The RPS includes the sensors, relays, and switches that detect abnormal conditions and initiate a rapid insertion of the control rods to shut down the reactor. The system consists of two independent trip systems (A and B) each having two automatically initiated scram channels (A1, A2, B1, and B2) and one manual scram channel (A3 and B3). Scram initiation requires a trip of at least one channel from each trip system. Power to each RPS trip system is supplied from an independent RPS bus fed by an AC-to-DC motor generator. The RPS channels are designed to initiate a scram upon loss of power to the system. Figure 34 shows RPS Channel A. Channel B is similar.

Application—The Browns Ferry RPS is very similar to the Peach Bottom system modeled in WASH-1400 and was not analyzed for this report. As mentioned in Section 2.9 of Appendix B, NUREG-0460 provided the value for failure to achieve subcriticality (3×10^{-5} per demand). This value takes into account RPS failures. For the majority of accident sequences, no mitigating systems other than the CRDH system required use of the RPS. For one case, transients where the PCS is available and the reactor subcriticality systems fail, the RPT requires an input from the RPS. The value used for RPS failure in this case is the 1.9×10^{-6} value for common mode failures from WASH-1400. This value was chosen since it represents failures that would disable both the reactor subcriticality systems and RPT system.



INEL 2 1612

Figure 33. Simplified RCW system diagram.



INEL 2 1614

Figure 34. RPS Channel A.

6.2.8 Equipment Area Cooling System. The equipment area cooling (EAC) system is not a system, per se. In this analysis, the EAC system is considered to be the particular area fan, the associated cooler, the cooling water interface with the cooler, and the power supply and control circuit for the fan.

Description—The EAC system is designed to cool the air in a specific area or room in the plant or to cool the air surrounding a specific component. This analysis determined that the only EAC system important for correctly modeling front-line system response was that associated with each of the RHR pumps. That is because the RHR pumps run for long periods in some modes of operation, while the remaining ECCS pumps run for relatively short periods.

Application—The EAC system associated with each of the RHR pumps is required to run when the RHR system is aligned to the shutdown cooling or torus cooling modes of operation. In either of these modes, the RHR pumps could be required to run for long periods (i.e., greater than 2 hours). Consequently, lack of area cooling for the pump surroundings will ultimately lead to RHR pump failure.

7. ACCIDENT SEQUENCE QUANTIFICATION

7.1 General Approach

Accident sequence quantification is a building block process. From the failure data and fault tree models, system unavailabilities can be calculated. The Boolean combination of systems from the systemic event trees combined with the system unavailabilities yields the functional unavailabilities. Combinations of functional unavailabilities and initiator frequencies produces accident sequence frequencies. Appendix C of this report describes in more detail the methodology for accomplishing this task. This section presents a general description of this procedure.

7.2 Data Sources

Table C-4 of Appendix C provided the majority of the failure data for quantification of fault trees. Most of this information comes directly from the WASH-1400 report; since failure data were not available for every component in the fault trees, other sources of data were occasionally used. Maintenance and testing contributions to system/component unavailabilities were derived from information provided by the utility company. A data summary table for each system appears in Appendix B, which describes the failure data and their sources.

Human errors of omission were included where appropriate in the fault tree models for errors involving test and maintenance, and those involving errors in response to an accident situation. Emergency operating instructions were reviewed with regard to potential accident sequences to determine the required human interactions with mitigating systems in response to the accidents. Section 3.2 of Appendix C describes in more detail these operator response errors. Explicit human error models were developed based on the procedures found in NUREG/CR-1278. It was especially important to create these models for human error events that affected multiple systems. For example, miscalibration of reactor vessel level switches could result in failure of the CSBCs to be auto-initiated when required. These human error models can be found in Section 4 of Appendix B.

7.3 System Unavailabilities

The Reliability Analysis System (RAS) computer code¹³ provided unavailability calculations based on the fault trees and failure data. The code calculates time dependent system unavailabilities using one algorithm to generate minimal cut sets and another to evaluate the unavailability associated with these cut sets. The code also ranks the cut sets from highest to lowest in terms of contribution to system unavailability.

7.4 Sequence Frequencies

The Boolean combination of systems combined with the sequence initiator produced the sequence frequencies. These frequencies served as the basis for determining the candidate dominant accident sequences. The process includes:

1. Accounting for commonalities between systems using the COMCAN II computer code¹⁴ and special bounding techniques.
2. Accounting for success events by recognizing when they can potentially be significant, and evaluating them.
3. Accounting for the effect of the initiator on the mitigating systems.

7.5 Candidate Dominant Accident Sequences

Sequences from the systemic event trees with frequencies greater than 1×10^{-6} per reactor-year were designated as candidate dominant accident sequences. Appendix C presents each of the 11 candidate dominant sequences and discusses the major contributors to the sequence frequency. The potential for recovery was considered for those sequences where the dominant contributors to sequence frequency were recoverable. Recovery considerations required taking into account such factors as the amount of time available for the recovery action, where the action must be taken, and what must be done to repair the fault. The candidate dominant sequence frequencies were requantified considering the potential for recovery.

7.6 Example Calculation

Sequence $T_U QR_B R_A$ is one of the dominant sequences that demonstrates the process of quantifying sequence frequencies. Figure 35 is the systemic event tree that includes this sequence. Table 11 lists the unavailabilities for the systems associated with this sequence. The sequence is initiated by a transient that causes the PCS to be unavailable. Following a successful scram and relief valve cycling, the RCIC system fails. The HPCI system operates to maintain reactor water level but the torus cooling and shutdown cooling modes of the RHR system fail.

The unavailability of the mitigating systems for this sequence, $Q(QR_B R_A)$, is equal to the unavailability of the Boolean combination of the systems making up the sequence. The bar over a system designator indicates success for that system. A system designator without a bar indicates system failure. The term $COM(\text{---})$ indicates the value of the commonalities between the systems indicated in parentheses. The unavailability of the mitigating systems is 3.2×10^{-6} as shown below.

$$\begin{aligned}
 Q(QR_B R_A) &= Q(\bar{B} \cap \bar{J} \cap \bar{K} \cap Q \cap \bar{D} \cap R_B \cap R_A) \\
 &= Q(Q \cap R_B \cap R_A) - COM[Q \cap R_B \cap R_A \cap (B \cup J \cup K \cup D)] \\
 &= Q[Q \cap (R_B \cap R_A)] - 0 \\
 &= Q(Q)Q(R_B \cap R_A) + COM(Q \cap R_B \cap R_A) \\
 &= Q(Q) Q(R_B \cap R_A) + 0 \\
 &= Q(Q)[Q(R_B)Q(R_A) + COM(R_B \cap R_A)] \\
 &= (0.042)[(3.1 \times 10^{-3})(2.0 \times 10^{-2}) + 1.4 \times 10^{-5}] \\
 &= 3.2 \times 10^{-6},
 \end{aligned}$$

where the Q in parentheses represents the RCIC system code.

The term $COM[Q \cap R_B \cap R_A \cap (B \cup J \cup K \cup D)]$ accounts for the effect of the success of the scram, relief valve, and HPCI systems on the failed systems. In this case, that effect is negligible. The term $COM(Q \cap R_B \cap R_A)$ accounts for commonalities between the RCIC, torus cooling, and shutdown cooling modes of RHR. This term is also negligible. The term $COM(R_B \cap R_A)$ accounts for commonalities between torus cooling and shutdown cooling modes of RHR. This term is not negligible and has a value of 1.4×10^{-5} . It consists of common minimum-flow bypass valve faults and common support system faults.

Table 11. Transients where the PCS is unavailable

System Designator	System	System Unavailability
B	CRD	$Q(B) = 3.0 \times 10^{-5}$
J	Relief valves (opening)	$Q(J) = 7.2 \times 10^{-9}$
K	Relief valves (closing)	$Q(K) = 5.7 \times 10^{-2}$
Q	RCIC	$Q(Q) = 4.2 \times 10^{-2}$
D	HPCI	$Q(D) = 4.4 \times 10^{-2}$
V	Manual depressurization	$Q(V) = 3.0 \times 10^{-3}$
F _B	Core spray	$Q(F_B) = 6.6 \times 10^{-4}$
G _D	LPCI	$Q(G_D) = 1.1 \times 10^{-4}$
W	Condensate	$Q(W) = 7.0 \times 10^{-3}$
X	SBCS	$Q(X) = 4.2 \times 10^{-2}$

The sequence frequency $P(T_U QR_B R_A)$ is then equal to the product of the initiator frequency $F(T_U)$, and the unavailability of the mitigating systems $Q(QR_B R_A)$. The initial sequence frequency is 5.5×10^{-6} per reactor-year as shown below.

$$\begin{aligned}
 P(T_U QR_B R_A) &= F(T_U)Q(QR_B R_A) \\
 &= (1.7)(3.2 \times 10^{-6}) \\
 &= 5.5 \times 10^{-6}.
 \end{aligned}$$

Considering recovery options reduces $Q(QR_B R_A)$ to 2.4×10^{-6} . The unavailability of torus cooling and shutdown cooling is reduced from 7.6×10^{-5} to 5.7×10^{-5} , while the unavailability of RCIC is unchanged since the majority of its faults are not recoverable. The mitigating system unavailability then is the product of RCIC unavailability, $Q(Q)$, and the unavailability of torus cooling and shutdown cooling considering recovery, $Q(R_B R_A \text{ considering recovery})$. This value is 2.4×10^{-6} as shown below.

$$\begin{aligned}
 Q(QR_B R_A) &= Q(Q)Q(R_B R_A \text{ considering recovery}) \\
 &= (0.042)(5.7 \times 10^{-5}) \\
 &= 2.4 \times 10^{-6}.
 \end{aligned}$$

The final sequence frequency is the product of the initiator frequency $F(T_U)$ and the unavailability just derived, $Q(QR_B R_A)$. Thus, the final sequence frequency $P(T_U QR_B R_A)$ is equal to 4.1×10^{-6} per reactor-year as shown below.

$$\begin{aligned} P(T_U QR_B R_A) &= F(T_U)Q(QR_B R_A) \\ &= (1.7)(2.4 \times 10^{-6}) \\ &= 4.1 \times 10^{-6} \end{aligned}$$

8. RESULTS

8.1 General

The quantification of the systemic event trees resulted in 11 candidate dominant sequences. Each of these sequences had an initial frequency value greater than 1.0×10^{-6} per reactor-year. The final value for each sequence consisted of the initial frequency modified by potential recoverability. Table 12 lists these 11 sequences giving the initiator, initial frequency, and final frequency.

8.2 Dominant Sequences

The dominant sequences appear in Table 13. These eight sequences all have final frequencies greater than 1.0×10^{-6} per reactor-year. Six of these sequences are transient sequences, while the other two are transient-induced LOCAs. Six of the sequences involve failure to remove long-term decay heat from the reactor, while two involve failure to achieve subcriticality. A general discussion of these sequences is presented in the following sections; a more detailed treatment can be found in Section 4.2 of Appendix C, which includes a systemic event tree representation of the sequence as well as a graphic display of the dominant contributors to the sequence frequency.

8.2.1 Transients Without PCS and with DHR Failure (T_{URBRA}). In this sequence, a transient occurs that renders the PCS unavailable as a heat sink for the reactor. A reactor scram occurs and the

Table 12. Candidate dominant sequences

Initiator	Designator	Frequency (per reactor-year)	
		Initial	Final
Transient-induced LOCAs	T_{KRBR_A}	1.2×10^{-5}	9.3×10^{-6}
LOSP-induced LOCAs	T_{PKRBR_A}	8.3×10^{-5}	1.6×10^{-6}
	$T_{PKDFB_{GD}}$	2.5×10^{-6}	8.7×10^{-8}
Transient with PCS unavailable	T_{URBR_A}	1.3×10^{-4}	9.7×10^{-5}
	T_{UQRBR_A}	5.5×10^{-6}	4.1×10^{-6}
	T_{UB}	5.1×10^{-5}	5.1×10^{-5}
	T_{UQDV}	9.2×10^{-6}	5.5×10^{-7}
Transient with PCS available	T_{ABM}	3.7×10^{-6}	3.7×10^{-6}
LOSP	T_{PRBR_A}	1.5×10^{-3}	2.8×10^{-5}
	T_{PQRBR_A}	6.2×10^{-5}	1.2×10^{-6}
	$T_{PQDFB_{GD}X}$	1.2×10^{-6}	3.6×10^{-8}

Table 13. Dominant sequences

Initiator	Designator	Frequency (per reactor-year)
Transients without PCS	T _{URBRA}	9.7 x 10 ⁻⁵
Transients without PCS	T _{UB}	5.1 x 10 ⁻⁵
LOSP	T _{PRBRA}	2.8 x 10 ⁻⁵
Transient-induced LOCA	T _{KRBRA}	9.3 x 10 ⁻⁶
Transients without PCS	T _{UQRBRA}	4.1 x 10 ⁻⁶
Transients with PCS	T _{ABM}	3.7 x 10 ⁻⁶
LOSP-induced LOCA	T _{PKRBRA}	1.6 x 10 ⁻⁶
LOSP	T _{PQRBRA}	1.2 x 10 ⁻⁶

nuclear chain reaction is stopped. As reactor decay continues to add heat to the coolant, reactor pressure increases until the relief valves open. Steam from the reactor is passed to the torus to reduce reactor pressure. Once pressure drops below the relief valve setpoints, the valves reclose until pressure increases again. This process is repeated until action is taken to remove decay heat by another means. Since the main condenser is not available as a heat sink, the MSIVs automatically shut to prevent excessive loss of reactor water inventory. Following this action, the RCIC system automatically starts to replace the inventory lost during relief valve operation. At this point, the reactor decay heat is being transferred to the torus water either by relief valve action or by operation of the RCIC system. However, the RHR system is the only system capable of removing the decay heat. Its failure causes the torus water temperature to increase until it can no longer be used to replace the lost reactor coolant inventory or condense the steam from the RCIC turbine discharge. As a result, the ECI systems will be unable to replace lost coolant, and vessel water level will decrease until core uncover occurs. A core melt will then occur.

The RHR system can provide the DHR function in either the torus cooling mode or the shutdown cooling mode. Torus cooling is the normal mode for this sequence. Both modes must be inoperable in order for the DHR function to fail. The unavailability of the shutdown cooling mode is dominated by control circuit faults of the three suction valves, resulting in the valves failing to open. These faults account for 84% of the 1.9×10^{-2} unavailability for shutdown cooling. Torus cooling unavailability is dominated by operator failure to initiate the system and combinations of control circuit faults of RHR and RHRSW system motor-operated valves. The unavailability of both modes is 7.6×10^{-5} and is dominated by combinations of control circuit faults. The minimum-flow bypass valves failing to close account for approximately 18% of the 7.6×10^{-5} unavailability for both systems.

There are approximately 6 to 8 hours available for the operators to take corrective action for this sequence before core melt occurs. This estimate is based on the time it takes to deplete the CST and heat the torus water to a temperature that prevents the RCIC system from pumping the water, assuming no containment back-pressure.¹⁵ There are two paths the operators may pursue to prevent a core melt. One path involves recovering the PCS as a heat sink for the reactor. The other involves recovery of the RHR system in torus cooling or shutdown cooling modes.

The ability to recover the PCS depends upon the transient initiator. Some initiators may be easily bypassed or repaired while others may not. For example, if a loss of feedwater flow were caused by a fault in the automatic level controller, the operator could manually control the flow after opening the MSIVs. If the loss of feed flow were due to a mechanical failure of the pumps, then recovery would be unlikely within the time of this sequence. No credit for PCS recovery was considered since there is inadequate information available on which to base a probability of recovery.

Since the dominant contributors to failure of both the torus cooling and shutdown cooling modes are control circuit faults, it is possible that the operators could either bypass the faulty control circuits or operate the valves manually. During the Browns Ferry fire of March 1975, the operators demonstrated the ability to improvise a fix on the relief valves so they could be operated. The final sequence frequency of 9.7×10^{-5} per reactor-year reflects recoverability of control circuit faults.

8.2.2 Transients Without PCS and with RS Failure (T_{UB}). In this sequence, a transient occurs that causes the PCS to be unavailable as a heat sink for the reactor. However, an insufficient number of control rods insert to make the reactor subcritical. As a result, the reactor continues to generate considerable heat depending upon the number and location of control rods that fail to insert. Because the reactor has been isolated from its normal heat sink, pressure rises until the relief valves open and begin to pass steam from the reactor to the torus. The rate of inventory loss due to relief valve action in this case is higher than the makeup capacity of the high pressure systems. Therefore, water level steadily decreases until core uncover and core melt occur.

The CRD system unavailability, taken from NUREG-0460, is 3.0×10^{-5} . As noted in NUREG-0460 and WASH-1400, the exact number of rods that must fail to insert and the position and relative location of those rods is not easily calculated and is considered to be beyond the scope of this analysis. Therefore, the NUREG-0460 value of 3.0×10^{-5} was used in lieu of a specific evaluation by the Browns Ferry IREP team.

For this sequence, there is very little time for the operator to take recovery actions. No credit is given for operator recovery during the first 5 min of a transient or LOCA. Furthermore, the actions available for the operator are neither clearly defined nor easily quantifiable. Therefore, the final sequence frequency of 5.1×10^{-5} per reactor-year takes no credit for operator recovery actions.

8.2.3 Loss of Offsite Power with DHR Failure (T_{pRBR_A}). After a LOSP, a reactor scram occurs. The relief valves open to relieve the reactor pressure increase caused by the turbine trip without bypass that follows a LOSP. The relief valves successfully reclose and the MSIVs isolate the reactor from the condenser. The RCIC system maintains reactor water level. Subsequently, the RHR system fails to remove the reactor decay heat. A sustained loss of RHR cooling will cause torus water temperature to increase until the ECI systems are incapable of pumping the torus water. Water level will decrease and core uncover will then occur, followed by core melt.

The dominant contributors to RHR unavailability for this sequence fall into two groups: EECW related faults and non-EECW related faults. Failure of the EECW system to provide its required cooling will eventually result in a loss of all diesel generators. The dominant contributors to the EECW system unavailability are combinations of two or more diesel generators failing to start. The non-EECW faults result in a direct failure of the RHR system to provide cooling. These faults are also dominated by combinations of diesel faults (three or more failing diesels, not necessarily the same as those for EECW failure).

There are several factors involved in RHR recoverability for this sequence. Given successful RCIC operation, at least 6 to 8 hours are available for the operator to take action to recover the RHR system.

One potential recovery option is the restoration of offsite power. Figure III 6-4 of WASH-1400 indicates that offsite power can be recovered 97% of the time within 6 to 8 hours. The restoration of offsite power changes the DHR unavailability from 4.9×10^{-2} to 7.6×10^{-5} .

Another potential recovery option is for the operator to manually start and valve into service additional RHR pumps to the EECW headers to provide the necessary cooling. The operator could also act to isolate nonessential EECW loads so that the flow from less than three of four pumps would still be sufficient. Flow from two of four pumps provides 91% of rated flow so that judicious isolation of other loads might allow two of four pumps to provide the required flow.

The operator could also attempt to restart diesel generators that have initially failed to start. However, the success or failure of such action depends largely on the original cause of the failure to start. No credit is taken for this action.

The final sequence frequency takes into account the probability of failing to recover offsite power and the probability of failing to recover the EECW system. It does not reflect any credit for restarting diesel generators. The final sequence frequency is 2.8×10^{-5} per reactor-year.

8.2.4 Transient-Induced SORV with DHR Failure (TKR_BR_A). The transient-induced SORV occurs when any transient (except a LOSP, which is covered separately) results in a reactor scram, relief valve opening, and a failure of one or more relief valves to reclose. This action is similar to an intermediate steam break in all but two respects. First, the steam discharges directly to the torus; consequently, there is no drywell pressure increase and, therefore, no high drywell initiation signal for the ECI systems. Second, because the steam goes directly to the torus, the SCI function of the intermediate steam break tree is not applicable.

Following the transient-induced SORV, the HPCI system successfully operates to maintain reactor water level. In this case, the HPCI systems actuate on low level. Subsequently, the RHR system fails to remove the reactor decay heat. This failure allows torus water temperature to rise to the point where the HPCI system can no longer pump the torus water back to the reactor to maintain level. Consequently, core uncover occurs and a core melt ensues. The dominant contributors to RHR system failure in this sequence are the same as that for sequence T_UR_BR_A discussed previously in Section 8.2.1. Likewise, the recoverability factors are essentially the same for this sequence. The final sequence frequency is 9.3×10^{-6} per reactor-year.

8.2.5 Transients Without PCS and with RCIC and DHR Failure (T_UQR_BR_A). This sequence is the same as T_UR_BR_A in Section 8.2.1 except that the RCIC system fails to operate to maintain reactor water level. Instead, the HPCI system operates to maintain level. Subsequent failure of torus cooling and shutdown cooling eventually causes a core melt. The most dominant contributor to RCIC failure is rupture disk failure in the drive turbine steam exhaust line. Should one of these two disks rupture, a pressure switch signal will be generated that isolates RCIC.

The recovery factors for torus cooling and shutdown cooling are the same as in sequence T_UR_BR_A. Thus, the final frequency for this sequence is 4.1×10^{-6} per reactor-year.

8.2.6 Transient with PCS and with RS and RPT Failure (T_ABM). For this sequence, a transient occurs that does not directly cause a failure of the PCS system. However, an insufficient number of control rods insert to stop the nuclear chain reaction. Therefore, reactor power remains high. If the recirculation pumps are tripped, then the reactor power level will be reduced to within the capacity of the bypass valves to remove heat to the condenser. Failure of the RPT feature allows reactor power to remain above the bypass valve capacity. Therefore, reactor pressure increases and the relief valves open to dump the excess steam into the torus. As a result, torus water temperature rapidly rises until the water can no longer condense the steam. Since the steam added to the torus is not condensed and returned to the reactor via the PCS system, the water supply to the feed pumps rapidly decreases until the feed pumps trip. Subsequently, reactor water level rapidly drops until core uncover occurs and core melt ensues. The dominant contributor to this sequence is a reactor protection system (RPS) failure that prevents actuation of a reactor scram or a recirculation pump trip. The operator could manually initiate these actions. However, the time available for the operator to take these actions is very short, and the final sequence frequency takes no credit for such action. The final sequence frequency is 3.7×10^{-6} per reactor-year.

8.2.7 LOSP Induced SORV and with DHR Failure (T_pKR_BRA). The phenomenological effects of a LOSP induced SORV are identical to those described in Section 8.2.4 for a transient induced SORV. The differences in the sequences lie in the frequency of occurrence and the unavailabilities of the mitigating systems due to the LOSP.

The dominant contributors to DHR unavailability for this sequence are identical to those for the LOSP with DHR failure (sequence T_pRBRA) discussed in Section 8.2.3. The potential recovery actions for this sequence are the same as sequence T_pRBRA . Applying these recovery factors results in a final sequence frequency of 1.6×10^{-6} per reactor-year.

8.2.8 Loss of Offsite Power and with RCIC and DHR Failure (T_pQRBRA). This sequence is the same as T_pRBRA except that the RCIC system fails to operate to maintain reactor water level. Instead, the HPCI system operates to perform this function. Subsequent failure of torus cooling and shutdown cooling lead to a core melt.

The recoverability factors associated with torus cooling and shutdown cooling are the same as the sequence T_pRBRA . Therefore, the final frequency for this sequence is 1.2×10^{-6} per reactor-year.

8.3 Containment Response and Release Categories

8.3.1 Introduction. The dominant BFI core melt sequences are listed in Table 14 along with the applicable containment failure modes. The accident processes, timing of core melt, containment failure modes, and consequences of fission product releases to the atmosphere for these sequences have been estimated based primarily on previous analyses for other BWRs. Previously analyzed BWRs include the Grand Gulf and Peach Bottom plants. The Peach Bottom plant, which was also analyzed in WASH-1400, is quite similar to BFI, and many of the present conclusions regarding BFI are based on these analyses. In addition, a few MARCH code¹⁶ calculations were performed specifically for BFI. However, no plant-specific CORRAL¹⁷ calculations were undertaken.

The containment failure modes (α , γ , and γ') listed in Table 14 for the various sequences are the same as those employed for the BWR in WASH-1400, Appendix I, Section 2.2. The notations for the fission product release categories are also the same. In WASH-1400, the probability of containment overpressure failure in the event of core meltdown was found to approach unity. Failure with direct release of the radioactivity to the atmosphere was assessed to occur about 20% of the time ($\gamma' \sim 0.2$); in the remaining cases ($\gamma \sim 0.8$), fission products were released into the annular region between the drywell liner and the concrete wall. Release to the atmosphere via the annulus results in additional fission product removal, which reduces the accident consequences. Fission product deposition in this annulus was intended to represent removal by passage through secondary containment structures.

The probabilities of release directly to the atmosphere and through the annulus were based in WASH-1400 on an analysis of the layout and structural strength of the building enclosing the wetwell or torus. No such analysis is available for BFI. Thus, the relative magnitudes of the γ' and γ probabilities for BFI are uncertain.

The probability that a steam explosion in the reactor vessel causes containment failure is assessed in Table 14 to be $\alpha = 0.01$ for LOCAs and $\alpha = 0.0001$ for transients. The higher value is identical to that in WASH-1400. The lower value is based on recent research that indicates steam explosions are suppressed at high system pressures. Thus, for cases in which core meltdown occurs with the primary system at high pressure, steam explosions are assessed to be less likely.

Table 14 contains no assessment of the consequences of containment isolation failure or failures of the standby gas treatment system. These containment failure modes did not contribute significantly to the WASH-1400 consequences, and are thus judged not likely to contribute significantly to the risk associated with the core melt sequences in Table 14.

Table 14. Dominant sequences versus containment failure modes

Sequence	Frequency	Containment Failure Mode Frequencies ^a		
		α	γ'	γ
T _U R _B R _A	9.7 x 10 ⁻⁵	9.7 x 10 ⁻⁹	1.9 x 10 ⁻⁵	7.8 x 10 ⁻⁵
T _U B	5.1 x 10 ⁻⁵	5.1 x 10 ⁻⁵	1.0 x 10 ⁻⁵	4.1 x 10 ⁻⁵
T _F R _B R _A	2.8 x 10 ⁻⁵	2.8 x 10 ⁻⁹	5.6 x 10 ⁻⁶	2.2 x 10 ⁻⁶
T _K R _B R _A	9.3 x 10 ⁻⁶	9.3 x 10 ⁻⁸	1.9 x 10 ⁻⁶	7.4 x 10 ⁻⁶
T _U Q _R B _R A	4.1 x 10 ⁻⁶	4.1 x 10 ⁻¹⁰	8.2 x 10 ⁻⁷	3.3 x 10 ⁻⁶
T _A BM	3.7 x 10 ⁻⁶	3.7 x 10 ⁻¹⁰	7.4 x 10 ⁻⁷	3.0 x 10 ⁻⁶
T _P K _R B _R A	1.6 x 10 ⁻⁶	1.6 x 10 ⁻⁸	3.2 x 10 ⁻⁷	1.3 x 10 ⁻⁶
T _P Q _R B _R A	1.2 x 10 ⁻⁶	1.2 x 10 ⁻¹⁰	2.4 x 10 ⁻⁷	9.6 x 10 ⁻⁷
Final	2.0 x 10 ⁻⁴	1.3 x 10 ⁻⁷	3.9 x 10 ⁻⁵	1.7 x 10 ⁻⁴

a. Probabilities of containment failure modes:

- α (in-vessel steam explosion) = 0.01 (LOCAs)
- α (in-vessel steam explosion) = 0.0001 (transients)
- γ (release through annulus) = 0.8
- γ' (direct release to atmosphere) = 0.2.

All containment failure modes of dominant sequences fell into WASH-1400 release categories as follows: α - 1, γ' - 2, γ - 3. Other release categories versus failure modes are possible for γ and γ' modes, but none of these sequences were dominant.

The core melt accidents in which containment failure occurs with direct release to the atmosphere (γ' cases) fall into three categories. The most severe accidents (i.e., those with the greatest fission product releases) are those in which core meltdown occurs while the pressure suppression pool is ineffective in scrubbing fission products. This generally occurs for meltdown sequences in which the DHR systems fail. In accident sequences in which the suppression pool temperatures remain low, significant scrubbing of fission products may occur. These accidents generally involve early failure of the primary coolant makeup system. Other types of meltdown accidents, including those that involve failures in the reactor shutdown system, are discussed in more detail below.

8.3.2 Failure of Decay Heat Removal System. In a transient or LOCA in which the DHR systems fail, water makeup to the primary system can generally be maintained initially by injection from the CST. If the operators choose to maintain sufficient makeup to just compensate for decay heat boiloff, the CST will empty (135,000 gallons assumed injected) after about 15 hours.^a The operators would then be

a. The accident timing is obtained from a MARCH calculation for a transient with DHR failure. The timing for LOCAs could be somewhat shorter. For large LOCAs the suppression pool temperature would be 20 to 30°F greater due to heating by the primary system blowdown at the time of depletion of the CST. Thus, for some LOCAs ECC pump cavitation may be concurrent with switch over to injection from the suppression pool.

expected to switch to injection of water from the suppression pool. However, in the absence of DHR, MARCH calculations indicate the suppression pool temperature would be increased to about 200°F and the containment pressure to 21 psia. TVA systems analysts said that BFI measurements show ECI pump cavitation will occur if the suppression pool temperature exceeds 185 to 190°F with the containment at 1 atm. These measurements imply pump cavitation is likely if the subcooling of the suppression pool is less than

$$TSAT - TPOOL = 212 (185 \text{ to } 190) = 17 \text{ to } 12^\circ\text{F}.$$

At 21 psia, the suppression pool is 30°F subcooled at the time of switch over to ECI injection from the suppression pool. Thus, pump cavitation is unlikely at this time even though the pool temperatures exceed the 185 to 190°F range. MARCH calculations were performed in which ECI pump cavitation (failure) was assumed when the subcooling fell below 10°F. ECI failure occurred for this case at 21.7 hours with the containment at a pressure of 27.3 psia and the suppression pool at 235°F. With no primary system makeup, the core starts to uncover at 25.6 hours and core melting at 26.2 hours. Containment overpressure failure (180 psia) is predicted to result from the release of steam and hydrogen from the primary system, which accompanies bottom head failure at about 27.7 hours.

CORRAL calculations indicate a BWR Category 2 release for this sequence for direct release to the atmosphere, and a Category 3 release for release through the drywell annulus. (Note: Release categories are defined in WASH-1400.) No credit is given in these release calculations for potential scrubbing while the suppression pool is saturated or after the containment fails.

8.3.3 Failure of Primary Coolant Makeup. Accidents develop quickly in which there is no primary coolant makeup following a LOCA or transient. For a large LOCA, core melting may start in several minutes. For a transient with boiloff through the safety valves at a nominally constant pressure of 1100 psia, core melting is delayed until about 100 min. The suppression pool will remain well subcooled in these accidents even in the absence of DHR (RHR failure), so there is significant scrubbing of fission products in the pool as long as the containment remains intact.

For LOCAs, MARCH calculations indicate containment overpressure failure shortly after bottom head melt through. For transients, MARCH indicates containment failure is delayed a few hours after bottom head failure. Because of the delayed containment failure, significant scrubbing of the fission products released during the concrete melting phase of the accident could take place. For the LOCAs, the fission products released during the concrete melting phase are not scrubbed because of containment failure. Most of the fission products released during the core heatup and meltdown phase of the accident are scrubbed by the pool for both LOCAs and transients. The difference in timing of containment failure results in BWR Category 3 releases for LOCAs and Category 4 releases for transients for direct containment leakage to the atmosphere. For release through the annulus, Category 4 releases are predicted for both LOCAs and transients.

The difference in timing of containment failure for transients and (pipe-break) LOCAs is due to the presence of water on the drywell floor and, consequently, in the reactor cavity for LOCAs.^a Rapid vaporization of this water by the molten debris following bottom head melt through results in a pressure spike that is likely to produce containment failure. For transients, there is generally little water in the reactor cavity because the primary system blowdown is released in the wetwell and condensed directly in the suppression pool. However, operation of building coolers and sprays in the drywell increases the amount of water on the drywell floor for transients. A MARCH calculation that considered drywell building cooler operation indicated insufficient accumulation of condensate on the drywell floor to threaten containment upon vaporization. Use of the RHR in a drywell spray mode could add sufficient water to the drywell floor that the subsequent pressure generation could threaten containment. However, operation of the containment spray is generally inconsistent with the assumed unavailability of primary system makeup. Thus, for

a. Battelle-Columbus Laboratories has not been able to definitively establish that water enters the reactor cavity for BFI LOCAs. However, this is believed to be the case for the similar Peach Bottom plant.

the ECI and VWI sequences, the containment spray is taken to be inoperative, and would not provide a means of placing water on the drywell floor. Thus, only LOCAs are likely to have significant water accumulation on the drywell floor.

8.3.4 Failure of Reactor Shutdown System. Following failure of the reactor (subcriticality) shutdown system, changes will occur in the core fuel temperatures, the water temperature in the core, and the steam or void fraction due to coolant boiling. Due to these changes (which naturally affect neutron kinetics and reactivity) the core power level will change. The subsequent core behavior is sensitive to the actual power level achieved. For the transient analyzed in WASH-1400, the core power level was calculated to stabilize at about 30% of rated power. Under steady state conditions, the BFI high pressure injection system can provide sufficient makeup to compensate for the coolant boiloff at power levels up to about 25%. Thus, at a 30% power level, there would be a net coolant loss from the system and core uncover would eventually occur. However, even in the situation where adequate makeup is initially provided, ECI failure would be expected to occur relatively quickly. This occurs because, for high core power levels, the RHR system is unable to prevent rapid heatup of the suppression pool. Thus, safety pumps taking suction from the suppression pool may fail due to cavitation as discussed previously for sequences involving failure of the DHR systems. Alternatively, the pumps may fail following containment failure due to pool overheating.

A MARCH calculation for a transient with a sequence similar to that discussed above indicates RHR failure at 24 min at a suppression pool temperature of 252°F and a containment pressure of 28 psia. ECI failure follows shortly at 27 min when the injection switches from the CST to the suppression pool. Core uncover starts at 28 min and core melting at 46 min. Containment failure is predicted shortly after bottom head failure. Because of the high suppression pool temperatures, little fission product scrubbing is expected. The fission product releases fall into BWR Categories 2 and 3, depending on whether release occurs directly to the environment or through the annulus. These results and accident behavior are similar to those discussed under failure of the DHR systems. The accident timing is greatly accelerated however.

Battelle-Columbus Laboratories has not made neutron kinetics calculations for LOCAs involving failures of the shutdown system. Thus, for LOCAs, an equilibrium or steady-state core power level similar to that for transients is not known. A similar behavior would be expected. In any case, assumption of a behavior similar to that for transients would conservatively place their fission product releases in the BWR release Categories 2 and 3. Since the LOCAs contribute little to the cases involving reactor shutdown failure, this assumption has insignificant impact on the overall consequences.

8.4 Engineering Insights

In the course of performing this analysis, many engineering insights were gained. Some are significant with respect to the frequency of core melt while others are significant only on a systemic level and have no affect on other systems. This section details some of the insights judged to be important by the BFI IREP team.

8.4.1 Core Melt Frequency Versus Initiators. Figure 36 is a plot of the core melt sequences with frequencies greater than 1.0×10^{-8} per reactor-year versus the sequence initiators. The values plotted are frequencies without recovery included. From this plot it is easy to see that transient core melt sequences occur more frequently than transient-induced SORV sequences and LOCA sequences. Furthermore, within the LOCA sequences, small break-initiated core melt sequences have higher frequencies than intermediate or large break sequences.

These findings are very significant. They indicate that the risk of core melt is orders of magnitude more likely from transients or small LOCAs than from larger LOCAs.

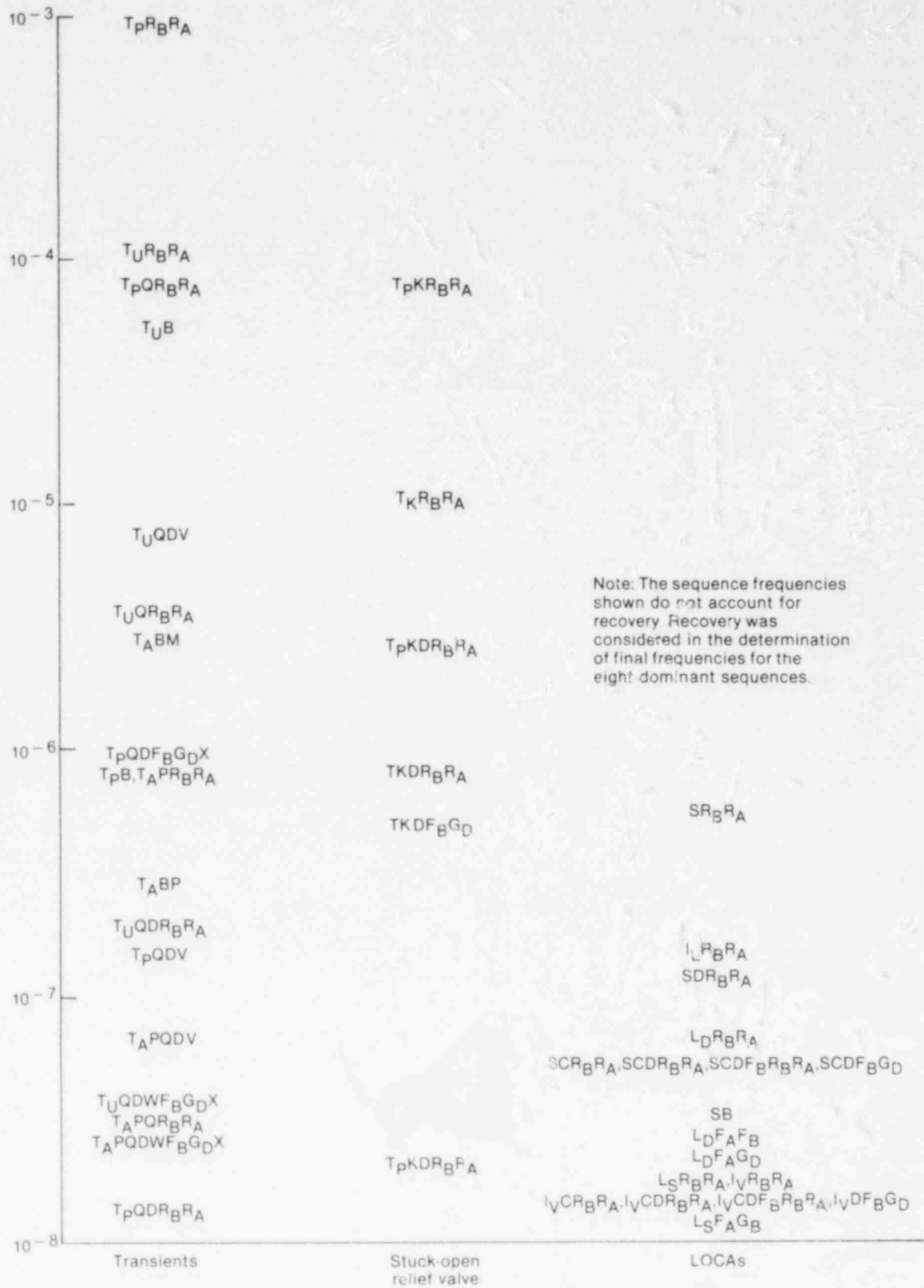


Figure 36. Core melt sequence frequencies versus initiators (recovery actions not considered).

8.4.2 Core Melt Frequency Versus Failed Function. Figure 37 is a plot of core melt sequences versus failed function. As with Figure 36 the frequencies plotted do not include recovery values. Again it is easy to see that core melt sequences resulting from DHR failure are more frequent than those caused by reactor subcriticality failures and those caused by ECI/VWI failures.

These findings are also significant. They indicate that the risk of core melt from failures of the RHR system is much higher than from failures of either the scram or injection systems. In fact, DHR failures account for about 73% of the sum of the final dominant sequence frequencies. The remaining 27% were failure to scram sequences and none were sequences involving failure to inject. This indicates that the RHR and scram systems are the two most important systems with respect to core melt frequency and that no significant improvement in the overall core melt frequency can be achieved without first improving the reliability of these two systems.

8.4.3 RHR System Contribution. Since 73% of the sum of the final dominant sequence frequencies is due to sequences involving RHR failures, it is appropriate to discuss this system further. In actuality, there are two different modes of RHR that must fail in order to cause failure of the long-term decay heat removal function.

One might expect that the unavailability of both the torus cooling and shutdown cooling modes of the RHR system would be quite low due to the built-in system redundancy. Indeed, the unavailability of torus cooling and shutdown cooling is 7.6×10^{-5} (before considering recovery). This factor is offset by the fact that, for any LOCA and many transients, the probability is unity that the RHR system alone will be required to perform the long-term decay heat removal function. Therefore, no matter what combination of systems succeed in providing the scram, overpressure protection, and ECI or VWI functions, the RHR system in either the torus cooling or shutdown cooling mode will be required to function in order to prevent a core melt from occurring.

In the absence of another means of removing decay heat, the RHR unavailability deserves additional attention. At first glance, the arrangement of four separate pump and heat exchanger combinations (two of which are needed for torus cooling and only one for shutdown cooling) would seem to provide the multiple redundancy necessary to limit the unavailability of torus cooling and shutdown cooling. The fact that they utilize different discharge paths would also tend to support this conclusion.

However, the four-loop redundancy is compromised by combining the pump discharges into two discharge paths. Thus, failure of any pair of two valves in opposite discharge paths negates the pump redundancy. Furthermore, failure of the minimum-flow bypass valves for the two paths poses a common failure mode for both torus cooling and shutdown cooling. This tends to negate the apparent redundancy of the discharge paths previously noted.

Unlike the torus cooling mode that has two separate suction paths, the shutdown cooling mode has only one. In that path, failure of any one of three valves to open disables the entire shutdown cooling mode. This is the reason that shutdown cooling unavailability is approximately an order of magnitude higher than torus cooling unavailability.

Together these factors tend to reduce the apparent redundancy of the two modes of RHR operation. Therefore, instead of two systems with low unavailabilities being combined (as in core spray and LPCI) two systems with higher unavailabilities and several commonalities are combined. The result is an unavailability for these two modes that is not as low as might be originally expected.

In order to reduce the frequency of the sequences involving RHR failure, there appears to be at least three choices:

1. Ensuring the PCS is available with a high reliability.
2. Changing the RHR system to eliminate those factors previously mentioned that compromise the four pump and heat exchanger redundancy.

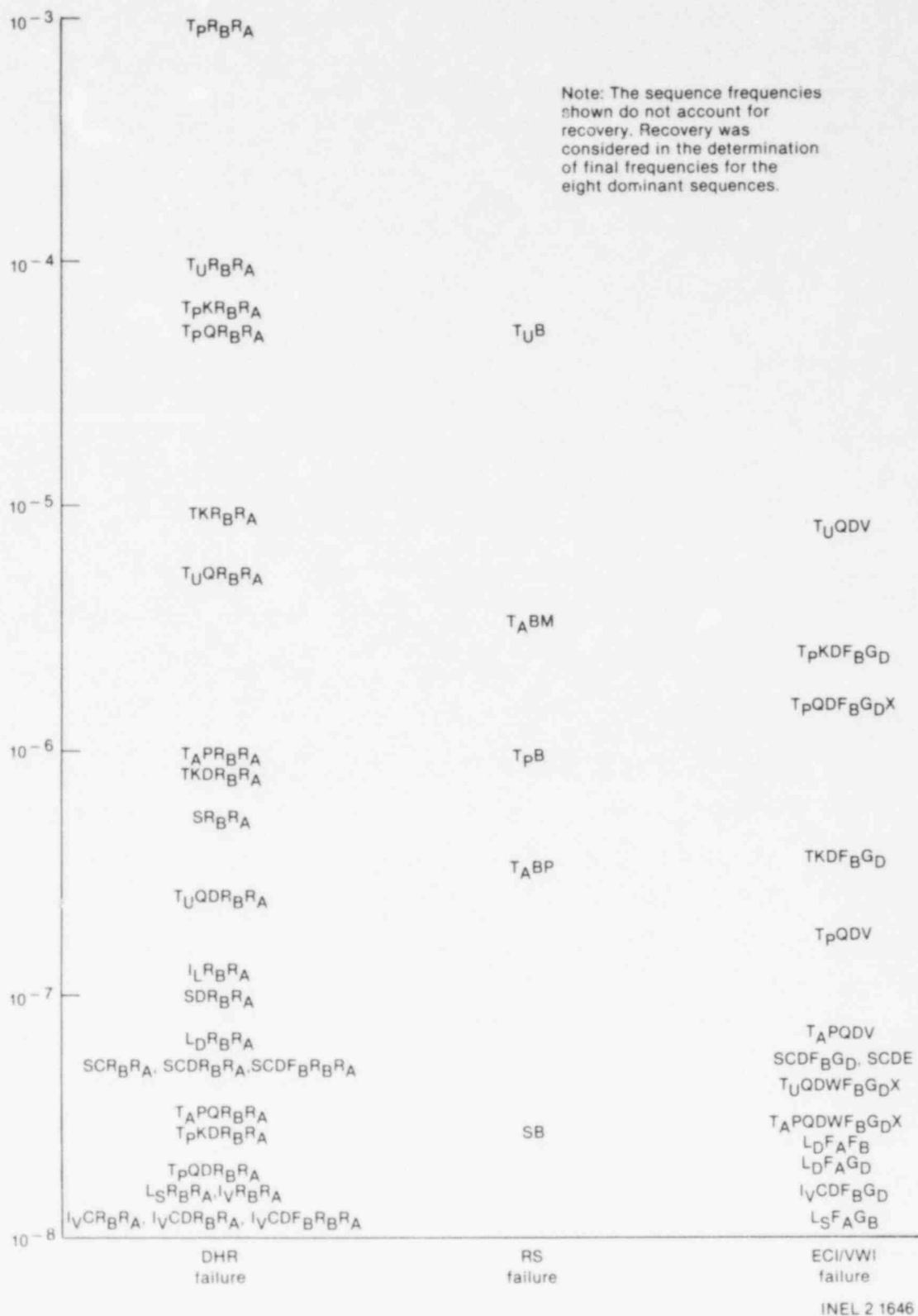


Figure 37. Core melt sequence frequencies versus failed function (recovery actions not considered).

3. Designing a separate system capable of removing reactor decay heat.

None of these apparent remedies would be easy or inexpensive. However, it is apparent from the dominant sequences that no significant reduction in the core melt frequency will occur without some change that reduces the probability of DHR failure.

8.4.4 HPCI and RCIC Unavailabilities. The dominant contributors to the unavailabilities of the HPCI and RCIC systems are the rupture disks. Although only two of the dominant sequences involve failures of the HPCI or RCIC systems, this failure mode is significant for another reason.

The rupture disks were installed as a backup to the normal turbine trip features to prevent turbine damage due to high exhaust pressure. In order to damage the system in this manner, two failures must occur: a flow blockage in the exhaust line and failure of the turbine to isolate on a high exhaust line pressure signal. Under these conditions, the rupture disks are designed to break to provide a depressurization path for the exhaust line.

It appears as if the designers recognized the potential for system failure if one rupture disk were to fail prematurely. Therefore, two disks in series were provided. Then, as a means of verifying disk integrity, a pressure detector was located between the disks. This detector was used to generate a turbine isolation signal upon failure of the first disk as an added safety precaution.

Routine operation and testing of these systems often leads to fatigue failure of the first rupture disk and subsequent turbine isolation. Therefore, the condition currently exists where a backup equipment protection feature (which is not even required until two other independent failures have occurred) is spuriously isolating a front-line system when no such isolation is necessary. In addition, this spurious isolation constitutes the dominant failure mode for these two systems.

For the HPCI system, an additional 25% of that system's unavailability is due to required testing. This particular value is significantly higher than the testing and maintenance contribution of any other system analyzed. The relatively high HPCI unavailability (compared to other front-line systems) makes the testing contribution even more significant. It appears that the testing schedule and the testing effect on system operability should be reviewed to ensure that the optimum reliability is being achieved.

8.4.5 EECW Unavailability During a Loss of Offsite Power. Under most transient and LOCA sequences, the EECW unavailability is not a significant contributor to the core melt frequency. However, under LOSP conditions, EECW failure contributes significantly as a common mode failure of all the diesel generators and, therefore, all AC powered systems.

There are three dominant sequences where EECW failure contributes to mitigating systems unavailabilities. As noted in the sensitivity analysis and the sequence evaluations in Appendix C, EECW failures do not contribute significantly to the dominant sequences when recovery factors are considered. EECW recovery actions essentially consist of providing additional EECW flow from standby pumps via cross-connect piping. In the event that flow from three of the four EECW pumps is not available, the operator can readily align the RHRSW C1 or C2 pump to the EECW north supply header by opening a motor-operated flow control valve (FCV-67-49) from the main control room.

However, it would appear to be a better engineering practice not to rely on the recoverability of the EECW systems as a means of minimizing its impact on these sequence frequencies. Instead, methods of minimizing its impact without considering later recovery would seem to be more judicious. It appears that sectionalizing the headers and/or aligning more pumps to automatically supply the EECW headers are among the most likely candidates for such an effort. The D pumps can be aligned to the EECW south supply header by opening a motor-operated valve (FCV-67-48); however, the technical specifications require that at least one of the D1 or D2 pumps be available as the SBCS system pump. In order to use the D1 pump for EECW supply, the discharge header cross-connect valve (563) would have to be closed. This

valve is a normally open manual valve remotely located at the pumping station. By keeping the valve (563) closed, the RHRSW D1 pump could be used for EECW supply and the D2 pump could be used for RHRSW or SBCS if needed.

8.5 Uncertainty Analysis

Uncertainty analyses were performed on the dominant accident sequences. The MOCARS computer code¹⁸ was used to perform a Monte Carlo simulation of system unavailabilities based on basic event information and the system cut sets. The lognormal distribution was used as the distribution for each basic event and for the initiating events. The resulting system distributions were then combined and analyzed to produce the sequence values. Error factors were obtained by dividing the value of the distribution at the 95% quantile by the point estimate. The analyses included MOCARS runs on the initial and final sequence frequencies. The sum of the initial sequence frequencies and the sum of the final sequence frequencies were also analyzed. Table 15 summarizes the analysis results.

Appendix C presents insights on the uncertainty analysis in detail. The following list summarizes the major points.

1. A relatively high error factor of 10 was used for control circuit faults since their unavailability estimates were based on generic models. A MOCARS evaluation of the generic control circuit model substantiated the conservative nature of this assumption. Since control circuit faults have a dominant effect on torus cooling and shutdown cooling, this conservatism is largely responsible for the high error factors in some of the sequences.
2. The uncertainty after recovery is about a factor of 2 less than that before recovery in spite of the conservative control circuit error factor. Control circuit faults are considered to be recoverable when there is enough time (a) to repair or bypass the control circuits, (b) to

Table 15. Dominant sequence uncertainties

<u>Sequence Designator</u>	<u>Initial Frequency</u>	<u>Error Factor</u>	<u>Final Frequency</u>	<u>Error Factor</u>
T _U R _B R _A	1.3 x 10 ⁻⁴	20.5	9.7 x 10 ⁻⁵	8.7
T _U B	5.1 x 10 ⁻⁵	5.0	5.1 x 10 ⁻⁵	5.0
T _P R _B R _A	1.5 x 10 ⁻³	5.6	2.8 x 10 ⁻⁵	2.8
T _K R _B R _A	1.2 x 10 ⁻⁵	21.5	9.3 x 10 ⁻⁶	9.0
T _U Q _R B _R A	5.5 x 10 ⁻⁶	36.3	4.1 x 10 ⁻⁶	15.3
T _A BM	3.7 x 10 ⁻⁶	4.6	3.7 x 10 ⁻⁶	4.6
T _P K _R B _R A	8.3 x 10 ⁻⁵	6.7	1.6 x 10 ⁻⁶	2.8
T _P Q _R B _R A	6.2 x 10 ⁻⁵	10.7	1.2 x 10 ⁻⁶	4.7
Total	1.9 x 10 ⁻³	5.8	2.0 x 10 ⁻⁴	5.6

manually operate a valve, or (c) to valve in another pump, as is the case with long-term decay heat removal. Thus, it is not surprising that the final sequence error factors, like the frequencies themselves, reflect the decreased dependence on control circuit faults after considering recovery.

3. Despite the fact that some sequences have relatively high error factors, their effect on the cumulative frequency error factor is relatively modest.
4. The cumulative frequency error factors before and after recovery are about the same, indicating that the cumulative frequency error factor is not significantly affected by recovery factors nor by the wide error spread of a few sequences.

8.6 Sensitivity Analysis

After selection of the dominant sequences and evaluation of the uncertainties associated with each, it is important to examine the assumptions and uncertainties that went into the original values. A sensitivity analysis can aid in understanding the contributors to dominant sequence frequencies. The method of performing such an analysis is to identify potential uncertainties and recalculate the sequence frequencies to show how much variations in that input parameter changes the final value.

Review of the dominant sequences revealed several areas where a sensitivity analysis would be desirable. These areas are summarized below.

1. The RHR trees assumed that failure of the minimum-flow bypass valves to close would disable the RHR loops. Since about 90% of the flow per loop would not be diverted by such a failure, what would be the effect on sequence frequency if such failures did not disable the RHR loops?
2. For the LOSP initiated sequences, failure of EECW was an important contributor to the sequence frequencies. The analysis assumed that three of four pumps were needed to supply adequate cooling. Since two of four pumps provides up to 91% of the necessary cooling, what change to the sequence frequency would occur if the EECW model were changed to require only two of four pumps for successful cooling?
3. The transient-induced LOCA initiator frequencies were derived from the transient systemic event trees using the WASH-1400 failure data for relief valves. What would be the change in these sequences if the generic SORV frequency from EPRI NP-801 were used instead?
4. Unavailabilities for valve and pump control circuits were based on analysis of typical systems. A more detailed analysis of the corresponding systems would be possible. In particular, what would be the effect of modeling differences between AC- and DC-powered valve control circuits and of modeling the effect of 4160 V AC rather than 480 V AC motor control circuits?

The methodology for this analysis was to replace the changed event(s) in the event or fault trees with the new value and reevaluate the sequence frequency. The results of the three analyses were that

1. Removal of the minimum bypass valve faults reduced the initial frequency by a factor of only 3.8 but reduced the final frequency of the affected sequences by a factor of 22. This is because many of the minimum-flow bypass valve faults are not recoverable, while many of the other faults of the shutdown cooling and torus cooling systems are recoverable.

2. Changing EECW success criteria from three of four to two of four pumps reduced the initial sequence frequency for affected sequences by a factor of 1.6 but had no significant effect on the final frequencies.
3. Plant-specific SORV frequencies would increase the affected sequences by a factor of approximately 6.0. Using generic frequencies (from General Electric plants) produced results comparable to those from the event trees (about 0.25 increase).
4. For both the generic control circuits analyzed, the differences in power assumptions do not have a significant influence on system unavailabilities.

Section 6 of Appendix C provides additional detail on these analyses.

8.7 Limitations of the IREP Methodology and Uses of the Models

The quantitative results of this IREP study must be viewed and used with a thorough understanding of the limitations of the methodology used. As previously identified, this is principally a reliability study. While inferences regarding risk-dominant accident sequences can be obtained from the analysis, a detailed risk analysis was not performed, nor was it intended. The analysis leading to the grouping of accident sequences into release categories relied heavily on previous studies performed on similar plants without extensive plant-specific analysis. Recognizing the inherent uncertainties in this type of categorization, the information generated was not used as an input to a calculation of consequence distribution. External events such as earthquakes, fires, floods, and other influences from without were not considered. Thus, the quantitative results must be regarded as being incomplete from a risk point of view.

In utilizing the results of this study, the following limitations should be recognized:

1. The generic data base used in the quantification analyses was very similar to the WASH-1400 data base (although with larger error bounds), with some modifications resulting from limited analyses of licensee event report (LER) submittals. Plant-specific data was utilized when the analyst found it different from the generic base. However, the detailed comprehensive examination of plant logs necessary to fully evaluate in-plant data was not performed.
2. Human performance was modeled using the techniques described in NUREG/CR-1278. However, the systematic bias in human response (either positive or negative) that may result because of morale or management practices was not included. In addition, human acts of commission were, in general, not included in the analysis.
3. An attempt was made to couple the root cause of the initiating event with system faults in analyzing accident sequences. The technique used is believed to be reasonably efficient to identify single failures that may initiate a transient and degrade the performance of one or more safety systems. However, multiple fault scenarios of this type may have been omitted.
4. Coupling of faults associated with design, fabrication, or environmental conditions was not treated explicitly.

There were also several assumptions made throughout the analysis regarding the depth of analysis that could influence the results. In many cases, these assumptions were made based on judgement that further modeling was not probabilistically important. The depth of the analysis in many ways defines the level of interactions or dependencies considered and, while we believe the assumptions made are valid, the possibility exists that additional dependencies might be identified with further analysis. Examples of the type of assumptions made include: (a) including only those single passive failures that can fail an entire

system, and (b) ignoring misposition faults for valves that automatically are commanded to the proper position by the engineered safety features actuation system and for valves that have position indicated in the control room and are monitored each shift using a checkoff procedure.

The incompleteness and subjectivity associated with the aforementioned topics does not invalidate the analysis performed. The important product of this project is the framework of engineering logic generated in constructing the models, not the precise numbers resulting from the mathematical manipulations of these models.

The patterns, ranges, and relative behaviors that are obtained can be used to develop insights into the design and operation of a plant that can only be gained from an integrated consistent approach such as this IREP analysis. These insights are applicable to utility and regulatory decision making, although they should not be the sole basis for such decisions. By comparative evaluations, those features of the plant that are predicted to have a more significant influence on risk can be identified and utility and regulatory efforts can be focused on them to determine if they are acceptable. Similarly, regulatory efforts addressed to items having an insignificant influence on predicted risk should also be evaluated. The ranking of risk dominant accident sequences provides a framework for future value-impact analysis of potential plant modifications.

8.8 Application of Results

The general views regarding the usefulness of the IREP analyses expressed above suggest several concrete applications that can be made. They are presented below in the form of suggestions to utilities for applications of the results. In many cases, the models may have to be modified somewhat to achieve the various goals. However, we have attempted to construct them in such a manner as to minimize the difficulty associated with such use. It is desirable for these models to be maintained in a current status and used as tools in operations management. Specific suggestions for utilities and regulators are discussed below:

Operator Training and Simulator Design. The IREP study generated a catalog of severe accident sequences, with rough assessments of the likelihood, severity, and principal root causes of each. Some of these could be included in operator training and simulator design. This information can also be used as a starting point for further studies intended to assess the similarity of the symptom profile among accidents requiring different operator response and to survey the hazards associated with misdiagnosis or less-than-optimum recovery actions. A natural follow-up is an assessment of the adequacy of instrumentation and status monitoring equipment.

Emergency Planning. The catalog of accident sequences and the likelihood estimates emerging from this IREP study can be used to train emergency response personnel in what to expect. IREP results can also serve as a basis to improve the set of symptoms to be used as trigger points for the declaration of site or general emergencies, and they can be used in developing guides on the diagnosis and prognosis of accidents as they develop.

Adequacy of Procedures. It is common in studies, such as the IREP studies, to discover a few instances in which emergency procedures or maintenance procedures should be improved and which are of prime importance to the accident susceptibility of the plant. The results herein should be studied to determine if this is the case here. Beyond these lessons, the IREP models can be used to measure the importance of individual procedures to safety and to explore the risk associated with errors in following procedures.

Adequacy of Limiting Conditions of Operation. An IREP study provides the tools with which to optimize allowable outage times and surveillance intervals. The IREP models can also be used in evaluating requests from utilities to continue power generation when equipment is out of service beyond their specified allowable outage times.

Systems Integration Reviews. An IREP study is designed to model explicit functional dependencies among systems. It is not uncommon to discover that an auxiliary system is a weak link with respect to reliability in such a manner that it governs plant risk. This IREP study provides visibility for recognizing the following system dependencies: hard-wired systems interactions, human behavior that can couple the unavailability of several safety systems, and the importance of auxiliary systems to safety. Although such findings are not complete or precise, they represent a vast improvement on safety analyses done to date.

Significance of Component Reliability. The IREP models can be used to develop quantitative measures of importance to safety for the reliability of components, trains, whole systems, and classes of accident sequences. These methods enable the use of cost-benefit analyses on reliability improvements for components, and the more discriminating use of the more expensive qualification or in-service inspection techniques.

System Reliability. Estimates of system reliability are produced in an IREP study. Quantitative measures of the importance of system components can be calculated from the IREP models and the more likely failure modes that are believed to dominate the unavailability of these systems can be identified. With this information one can assess the possibility that a failed system could be repaired before its failure reaches a point of no return under accident conditions. Operators can be trained in fault diagnosis and in quick fixes. The adequacy of diagnostic instrumentation and status monitoring can be assessed. Surveillance practices can be altered to improve the availability of particularly critical systems.

Accident Sequences. In addition to identifying accident sequences and estimating their frequency, the IREP models can also serve as a test-bed with which to explore the effects of changes in design or operations practices. Possible improvements may be obvious in light of the results. In other cases, the effectiveness of hypothetical improvements can be assessed (within the limits of the completeness of the models). A particularly valuable use of these models lies in the evaluation of risks associated with changes, i.e., will a fix for one safety problem make different accident sequences more likely? The IREP study results provide a tool that can be used to address such questions.

Evaluation of Operating Occurrences. The IREP models and results can be used to evaluate whether a fault occurring in plant operation or testing was a precursor of a more serious event, and to evaluate its importance. One can explore each of the classes of severe accident sequences for the role that might have been played by the precursor. In addition, patterns of licensee-reported events or trends can be assessed for risk significance with the IREP models.

Validation of IREP Analyses. The occurrence of faults or errors in the operation or testing of the plant can be used to update, validate, or improve the completeness or accuracy of the IREP models and the projected failure frequencies. Doing so has the dual advantage of improving the IREP model for its many other uses as well as assessing the safety significance of the operating experience.

Design Errors and Generic Safety Issues. There are several classes of safety problems in reactor plants that IREP studies do not analyze. Among these are susceptibility to fires, floods, sabotage, earthquakes, design or installation errors that are not revealed by the explicitly known, hard-wired functional dependencies among systems, and effects assumed to be negligible in the IREP study, such as the role of snubber failures. However, the models generated in IREP can be used to put such concerns into perspective once the concern has been explicitly postulated. For example, one can use IREP to assess which accident sequences might be affected by the postulated safety issue and estimate at what level of severity the deficiency, if any, might emerge (from the background of minor contributors to risk) into one of the dominant concerns. Thus, IREP can be useful even in contexts in which its predictive power is poor.

It should be noted that none of the uses suggested above depend upon the predictions of risk. They all depend upon measures of importance and upon the kind of accident sequences to which the subject plant is susceptible.

Some of the applications are sensitive to the limitations of the study, particularly in completeness and quantitative accuracy. Nonetheless, the applications can be tailored to the known limitations and the models can provide a coherent framework to address the "what if" questions concerning its accuracy in these applications.

The suggested applications of the models in this report do not require a precise analysis of the phenomenology of reactor accidents. Phenomenological analyses, etc., need only be good enough to develop the general forms of the accident processes, although there are rare occasions when uncertainties in the modeling of accident processes can make large differences in the course or consequences of reactor accidents.

In general, formal, plant-specific consequence analysis is unnecessary for these applications. It is useful to identify accident sequences, their associated release categories, and to do emergency planning using this information.

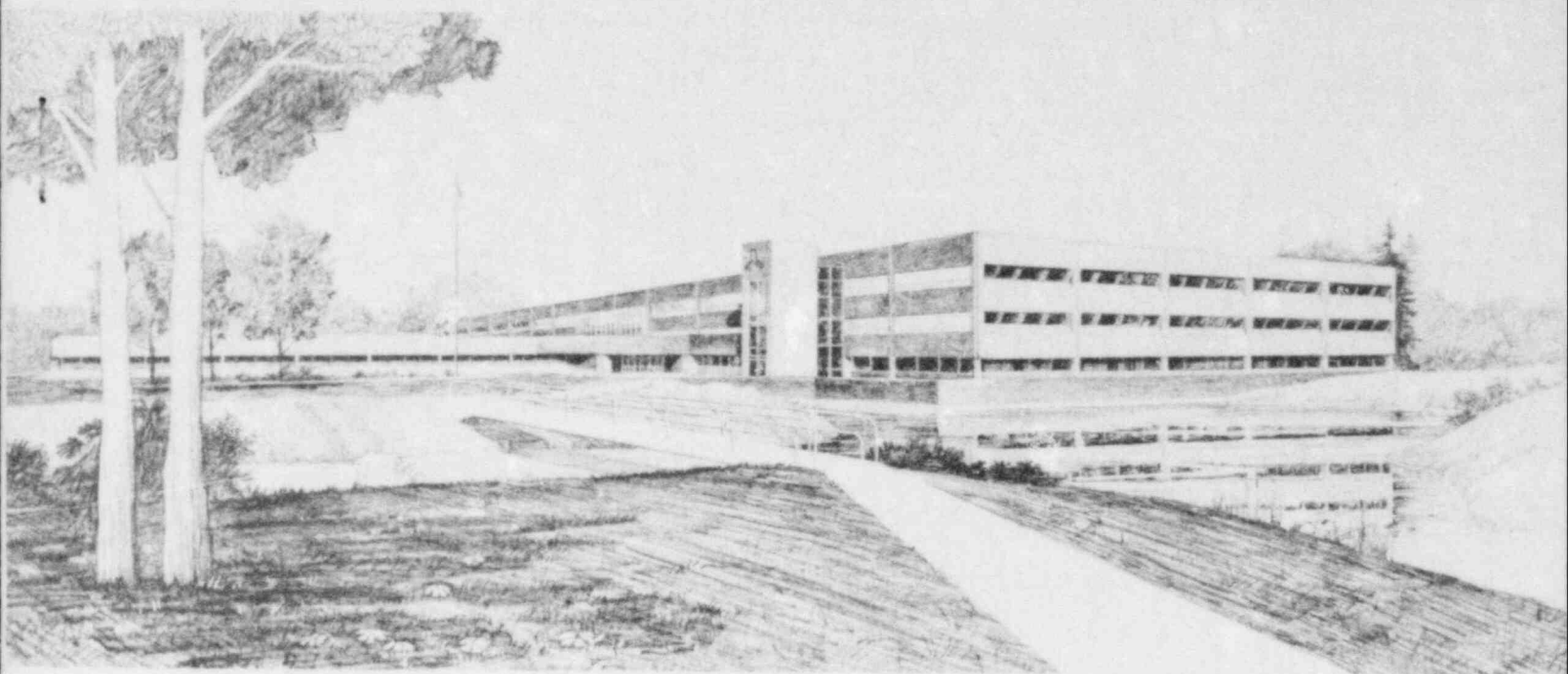
It is hoped that studies similar to this IREP analysis will be a means by which safety issues can be mutually understood by the NRC and the licensees. The methods employed in the IREP studies provide a systematic way of identifying safety issues and putting these issues into proper perspective, and at the same time improve the cost-effectiveness and risk-relevance of NRC regulatory initiatives.

REFERENCES

1. *NRC Action Plan Developed as a Result of the TMI-2 Accident*, NUREG-0660, Rev. 1, August 1980, Section II.C.
2. *Reactor Safety Study—An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*, WASH-1400 (NUREG-75/014), October 1975.
3. *Anticipated Transients without Scram, Vol. 1*, NUREG-0460, April 1978, p. 28.
4. A. A. Garcia, R. T. Liner, P. J. Amico, and E. V. Lofgren, *Crystal River-3 Safety Study*, NUREG/CR-2515, SAND81-7229/1, Science Applications, Inc., December 1981.
5. D. D. Carlson, *Interim Reliability Evaluation Program Phase II, Procedures Guide*, NUREG/CR-2728, SAND82-1100, Sandia National Laboratories, to be published.
6. *Browns Ferry Nuclear Plant Final Safety Analysis Report*, NRC Docket 50-259, Tennessee Valley Authority, September 1970.
7. F. L. Leverenz, Jr., J. M. Koren, R. C. Erdmann, and G. S. Lellouche, *ATWS: A Reappraisal, Part II: Frequency of Anticipated Transients*, EPRI NP-801, Electric Power Research Institute, June 1978.
8. A. D. Swain and H. E. Guttman, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, October 1980.
9. *Licensee Event Reports, Output of Browns Ferry 1, 2, and 3 Events from 1969 to Sept. 1980*, Tennessee Valley Authority, September 1980.
10. *ASME Boiler and Pressure Vessel Code*, Section XI, "Rules for Inservice Inspection of Nuclear Power Plant Components," Subsection IWV, Division 1, ASME, July 1980.
11. *Reporting Procedures Manual for the Nuclear Plant Reliability Data System*, NPRDS Manual No. 270, Southwest Research Institute, December 1979.
12. M. E. Stewart, "Interim Reliability Evaluation Program, Browns Ferry Fault Trees," *International ANS/ENS Topical Meeting on Probabilistic Risk Assessment, Port Chester, NY, September 20-24, 1981*, Log No. VIII.7.
13. N. H. Marshall, et al., *User's Guide for the Reliability Analysis System (RAS)*, TREE-1168, EG&G Idaho, September 1977.
14. N. H. Marshall, et al., *COMCAN II: A Computer Program for Common Cause Failure Analysis*, TREE-1289, EG&G Idaho, September 1978.
15. *Browns Ferry Nuclear Plant Final Safety Analysis Report*, NRC Docket 50-259, Tennessee Valley Authority, September 1970, Appendix Q, Question 4.8.
16. R. O. Wooten and H. I. Avci, *MARCH (Meltdown Accident Response Characteristics) Code Description and User's Manual*, NUREG/CR-1711, BMI-2064, Battelle-Columbus Laboratories, October 1980.

17. R. J. Burian and P. Cybulskis, *CORRAL 2 User's Manual*, Battelle-Columbus Laboratories, January 1977.
18. S. D. Matthews and J. P. Poloski, *MOCARS: A Monte Carlo Code for Determining Distribution and Simulation Limits and Ranking System Components by Importance*, TREE-1138, Rev. 1, EG&G Idaho, August 1978.

EG&G Idaho, Inc.
P.O. Box 1625
Idaho Falls, Idaho 83415



U.S. Department of Energy

Idaho Operations Office • Idaho National Engineering Laboratory

Interim Reliability Evaluation Program: Analysis of the Browns Ferry, Unit 1, Nuclear Plant

Appendix A—Event Trees

EG&G Idaho, Inc.

S. E. Mays
J. P. Poloski
W. H. Sullivan
J. E. Trainer

July 1982

Energy Incorporated, Seattle Office

R. C. Bertucio
T. J. Leahy

Prepared for the
U.S. Nuclear Regulatory Commission
Under Sandia National Laboratories
Purchase Order No. 62-7776

 **EG&G** Idaho

8209270446

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, nor 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

**INTERIM RELIABILITY EVALUATION PROGRAM:
ANALYSIS OF THE BROWNS FERRY,
UNIT 1, NUCLEAR PLANT**

APPENDIX A—EVENT TREES

EG&G Idaho, Inc.

S. E. Mays
J. P. Poloski
W. H. Sullivan
J. E. Trainer

Energy Incorporated, Seattle Office

R. C. Bertucio
T. J. Leahy

Published July 1982

EG&G Idaho, Inc.
Idaho Falls, Idaho 83415

Prepared for the
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
Under Sandia National Laboratories
Purchase Order No. 62-7776
FIN No. A1241

FOREWORD

This report describes a risk study of the Browns Ferry, Unit 1, nuclear plant. The study is one of four such studies sponsored by the NRC Office of Research, Division of Risk Assessment, as part of its Interim Reliability Evaluation Program (IREP), Phase II. Other studies include evaluations of Arkansas One, Unit 1, by Sandia National Laboratories; Calvert Cliffs, Unit 1, by Science Applications, Inc.; and Millstone, Unit 1, by Science Applications, Inc. EG&G Idaho, Inc. was assisted by Energy Inc., Seattle, in its evaluation of the Browns Ferry, Unit 1, plant. Battelle-Columbus Laboratories provided information regarding the fission product releases that result from risk-significant accident scenarios. Sandia National Laboratories has overall project management responsibility for the IREP studies. It also has responsibility for the development of uniform probabilistic risk assessment procedures for use on future studies by the nuclear industry.

This report is contained in four volumes: a main report and three appendixes. The main report provides a summary of the engineering insights acquired in doing the study and a discussion regarding the accident sequences that dominate the risks of Browns Ferry, Unit 1. It also describes the study methods and their limitations, the Browns Ferry plant and its systems, the identification of accidents, the contributors to those accidents, and the estimating of accident occurrence probabilities. Appendix A provides supporting material for the identification of accidents and the development of logic models, or event trees, that describe the Browns Ferry accidents. Appendix B provides a description of Browns Ferry, Unit 1, plant systems and the failure evaluation of those systems as they apply to accidents at Browns Ferry. Appendix C generally describes the methods used to estimate accident sequence frequency values.

Numerous acronyms are used in the study report. For each volume of the report, these acronyms are defined in a listing immediately following the table of contents.

CONTENTS

FOREWORD	A-ii
NOMENCLATURE	A-v
1. FRONT-LINE AND SUPPORT SYSTEMS	A-1
2. INITIATING EVENT INVESTIGATIONS	A-7
2.1 LOCA Initiators	A-7
2.2 Transient Initiators	A-9
2.3 Initiator Effects On Mitigating Systems	A-15
3. LOCA AND TRANSIENT SYSTEMIC EVENT TREES	A-38
3.1 LOCA Systemic Event Trees	A-38
3.2 Transient Systemic Event Tree Description	A-53
4. SEQUENCE DEPENDENT OPERATOR ACTIONS	A-59
4.1 Introduction	A-59
4.2 System/Sequence Operator Actions	A-59
5. REFERENCES	A-63

FIGURES

A-1. Causal failure diagram for MSIV closure	A-31
A-2. Causal failure diagram for loss of condenser vacuum	A-32
A-3. Causal failure diagram for loss of feedwater	A-33
A-4. Causal failure diagram for generator load reject	A-34
A-5. Causal failure diagram for turbine trip	A-34
A-6. Causal failure diagram for turbine trip without bypass	A-34
A-7. Causal failure diagram for closure one MSIV	A-35
A-8. LOCA systemic event tree for large liquid break, suction-side of recirculation pumps (L _S)	A-39
A-9. LOCA systemic event tree for large liquid break, discharge-side of recirculation pumps (L _D)	A-40

A-10. LOCA systemic event tree for large steam break (L_L)	A-41
A-11. LOCA systemic event tree for intermediate liquid break (I_L)	A-42
A-12. LOCA systemic event tree for intermediate steam break (I_V)	A-43
A-13. LOCA systemic event tree for small liquid-line or steam-line break (S)	A-44
A-14. Transient systemic event tree where PCS is unavailable (T_U)	A-54
A-15. Transient systemic event tree where PCS is available (T_A)	A-55

TABLES

A-1. Front-line systems versus support systems.....	A-2
A-2. LOCA mitigation success criteria	A-3
A-3. Transient mitigation success criteria	A-6
A-4. LOCA pipe rupture frequencies	A-7
A-5. Transient initiator categories	A-9
A-6. Transient initiator groupings and frequencies	A-14
A-7. LOCA initiator effects on mitigation systems	A-17
A-8. Electrical equipment failure summary	A-18
A-9. Electrical equipment failure chart details	A-22
A-10. Cooling water failure chart	A-30
A-11. Event tree legend	A-45
A-12. Front-line systems legend	A-46

NOMENCLATURE

\bar{A}	The complement of A (a success event if A is a failure event). (\bar{A} may also be used to mean "unavailability.")
A	Alarm
AC	Alternating current
ACC	Accumulator
ADS	Automatic depressurization system
AH	Alarm-high
AO	Air operator
APRM	Average power range monitor
AT	Anticipated transient
ATWS	Anticipated transient without scram
Bf1	Browns Ferry, Unit 1, nuclear plant
BI	Break isolation
BWR	Boiling water reactor
CAD	Containment atmosphere dilution
CCW	Condenser circulating water
CD	Complete dependence
CE	Conductivity element
CIS	Containment isolation system
Clg	Cooling
COND	Main condenser
CR-3	Crystal River, Unit 3, nuclear plant IREP study
CRD	Control rod drive
CRDH	Control rod drive hydraulic
CRDHS	Control rod drive hydraulic system
CRW	Clean rad waste
CS	Core spray
CS&T	Condensate storage and transfer
CSCS	Core standby cooling system
CSS	Core spray system
CST	Condensate storage tank
CV	Control valve
D	Demand
DC	Direct current
DEP	Depressurization
DG	Diesel generator
DHR	Decay heat removal
Diff	Different
DPI	Differential pressure indicator
DPIS	Differential pressure indicating switch
DPS	Differential pressure switch
DPT	Differential pressure transmitter
EAC	Equipment area cooling
EGCS	Emergency core cooling system
ECI	Emergency coolant injection
EECW	Emergency equipment cooling water
EHC	Electro-hydraulic control

EMI	Electrical Maintenance Instruction
EOI	Equipment Operating Instructions
EPRI	Electric Power Research Institute
EPS	Electrical power system
ESFAS	Engineered safety features actuation system
F(•)	Frequency of initiator in parentheses
FCV	Flow control valve
FE	Flow element
FI	Flow indicator
FIC	Flow indicating controller
FLS	Front-line system
FMEA	Failure mode effects analysis
FR	Flow recorder
FS	Flow switch
FSAR	Final Safety Analysis Report
FT	Flow transmitter
FWC	Feedwater control
FWCS	Feedwater control system
G	Green
GOI	General Operating Instructions
H	High
H/L	High/low
HCU	Hydraulic control unit
HCV	Hand control valve
HEP	Human error probability
HPCI	High pressure coolant injection
HPCS	High pressure core spray
HPI	High pressure injection
HS	Handswitch
HSS	High speed stop
HVAC	Heating, ventilation, and airconditioning
HX	Heat exchanger
I&C	Instrumentation and control
I&E	Inspection and enforcement
IMI	Instrument Maintenance Instruction
INJ	Injection
IREP	Interim Reliability Evaluation Program
IRM	Intermediate range monitor
L	Low
LA	Level alarm
LD	Low dependence
LER	Licensee Event Report
LIC	Level indicating controller
LIS	Level indicating switch
LL	Low-low
LOCA	Loss of coolant accident
LOSP	Loss of offsite power
LPCI	Low pressure coolant injection
LPI	Low pressure injection

LS	Limit switch
LSS	Low speed stop
LT	Level transmitter
M	Motor (operated valve)
MCR	Main control room
MD	Moderate dependence
MGU	Master governor unit
MMG	Motor generator
MMI	Mechanical Maintenance Instruction
MO	Motor operated
MOV	Motor-operated valve
MSC	Manual speed control
MSI	Main steam isolation
MSIV	Main steam isolation valve
MSL	Main steam line
NA; N/A	Not applicable
NC	Normally closed
NMS	Neutron monitoring system
NO	Normally open
OI	Operating Instructions
OL	Overload
OP	Overpressure protection
OP(C)	Overpressure protection (relief valves closed)
OP(O)	Overpressure protection (relief valves open)
PA	Pressure alarm
PB	Pipe break
PCIS	Primary containment isolation system
PCS	Power conversion system
PCV	Pressure control valve
PG	IREP Procedure Guide
PI	Pressure indicator
PORV	Power-operated relief valve
PRA	Probabilistic risk assessment
PS	Pressure switch
PSCWT	Pressure suppression chamber water transfer
PT	Pressure transmitter
PWR	Pressurized water reactor
Q(•)	Unavailability of system in parentheses
QA	Quality assurance
R	Red
RBCCW	Reactor building component cooling water
RBEDT	Reactor building equipment drain tank
RCB	Reactor coolant boundary
RCIC	Reactor core isolation cooling
RCS	Reactor coolant system
RCW	Raw cooling water
RCWS	Raw cooling water system
Recirc	Recirculation

RFP Reactor feed pump
 RFPT Reactor feed pump turbine
 RFWPT Reactor feedwater pump turbine
 RHR Residual heat removal
 RHRSW Residual heat removal service water
 RMOV Reactor motor-operated valve
 RMS Remote manual switch
 RPS Reactor protection system
 RPT Recirculation pump trip
 RS Reactor subcriticality; reactor shutdown; reactor scram
 RV(C) Relief valve (closed)
 RV(O) Relief valve (open)
 RWCU Reactor water cleanup
 RX Reactor

S/D Shutdown
 S/RV Safety relief valve
 S/V Safety valve
 SBSCS Standby coolant supply
 SBGT Standby gas treatment
 SCI Short-term containment integrity
 SD-BD Shutdown board
 SDV Scram discharge volume
 SIV Scram instrument volume
 SJAE Steam jet air ejector
 SLCS Standby liquid control system
 SORV Stuck-open relief valve
 SRM Source range monitor

TA Temperature alarm
 TCV Turbine control valve
 TD Time delay
 TDC Time delay contact
 TDPU Time delay pickup
 TE Temperature element
 TIP Traversing in-core probe
 TMI Three Mile Island
 TR Temperature recorder
 Trans Transient
 TS Technical Specifications; torque switch
 TVA Tennessee Valley Authority

UV Undervoltage

V Volts
 VB Vacuum breaker
 VO Valve open
 VS Vapor suppression
 VSS Vapor suppression system
 VWI Vessel water inventory

ε An insignificant quantity, generally less than 10^{-8}

INTERIM RELIABILITY EVALUATION PROGRAM:
ANALYSIS OF THE BROWNS FERRY, UNIT 1, NUCLEAR PLANT

APPENDIX A--EVENT TREES

1. FRONT-LINE AND SUPPORT SYSTEMS

One of the initial tasks undertaken in this study was that of front-line and support system identification. A front-line system is defined as a system whose function is necessary to successfully mitigate the effects of a loss-of-coolant accident (LOCA) or operational transient at BFl. A support system is defined as a system that affects the course of an accident or transient only by way of its effect on the operation of a front-line system.

This section contains a list of the front-line and support systems used in this study as well as a table of front-line system success criteria, i.e., minimum equipment needed for LOCA and transient mitigation. The front-line versus support system list is given in Table A-1. LOCA mitigation success criteria are given in Table A-2. Transient mitigation success criteria are given in Table A-3. Success is defined as the minimum equipment combinations needed for accident mitigation.

Front-line system response for a specific LOCA or transient mitigation is discussed in detail in Section 3. Detailed system functions and descriptions are contained in Appendix B, Section 1.

TABLE A-1. FRONT-LINE SYSTEMS VERSUS SUPPORT SYSTEMS

Front-Line Systems ^a	Support Systems									
	AC Power	DC Power	EAC ^b	EECW	RHRSW	RCW	Circulation Water	RPS	Keep- Full System	Operator
RCIC	--	X	--	--	--	--	--	--	--	--
RHR (shutdown cooling)	X	X	X	X	X	X	--	--	X	E01-74
RHR (LPCI)	X	X	--	--	--	--	--	--	X	--
RHR (torus cooling)	X	X	X	X	X	X	--	--	X	E01-74
RPT	--	X	--	--	--	--	--	X	--	--
HPCI	--	X	--	--	--	--	--	--	--	--
ADS	--	X	--	--	--	--	--	--	--	--
Core spray	X	X	--	--	--	--	--	--	X	--
SBCS	X	X	--	--	X	--	--	--	--	E01-74
PCS	X	X	--	--	--	X	X	--	--	E01-1,2,3
CRD	X	X	--	--	--	--	--	X	--	E01-85
Relief valves	--	X	--	--	--	--	--	--	--	E01-100-1
Vapor suppression	--	--	--	--	--	--	--	--	--	--
MSI	X	X	--	--	--	--	--	--	--	--

a. The front-line systems are given a one-letter name on the systemic event trees (see Table A-12).

b. Equipment area cooling.

TABLE A-2. LOCA MITIGATION SUCCESS CRITERIA

<u>Reactor Subcriticality</u>	<u>Short-Term Containment Integrity</u>	<u>Emergency Coolant Injection</u>	<u>Decay Heat Removal</u>
Large Break--Liquid Line--0.3 to 4.3 ft ² --Suction			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	Two core spray loops and two of four LPCI pumps or Four of four LPCI pumps	Two of four RHR pumps with associated heat exchangers in torus cooling mode or
or			
No more than five adjacent rods not fully inserted		One of two core spray loops and two of four LPCI pumps (one LPCI pump per injection loop)	One of four RHR pumps with associated heat exchangers in shutdown cooling mode
Large Break--Liquid Line--0.3 to 4.3 ft ² --Discharge			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	Two core spray loops or One of two core spray loops and one of two LPCI pumps on unaffected side	Two of four RHR pumps with associated heat exchangers in torus cooling mode or
or			
No more than five adjacent rods not fully inserted			One of four RHR pumps with associated heat exchangers in shutdown cooling mode

TABLE A-2. (continued)

<u>Reactor Subcriticality</u>	<u>Short-Term Containment Integrity</u>	<u>Emergency Coolant Injection</u>	<u>Decay Heat Removal</u>
Large Break--Steam Line--1.4 to 4.1 ft ²			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	Two core spray loops or Four of four LPCI pumps	Two of four RHR pumps with associated heat exchangers in torus cooling mode
or		or	or
No more than five adjacent rods not fully inserted		One of two core spray loops and one of four LPCI pumps	One of four RHR pumps with associated heat exchangers in shutdown cooling mode
Intermediate Break--Liquid Line--0.12 to 0.3 ft ²			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	One of one HPCI pump or Four of six ADS relief valves	Two of four RHR pumps with associated heat exchangers in torus cooling mode
or		and	or
No more than five adjacent rods not fully inserted		One of four LPCI pumps or One of two core spray loops	One of four RHR pumps with associated heat exchangers in shutdown cooling mode

TABLE A-2. (continued)

<u>Reactor Subcriticality</u>	<u>Short-Term Containment Integrity</u>	<u>Emergency Coolant Injection</u>	<u>Decay Heat Removal</u>
Intermediate Break--Steam Line--0.12 to 1.4 ft ²			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	One of one HPCI pump or One of four LPCI pumps	Two of four RHR pumps with associated heat exchangers in torus cooling mode or One of four RHR pumps with associated heat exchangers in shutdown cooling mode
or		or	
No more than five adjacent rods not fully inserted		One of two core spray loops	
Small Break--Liquid or Steam--Up to 0.12 ft ²			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	One of one HPCI pump or Four of six ADS relief valves and one of four LPCI pumps	Two of four RHR pumps with associated heat exchangers in torus cooling mode or One of four RHR pumps with associated heat exchangers in shutdown cooling mode
or		or	
No more than five adjacent rods not fully inserted		Four of six ADS relief valves and one of two core spray loops	

TABLE A-3. TRANSIENT MITIGATION SUCCESS CRITERIA

Anticipated Transient	Reactor Shutdown		Overpressure Protection			Vessel Water Inventory				DHR
	CRD	RPT	OP(O) ^a	OP(C) ^b	PCS	MSI	HPCI	DEP	INJ	RHR
Transients where PCS is available	No more than 30 rods fail to insert	Both recirculation pumps trip ^b	NA	All relief valves reclose ^c	Condenser available and Feed system providing makeup	MSIVs shut ^d	HPCI	Manual operation of at least four relief valves	One LPCI pump	Two RHR pumps and two heat exchangers in torus cooling mode
	or					or	or		One core spray loop	
	No more than five adjacent rods fail to insert					Turbine valves ^d and bypass valves shut	RCIC		or	One RHR pump and one heat exchanger in shutdown cooling mode
								One booster and one condensate pump	or	
								or		
								One RHRSW pump in SBCS mode		
Transients where PCS is unavailable	No more than 30 rods fail to insert		Direct scram 2 of 13 valves	All relief valves reclose	NA	MSIVs shut	HPCI	Manual operation of at least four relief valves	One LPCI pump	Two RHR pumps and two heat exchangers in torus cooling mode
	or		or		or	or	or			
	No more than five adjacent rods fail to insert		Flux scram 7 of 13 valves			Turbine valves and bypass valves shut	RCIC		One core spray loop	or
			Pressure scram 10 of 13 valves						or	One RHR pump and one heat exchanger in shutdown cooling mode
								One booster and one condensate pump ^e	or	
								or		
								One RHRSW pump in SBCS mode		

a. Relief valves open OP(O) and reclose OP(C).

b. If both recirculation pumps trip and PCS remains available, the resulting power level is such that the capacity of the bypass valves is adequate to remove the heat being generated.

c. Even though relief valve action is not required some relief valves will open.

d. MSI only necessary if PCS fails.

e. Although PCS is unavailable, the condensate system may still be operable.

2. INITIATING EVENT INVESTIGATIONS

This section describes how initiating events were identified for BFI and how frequency of occurrence values were derived for those accident initiators. It also describes special investigations to identify potential dependencies between the accident initiating events and the mitigating systems needed to cope with those initiators.

2.1 LOCA Initiators

The initiating event frequencies for the various LOCA pipe rupture sizes are listed in Table A-4. These initiating event frequencies for the various liquid and steam LOCA break sizes were derived by multiplying the probability for a given break size times the relative probability the break occurs in a specific portion of that size piping. It was assumed that within a given break range category (e.g., intermediate piping, 2 in. to 6 in.) the rupture was equally likely to occur in any of the piping, whether it be for liquids or steam.

TABLE A-4. LOCA PIPE RUPTURE FREQUENCIES

<u>Type</u>	<u>Size</u>	<u>Location</u>	<u>Frequency (per reactor-year)</u>
Liquid	Large	Suction side	9.9×10^{-6}
		Discharge side	3.9×10^{-5}
Steam	Large		5.2×10^{-5}
Liquid	Intermediate		9.0×10^{-5}
Steam	Intermediate		2.1×10^{-4}
Liquid or steam	Small		1.0×10^{-3}

Table III 6-9 of WASH-1400¹ provided the following median pipe rupture probabilities:

<u>Pipe Rupture Size</u>	<u>Piping Rupture Rate (per plant per year)</u>
Small	1×10^{-3}
Intermediate	3×10^{-4}
Large	1×10^{-4}

Differing success requirements for emergency coolant injection systems for types of liquid breaks (suction versus discharge) and steam breaks required that separate LOCA event trees be drawn. The above LOCA rates are not apportioned as to steam and liquid piping nor do they account for the suction versus discharge break effects. Thus, BFI piping isometrics for those systems that interface with the primary pressure boundary were examined to determine for a given break size:

1. What portion of the piping represented liquid versus steam.
2. For liquid breaks, what portion of the piping was a suction versus discharge side break.

The piping examination was not required for small LOCA piping since the small LOCA event tree was valid for liquid or steam breaks, and the ECI success criteria for both type breaks were the same. In addition, the piping was only considered up to the first valve that could isolate the break. As discussed in Section 5 of the main volume, breaks outside containment are relatively unimportant from a probability standpoint.

From the plant piping isometrics, it was determined that the length of liquid and steam piping susceptible to a large-size break is:

	<u>Length</u>	
	<u>Feet</u>	<u>Percent of Total Piping</u>
Liquid discharge	348.4	38.5
Liquid suction	89.3	9.9
Steam	<u>466.5</u>	<u>51.6</u>
Total	904.2	100.0

Thus, the probability for a large liquid break occurring on the discharge side of a recirculation pump was determined by multiplying the large pipe rupture rate times the relative probability the break occurs in the discharge piping:

$$(1 \times 10^{-4} \text{ per reactor-year})(38.5\%) = 3.9 \times 10^{-5} \text{ per reactor-year.}$$

Similarly, the suction-side break frequency was determined to be 9.9×10^{-6} per reactor-year, and the frequency of large steam breaks to be 5.2×10^{-5} per reactor-year.

The intermediate LOCA frequencies were calculated in the same manner with the exception that the large break liquid and steam piping lengths were added to the intermediate piping lengths since an intermediate size break (i.e., a partial break) can occur in the larger piping. The same rationale was applied to breaks in small piping.

2.2 Transient Initiators

Malfuncions, failures or faults in the mechanical/electrical systems that result in a demand for trip of the control rods (scram) and removal of heat from the reactor core are transient initiators. The transient initiators used in this analysis are referred to as events, that is, failures or faults in systems that result in a demand for trip of the control rods (scram) and removal of heat from the reactor core. Therefore, only those events that require a scram and have the potential of overheating the core were considered as valid transients. Transients that could possibly lead to LOCA were treated with an appropriate transfer to the LOCA event trees.

The transient initiators identified for this analysis were taken from EPRI NP-801.² Table A-5 defines these transient initiators. The LERS

TABLE A-5. TRANSIENT INITIATOR CATEGORIES

1. Electric load rejection	Occurs when electrical grid disturbances result in significant loss of load on the generator. Also included are intentional generator trips.
2. Electric load rejection with turbine bypass valve failure	Identical to Number 1 except that the turbine bypass valves do not open simultaneously with shutdown of the turbine.
3. Turbine trip	Occurs when any one of a number of turbine or nuclear system malfunctions requires the turbine to be shut down. Turbine trips that occur as a byproduct of other transients, such as loss of condenser vacuum or reactor high level trip, are not included. Intentional turbine trips are also included.
4. Turbine trip with turbine bypass valve failure	Identical to Number 3 except that the turbine bypass valves fail to open.
5. MSIV closure	Occurs when any one of various steam line and nuclear system malfunctions requires termination of steam flow from the vessel, or occurs by operator action.
6. Inadvertent closure of one MSIV	Occurs when only one MSIV closes (the rest remaining open) due to operator or equipment error.
7. Partial MSIV closure	Occurs when partial closure of one or more MSIVs results from a hardware or human error.

TABLE A-5. (continued)

8. Loss of normal condenser vacuum	Occurs when either a complete loss or decrease in condenser vacuum results from a hardware or human error.
9. Pressure regulator fails open	Occurs when either the controlling pressure regulator or backup regulator fails in an open direction. The failure causes a decreasing coolant inventory as the mass flow of water entering the vessel decreases.
10. Pressure regulator fails closed	Occurs when either the controlling pressure regulator or backup regulator fails in a closed direction. The failure causes increasing pressure and thus decreasing steam flow from the vessel.
11. Inadvertent opening of a safety/relief valve (stuck)	Occurs when a safety/relief valve sticks open. Due to an operator or equipment error, a single safety/relief valve can be opened, increasing steam flow from the vessel. If the valve cannot be closed, a scram is initiated. This transient includes only those openings that cannot be subsequently closed before a scram occurs.
12. Turbine bypass fails open	Occurs when equipment or operator error results in inadvertent or excessive opening of turbine bypass valves so as to decrease vessel level.
13. Turbine bypass or control valves cause increase pressure (closed)	Occurs when either operator error or equipment failure causes the turbine bypass or control valves to close, resulting in increased system pressure.
14. Recirculation control failure--increasing flow	Occurs when a failure of a flow controller, either in one loop or the master flow controller, causes an increasing flow in the core.
15. Recirculation control failure--decreasing flow	Occurs when any flow controller failure causes a decreased flow to the core.
16. Trip of one recirculation pump	Occurs when one recirculation pump trips due to a hardware or human error.
17. Trip of all recirculation pumps	Occurs with the simultaneous loss of all recirculation pumps.

TABLE A-5. (continued)

18. Abnormal startup of idle recirculation pump	Occurs when an idle recirculation pump is started at an improper power and flow condition. The increased flow could cause a flux spike, or core inlet subcooling, if the loop has been idle so as to allow coolant in the pump loop to cool.
19. Recirculation pump seizure	Occurs when the failure of a recirculation pump is such that no coastdown occurs and a sudden flow decrease ensues.
20. Feedwater--increasing flow at power	Occurs when any event causes increasing feedwater flow at power. Excluded (see Number 26) are increasing flow events during startup or shutdown when manual feedwater control is being used.
21. Loss of feedwater heater	Occurs when the loss of feedwater heating is such that the reactor vessel receives feedwater cool enough to exceed core scram parameters.
22. Loss of all feedwater flow	Occurs with the simultaneous loss of all main feedwater flow, excluding that due to loss of station power (see Number 31).
23. Trip of one feedwater pump (or condensate pump)	Occurs when the loss of one feedwater pump or condensate pump is such that a partial loss of feedwater occurs.
24. Feedwater--low flow	Occurs when any plant occurrence causes decreasing feedwater flow at power. Excluded are events at low power (see Number 25).
25. Low feedwater flow during startup or shutdown	Occurs when any event results in low feedwater flow at essentially zero power. This definition includes only startup or shutdown operations.
26. High feedwater flow during startup or shutdown	Occurs when excessive feedwater flow occurs during startup or shutdown. The reactor is essentially at zero power.
27. Rod withdrawal at power	Occurs when one or more rods are withdrawn inadvertently in the power range of plant operation.
28. High flux due to rod withdrawal at startup	Occurs when inadvertent withdrawal of a rod causes a local power increase.

TABLE A-5. (continued)

29. Inadvertent insertion of rod or rods	Occurs when any malfunction causes an inadvertent insertion of rod or rods during power operation.
30. Detected fault in reactor protection system	Occurs when a scram is initiated due to an indicated fault in the reactor protection system. An example is the indication of a high level in the scram discharge volume.
31. Loss of offsite power	Occurs when all power to the plant from external sources (the grid or dedicated transmission lines from other plants) is lost. This event requires the plant emergency power sources to be available.
32. Loss of auxiliary power (loss of auxiliary transformer)	Occurs when the loss of incoming power to the plant results from onsite failures such as the loss of an auxiliary transformer.
33. Inadvertent startup of HPCI/HPCS	Occurs when any of the systems inadvertently start up supplying high pressure cold water to the vessel. In general, a BWR will have either a HPCI system or a HPCS system.
34. Scram due to plant occurrences	Occurs when a scram, either automatic or manual, is initiated by an occurrence that does not cause an out-of-tolerance condition in the primary system, but requires shutdown. Examples are turbine vibration, off-gas explosion, fire, and excess conductivity of reactor coolant.
35. Spurious trip via instrumentation, RPS fault	Occurs when a scram resulting from hardware failure or human error in instrumentation or logic circuits occurs.
36. Manual scram--no out-of-tolerance condition	Occurs when a manual initiation of a scram, either purposely or by error, occurs and there are no out-of-tolerance conditions.
37. Cause unknown	Occurs when a scram occurs, but the cause is not determinable.

submitted for Browns Ferry were examined to identify those transient initiators not identified in EPRI NP-801. No other additional events were identified from this set of LERs. Each of the transient initiators pertaining to various electric power bus and cooling water system failures were further examined to identify transient initiator effects on front-line system availability. This analysis is described in Section 2.3.2. The transient initiators were grouped according to their effect on mitigating systems.

The transient initiators were subsequently grouped according to their effect on the PCS since this was the only mitigating system found to be affected by the transients. Seven of the 37 EPRI NP-801 events were classified as transient initiators that resulted in PCS being unavailable for mitigation of the transient. Of the remaining 30 events, 8 were identified as having no effect on PCS availability and 22 were considered not applicable for this study. Reasons for exclusion of these events are summarized in Table A-6, which lists the transient initiators and their frequencies.

One final consideration to the transient-type event was given in the case of the LOSP event. The LOSP event was originally grouped as a PCS-unavailable transient initiator. However, due to the dependency factor of this event with other mitigation systems, this particular event was treated separately in the transient event tree analysis.

The frequencies of the transient initiators were estimated using the techniques discussed in EPRI NP-801^a (see Table A-6). The transient frequencies were estimated based on the BFl-specific data and all pertinent BWR experience in EPRI NP-801. For this analysis, the plant-specific frequencies were used in the transient tree quantification.

To illustrate the method used to calculate the frequency of the various transient initiators used in this study, the electric load rejection event will be utilized. From EPRI NP-801, the expected frequency for the event is calculated according to a 40 year life of the reactor plant by the following formula:

$$E(\text{transient frequency}) = [\text{frequency of first year} + 39 \times (\text{remaining years average})] \div 40.$$

a. Data from EPRI NP-2230,³ a recent revision to EPRI NP-801, were not available in time for use in this study. NP-2230 data produce different results than those reported in EPRI NP-801 because of the inclusion of events occurring at BFl between January 1977 and April 1980 and, to a lesser extent, because of the omission of events occurring between October 1973 and August 1974 prior to commercial operation. In particular, a LOSP occurring at BFl in late 1978 early 1979 and reported in NP-2230 increases the estimated frequency of that event by a factor of nearly seven. NP-2230 estimates for other transients that cause the PCS to be unavailable are lower than those in EPRI NP-801, and estimates for those that keep it available (Group 2, Table C-6) are higher. However, the differences here involve factors of less than three, and thus do not have an appreciable effect on numerical results of this study.

TABLE A-6. TRANSIENT INITIATOR GROUPINGS AND FREQUENCIES

Transient	Frequency (events/year)	
	BFI	BWRs
<u>Group 1--Transients That Cause PCS to be Unavailable</u>		
a. MSIV closure.	0.58	0.24
b. Loss of normal condenser vacuum.	0.56	0.41
c. Pressure regulator fails open.	0.	0.25
d. Loss of feedwater flow.	0.51	0.17
e. Loss of offsite power.	0.03	0.11
f. Loss of auxiliary power.	0.	0.03
g. Increased feed flow at power.	<u>0.05</u>	<u>0.18</u>
Total	1.73	1.39
<u>Group 2--Transients That Do Not Cause PCS to be Unavailable</u>		
a. Electric load rejection.	1.02	0.74
b. Electric load rejection with bypass failure.	0.	0.
c. Turbine trip.	0.58	0.77
d. Turbine trip with bypass failure.	0.	0.
e. Inadvertent closure of one MSIV.	0.	0.10
f. Pressure regulator fails closed.	0.	0.11
g. Bypass/control valve fails causing pressure increase.	0.05	0.25
h. Recirculation control fails causing increased flow.	<u>0.03</u>	<u>0.10</u>
Total	1.68	2.07
<u>Group 3--Transients from EPRI NP-801 Not Applicable</u>		
a. Partial MSIV closure--partial failures not addressed since full closure is addressed above.		
b. Inadvertent open safety/relief valve (stuck)--considered in LOCA analysis.		
c. Recirculation control fails causing decreased flow--less severe than trip of all pumps (FSAR 14.5.5.3).		
d. Trip of one recirculation pump--less severe than trip of all pumps (FSAR 14.5.5.2).		
e. Trip of all recirculation pumps--no scram occurs (FSAR 14.5.5.3).		
f. Abnormal startup of recirculation pumps--no scram occurs (FSAR 14.5.6.2).		
g. Recirculation pump seizure--less severe than trip of all pumps (FSAR 14.5.5.4).		
h. Bypass valves fail open--mild transient, no scram occurs (FSAR Q14.5).		
i. Loss of feedwater heater--no scram occurs (FSAR 14.5.2.1).		
j. Trip of one feedwater pump--no scram occurs.		

TABLE A-6. (continued)

Transient	Frequency (events/year)	
	BFl	BWRs
<u>Group 3 (continued)</u>		
k. Low feedwater flow--less severe than loss of feed flow.		
l. Low feedwater flow during startup or shutdown--startup and shutdown transients not considered.		
m. High feedwater flow during startup or shutdown--same as above.		
n. Rod withdrawal at power--no scram occurs (FSAR 14.5.3.1).		
o. High flux rod withdrawal during startup--startup transients not considered.		
p. Inadvertent rod insertion--no scram occurs.		
q. Detected faults in reactor protection system--not applicable.		
r. Inadvertent HPCI initiation--less severe than increased feedwater flow at power.		
s. Scram due to plant occurrence--no challenge of reactor protection system.		
t. Spurious trip--no challenge of reactor protection system.		
u. Manual scram--no challenge of reactor protection system.		
v. Cause unknown--not applicable.		

The load rejection occurrences experienced at BFl during the first 4 years of operation are as follows:

<u>Year</u>	1	2	3	4
Occurrences	4	0	1	1

The number of occurrences for the fourth year is for only 1.3 months (0.11 year) of data. By the above formula, the expected frequency for electric load rejection event at BFl is calculated to be 1.02 events per reactor-year, that is:

$$E(\text{electric load rejection}) = [4 + 39 (2 \div 2.11)] \div 40 = 1.02 \text{ events per year.}$$

2.3 Initiator Effects On Mitigating Systems

In addition to identifying the initiating events, it is important to determine what effect the initiator may have on those systems designed to respond to the accident. In some cases, the initiating event may originate

in a mitigating system. The resulting accident sequence could be significant since the ability of the plant to cope with the accident has been degraded. The following sections discuss the LOCA and transient initiator effects on mitigating systems.

2.3.1 LOCA Effects On Mitigation

Some of the LOCA initiators have the potential to render LOCA mitigation systems partially or completely inoperable by virtue of the system location of the LOCA.

If a LOCA initiator could disable a mitigating system, the length of piping for the mitigating system susceptible to that LOCA was calculated using TVA supplied isometric drawings. Then, the total length of piping susceptible to that initiator was calculated. It was assumed that for a particular break size, the LOCA was equally likely to occur at any point on the piping susceptible to the LOCA.

Table A-7 provides a list of the systems lost and the percentage of their piping susceptible to a particular LOCA initiator. These values are used in the quantification of LOCA sequences. The quantified systemic tree in Section 2 of Appendix C provides an example of how sequence frequencies were obtained using these values.

2.3.2 Transient Initiator Effects On Mitigation

Transient initiators were identified as discussed in Section 2.2 and were grouped according to their effect on the PCS availability. However, it was necessary to examine the plant further to determine whether these transients could originate in mitigating systems or affect front-line systems other than the PCS. The goal of this transient initiator analysis was to identify those plant failures at a component or system level that could effect mitigating systems availability. The identification of transient initiator effects was done by a three part process as described below:

1. Consequence evaluation of electrical failures--Failure of each plant electrical bus was postulated. Equipment powered by the bus was tracked and the effect of its failure on the plant was identified.
2. Consequence evaluation of cooling system failures--Failure of each cooling system was postulated. Loads cooled by the system were tracked and the effect of their loss on the plant was identified.
3. Causal analysis of transient categories--Causal-type failure analysis was performed on the 15 transient categories retained for this study, as discussed in Section 2.2. The causal analysis is similar to fault tree analysis in that events that can lead to occurrence of an initiating event are logically depicted.

This evaluation was not intended to be all-encompassing. Some appropriate constraints were imposed to limit the depth of the investigation. The primary constraint was that the analysis only apply to identification of failures that could affect other systems. Failures that are internal to

TABLE A-7. LOCA INITIATOR EFFECTS ON MITIGATING SYSTEMS

LOCA Type	Mitigating Systems Lost	Piping Susceptible to LOCA (%)	Remarks
Large break on discharge of recirculation loops	One LPCI loop and one shutdown cooling discharge path	NA	Both are lost due to break location
Large break on suction of recirculation loops	All of shutdown cooling or None	55 (suction of recirculation Loop A) 45 (suction of recirculation Loop B)	Suction for both shutdown cooling loops comes from recirculation Loop A
Large steam	None	--	--
Intermediate steam	HPCI or One core spray loop or None	23.2 (HPCI) 3.8 (core spray) 73.0 (other piping)	Majority of piping susceptible to LOCA does not affect mitigating systems
Intermediate liquid	One LPCI loop and one shutdown cooling discharge path or All shutdown cooling or None	78.2 (discharge of Loop A or B) 11.2 (suction of recirculation Loop A) 10.6 (suction of recirculation Loop B)	--
Small liquid or steam	HPCI or	16.3 (HPCI)	Assumes small break can occur in larger piping and renders mitigating systems unavailable as in large break cases
Steam	One core spray loop or	1.3 (core spray)	
Liquid	One LPCI loop and one shutdown cooling discharge path or	23.3 (recirculation discharge)	
Steam and liquid	All shutdown cooling or None	3.4 (suction or recirculation Loop A) 55.7 (other piping)	

a system and have no consequences outside the system, (i.e., failures that have no capability to introduce dependencies in other systems) were of limited interest. For example, failure of feedwater control may result in the loss of feedwater. But other than the main feedwater system, no other mitigating systems are affected by this internal initiating event. However, an initiating event such as LOSP not only fails PCS but results in the common dependence of the mitigating systems powered by onsite electrical power sources, which significantly increases their probability of failure.

A second guideline was to examine failures to a level of detail commensurate with that found in the interfacing FMEAs of Appendix B, that is, to only postulate single failures. However, in many cases, the postulated failure was only significant when other concurrent conditional events or failures were considered, and these were noted as such.

Operator action was generally ignored in this evaluation. This is consistent with the rationale that no credit for operator action is taken during the first 10 min of the transient. This assumption was conservative because, in reality, operator action occurs early in most transients. Many of the failures examined are clearly annunciated and represent familiar transients for the trained operator.

Postulated Electrical Faults. The results of the first task pertaining to the effects of electrical equipment failures are summarized in Table A-8. More detail is shown in Table A-9. A wide variety of sources were utilized for information. The most useful source was the FMEAs generated by TVA⁴ in response to NRC Inspection and Enforcement Bulletin 79-27. [These are cited in Table A-9 as "I&C FMEA (79-27)"]. The postulated fault for the electrical systems was one wherein all loads powered by the bus in question were assumed to fail. Mechanisms for this failure mode were not postulated.

TABLE A-8. ELECTRICAL EQUIPMENT FAILURE SUMMARY

<u>Equipment</u>	<u>Scram on Single Failure</u>	<u>Conditional Events to Scram</u>	<u>FLS or CSCS Failed</u>
4160 V SD-BD A	No	1. Erroneous signal in RPS, Channel B 2. Failure of 250 V DC RMOV 1A 3. Existing failure of FSV-1-15B, FSV-1-27B, FSV-1-38B, FSV-1-52B	RHR Pump A core spray Pump A -- --
4160 V SD-BD B	No	None	NA

TABLE A-8. (continued)

<u>Equipment</u>	<u>Scram on Single Failure</u>	<u>Conditional Events to Scram</u>	<u>FLS or CSCS Failed</u>
4160 V SD-BD C	No	1. Erroneous signal in RPS, Channel A 2. Failure of 250 V DC RMOV 1B 3. Existing failure of FSV-1-14B, FSV-1-26B, FSV-1-51B	RHR Pump B core spray Pump B -- --
4160 V SD-BD D	No	None	NA
Offsite power	Yes	--	All PCS
500 kV system	Yes	--	None
161 kV system	No	NA	None
4 kV unit board (any one board)	No	NA	None
4 kV recirculation board	No	NA	None
480 V SD-BD or 480 V RMOV (any one board)	No	For RMOV 1A failure, see RPS A For RMOV 1B failure, see RPS B	--
RPS Bus A	No	1. Erroneous signal in RPS, Channel B 2. Failure of 250 V DC RMOV 1A 3. Existing failure of FSV-1-15B, FSV-1-27B, FSV-1-38B, FSV-1-52B	None -- --
RPS Bus B	No	1. Erroneous signal in RPS, Channel A 2. Failure of 250 V DC RMOV 1B	None --

TABLE A-8. (continued)

<u>Equipment</u>	<u>Scram on Single Failure</u>	<u>Conditional Events to Scram</u>	<u>FLS or CSCS Failed</u>
RPS Bus B (continued)		3. Existing failure of FSV-1-14B, FSV-1-26B, FSV-1-37B, FSV-1-51B	--
250 V DC RMOV 1A	No	NA	HPCI system failed Core spray B and D failed RHR B and D failed
250 V DC RMOV 1B	No	NA	ADS failed RHR A and C failed Core spray A and C failed
250 V DC RMOV 1C	No	NA	RCIC system failed Two ADS valves fail
250 V DC nonclass 1E	Yes	Operator fails to terminate feedwater on high reactor water level annunciation	PCS unavailable ^a
250 V DC turbine building distri- bution board	No	Significant generator load change demand	PCS failed
Battery Board 1	Yes	--	See 250 V DC nonclass 1E See 250 V DC RMOV 1A See 250 V DC turbine distribution
Battery Board 2	No	NA	See 250 V DC RMOV 1C

TABLE A-8. (continued)

<u>Equipment</u>	<u>Scram on Single Failure</u>	<u>Conditional Events to Scram</u>	<u>FLS or CSCS Failed</u>
Battery Board 3	No	NA	See 250 V DC RMOV 1B
Battery Board 4	No	NA	--
I&C Bus A	Yes	--	Drywell air unavailable MSIV isola- tion reset unavailable
I&C Bus B	No	Leaky MSIV accumulators	Drywell air unavailable
Unit-preferred bus	No	Power demand change	PCS failed RCIC system failed
24 V DC Channel A	No	Failure 24 V DC Channel B	--
24 V DC Channel B	No	Failure 24 V DC Channel A	--
48 V DC	No	--	--
125 V DC diesel control	No	NA	--
Unit nonpreferred	Yes	--	Condenser unavailable
Plant preferred	Yes	Cold weather	Feedwater unavailable

a. HPCI system and RCIC system could fail due to water in the steam line, but these systems not required during over fill. ADS operability unknown due to the possibility of water in steam line.

TABLE A-9. ELECTRICAL EQUIPMENT FAILURE CHART DETAILS

Failed Equipment	Scram Type	Primary Failure Effects	Disabled Systems/Secondary Effects	Comments, Notes, References
4160 V SD-BD A	None	<ol style="list-style-type: none"> 1. Loss of RPS Bus A. 2. No other loads essential to normal operation are powered by this board. 	<ol style="list-style-type: none"> 1. Outboard MSIVs go into "half-isolate" state. 2. RPS goes into "half scram" state. 3. RHR Pump A inoperable. 4. Core spray Pump A inoperable. 	<ol style="list-style-type: none"> 1. If any signal requirement in Channel B is satisfied, the reactor will scram. 2. Alternate power source for RPS bus is manual transfer. 3. Refs.--EOI-5 I&C FMEA (79-27) 45N-724-1 45N-749-1 45N-751-1.
4160 V SD-BD B	None	<ol style="list-style-type: none"> 1. No equipment essential for Unit 1 normal operation is powered from this board. 	<ol style="list-style-type: none"> 1. RHR Pump C inoperable. 2. Core spray Pump C inoperable. 	<ol style="list-style-type: none"> 1. Refs.--same as above.
4160 V SD-BD C	None	<ol style="list-style-type: none"> 1. Loss of RPS Bus B. 2. No other loads essential for normal operation are powered by this board. 	<ol style="list-style-type: none"> 1. Inboard MSIVs go into "half isolate" state. 2. RPS goes into "half scram" state. 3. RHR Pump B inoperable. 4. Core spray Pump B inoperable. 	<ol style="list-style-type: none"> 1. If an erroneous signal is made up through Channel A, the reactor will scram and/or isolate. 2. Alternate power source for RPS bus is manual transfer. 3. Refs.--same as above.
4160 V SD-BD D	None	<ol style="list-style-type: none"> 1. No equipment essential for Unit 1 normal operation is powered by this board. 	<ol style="list-style-type: none"> 1. RHR Pump D inoperable. 2. Core spray Pump D inoperable. 	<ol style="list-style-type: none"> 1. Refs.--same as above.
Complete loss of offsite power	Yes, scram on loss of RPS buses	<ol style="list-style-type: none"> 1. Loss of RPS Buses A and B. 2. I&C Bus A and B lost until diesels available. 	<ol style="list-style-type: none"> 1. Reactor scrams on loss of RPS bus. 2. Reactor isolates on loss of RPS bus. 	<ol style="list-style-type: none"> 1. Plant undergoes complex sequence of events upon loss of offsite power; only the most significant affects were noted. 2. Diesels start on low voltage.
500 kV system	Yes, if above 30% power; generator trip	<ol style="list-style-type: none"> 1. Generator trip. 2. Loss of power to 4 kV unit boards, 4 kV common boards, and 4 kV recirculation boards. 	<ol style="list-style-type: none"> 1. 4 kV unit boards auto-transfer to start board. 2. Power to recirculation boards not necessary if reactor is less than 30% power. 	<ol style="list-style-type: none"> 1. Refs.--EOI-5 15W500-1.
161 kV system	None		<ol style="list-style-type: none"> 1. 4 kV common boards auto-transfer. 	<ol style="list-style-type: none"> 1. Refs.--EOI-5 15W500-1.

TABLE A-9. (continued)

Failed Equipment	Scram Type	Primary Failure Effects	Disabled Systems/Secondary Effects	Comments, Notes, References
4 kV unit boards	None, assuming loss of one board	<ol style="list-style-type: none"> Loss of one unit board disables: one CCW pump one condensate booster pump one condensate pump one raw water cooling pump. Loss of corresponding 480 V unit board. 	<ol style="list-style-type: none"> Unit will run back to 92% power if one condensate train is lost. 480 V unit boards auto-transfer to alternate power supply. 	<ol style="list-style-type: none"> Refs.--EOI-5 15W500-1.
4 kV recirculation boards	No	<ol style="list-style-type: none"> Power lost to recirculation Pump YG sets. 		<ol style="list-style-type: none"> Loss of both recirculation pumps does not cause a scram.
480 V SD-BD 480 V RMOVs	None, assuming only one RMOV or one shut-down board fails	<ol style="list-style-type: none"> Loss of RPS Bus A if RMOV 1A or SD-BD 1A fails. Loss of RPS Bus B if RMOV 1B or SD-BD 1B fails. 	<ol style="list-style-type: none"> "Half scram" and "half-isolate" states occur. All other I&C buses are on non-interruptable power supplies (with respect to 480 V board failures). 	
RPS Bus A	None	<ol style="list-style-type: none"> Channel A of the RPS logic is tripped. Miscellaneous false isolation and trip signals will occur. 	<ol style="list-style-type: none"> RPS in "half scram" state. Outboard MSIVs in "half isolate" state. 	<ol style="list-style-type: none"> Any erroneous signals in Channel B logic will scram reactor and/or trip MSIVs. Refs.--EOI-5 I&C FMEA (79-27) 45W 710 4.
RPS Bus B	None	<ol style="list-style-type: none"> Channel B of the RPS logic is tripped. Miscellaneous false isolation and trip signals will occur. 	<ol style="list-style-type: none"> RPS in "half scram" state. Inboard MSIVs in "half isolate" state. 	<ol style="list-style-type: none"> Any erroneous signal in Channel A logic will scram and/or isolate reactor. A failed 250 V solenoid on inboard MSIV will cause valve to close. One closed MSIV will not directly trip plant. Refs.--EOI-5 I&C FMEA (79-27) 45W 710 4.
250 V RMOV 1A	None	<ol style="list-style-type: none"> HPCI system inoperable. Core spray Train B and D inoperable. RHR Train B and D inoperable. S/RV 1-41 and 1-4 inoperable in manual initiation mode. 	<ol style="list-style-type: none"> Loss of bus is annunciated in MCR. Operator can transfer to battery Board 2. 	<ol style="list-style-type: none"> If a 120 V AC solenoid on the outboard MSIVs is failed, that MSIV will close; one MSIV closure may cause a scram but multiple faults are required. Refs.--45N712-1 I&C FMEA (79-27).

TABLE A-9. (continued)

Failed Equipment	Scram Type	Primary Failure Effects	Disabled Systems/Secondary Effects	Comments, Notes, References
250 V RMOV 1A (continued)		5. Two valves in backup scram system are inoperable. 6. Solenoids on outboard MSIVs close. 7. Recirculation Pump A speed is fixed. Pump can be tripped.		3. Transfer to alternate power supply is manual.
250 V RMOV 1B	None	1. ADS inoperable. 2. S/RV 1-18, 1-19, 1-31, 1-42, 1-179 inoperable in manual activation mode. 3. RHR Train A and C inoperable. 4. Core spray Train A and C inoperable. 5. Recirculation Pump B speed is fixed. Pump can be tripped. 6. FCV-74-47 fails as is. 7. Solenoids on inboard MSIVs close.	1. No shutdown cooling. 2. Loss of bus is annunciated in MRC. Operator can transfer to battery Board 1.	1. See above comment. 2. Refs.--45N712-2 I&C FMEA (79-27). 3. Transfer to alternate power supply is manual.
250 V RMOV 1C	None	1. RCIC system inoperable. 2. S/RV 1-23, 1-5, 1-180, 1-34 inoperable in the manual initiation mode.	1. Same as 2 above.	1. Refs.--45N712-3 I&C FMFA (79-27). 2. Transfer to alternate power supply is manual.
250 V DC nonclass 1E power	Yes, pressure regulator closes	1. All main turbine trips except the following are lost: a. High vibration. b. Back-up overspeed. c. Loss of both turbine speed feedback channels. d. Manual trip. 2. All RFPT are lost. Feedwater can be manually terminated by closing valve in steam supply line. 3. Motor speed changer on RFPT is inoperable. 4. EHC instrumentation is lost.	1. Manual control of feedwater is lost; automatic control between 3000 and 5500 rpm is unaffected. 2. Power loss to PT-1-16A and PT-1-16B cause pressure regulator to fail closed.	1. Loss of bus voltage is not annunciated. 2. Refs.--I&C FMEA (79-27). 3. Transfer to alternate power supply (battery Board 2) is manual. 4. Reactor scram on high pressure; turbine trip on overspeed. Feedwater drops to low speed stop. Bypass fails closed.

TABLE A-9. (continued)

Failed Equipment	Scram Type	Primary Failure Effects	Disabled Systems/Secondary Effects	Comments, Notes, References
250 V DC turbine building distribution board	No direct scram; significant grid demand change will cause scram	<ol style="list-style-type: none"> 1. Loss of alterrex excitation system. 2. Loss of control power to: <ol style="list-style-type: none"> a. 4 kV unit boards. b. 4 kV recirculation boards. c. 4 kV common boards. d. 4 kV unit boards. e. 480 V unit boards. f. 480 V common boards. 	<ol style="list-style-type: none"> 1. Loss of ability to regulate excitation voltage of the main generator. 2. If generator trip occurs before control power is restored, these boards cannot be transferred to offsite power. The generator normally supplies these boards through TUSS-1A and 1B. 	<ol style="list-style-type: none"> 1. If significant change in grid demand occurs when Alterrex is out, a generator trip will occur, causing a scram if above 30% power. 2. Normal power supply is battery Board 1 with manual transfer. 3. Transfer is manual. 4. Refs.--I&C FMEA (79-27).
250 V DC battery Board 1	<p>If in feedwater control Channel A, scram will occur due to high reactor water level</p> <p>If in feedwater control Channel B, no direct scram; significant grid demand change will cause scram</p> <p>Pressure regulator will fail closed causing high pressure scram</p>	<ol style="list-style-type: none"> 1. Loss of normal power to: <ol style="list-style-type: none"> a. 250 V DC RMOV 1A. b. 250 V DC nonclass 1E. c. 250 V DC turbine building distribution. d. Feedwater inverter. e. 480 V shutdown load shed Logic A. 	<ol style="list-style-type: none"> 1. See other sections for effects of loss of 250 V DC boards. 2. Failure of feedwater inverter causes feedwater to go to high speed stop if in Channel A control. 3. Failure of feedwater inverter has no effect if in Channel B. 	<ol style="list-style-type: none"> 1. If feedwater control is in Channel A, feedwater will go to high speed stop. Turbine will not trip on water Level 8. RFPT will not trip on water Level 8. Reactor will not scram until turbine trips (likely on high vibration or manual trip). 2. If feedwater control is in Channel B, there is no imminent direct scram. Manual feedwater control is lost. Master governor unit controls feedwater between 3000 and 5500 rpm. Should the load demand the turbine to trip (on backup overspeed) and subsequent reactor scram, three feedwater pumps drop to their low speed stop (manual speed control unavailable). When generator trips, the 4 kV unit boards lose power; this will fail condensate pumps, which will subsequently fail (or trip) feedwater pumps. <p>If boards are switched to offsite power before generator trip, feedwater will be available and will fill up vessel, unless manually terminated. (Installation of generator breakers will eliminate need for manual power change, i.e., CCW condensate pump will be available.)</p>

TABLE A-9. (continued)

Failed Equipment	Scram Type	Primary Failure Effects	Disabled Systems/Secondary Effects	Comments, Notes, References
250 V DC battery Board 1 (continued)				3. Refs.--45N701 I&C FMEA (79-27). 4. Third alternative is that pressure regulator fail closed; scram on high pressure.
250 V DC battery Board 2	None	1. Loss of normal power supply to: a. 250 V DC RMOV-1C. b. 480 V shutdown load shed Logic B.		1. No significant effects on Unit 1. 2. Refs.--45N702 I&C 45N702.
250 V DC battery Board 3	None	1. Loss of normal power supply to: a. 250 V DC RMOV-1B. b. Control bus for 480 V SD-BD 1A.		1. No significant effects on Unit 1. 2. Refs.--45N703 I&C FMEA (79-27).
250 V DC battery Board 4	None	1. Power lost to all DC air compressors on the diesels. 2. Power lost to main turbine DC emergency bearing oil pump.		1. No significant effects on Unit 1. 2. Refs.--45N704 I&C FMEA (79-27).
I&C Bus A	If feedwater control system in Channel B, reactor will scram on L-8 turbine trip; delayed scram may occur on high drywell pressure due to loss of cooling Scram may occur on turbine trip due to low condenser vacuum if SJAE-B does not catch pressure rise Scram may occur if MSIV accumulator leaks	1. If feedwater control in Channel B, RFPT goes to high speed stop. If in Channel A, no effect. LT-3-60 goes to zero. 2. Feedwater bypass valve to condenser opens. 3. Recirculation Pump A speed fixed. 4. Recirculation Pump B speed goes to 50%. 5. FCV-32-62 (drywell control air suction valve) fails closed. 6. SJAE-A fails. Auto-start of SJAE-B on loss of Train A also fails. 7. HSIV isolation reset signal fails. 8. Loss of some RHR-I instrumentation. 9. Loss of some CSS-I instrumentation.	1. Effect of recirculation pump speed mismatch unknown. 2. Drywell cooling lost. 3. Air to inboard MSIVs and safety relief valves isolated. MSIV and ADS valves have accumulator inside isolation. 4. SJAE-B will start on low condenser vacuum (25 in. high). 5. RHR, CSS, RHRSW are not disabled.	1. Channel B is preferred operating mode, so it is likely a scram will occur on high water level. 2. All trips are available to main turbine and RFPT. 3. CSCSs are unaffected. 4. MSIVs may drift closed if accumulators leak. 5. Loss of some CSCS instrumentation increases chance for operator error. 6. Normal power source to I&C Bus A is 480 V SD-BD 1A, through a 480/120 V transformer. Auto-transfer to 480 V SD-BD 2A. 7. Refs.--EOI-5 45W710-4 I&C FMEA (79-27).

TABLE A-9. (continued)

Failed Equipment	Scram Type	Primary Failure Effects	Disabled Systems/Secondary Effects	Comments, Notes, References
I&C Bus A (continued)		10. Loss of some RHRSW-1 instrumentation.		8. I&C Bus A is fed from bus at battery Board 1. Transfer to bus at battery Board 2 is automatic. Buses at battery board fed from 480 V shutdown boards.
I&C Bus B	Delayed trip may occur on high drywell pressure due to loss of drywell cooling Delayed scram may occur if SJAE-B is operating. Scram may occur if MSIV accumulator leaks	1. FSV-32-63 fails closed. Drywell control air lost. 2. Recirculation Pump B speed is fixed. 3. Recirculation Pump A speed goes to 50%. 4. Feedwater control unaffected. 5. SJAE-B inoperable. SJAE-A is normally in use. 6. Loss of some RCIC system instrumentation. 7. Loss of some RHR-II instrumentation.	1. Drywell cooling is lost. 2. Air to inboard MSIVs and safety relief valve is lost. MSIVs and ADS valves have accumulator inside isolation.	1. Reactor scram is not obvious. 2. CSCS are unaffected. 3. MSIVs may drift closed if accumulators leak. 4. Normal power source for Bus B is 480 V SD-BD 1B. Auto-transfer to 480 V SD-BD 3B. 5. Refs.--EOI-5 45W710-9 I&C FMEA (79-27).
Unit preferred bus	None, unless power demand changes and feedwater flux/flow level mismatches occur	1. Recirculation pump speed locks in on both pumps. 2. EHC loses normal power source. 3. CRD positioning capability lost. 4. RCIC system start logic fails. 5. Power lost to: a. LM-46-6. b. LT-3-206. c. LC-46-5 (master feedwater controller). d. LC-3-53 (safety valve level controller).	1. As long as turbine is operating, EHC is powered by permanent magnet on shaft. Should trip occur, EHC is inoperable, thereby failing turbine bypass. 2. Scram capability exists. No rod positioning available. 3. Loss of power to LC-46-5 causes master government to lock in place. Operator must take manual control with manual speed control.	1. Unit preferred is a continuous power supply; driven by motor-generated set. 2. All Cf_Ss, except RCIC system operable. 3. Refs.--EOI-6 45W710-4 I&C FMEA (79-27).
24 V DC Channel A	None	1. Power lost to EHC master trip Solenoid A. 2. Various process radiation monitors lost.	1. EHC will not trip unless both A and B solenoid are tripped. 2. Loss of intermediate range monitor and source range monitor will cause a "half scram."	1. Refs.--EOI-5 I&C FMEA (79-27).

TABLE A-9. (continued)

Failed Equipment	Scram Type	Primary Failure Effects	Disabled Systems/Secondary Effects	Comments, Notes, References
24 V DC Channel B (continued)		<ol style="list-style-type: none"> Channels A and C source range monitor lost. Channels A, C, E, and G-- intermediate range monitor lost. 		
24 V DC Channel B	None	<ol style="list-style-type: none"> Power lost to EHC master trip Solenoid B. Various process radiation monitors lost. Channels B and D source range monitors lost. Channels B, D, F, and H-- intermediate range monitor lost. 	<ol style="list-style-type: none"> See comments above. 	<ol style="list-style-type: none"> Refs.--EOI-5 I&C FMEA (79-27).
48 V DC system	None	<ol style="list-style-type: none"> Annunciator system lost. 		<ol style="list-style-type: none"> No significant affects I&C FMEA (79-27).
125 V DC diesel control power system	None			
Unit nonpreferred bus	Eventually, loss of condenser vacuum	<ol style="list-style-type: none"> SJAE exhaust valves close. Recirculation scoop tube positioner locks in place. All high point vent valves in RHR, CSS, HPCI, RCIC system will fail closed. Reactor manual control lost. FCV-68-3, FCV-68-79 jog circuit power is lost. 	<ol style="list-style-type: none"> Condenser vacuum will gradually be lost. At 600 psig (reactor pressure) the vacuum pumps can be used. 	<ol style="list-style-type: none"> Refs.--I&C FMEA (79-27).
Plant preferred bus	None	<ol style="list-style-type: none"> TM-24-70, TM-24-80, TM-24-85 open upon loss of power. 	<ol style="list-style-type: none"> These valves are the RCW valves to the RFPT coolers. In cold weather, this will cause turbine oil overcooling and subsequent turbine vibration. 	<ol style="list-style-type: none"> Orderly shutdown recommended. Refs.--EOI-5 I&C FMEA (79-27).

A-28

As can be seen from Tables A-8 and A-9, the most significant power failure that results in a scram and causes loss of a front-line system (i.e., the PCS) is a LOSP event. The effect of this important transient on the mitigating systems was accounted for separately during sequence quantification.

Failure of the 250 V DC nonclass 1E bus or battery Board 1, since it supplies power to 250 V DC nonclass 1E bus, also causes a scram on high reactor pressure due to the pressure regulator failing closed. Manual control of feedwater is lost including reactor feedwater pump trip on high reactor water level. If the operator fails to respond to high reactor water level annunciation (i.e., manually terminate feedwater, or, in the case of loss of battery Board 1, manually transfer power to battery Board 2) a possible overflow condition could occur. The HPCI and RCIC systems could be inoperable due to water in the steam lines, and relief valve operability is not known under this condition. BFl EOI-5, Section M, delineates the procedures the operator should follow given this initiator. Immediate operator action requires manual transfer of the affected board to the alternate source. Subsequently, the procedure requires that if a reactor scram occurs, the operator should manually trip the main turbine and close the high and low pressure steam supply to the reactor feed pump turbines. The latter action is required to terminate feed pump flow since manual control is inoperative (i.e., the operator can stop flow but he cannot control it). Thus, the probability of losing a DC bus (approximately 10^{-6}) times the probability of the operator failing to subsequently respond to terminate feedwater flow (approximately 10^{-2}) makes this scenario insignificant when compared to other transient sequences.

Postulated Cooling System Failures. The cooling water systems and the drywell atmospheric cooling system were treated in an analogous manner to the electrical systems. The results are shown in the cooling water failure chart, Table A-10.

Cooling system failures are not as significant as electrical system failures. Loss of cooling loads does not represent as dynamic a situation as loss of electrical power. System response and plant response is gradual with significant time for operator action or recovery by alternate cooling systems. Failure of cooling systems is not considered to be a significant transient initiator.

Causal Analysis of Transient Categories. Causal-type failure analysis was performed on the 15 transient categories identified previously in Section 2.2. Causal analysis is similar to fault tree analysis in that events that can lead to occurrence of some undesired initiating event category are depicted. However, in keeping with the rationale of identifying events that can affect other systems, as discussed previously in Section 2.3.2, only those events that could originate in front-line or support systems and cause the transient are represented on the causal failure diagrams.

The 15 transient categories applicable to BFl are:

1. Closure of all MSIVs (Figure A-1).
2. Loss of condenser vacuum (Figure A-2).

TABLE A-10. COOLING WATER FAILURE CHART

Failed Equipment	Scram/Type	Primary Failure Effects	Disabled Systems/Secondary Effects	Comments, Notes, References
Reactor building closed-cycle cooling	None	<ol style="list-style-type: none"> 1. Loss of recirculation pump cooling. 2. Loss of drywell cooling. 		<ol style="list-style-type: none"> 1. No CSCS affected.
Drywell atmosphere cooling system		<ol style="list-style-type: none"> 1. Loss of drywell cooling. 	<ol style="list-style-type: none"> 1. If failure mode of the drywell air is through isolation, drywell pressure will increase, causing reactor scram. 2. If failure mode is through loss of heat sink, temperature will increase but pressure may not. Operator will initiate manual shutdown. 	<ol style="list-style-type: none"> 1. If scram on drywell isolation, ADS valves will not be available if their accumulators leak. 2. Operator instructed to vent drywell to the vapor space above the suppression pool. 3. Ref.--EOL-26.
RHRSW	None	<ol style="list-style-type: none"> 1. No RHR heat exchanger cooling available. 		
EECW	None			
Raw cooling water	Eventually	<ol style="list-style-type: none"> 1. Loss of EHC cooling. 2. Loss of turbine oil coolers. 3. Loss of reactor building component cooling water heat sink. 4. Loss of generator cooling. 5. Loss of reactor feedwater pump turbine cooling. 6. Loss of condensate pump cooling. 7. Loss of drywell cooling (through RBCCWs). 	<ol style="list-style-type: none"> 1. Loss of generator cooling is likely to be the first thing to cause a trip. 2. If EHC has no cooling, turbine bypass will not be available. 3. Feedwater probably not available. 	<ol style="list-style-type: none"> 1. NO CSCS equipment is disabled. 2. EECW provides backup water supply to critical loads.

A-30

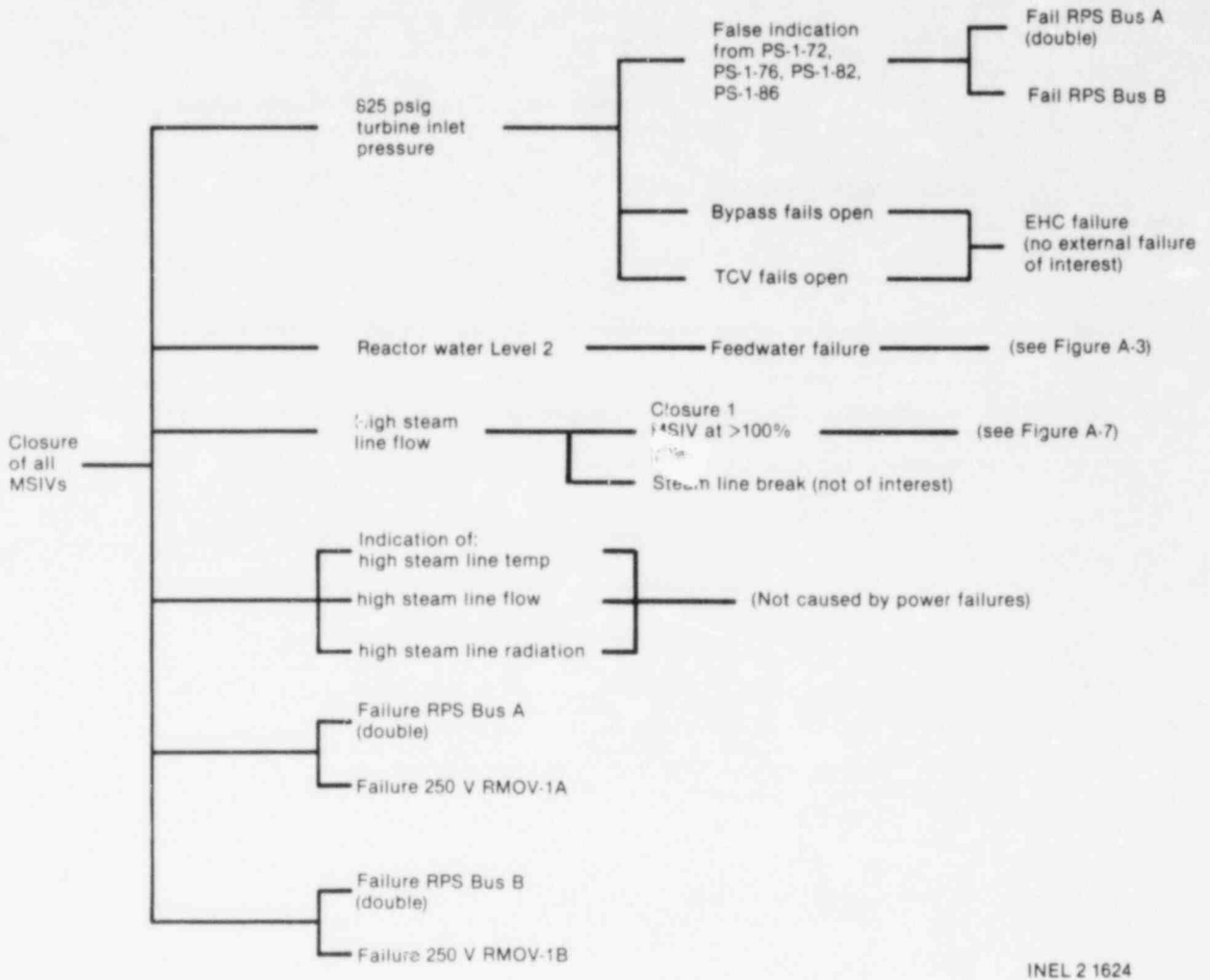


Figure A-1. Causal failure diagram for MSIV closure.

3. Pressure regulator fails open.
4. Loss of feedwater flow (Figure A-3).
5. Loss of offsite power (LOSP).
6. Loss of auxiliary power.
7. Increased feed flow at power.
8. Load rejection (Figure A-4).
9. Load rejection with bypass failure.
10. Turbine trip (Figure A-5).
11. Turbine trip with bypass failure (Figure A-6).

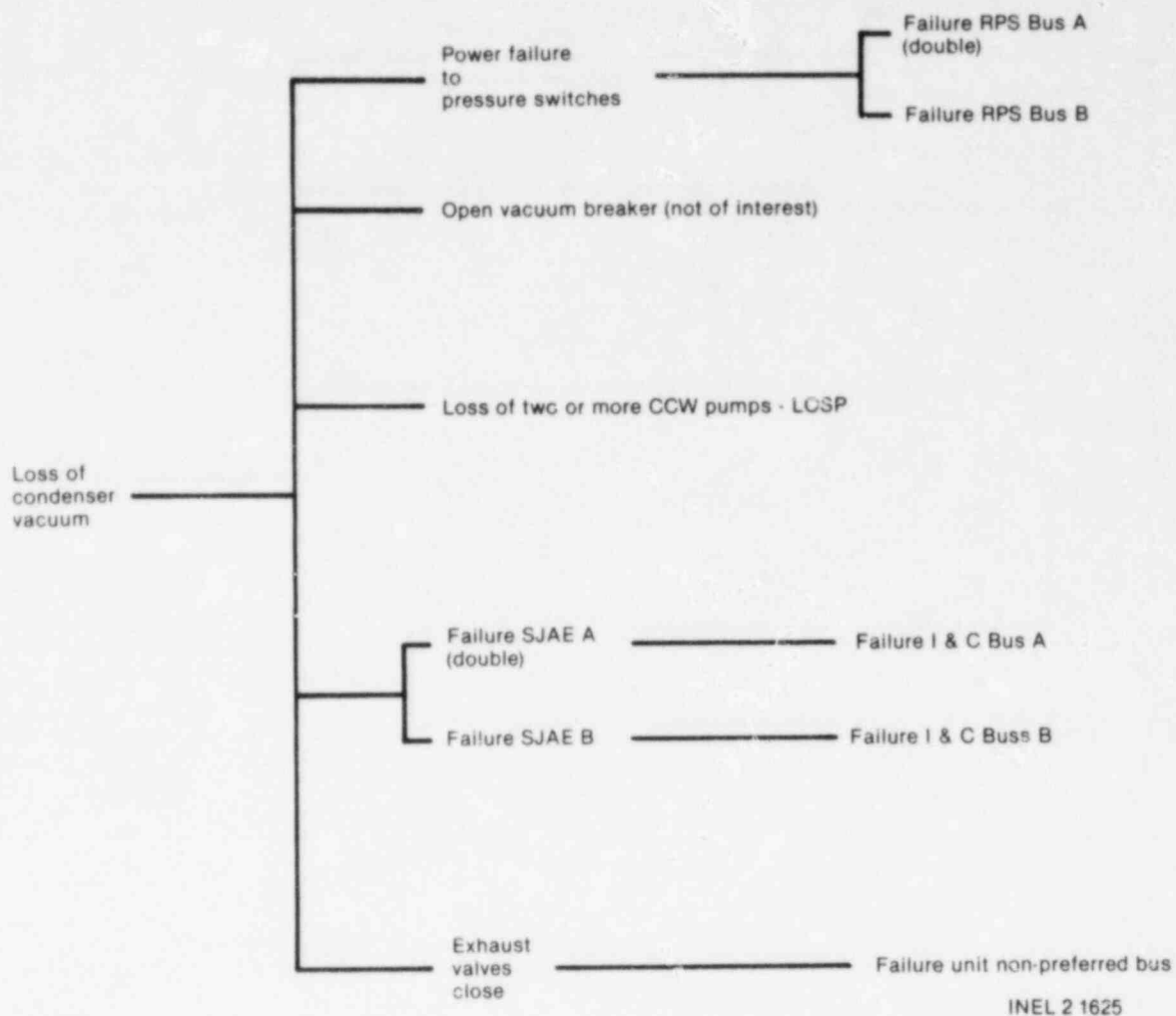
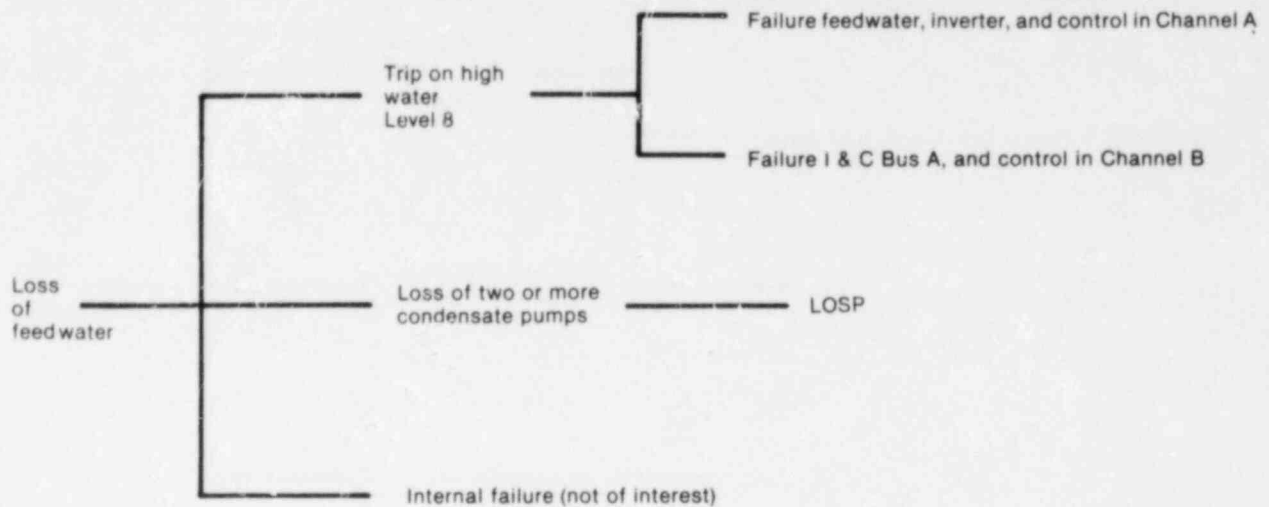


Figure A-2. Causal failure diagram for loss of condenser vacuum.

12. Inadvertent closure of one MSIV (Figure A-7).
13. Pressure regulator fails closed.
14. Bypass valve fails, causing pressure increase.
15. Uncontrolled increase in recirculation flow.

Causal failure diagrams were prepared for those transient initiator categories where failures in other systems can cause the initiating event and at the same time, nullify portions of the mitigating systems. No diagrams were drawn for those initiating events that have a direct causal relationship (transient Categories 3, 5, 6, 7, 9, 13, 14, and 15). Figures A-1 through A-7, as noted above, represent the causal failure diagrams for the remaining seven transient categories. These diagrams should be read from right to left, because the causes of the event are depicted to the right. All branch points can be considered as OR logic except where noted by "double," indicating AND logic, i.e., where multiple failure conditions must exist. A discussion of each of the 15 categories follows:

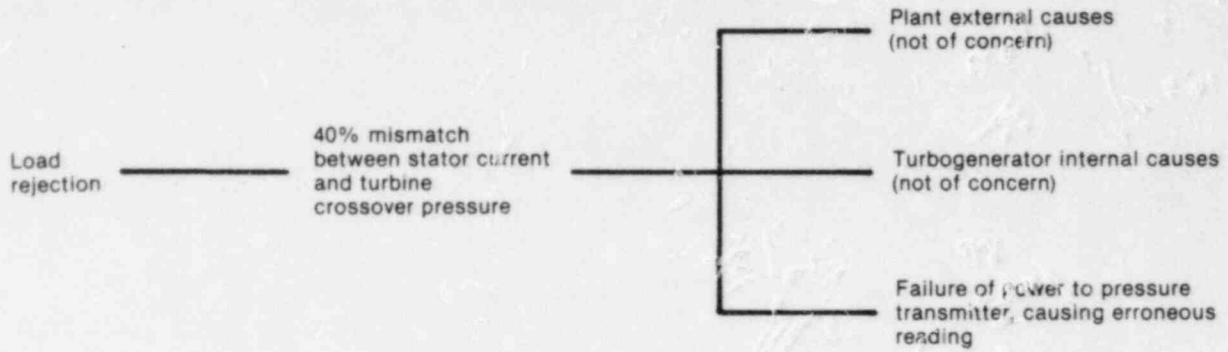


INEL 2 1626

Figure A-3. Causal failure diagram for loss of feedwater.

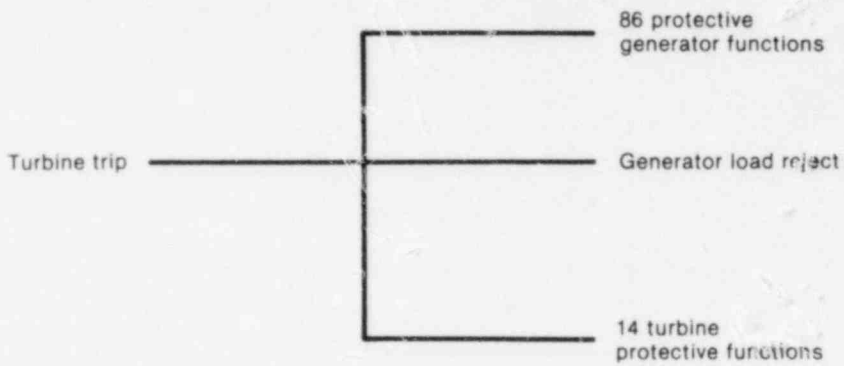
1. Closure of all MSIVs--This can be caused by steam line breaks, low turbine inlet pressure, or low reactor water level. There are no other single failures outside the system that can cause this event.
2. Loss of condenser vacuum--Many actions start to happen on loss of condenser vacuum. The second steam jet air ejector starts at 25 in. Hg, reactor scrams at 23 in., turbine trips at 22 in., bypass valves close at 7 in., and RFPT occurs at 7 in. The initiation logic for these actions were determined to be powered as follows:

SJAE A start	I&C Bus A
SJAE B start	I&C Bus B
RPS scram	RPS Buses A and B
Turbine trip	Instrumentation and trip solenoid power by 250 V DC nonclass 1E
Bypass valve	Controlled and powered by electro-hydraulic control power sources (i.e., 250 V DC nonclass 1E and 120 V AC unit preferred)
RFPT	Instrumentation and trip solenoid powered by 250 V DC nonclass 1E.
3. Pressure regulator fails open--This will cause a scram through MSIV closure caused by low turbine inlet pressure or a direct scram from high reactor water level.



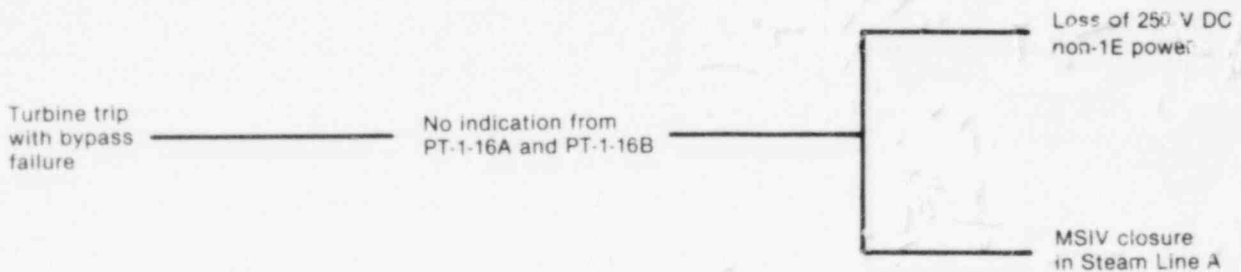
INEL 2 1627

Figure A-4. Causal failure diagram for generator load reject.



INEL 2 1628

Figure A-5. Causal failure diagram for turbine trip.



INEL 2 1629

Figure A-6. Causal failure diagram for turbine trip without bypass.

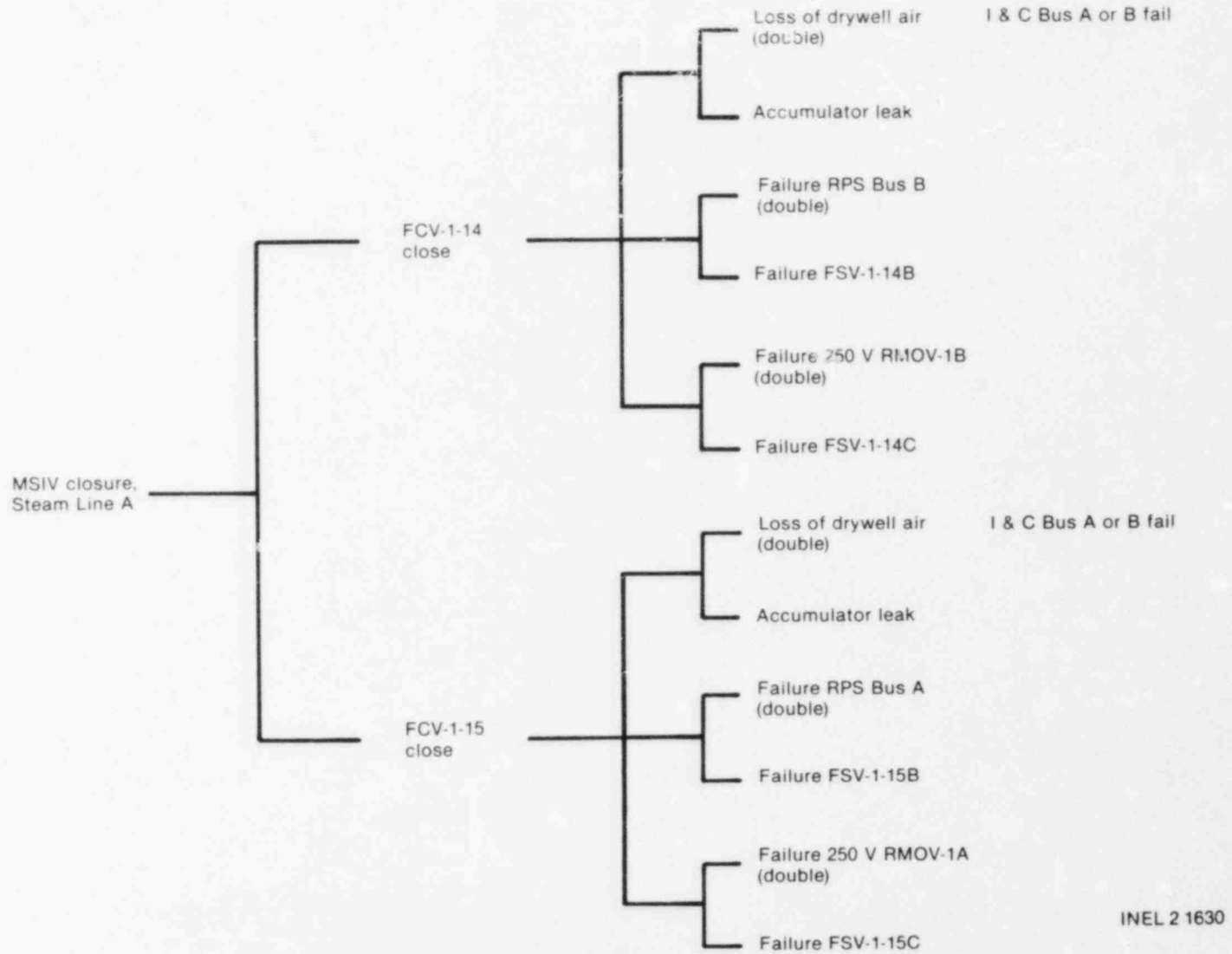


Figure A-7. Causal failure diagram for closure one MSIV.

4. Loss of feedwater--This was interpreted to occur in two ways: (a) reduction of feedwater flow such that water level reaches Level 2, closing the MSIV's, and (b) feedwater increases to water Level 8, whereupon reactor trips, feedwater trips, and the turbine trips. Operator action is required to restore feedwater. Water level was assumed to drop to water Level 2, whereupon MSIVs close (making feedwater unavailable) and HPCI system starts. Both of these cases were addressed in the causal chart.
5. Loss of offsite power--The dependencies of the front-line systems on offsite power are clearly documented in all fault tree work to date. No further analysis was done.
6. Loss of auxiliary power--Loss of incoming power to the plant due to yard station faults is similar to transient Category 5. No further analysis was done.
7. Increased feedwater flow--This is addressed in the causal chart, Figure A-3.
8. Load rejection--There is one load reject trip function i.e., a greater than 40% mismatch between stator electrical current and turbine crossover pressure. This trips the turbine, which scrams the plant if above 30% power. It was assumed that the originating faults for load reject are largely external to the plant. Consequently, no further analysis of this transient was done.
9. Load rejection with bypass failure--No single event was found to cause this transient. There were no occurrences of this category reported in EPRI NP-801 for any BWRs.
10. Turbine trip--There are 101 trip functions that cause turbine trip. They were considered beyond the scope of the study.
11. Turbine trip with bypass failure--Failure of the 250 V DC nonclass 1E power supply has been identified to cause turbine trip and no bypass. Lack of the 250 V DC nonclass 1E fails power to PT-1-16A and PT-1-16B, which are redundant pressure inputs to the electro-hydraulic control. No pressure indication will cause the pressure regulator to close. The reactor will scram on high pressure or high flux. The bypass will also be unavailable since it is controlled by the electro-hydraulic control.

Closure of MSIVs on steam Line A will also cause the same event, because both pressure detectors are on Line A, downstream of the MSIVs.

There were no occurrences of this category reported in EPRI NP-801 for any BWR.

12. Inadvertent closure of one MSIV--This event will not cause a scram through RPS logic. Depending on power level, it may cause a trip through high flux or high steam line flow. Additionally, if steam Line A is isolated, the pressure regulator will fail closed.

13. Pressure regulator fails closed--See causal sheet, Figure A-6. Same as Category 11.
14. Bypass valve fails closed, causing pressure increase--This transient can be initiated by operator error or electro-hydraulic control failures. These failures were considered beyond the scope of this study.
15. Recirculation flow increase--No external failures were identified that can cause this event.

Conclusions. The only significant power failure that causes scram and a loss of a front-line system is the LOSP. This event will cause PCS to be unavailable, and the effect is immediate. Failure of HPCI and RCIC upon loss of 250 V DC nonclass 1E power is possible, but relatively improbable. Loss of equipment cooling water systems is not significant because of the allowable time for the operator to recover, e.g., to initiate alternate cooling systems. The causal diagrams indicate that multiple failures must coexist in mitigating systems in order to produce a transient initiator.

3. LOCA AND TRANSIENT SYSTEMIC EVENT TREES

A functional event tree describes the meaningful outcomes of accident sequences, given that mitigating functions either respond or do not respond to an accident initiator. A systemic event tree describes the meaningful outcomes of accidents, given that systems (i.e. systems provided to perform the mitigating functions) either respond or do not respond to an accident initiator. This section describes the systemic event trees developed in this study.

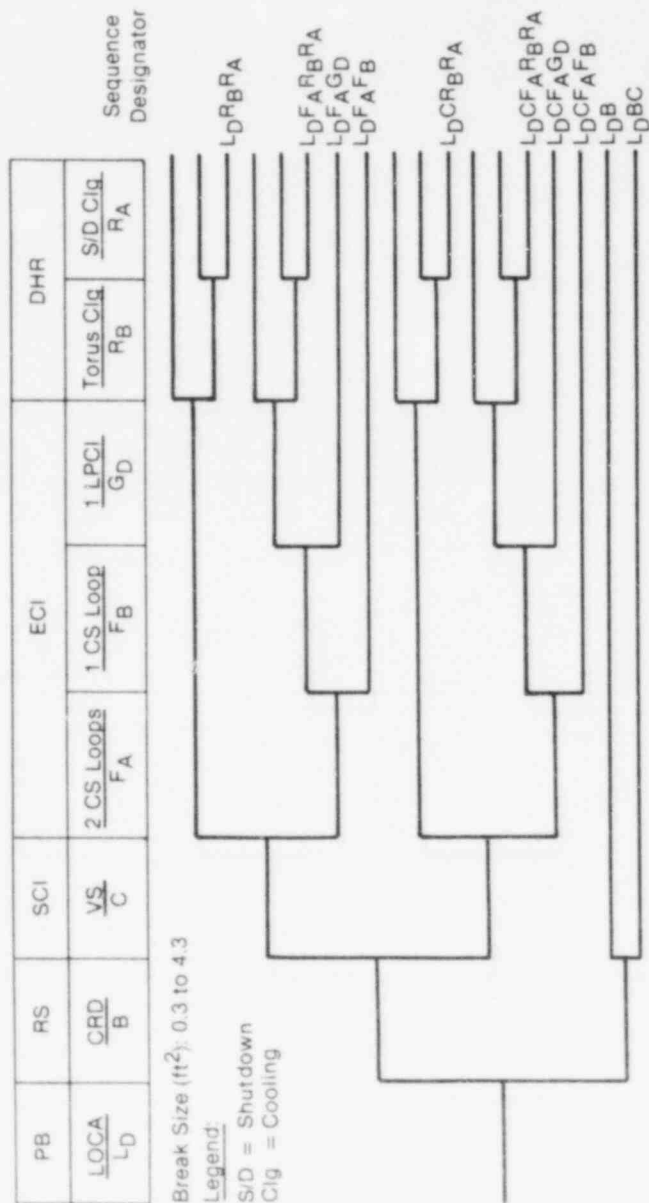
3.1 LOCA Systemic Event Trees

The LOCA systemic event trees are shown in Figures A-8 through A-13. The purpose of these trees is to show the interrelationships among the various systems that perform the functions necessary to successfully mitigate the effects of a LOCA. These systems are defined as front-line systems since their success or failure will directly affect the course of the accident. The event tree headings consist of various arrangements of these front-line systems in order of their response requirements or interdependencies necessary for the systems to mitigate the accident. The function that the system (or systems) is performing is listed in the area above the system identification block.

The systemic event trees begin with an initiating event; then each front-line system necessary for mitigation of the particular event is challenged for success or failure progressing from left to right across the tree. This develops the meaningful accident sequences in terms of the system interrelationships. If no branch is depicted for a particular system on the tree, it is assumed the system's response will not affect the consequences associated with that sequence or that system operation is precluded by other systems operation or phenomenological considerations. Each sequence is given a unique identification code based upon the initiating event identifier and the systems which fail for that particular sequence.

LOCA initiating events for BFI were identified by break size and break location with respect to fluid initially discharged from the break. This was necessary because it was determined that the front-line system responses and the consequences associated with the various initiating events varied with break size and break location. For example, a large suction-line break in the recirculation system requires different system responses than a large discharge-line break in the same system. Where different system responses are required, it is usually necessary to construct a different event tree to adequately illustrate those responses. As a result, a number of LOCA initiating events were identified and six systemic event trees were constructed to illustrate the system responses to these LOCAs.

Since many LOCA initiating events are used in this analysis, a mnemonic coding scheme was developed to identify each initiating event. Break size was considered the most important factor in LOCA initiating event identification. Three break sizes were identified for this analysis--large (L), intermediate (I), and small (S). An L, I, or S is used to identify each LOCA break size. A subscript denotes the fluid initially discharged from the break: L for liquid, V for vapor. During the course of the study, it



X = Function failure

R	S	E	D	Remarks
S	C	C	H	
I	I	I	R	
			X	Core cooled
				Core cooled
			X	Slow melt
				Core cooled
			X	Core cooled
			X	Slow melt
		X	N/A	Melt
		X	N/A	Melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X			Core cooled
	X		X	Core cooled
	X			Slow melt
	X	X		Melt
	X	X		Melt
X		N/A	N/A	Melt
X		N/A	N/A	Melt

INEL 2 1632

Figure A-9. LOCA systemic event tree for large liquid break, discharge-side of recirculation pumps (L_p).

was determined that a recirculation pump suction-line break required different system responses than a recirculation pump discharge line break. Since these are both liquid line breaks, any initiating event involving these break locations will have an S (suction) or D (discharge) substituted for the L that would normally be present for the subscript letter.

For example, a large break on the recirculation pump suction line requires a specific front-line system response for accident mitigation. This LOCA initiating event identification code is L_S. In contrast, a small break on the recirculation pump suction line has the same system response requirements as any small break, regardless of the break location or the fluid being discharged from the break. Therefore the identification code for any small break is S. Table A-11 provides a listing of the various initiating event identifiers used in this study.

TABLE A-11. EVENT TREE LEGEND

<u>Initiating Event Identifier</u>	<u>Initiating Event Description</u>
L _S	Transients where PCS is unavailable
L _D	Large discharge-side break
L _V	Large steam break
I _L	Intermediate liquid break
I _V	Intermediate steam break
S	Small liquid or steam break
T _U	Transients where PCS is unavailable
T _A	Transients where PCS is available
T _P	Loss of offsite power transient

The event tree headings that follow the LOCA initiating event heading identify the front-line systems that are necessary to mitigate the LOCA. A letter with no mnemonic connotation was arbitrarily assigned to each system. That letter represents the system throughout the event tree discussion. In cases where a combination of various configurations of the same system could satisfy a particular function and thus appreciably affect the course of the sequence, each definition of success was listed as a system heading, and the original system code letter (or identifier) with an arbitrary subscript was assigned to the specific system success definition. For example, the core spray system has two success definitions, depending upon the initiating event. The core spray system code is F. F_A represents successful operation of two core spray loops. F_B represents successful operation of

one core spray loop. Specific system success definitions are discussed in Appendix B. The success codes, like the front-line system codes, preserve their identity throughout the analysis. Table A-12 provides a listing of the various front-line system identifiers used in the event tree headings.

TABLE A-12. FRONT-LINE SYSTEMS LEGEND

Designator	System	Subscript Meaning
B	CRD	--
C	VS	--
D	HPCI	--
E	ADS	--
F _A	CS	Two core spray loops
F _B	CS	One core spray loop
G _A	RHR (LPCI mode)	Two LPCI pumps in same loop
G _B	RHR (LPCI mode)	Two LPCI pumps--one in each loop
G _C	RHR (LPCI mode)	Four LPCI pumps
G _D	RHR (LPCI mode)	One LPCI pump
J	OP(O)	--
K	OP(C)	--
M	RPT	--
N	MSIV	--
P	PCS	--
Q	RCIC	--
R _A	RHR (shutdown cooling)	One RHR pump and associated heat exchanger
R _B	RHR (torus cooling)	Two RHR pumps and associated heat exchangers
V	Manual depressurization	--
W	Booster and condensate pumps	--
X	RHR (SBCS mode)	--

Each sequence on an event tree is assigned a unique identifier. The identifier consists of the initiating event letter code along with the system(s) failure code associated with a particular sequence. For example, the sequence identifier for a large suction-side liquid break with subsequent failure of the torus and shutdown cooling modes of RHR would be designated $L_S R_B R_A$. This identifier will always refer to this sequence throughout this analysis.

Following each sequence (right side of figure) is an entry in a table that shows the front-line system function failures associated with each sequence. The table also contains a remarks section that shows the sequence effects on the reactor core.

Specific conditions and requirements that govern the construction of each event tree will be covered in the following discussion. Detailed system descriptions for the front-line systems discussed in the following sections will be found in Appendix B.

The success criteria delineated for each of the accident mitigating systems are based primarily on information contained in the Browns Ferry FSAR. In many cases, discussions with TVA personnel provided further clarification or supporting analyses that resulted in the specific system success criteria as given in the following sections.

3.1.1 Large Suction-side Break(L_S)

The systemic event tree for large breaks on the suction side of the recirculation pumps is shown in Figure A-8. The initiating event (L_S) for this tree is a pipe break in the range from 0.3 to 4.3 ft² (approximately to-28 in. diameter). This is a liquid break somewhere on the suction side of the large recirculation pumps used for recirculation of the primary coolant within the reactor vessel.

Front-Line System Requirements. The following front-line systems will be required to mitigate the effects of the initiating event.

Control Rod Drive (B)--Successful operation of the CRD system will be necessary to successfully perform the reactor subcriticality function. For this analysis, the control-rod drive system is considered to be failed if: (a) more than 30 control rods throughout the core fail to fully insert, (b) more than five adjacent control rods fail to fully insert.

Vapor Suppression (C)--Successful operation of the vapor suppression system will be necessary to successfully perform the SCI function. For the vapor suppression system to successfully prevent drywell pressure from exceeding design limits, LOCA effluents must be discharged from the drywell to the torus water. Therefore, the vapor suppression system is considered to be failed if bypass leakage exists between the drywell and torus airspace such that the LOCA effluents are not driven through the downcomer pipes and below the surface of the torus water where the condensibles are condensed.

Bypass could occur if one or more of the 12 vacuum breakers were open during a small LOCA or if two or more breakers are open during a large LOCA. These vacuum breakers are normally closed, with position indication lights

in the control room. They should be forced closed by the accident, and they would not be opened until long after the initial occurrence of the accident when the pressure in the wetwell might exceed the drywell pressure.

Should the torus rupture, the accident would be much more severe if the rupture were to occur below the minimum water surface because vapor suppression would be ineffective, and the break could threaten a source of water for ECI and DHR.

Core Spray (F); Low Pressure Coolant Injection (G)--Successful operation of the core spray system in conjunction with the low pressure coolant injection (LPCI) system will be necessary to successfully perform the ECI function. Failure to provide at least one of the following arrangements of the core spray and low pressure coolant injection systems will result in failure of the ECI function:

1. Two of two core spray loops (F_A), and any two of four LPCI pump combinations [i.e., two LPCI pumps in the same LPCI loop (G_A) or two LPCI pumps in different LPCI loops (G_B)].
2. One of two core spray loops (F_B), and two LPCI pumps in different loops (G_B).
3. Four of four LPCI pumps (G_C).

Residual Heat Removal--Successful operation of the RHR system will be necessary to successfully perform the DHR function. Failure to provide at least one RHR pump with its associated heat exchanger will result in failure of the DHR function.

There are two valve alignments or operating modes of the RHR system that are available for successful performance of this function. The torus cooling mode (R_B) pumps water from the torus, through the RHR heat exchangers, and returns it to the torus. The shutdown cooling mode (R_A) pumps water from the suction side of recirculation Pump A, through the RHR heat exchangers, and back into the discharge side of recirculation Pump A. Failure to provide at least two pumps and the two associated heat exchangers in the torus cooling mode (R_B) or at least one pump and its associated heat exchanger in the shutdown cooling mode (R_A) will result in failure to adequately remove decay heat from the core.

Front-Line System Interrelationships. When a large break occurs on the suction side of the recirculation pump (L_S), the CRD system is immediately challenged. Should CRD fail, a vapor suppression system branch is still included because, if the vapor suppression system is successful, the radioactivity release as a result of the imminent core melt and subsequent containment failure will be less severe than a release with no vapor suppression action. A no-decision branch is included for the ECI systems if CRD fails. It is assumed that core melt will result due to the "chugging" phenomenon. Chugging refers to the situation where the reactor becomes critical due to the introduction of relatively cold water into the core, the water heats up and causes voiding which, in turn, cause the reactor to become subcritical, and the process repeats. It was assumed that sustained chugging will ultimately lead to core melt.

With CRD success, a branch for vapor suppression system is necessary. If vapor suppression fails, core melt will not necessarily ensue. Branches will still be necessary for ECI systems. Vapor suppression success will lead to branches for the core spray and LPCI systems.

Core spray and LPCI system branches follow the logic discussed in the front-line system requirements section. Should these systems fail to perform the ECI function, the core will rapidly melt, and no branches will be necessary for RHR. When these systems are successful, the torus cooling or shutdown cooling modes of RHR will have branches. ECI is required throughout the accident; RHR functionality is dependent upon ECI success.

When the RHR system fails to perform the DHR function, decay heat will not be removed. Long-term cooling is therefore lost and ultimately the core will melt and containment overpressure failure will result. And, as indicated above, if the break occurs in Loop A, the DHR function is unavailable in the shutdown cooling mode whereby water is taken from Loop A, cooled, and returned to Loop A.

3.1.2 Large Discharge-Side Break (L_D)

The systemic event tree for large breaks on the discharge side of the recirculation pumps is shown in Figure A-9. The initiating event (L_D) for this tree is a pipe break in the same range as the suction-line break (L_S). This, too, is a liquid break. However, the break is located on the discharge side of the recirculation pumps.

A point of interest with this break is the effect that it has with regard to LPCI system response. The LPCI system is designed and operated such that each of the two LPCI discharge headers delivers flow to a separate recirculation loop. The LPCI header discharges to the recirculation system on the discharge side of the recirculation pump and prior to the recirculation pump discharge nozzles. Since the LPCI discharge header cross-connection valve is shut and deenergized, a break in the recirculation pump discharge line automatically precludes the use of one loop (two pumps) of the LPCI system. This is because the flow from the LPCI pumps in the broken loop is lost through the break. Therefore, some of the branches for accident mitigation available in the large suction break event tree will not be available for discharge-line breaks that are in the same range of break sizes.

Front-Line System Requirements. With the exception of the front-line system requirements for the ECI function, all front-line system requirements for this initiating event are the same as the requirements for mitigation of the large suction-side break (L_S). The ECI requirements are as follows:

Core Spray (F); Low Pressure Coolant Injection (G)--Successful operation of the core spray system in one arrangement, or the core spray in conjunction with the low LPCI system in another arrangement, will be necessary to successfully perform the ECI function.⁵ Failure to provide at least one of the following system arrangements will result in failure of the ECI function for this initiating event:

1. Two of two core spray loops (F_A).
2. One of two core spray loops (F_B) and one of two LPCI pumps (G_D).

Front-Line System Interrelationships. The front-line system interrelationships for this initiating event are the same as for the large suction-side break (L_S). LPCI Loop A and LPCI Pumps A and C are unavailable if the break should occur in Loop A because the coolant would be lost out the break.

3.1.3 Large Steam Line Break (L_L)

The systemic event tree for large steam breaks is shown in Figure A-10. The initiating event (L_V) for this tree is a pipe break in the range from 1.4 to 4.1 ft² (approximately 16 to 27 in. diameter).

Front-Line System Requirements. All front-line system requirements for this initiating event are similar to the requirements for mitigation of the large suction-side break (L_S) except the front-line system requirements for the ECI function.

Core Spray (F); Low Pressure Coolant Injection (G)--Successful operation of the core spray system in conjunction with the LPCI system will be necessary to successfully perform the ECI function. Since this is a steam break instead of a liquid break, the thermohydraulic effects of the break will be considerably different from those associated with liquid breaks. As a result, the system response requirements for performance of the ECI function will be different from those necessary for liquid break mitigation. Failure to provide at least one of the following system arrangements will result in failure of the ECI function:

1. Two of two core spray loops (F_A).
2. One of two core spray loops (F_B) and one of four LPCI pumps (G_D).
3. Four of four LPCI pumps (G_C).

Front-Line System Interrelationships. The front-line system interrelationships for this initiating event are the same as for the large suction-side break (L_S). The break location should have no effect on the availability of front-line systems to cope with the accident.

3.1.4 Intermediate Liquid Break (I_L)

The systemic event tree for intermediate liquid-line break is shown in Figure A-11. The initiating event (I_L) for this tree is a liquid-line break ranging from 0.12 to 0.3 ft² (approximately 4 to 7 in. diameter).

Front-Line System Requirements. With the exception of the front-line system requirements for the ECI function, all front-line system requirements for this initiating event are the same as the requirements for mitigating the large suction-side break (L_S).

HPCI (D); ADS (E); Core Spray (F); LPCI (G)--Since a liquid-line break in the intermediate range will not depressurize the reactor as quickly as a large break, the low pressure core spray system or LPCI system will not effectively perform the ECI function until reactor pressure has been lowered to the core spray/LPCI upper operating pressure limit, which is approximately 350 psig. Therefore, the HPCI system or the ADS must operate in order for the reactor pressure to decrease fast enough to allow the core spray or LPCI systems to adequately provide the ECI function. It should be noted that, for the intermediate liquid-line break, the HPCI system will not in itself provide adequate ECI function. However, the combination of the HPCI flow and depressurization of the reactor due to HPCI operation (steam is withdrawn from the reactor to run the HPCI turbine-driven pump) allows HPCI to be an alternate depressurization method, allowing the low pressure systems to inject the additional water for successful ECI.

Failure to provide at least one of the following arrangements of these systems will result in failure of the ECI function for an intermediate liquid-line break (I_L):

1. One of one HPCI pump (D) and one of four LPCI pumps (G_D) or one of two core spray loops (F_B).
2. Four of six ADS relief valves (E) and one of four LPCI pumps (G_D) or one of two core spray loops (F_B).

Front-Line System Interrelationships. The front-line system interrelationships for this initiating event are similar to those for the large suction-side break (I_S). The only difference is that for the intermediate liquid-line break the HPCI or ADS systems must assist the ECI function. ECI function failure will still have the same results.

3.1.5 Intermediate Steam Break (I_V)

The systemic event tree for intermediate steam-line breaks is shown in Figure A-12. The initiating event (I_V) for this tree is a steam-line break ranging from 0.12 to 1.4 ft² (approximately 5 to 16 in. diameter).

Front-Line System Requirements. With the exception of the front-line system requirements for the ECI function, all front-line system requirements for this initiating event are the same as the requirements for mitigation of the intermediate liquid break (I_L).

HPCI (D); Core Spray (F); LPCI (G)--For this initiating event (I_V), the HPCI system will provide adequate flow for successful ECI. This is because a steam-line break with equivalent size and upstream pressure as a liquid-line break will pass more heat per unit time. This in turn will drop pressure faster with less loss of coolant inventory than an equivalent liquid-line break. The steam flow through the break will depressurize the reactor rapidly enough for operation of the core spray or LPCI systems so no operation of the ADS is necessary. Failure to provide at least one of the following system arrangements will result in ECI failure for this initiating event:

1. One of one HPCI pump (D).
2. One of two core spray loops (F_B).
3. One of four LPCI pumps (G_D).

Front-Line System Interrelationships. The front-line system interrelationships for this initiating event are similar to those for the intermediate liquid-line break (I_L). The only difference is that, for the intermediate steam break, the HPCI system will successfully perform the ECI function without assistance from the core spray or LPCI systems, and ADS pressure relief is not required for core spray/LPCI success.

3.1.6 Small Liquid or Steam Break (S)

The systemic event tree for a small liquid-line or steam-line break is shown in Figure A-13. The initiating event (S) for this tree is a liquid-line or steam-line break that is less than 0.12 ft² (approximately 5 in. diameter).

Front-Line System Requirements. With the exception of the front-line system requirements for the ECI function, all front-line system requirements for this initiating event are the same as the requirements for mitigation of the intermediate liquid break (I_L).

HPCI (D); ADS (E); Core Spray (F); LPCI (G)--The HPCI system is designed to perform the ECI function without assistance from any other ECI front-line system when the LOCA (whether liquid or steam) is in the small-break range. That is, HPCI provides sufficient flow to compensate for the liquid or steam loss from the break (as opposed to an intermediate liquid break). Thus, for this initiating event (S), the successful operation of the HPCI system will adequately perform the ECI function regardless of reactor pressure. Should the HPCI system fail, the ADS system must depressurize the reactor for successful operation of the core spray or LPCI systems. Failure to provide at least one of the following system arrangements will result in failure of the ECI function for this initiating event:

1. One of one HPCI pump (D).
2. Four of six ADS relief valves (E) and one of four LPCI pumps (G_D) or one of two core spray loops (F_B).

Front-Line System Interrelationships. The front-line system interrelationships for this initiating event are similar to those for the intermediate liquid break (I_L). The only difference is that, unlike the intermediate break event sequence, the reactor will not depressurize immediately following the break. This will preclude the use of the core spray or LPCI systems for ECI because they are not effective at high reactor pressures. Therefore, some means of high pressure injection is necessary for performance of the ECI function at high reactor pressure. This is accomplished by the HPCI system. For this break range, the HPCI system will deliver adequate injection flow regardless of the break location. Should the HPCI system fail to perform this function satisfactorily, the

ADS system will activate on increasing drywell pressure and depressurize the reactor so the core spray and LPCI systems can perform the ECI function. As in the other cases, should ECI fail, the core will melt.

3.2 Transient Systemic Event Tree Description

The transient systemic event tree identifies the combinations of systems necessary to achieve the functional success described in the functional event tree description. There are two systemic event trees describing the two categories of transients: those where the PCS is unavailable (Figure A-14) and those where the PCS is available (Figure A-15).

Specific conditions and requirements that govern the construction of each event tree will be covered in the following discussion. Detailed system descriptions for the front-line systems discussed in the following sections are found in Appendix B.

3.2.1 Transients Where PCS is Unavailable (T_U)

The systemic event tree for transients that render the PCS unavailable for accident mitigation is shown in Figure A-14.

Front-Line Systems Requirements. The following front-line systems will be required to mitigate the effects of the T_U transients.

Control Rod Drive (B)--Successful operation of the CRD system will be necessary to successfully perform the reactor subcriticality function. For this analysis, the control-rod drive system is considered to be failed if: (a) more than 30 control rods throughout the core fail to fully insert, (b) more than five adjacent control rods fail to fully insert.

Overpressure Protection--The overpressure protection function consists of a two-part requirement on the primary system safety relief valves. The first requires that a sufficient number of relief valves open (Event J) to limit the pressure rise to below emergency stress levels. Depending upon the transient and whether or not the reactor scram was caused by a direct signal (valve position for example) or an indirect signal (high flux or high pressure), a different number of valves must open to accomplish this function (see Table A-3). Sequence T_UJ is probabilistically insignificant because of the large number of relief valves available (13) versus the maximum number required (10) per Table A-3. It was therefore not considered further in the analysis.

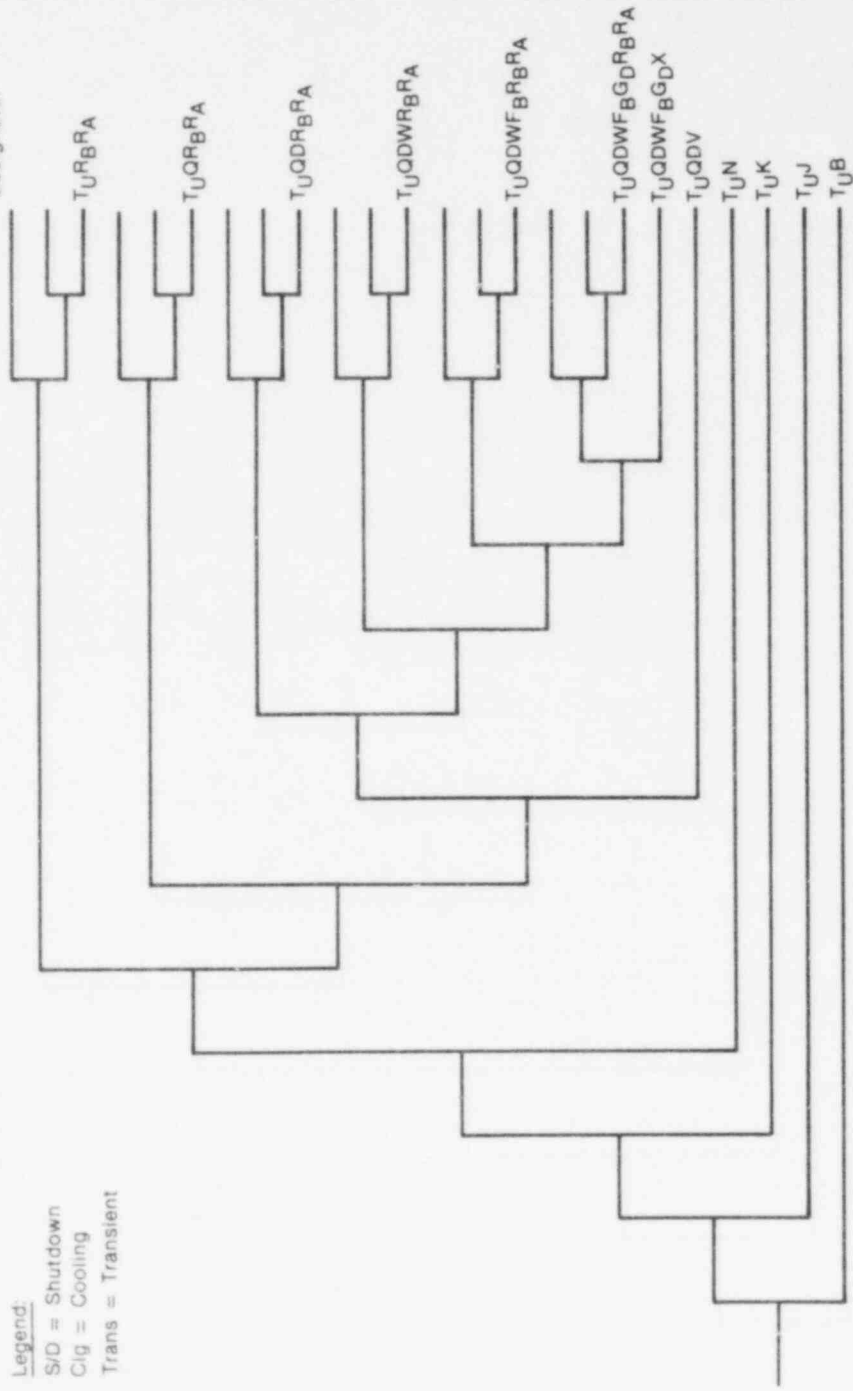
The second part of overpressure protection requires that all relief valves reclose (Event K) after pressure has been reduced below their set-points. Failure of either of these functions results in a transient-induced LOCA sequence.

MSI; HPI; LPI--Successful operation of the VWI function requires isolation of the main condenser from the reactor vessel and injection of water from either the high or low pressure systems.

For this analysis, main steam isolation (Event N) is considered to succeed if:

AT		RS		OP		MSI				HPI			VWI				DHR	
Trans	CRD	RV(O)	RV(C)	MSIV	RCIC	HPCI	DEP	COND	1 CS Loop	1 LPCI	SBCS	Torus Cig	RHR	S/D Cig	RA			
T _U	B	J	K	N	Q	D	V	W	F B	G D	X	R _B						

Legend:
 S/D = Shutdown
 Cig = Cooling
 Trans = Transient



X = Function failure

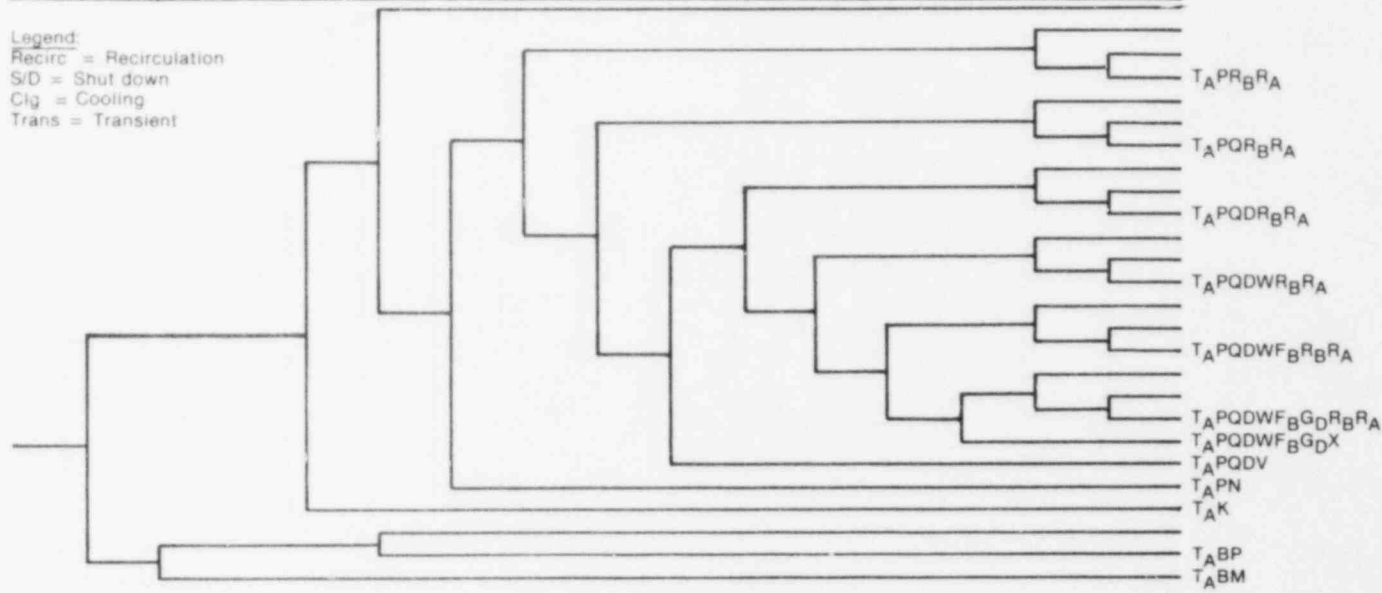
R S	O P	V W	D H R	Remarks
				Core cooled
			X	Core cooled
			X	Slow melt
			X	Core cooled
			X	Core cooled
			X	Slow melt
			X	Core cooled
			X	Core cooled
			X	Slow melt
			X	Core cooled
			X	Core cooled
			X	Slow melt
			X	Core cooled
			X	Core cooled
			X	Slow melt
			X	Melt
			X	Melt
			X	LOCA initiator
X			N/A	LOCA initiator
X			N/A	LOCA initiator
X			N/A	LOCA initiator
X			N/A	Melt

INEL 2 1637

Figure A-14. Transient systemic event tree where PCS is unavailable (T_U).

AT	RS		OP		VWI								DHR		
AT	RS	RPT	OP		PCS	MSI	HPI		LPI			RHR			
Trans	CRD	Recirc Pumps	RV(O)	RV(C)	PCS	MSIV	RCIC	HPCI	DEP	COND	1 CS Loop	1 LPCI	SBCS	Torus Clg	S/D Clg
T _A	B	M	J	K	P	N	Q	D	V	W	F _B	G _D	X	R _B	R _A

Legend:
 Recirc = Recirculation
 S/D = Shut down
 Clg = Cooling
 Trans = Transient



X = Function failure

R	O	V	D	Remarks
S	P	W	H	
	I		R	
				Core cooled
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
			X	Slow melt
				Core cooled
			X	Slow melt
				Core cooled
			X	Slow melt
				Core cooled
			X	Slow melt
				Core cooled
			X	Slow melt
				Core cooled
			X	Melt
			X	N/A Melt
			X	N/A LOCA initiator
			X	N/A LOCA initiator
X	N/A		N/A	Core cooled
X	N/A	X	N/A	Melt
X	N/A	N/A	N/A	Melt

INEL 2 1638

Figure A-15. Transient systemic event tree where PCS is available (T_A).

1. Either an inboard or an outboard valve in all four main steam lines shuts.
2. All four turbine valves and all four bypass valves shut.

HPI is considered to succeed if either the RCIC or HPCI succeed.

LPI will fail if one of the following LPI systems in conjunction with manual depressurization is not provided:

1. One of four LPCI pumps (G_D).
2. One of two core spray loops (F_B).
3. One booster and one condensate pump (W).
4. One RHRSW pump in the SBCS mode (X).

It should be noted that the one booster and condensate pump (Event W) may still be available depending on how the transient effects the PCS; i.e., the PCS can be unavailable but the condensate and booster pumps might still work.

Residual Heat Removal--Successful operation of the RHR system will be necessary to successfully perform the DHR function. There are two valve alignments or operating modes of the RHR system that are available for successful performance of this function. The torus cooling mode (R_B) pumps water from the torus through the RHR heat exchangers and returns it to the torus. The shutdown cooling mode (R_A) pumps water from the suction side of recirculation Pump A through the RHR heat exchangers and back into the discharge side of recirculation Pump A. Failure to provide at least two pumps and the two associated heat exchangers in the torus cooling mode (R_B) or at least one pump and its associated heat exchanger in the shutdown cooling mode (R_A) will result in failure to adequately remove decay heat from the core.

Front-Line System Interrelationships. For transients where the PCS is unavailable, the CRD system must respond to achieve reactor subcriticality. Should CRD fail, a core melt is assumed. With CRD success, the safety relief valves must open to relieve primary system pressure. Failure of these valves to open is assumed to result in a primary system pressure boundary rupture. Failure of these valves to reclose after opening or failure of isolation valves in the main steam lines to close will also result in LOCA initiation. Failure of a sufficient number of safety relief valves to open and failure of isolation valves in the main steam lines to close were determined to be probabilistically insignificant compared to other LOCA initiation frequencies. However, initiation LOCA due to a SORV is the most likely of all LOCA initiators and is similar to an intermediate steam line break. However, since reactor subcriticality is already successful and no choice for short-term containment integrity is required (the discharge from the relief valves goes directly to the torus), this LOCA sequence transfers directly into the intermediate steam break systemic event tree (Figure A-12) at the ECI decision branchpoint. This initiator is designated T_{JK} for transients where PCS is unavailable and T_{PK} for the LOSP transient.

The HPI systems branches follow the logic discussed in the front-line systems requirements section. Should these systems fail to perform the VWI function, manual depressurization will be necessary in order that one of various LPI systems can function. VWI failure will result in a rapid core melt and no branches are developed for RHR. When VWI is successful, the torus cooling or shutdown cooling modes of RHR will have branches.

When the RHR system fails to perform the DHR function, decay heat will not be removed. Long-term cooling is therefore lost and ultimately the core will melt and containment failure will result.

3.2.2 Transients Where PCS is Available (T_A)

The systemic event tree for transients where the PCS remains available for accident mitigation is shown in Figure A-15.

Front-Line Systems Requirements. The front-line systems needed to cope with transients where PCS is available are as follows:

Control Rod Drive (B)--The success requirements for the CRD system are the same as described previously for the T_U transient systemic event tree.

Reactor Pump Trip (M)--For one special case, failure to achieve a subcritical condition with the control rods after a scram does not necessarily result in a core melt. If the RPT system and PCS are available to remove heat via the bypass valves, then core melt will not occur. The resulting power level after successful RPT is such that the capacity of the bypass valves is adequate to remove the heat being generated. Successful RPT requires that both recirculation pumps trip upon receipt of the proper reactor protection system signals.

Overpressure Protection--Since the PCS is still initially available following the initiating event, sufficient steam is being removed so that no relief valves are required to open (Event J). However, it is likely that some may open and therefore are required to reclose (Event K). Failure of any valve to reclose results in a LOCA initiation.

Power Conversion System (P)--The PCS provides both the VWI and DHR systems function by removing steam from the reactor, condensing the steam, and returning the water to the reactor via the feed pumps. Successful PCS operation requires that the condenser is available and the feed system is providing makeup water to the reactor vessel.

The success criteria for the remaining functions and systems are the same as those described previously for the systemic event trees for the transients where PCS is unavailable.

Front-Line System Interrelationships. For transients where the PCS remains available following the initiating event, the CRD system is challenged to provide a reactor scram. CRD failure does not necessarily result in a core melt if the recirculation pumps trip and PCS remains available. Either failure of either pump to trip or subsequent loss of the PCS results in a core melt. With CRD success, spurious actuation of relief valves could

result in a SORV condition. This LOCA initiator transfers to the intermediate steam break LOCA systemic event tree (Figure A-12) at the ECI decision branchpoint. This initiator is designated T_AK for transients where PCS is available.

The PCS (if it remains available) can be used to bring the reactor to a stable shutdown condition. If the PCS fails before hot shutdown is achieved, MSI will be required so that the HPI and LPI systems can function. The front-line system interrelationships for the HPI, LPI, and RHR systems are the same as discussed previously for the T_U transient systemic event tree.

4. SEQUENCE DEPENDENT OPERATOR ACTIONS

4.1 Introduction

The BFI is designed to provide automatic safety system response to accidents that could occur at the plant. The plant EOIs tell the operator to verify that all automatic actions have occurred and, if not, place controls on manual and make corrective manipulations. However, the operator is cautioned not to place controls on manual unnecessarily when automatic control is functioning properly unless some unsafe plant condition will result.

In some cases, the operator is instructed to take equipment out of service when it is no longer needed or when less than full system response is required. For example, for a large break LOCA, EOI-36 instructs the operator in Step IV.A, "Subsequent Operator Actions," to do the following:

When reactor level approaches normal, upon SRO approval, start reducing the number of LPCI and core spray pumps until equilibrium is reached before the vessel is completely filled.

The following safety systems at BFI rely solely on manual actuation for proper system operation:

- RHRSW
- RHR
- EPS (bus transfers)
- ADS (manual depressurization)
- SBCS.

Of these systems, only the manual operation of the RHR, and associated service water system, and manual depressurization of the reactor vessel were important from an accident sequence standpoint. The correct manual operation of the RHR and RHRSW systems is obviously required for a LOCA or transient sequence (where PCS is unavailable) to eventually result in successful long-term DHR core cooling. Similarly, since the transient initiators do not result in automatic ADS actuation (the high drywell pressure signal is not present as it is for a LOCA), depressurization by the operator of the reactor vessel with the relief valves is required to allow the LPI systems to function, given that the HPI systems have failed.

4.2 System/Sequence Operator Actions

The following sections describe the operator actions required for each of the above systems, the coded event name that appears on the fault trees, and the rationale for the failure probability value assigned to the event.

4.2.1 Residual Heat Removal Service Water

When it is determined by the operator that a RHRSW pump is needed and which one is to be used, the appropriate pump is started. After the pump is running, the service water discharge valve for the associated heat exchanger is opened until the desired flow is reached. All of these actions are done from the control room.

The coded event name on the RHRSW fault tree for the operator failing to initiate cooling is SOIO23_D, where S is the RHRSW system identifier; OIO23 refers to Operating Instruction 23, which establishes the procedure; and D is the failure-mode code for operator response error. The blank space is filled in with A, B, C, or D depending upon the appropriate RHRSW header.

An explicit human error model was developed for failure to perform this action using Swain and Guttman's human reliability handbook.⁶ The HEP obtained from this model is 5.5×10^{-4} per act. The human error models that were developed can be found in Section 4 of Appendix B.

4.2.2 Residual Heat Removal

All modes of RHR operation other than the LPCI mode are manually initiated. In the torus cooling mode, the operator must start the RHR pumps and align the discharge valves to the desired flow path. In the shutdown cooling mode, the operator must align the suction valves of the desired RHR loop to the recirculation Loop A, start a RHR pump, and align the discharge valves to the recirculation loop discharge path desired. All of these actions are done from the control room. Operation in either of these modes requires that the RHRSW system be put into service. OI-74 governs the procedure for establishing the above-mentioned RHR modes. The EOIs for the potential accidents at BFl instruct the operator to: "If necessary, initiate suppression pool cooling to maintain suppression pool temperature below 95°F." This can be achieved by removing heat directly from the torus (torus cooling mode) or by removing heat from the reactor core directly, thereby preventing further heat from being added to the suppression pool (shutdown cooling mode).

The coded event names on the RHR fault tree for the operator failing to initiate cooling are RRBO001D for torus cooling and RRA0001D for shutdown cooling, respectively.

Detailed human reliability models were not developed for the operator response to initiate these modes of RHR cooling since the actions required of the operator are very similar to those required for establishing RHRSW flow. However, since explicit models were not developed, a conservative estimate of 10^{-3} per act was used for each RHR cooling mode rather than the 5.5×10^{-4} per act probability obtained from quantification of the RHRSW HEP model. Since these actions did not contribute significantly to any probabilistically significant accident sequences (even using this conservative value) a detailed model was not constructed.

4.2.3 Automatic Depressurization System

As previously mentioned, for those transient accident sequences where the high pressure systems (HPCI and RCIC) are failed, the operator must use the safety relief valves to depressurize the reactor vessel in order for the LPI systems to function. BFl GOI-100-1 governs these actions for those sequences where the PCS is not available. GOI-100-1, Step VII, "Emergency Shutdown with MSIVs Closure," Item I states:

If MSIVs cannot be reopened, start suppression pool cooling with RHR Sys. per OI-74. Upon the shift engineer's approval, start depressurization of the reactor at a rate to decrease temperature $<90^{\circ}\text{F}$ per hour by manually operating relief valves. Alternate relief valve operations so that each valve is opened approximately the same amount of time.

Since only 4 of 13 valves are required to successfully depressurize, failure of the operator to perform this act when required dominates the probability of failure for this function. This event is Event V on the transient systemic event trees.

An explicit HEP model was developed for this important operator response. A value of 3×10^{-3} per act was obtained from this model. This model is included in Section 4 of Appendix B. Further investigation revealed that recovery actions should be considered for this model. A recovery model was developed that resulted in an HEP of 1.8×10^{-4} . Details of this model are also included in Section 4 of Appendix B.

4.2.4 Electrical Bus Transfers

EOI-5 for BFl covers a variety of postulated EPS bus failures. Subsequent operation actions called for in these procedures provides for manual transfer to alternate equipment (such as battery chargers) on buses to restore a given bus to service. These transfers basically require opening a circuit breaker to isolate the failed source and then closing the breaker to the alternate power source. These events are coded in the basic form of ACB__D, where:

- A = system identifier for the EPS
- CB = code for circuit breaker
- D = failure mode code for operator response error.

No explicit models were developed for "Operator fails to initiate transfer." Due to the limited action required of the operator (i.e., opening and closing circuit breakers in the main control room), an assigned value of 10^{-3} per act was felt to be conservative since these actions are similar to those required for placing RHRSW in service. Transfers as a means of recovery, as such, were not important to sequence quantification for two reasons:

1. Electrical bus failures were dominated by local bus faults that would not be corrected by transferring to alternate power sources.

2. In a separate analysis (discussed in Section 1.3.2), various electrical buses were postulated to be failed to determine the effect on mitigating systems. The only significant bus failure identified was LOSP. LOSP becomes important with subsequent loss of the diesel generators. Under these conditions alternate power sources (other than battery systems) are not available.

4.2.5 Standby Coolant Supply System

The SBCS is a special mode of aligning the RFRSW to provide a "last-ditch" effort to provide river water injection to the core via the RHRSW and RHR systems. EOI-41 instructs the operator to verify that one of the two D header pumps, D₁ or D₂, is running. Then the cross-connect valves between the RHRSW and RHR systems are opened and the D heat exchanger outlet valve closed.

The coded event name on the SBCS fault tree model for the operator failing to initiate cooling is XE01041D, where:

X = system identifier for the SBCS
EOI041 = EOI-41
D = failure mode code for operator response error.

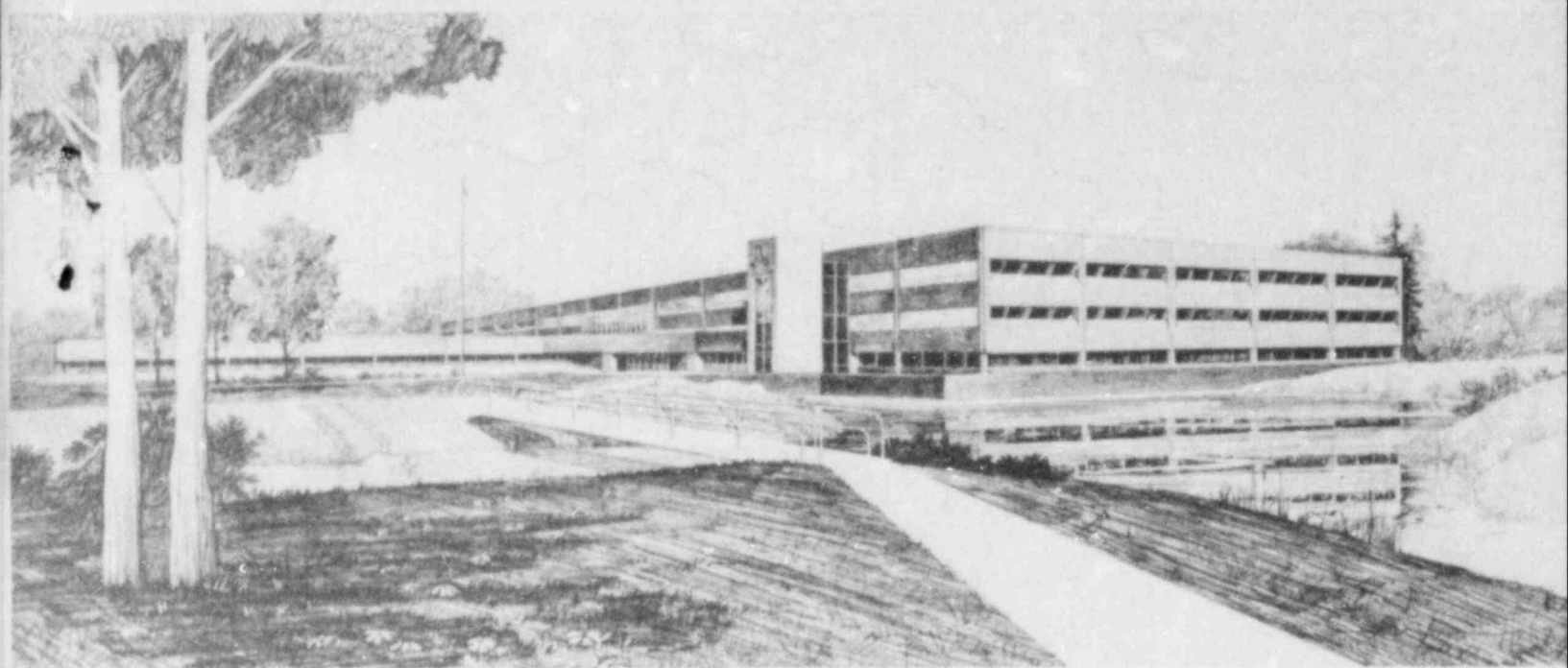
A value of 5×10^{-3} per act was obtained from a human error model for these required actions. The model for this action is presented in Section 4 of Appendix B.

No sequences involving SBCS failure were probabilistically important since before the SBCS would be used, the high pressure injection systems would have to be failed along with the other low pressure systems, i.e., the condensate system, core spray system, and LPCI system.

REFERENCES

1. Reactor Safety Study--An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014), October 1975.
2. F. L. Leverenz, Jr., J. M. Koren, R. C. Erdmann, and G. S. Lellouche, ATWS: A Reappraisal Part II: Frequency of Anticipated Transients, EPRI NP-801, Electric Power Research Institute, June 1978.
3. A. S. McClymont and B. W. Poehlman, ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients, EPRI NP-2230, Electric Power Research Institute, January 1982.
4. R. B. Ruger, Browns Ferry Nuclear Plant Bus Failure Analysis, Rev. 0, Tennessee Valley Authority, June 1980.
5. Browns Ferry Nuclear Plant Units 1 and 2 Emergency Core Cooling Systems Low Pressure Coolant Injection Modifications for Performance Improvements, Rev. 1, TVA's proposal to NRC for changes to Technical Specifications (J. E. Gilliland to B. C. Rusche), February 12, 1976.
6. A. D. Swain and H. E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, October 1980.

EG&G Idaho, Inc.
P.O. Box 1625
Idaho Falls, Idaho 83415



U.S. Department of Energy

Idaho Operations Office • Idaho National Engineering Laboratory

Interim Reliability Evaluation Program: Analysis of the Browns Ferry, Unit 1, Nuclear Plant

Appendix B— System Descriptions and Fault Trees

EG&G Idaho, Inc.


Energy Incorporated, Seattle Office

S. E. Mays
J. P. Poloski
W. H. Sullivan
J. E. Trainer

R. C. Bertucio
T. J. Leahy

July 1982

Prepared for the
U.S. Nuclear Regulatory Commission
Under Sandia National Laboratories
Purchase Order No. 62-7776

 **EG&G** Idaho
8209270364

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, nor 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

**INTERIM RELIABILITY EVALUATION PROGRAM:
ANALYSIS OF THE BROWNS FERRY,
UNIT 1, NUCLEAR PLANT**

**APPENDIX B—SYSTEM DESCRIPTIONS AND
FAULT TREES**

EG&G Idaho, Inc.

S. E. Mays
J. P. Poloski
W. H. Sullivan
J. E. Trainer

Energy Incorporated, Seattle Office

R. C. Bertucio
T. J. Leahy

Published July 1982

**EG&G Idaho, Inc.
Idaho Falls, Idaho 83415**

Prepared for the
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
Under Sandia National Laboratories
Purchase Order No. 62-7776
FIN No. A1241

FOREWORD

This report describes a risk study of the Browns Ferry, Unit 1, nuclear plant. The study is one of four such studies sponsored by the NRC Office of Research, Division of Risk Assessment, as part of its Interim Reliability Evaluation Program (IREP), Phase II. Other studies include evaluations of Arkansas One, Unit 1, by Sandia National Laboratories; Calvert Cliffs, Unit 1, by Science Applications, Inc.; and Millstone, Unit 1, by Science Applications, Inc. EG&G Idaho, Inc. was assisted by Energy Inc., Seattle, in its evaluation of the Browns Ferry, Unit 1, plant. Battelle-Columbus Laboratories provided information regarding the fission product releases that result from risk-significant accident scenarios. Sandia National Laboratories has overall project management responsibility for the IREP studies. It also has responsibility for the development of uniform probabilistic risk assessment procedures for use on future studies by the nuclear industry.

This report is contained in four volumes: a main report and three appendixes. The main report provides a summary of the engineering insights acquired in doing the study and a discussion regarding the accident sequences that dominate the risks of Browns Ferry, Unit 1. It also describes the study methods and their limitations, the Browns Ferry plant and its systems, the identification of accidents, the contributors to those accidents, and the estimating of accident occurrence probabilities. Appendix A provides supporting material for the identification of accidents and the development of logic models, or event trees, that describe the Browns Ferry accidents. Appendix B provides a description of Browns Ferry, Unit 1, plant systems and the failure evaluation of those systems as they apply to accidents at Browns Ferry. Appendix C generally describes the methods used to estimate accident sequence frequency values.

Numerous acronyms are used in the study report. For each volume of the report, these acronyms are defined in a listing immediately following the table of contents.

CONTENTS

FOREWORD	B-ii
NOMENCLATURE	B-xi
1. INTRODUCTION	B-1
1.1 General Discussion of Appendix B Contents	B-1
1.2 Shared Systems Between Browns Ferry, Units 1, 2, and 3	B-3
1.3 Treatment of Test and Maintenance Restoration Errors	B-6
2. FRONT-LINE SYSTEM FAULT ANALYSES	B-7
2.1 Reactor Core Isolation Cooling System	B-7
2.2 Residual Heat Removal System	B-36
2.3 High Pressure Coolant Injection (HPCI) System	B-109
2.4 Automatic Depressurization System	B-146
2.5 Safety Relief Valves	B-169
2.6 Manual Depressurization	B-172
2.7 Core Spray System	B-173
2.8 Vapor Suppression System	B-234
2.9 Control Rod Drive Hydraulic System	B-243
2.10 Power Conversion System, Including Condensate/ Booster Pumps	B-251
2.11 Standby Coolant Supply System	B-255
2.12 Recirculation Pump Trip System	B-255
2.13 Main Steam Isolation Valves	B-260
3. SUPPORT SYSTEM FAULT ANALYSES	B-266
3.1 Electrical Power System	B-266
3.2 Residual Heat Removal Service Water System	B-351
3.3 Emergency Equipment Cooling Water System	B-381
3.4 Keep-Full System	B-419
3.5 Condenser Circulating Water System	B-421

3.6	Raw Cooling Water System	B-425
3.7	Reactor Protection System	B-427
3.8	Equipment Area Cooling System	B-431
4.	HUMAN ERROR MODELS AND PROBABILITIES	B-433
4.1	Miscalibration Errors	B-433
4.2	Operational Errors	B-454
4.3	Recovery Model	B-456
4.4	Relevant Procedures	B-456
5.	GENERIC CONTROL CIRCUIT ANALYSES	B-457
5.1	Introduction	B-457
5.2	Generic Motor-Operated Valve Control Circuit	B-457
5.3	Generic Motor-Driven Pump Control Circuit	B-461
	ATTACHMENT A--EVENT NAMING CODE	B-465
	ATTACHMENT B--SI 4.2.B-1	B-473
	ATTACHMENT C--SI 4.2.B-5 and IMI-202	B-479
	ATTACHMENT D--EOI-41	B-487

FIGURES

B-1.	RHR/RHRSW/EECW systems power dependencies	B-5
B-2.	RCIC system	B-8
B-3.	RCIC initiation circuitry	B-15
B-4.	RCIC fault tree	B-22
B-5.	RHR system, Loop 1	B-37
B-6.	RHR initiation circuitry	B-46
B-7.	RHR fault trees	B-53
B-8.	HPCI system	B-111
B-9.	HPCI initiation circuitry	B-118
B-10.	Auxiliary oil pump starting circuitry	B-119

B-11. HPCI fault tree	B-127
B-12. Automatic depressurization system (ADS)	B-148
B-13. ADS initiation circuitry	B-152
B-14. ADS reduced fault tree	B-157
B-15. Core spray system	B-174
B-16. Core spray initiation circuitry	B-181
B-17. Core spray fault tree	B-191
B-18. Vapor suppression part of the primary containment system	B-237
B-19. Vapor suppression fault tree	B-240
B-20. CRDH system	B-244
B-21. Scram discharge volume equipment	B-246
B-22. CRDH fault tree	B-248
B-23. Main steam system	B-252
B-24. Condensate and feedwater systems	V-253
B-25. Recirculation-pump trip circuit	B-257
B-26. Recirculation-pump trip-circuit fault tree	B-258
B-27. Main steam isolation system	B-261
B-28. Logic diagram for closure of a MSIV	B-263
B-29. MSI fault tree	B-264
B-30. EPS diagram showing AC and DC systems	B-267
B-31. EPS fault tree	B-288
B-32. RHRSW system	B-352
B-33. RHRSW/EECW systems power dependencies	B-355
B-34. RHRSW fault tree	B-362
B-35. EECW system	B-382
B-36. EECW auto-initiation logic for B3 pump.....	B-387
B-37. EECW fault tree	B-393

B-38. Keep-full system	B-420
B-39. CCW system	B-423
B-40. RCW system	B-426
B-41. RCW fault tree	B-428
B-42. RPS Channel A	B-430
B-43. Simplified diagram of EAC system	B-432
B-44. HEM--maintenance person causes failure of reactor level switches (see Box A)	B-436
B-45. HEM--maintenance person causes failure of drywell pressure switches (see Box B)	B-438
B-46. HEM--operator fails to manually depressurize the reactor (see Box C)	B-440
B-47. HEM--operator fails to transfer RCIC suction to the torus (see Box D)	B-442
B-48. HEM--operator fails to manually isolate RCIC pump suction for the CST (see Box E)	B-444
B-49. HEM--operator fails to initiate RHRSW cooling (see Box F)	B-446
B-50. HEM--operator fails to initiate SBCS (see Box G)	B-448
B-51. HEM--operator fails to manually depressurize the reactor (with recovery) (see Box H and Table 88)	B-550
B-52. Motor-operated valve-control circuit	B-458
B-53. Motor-driven pump-control circuit	B-462

TABLES

B-1. RCIC system FMEA of component/supporting-system interactions	B-10
B-2. RCIC system test requirements summary	B-17
B-3. RCIC system maintenance acts summary	B-19
B-4. RCIC system fault summary short form	B-27
B-5. RCIC system failure data summary	B-33
B-6. RCIC system cut sets	B-36

B-7.	RHR system operational mode success criteria	B-38
B-8.	RHR system FMEA of component/support-system interactions	B-40
B-9.	RHR system test requirements summary	B-51
B-10.	RHR system maintenance acts summary	B-52
B-11.	RHR system fault summary short form	B-79
B-12.	RHR system house events status	B-95
B-13.	RHR system failure data summary	B-97
B-14.	RHR system cut sets (G_A)	B-99
B-15.	RHR system cut sets (G_B)	B-100
B-16.	RHR system cut sets (G_C)	B-101
B-17.	RHR system cut sets (G_D)	B-102
B-18.	RHR system cut sets (G_D with break on Loop 2)	B-103
B-19.	RHR system cut sets (R_A for Loop 1)	B-103
B-20.	RHR system cut sets (R_A for Loop 2)	B-104
B-21.	RHR system cut sets (R_B)	B-105
B-22.	RHR system cut sets (G_D with LOSP)	B-106
B-23.	RHR system cut sets (R_A Loop 1 with LOSP)	B-107
B-24.	RHR system cut sets (R_A Loop 2 with LOSP)	B-108
B-25.	RHR system cut sets (R_B with LOSP).....	B-109
B-26.	HPCI system FMEA of component/support-system interactions	B-113
B-27.	HPCI system test requirements summary	B-123
B-28.	HPCI system maintenance acts summary	B-126
B-29.	HPCI system house events status	B-132
B-30.	HPCI system fault summary short form	B-135
B-31.	HPCI system failure data summary	B-142
B-32.	HPCI system cut sets (transient)	B-145

B-33. HPCI system cut sets (LOCAs)	B-145
B-34. ADS FMEA of component/support-system interactions	B-149
B-35. ADS fault summary short form	B-162
B-36. ADS failure data summary	B-168
B-37. ADS cut sets	B-169
B-38. Core spray system FMEA of component/support-system interactions	B-178
B-39. Core spray system test requirements summary	B-185
B-40. Core spray system maintenance acts summary	B-188
B-41. Core spray system house events status	B-206
B-42. Core spray system LOCA mitigation success criteria	B-207
B-43. Core spray system transient mitigation success criteria	B-210
B-44. Core spray system fault summary short form	B-212
B-45. Core spray system failure data summary	B-230
B-46. Core spray system cut sets (F_A)	B-232
B-47. Core spray system cut sets (F_B)	B-233
B-48. Core spray system cut sets (F_B with LOSP)	B-234
B-49. Vapor suppression system FMEA of component/supporting- system interactions	B-238
B-50. Vapor suppression system test requirements summary	B-239
B-51. Vapor suppression system fault summary short form	B-241
B-52. Vapor suppression system failure data summary	B-242
B-53. Vapor suppression system cut sets	B-243
B-54. SBCS system cut sets (normal power)	B-256
B-55. SBCS system cut sets (with LOSP)	B-256
B-56. RPT fault summary short form	B-259
B-57. RPT system cut sets	B-260
B-58. EPS FMEA of component/supporting-system interactions	B-269

B-59. EPS breaker interlock and control description	B-277
B-60. EPS test requirements summary	B-284
B-61. EPS maintenance acts summary	B-285
B-62. EPS fault summary short form	B-320
B-63. EPS failure data summary	B-347
B-64. EPS cut sets (4160 V shutdown Board A) (Gate SDA)	B-349
B-65. EPS cut sets (480 V AC RMOV Board 1A) (Gate AR1A)	B-349
B-66. EPS cut sets (480 V AC RMOV Board 1D) (Gate AR1D)	B-349
B-67. EPS cut sets (250 V DC RMOV Board 1A) (Gate DR1A)	B-350
B-68. EPS cut sets (diesel auxiliary Board A) (Gate DA)	B-350
B-69. EPS cut sets (shutdown Board A with LOSP) (Gate SDA with LOSP).....	B-350
B-70. RHRSW system FMEA of component/supporting-system interactions	B-356
B-71. RHRSW system test requirements summary	B-359
B-72. RHRSW system maintenance acts summary	B-360
B-73. Service assignments for RHRSW pumps	B-360
B-74. RHRSW system fault summary short form	B-369
B-75. RHRSW system failure data summary	B-379
B-76. RHRSW system cut sets (RHRSW Header A)	B-381
B-77. EECW FMEA of component/support-system interactions	B-384
B-78. EECW system test requirements summary	B-388
B-79. EECW system failure data summary	B-389
B-80. EECW system maintenance acts summary	B-391
B-81. EECW system fault summary short form	B-403
B-82. EECW system cut sets (Gate K2)	B-417
B-83. EECW system cut sets (LOSP)	B-418
B-84. Head tank levels	B-421

B-85. RCW system fault summary short form	B-429
B-86. IREP human error probabilities	B-434
B-87. Event descriptions for the level switch model	B-452
B-88. Event descriptions for the manual depressurization model (with recovery)	B-455
B-89. Motor-operated valve generic control circuit	B-459
B-90. Motor-driven pump control circuit	B-463

NOMENCLATURE

\bar{A}	The complement of A (a success event if A is a failure event). (\bar{A} may also be used to mean "unavailability.")
A	Alarm
AC	Alternating current
ACC	Accumulator
ADS	Automatic depressurization system
AH	Alarm-high
AO	Air operator
APRM	Average power range monitor
AT	Anticipated transient
ATWS	Anticipated transient without scram
BF1	Browns Ferry, Unit 1, nuclear plant
BI	Break isolation
BWR	Boiling water reactor
CAD	Containment atmosphere dilution
CCW	Condenser circulating water
CD	Complete dependence
CE	Conductivity element
CIS	Containment isolation system
C _{lg}	Cooling
COND	Main condenser
CR-3	Crystal River, Unit 3, nuclear plant IREP study
CRD	Control rod drive
CRDH	Control rod drive hydraulic
CRDHS	Control rod drive hydraulic system
CRW	Clean rad waste
CS	Core spray
CS&T	Condensate storage and transfer
CSCS	Core standby cooling system
CSS	Core spray system
CST	Condensate storage tank
CV	Control valve
D	Demand
DC	Direct current
DEP	Depressurization
DG	Diesel generator
DHR	Decay heat removal
Diff	Different
DPI	Differential pressure indicator
DPIS	Differential pressure indicating switch
DPS	Differential pressure switch
DPT	Differential pressure transmitter
EAC	Equipment area cooling
ECCS	Emergency core cooling system
ECI	Emergency coolant injection
EECW	Emergency equipment cooling water
EHC	Electro-hydraulic control

EMI	Electrical Maintenance Instruction
EOI	Equipment Operating Instructions
EPRI	Electric Power Research Institute
EPS	Electrical power system
ESFAS	Engineered safety features actuation system
F(•)	Frequency of initiator in parentheses
FCV	Flow control valve
FE	Flow element
FI	Flow indicator
FIC	Flow indicating controller
FLS	Front-line system
FMEA	Failure mode effects analysis
FR	Flow recorder
FS	Flow switch
FSAR	Final Safety Analysis Report
FT	Flow transmitter
FWC	Feedwater control
FWCS	Feedwater control system
G	Green
GOI	General Operating Instructions
H	High
H/L	High/low
HCU	Hydraulic control unit
HCV	Hand control valve
HEP	Human error probability
HPCI	High pressure coolant injection
HPCS	High pressure core spray
HPI	High pressure injection
HS	Handswitch
HSS	High speed stop
HVAC	Heating, ventilation, and airconditioning
HX	Heat exchanger
I&C	Instrumentation and control
I&E	Inspection and enforcement
IMI	Instrument Maintenance Instruction
INJ	Injection
IREP	Interim Reliability Evaluation Program
IRM	Intermediate range monitor
L	Low
LA	Level alarm
LD	Low dependence
LER	Licensee Event Report
LIC	Level indicating controller
LIS	Level indicating switch
LL	Low-low
LOCA	Loss of coolant accident
LOSP	Loss of offsite power
LPCI	Low pressure coolant injection
LPI	Low pressure injection

LS	Limit switch
LSS	Low speed stop
LT	Level transmitter
M	Motor (operated valve)
MCR	Main control room
MD	Moderate dependence
MGU	Master governor unit
MMG	Motor generator
MMI	Mechanical Maintenance Instruction
MO	Motor operated
MOV	Motor-operated valve
MSC	Manual speed control
MSI	Main steam isolation
MSIV	Main steam isolation valve
MSL	Main steam line
NA; N/A	Not applicable
NC	Normally closed
NMS	Neutron monitoring system
NO	Normally open
OI	Operating Instructions
OL	Overload
OP	Overpressure protection
OP(C)	Overpressure protection (relief valves closed)
OP(O)	Overpressure protection (relief valves open)
PA	Pressure alarm
PB	Pipe break
PCIS	Primary containment isolation system
PCS	Power conversion system
PCV	Pressure control valve
PG	IREP Procedure Guide
PI	Pressure indicator
PORV	Power-operated relief valve
PRA	Probabilistic risk assessment
PS	Pressure switch
PSCWT	Pressure suppression chamber water transfer
PT	Pressure transmitter
PWR	Pressurized water reactor
Q(•)	Unavailability of system in parentheses
QA	Quality assurance
R	Red
RBCCW	Reactor building component cooling water
RBEDT	Reactor building equipment drain tank
RCE	Reactor coolant boundary
RCIC	Reactor core isolation cooling
RCS	Reactor coolant system
RCW	Raw cooling water
RCWS	Raw cooling water system
Recirc	Recirculation

RFP Reactor feed pump
 RFPT Reactor feed pump turbine
 RFWPT Reactor feedwater pump turbine
 RHR Residual heat removal
 RHRSW Residual heat removal service water
 RMOV Reactor motor-operated valve
 RMS Remote manual switch
 RPS Reactor protection system
 RPT Recirculation pump trip
 RS Reactor subcriticality; reactor shutdown; reactor scram
 RV(C) Relief valve (closed)
 RV(O) Relief valve (open)
 RWCU Reactor water cleanup
 RX Reactor

S/D Shutdown
 S/RV Safety relief valve
 S/V Safety valve
 SBCS Standby coolant supply
 SBGT Standby gas treatment
 SCI Short-term containment integrity
 SD-BD Shutdown board
 SDV Scram discharge volume
 SIV Scram instrument volume
 SJAE Steam jet air ejector
 SLCS Standby liquid control system
 SORV Stuck-open relief valve
 SRM Source range monitor

TA Temperature alarm
 TCV Turbine control valve
 TD Time delay
 IDC Time delay contact
 TDPU Time delay pickup
 TE Temperature element
 TIP Traversing in-core probe
 TMI Three Mile Island
 TR Temperature recorder
 Trans Transient
 TS Technical Specifications; torque switch
 TVA Tennessee Valley Authority

UV Undervoltage

V Volts
 VB Vacuum breaker
 VO Valve open
 VS Vapor suppression
 VSS Vapor suppression system
 VWI Vessel water inventory

ε An insignificant quantity, generally less than 10^{-8}

INTERIM RELIABILITY EVALUATION PROGRAM:
ANALYSIS OF THE BROWNS FERRY, UNIT 1, NUCLEAR PLANT

APPENDIX B--SYSTEM DESCRIPTIONS AND FAULT TREES

1. INTRODUCTION

1.1 General Discussion of Appendix B Contents

Sections 2 and 3 of this appendix contain the purpose of the system, the system descriptions (configuration and operation), and fault trees for the various front-line and support systems listed below:

Front-line Systems

- Reactor core isolation cooling (RCIC) system
- Residual heat removal (RHR) system
- High pressure coolant injection (HPCI) system
- Automatic depressurization system (ADS)
- Safety relief valves
- Manual depressurization
- Core spray system
- Vapor suppression system
- Control rod drive hydraulic (CRDH) system
- Power conversion system (PCS), including condensate/booster pumps
- Standby coolant supply (SBCS) system
- Recirculation pump trip (RPT) system
- Main steam isolation valves (MSIVs)

Support Systems

- Electrical power system (AC power and DC power)
- Residual heat removal service water (RHRSW) system
- Emergency equipment cooling water (EECW) system
- Keep-full system
- Condenser circulating water (CCW) system
- Raw cooling water (RCW) system
- Reactor protection system (RPS)

Equipment area cooling (EAC) and engineered safety features actuation system (ESFAS) are not distinct systems at Browns Ferry Nuclear Plant. Therefore, room cooling faults and ESFAS faults, i.e., faults in the auto-initiation circuitry, are discussed under the corresponding system they serve.

In some cases, fault trees were not drawn for the system under consideration. Instead, experience data from U.S. power reactor operating plants or values from WASH-1400,¹ or similar NRC-sponsored studies, were used. (Browns Ferry Unit 1 is functionally identical to the Peach Bottom Nuclear Plant analyzed in WASH-1400.) Analysis of front-line and support systems not employing standard fault tree techniques are identified in this appendix along with the method utilized. In general, each section for a front-line and support system for which a fault tree was drawn and quantified contains information in the following areas:

1. System configuration, including:
 - a. Overall configuration, with corresponding simplified diagram.
 - b. Support system interfaces and failure mode effects analysis (FMEA).
 - c. Instrumentation and control.
 - d. Testing and maintenance during normal operations.
2. System operation, including automatic and manual operation of the system.
3. System fault tree model, including:
 - a. Success/failure criteria.
 - b. Major assumptions used in the fault tree construction.
 - c. Basic events including: tables about the fault events represented in the model; a failure data summary table, supplying the failure data associated with these basic events; and a list of the dominant contributors to the system's unavailability.

For Item 3, the dominant contributor cut-set list is shown for up to 90% cumulative importance. In some cases, the list goes only up to some lesser cumulative value when a reasonable number of cut sets have been listed, indicating that each cut-set contribution to the unavailability of the system is small and would require the listing of hundreds to reach 90% importance.

The criteria for listing the cut sets are:

1. Try to list at least the top 20 cut sets contributing to the system unavailability.
2. List the cut sets until 90% of the system unavailability is achieved.
3. If there exist so many cut sets that the listing becomes unmanageable (e.g. core spray has over 700 cut sets that contribute up to 90% of the system unavailability), then attempt to list only 20 cut sets and when the individual cut set contribution to the system unavailability is less than 1%, stop listing at the next incremental change in contribution.

In addition, the cumulative importance contribution of the cut sets listed is indicated.

Section 4 discusses the human error models and corresponding human error probabilities that were derived for use in the fault tree models. Section 5 discusses the rationale for arriving at the generic control circuit unavailabilities used in this study.

An event-naming code describing the eight-character events on the fault tree is given in Attachment A.

1.2 Shared Systems Between Browns Ferry, Units 1, 2, and 3

Browns Ferry is a three unit nuclear station. The three units are not independent and, in fact, share many systems between the units. The front-line and support systems for Unit 1 that are shared with other units are listed below:

- Power conversion system
- Control rod drive hydraulic system
- Residual heat removal system
- Electric power system (AC and DC)
- Residual heat removal service water system
- Emergency equipment cooling water system
- Raw cooling water system.

This study was intended to address only Unit 1. However, because of the large number of shared systems between units, it was necessary to address the effects of certain failures, (e.g., loss of offsite power), on a plant-wide basis. The following discussion details the extent of the sharing of systems and the extent of the modeling of that interface in the fault trees.

1.2.1 Shared Front-Line Systems

Control Rod Drive Hydraulic System. The CRDH systems for Units 1 and 2 share a spare pump. Since pump operation is not required to accomplish a reactor scram, this shared interface has no effect on the analysis. Furthermore, since the NUREG-0460² value of 3×10^{-5} per demand-for-failure-to-scram is used in this analysis, no fault tree was evaluated for the Browns Ferry, Unit 1 (BF1) CRDH system.

Power Conversion System. Portions of the PCS for each unit are shared, notably the condenser circulating water (CCW) system and the condensate storage and transfer (CS&T) system. The WASH-1400 value of 7×10^{-3} was used for PCS unavailability in this analysis of the system, as discussed in Section 2.9. The PCS unavailability was derived assuming one CCW pump operating (WASH-1400, Appendix I, Page I-68). Considering all three pumps are on-line at the time of the transient, we considered the probability of losing all three CCW pumps to be small. Based on this assumption, no consideration was given to account for the capability of cross-connecting to the remaining units' CCW systems. Therefore, the sharing of the CCW system was not modeled.

The CS&T system provides water to the individual condensate storage tanks (CSTs) for each of the three units. The CSTs not only affect PCS

operation but also HPCI and RCIC system operation. In modeling this interface, each CST was treated as a separate unit. Availability of water from the CST is considered to be insignificant relative to active component failures of the system, assuming normal operating level in the CST. During the initial phases of an accident, availability of water in the CST is not of prime importance, since there exists adequate inventory initially to mitigate the effects of the accident. However, in the long term, this may be an important factor and would be treated as recovery action if deemed necessary for recovery. Because recovery was not explicitly treated in the initial analysis of dominant accident scenarios, no credit is taken for the ability to supply water from the other units' CSTs to the Unit 1 CST for its HPCI and RCIC systems operation.

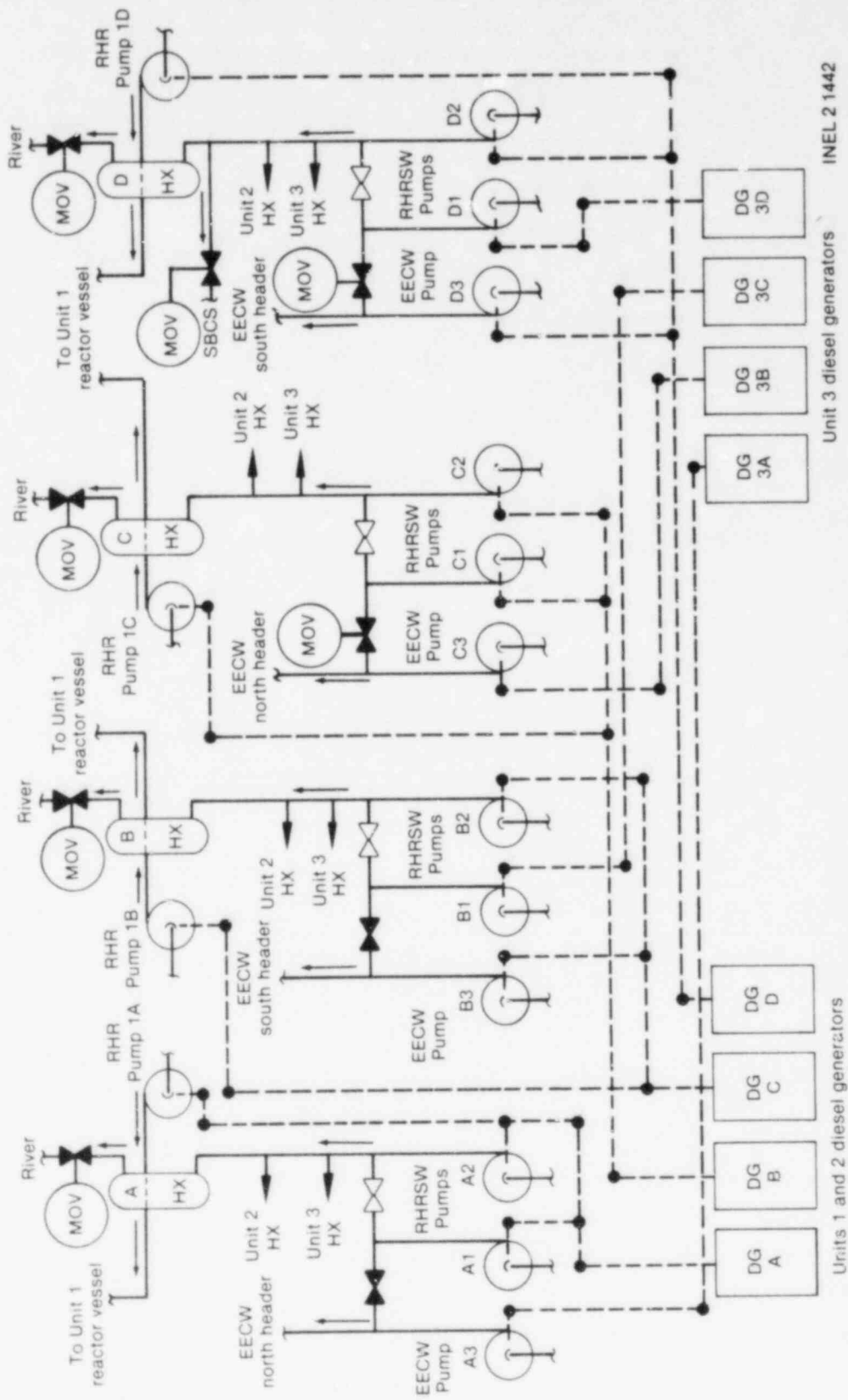
Residual Heat Removal System. There are two important interfaces between the RHR system and the other units. The first is the standby coolant supply system (SBCS) (see Section 3.2), which allows the RHRSW system to supply river water to the Unit 1 reactor or torus. The other interface is a direct RHR-to-RHR interface, which allows the RHR system of one unit to supply injection or cooling services to the other. Under normal conditions the systems are isolated by valves and they act independently. Sharing between units requires manual initiation and operator intervention. Therefore, the RHR models for Unit 1 take credit for SBCS but do not take credit for any other RHR cross-connections.

1.2.2 Shared Support Systems

AC Electric Power System. The EPS for the Browns Ferry are shared in various ways. The nonemergency buses, which are powered, only by offsite power, are shared between units. However, most of these buses do not supply power to front-line systems, except the PCS. The emergency buses receive power from either offsite power or the diesel generators. These buses supply the bulk of the front-line and support systems.

Units 1 and 2 share the services of four of the eight diesel generators. The other four diesel generators are dedicated to Unit 3. A cross tie from one generator in Unit 3 to its corresponding generator for Units 1 and 2 exists to provide power from one unit to another in emergencies. This operation is completely manual and no credit was taken for this capability.

Unlike the other systems previously described, it is not possible to isolate the Unit 3 buses from consideration when modeling EPS faults. This is because some of the pumps necessary for operation in Unit 1 during an accident are powered from Unit 3 buses, and vice versa. The RHRSW and EECW systems are support systems that serve all three Browns Ferry units. These systems are necessary for successful operation of accident mitigating systems in Unit 1 and require AC power from the standby AC power system of Unit 3. Since these two systems require power from Unit 3's 4160 V shutdown boards for successful support capability to Unit 1 following an accident, it was necessary to model this interface. However, no credit was taken for Unit 3's capability to supply Unit 1 power buses in the case where Unit 1's diesel generators fail. Figure B-1 displays the dependency of the RHRSW and EECW systems on the various buses.



INEL 2 1442

Figure B-1. RHR/RHRSW/EECW systems power dependencies.

DC Electric Power System. Sharing of DC power is less complicated than the sharing of AC power. All the major DC loads necessary for accident mitigation at all three units are supplied by three 250 V DC battery boards and their associated batteries and chargers. Therefore, each battery board was modeled.

Residual Heat Removal Service Water System. The RHRSW system has 12 pumps providing cooling water to all three units. Four of the 12 pumps are dedicated to providing EECW flow, while the other eight are dedicated to RHRSW flow. The model for this system takes no credit for those pumps dedicated to EECW service providing RHRSW flow, and vice versa.

An additional sharing feature involving RHRSW is that each cooling header provides cooling to the associated RHR loop in each of the three units. Two RHRSW pumps are normally aligned to each cooling header (A, B, C, and D). The nature of the RHR/RHRSW/EECW/EPS dependencies appears in Figure B-1.

Emergency Equipment Cooling Water System. The EECW system model takes no credit for the eight RHRSW pumps not normally aligned to EECW service, as mentioned in the RHRSW discussion. The EECW is completely shared between the three units, which required modeling all four pumps and the associated headers. The EECW system also interfaces with the RCW system to provide cooling to the RHR room and to seal coolers when the RCW system is inoperable. Credit is taken for both systems when modeling faults associated with RHR room and pump seal cooling.

Raw Cooling Water System. Each unit has three RCW pumps. Units 1 and 2 share a spare pump. Unit 3 has its own spare pump. All the RCW pumps discharge to a common header, which in turn supplies the cooling loads in each unit. When a unit is operating, three pumps per unit are required. EECW automatically provides RCW cooling loads following an abnormal event. In addition to this capability, should EECW fail, the appropriate recovery action would be to cross-connect EECW with RHRSW. Considering these additional capabilities to supply the RHR room and seal coolers under nonloss of offsite power conditions, the capability of supplying Unit's 1 RCW loads from Units 2 and 3 was considered inconsequential for this study. Hence, no credit is taken for the pumps from Units 2 or 3 supplying the Unit 1 loads.

1.3 Treatment of Test and Maintenance Restoration Errors

In general, test and maintenance restoration errors were not significant in the BfI study except for miscalibration errors, which are discussed in Section 4. The test and maintenance restoration errors were not included since BfI maintenance and testing procedures require operability of components to be demonstrated when returning equipment to service after maintenance; these procedures assure that components are not left in an inoperable state. For example, the emergency equipment cooling water Surveillance Instruction (SI) 4.5.C states, "When returning an EECW pump to service after maintenance to the pump, the following data must be included on SI 4.5.C.2 (EECW System Functional Test): pump flow, pump discharge pressure, and vibration amplitude. Additionally, SI 4.5.C.4 (EECW System Annual Flow Rate Test) must also be performed to provide operability per technical specifications."

2. FRONT-LINE SYSTEM FAULT ANALYSES

2.1 Reactor Core Isolation Cooling System

When the reactor is operating at power and loses normal feedwater flow, the resulting transient may require a backup source of high pressure makeup water to maintain vessel water level. In addition, during periods when the reactor is in hot standby, a high pressure source of makeup water is needed to maintain vessel water inventory. The RCIC system is designed to meet both of these operational requirements.

2.1.1 Purpose

The purpose of the RCIC system is to provide a source of high pressure coolant makeup water to the reactor vessel in case of a loss of feedwater flow transient. The RCIC system is also used to maintain the reactor in a hot standby condition.

For events other than pipe breaks or transient-induced loss of coolant accidents (LOCAs), the RCIC system has a makeup capacity sufficient to prevent the reactor vessel water level from decreasing to the level where the core is uncovered. This is accomplished without the assistance of an emergency core cooling system.

2.1.2 System Configuration

Overall Configuration. The RCIC system consists of a steam turbine assembly that drives a constant-flow pump and includes the associated piping, valves, controls, and instrumentation. Figure B-2 is a simplified diagram of the system.

The RCIC turbine is driven by steam that is generated in the reactor vessel. The steam is extracted from main steam Line C upstream of the main steam isolation valves. The turbine exhaust is directed to the suppression pool. Rupture disks in the turbine exhaust line provide turbine protection should turbine exhaust line blockage occur.

The turbine-driven pump is provided with two sources of water for injection into the reactor vessel. Normally, demineralized water from the CST is used instead of injecting the less desirable water from the suppression pool into the reactor. However, the operator does have the option to shift suction to the suppression pool if the need for this suction path arises. Water from either source is pumped into the reactor vessel via feedwater Line B.

To prevent the RCIC pump from overheating during periods of reduced system flow, a minimum-flow bypass line is provided. This line routes approximately 75 gpm of water from the pump discharge path to the suppression pool. Flow is controlled by the minimum-flow bypass valve (FCV-71-34).

Another line in the pump discharge path is used for full-flow operational testing of the RCIC system while the plant is operating. A 1.5-inch orifice in this line provides a discharge head to simulate reactor pressure. If, during testing, an RCIC initiation signal is received, the two test

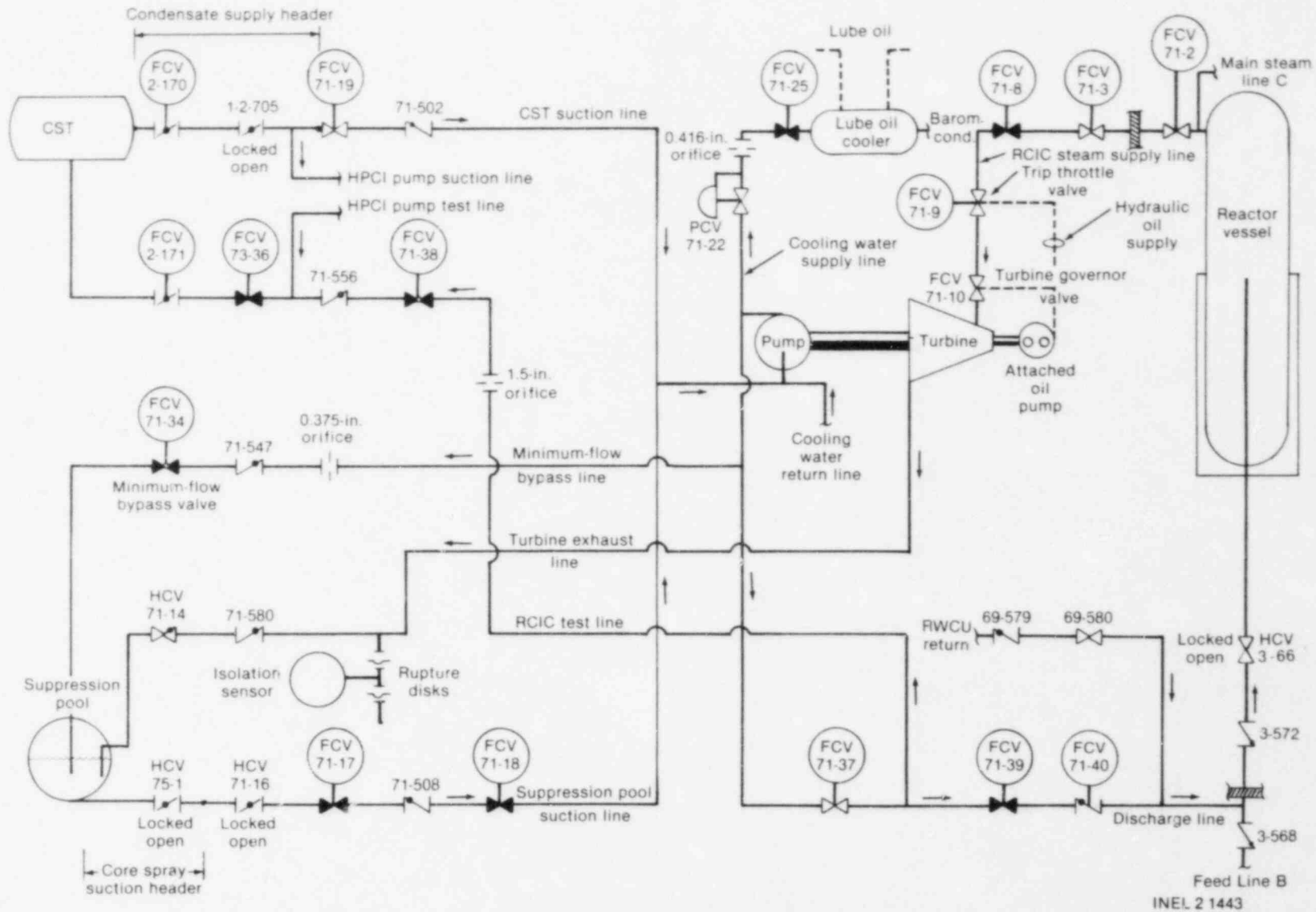


Figure B-2. RCIC system.

line isolation valves (FCV-71-38 and FCV-73-36) will automatically close. FCV-71-38 will also close if either of the suppression pool suction valves (FCV-71-17 and 18) is opened. FCV-73-36 will close if a high drywell pressure signal is received.

Some of the RCIC pump discharge flow is directed through a pressure regulator (PCV-71-22) and a cooling water supply valve (FCV-71-25). The flow then passes through the tubes of the lube oil cooler and into the barometric condenser.

The lube oil cooler removes heat from the turbine lubricating oil system. Oil flow through the lube oil system is accomplished by the attached lube oil pump. The lube oil pump supplies oil to the turbine bearings, to the turbine trip throttle valve (FCV-71-9) to hold it open, and to the governor control oil system. The attached lube oil pump is designed to meet total oil requirements of the lube oil system over the entire speed range of the turbine.

The barometric condenser receives drainage from the turbine gland seals, the trip throttle valve packing, the governor valve (FCV-71-10) packing, and the turbine exhaust thermostatic drain pot. The steam is condensed by a water spray from the cooling water supply line. Noncondensables are removed by a DC-powered vacuum pump and discharged to the suppression pool. Condensate and liquid from the spray is collected in the receiver section of the condenser and pumped back to the suction side of the RCIC pump by a DC-powered condensate pump. Startup of the barometric condenser equipment is automatic upon RCIC system initiation. However, failure of the barometric condenser equipment does not prevent the RCIC system from fulfilling its design objectives.

The RCIC system controls automatically start the system and bring it to the design flow rate of 600 gpm within 30 sec after receipt of a reactor vessel low-low water level signal. The system is designed to deliver the design flow rate to the core at reactor vessel pressures ranging from 1120 to 150 psig. The RCIC system automatically stops either when a high water level in the reactor vessel is signaled, when steam supply pressure drops below 50 psig, or when other system parameters generate a trip signal.

RCIC system operation is designed to be completely independent of AC power although some components interface with AC power systems. Only DC power from the plant batteries and steam extracted from the reactor vessel are necessary for startup and operation of the system.

Support System Interfaces FMEA. The RCIC system components interface with various AC and DC electrical systems, the control air system, and the EAC system. RCIC pump lubrication and control system components are integral to the RCIC system. Component/supporting system interactions are given in Table B-1.

Instrumentation and Control. RCIC system initiation, trip, and isolation are automatically controlled by various plant and system parameters.

System Initiation--The RCIC system will automatically start and inject water into the reactor vessel when a reactor vessel low water level is received at 476.5 inches above vessel zero.

line isolation valves (FCV-71-38 and FCV-73-36) will automatically close. FCV-71-38 will also close if either of the suppression pool suction valves (FCV-71-17 and 18) is opened. FCV-73-36 will close if a high drywell pressure signal is received.

Some of the RCIC pump discharge flow is directed through a pressure regulator (PCV-71-22) and a cooling water supply valve (FCV-71-25). The flow then passes through the tubes of the lube oil cooler and into the barometric condenser.

The lube oil cooler removes heat from the turbine lubricating oil system. Oil flow through the lube oil system is accomplished by the attached lube oil pump. The lube oil pump supplies oil to the turbine bearings, to the turbine trip throttle valve (FCV-71-9) to hold it open, and to the governor control oil system. The attached lube oil pump is designed to meet total oil requirements of the lube oil system over the entire speed range of the turbine.

The barometric condenser receives drainage from the turbine gland seals, the trip throttle valve packing, the governor valve (FCV-71-10) packing, and the turbine exhaust thermostatic drain pot. The steam is condensed by a water spray from the cooling water supply line. Noncondensables are removed by a DC-powered vacuum pump and discharged to the suppression pool. Condensate and liquid from the spray is collected in the receiver section of the condenser and pumped back to the suction side of the RCIC pump by a DC-powered condensate pump. Startup of the barometric condenser equipment is automatic upon RCIC system initiation. However, failure of the barometric condenser equipment does not prevent the RCIC system from fulfilling its design objectives.

The RCIC system controls automatically start the system and bring it to the design flow rate of 600 gpm within 30 sec after receipt of a reactor vessel low-low water level signal. The system is designed to deliver the design flow rate to the core at reactor vessel pressures ranging from 1120 to 150 psig. The RCIC system automatically stops either when a high water level in the reactor vessel is signaled, when steam supply pressure drops below 50 psig, or when other system parameters generate a trip signal.

RCIC system operation is designed to be completely independent of AC power although some components interface with AC power systems. Only DC power from the plant batteries and steam extracted from the reactor vessel are necessary for startup and operation of the system.

Support System Interfaces FMEA. The RCIC system components interface with various AC and DC electrical systems, the control air system, and the EAC system. RCIC pump lubrication and control system components are integral to the RCIC system. Component/supporting system interactions are given in Table B-1.

Instrumentation and Control. RCIC system initiation, trip, and isolation are automatically controlled by various plant and system parameters.

System Initiation--The RCIC system will automatically start and inject water into the reactor vessel when a reactor vessel low water level is received at 476.5 inches above vessel zero.

TABLE B-1. RCIC SYSTEM FMEA OF COMPONENT/SUPPORTING-SYSTEM INTERACTIONS

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
FCV-71-2	480 V AC RMOV-1B	Terminal 13A	No power to board; breaker open	Valve remains in position	FCV-71-2 is inboard isolation valve on RCIC turbine steam line; normally open valve
	250 V DC RMOV Boards: -1C -1A	Isolation Relays: 13A-K15 13A-K33	No signal from control logic	Valve remains in position unless manually actuated	Both Relay 13A-K15 and 13A-K33 must fail before valve will fail to change state
FCV-71-3	250 V DC RMOV-1C	Terminal 6B	No power to board; breaker open	Valve remains in position	FCV-71-3 is in series with FCV-71-2, but located outside of drywell; normally open valve
	250 V DC RMOV Boards: -1C -1A	Isolation Relays: 13A-K16 13A-K33	No signal from control logic	Valve remains in position unless manually actuated	Both Relay 13A-K16 and 13A-K33 must fail before valve will fail to change state
LCV-71-5	Control air	--	Insufficient air	Valve fails closed	LCV-71-5 is a solenoid-operated valve that drains main steam line condensate from the drain pot
	250 V DC RMOV Board-1C	LS-71-5	No signal from	LCV-71-5 will not open	If there is sufficient condensate in the steam line, failure of the steam line high pressure drain trap and coincident failure of LCV-71-5 to open, combined with operator failure to recognize associated valve position indication and alarms, may cause turbine damage
FCV-71-6A FCV-71-6B	Control air	--	Insufficient air pressure	Valves fail closed	These valves are normally open when the system is idle, and closed when the system is running
	250 V DC RMOV Board-1C	13A-K41	No signal from control logic	Valves fail closed	If there is sufficient condensate in the steam line and if the operator ignores high drain pot level annunciators and valve position indicators, turbine damage could result
FCV-71-8	250 V DC RMOV-1C	Terminal 4B	No power to board; breaker open	Valve remains in position	FCV-71-8 is a motor-operated valve used to isolate RCIC turbine from steam supply; closed when system is idle
	250 V DC RMOV Board-1C	13A-K2 (closes on reactor low water level)	No signal from control logic	Valve remains in position unless manually actuated	--
FCV-71-9	250 V DC RMOV-1C	Terminal 5B	No power to board;	Valve remains in position	Normally open turbine trip throttle valve

TABLE B-1. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
FCV-71-9 (continued)	Mechanical over-speed trip	Opens contact in valve open control circuit	Fails to reset	Valve cannot be reopened	Must be reset locally at the turbine
FCV-71-17	250 V DC RMOV-1C	Terminal 8B	No power to board; breaker open	Valve remains in position	FCV-71-17 is a normally closed isolation valve in pump suction line from suppression pool
FCV-71-18	250 V DC RMOV-1C	Terminal 7D	No power to board; breaker open	Valve remains in position	FCV-71-18 is a normally closed isolation valve in pump suction line from suppression pool
FCV-71-19	250 V DC RMOV-1C	Terminal 6D	No power to board; breaker open	Valve remains in position	FCV-71-19 is a normally open isolation valve in the pump suction line from the condensate supply; failure to change position could cause RCIC unavailability due to loss of suction when the CST is empty
	250 V DC RMOV Board-1C	Relays: 13A-K2--low reactor water level 13A-K20--interlocked with FCV-71-18 13A-K21--interlocked with FCV-71-17	No signal from control logic	Valve must be manually activated	FCV-71-19 is a normally open isolation valve in the pump suction line from the condensate supply; failure to change position could cause RCIC unavailability due to loss of suction when the CST is empty Will open automatically when reactor vessel low water level signal is present; however, will not open if FCV-71-17 and 18 are both open; will close automatically if FCV-71-17 and 18 are both open
FCV-71-25	250 V DC RMOV-1C	Terminal 8D	No power to board; breaker open	Valve remains in position	FCV-71-25 is a normally closed isolation valve in the lube oil cooling line; failure to open will cause turbine lube oil overheating and barometric condenser faults
	250 V DC RMOV Board-1C	Relay 13A-K2--low reactor water level	No signal from control logic	Valve must be manually activated	
FCV-71-34	250 V DC RMOV-1C	Terminal 4D	No power to board; breaker open	Valve remains in position unless manually activated	FCV-71-34 is the flow control valve in the minimum-flow bypass line
	250 V DC RMOV-1C	Relays: 13A-K5--initiation 13A-K8--high water level, isolation 13A-K19--low flow	No signal from control logic	--	Condensate will drain from the CST to the suppression pool when suction is from the CST, the RCIC system is tripped, and FCV-71-34 remains open

TABLE B-1. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
FCV-71-34 (continued)		13A-K39--high water level, low suction pressure, high exhaust pressure FS-71-36--high flow			
FCV-71-37	250 V DC RMOV-1C	Terminal 3b	No power to board; breaker open	Valve remains in position	FCV-71-37 is a normally open isolation valve in the pump discharge line to the reactor vessel
	250 V DC RMOV Board-1C	Relay 13A-K3--low reactor water level	No signal from control logic	Valve must be manually activated	Will automatically open on low water level signal, if closed
FCV-71-38	250 V DC RMOV-1C	Terminal 7B	No power to board; breaker open	Valve remains in position	FCV-71-38 is a normally closed isolation valve in the pump test line to the condensate storage tank
	250 V DC RMOV Board-1C	Relays: 13A-K20--interlocked with FCV-71-18 13A-K21--interlocked with FCV-71-17 13A-K2--low reactor water level	No signal from control logic	Valve must be manually activated	Failure of this valve to close combined with failure of HPCI test valve (FCV-73-36) to close could result in insufficient RCIC injection flow to the reactor vessel or in contamination of the CST with suppression pool water
FCV-71-39	250 V DC RMOV-1C	Terminal 3D	No power to board; breaker open	Valve remains in previous position	FCV-71-39 is a normally closed isolation valve in the pump discharge line; failure of this valve to open results in failure of RCIC injection to vessel
	250 V DC RMOV Board-1C	Relay 13A-K2--low reactor water level	No signal from control logic	Valve must be manually activated	Same as above
FCV-71-40	Air operated via solenoid valve	Test switch	No signal to solenoid; loss of control air pressure	Valve will operate normally, regardless of switch position, power availability, or control air pressure	FCV-71-40 is a testable check valve in the RCIC pump discharge line to the reactor
Turbine	Equipment area cooling	Core spray Pump A and C room coolers	No heat removal by EECW; no forced convection by HVAC	Turbine room will heat until turbine isolates at 200°F	RCIC can operate for at least 8 hours without EAC
Vacuum tank condensate pump	250 V DC RMOV-1C	Terminal 1E	No power to board; breaker open	Pump inoperable; barometric condenser fills with water	RCIC can function with pump inoperable
	250 V DC RMOV Board-1C	LS-71-29 activates Relay 13A-K22	No signal from control circuit	Pump must be manually activated	Starts on high vacuum tank level

TABLE B-1. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
Vacuum pump	250 V DC RMOV-1C	Terminal 10E	No power to board; breaker open	Vacuum pump inoperable	RCIC can function with pump inoperable
	250 V DC RMOV Board-1C	Relay 13A-K3--low reactor water level	No signal from control circuit	Pump must be manually activated	Same as above
Division I control logic	250 V DC RMOV-1C	Terminal 1B2	No power to board; breaker open	Division I control logic inoperable	RCIC inoperable
Division II control logic	250 V DC RMOV-1A	Terminal 9A1	No power to board; breaker open	Division II control logic changes	One channel of RCIC isolation signal is lost; initiation logic changes from one-out-of-two-twice to two-of-two
	250 V DC RMOV-1B	Terminal 1E2	No power to board; breaker open	Initiation logic changes	Initiation logic changes from one-out- of-two-twice to two-of-two

Four level switches are used to sense reactor vessel water level. Relays associated with these switches are arranged in a one-out-of-two-twice logic for RCIC initiation. Figure B-3 is a simplified diagram of the RCIC system initiation circuitry.

When the RCIC initiation signal is received, the RCIC steam supply valve (FCV-71-8) opens, the RCIC pump discharge valve (FCV-71-39) opens, the cooling water supply line stop valve (FCV-71-25) opens and the minimum-flow bypass valve (FCV-71-34) opens. The barometric condenser vacuum pump and the vacuum tank condensate return pump will start. These component responses will result in water being pumped from the CST to the reactor vessel via feedwater Line B.

In addition, the initiation signal will cause the CST suction header isolation valve (FCV-71-19) to open if it is closed, unless both of the suppression pool suction isolation valves (FCV-71-17 and 18) are already open. The signal will close the two test line isolation valves (FCV-71-38 and FCV-73-36) if they are open. The normally open discharge line isolation valve (FCV-71-37) will also open if it is closed.

The attached oil pump will meet the total requirements of the turbine hydraulic and lubrication system over the complete range of turbine speed.

When system flow reaches 120 gpm the minimum-flow bypass valve (FCV-71-34) will close.

Turbine Trip--Any of the following conditions will cause the RCIC turbine to trip:

1. High reactor vessel water level (582 inches above vessel zero).
2. Low pump suction pressure (greater than 15 inches Hg vacuum).
3. High turbine exhaust pressure (25 psig).
4. Any isolation signal.
5. Electrical overspeed (110% of rated speed).
6. Mechanical overspeed (125% of rated speed).
7. Remote manual trip from control room.
8. Local trip with manual trip lever.

A turbine trip will cause the following system effects:

1. Turbine trip throttle valve (FCV-71-9) closes.
2. Minimum-flow bypass valve (FCV-71-34) closes.

The latter action is necessary to prevent drainage of the condensate storage tank to the suppression pool.

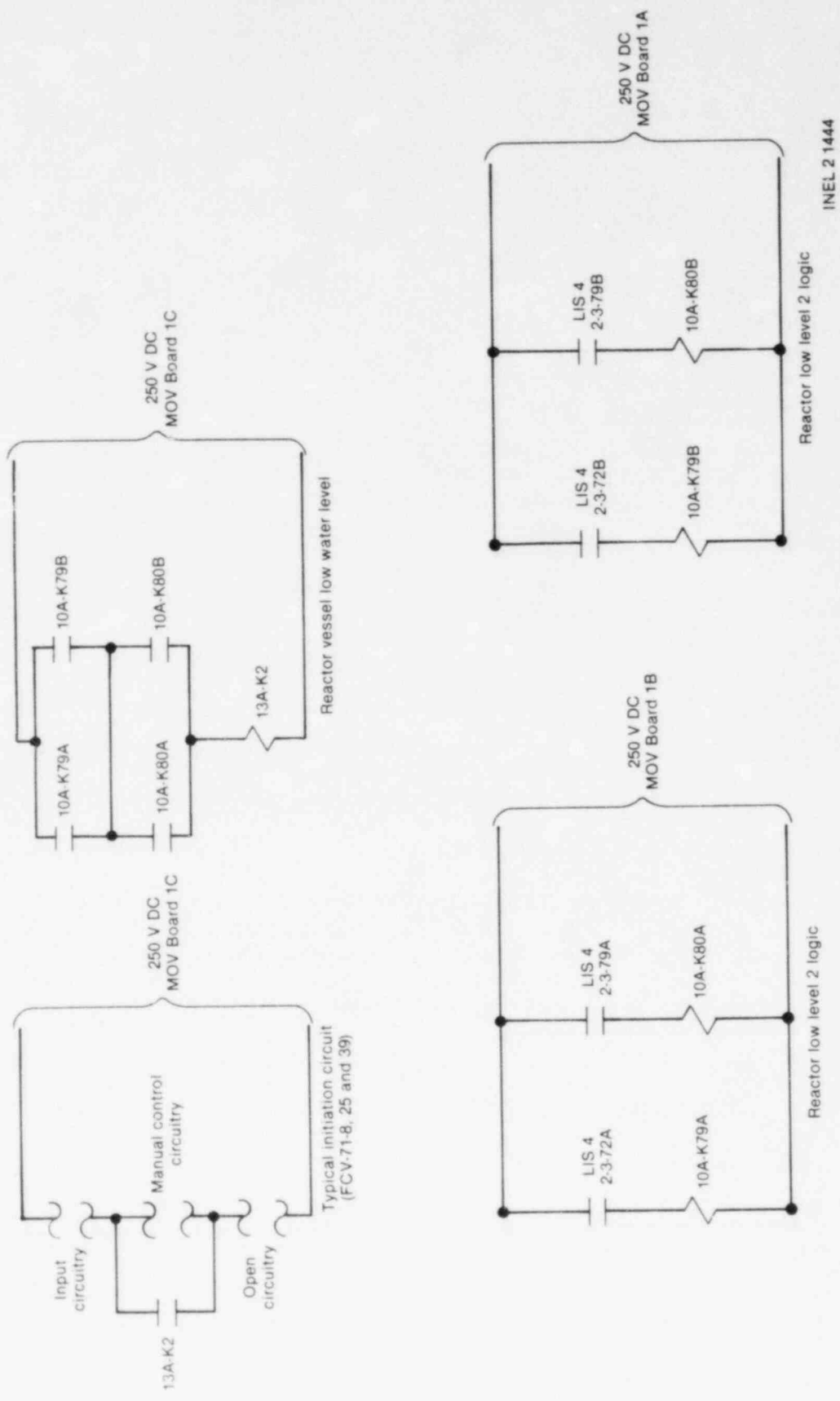


Figure B-3. RCIC initiation circuitry.

All of the turbine trip signals except the mechanical overspeed trip energize a trip solenoid valve that dumps oil from the trip throttle valve (FCV-71-9) and allows spring pressure to close the valve. The solenoid deenergizes after the trip signals are clear, but the trip throttle valve must be manually reopened. This is accomplished by using manual control of the valve from the control room and running the valve to the closed position, (which relatches the trip mechanism), and then by running the valve to the open position, (which reopens the valve).

When the mechanical overspeed device trips the trip throttle valve, the overspeed device must be reset locally at the RCIC turbine before the trip throttle valve can be reopened, as discussed above.

System Isolation--Any of the following conditions will cause the RCIC system to be automatically isolated:

1. High temperature (200°F) of RCIC steam line space.
2. High differential pressure of RCIC steam line (steam line break; 442 inches of water or approximately 300% of rated flow).
3. Low RCIC steam supply pressure (low reactor pressure; 50 psig).
4. High pressure of turbine exhaust line rupture disk (10 psig in the space between rupture disks). (The rupture disks are designed to rupture at 150 psig at 365°F.)
5. Manual isolation from the control room.

The RCIC isolation signal will cause the following system effects:

1. Turbine trip:
 - a. Trip throttle valve (FCV-71-9) closes.
 - b. Minimum-flow bypass valve (FCV-71-34) closes.
2. Inboard (AC) steam line isolation valve (FCV-71-2) closes.
3. Outboard (DC) steam line isolation valve (FCV-71-3) closes.

All isolation signals are sealed in and must be manually reset when the condition that caused the isolation signal has cleared. An RCIC control panel push button is provided for this purpose.

Testing. RCIC system testing requirements are summarized in Table B-2. When a test places any part of the RCIC system in a condition that would preclude proper system operation on demand, it is assumed that the test contributes to the overall system unavailability. Consequently, the test is coded as a basic event and included in the system fault tree.

Where applicable, the basic event code for each test is included in parentheses under the "Component Undergoing Test" column of Table B-2.

TABLE B-2. RCIC SYSTEM TEST REQUIREMENTS SUMMARY

Component Undergoing Test	Type of Test	Test Procedure Number	Components Aligned Away from Engineered Safeguards Position for Test	Expected Test Frequency	Expected Test Outage Time	Remarks
FCV-71-2 FCV-71-3	Turbine steam line high flow functional test and calibration	SI 4.2.B-31	None (see remarks)	Once every month	2 hr	Power removed from both valves
FCV-71-8	RCIC steam line space high temperature functional test and calibration	SI 4.2.B-32	FCV-71-8 (see remarks)	Once every 3 months	--	Shut and tagged (only if instrument needs to be replaced)
FCV-71-2 FCV-71-3 FCV-71-8 FCV-71-19 FCV-71-25 FCV-71-34 FCV-71-37 FCV-71-38 FCV-71-39 (QS42B40J)	RCIC system initiation and isolation logic--functional test	SI 4.2.B-40A	-- FCV-71-8 FCV-71-25 FCV-71-34 FCV-71-39	Once every 6 months	Assume: 8 hr	Valves FCV-71-8, 25, 34, and 39 have their power removed System rendered inoperable for duration of test
RCIC system (QS45F1AJ)	Automatic actuation	SI 4.5.F.1.a	FCV-71-2 ^a FCV-71-3 ^a FCV-71-9 (tripped) FCV-71-19 ^a FCV-71-37 ^a FCV-71-38 ^a	Once every operating cycle	Assume: 1 hr	Valves FCV-71-2, 3, 19, 37, and 38 are repositioned to "normal" by test signal and procedure Renders entire system inoperable; repositioned when test complete
RCIC pump (QS45F1BJ)	Operability	SI 4.5.F.1.b	Flow controller (manual) FCV-71-9 (tripped)	Once every month	Assume: 10 min (Repositioned when test complete)	System will not deliver design flow with controller in manual, repositioned when test complete
FCV-71-5 FCV-71-6A FCV-71-6B FCV-71-17 FCV-71-18 FCV-71-25 FCV-71-34	Stroke	SI 4.5.F.1.c	None	Once every month	--	Cycled from standby to engineered safeguards position and back

B-17

TABLE B-2. (continued)

Component Undergoing Test	Type of Test	Test Procedure Number	Components Aligned Away from Engineered Safeguards Position for Test	Expected Test Frequency	Expected Test Outage Time	Remarks
RCIC system (QS45F1DJ)	Flow (normal steam pressure)	SI 4.5.F.1.d and e	Flow controller (manual) FCV-71-9 (tripped) FCV-73-36 ^a FCV-71-38 ^a	Once every 3 months	Assume: 1 hr	System will not deliver design flow with controller in manual; renders system inoperable
RCIC system	Flow (150 psig steam pressure)	SI 4.5.F.1.d and e	Same as above	Once every operating cycle	Same as above	Same as above; [assume: this SI is normally done when reactor is shut down (i.e., SI 4.5.F.2.d and e)]

a. Will reopen automatically if accident signal is present.

Maintenance. Upon reviewing the BFi maintenance schedules, only one maintenance act was identified that was assumed to contribute to the overall RCIC system unavailability. The RCIC turbine oil is changed semiannually. This requires that the system be taken out of service for approximately 4 hours. It is assumed that the RCIC system will be unavailable for the total duration of the maintenance act.

Table B-3 is a summary of the RCIC system maintenance acts identified as a result of the review mentioned above. When the maintenance act is considered to contribute to RCIC system unavailability, the act is coded as a basic event and included in the system fault tree. Where applicable, the basic event code associated with the corresponding maintenance act is included in parentheses under the "Maintenance Requirement" column.

Technical Specification Limitations

1. The RCIC system must be operable prior to startup from a cold condition or whenever there is irradiated fuel in the reactor and the reactor vessel pressure is above 122 psig.

If the RCIC system is inoperable, the reactor may remain in operation for a period not to exceed 7 days if the HPCI system is operable during such time. When it is determined that the RCIC system is inoperable, the HPCI system must be demonstrated to be operable immediately, and weekly thereafter.

TABLE B-3. RCIC SYSTEM MAINTENANCE ACTS SUMMARY

<u>Maintenance Requirement</u>	<u>Instruction Number</u>	<u>Frequency</u>	<u>Duration</u>	<u>Remarks</u>
Sample RCIC turbine oil	1/2 day after SI 4.5.F.1.d and e	Once every 6 months	1 hr	Assumed: does not take system out of service (drain 1 pint, add 1 pint)
Perform quarterly inspection of RCIC system	MMI-22	Once every 3 months	4 hr	Visual inspection only
Change RCIC turbine oil (QMOILCGJ)	1 day before SI 4.5.F.1.d and e	Once every 6 months	4 hr	Assumed: system out of service for 4 hr, per plant maintenance supervisor
Check movement of RCIC pedestal sliding foot	MMI-22	Once every year	--	Assumed: does not take system out of service

If these conditions are not met, an orderly shutdown of the reactor must be initiated, and the reactor depressurized to less than 122 psig within 24 hours.

2. RCIC testing shall be performed as follows:
 - a. Simulated automatic actuation test (SI 4.5.F.1.a) once per operating cycle.
 - b. Pump operability (SI 4.5.F.1.b) once every month.
 - c. Motor-operated valve operability (SI 4.5.F.1.c) once every month.
 - d. Flow rate at normal reactor vessel operating pressure (SI 4.5.F.1.d and e) once every 3 months.
 - e. Flow rate at 150 psig (SI 4.5.F.1.d and e or SI 4.5.F.2.d and e) once per operating cycle.

The RCIC pump shall deliver at least 600 gpm during each flow test.

3. Whenever RCIC is required to be operable, the piping from the pump discharge to the last flow-blocking valve shall be filled. Water flow from the high point vent must be observed monthly (SI 4.5.F.1.b, d and e or SI 4.5.F.2.d and e).

2.1.3 System Operation

As discussed earlier, the RCIC system is designed to start and inject water into the reactor vessel without operator intervention. However, it is necessary to manually shift RCIC pump suction from the condensate storage tank to the suppression pool. It is also possible to manually start the system. Both automatic and manual operation of the RCIC system will be discussed below.

Automatic Operation. When reactor vessel level decreases to 476.5 inches above vessel zero the RCIC logic circuitry sends an initiation signal to various RCIC components. Given a normal system lineup, as depicted in Figure B-2, the following actions will take place. The turbine steam supply valve (FCV-71-8), the cooling water supply valve (FCV-71-25), the minimum-flow bypass valve (FCV-71-34), and the RCIC pump discharge valve (FCV-71-39) will open. Since the trip throttle valve (FCV-71-9) and the turbine governor valves (FCV-71-10) are normally open, the turbine will begin to rotate. As the turbine increases speed, the RCIC pump discharge flow will also increase. When pump flow reaches 120 gpm the minimum-flow bypass valve (FCV-71-34) will close. The turbine will continue to accelerate until pump output reaches 600 gpm. When this flow rate is obtained, the turbine governor will act to maintain a constant pump flow rate of 600 gpm, regardless of steam inlet pressure to the turbine.

The turbine control system will maintain turbine speed to provide constant flow to the reactor vessel until a turbine trip signal or an isolation signal shuts the system down.

Manual Operation. The system is manually started by transferring the flow controller to "manual" and zeroing the controller. After verification of a normal valve lineup, the cooling water supply valve (FCV-71-25) is opened. The barometric condenser vacuum pump and condensate pump are started. The minimum-flow bypass valve (FCV-71-34) is opened and the turbine steam supply valve (FCV-71-8) is opened. This will start and accelerate the turbine to approximately 2000 rpm. The flow controller is then adjusted as necessary to maintain reactor vessel level.

Whether the system is started automatically or manually, it is always necessary to manually shift the RCIC pump suction from the condensate storage tank to the suppression pool, if the need for transfer arises. The operator is alerted by either a high level alarm in the suppression pool or low level alarm in the CST. This is accomplished by opening the two motor-operated suppression pool suction valves (FCV-71-17 and 18). When both FCV-71-17 and 18 are fully open, the CST suction valve (FCV-71-19) should close automatically. If not, it will be necessary to close FCV-71-19 with the switch on the RCIC control panel. Otherwise, pump suction could be lost if the CST is pumped dry. However, for transients where the PCS is unavailable, it will not be necessary to shift RCIC suction to the suppression pool.

2.1.4 Fault Tree

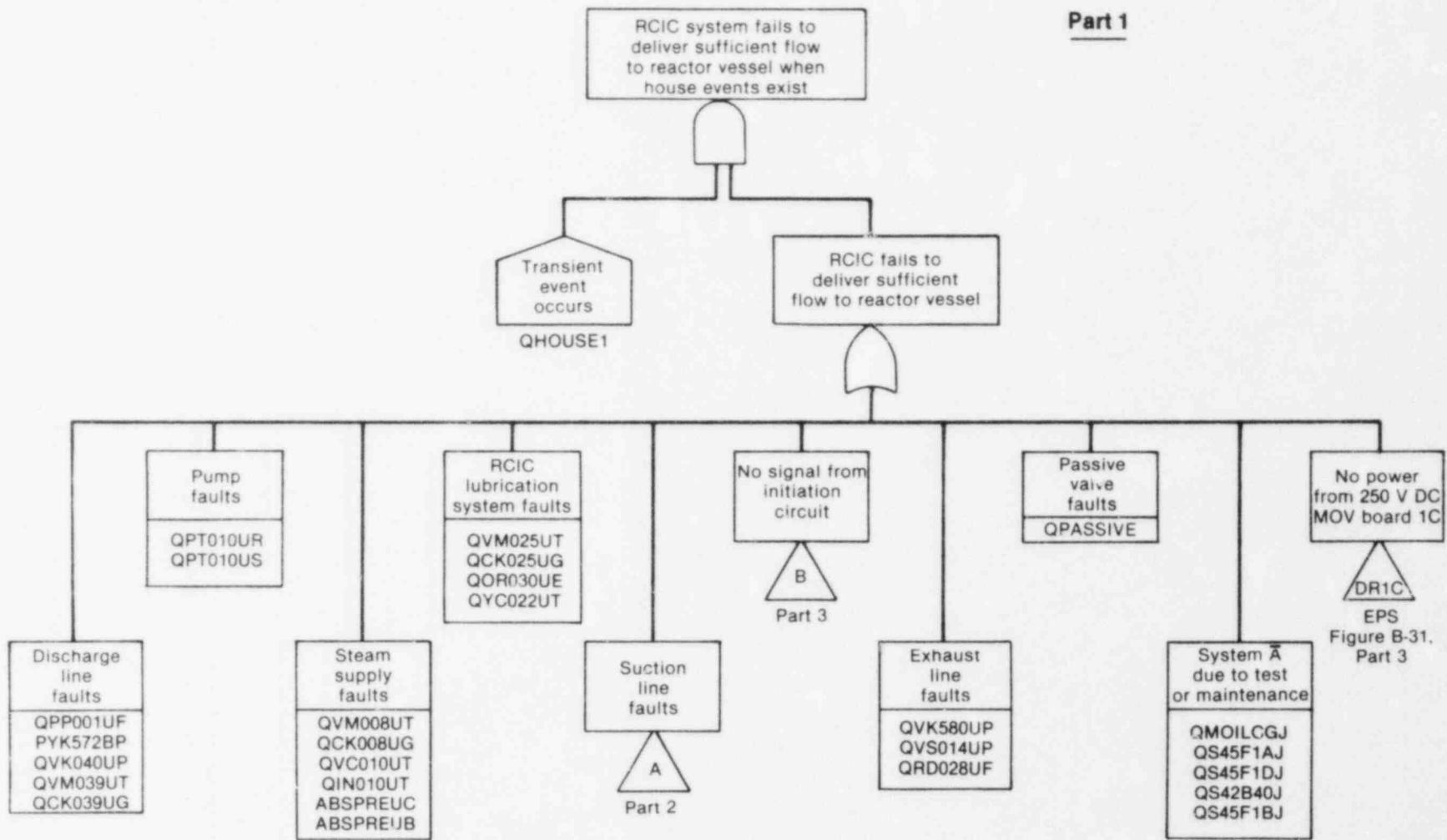
Figure B-4 is the RCIC system fault tree. The RCIC system, like the HPCI system, is, in effect, a single-train system. Consequently, many logical OR gates exist in the system fault tree. Since a reduced tree is depicted in Figure B-4, many of these OR gates have been combined into one tabulation OR (TAB OR) gate in order to save space and make the tree easier to comprehend. The TAB OR gates were only used where system fault logic would not be compromised by compressing the appropriate gates and their corresponding basic events into one logic gate. Where this could not be accomplished, reduction was not attempted and the fault logic is fully developed.

The RCIC pump suction transfer logic is an example of fully developed logic. In this case, the house event, QHOUSE2, is used to model suction transfer faults when LOCA initiating events are being considered. For our analysis, this section of the tree was not used since QHOUSE2 was never turned on. The RCIC system is only used for transient mitigation. However, should further study require consideration of the RCIC transfer capability, the model has been structured to meet this requirement. A human error probability (HEP) model was developed to cover this eventuality and is included in Section 4. The following tabulation gives the house events and describes when each is "on" or "off":

<u>House Event</u>	<u>LOCAs</u>	<u>Transients</u>
QHOUSE1	Off	On
QHOUSE2	Off	Off

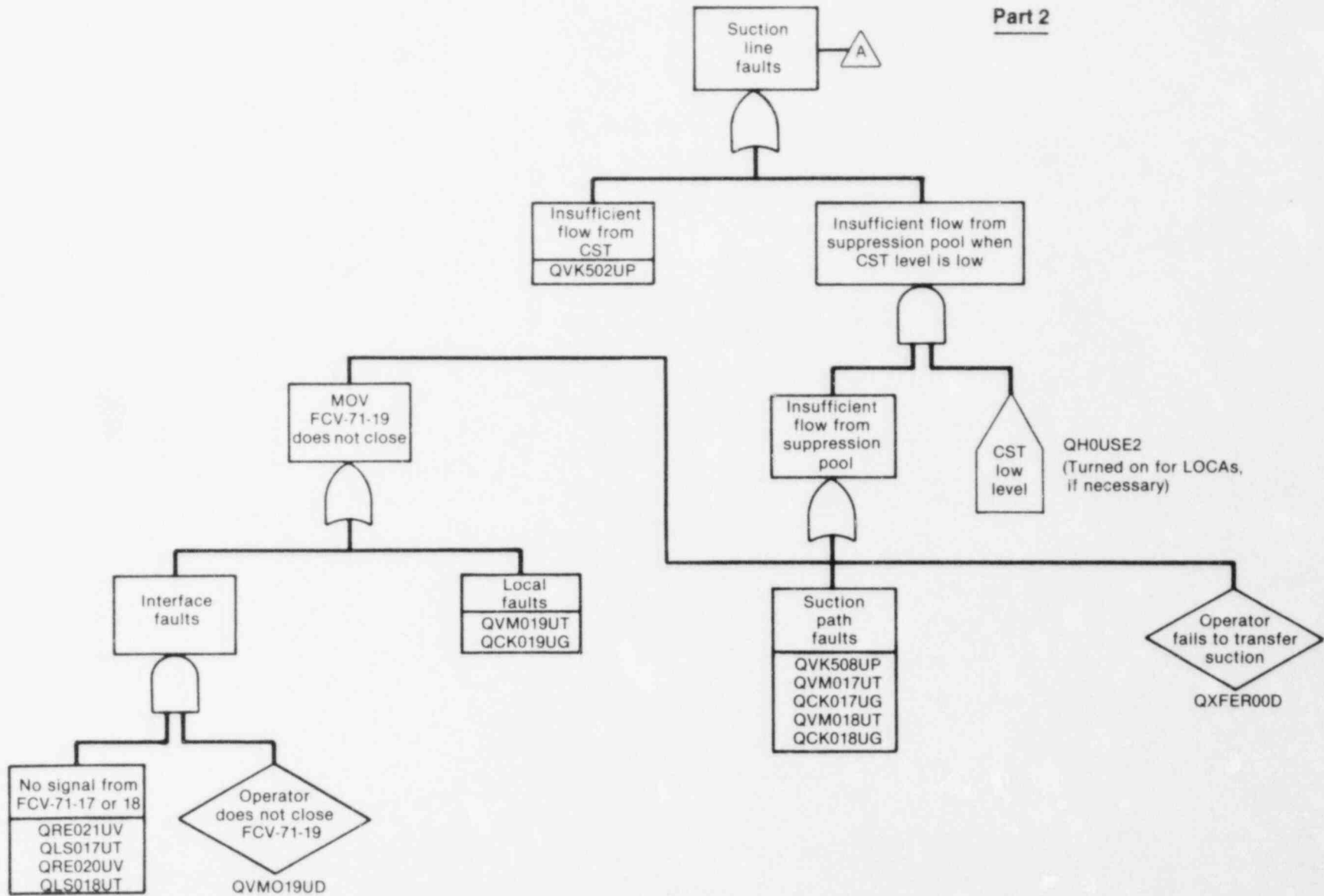
RCIC initiation circuit faults largely involve one-out-of-two-twice logic and are relatively complicated to model. Consequently, the logic associated with these faults is also fully developed where necessary.

Part 1



INEL 2 1445

Figure B-4. RCIC fault tree.



B-23

Figure B-4. (continued).

In light of the major assumptions used to develop the tree, the remaining gates and system logic should be self-explanatory. These major assumptions will be discussed in the next following subsection.

Success/Failure Criteria. The top event in the RCIC system fault tree is "RCIC system fails to deliver sufficient flow to reactor vessel when house events exist." This top event represents the system failure definition. The house events are: (a) transients where the PCS is unavailable, and (b) LOCAs (if necessary; see previous discussion).

Therefore, failure of the RCIC system occurs if the system cannot deliver sufficient flow to the reactor vessel during transients where PCS is unavailable or during LOCAs, if the system is ever required for LOCAs. For this analysis "sufficient flow" was considered to be the design flow of 600 gpm. Any flow less than this amount was considered insufficient for recovery and maintenance of vessel water inventory.

Major Assumptions. The following major assumptions were used in construction of the RCIC system fault tree:

1. The RCIC system will be required to perform the HPCI function for all transients where the PCS becomes unavailable.
2. The system is initially aligned as shown in Figure B-2. This implies, that to achieve successful injection to the vessel, the only valves required to change state, other than those required for turbine control, are: the steam supply valve (FCV-71-8); the pump discharge valve to the feedwater line (FCV-71-39); and the cooling water supply valve (FCV-71-25).
3. Faults in the minimum-flow bypass line downstream of the orifice are not considered in this tree. The RCIC pump is designed to maintain a constant discharge flow of 600 gpm. Since the minimum-flow bypass line taps off of the discharge line upstream of the discharge flow sensor, any flow diversion through the bypass line will be detected by the flow sensor, and the pump output will be adjusted to maintain the 600 gpm flow setting. The orifice will tend to reduce flow diversion to a minimum. Ruptures in the minimum-flow bypass line were not considered due to the size of the piping (see Assumption 4) and the fact that the RCIC system is a constant-discharge flow system. It is further assumed that failure of the minimum-flow bypass to open will not significantly affect system operation unless a fault in the RCIC pump discharge path to the reactor vessel exists. However, if a discharge path fault causes a need for the minimum-flow bypass valve to be open, the flow blockage in the discharge path will cause the RCIC system to be unavailable, by definition, regardless of the position of the minimum-flow bypass valve.
4. Faults in pipes, valves, or system connections of a 2-inch diameter or less are considered to have an insignificant effect on

system operation. One exception to this assumption is the lubricating oil system. Since many of the system components have a direct dependence on this system, it is assumed that lube oil supply and cooling faults could significantly affect system operation. Therefore, these faults are considered in the fault model.

5. For transients where the PCS system is unavailable, it will not be necessary to shift RCIC suction to the suppression pool. In a transient or LOCA in which the decay heat removal systems fail, water makeup to the primary system can generally be maintained initially by injection from the CST. If the operators choose to maintain sufficient makeup to just compensate for decay heat boil-off, the CST will empty (135,000 gallons assumed injected) after about 15 hours. The operators would then be expected to switch to injection of water from the suppression pool. Since stable hot shutdown is defined to be the termination point for the analysis, it was assumed that 8 hours was a realistic time frame to achieve a stable hot shutdown condition at BFI (see Appendix C, Section 1.1 for further discussion of the 8 hour time frame).
6. Any faults in the turbine exhaust piping that cause turbine exhaust piping overpressure are assumed to actuate the turbine exhaust line pressure switches. This action sends a signal to the turbine control circuitry that will initiate a turbine trip. Turbine exhaust line rupture disk leakage will cause a turbine isolation signal to be generated in the control circuitry, which also causes a turbine trip.
7. Faults in the condensate drain systems were analyzed and found to be insignificant relative to the dominant contributors to RCIC system unavailability. Essentially, in order for drain system faults to cause turbine damage, there must be either a flooded steam supply line or steam line drain system faults that would cause the condensate drain pots to fill. These faults must then be combined with condensate drain pot level switch failure in order for significant amounts of condensate to remain undetected in the steam supply line.
8. Passive failures of normally open valves that do not need to change state were considered if the passive failure could disable the entire system. There were nine valves for this system, three CST suction valves (FCV-2-170, 1-2-705, and FCV-71-19), two discharge valves (FCV-71-37 and HCV-3-66), and four steam valves (FCV-71-2, 3, 9, and 10).

Basic Events. The information associated with the various basic events listed in the fault tree are summarized in the RCIC fault summary short form, Table B-4. In addition, the failure data associated with these basic events is summarized in Table B-5. Table B-6 summarizes the dominant contributors to RCIC unavailability.

TABLE B-4. RCIC SYSTEM FAULT SUMMARY SHORT FORM

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
QPP001UF	RCIC pipe break (anywhere)	Leakage/ section	1E-10H/ section	384	30
PVK572BP	Check Valve 3-572	Does not open	1E-4/D	--	3
QVK040UP	Testable check Valve FCV-71-40	Does not open	1E-4/D	--	3
QVM039UT	Discharge Valve FCV-71-39	Does not operate	1E-3/D	--	3
QCK039UG	FCV-71-39 control circuit	No output	3.2E-3	--	10
QPT010UR	RCIC pump	Does not start	3E-3/D	--	3
QPT010US	RCIC pump	Does not continue to run	3E-5/hr	37	3
QVM008UT	Steam stop Valve FCV-71-P	Does not operate	1E-3/D	--	3
QCK008UG	FCV-71-P control circuit	No output	3.2E-3	--	10
QVC010UT	Turbine govern control Valve FCV-71-10	Does not operate	3E-4/D	--	3

TABLE B-4. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
QIN010UT	FCV-71-10 control circuit instrument	Does not operate	1E-6/hr	367	10
ABSPREUC	120 V AC unit preferred bus	Short to ground	3E-7/hr	7	10
ABSPREUB	120 V AC unit preferred bus	Open circuit	3E-8/hr	7	10
QVMD25UT	Cooling water supply Valve FCV-71-25	Does not operate	1E-3/D	--	3
QCK025UG	FCV-71-25 control circuit	No output	3.2E-3	--	10
QOR030UE	Lube oil cooler supply line orifice	Plugged	3E-4/D	--	3
QVC022UT	Pressure control Valve PCV-71-22	Does not operate	3E-4/D	--	
QVK580UP	Turbine exhaust line check Valve 71-580	Does not open	1E-4/D	--	
QVS014UP	Turbine exhaust line stop check Valve HCV-71-14	Does not open	1E-4/D	--	
QRD028UF	Turbine exhaust line rupture disk	Leakage/rupture	5.7E-5/hr/section	372	

TABLE B-4. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
QMOILCGJ	Change RCIC turbine oil	Unavailable due to test or maintenance	9.3E-4	--	0
QS45F1AJ	RCIC system automatic actuation Test SI 4.5.F.1.a		7.7E-5	--	↓
QS45F1DJ	RCIC system flow Test SI 4.5.F.1.d and e		4.6E-4	--	
QS42B40J	Initiation and isolation logic functional Test SI 4.2.B-40A		1.9E-3	--	
QS45F1BJ	RCIC pump operability Test SI 4.5.F.1.b		2.3E-4	--	
QVK502UP	CST suction line check Valve 71-502	Does not open	1E-4/D	--	3
QRE021UV	Relay 13A-K21	Does not energize	1E-4/D	--	↓
QLS017UT	Valve open limit Switch LS-2 on FCV-71-17	Does not operate	3E-4/D	--	
QRE020UV	Relay 13A-K20	Does not energize	1E-4/D	--	

B-29

TABLE B-4. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
QLS018UT	Valve open limit Switch LS-2 on FCV-71-18	Does not operate	3E-4/D	--	3
QVM019UD	Operator does not close FCV-71-19	Operator response error	4.5E-3/D	--	10
QVM019UT	CST suction isolation Valve FCV-71-19	Does not operate	1E-3/D	--	3
QCK019UG	FCV-71-19 control circuit	No output	3.2E-3	--	10
QVK508UP	Suppression pool suction check Valve 71-508	Does not open	1E-4/D	--	3
QVM017UT	Suppression pool suction Valve FCV-71-17	Does not operate	1E-3/D	--	3
QCK017UG	FCV-71-17 control circuit	No output	3.2E-3	--	10
QVM018UT	Suppression pool suction Valve FCV-71-18	Does not operate	1E-3/D	--	3
QCK018UG	FCV-71-18 control circuit	No output	3.2E-3	--	10
QXFEROOD	Operator fails to transfer suction	Operator response error	1.5E-3/D	--	10

TABLE B-4. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
QRE002UV	Relay 13A-K2	Does not energize	1E-4/D	--	3
RRE080AV	Relay 10A-K80A	↓	↓	--	↓
RRE080BV	Relay 10A-K80B			--	
RRE079AV	Relay 10A-K79A			--	
RRE079BV	Relay 10A-K79B			--	
OPS079AT	Level indicating transmitter, Switch 4, LITS-2-3-79A	Does not operate		--	
OPS079BT	Level indicating transmitter, Switch 4, LITS-2-3-79B	↓	↓	--	↓
OPS072AT	Level indicating Switch 4, LIS-2-3-72A			--	
OPS072BT	Level indicating Switch 4, LIS-2-3-72B			--	

B-31

TABLE B-4. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
O42B19AJ	Reactor low water Level 79A functional Test SI 4.2.B-1	Unavailable due to test or maintenance	1.4E-4	--	0
O42B19BJ	Reactor low water Level 79B functional Test SI 4.2.B-1	↓	↓	--	↓
O42B12AJ	Reactor low water Level 72A functional Test SI 4.2.B-1	↓	↓	--	↓
O42B12BJ	Reactor low water Level 72B functional Test SI 4.2.B-1	↓	↓	--	↓
OPSLVLX	Core spray reactor low level switches	Operator miscalibration	2.4E-6/D	--	10
QPASSIVE	Passive valve faults	Does not remain open	1.1E-3/D	--	3

TABLE B-5. RCIC SYSTEM FAILURE DATA SUMMARY

Component/Activity (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (\bar{A})	Remarks
Electrical bus (BS)	Open circuit (B)	0 hr	7 hr	7 hr	3E-8/hr	2.1E-7	$T_D = 0$, because fault will be detected immediately T_R , WASH-1400, Table III 5-2, (instrumentation) $\lambda =$ IREP, Table 3B, wire data; decreased by order of magnitude because buses are much less likely to open than wires (engineering judgement)
Electrical bus (BS)	Short to ground (C)	0 hr	7 hr	7 hr	3E-7/hr	2.1E-6	$T_D = T_R$, same as above $\lambda =$ IREP, Table 3E, wire data
Motor-operated valve control circuit (CK)	No output (G)	360 hr	7 hr	367 hr	7.7E-6/hr + 4.1E-4/D	3.2E-3	$\bar{A} = 4.1E-4 + 7.7E-6T$ T_R --WASH-1400, Table III 5-2 $T_D =$ half test interval; based on pump operability test and stroke time test; once per month
Governor instrumentation (transmitter, amplifier, output devices) (IN)	Does not operate (T)	360 hr	7 hr	367 hr	1E-6/hr	3.7E-4	T_D --based on pump operability check; once per month T_R --WASH-1400, Table III 5-2
Limit switch (LS)	Does not operate (T)	--	--	--	3E-4/D	3E-4	--
Orifice (OR)	Plugged (E)	--	--	--	3E-4/D	3E-4	--
Pipe (PP)	Leakage/rupture (F)	360 hr	24 hr	384 hr	1E-10/hr	3.8E-8	$T_R = 24$ hr, assumed time to shut down plant T_D --based on pump operability test; once per month
Process switch (PS)	Does not operate (T)	--	--	--	1E-4/D	1E-4	--
RCIC pump (PT)	Does not start (R)	--	--	--	1E-3/D	1E-3	--
RCIC pump (PT)	Does not run (S)	0 hr	37 hr	8 hr	3E-5/hr	2.4E-4	T_R --WASH-1400, Table III 5-2
Rupture disk (RD)	Leakage/rupture (F)	360 hr	12 hr	372 hr	5.7E-5/hr	2E-2	T_D --based on pump operability check; once per month T_R --plant-specific data λ --based on plant-specific data

TABLE B-5. (continued)

Component/Activity (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (A)	Remarks
Relay (RE)	Does not energize (V)	--	--	--	1E-4/D	1E-4	--
Control valve (VC)	Does not operate (T)	--	--	--	3E-4/D	3E-4	--
Check valve (VK)	Does not open (P)	--	--	--	1E-4/D	1E-4	--
Motor operated valve (VM)	Does not operate (T)	--	--	--	1E-3/D	1E-3	--
RCIC turbine oil change (QMOILCGJ)	Unavailability due to test or maintenance (J)	--	--	--	--	9.3E-4	Performed once every 6 months; duration, 4 hr
Initiation and isolation logic functional test (QS42B40J)	Unavailability due to test or maintenance (J)	--	--	--	--	1.9E-3	Performed once every 6 months; duration, 8 hr
RCIC pump operability (QS45F1BJ)	Unavailability due to test or maintenance (J)	--	--	--	--	2.3E-4	Performed once per month; duration, 10 min
Stop check valve (VS)	Does not open (P)	--	--	--	1E-4/D	1E-4	Used same unavailability as for check valve (VK)
Governor instrumentation (transmitting, amplifier, output devices) (IN)	Does not operate (T)	360 hr	7 hr	367 hr	1E-6/hr	3.7E-4	T_D --based on pump operability check; once per month T_R --WASH-1400, Table III.5-2
System flow test (QS45F1DJ)	Unavailability due to test or maintenance (J)	--	--	--	--	4.6E-4	Performed once every 3 months; duration, 1 hr; see Table B-2
Core spray system process switches (QPS0, J)	Unavailability due to test or maintenance (J)	--	--	--	--	1.4E-3	See core spray system documentation
Control valve (VC)	Does not operate (T)	--	--	--	3E-4/D	3E-4	--

TABLE B-5. (continued)

Component/Activity (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (A)	Remarks
Normally open valves (QPASSIVE)	Does not remain open	--	--	--	1E-4/D	9E-4	Nine normally open valves
Core spray system low level switches (OPSLVLX)	Operate miscalibrates switches (X)	--	--	--	--	2.4E-6	See model, Section 4

a. If $T_D = 0$, then $T = T_R$ if the mission time (8 hr) $> T_R$. If $T_D = 0$, then $T =$ mission time (8 hr) if mission time $\leq T_R$.

TABLE B-6. RCIC SYSTEM CUT SETS

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
2.0E-2	47.5	QRD028UF	No
3.2E-3	7.6	QCK039UG	No
3.2E-3	7.6	QCK025UG	No
3.2E-3	7.6	QCK008UG	No
3.0E-3	7.1	QPT010UR	No
1.9E-3	4.5	QS42B40J	No
1.0E-3	2.4	QVM039UT	No
1.0E-3	2.4	QVM025UT	No
1.0E-3	2.4	QVM008UT	No
Cumulative importance	89.1		

2.2 Residual Heat Removal System

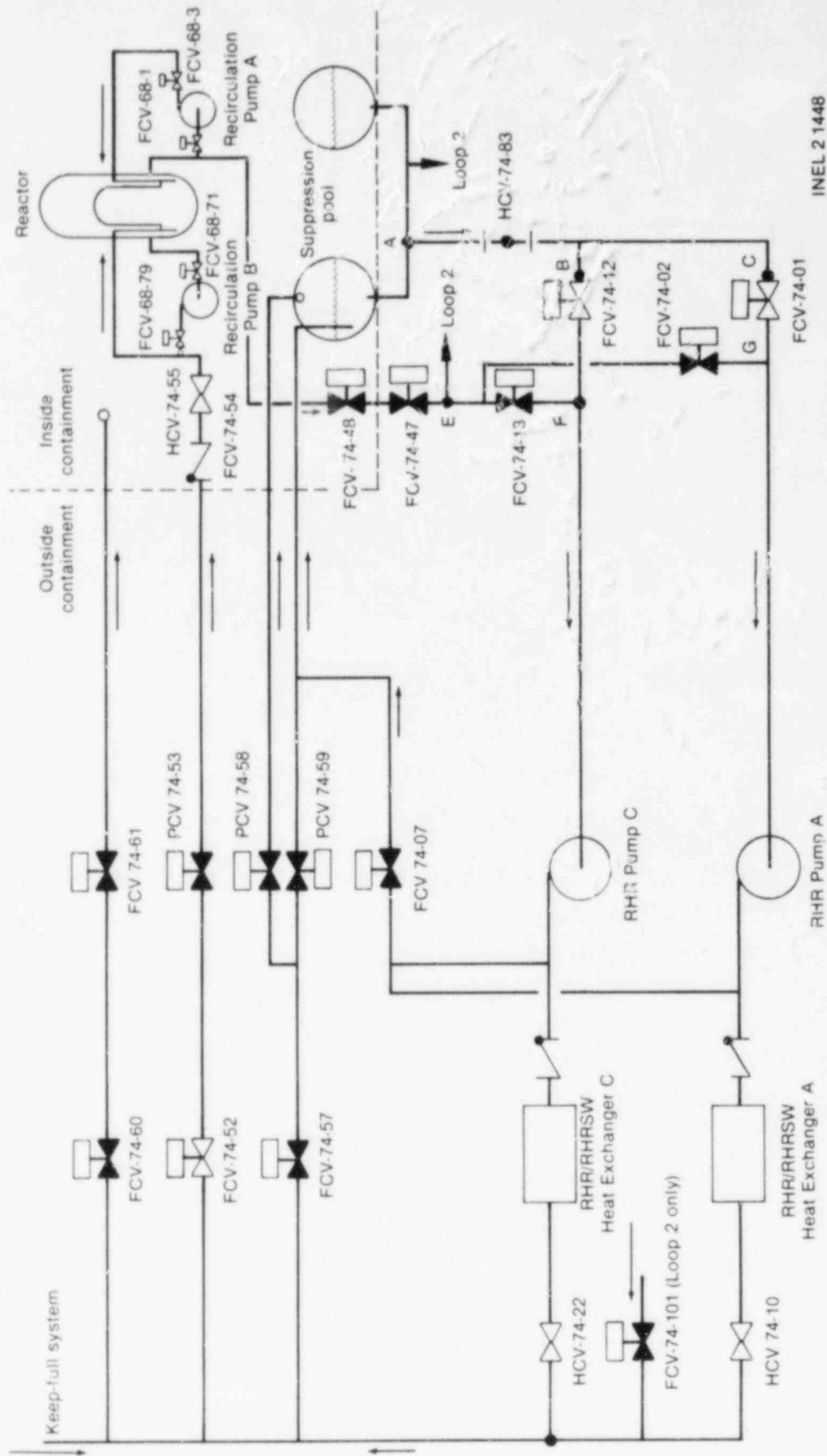
2.2.1 Purpose

The RHR system provides water at low pressure to the reactor to restore and maintain water level following a LOCA. It also provides a means of removing the residual heat of the reactor after shutdown either by direct cooling of the reactor water or by cooling of the torus water.

2.2.2 System Configuration

Overall Configuration. The RHR system consists of two loops. Each loop has a suction line, two pump and heat exchanger combinations, and a discharge line. The loops take suction on the pressure suppression pool (torus) or the reactor recirculation Loop A. Each loop discharges to the reactor, containment sprays, or torus cooling headers, depending on the mode of RHR operation. The low pressure coolant injection (LPCI) mode takes water from the torus and pumps it into the reactor recirculation discharge piping. Shutdown cooling takes water from recirculation Loop A, cools it in the heat exchanger and returns it to the reactor via the same discharge path as the LPCI mode. In torus cooling, the cooled torus water discharges to the torus spray header or torus test return line. The standby coolant supply (SBCS) system uses the RHRSW system to inject river water into the reactor via the same discharge path as LPCI mode (on Loop 2 only). Figure B-5 shows a simplified drawing of Loop 1 of the RHR system. The RHR system drawing shows all the major components included in the fault trees. The valves are shown in their normal positions with the suction aligned to the torus. Loop 1 is shown in the drawing; Loop 2 is similar.

There are four modes of RHR operation modeled in the fault trees: the LPCI mode, shutdown cooling mode, torus cooling mode, and SBC mode. For



INEL 2 1448

Figure B-5. RHR system, Loop 1.

the LPCI mode, there are four different success criteria, each with its own fault tree. The letter designations in the LPCI fault trees correspond to the designation in the event trees for the various LPCI success criteria.

LPCI Modes--There are four combinations of the LPCI mode of RHR modeled in the fault trees. The differences between the modes concern the number of RHR pumps necessary to mitigate the accident or transient. Table B-7 gives the success criteria (G_A , G_B , G_C , and G_D) for the appropriate modes.

No operator action is required to initiate the LPCI mode. With the valves aligned as in Figure B-5, the RHR pumps receive a start signal from the initiation circuitry. The normally closed discharge valve in each loop opens upon receipt of this same signal and a reactor low pressure permissive. The other valves in the torus cooling and containment spray discharge paths automatically receive "close" signals as do the shutdown cooling suction valves. This interlock signal drops out after 5 min allowing the operator to switch to another mode of RHR.

Shutdown Cooling Mode--The shutdown cooling mode of RHR is used in both transients and accident mitigation. All operations to initiate shutdown cooling are manual. The suction valves are manually opened, and

TABLE B-7. RHR SYSTEM OPERATIONAL MODE SUCCESS CRITERIA

<u>Designation</u>	<u>Success Criteria</u>	<u>Applicable Event Trees</u>
G_A	Two LPCI pumps in the same loop deliver rated flow to the core	Large suction break
G_B	Two LPCI pumps in different loops deliver rated flow to the core	Large suction break
G_C	Four LPCI pumps deliver rated flow to the core	Large suction break Large steam break
G_D	One LPCI pump delivers rated flow to the core	Large discharge break Large steam break Intermediate breaks small breaks transients
R_A	One pump and heat exchanger circulating reactor coolant	All
R_B	Two pumps and heat exchangers circulating torus water	All
R_S	One RHRSW pump delivering rated flow transients to reactor through RHR Loop 2	Transients

the normally open torus suction valve for the pumps being used are closed. Injection into the reactor is via the same lines and piping as the LPCI mode. The pressure interlock on the discharge valves is the same as the LPCI mode. Cooling to the heat exchangers from the RHRSW system is required in this mode.

Torus Cooling Mode--The torus cooling mode takes water from the torus, cools it in the heat exchangers, and returns the water to the torus through either the torus spray or torus recirculation lines. All operations of the torus cooling mode are manual. This mode may be used for either accident or transient mitigation.

Standby Coolant Supply System Mode--The SBCS mode is a "last resort" mode, which uses the RHRSW pumps to pump water from the river into the reactor via the LPCI discharge line of Loop 2. Initiation is completely manual.

System Interfaces. There are six system interfaces with the RHR system: AC and DC power, logic initiation circuitry, keep-full system, EECW, RCW, and RHRSW system. There are multiple combinations of AC and DC power necessary to operate the RHR system depending on which mode of RHR is in use. The logic circuitry provides automatic initiation signals and protective interlocks to prevent overpressurization of the RHR system. The logic circuitry also provides automatic isolation signals to containment cooling isolation valves and shutdown cooling suction valves to prevent diversion of water from the reactor during the LPCI mode of operation. The EECW system or RCW system provides room cooling and pump seal cooling for the RHR system. The keep-full system insures that the discharge piping of each RHR loop is filled with water. This prevents water hammer damage when the pumps start. The RHRSW system provides cooling to the RHR heat exchangers for the shutdown cooling, torus cooling and containment spray modes of RHR operation component/system interactions are given in Table B-8.

Instrumentation and Control. There are two divisions of logic circuitry for initiating and controlling the RHR system. Division I provides signals to RHR Pumps A and C and the Loop 1 valves, while Division II serves Loop 2 valves and Pumps B and D. Figure B-6 is a simplified drawing of the RHR initiation circuitry.

The LPCI mode is automatically initiated upon receipt of a low level signal or a high drywell pressure signal coincident with low reactor pressure signal. Each of these signals is based on input from four separate sensors and is arranged in a one-out-of-two-taken-twice scheme. The LPCI initiation signal also causes closure of the containment cooling isolation valves (FCV-74-60, 61, 57, and 59) (if they were open) and prevents their opening for 5 min after receipt of this signal. It also isolates the recirculation pump discharge valves (FCV-68-79 and 3) and shutdown cooling suction valves (FCV-74-47 and 48) if they were open at the time.

All other modes of RHR operation are manually initiated. The logic circuitry provides reactor pressure interlocks to prevent system overpressurization during shutdown cooling and provides signals to open and close the minimum-flow bypass valves for each loop.

TABLE B-6. RHR SYSTEM FMEA OF COMPONENT/SUPPORTING-SYSTEM INTERACTIONS

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on From-Line System	Remarks
RHR Pump A	4160 V SD-BD-1A	Terminal 19	No power to board	Pump unavailable	--
	250 V DC control power	SD-BD-1A control power bus	No power to board	Breaker will not close; pump will not energize	--
	EECW or RCWS	Pump A seal cooler	Inadequate heat removal	Eventual seal failure	--
	EECW or RCWS	RHR A and C room coolers	Inadequate heat removal	Motor overheats; eventual failure	--
RHR Pump A cooler fan	480 V RMOV-1A	Terminal 4A	No power to board	Motor overheats; eventual failure	--
RHR Pump B	4160 V SD-BD-1C	Terminal 17	No power to board	Pump unavailable	--
	250 V DC control power	SD-BD-1C control power bus	No power to board	Breaker will not close; pump will not energize	--
	EECW or RCWS	Pump B seal cooler	Inadequate heat removal	Eventual seal failure	--
	EECW or RCWS	RHR B and D room coolers	Inadequate heat removal	Motor overheats; eventual failure	--
RHR Pump B cooler fan	480 V RMOV-1B	Terminal 7B	No power to board	Motor overheats; eventual failure	--
RHR Pump C	4160 V SD-BD-1B	Terminal 16	No power to board	Pump unavailable	--
	250 V DC control power	SD-BD-1B control power bus	No power to board	Breaker will not close; pump will not energize	--
	EECW or RCWS	Pump C seal cooler	Inadequate heat removal	Eventual seal failure	--
	EECW or RCWS	RHR A and C room coolers	Inadequate heat removal	Motor overheats; eventual failure	--
RHR Pump C cooler fan	480 V RMOV-1A	Terminal 14A	No power to board	Motor overheats; eventual failure	--
RHR Pump D	4160 V SD-BD-1D	Terminal 16	No power to board	Pump unavailable	--
	250 V DC control power	SD-BD-1C control power bus	No power to board	Breaker will not close; pump will not energize	--
	EECW or RCWS	Pump D seal cooler	Inadequate heat removal	Eventual seal failure	--

B-40

TABLE B-8. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
RHR Pump D (continued)	EECW or RCWS	RHR B and D room coolers	Inadequate heat removal	Motor overheats; eventual failure	--
RHR Pump D cooler fan	480 V RMOV-1B	Terminal 12B	No power to board	Motor overheats; eventual failure	--
RHR logic, Division I	250 V RMOV-1B	Terminal 1E2	No power to board	Division I logic unavailable	Automatic operation of RHR Loop 1 pumps and valves lost
RHR logic, Division II	250 V RMOV-1A	Terminal 8D1	No power to board	Division II logic unavailable	Automatic operation of RHR Loop 2 pumps and valves lost
RHR heat Exchanger B	RHRSW Pumps B1, B2	RHR heat Exchanger B	Inadequate heat removal through secondary side	--	--
RHR heat Exchanger A	RHRSW Pumps A1, A2	RHR heat Exchanger A	Inadequate heat removal through secondary side	--	--
RHR heat Exchanger C	RHRSW Pumps C1, C2	RHR heat Exchanger C	Inadequate heat removal through secondary side	--	--
RHR heat Exchanger D	RHRSW Pumps D1, D2	RHR heat Exchanger D	Inadequate heat removal through secondary side	--	--
FCV-74-75	480 V RMOV-1B	Terminal 10E	No power to board; breaker open	Valve remains in previous position	Normally closed isolation valve for drywell spray--Loop B/D
	Division II logic	Relay 10A-K68B	No signal from control logic	Valve does not automatically close on accident signal if open	--
FCV-74-52	480 V RMOV-1A	Terminal 2C	No power to board; breaker open	Valve remains in previous position	Normally open stop valve in line to recirculation system--Loop A/C
	Division I logic	Relay 10A-K46A	No signal from control logic	Valve does not auto-open on accident signal if closed	--
FCV-74-35	480 V RMOV-1B	Terminal 5C2	No power to board; breaker open	Valve remains in previous position	Normally open Pump D suction valve from torus
	Manual control	LS-11 interlocks with FCV-74-36	--	--	--

TABLE B-8. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
FCV-74-24	480 V RMOV-1B	Terminal 4C	No power to board; breaker open	Valve remains in previous position	Normally open isolation valve in Pump B suction line from torus
	Manual control	LS-6 interlocks with FCV-74-25	--	--	--
FCV-74-12	480 V RMOV-1A	Terminal 5B	No power to board; breaker open	Valve remains in previous position	Normally open isolation valve in Pump C suction line from torus
	Manual control	LS-15 interlocks with FCV-74-13	--	--	--
FCV-74-1	480 V RMOV-1A	Terminal 4B	No power to board; breaker open	Valve remains in previous position	Normally open isolation valve in Pump A suction line from torus
	Manual control	LS-5 interlocks with FCV-74-2	--	--	--
FCV-74-36	480 V RMOV-1B	Terminal 7C	No power to board; breaker open	Valve remains in previous position	Normally closed Pump D suction valve from recirculation system
	Manual control	LS-5 interlocks with FCV-74-35; LS-6, 15 interlocks with FCV-74-30	--	--	--
FCV-74-25	480 V RMOV-1B	Terminal 6C2	No power to board; breaker open	Valve remains in previous position	Normally closed Pump B suction valve from recirculation system
	Manual control	LS-5 interlocks with FCV-74-24; LS-6, 15 interlocks with FCV-74-30	--	--	--
FCV-74-57	480 V RMOV-1A	Terminal 11E	No power to board; breaker open	Valve remains in previous position	Normally closed isolation valve in torus spray line--Loop A/C
	Division I logic	Relay 10A-K61A	No signal from control logic	Valve does not auto-close on accident signal if open	--
FCV-74-72	480 V RMOV-1B	Terminal 11E	No power to board	Valve remains in previous position	Normally closed isolation valve in torus spray line--Loop B/D
	Division II logic	Relay 10A-K68B	No signal from control logic	Valve does not auto-close on accident signal if open	--

TABLE B-8. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
FCV-74-58	480 V RMOV-1A	Terminal 12E	No power to board	Valve remains in previous position	Normally closed isolation valve in torus spray line--Loop A/C
	Division I logic	Relay 10A-K68A	No signal from control logic	Valve does not auto-close on accident signal if open	--
FCV-74-73	480 V RMOV-1E	Terminal 4C	No power to board; breaker open	Valve remains in previous position	Normally closed isolation valve in torus cooling line--Loop B/D
	Division II logic	Relay 10A-K68B	No signal from control logic	Valve does not auto-close on accident signal	--
FCV-74-59	480 V RMOV-1D	Terminal 5C	No power to board; breaker open	Valve remains in previous position	Normally closed isolation valve to torus cooling line--Loop A/C
	Division I logic	Relay 10A-K68A	No signal from control logic	Valve does not auto-close on accident signal if open	--
FCV-74-67	480 V RMOV-1E	Terminal 2C	No power to board; breaker open	Valve remains in previous position	Normally closed isolation valve to recirculation system--Loop B/D
	Division II logic	Relays 10A-K67A and 10A-K67B	No signal from control logic	Valve does not auto-open on accident signal	--
FCV-74-53	480 V RMOV-1E	Terminal 2C	No power to board; breaker open	Valve remains in previous position	Normally closed isolation valve to recirculation system--Loop A/C
	Division I logic	Relays 10A-K67A and 10A-K67B	No signal from control logic	Valve does not auto-open on accident signal	--
FCV-74-66	480 V RMOV-1B	Terminal 3A	No power to board; breaker open	Valve remains in previous position	Normally open stop valve in line to recirculation system--Loop B/D
	Division II logic	Relay 10A-K46B	No signal from control logic	Valve does not auto-open on accident signal if shut	--
FCV-74-61	480 V RMOV-1A	Terminal 7B	No power to board; breaker open	Valve remains in previous position	Normally closed isolation valve for drywell spray--Loop A/C
	Division I logic	Relay 10A-K68A	No control signal	Valve does not auto-close on accident signal if open	--
FCV-74-74	480 V RMOV-1B	Terminal 10C	No power to board	Valve remains in previous position	Normally closed isolation valve in series with FCV-74-75
	Division II logic	Relay 10A-K61B	No control signal	Valve does not auto-close on accident signal if open	--

B-43

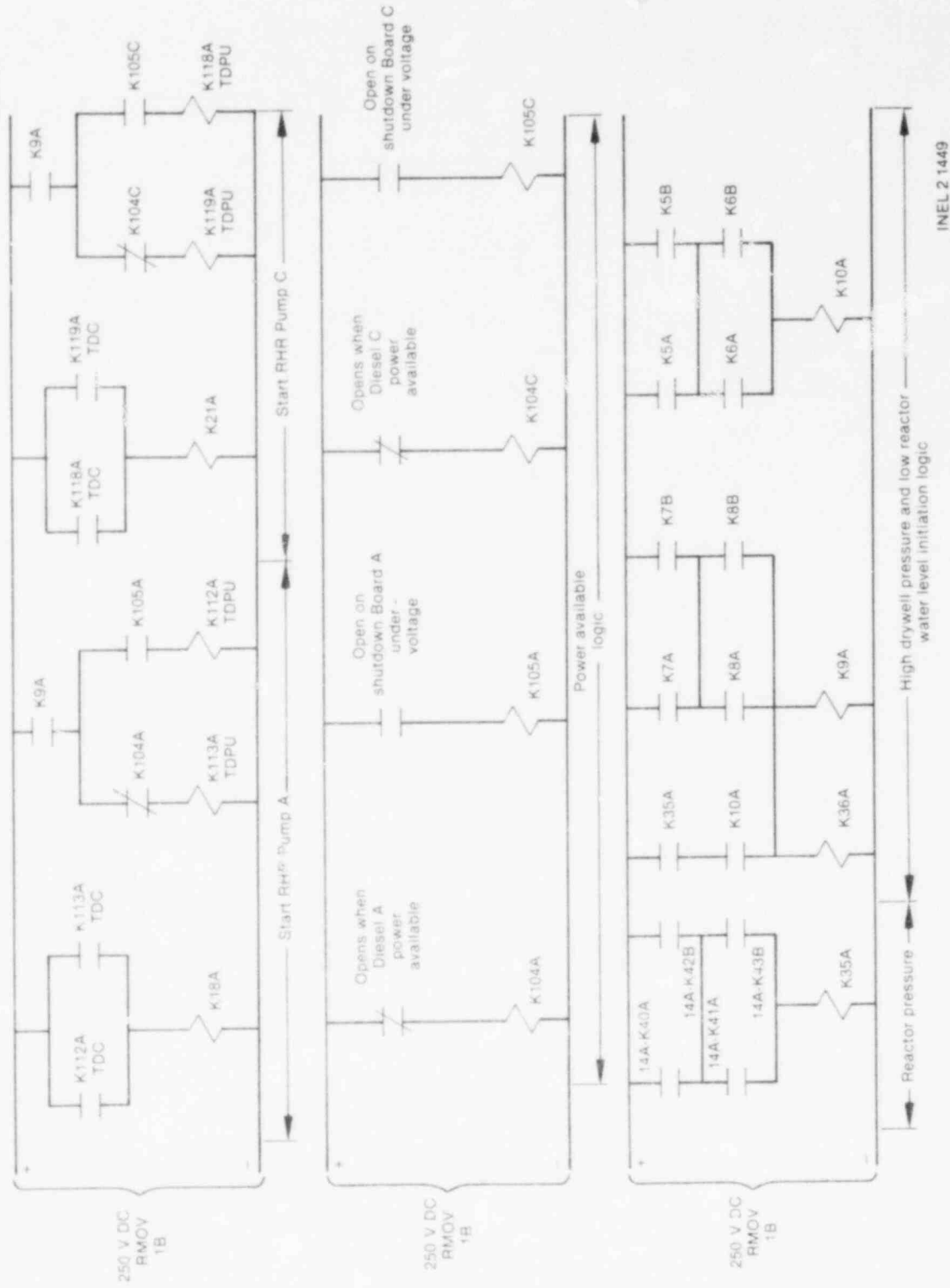
TABLE B-8. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-line System	Remarks
FCV-74-60	480 V RMOV-1A	Terminal 6B	No power to board	Valve remains in previous position	Normally closed isolation valve in series with FCV-74-61
	Division I logic	Relay 10A-K61A	No control signal	Valve does not auto-close on accident signal if open	--
FCV-74-78	480 V RMOV-1A	--	--	--	--
FCV-74-77	250 V RMOV-1B	These valves are head spray isolation valves; head spray is not required for mitigation of accidents or transients			
FCV-74-76	Control air system	--	--	--	--
Drywell spray Line A	Keep-full system	FCV-74-792 FCV-74-804	Empty PSC tank	Allows air to enter RHR piping upstream of closed isolation valves	Rhr pump startup into a partially voided system will cause water hammer with a significant possibility of component damage
Drywell spray Line B	Keep-full system	FCV-74-803 FCV-74-802	Empty PSC tank	Allows air to enter RHR piping upstream of closed isolation valves	RHR pump startup into a partially voided system will cause water hammer with a significant possibility of component damage
FCV-74-71	480 V RMOV-1B	Terminal 11C	No power to board; breaker open	Valve remains in previous position	Normally closed isolation valve to torus spray--Loop B/D
	Division II logic	Relay 10A-K61B	No signal from control logic	Valve does not auto-close on accident signal if open	--
FCV-74-2	480 V RMOV-1A	Terminal 6C	No power to board; breaker open	Valve remains in previous position	Normally closed Pump A suction valve from recirculation system
	Manual control	LS-5 interlocks with FCV-74-1; LS-6, 15 interlocks with FCV-74-7	--	--	--
FCV-74-13	480 V RMOV-1A	Terminal 7C	No power to board; breaker open	Valve remains in previous position	Normally closed Pump C suction valve from recirculation system
	Manual control	LS-5 interlocks with FCV-74-12; LS-6, 15 interlocks with FCV-74-7	--	--	--
FCV-74-30	480 V RMOV-1E	Terminal 4E	No power to board; breaker open	Valve remains in previous position	Normally open pump bypass to torus--Loop E/D
	Division II logic	Relay 10A-K108B	No signal from control logic	Valve does not auto-open or auto-close	--

TABLE B-8. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
FCV-74-7	480 V RMOV-1D	Terminal 5E	No power to board; breaker open	Valve remains in previous position	Normally open pump bypass to torus--Loop A/C
	Division I logic	Isolation Relay 10A-K108A	No signal from control logic	Valve does not auto-close or auto-open	--
FCV-74-48	480 V RMOV-1A	Terminal 8C	No power to board; breaker open	Valve remains in previous position	Normally closed inboard isolation valve in pump suction line from recirculation system
	Division I logic	Relay 10A-K98A	No signal from control logic	Valve does not auto-close	--
FCV-74-47	250 V RMOV-1B	Terminal 5A	No power to board; breaker open	Valve remains in previous position	Normally closed outboard isolation valve in pump suction line from recirculation system
	Division II logic	Relay 10A-K98B	No signal from control logic	Valve does not auto-close	--

Part 1



INEL 2 1449

Figure B-6. RHR initiation circuitry.

Part 2

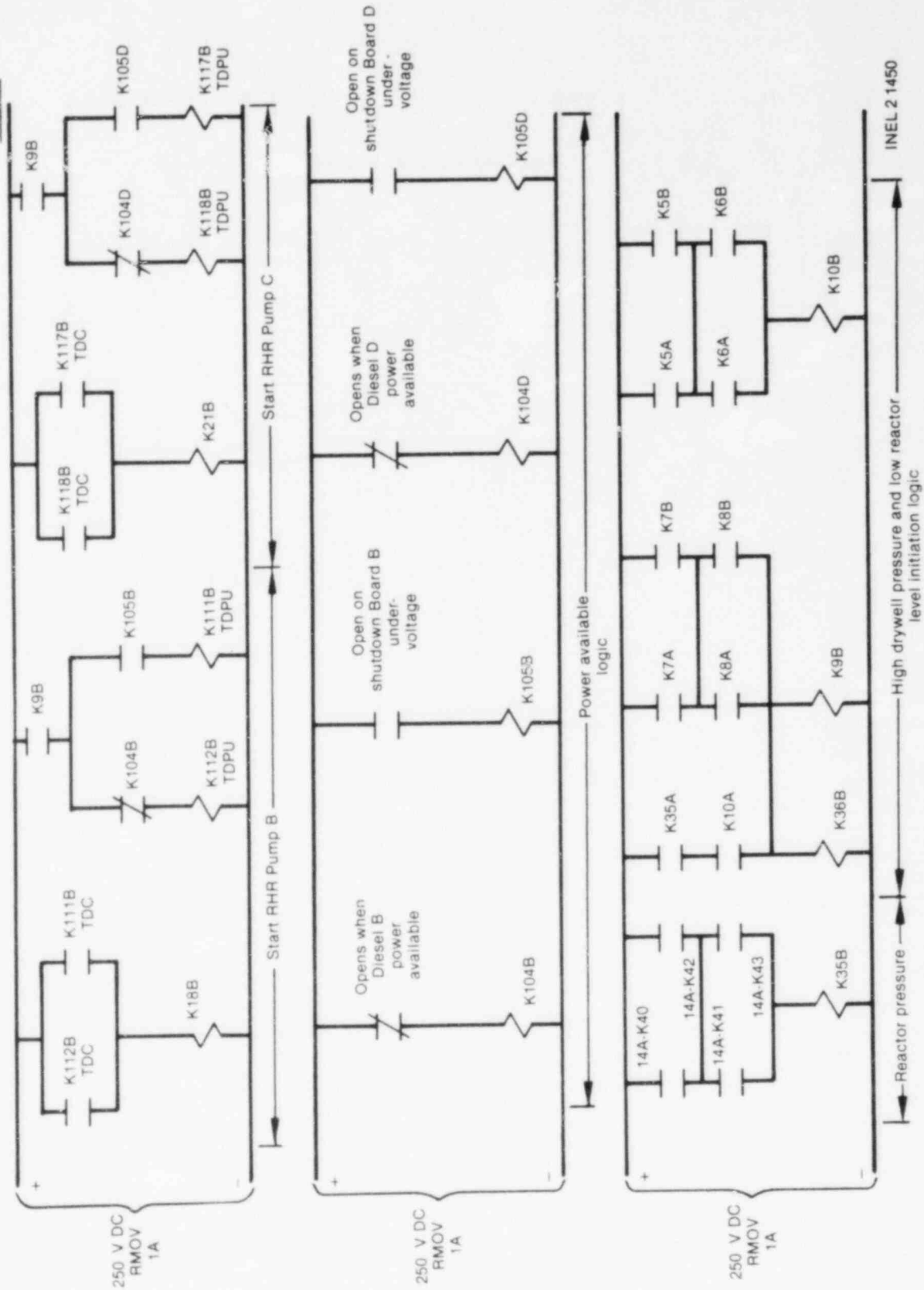
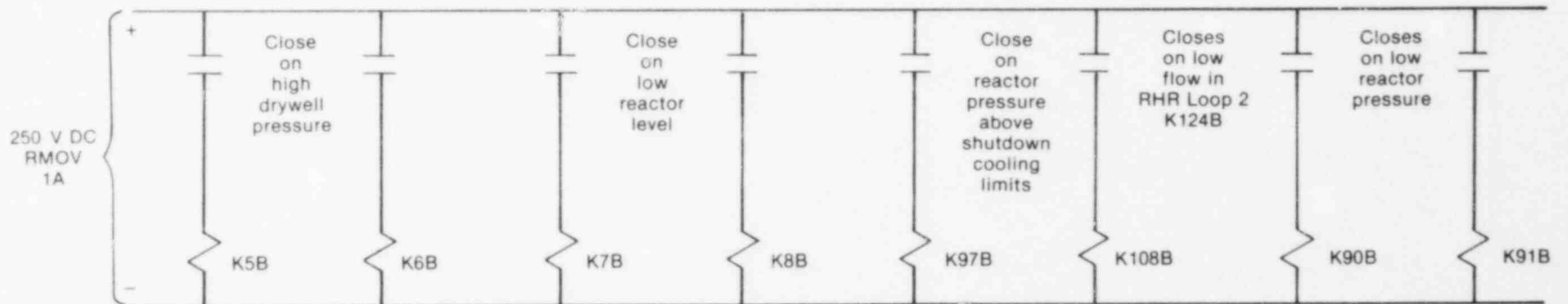
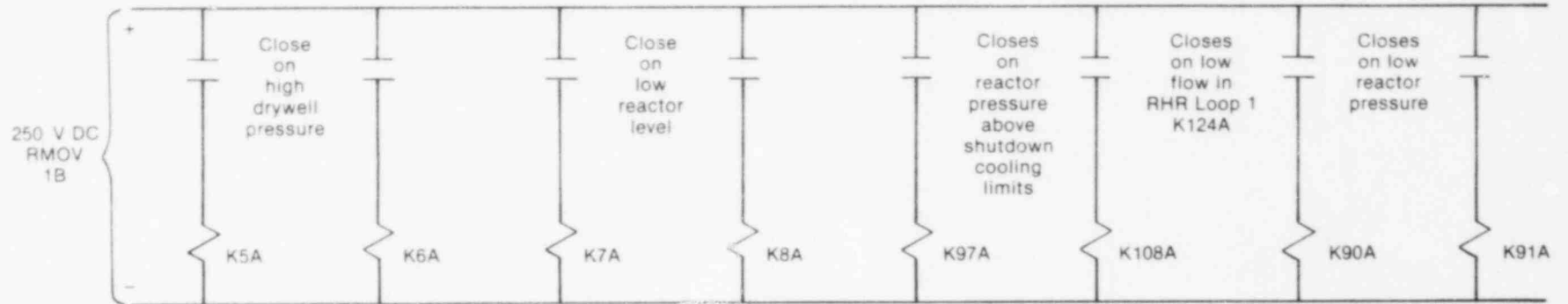


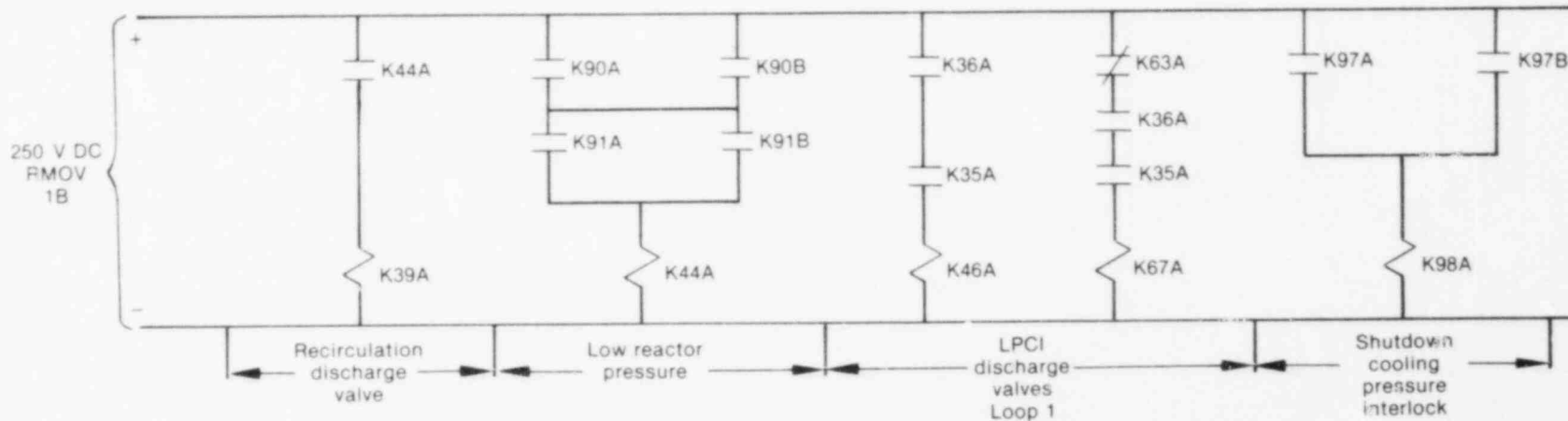
Figure B-6. (continued).

B-4-B



INEL 2 1451

Figure B-6. (continued).



B-49

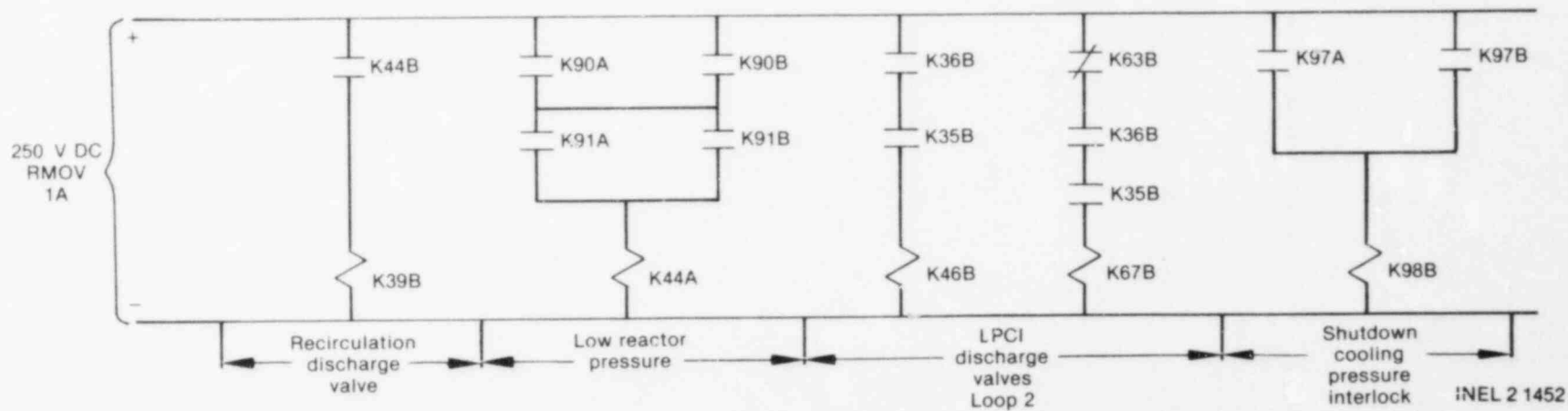


Figure B-6. (continued).

Testing. Periodic testing of the RHR system and its control systems is required by technical specifications. Of these required tests, only those involving initiation and control circuitry render portions of the system inoperable. Table B-9 lists these tests, their frequency, affected components, and calculated unavailabilities. The outage times are based on information obtained from plant personnel who schedule and perform these tests.

The auto-initiation test is performed once every 6 months and takes 4 hours to complete. Only one division of initiation logic is tested at a time. The loop under test is inoperable because the pump breakers for the pumps of that loop are racked out to the test position to verify that the circuitry will cause the breaker to close.

The loop flow instrument calibration occurs once per operating cycle (18 months) and requires 2 hours per instrument to complete. The sensor that provides a flow signal to the minimum-flow bypass valve for one loop is valved out of service preventing automatic operation of that valve. Failure to receive a close signal when loop flow exceeds 1000 gpm will cause diversion of water from the required flow path.

The reactor low pressure sensors that provide shutdown cooling interlocks are tested one at a time on a monthly basis. Each instrument requires 1.5 hours to test. The sensor is valved out and is unavailable to provide the pressure interlock during this test.

The individual reactor level, high drywell pressure, and low reactor pressure sensors that provide signals to the logic circuits are tested monthly, one at a time. These are the same sensors that initiate the core spray system; their testing is discussed in Section 2.6.

Maintenance. Scheduled maintenance (i.e., other than maintenance that is performed due to a random component failure) can cause portions of the system to be inoperable. Table E-10 lists those scheduled maintenance items that cause portions of the RHR system to be made inoperable. It also lists the frequency, duration, and calculated unavailabilities for these items. This information was obtained from plant personnel who schedule and perform these tasks.

Once per year the oil in each RHR pump is changed. Only one pump at a time may be removed from service if this procedure is performed during reactor operation. Four hours are required to complete the task.

Once every operating cycle the pump seal heat exchangers are removed and cleaned. Only one heat exchanger at a time may be removed. Four hours are necessary to complete this task.

While both of these scheduled maintenance items are usually performed during shutdown periods, there are no procedures prohibiting their performance during operation. The unavailability calculation assumes they are done while the plant is operating.

Technical Specification Limitations. Technical specifications require the RHR system to be operable prior to reactor startup. If one pump (IPCI

TABLE B-9. RHR SYSTEM TEST REQUIREMENTS SUMMARY

Component Undergoing Test	Type of Test	Test Procedure Number	Components Aligned Away from Engineered Safeguards Position for Test	Expected Test Frequency	Expected Test Outage Time	Remarks
RHR Loop 1 (R42B45AJ)	Auto-initiation test (logic test)	SI 4.2.B.4.5.a	Pump breaker for Pumps A and C racked out during this test	Once every 6 months	4 hr	Unavailability is accounted for under Pumps A and C $\bar{A} = \frac{4 \text{ hr}}{(720)(6)} = 0.000913$
RHR Loop 2 (R42B45AJ)	Auto-initiation test (logic test)	SI 4.2.B.4.5.b	Same as above for Pumps B and D	Once every 6 months	4 hr	Same as above; Technical Specifications require loops be tested at different times
Loop flow instrumentation (for minimum-flow bypass valve input)	Sensor calibration	IMI-224	Sensors valved out of system and connected to tester; bypass valves will not operate automatically	Once every operating cycle	2 hr per instrument	Provides flow input signal to minimum-flow bypass valves; only one loop tested at a time $\bar{A} = \frac{2 \text{ hr}}{(8760)(1.5)}$ $\bar{A} = 0.000152$
Reactor low pressure sensor (for shutdown cooling interlock)	Sensor calibration	SI 4.2.B.8	Sensor valved out of system and connected to tester; shutdown cooling valve interlocks are inoperable for this test	Once every month	1.5 hr per instrument	Provides pressure interlock to shut down cooling isolation valves; only one sensor tested at a time $\bar{A} = \frac{1.5 \text{ hr}}{720}$ $\bar{A} = 0.0021$

B-51

TABLE B-10. RHR SYSTEM MAINTENANCE ACTS SUMMARY

Maintenance Requirement	Instruction Number	Frequency	Duration	Remarks
RHR pump oil Change A	--	Once every year	4 hr	Only one pump at a time
B				$A = \frac{4 \text{ hr}}{8760} = 0.000456$
C				
D				
RHR pump seal heat exchanger clean-out	--	Once every operating cycle	4 hr	Only one heat exchanger at a time
				$A = \frac{4 \text{ hr}}{(8760)(1.5)} = 0.000304$

Note: Above maintenance combined in fault tree under code: RPM001AJ at
 -
 A = 0.000761; RPM001BJ; RPM001CJ; and RPM001DJ.

mode) is inoperable, operation may continue for 7 days provided that all other RHR pumps (LPCI mode), the core spray system, and the diesel generators are demonstrated to be operable. If two RHR pumps (LPCI mode) are inoperable, the reactor must be in cold shutdown mode within 24 hours. If any containment cooling mode path is inoperable, the reactor may continue to operate for 7 days provided that at least one path for each mode (drywell spray, torus spray, and torus cooling) is operable. Otherwise, the reactor must be in cold shutdown mode within 24 hours.

2.2.3 System Operation

As noted previously, operation of the RHR system in the LPCI mode is automatic. Low water level or high drywell pressure coincident with low reactor pressure initiates the system. The RHR pumps will pump water from the torus to the reactor via the recirculation system discharge lines.

All other modes of RHR operation are manually initiated. In the torus cooling mode, the operator must start the RHRSW pumps to provide cooling to the heat exchangers, start the RHR pumps, and align the discharge valves to the desired flow path. In the shutdown cooling mode, the operator must start the RHRSW pumps, align the suction valves of the desired RHR loop to the recirculation Loop A, start a RHR pump, and align the discharge valves (same valves as LPCI modes) to the recirculation loop discharge path desired. All of these actions are done from the control room.

2.2.4 Fault Tree

Figure B-7 shows the seven fault trees associated with the RHR system. Parts 1 through 17 of Figure B-7 show the four LPCI modes while Parts 18 through 26 show the shutdown cooling, torus cooling, and SBCS modes of RHR.

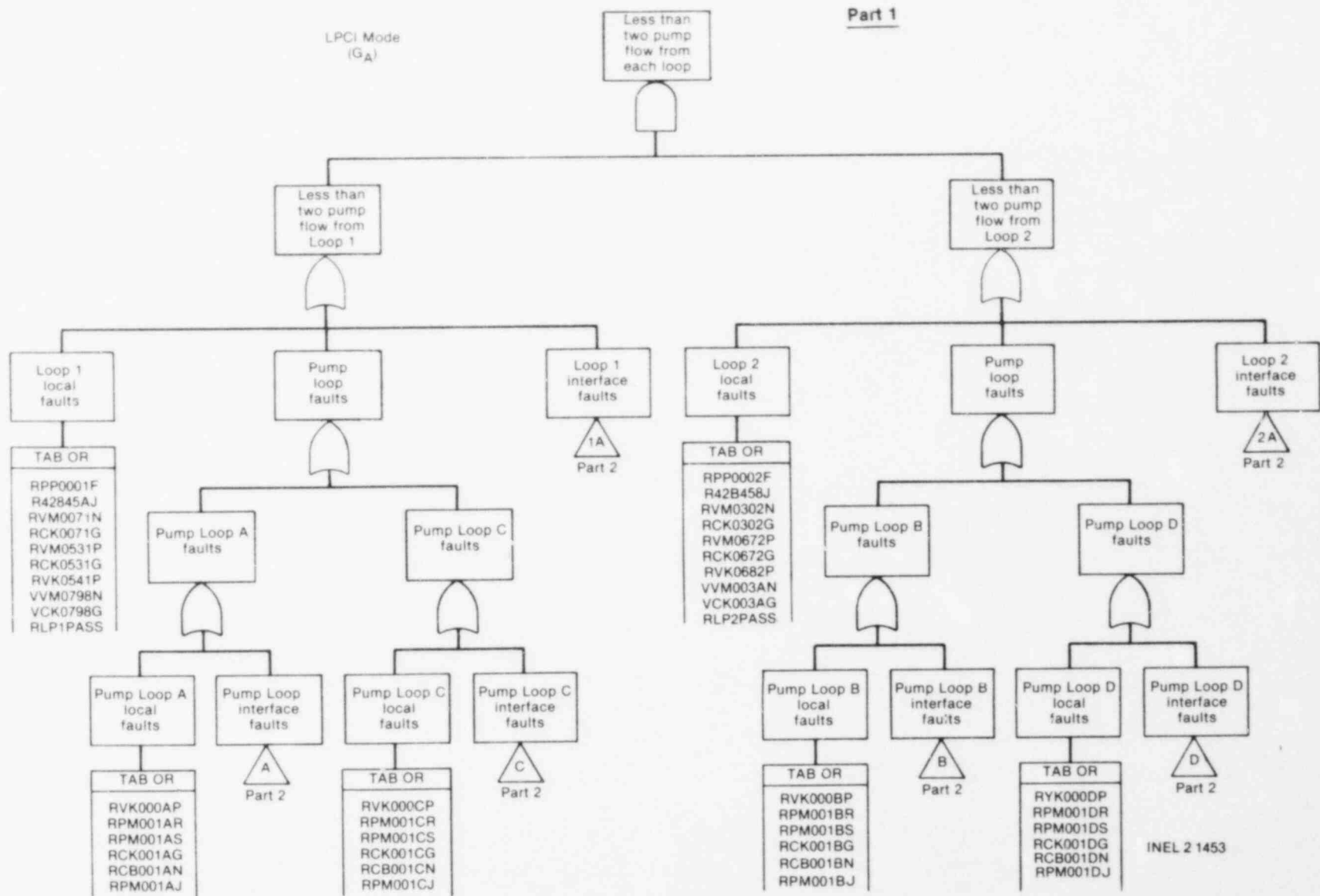
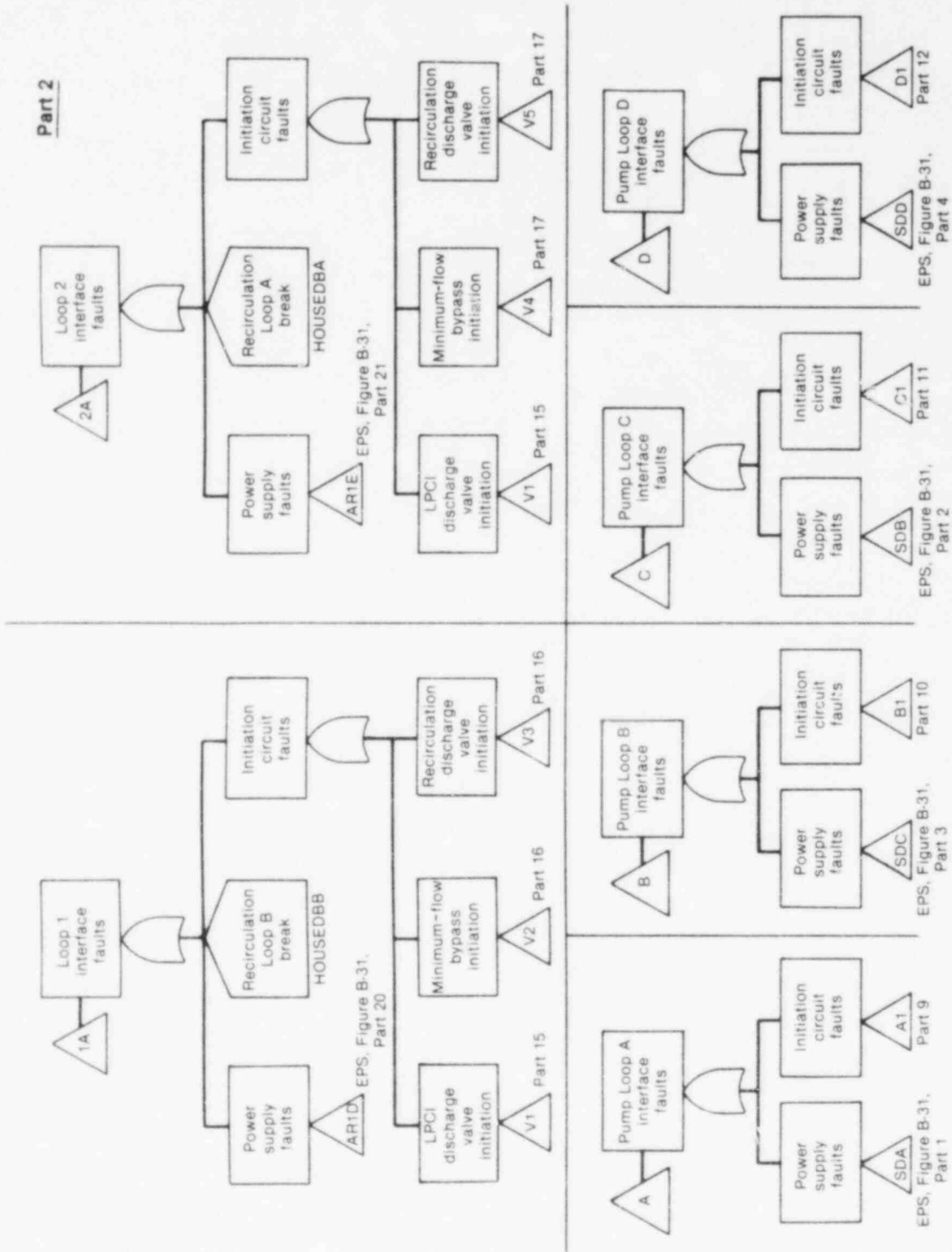


Figure B-7. RHR fault trees.



INEL 2 1454

Figure B-7. (continued).

B-55

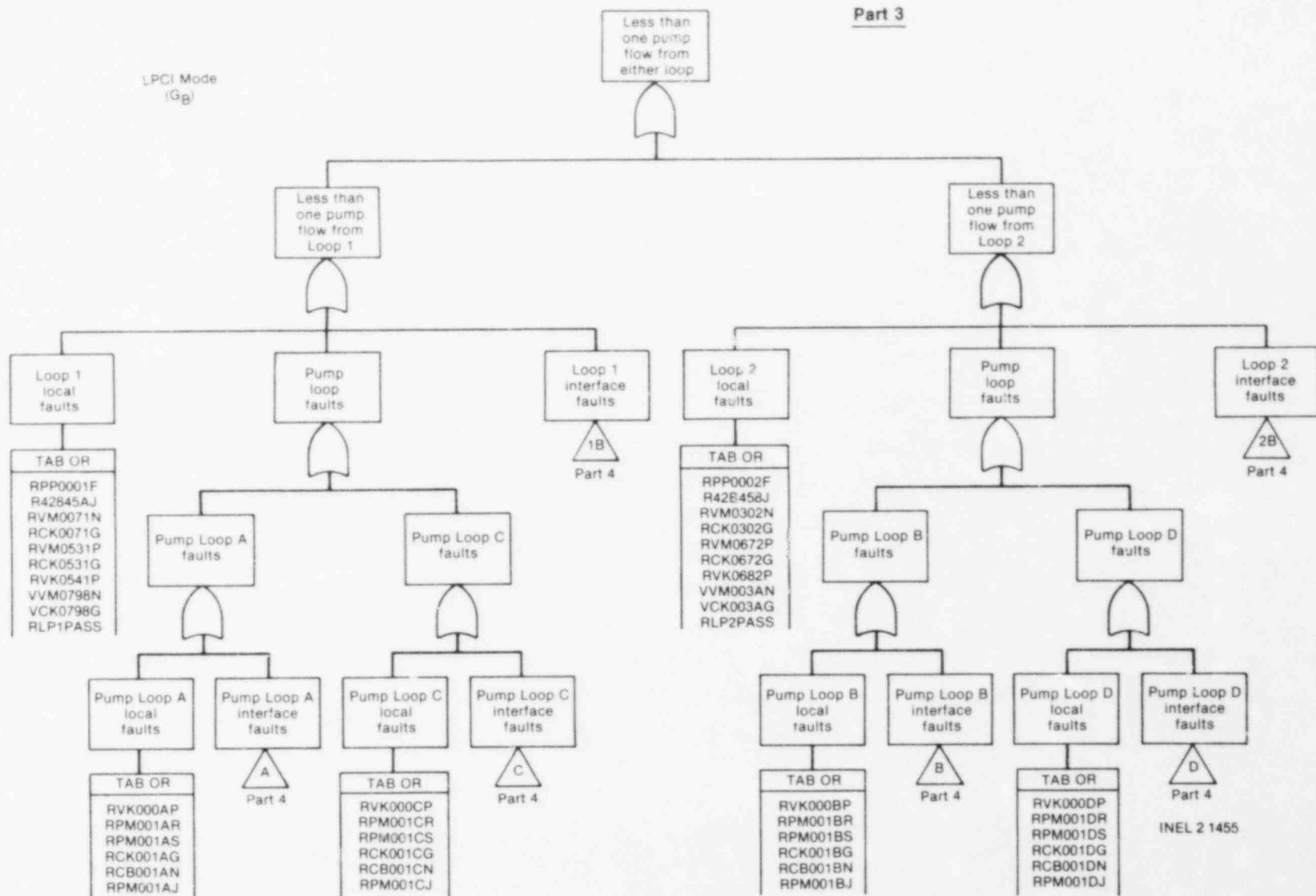


Figure B-7. (continued).

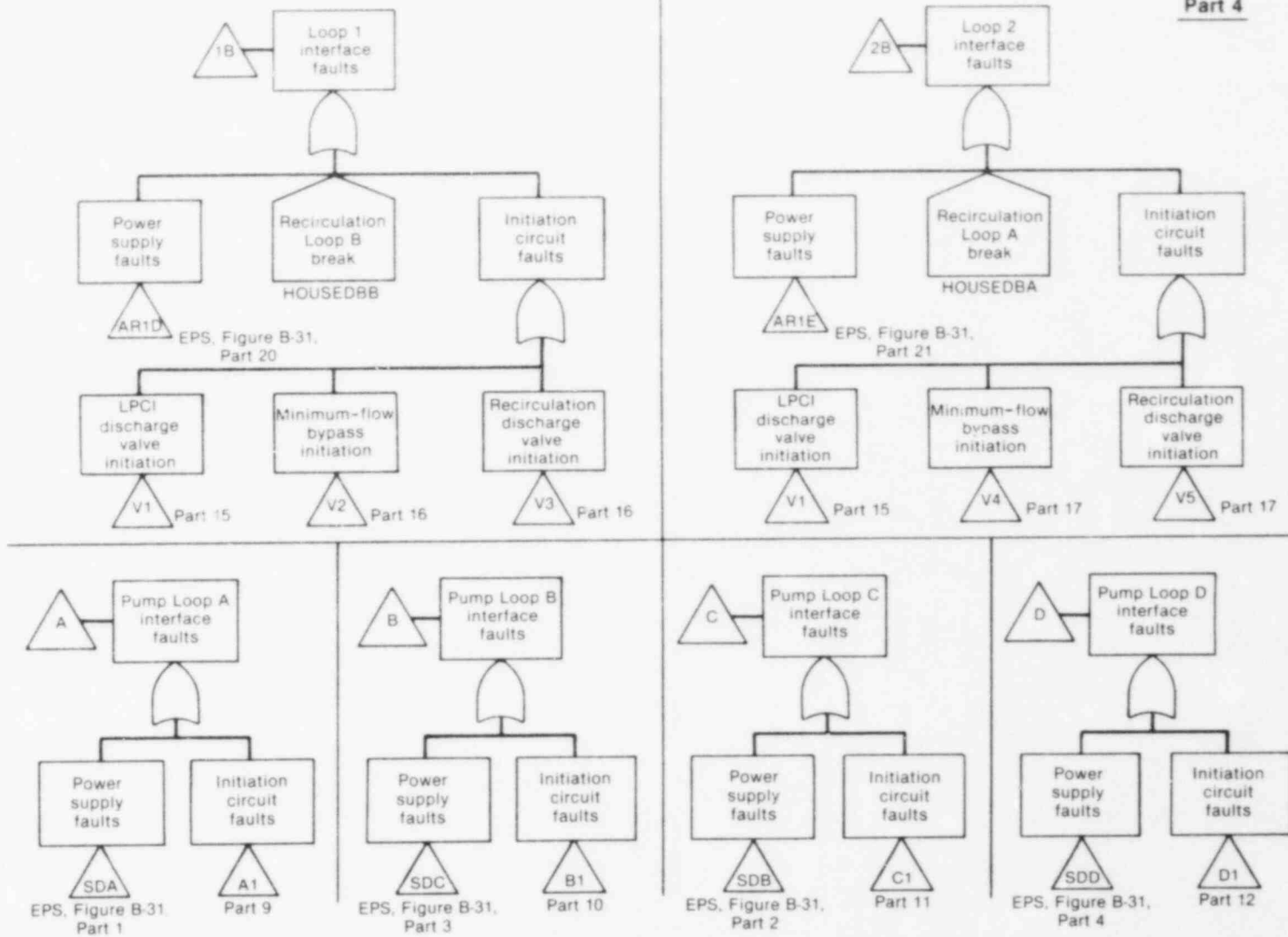


Figure B-7. (continued).

B-57

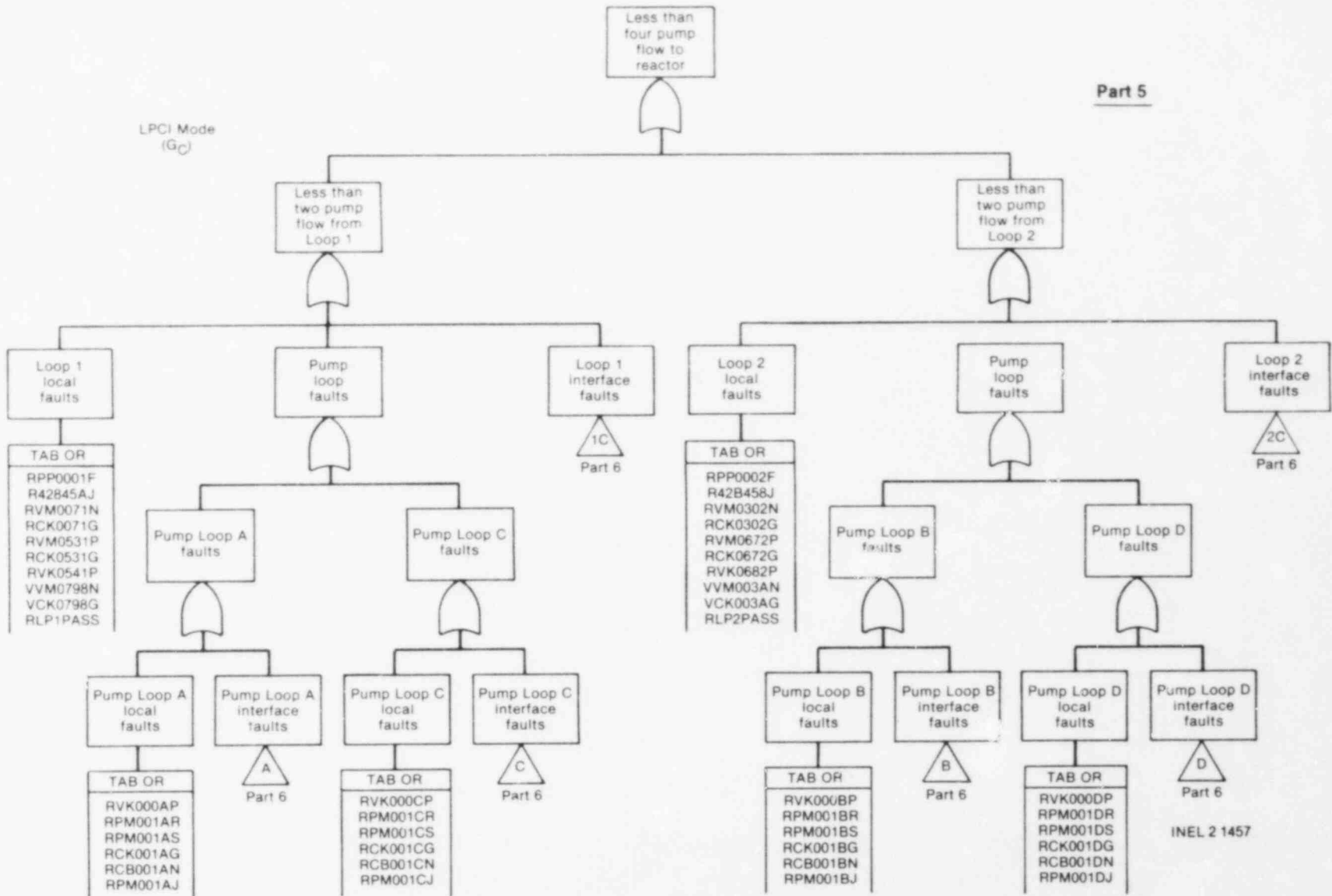
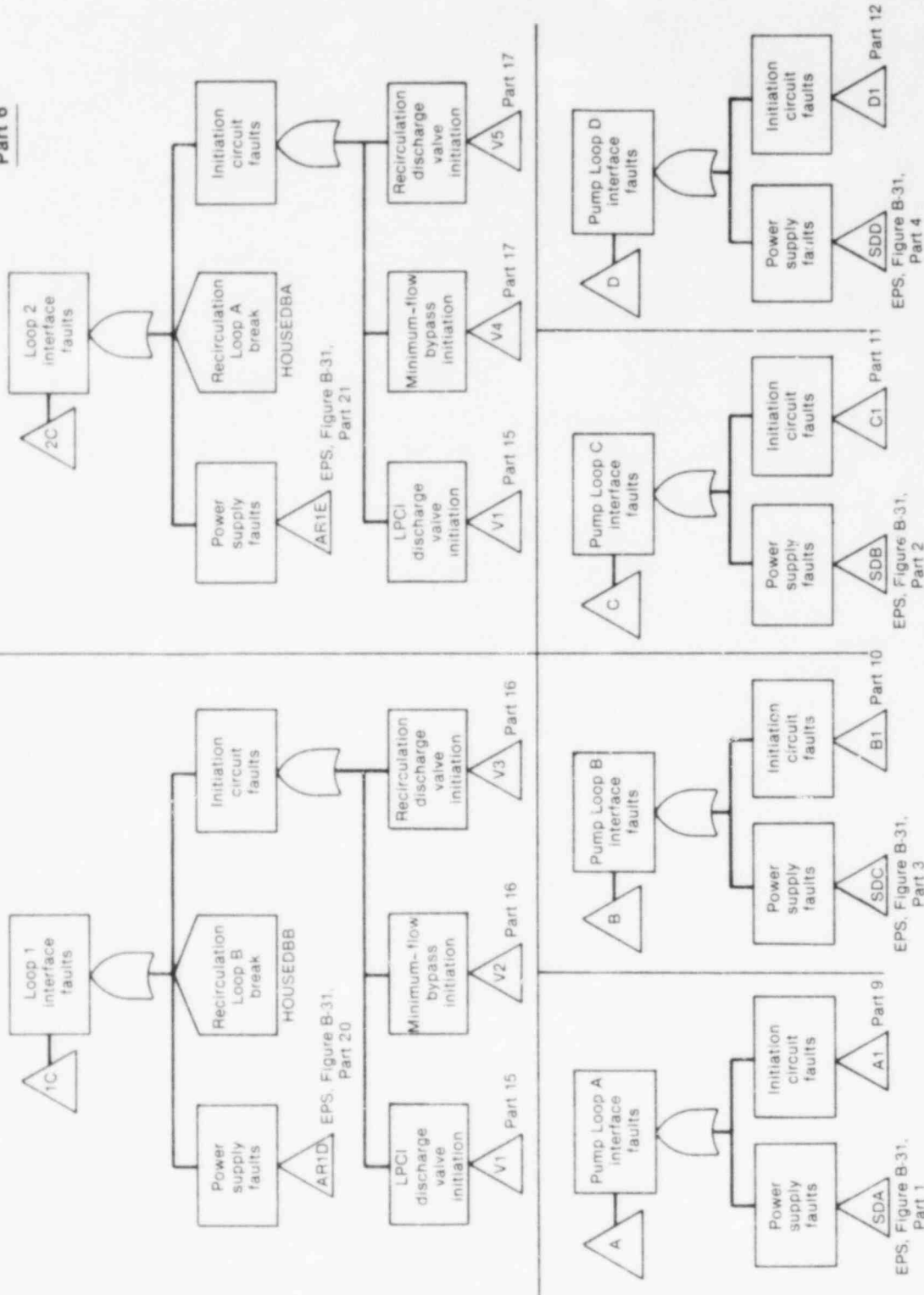


Figure B-7. (continued).

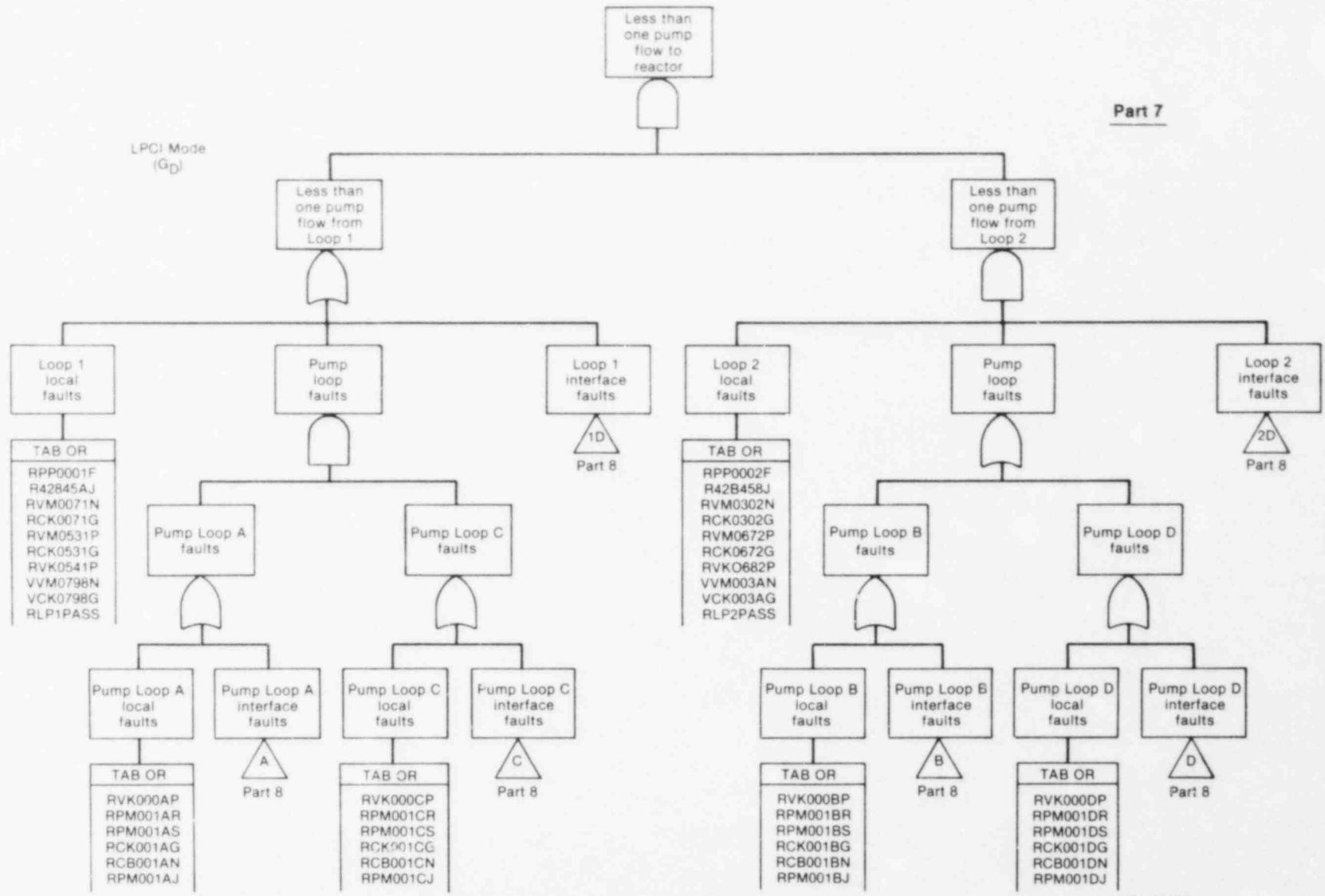
Part 6



INEL 2 1458

Figure B-7. (continued).

B-59



INEL 2 1459

Figure B-7. (continued).

B-60

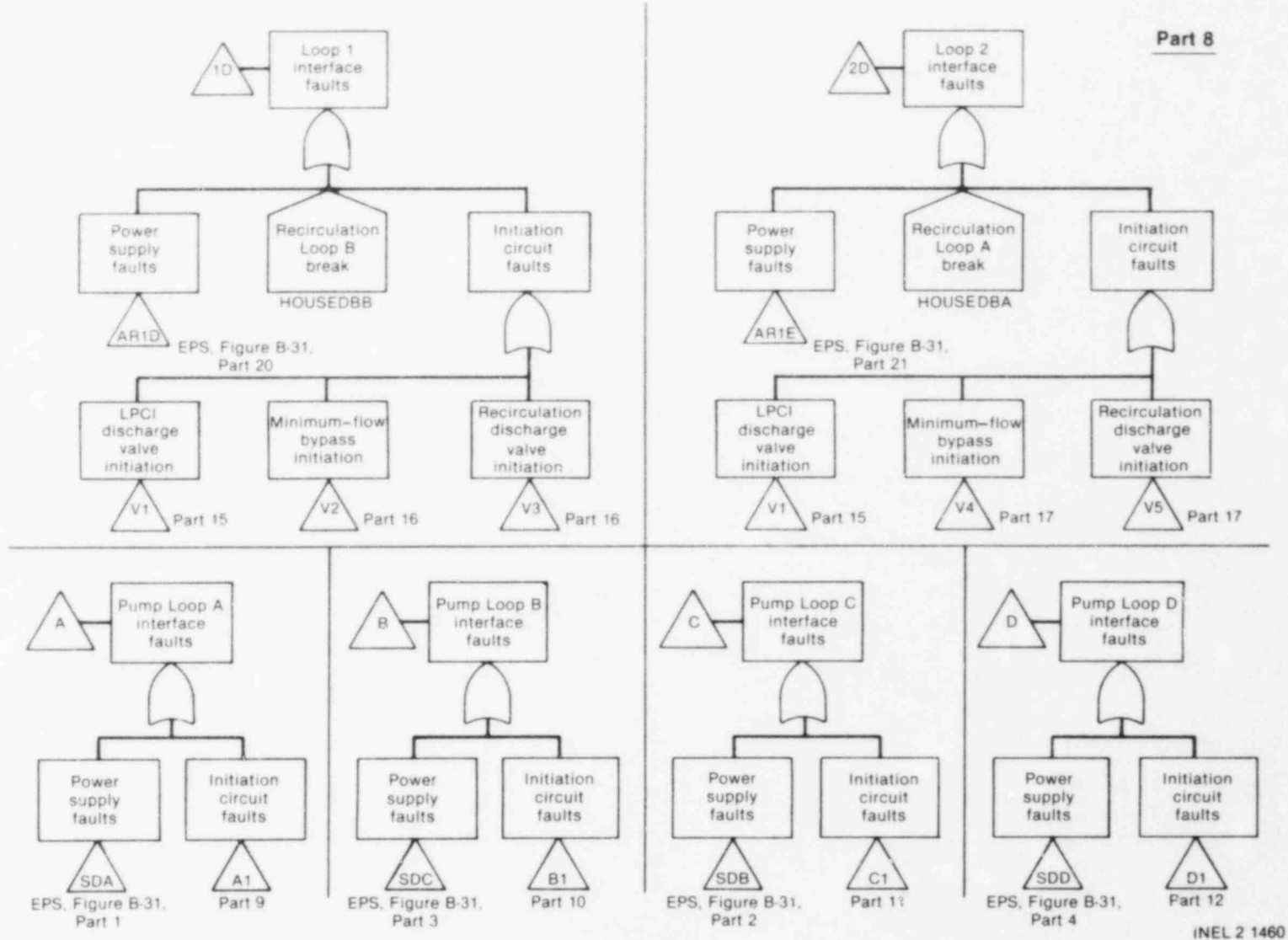


Figure B-7. (continued).

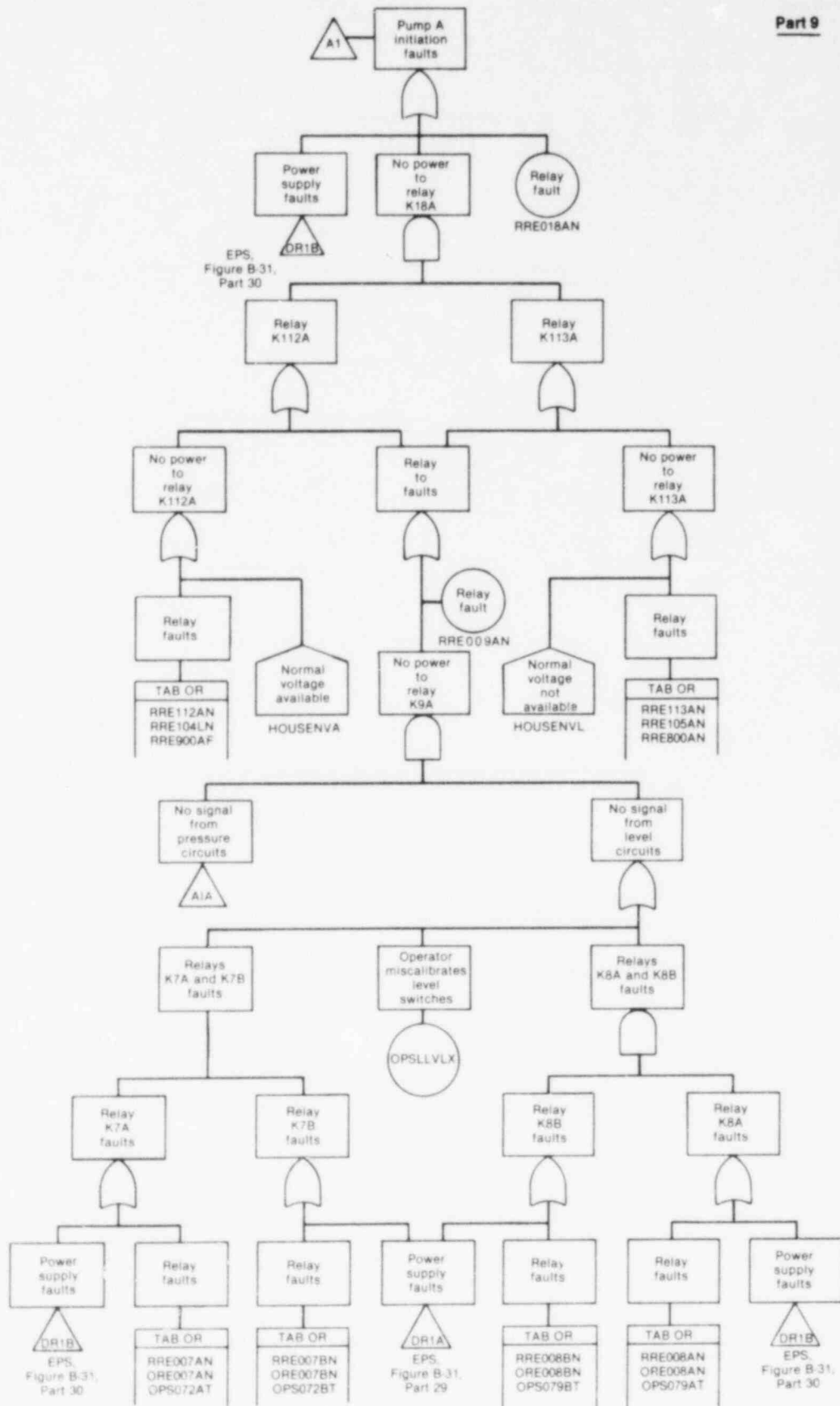


Figure B-7. (continued).

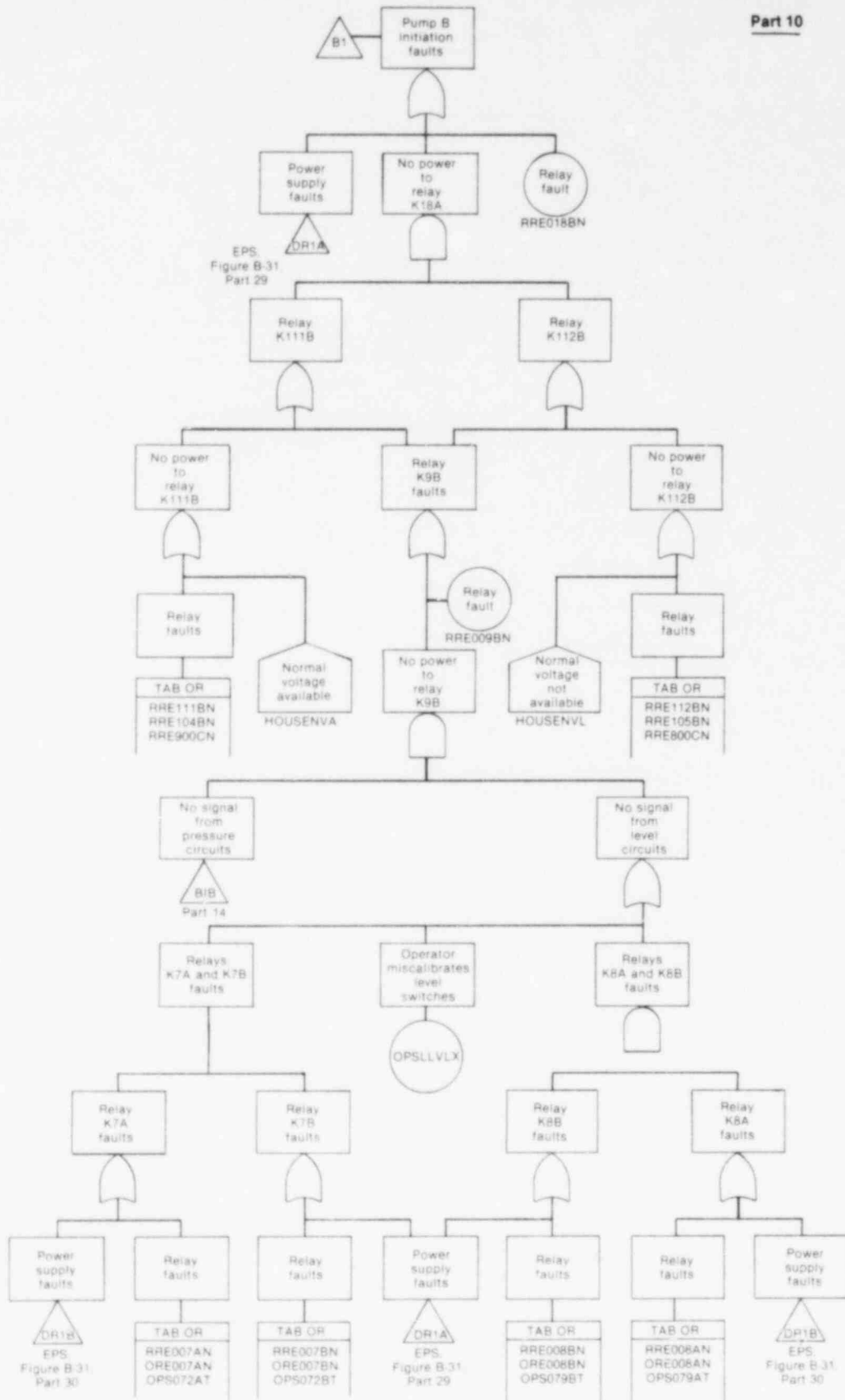


Figure B-7. (continued).

INEL 2 146V

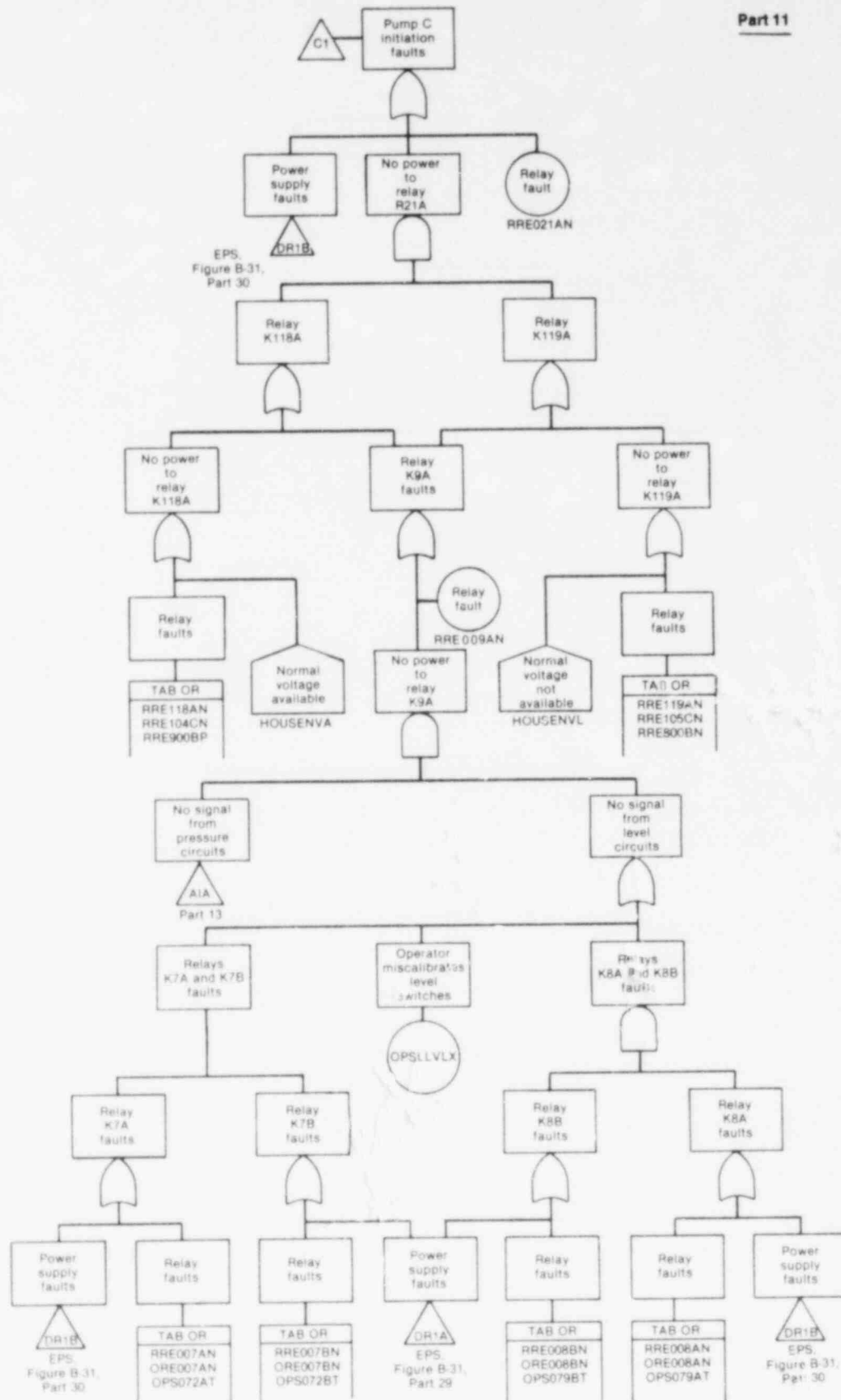


Figure B-7. (continued).

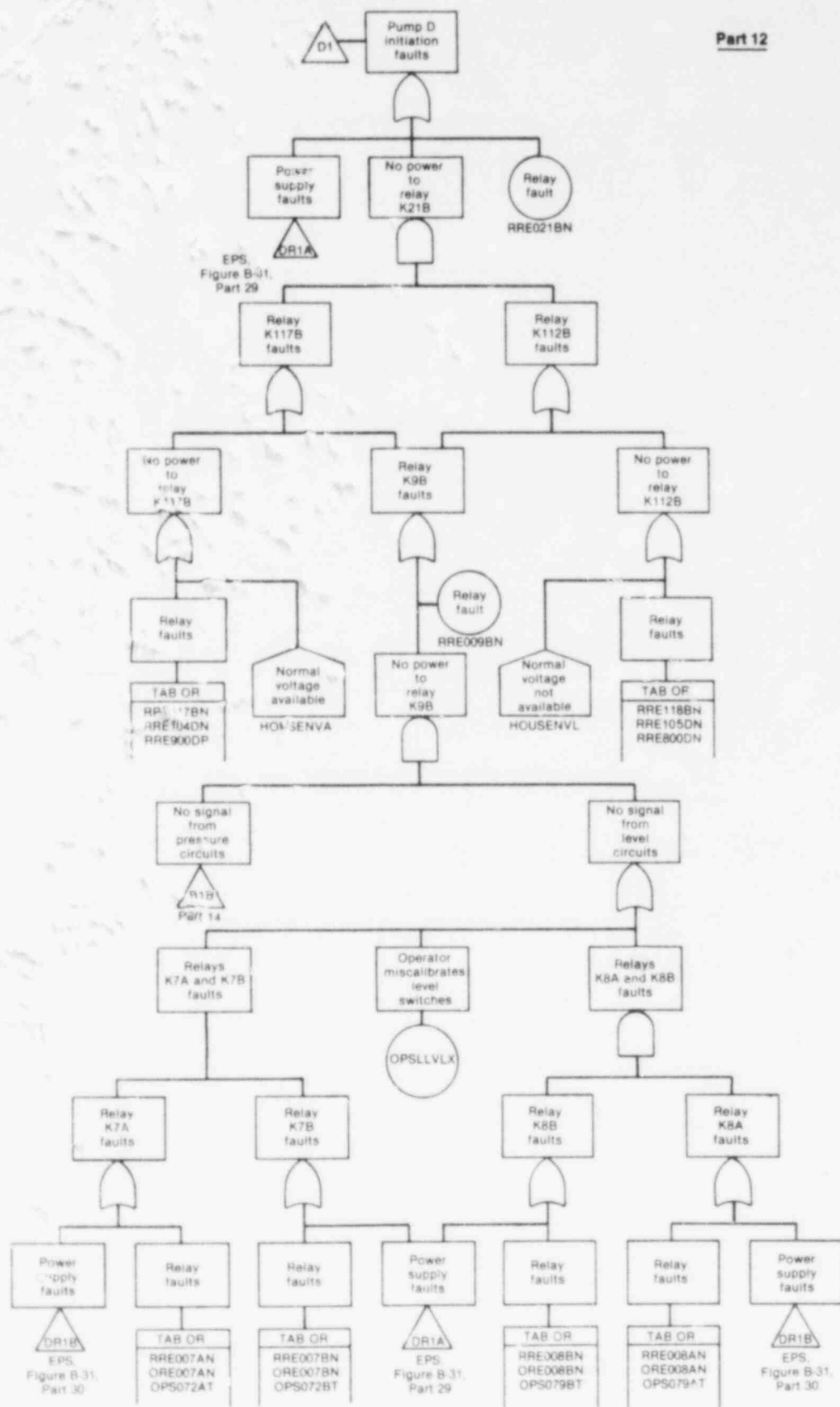


Figure B-7. (continued).

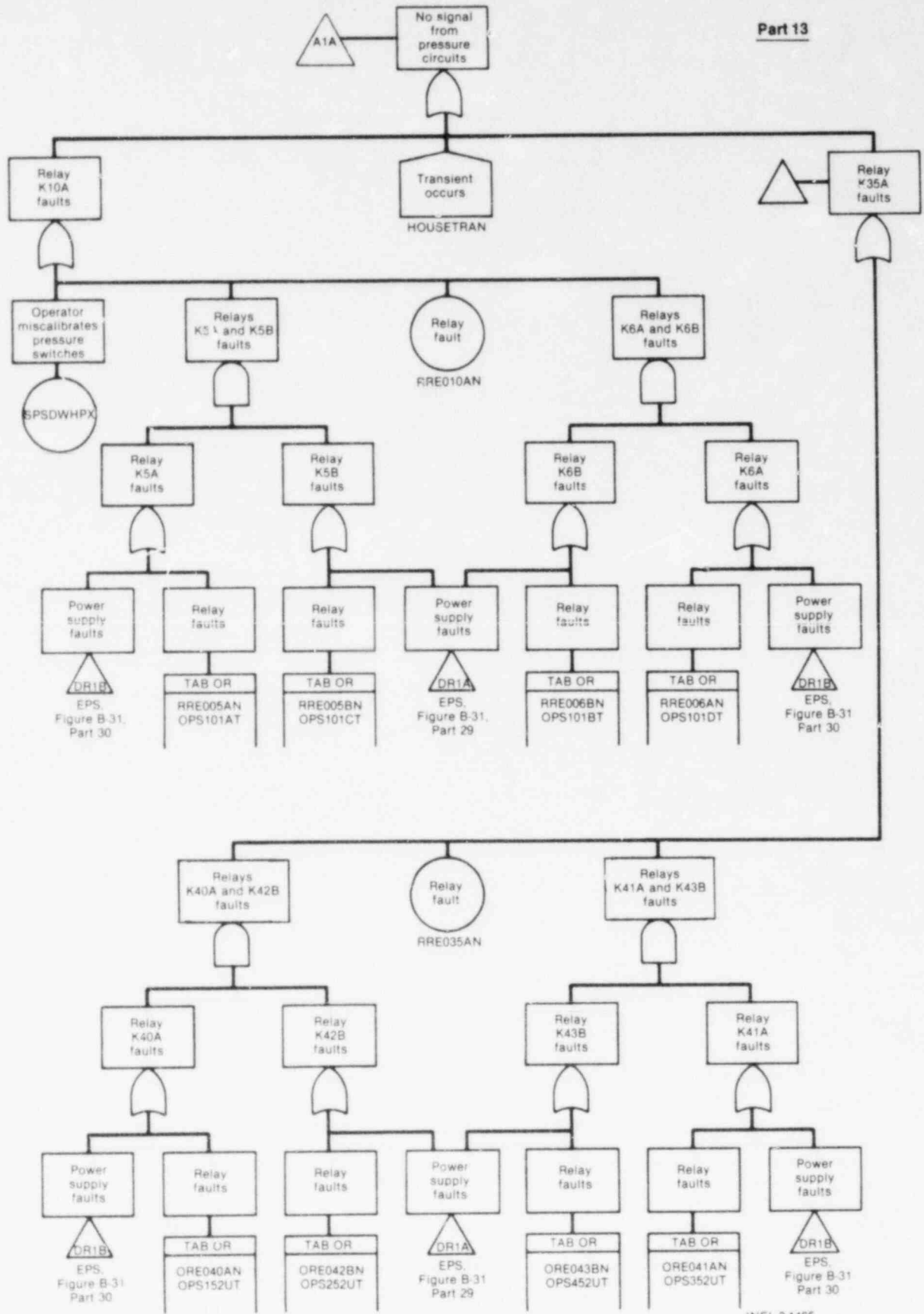


Figure B-7. (continued).

INEL 2 1465

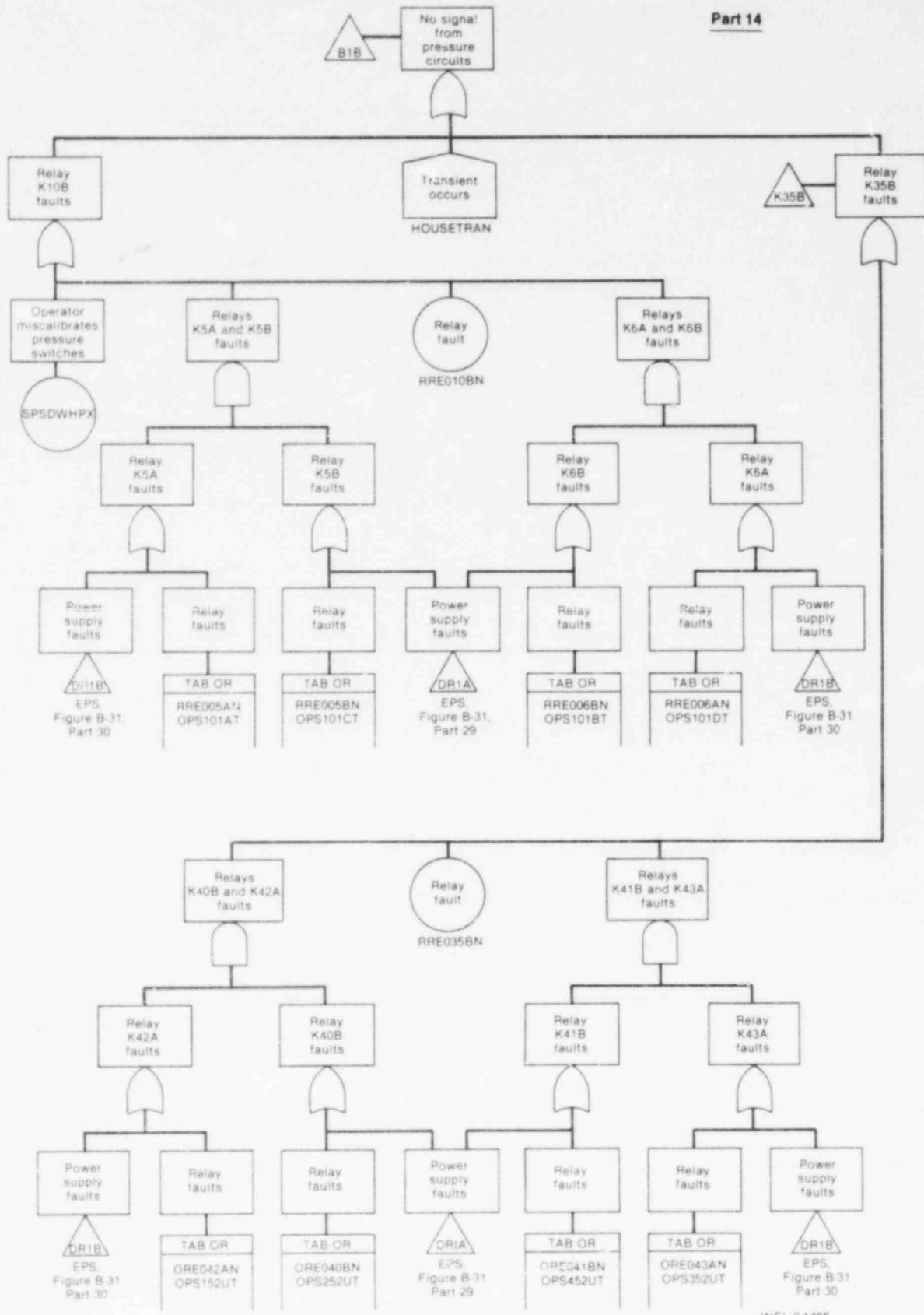


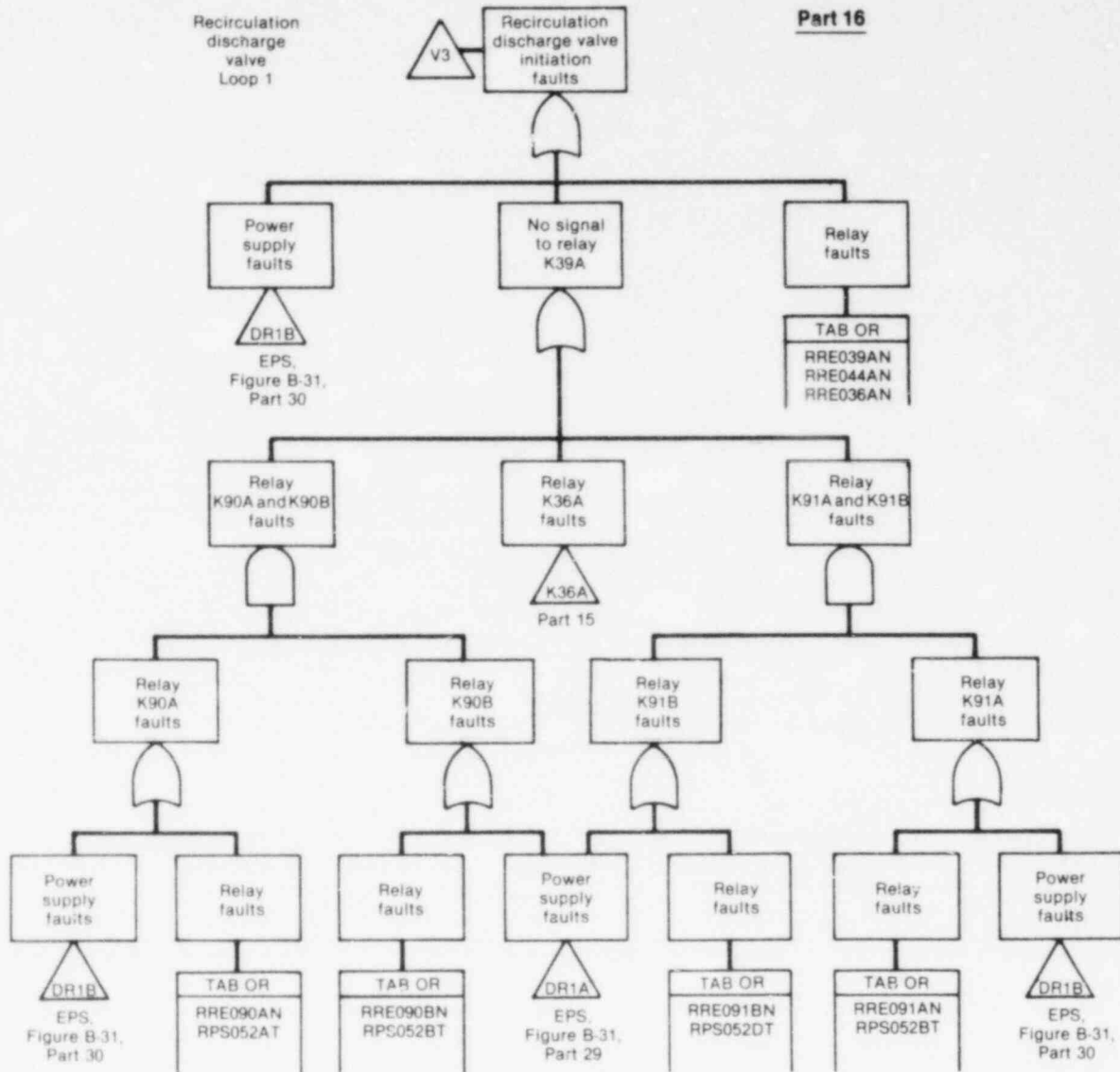
Figure B-7. (continued).



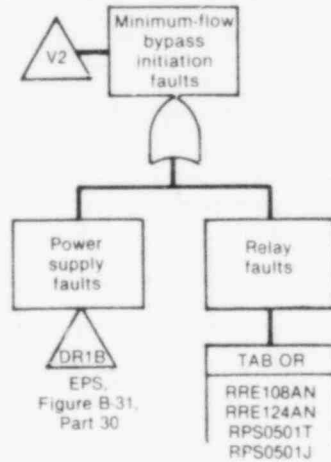
Figure B-7. (continued).

Recirculation discharge valve Loop 1

Part 16

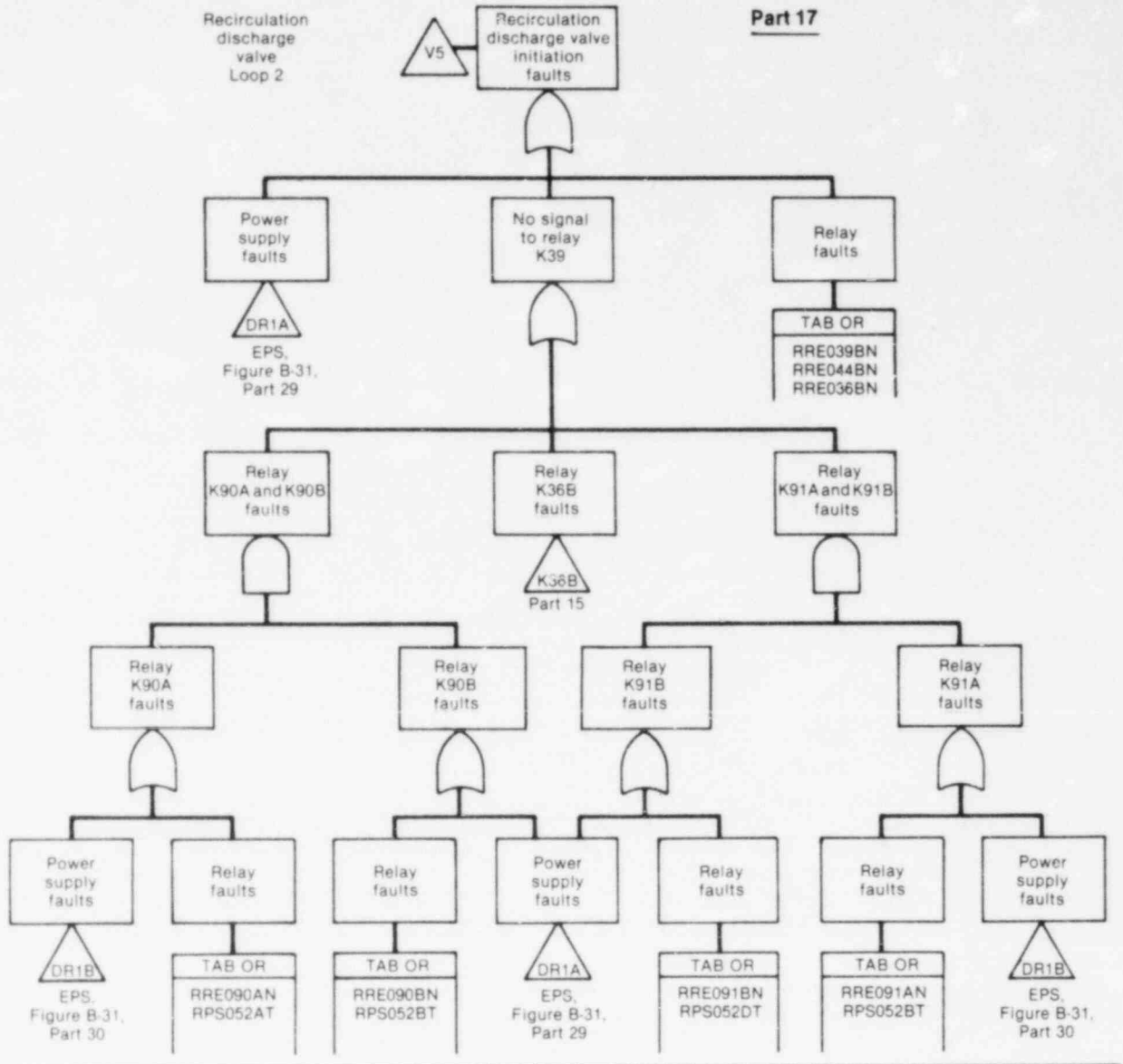


Minimum-flow bypass valve Loop 1

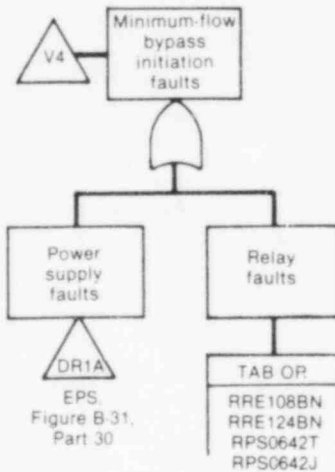


INEL 2 1468

Figure B-7. (continued).



Minimum-flow bypass valve Loop 2



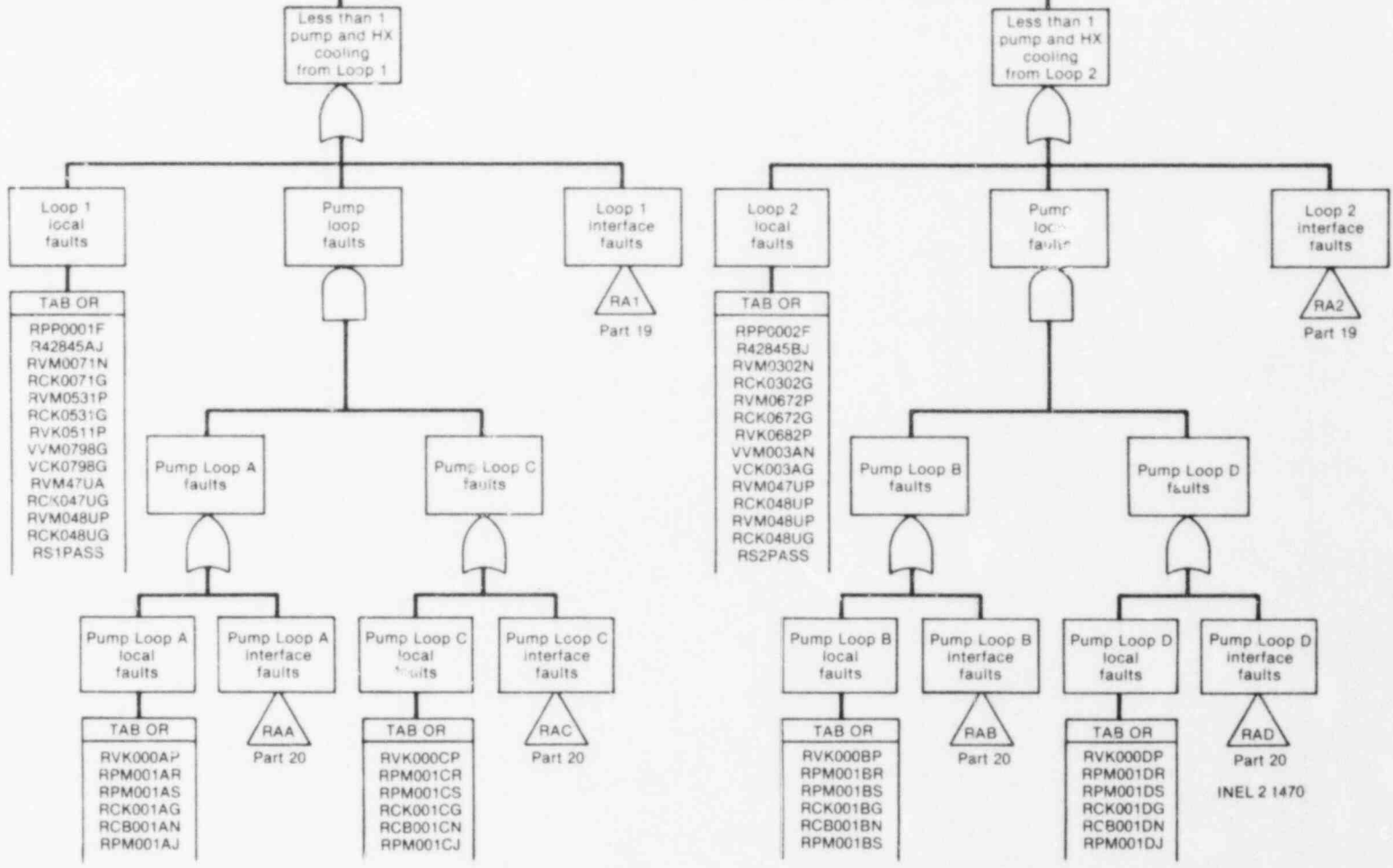
INEL 2 1469

Figure B-7. (continued).

Less than 1 pump and HX cooling reactor

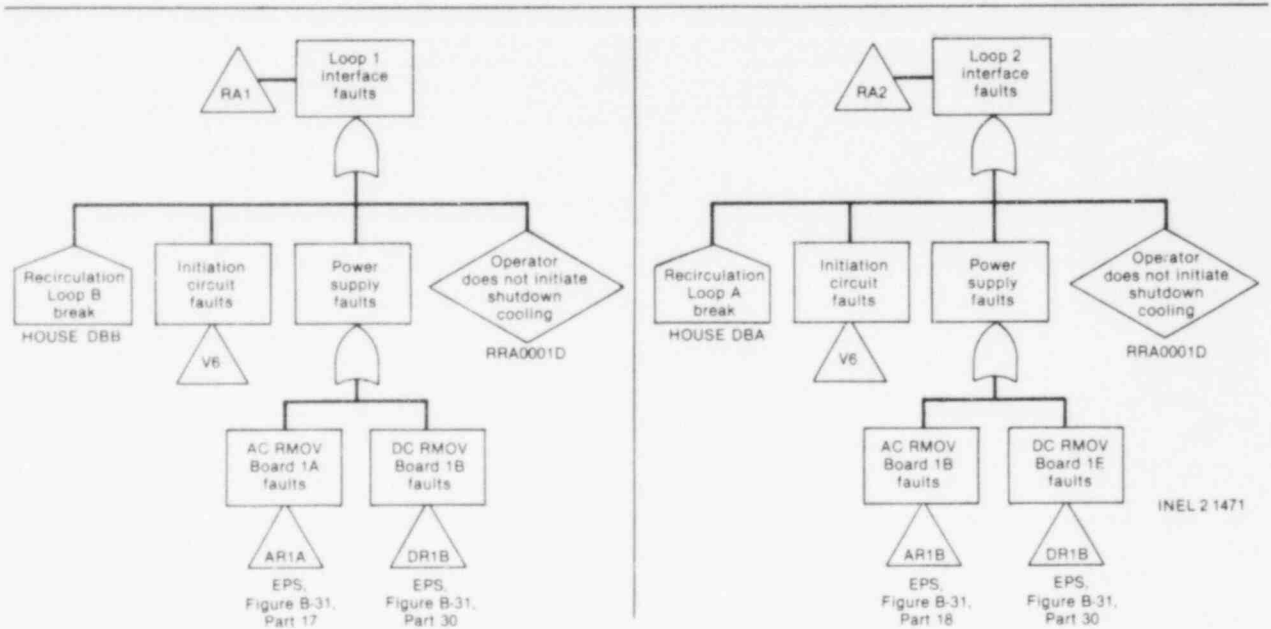
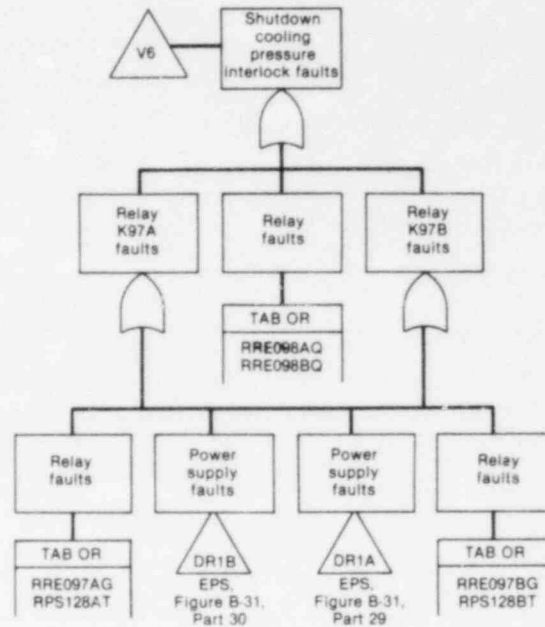
Part 18

Shutdown cooling (RA)



B-70

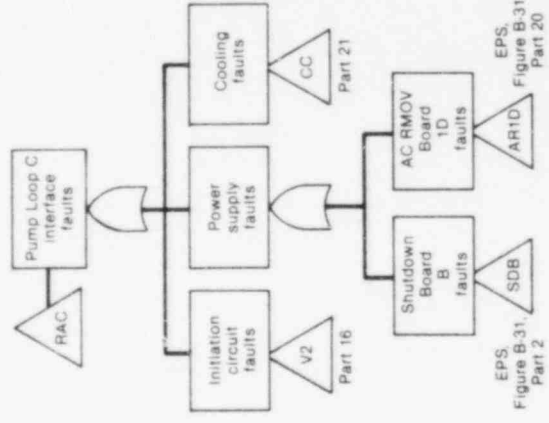
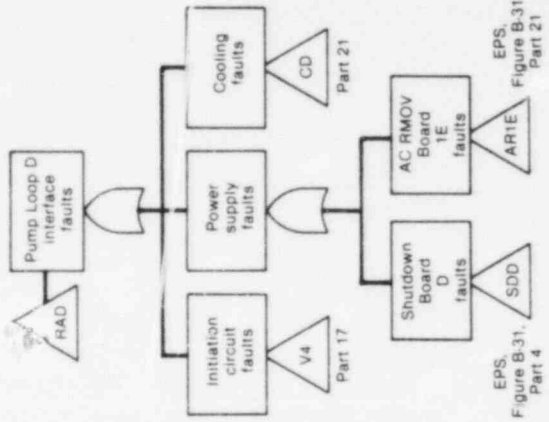
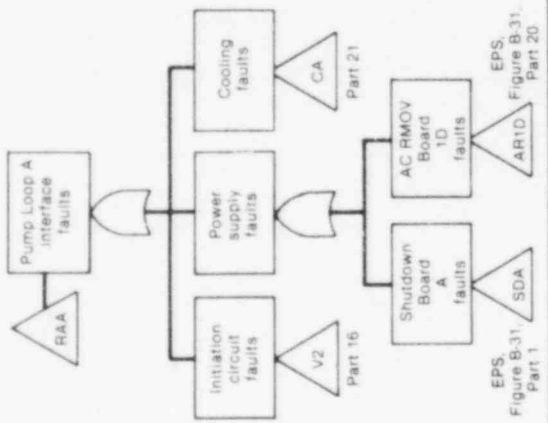
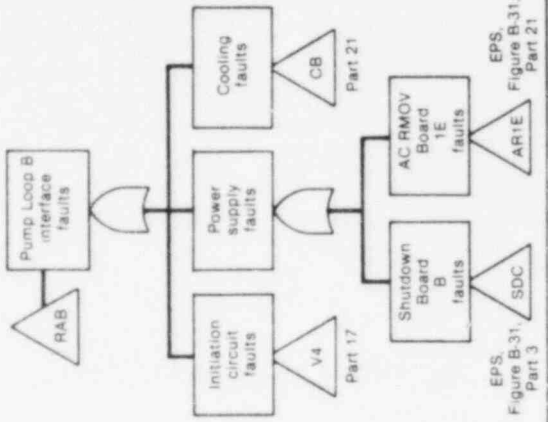
Figure B-7. (continued).



INEL 2 1471

Figure B-7. (continued).

Part 20



INEL 2 1472

Figure B-7. (continued).

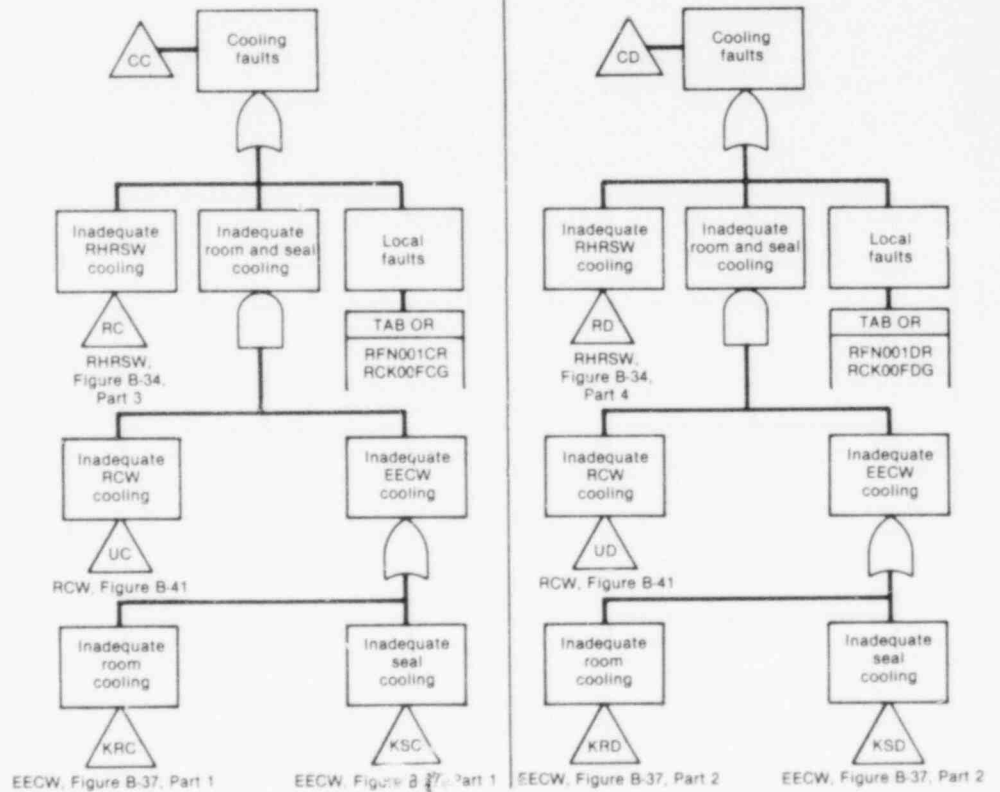
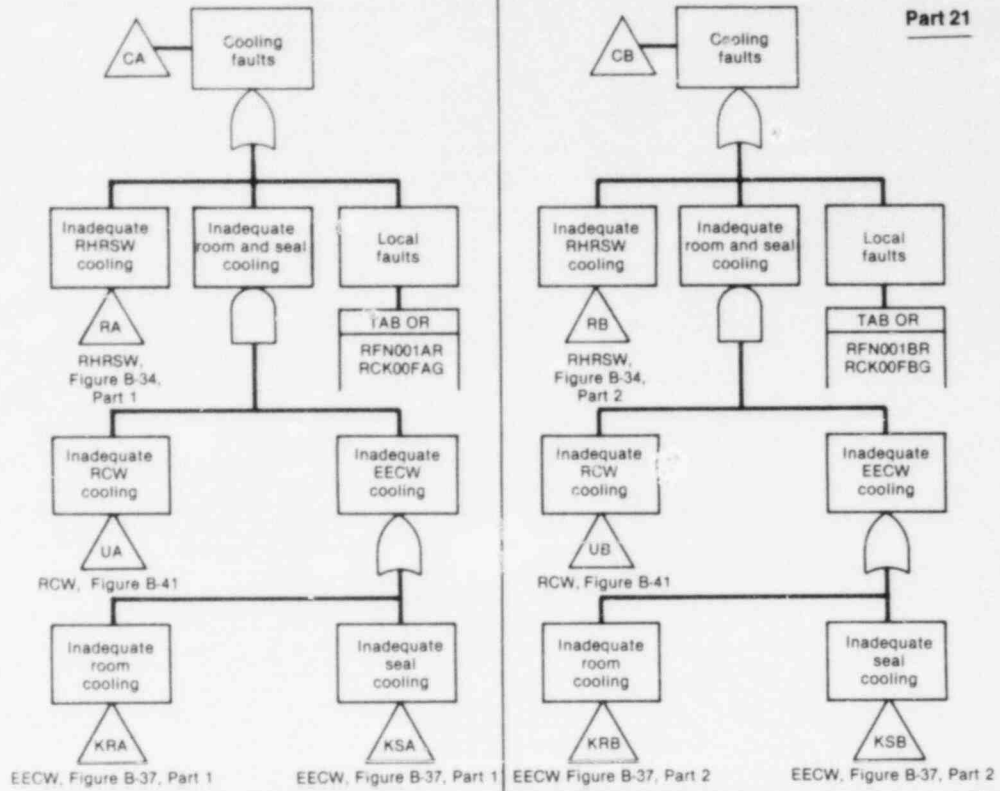
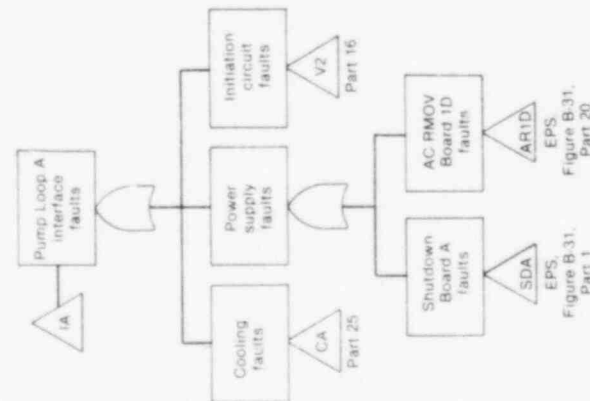
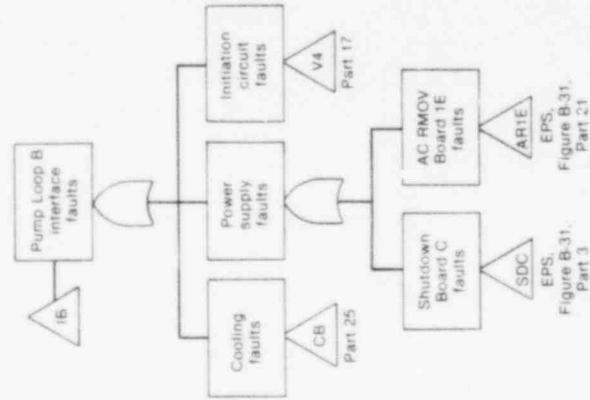
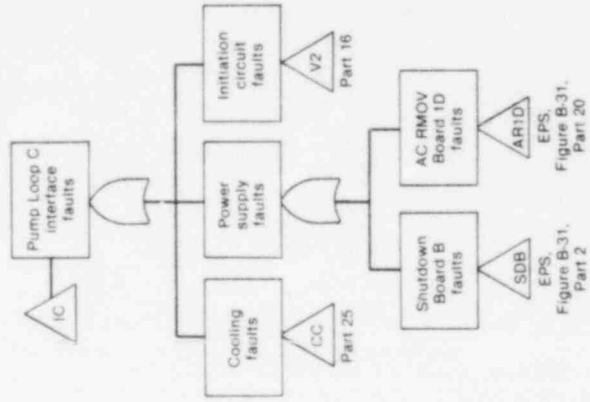
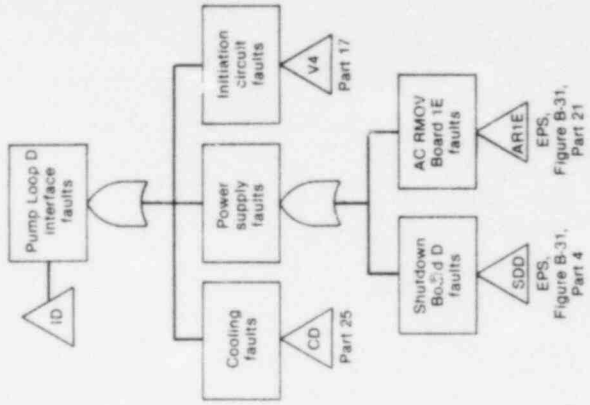
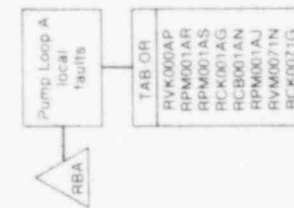
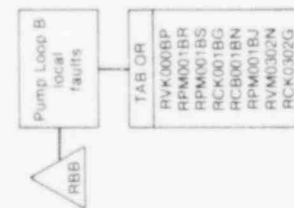
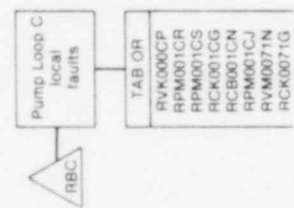
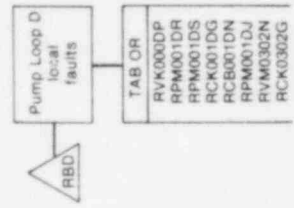


Figure B-7. (continued).

Part 24



INEL 2 1476

Figure B-7. (continued).

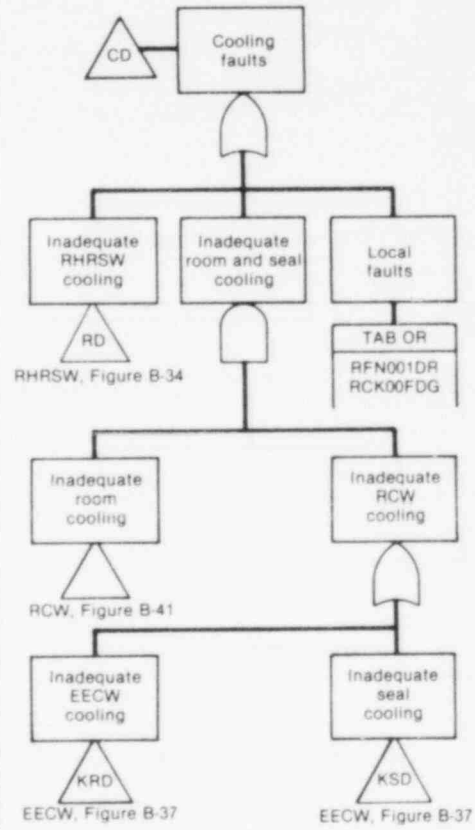
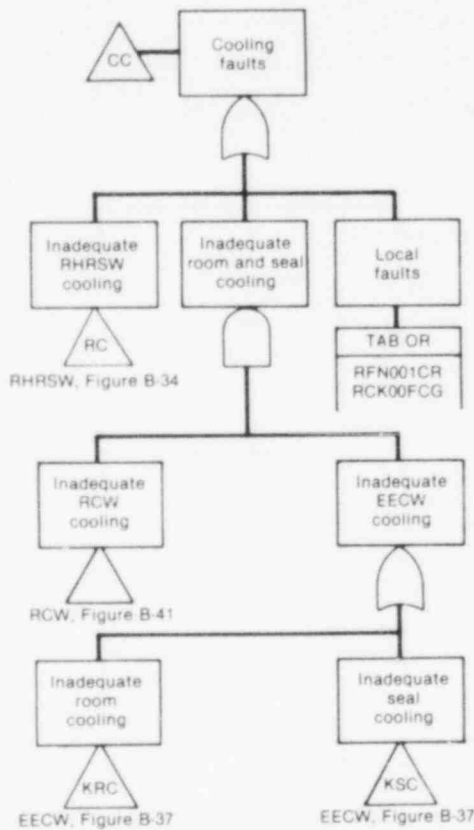
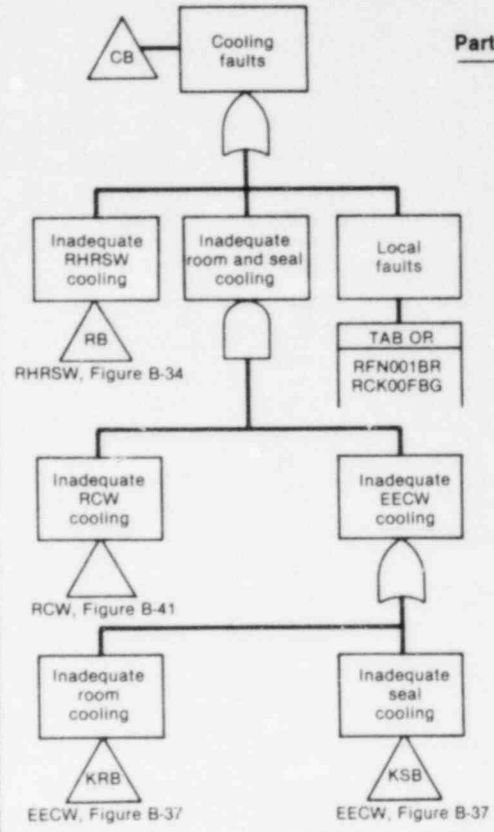
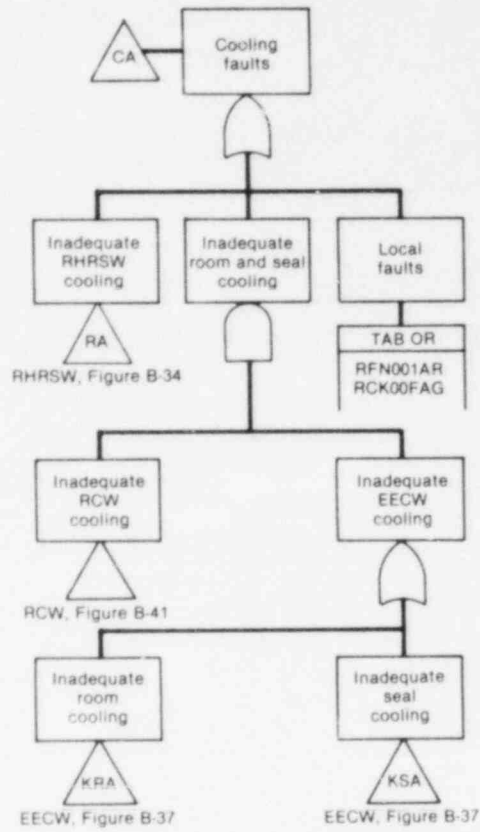


Figure B-7. (continued).

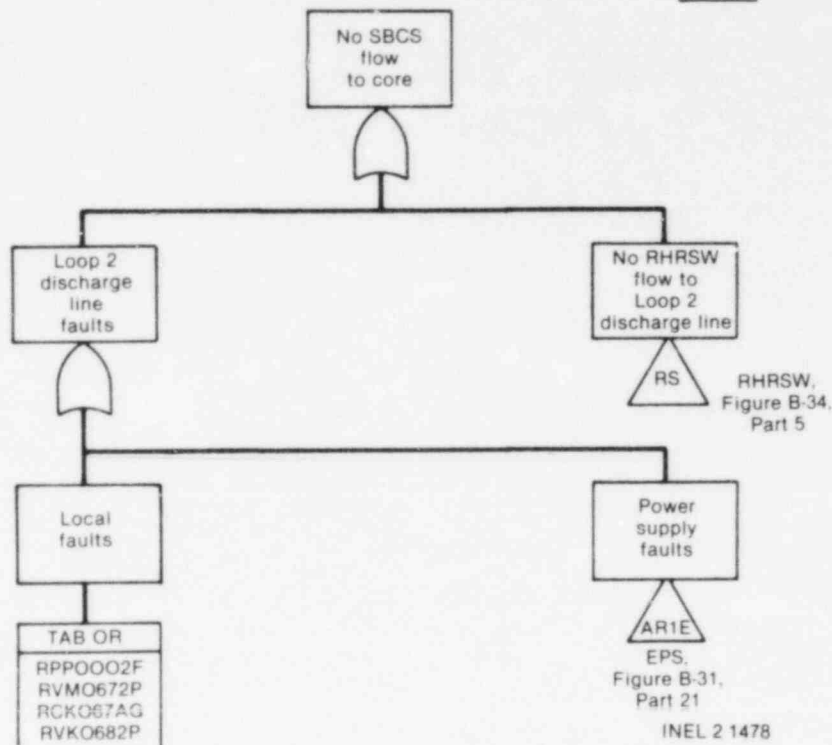


Figure B-7. (continued)

Table B-11 is the fault summary short form for these fault trees and lists the data associated with each basic event.

Each LPCI mode of RHR is represented by a fault tree in Parts 1 through 8 of Figure B-7. Parts 9 through 17 are the initiation logic for the pumps and valves common to each LPCI mode. Similarly the shutdown cooling and torus cooling fault trees appear in Parts 18 through 25. Part 26 shows the logic for the SBCS.

There are five house events appearing in the RHR fault trees. The HOUSEDBA and HOUSEDBB events allow for calculating RHR unavailabilities when a break occurs on the discharge piping of a recirculation loop. Note that these are mutually exclusive. That is, if one house event is "on" the other is "off." Both are "off" when no recirculation discharge break occurs. The HOUSETRAN event is "on" for RHR unavailabilities with transient initiators. This house event accounts for the lack of high drywell initiation for transients. The HOUSENVA and HOUSENVL are mutually exclusive houses appearing in the pump initiation circuitry model. One house will be "on" while the other is "off." This accounts for the initiation unavailability due to failures in the power available sensing circuits. Table B-12 summarizes the treatment of house events for the RHR systems.

In Figure B-7, the transfer devices show an alphanumeric code and a part number if the transfer appears in another part of the RHR tree. If

TABLE B-11. RHR SYSTEM FAULT SUMMARY SHORT FORM

Event Name	Event Component	Failure Mode	Primary Failure			
			Failure Rate	Fault Duration (hr)	Error Factor	
RPM001AR	RHR Pump A	Does not start	1E-3/D	--	3	
RPM001AS	↓	Does not run	3E-5/hr	8	10	
RCB001AN		Does not close	1E-3/D	--	3	
RCK001AG		No output	3.3E-3	--	10	
RPM001AJ	↓	Maintenance	7.6E-4	--	0	
RPM001BR		RHR Pump B	Does not start	1E-3/D	--	3
RPM001BS		↓	Does not run	3E-5/hr	8	10
RCB001BN	Does not close		1E-3/D	--	3	
RCK001BG	No output		3.3E-3	--	10	
EPM001BJ	↓	Maintenance	7.6E-4	--	0	
RPM001CR		RHR Pump C	Does not start	1E-3/D	--	3

B-79

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RPM001CS	RHR Pump C	Does not run	3E-5/hr	8	10
RCB001CN	↓	Does not close	1E-3/D	--	3
RCK001CG		No output	3.3E-3	--	10
RPM001CJ		Maintenance	7.6E-4	--	0
RPM001DR		RHR Pump D	Does not start	1E-3/D	--
RPM001DS	↓	Does not run	3E-5/hr	8	10
RCB001DN		Does not close	1E-3/D	--	3
RCK001DG		No output	3.3E-3	--	10
RPM001DJ		Maintenance	7.6E-4	--	0
RVK000AP	Pump A check valve	Does not open	1E-4/D	--	3
RVK000BP	Pump B check valve	Does not open	1E-4/D	--	3
RVK000CP	Pump C check valve	Does not open	1E-4/D	--	3

B-80

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RVK000DP	Pump D check valve	Does not open	1E-4/D	--	3
RVM0071N	Loop 1 minimum flow bypass	Does not close	1E-3/D	--	3
RCK0071G	Minimum flow bypass continued check	No output	3.3E-3	--	10
RVM0302N	Loop 2 minimum flow bypass	Does not close	1E-3/D	--	3
RCK0302G	Minimum flow bypass continued check	No output	3.3E-3	--	10
RVM0531P	Loop 1 LPCI disk valve	Does not open	1E-3/D	--	3
RCK0531G	Loop 1 LPCI disk valve	No output	3.3E-3	--	10
RVK0541P	Loop 1 LPCI check valve	Does not open	1E-4/D	--	3
RVM0672P	Loop 2 LPCI disk valve	Does not open	1E-3/D	--	3
RCK0672G	Loop 2 LPCI disk valve	No output	3.3E-3	--	10
RVK0682P	Loop 2 LPCI check valve	Does not open	1E-4/D	--	3

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RPP0001F	Loop 1 piping	Rupture	1E-10/ hr/ section	8	30
RPP0002F	Loop 2 piping	Rupture	1E-10/ hr/ section	8	30
RVM0571P	Loop 1 inboard torus cooling valve	Does not open	1E-3/D	--	3
RCK0571G	Loop 1 inboard torus cooling valve	No output	3.3E-3	--	10
RVM0581P	Loop 1 outboard torus spray valve	Does not open	1E-3/D	--	3
RCK0581G	Loop 1 outboard torus spray valve	No output	3.3E-3	--	10
RVM0591P	Loop 1 outboard torus cooling valve	Does not open	1E-3/D	--	3
RCK0591G	Loop 1 outboard torus cooling valve	No output	3.3E-3	--	10
RVM0712P	Loop 2 inboard torus cooling valve	Does not open	1E-3/D	--	3

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RCK0712G	Loop 2 inboard torus cooling valve	No output	3.3E-3	--	10
RVM0722P	Loop 2 outboard torus spray valve	Does not open	1E-3/D	--	3
RCK0722G	Loop 2 outboard torus spray valve	No output	3.3E-3	--	10
RVM0732P	Loop 2 outboard torus cooling valve	Does not open	1E-3/D	--	3
RCK0732G	Loop 2 outboard torus cooling valve	No output	3.3E-3	--	10
RVM001AN	RHR Pump A torus suction valve	Does not close	1E-3/D	--	3
RCK000AG	RHR Pump A torus suction valve	No output	3.3E-3	--	10
RVM002AP	RHR Pump A shutdown cooling suction valve	Does not open	1E-3/D	--	3
RCK002AG	RHR Pump A shutdown cooling suction valve	No output	3.3E-3	--	10
RVM024BN	RHR Pump B torus suction valve	Does not close	1E-3/D	--	3

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RCK024BG	RHR Pump B torus suction valve	No output	3.3E-3	--	10
RVM025BP	RHR Pump B shutdown cooling suction valve	Does not open	1E-3/D	--	3
RCK025BG	RHR Pump B shutdown cooling suction valve	No output	3.3E-3	--	10
RVM012CN	RHR Pump C torus suction valve	Does not close	1E-3/D	--	3
RCK012CG	RHR Pump C torus suction valve	No output	3.3E-3	--	10
RVM013CP	RHR Pump C shutdown cooling suction valve	Does not open	1E-3/D	--	3
RCK013CG	RHR Pump C shutdown cooling suction valve	No output	3.3E-3	--	10
RVM0350N	RHR Pump D torus suction valve	Does not close	1E-3/D	--	3
RCK035DG	RHR Pump D torus suction valve	No output	3.3E-3	--	10
RVM036DP	RHR Pump D shutdown cooling suction valve	Does not open	1E-3/D	--	3

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RCK036DG	RHR Pump D shutdown cooling suction valve	No output	3.3E-3	--	10
R42B45AJ	RHR Loop 1 initial check	Test	9.1E-4	--	0
R42B45BJ	RHR Loop 2 initial check	Test	9.1E-4	--	0
RRB0001D	Manual initiation torus cooling mode	Operator error	1E-3/D	--	10
RRA0001D	Manual initiation shutdown cooling mode	Operator error	1E-3/D	--	10
VVM079BN	Recirculation Loop B disk valve	Does not close	1E-3/D	--	3
VCK079BG	--	No output	3.3E-3	--	10
VVM003AN	--	Does not close	1E-3/D	--	3
VCK003AG	--	No output	3.3E-3	--	10

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RVM048UP	--	Does not open	1E-3/D	--	3
RCK048UG	--	No output	3.3E-3	--	10
RVM047UP	--	Does not open	1E-3/D	--	3
RCK047UG	--	No output	3.3E-3	--	10
RLPIPASS	Passive valve faults LPCI Loop 1	Does not remain open	3E-4/D	--	3
RLR2PASS	Passive valve faults LPCI Loop 2	↓	3E-4/D	--	↓
RSD1PASS	Passive valve faults shutdown cooling Loop 1		2E-4/D	--	
RSD2PASS	Passive valve faults shutdown cooling Loop 2		2E-4/D	--	
RTC1PASS	Passive valve faults torus cooling Loop 1		1E-4/D	--	
RTC2PASS	Passive valve faults torus cooling Loop 2		1E-4/D	--	

B-86

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RRE005AN	Relay K5A	Does not close	1E-4/D	--	3
RRE005BN	Relay K5B			--	
RRE006AN	Relay K6A			--	
RRE006BN	Relay K6B			--	
RRE007AN	Relay K7A			--	
RRE007BN	Relay K7B			--	
RRE008AN	Relay K8A			--	
RRE008BN	Relay K8B			--	
RRE009AN	Relay K9A			--	
RRE009BN	Relay K9B			--	
RRE010AN	Relay K10A			--	
RRE010BN	Relay K10B			--	
RRE018AN	Relay K18A			--	
RRE018BN	Relay K18B			--	
RRE021AN	Relay K21A			--	

B-87

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RRE021BN	Relay K21B	Does not close	1E-4/D	--	3
RRE035AN	Relay K35A	↓	↓	--	↓
RRE035BN	Relay K35B			--	
RRE036AN	Relay K36A			--	
RRE036BN	Relay K36B			--	
RRE039AN	Relay K39A			--	
RRE039BN	Relay K39B			--	
RRE044AN	Relay K44A			--	
RRE044BN	Relay K44B			--	
RRE046AN	Relay K46A			--	
RRE046BN	Relay K46B			--	
RRE063A0	Relay K63A			Does not remain closed	
RRE063B0	Relay K63B	Does not remain closed	1E-7/hr	8	

B-88

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RRE067AN	Relay K67A	Does not close	1E-4/D	--	3
RRE067BN	Relay K67B	↓	↓	--	↓
RRE090AN	Relay K90A			--	
RRE090BN	Relay K90B			--	
RRE091AN	Relay K91A			--	
RRE091BN	Relay K91B			--	
RRE097AN	Relay K97A			--	
RRE097BN	Relay K97B			--	
RRE098AN	Relay K98A			--	
RRE098BN	Relay K98B			--	
RRE104AP	Relay K104A			Does not open	
RRE104BP	Relay K104B	↓	↓	--	↓
RRE104CP	Relay K104C			--	
RRE104DP	Relay K104D			--	

B-89

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RRE105AN	Relay K105A	Does not close	1E-4/D	--	3
RRE105BN	Relay K105B	↓	↓	--	↓
RRE105CN	Relay K105C			--	
RRE105DN	Relay K105D			--	
RRE108AN	Relay K108A			--	
RRE108BN	Relay K108B			--	
RRE112AN	Relay K112A			--	
RRE112BN	Relay K112B			--	
RRE113AN	Relay K113A			--	
RRE113BN	Relay K113B			--	
RRE117AN	Relay K117A			--	
RRE117BN	Relay K117B			--	
RRE118AN	Relay K118A			--	
RRE118BN	Relay K118B			--	

B-90

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ORE007AN	Relay 14A-K7A	Does not close	1E-4/D	--	3
ORE007BN	Relay 14A-K7B	↓	↓	--	↓
ORE008AN	Relay 14A-K8A			--	
ORE008BN	Relay 14A-K8B			--	
ORE040AN	Relay 14A-K40A			--	
ORE040BN	Relay 14A-K40B			--	
ORE041AN	Relay 14A-K41A			--	
ORE041BN	Relay 14A-K41B			--	
ORE042AN	Relay 14A-K42A			--	
ORE042BN	Relay 14A-K42B			--	
ORE043AN	Relay 14A-K43A			--	
ORE043BN	Relay 14A-K43B			--	
RPS0501J	Loop 1 minimum-flow bypass flow sensor	Test	1.5E-4	--	0
RPS0642J	Loop 2 minimum-flow bypass flow sensor	Test	1.5E-4	--	0

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
OPSLLV LX	Core spray reactor low level switches	Operator miscalibration	2.4E-6/D	--	3
OPSDWHPX	Core spray drywell high pressure switches	Operator miscalibration	2.9E-4/D	--	
OPS072AT	Core spray reactor low level Switch 072A	Does not operate	1E-4/D	--	
OPS072BT	Core spray reactor low level Switch 072B			--	
OPS079AT	Core spray reactor low level Switch 079A			--	
OPS079BT	Core spray reactor low level Switch 079B			--	
OPS152UT	Core spray reactor pressure Switch 152			--	
OPS252UT	Core spray reactor pressure Switch 252			--	
OPS352UT	Core spray reactor pressure Switch 352			--	
OPS452UT	Core spray reactor pressure Switch 452			--	

B-92

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
OPSI01AT	Core spray drywell pressure Switch 101A	Does not operate	1E-4/D	--	3
OPSI01BT	Core spray drywell pressure Switch 101B	↓	↓	--	↓
OPSI01CT	Core spray drywell pressure Switch 101C			--	
OPSI01DT	Core spray drywell pressure Switch 101D			--	
RPS052AT	RHR reactor low pressure Switch 052A			--	
RPS052BT	RHR reactor low pressure Switch 052B			--	
RPS052CT	RHR reactor low pressure Switch 052C			--	
RPS052DT	RHR reactor low pressure Switch 052D			--	
RPS0501T	RHR loop low flow Switch 050			--	
RPS0642T	RHR loop low flow Switch 064			--	

B-93

TABLE B-11. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RPS128AT	RHR reactor low pressure Switch 128A	Does not operate	1E-4/D	--	3
RPS128BT	RHR reactor low pressure Switch 128B	Does not operate	1E-4/D	--	3

B-94

TABLE B-12. RHR SYSTEM HOUSE EVENTS STATUS

Sequence Initiator	HOUSEDBA	HOUSEDBB	HOUSENVL	HOUSENVA	HOUSETRAN
L _S	Off	Off	Off	On	Off
L _D *	On/Off	Off/On	Off	On	Off
L _V	Off	Off	Off	On	Off
L _L *	On/Off	Off/On	Off	On	Off
L _V	Off	Off	Off	On	Off
S*	On/Off	Off/On	Off	On	Off
T _U	Off	Off	Off	On	On
T _P	Off	Off	On	Off	On
T _A	Off	Off	Off	Off	On
T _K	Off	Off	Off	Off	On
T _{pK}	Off	Off	On	Off	On

* For these initiators, when HOUSEDBA is "on" HOUSEDBB is "off," and vice versa. Some of the breaks associated with L_L and S have both HOUSEDBA and HOUSEDBB "off." See Appendix C, Section 1.4 for details of how sequence values were calculated.

the transfer appears in the tree (i.e., Figure B-7) for another system, then the transfer device shows a code and lists the figure number and part number where the transfer appears.

All valves and piping in the normal flow path for each mode of the RHR system that must change states (i.e., open or close) are included in the fault trees. Interfacing lines and valves for the different modes of RHR, such as the two possible suction paths and three possible discharge paths, are included where appropriate. For example, in the LPCI mode, the torus cooling valves and piping are excluded because the valves are normally closed, they receive a shut signal automatically if open, operator action to open the valve is blocked, and multiple valves must fail in order to divert flow from the desired path.

Success/Failure Criteria. Table B-7 summarizes the success criteria for each mode of RHR operation. A fault tree exists for each of these different success criteria. The letter designation in the fault tree corresponds to the event tree designations described previously.

The LPCI mode encompasses four different success criteria labeled G_A, G_B, G_C and G_D. The success criteria for these submodes of LPCI depend on factors such as break size, location, and success/failure of other systems.

Shutdown cooling mode (R_A) requires at least one pump and heat exchanger combination to circulate flow from the recirculation Loop A, through the heat exchanger, and back to the reactor via the LPCI discharge

valves. Torus cooling (R_B) requires two of four pumps and heat exchangers to circulate water from the torus through the heat exchanger and back to the torus.

Major Assumptions. The following major assumptions were used in constructing the RHR system fault tree:

1. There are numerous piping and valve interfaces with the RHR system that are not included on the fault trees. Drain and vent lines 1 inch or less in diameter are excluded. Connections to other systems such as the RHR flushing system where lines are greater than 1 inch in diameter, but where isolation is provided by normally locked-closed valves or by two or more normally closed valves, are also excluded.
2. Passive failures of normally open valves that are not required to change state are considered only if a single valve failure will cause loss of an entire RHR loop. Passive failures of active components are insignificant compared to the active failure rates. There are three valves in each loop that meet this criteria: the locked-open torus suction valves (HCV-74-83 and 88) and the LPCI discharge line valves (HCV-74-55 and 69 and FCV-74-52 and 66).
3. Failure of the minimum-flow bypass valves to close when required results in a flow diversion of approximately 10% of rated flow from the desired flow path. Therefore, this fault is considered to fail that particular loop even though some 90% of rated flow will not be diverted.
4. Since the time period during which the LPCI mode is used is very short (approximately 10 min) seal cooling and room cooling are not considered in these fault trees. For the shutdown cooling and torus cooling modes where the pumps will run for a long time (greater than 2 hours) these cooling faults are in the tree.
5. No credit is taken for operator backup of automatic initiation. The operator is included in the trees only where a specific procedure requires him to initiate a system and that system has no automatic initiation capability.
6. If a break occurs on a recirculation loop discharge side, the LPCI and shutdown cooling loop that discharge to that recirculation loop are assumed to fail due to flow diversion.

Basic Events. The information associated with the various basic events listed in the fault tree is summarized in the RHR fault summary short form, Table B-11. In addition, the failure data associated with these basic events is summarized in Table B-13. Dominant contributors to RHR unavailabilities are listed in Tables B-14 through B-21 for normal power conditions, and in Table 22 through 25 for loss of offsite power.

TABLE B-13. RHR SYSTEM FAILURE DATA SUMMARY

Component (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (A)	Remarks
Pump (PM)	Does not start (R)	--	--	--	1E-3/D	1E-3	From Table C-4
Pump (PM)	Does not run (S)	0	37	8	3E-5/hr	2.4E-4	From Table C-4
Control circuit (CK)	No output (G)	--	--	--	--	3.3E-3	Calculated from generic control circuit model
Pump (PM)	Maintenance (J)	--	--	--	--	7.6E-4	From Table B-10
Circuit breaker (CB)	Does not close (N)	--	--	--	1E-3/D	1E-3	From Table C-4
Check valve (VK)	Does not open (P)	--	--	--	1E-4/D	1E-4	From Table C-4
Motor-operated valve (VM)	Does not open (P)	--	--	--	1E-3/D	1E-3	From Table C-4
Motor-operated valve (VM)	Does not close (N)	--	--	--	1E-3/D	1E-3	From Table C-4
Piping (PP)	Rupture (F)	1	24	25	1E-10/hr/section	2.5E-9	$T_D = 1$ hr, assumed since keep-full should alarm by then to indicate a ruptured pipe
RHR mode initiation (RA, RB, RC)	Operator error (D)	--	--	--	--	1E-3	Estimated based on similar actions modeled in other systems
Initiation circuit (R42B45AJ, R42B45BJ)	Test (J)	--	--	--	--	9.1E-4	From Table B-9
Relay (RE)	Does not close (N)	--	--	--	1E-4/D	1E-4	From Table C-4; no distinction made between relay energizing and contacts closing
Relay (RE)	Does not remain closed (O)	0	7	7	1E-7/hr	7E-7	From Table C-4
Relay (RE)	Does not open (P)	--	--	--	1E-4/D	1E-4	From Table C-4; no distinction made between relay energizing and contacts opening

TABLE E-13. (continued)

Component (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (A)	Remarks
Flow sensor (PS) (minimum flow bypass valve)	Test	--	--	--	--	1.5E-4	From Table B-9
Level switch (PS)	Does not operate (T)	--	--	--	1E-4/D	1E-4	From Table C-4
Pressure switch (PS)	Does not operate (T)	--	--	--	1E-4/D	1E-4	From Table C-4
Normally open valves (R _____ PAS)	Does not remain open	--	--	--	1E-4/D	3E-4 2E-4 1E-4	Three valves/loop for LPCI Two valves/loop for shutdown cooling One valve/loop for torus cooling
Core spray level switches (OPSLVLX)	Operator miscalibrates (X)	--	--	--	--	2.4E-6	See Section 4
Core spray drywell pressure switches (OPSDWHPX)	Operator miscalibrates (X)	--	--	--	--	2.9E-4	See Section 4

a. If $T_D = 0$, then $T = T_R$ if mission time (8 hr) $> T_R$. If $T_D = 0$, then $T =$ mission time (8 hr) if mission time $\leq T_R$.

TABLE B-14. RHR SYSTEM CUT SETS
(G_A)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
1.1E-5	1.7	RCK001AG, RCK001BG	No
1.1E-5	1.7	RCK0531G, RCK001BG	No
1.1E-5	1.7	RCK0531G, RCK0302G	No
1.1E-5	1.7	RCK0071G, RCK001BG	No
1.1E-5	1.7	RCK001AG, RCK0672G	No
1.1E-5	1.7	RCK001AG, RCK0302G	No
1.1E-5	1.7	RCK0071G, RCK0302G	No
1.1E-5	1.7	RCK0071G, RCK0672G	No
1.1E-5	1.7	RCK001AG, RCK001DG	No
1.1E-5	1.7	RCK0071G, RCK001DG	No
1.1E-5	1.7	RCK0531G, RCK0672G	No
1.1E-5	1.7	RCK0531G, RCK001DG	No
1.1E-5	1.7	RCK001CG, RCK0672G	No
1.1E-5	1.7	RCK001CG, RCK0302G	No
1.1E-5	1.7	RCK001CG, RCK001BG	No
1.1E-5	1.7	RCK001CG, RCK001DG	No
3.3E-6	0.5	RVM0071N, RCK0672G	No
3.3E-6	0.5	RPM001CR, RCK0672G	No
3.3E-6	0.5	RVM0531P, RCK0302G	No
3.3E-6	0.5	RPM001CR, RCK001DG	No
3.3E-6	0.5	RVM0071N, RCK001BG	No
3.3E-6	0.5	RCK0531G, RVM0302N	No
3.3E-6	0.5	RCK0071G, RVM0672P	No
3.3E-6	0.5	RCK001CG, RVM0302N	No
3.3E-6	0.5	RVM0071N, RCK0302G	No
3.3E-6	0.5	RCK0071G, RPM001BR	No
3.3E-6	0.5	RPM001CG, RCK0302G	No
3.3E-6	0.5	RCB001AN, RCK001DG	No
3.3E-6	0.5	RPM001AR, RCK0672G	No
3.3E-6	0.5	RCB001CN, RCK0302G	No
Cumulative importance	34.2		

TABLE B-15. RHR SYSTEM CUT SETS
(G_B)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
3.3E-3	15.9	RCK0672G	No
3.3E-3	15.9	RCK0302G	No
3.3E-3	15.9	RCK0531G	No
3.3E-3	15.9	RCK0071G	No
1.0E-3	4.7	RVM0302N	No
1.0E-3	4.7	RVM0531P	No
1.0E-3	4.7	RVM0071N	No
1.0E-3	4.7	RVM0672P	No
9.1E-4	4.3	R42B45AJ	No
9.1E-4	4.3	R42B45BJ	No
Cumulative importance	91.0		

TABLE B-16. RHR SYSTEM CUT SETS
(G_C)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
3.3E-3	6.5	RCK0071G	No
3.3E-3	6.5	RCK001DG	No
3.3E-3	6.5	RCK0672G	No
3.3E-3	6.5	RCK001AG	No
3.3E-3	6.5	RCK0531G	No
3.3E-3	6.5	RCK0302G	No
3.3E-3	6.5	RCK001CG	No
3.3E-3	6.5	RCK001BG	No
1.0E-3	1.9	RPM001BR	No
1.0E-3	1.9	RVM0672P	No
1.0E-3	1.9	RPM001AR	No
1.0E-3	1.9	RPM001CR	No
1.0E-3	1.9	RCB001DN	No
1.0E-3	1.9	RVM0071N	No
1.0E-3	1.9	RPM001DR	No
1.0E-3	1.9	RCM001AN	No
1.0E-3	1.9	RCM001CN	No
1.0E-3	1.9	RVM0531P	No
1.0E-3	1.9	RCB001BN	No
1.0E-3	1.9	RVM0302N	No
9.1E-4	1.8	R42B45AJ	No
9.1E-4	1.8	R42B45BJ	No
7.6E-4	1.5	RPM001AJ	No
7.6E-4	1.5	RPM001BJ	No
7.6E-4	1.5	RPM001CJ	No
7.6E-4	1.5	RPM001DJ	No
Cumulative importance	84.4		

TABLE B-17. RHR SYSTEM CUT SETS
(G_D)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
1.1E-5	10.3	RCK0531G,RCK0672G	No
1.1E-5	10.3	RCK0071G,RCK0302G	No
1.1E-5	10.3	RCK0071G,RCK0672G	No
1.1E-5	10.3	RCK0531G,RCK0302G	No
3.3E-6	3.1	RVM0071N,RCK0672G	No
3.3E-6	3.1	RVM0531P,RCK0302G	No
3.3E-6	3.1	RCK0071G,RVM0302G	No
3.3E-6	3.1	RCK0531G,RVM0302G	No
3.3E-6	3.1	RCK0531G,RVM0672P	No
3.3E-6	3.1	RCK0071G,RVM0672P	No
3.3E-6	3.1	RVM0071N,RCK0302G	No
3.3E-6	3.1	RVM0531P,RCK0672G	No
3.1E-6	2.8	R42B45AJ,RCK0672G	No
3.1E-6	2.8	R42B45AJ,RCK0302G	No
3.1E-6	2.8	RCK0531G,R42B45BJ	No
3.1E-6	2.8	RCK0071G,R42B45BJ	No
1.5E-6	1.4	RCK0071G,RG4B22	No
1.5E-6	1.4	RG4A22* ,RCK0672G	No
1.5E-6	1.4	RG4A22* ,RCK0302G	No
1.5E-6	1.4	RCK0531G,RG4B22*	Yes
1.0E-6	0.9	RCK0531G,RGB222*	Yes
1.0E-6	0.9	RCK0071G,RGB222*	Yes
1.0E-6	0.9	RGB122* ,RCK0672G	Yes
1.0E-6	0.9	RGB122* ,RCK0302G	Yes
1.0E-6	0.9	RVM0531P,RVM0672P	No
1.0E-6	0.9	RVM0071N,RVM0302N	No
1.0E-6	0.9	RVM0071G,RVM0672P	No
1.0E-6	0.9	RVM0531P,RVM0302N	No
Cumulative importance	90.0		

* RG4A22, RG4B22, RGB122, RGB222--notation for initiation signal faults.

TABLE B-18. RHR SYSTEM CUT SETS
(G_D with Break on Loop 2)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
3.3E-3	31.8	RCK0531G	No
3.3E-3	31.8	RCK0071G	No
1.0E-3	9.5	RVM0531P	No
1.0E-3	9.5	RVM0071N	No
9.1E-4	<u>8.6</u>	R42B45AJ	No
Cumulative importance	91.2		

TABLE B-19. RHR SYSTEM CUT SETS
(R_A for Loop 1)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
4.7E-3	14.9	RR3A112*	Yes
4.7E-3	14.9	RR3A122*	Yes
3.3E-3	10.7	RCK0531G	Yes
3.3E-3	10.7	RCK048UG	Yes
3.3E-3	10.7	RCK0071G	Yes
3.3E-3	10.7	RCK047UG	Yes
1.0E-3	3.2	RVM0531G	No
1.0E-3	3.2	RVM048UP	No
1.0E-3	3.2	RVM0071N	No
1.0E-3	3.2	RVM0471N	No
1.0E-3	3.2	RRA0001D	Yes
9.1E-4	<u>2.9</u>	R42B45AJ	No
Cumulative importance	91.5		

* RR3A112, RR3A122--notation for isolation signal faults.

TABLE B-20. RHR SYSTEM CUT SETS
(R_A for Loop 2)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
4.7E-3	14.9	RR3A112*	Yes
4.7E-3	14.9	RR3A122*	Yes
3.3E-3	10.7	RCK0672G	Yes
3.3E-3	10.7	RCK0302G	Yes
3.3E-3	10.7	RCK048UG	Yes
3.3E-3	10.7	RCK047UG	Yes
1.0E-3	3.2	RVM048UG	No
1.0E-3	3.2	RVM047UP	No
1.0E-3	3.2	RVM0302G	No
1.0E-3	3.2	RVM0672P	No
1.0E-3	3.2	RRA0001D	Yes
9.1E-4	2.9	R42B45BJ	No
Cumulative importance	91.5		

* RR3A112, RR3A122--notation for isolation signal faults.

TABLE B-21. RHR SYSTEM CUT SETS
(R_B)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets*</u>	<u>Potentially Recoverable</u>
1.0E-3	32.3	RRB0001D	Yes
6.7E-5	2.2	SUPRA,RCK0302G	Yes
6.7E-5	2.2	SUPRA,RCK0712G	Yes
6.7E-5	2.2	RCK0571G,SUPRB	Yes
6.7E-5	2.2	SUPRC,RCK0712G	Yes
6.7E-5	2.2	RCK0517G,SUPRD	Yes
6.7E-5	2.2	SUPRC,RCK0302G	Yes
6.7E-5	2.2	RCK0071G,SUPRB	Yes
6.7E-5	2.2	RCK0071G,SUPRD	Yes
2.0E-5	0.6	RVM0071N,SUPRD	Yes
2.0E-5	0.6	SUPRA,RVM0302N	Yes
2.0E-5	0.6	SUPRC,RVM0712P	Yes
2.0E-5	0.6	RVM0571P,SUPRB	Yes
2.0E-5	0.6	RVM0571P,SUPRD	Yes
2.0E-5	0.6	SUPRC,RVM0302N	Yes
2.0E-5	0.6	SUPRA,RVM0712P	Yes
2.0E-5	0.6	RVM0071N,SUPRB	Yes
1.8E-5	0.6	SUPRA,R42B45BJ	Yes
1.8E-5	0.6	SUPRC,R42B45BJ	Yes
1.8E-5	0.6	R42B45AJ,SUPRB	Yes
1.8E-5	0.6	R42B45AJ,SUPRD	Yes
Cumulative importance	57.1		

* SUPRA, SUPRB, SUPRC, SUPRD--notation for RHRSW interface faults.

TABLE B-22. RHR SYSTEM CUT SETS
(G_D with LOSP)

Unavailability	Importance (%)	Cut Sets*	Potentially Recoverable
1.1E-5	4.1	RCK0672G,RCK0071G	No
1.1E-5	4.1	RCK0531G,RCK0672G	No
1.1E-5	4.1	RCK0531G,RCK0302G	No
1.1E-5	4.1	RCK0071G,RCK0302G	No
1.1E-5	4.1	RCK0302G,SUPSDA,SUPSDB	No
1.1E-5	4.1	RCK0071G,SUPSDC,SUPSDD	No
1.1E-5	4.1	RCK0672G,SUPSDA,SUPSDB	No
1.1E-5	4.1	RCK0531G,SUPSDC,SUPSDD	No
1.1E-5	4.1	SUPSDA,SUPSDC,SUPSDB,SUPSDD	No
3.3E-6	1.2	RVM0531P,RCK0302G	No
3.3E-6	1.2	RVM0672P,RCK0071G	No
3.3E-6	1.2	RCK0071G,RVM0302N	No
3.3E-6	1.2	RCK0531G,RVM0302N	No
3.3E-6	1.2	RCK0531G,RVM0672P	No
3.3E-6	1.2	RVM0071N,RCK0302G	No
3.3E-6	1.2	RCK0672G,RVM0071N	No
Cumulative importance	45.3		

* SUPSDA, SUPSDB, SUPSDC, SUPSDD--notation for the 4160 V shutdown board faults.

TABLE B-23. RHR SYSTEM CUT SETS
(R_A Loop 1 with LOSP)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets*</u>	<u>Potentially Recoverable</u>
4.8E-3	12.2	RR3A122	Yes
4.8E-3	12.2	RR3A112	Yes
3.3E-3	8.5	RCK0531G	Yes
3.3E-3	8.5	RCK0071G	Yes
3.3E-3	8.5	RCK047UG	Yes
3.3E-3	8.5	RCK048UG	Yes
1.2E-3	2.9	SUPSDA, SUPSDB	Yes
1.2E-3	2.9	SUPRA, SUPSDB	Yes
1.2E-3	2.9	SUPSDA, SUPRC	Yes
1.0E-3	2.5	RVM0531P	No
1.0E-3	2.5	RVM0071N	No
1.0E-3	2.5	RVM047UP	No
1.0E-3	2.5	RVM048UP	No
1.0E-3	2.5	RRA001AD	Yes
9.1E-4	2.3	R42B45AJ	Yes
5.3E-4	1.3	RG4A22	Yes
Cumulative importance	83.2		

* SUPSDA, SUPSDB--notation for the 4160 V shutdown board faults; RR3A112, RR3A122--notation for isolation signal faults; RG4A22--notation for initiation signal faults; SUPRA, SUPRC--notation for RHRSW interface faults.

TABLE B-24. RHR SYSTEM CUT SETS
(RA Loop 2 with LOSP)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets*</u>	<u>Potentially Recoverable</u>
4.8E-3	12.2	RR3A122	Yes
4.8E-3	12.2	RR3A112	Yes
3.3E-3	8.5	RCK0672G	Yes
3.3E-3	8.5	RCK0302G	Yes
3.3E-3	8.5	RCK047UG	Yes
3.3E-3	8.5	RCK048UG	Yes
1.2E-3	2.9	SUPSDC, SUPSDD	Yes
1.2E-3	2.9	SUPRB, SUPSDD	Yes
1.2E-3	2.9	SUPSDC, SUPRD	Yes
1.0E-3	2.5	RVM0672P	No
1.0E-3	2.5	RVM0302N	No
1.0E-3	2.5	RVM047UP	No
1.0E-3	2.5	RVM048UP	No
1.0E-3	2.5	RRA001AD	Yes
9.1E-4	2.3	R42B45BJ	Yes
5.3E-4	1.3	RG4B22	Yes
Cumulative importance	83.2		

* SUPSDC, SUPSDD--notation for the 4160 V shutdown board faults; RR3A122, RR3A112--notation for isolation signal faults; RG4B22--notation for initiation signal faults; SUPRB, SUPRD--notation for RHRSW interface faults.

TABLE B-25. RHR SYSTEM CUT SETS
(R_B with LOSP)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets*</u>	<u>Potentially Recoverable</u>
1.0E-3	13.9	RRB0001D	Yes
1.9E-4	2.6	RCK0571G, SUPSDD	Yes
1.9E-4	2.6	RCK0071G, SUPSDC	Yes
1.9E-4	2.6	RCK0571G, SUPSDC	Yes
1.9E-4	2.6	RCK0302G, SUPSDA	Yes
1.9E-4	2.6	RCK0302G, SUPSDB	Yes
1.9E-4	2.6	RCK0712G, SUPSDA	Yes
1.9E-4	2.6	RCK0712G, SUPSDB	Yes
1.9E-4	2.6	RCK0071G, SUPSDD	Yes
1.9E-4	2.6	SUPSDA , SUPSDB, SUPSDC	Yes
1.9E-4	2.6	SUPSDA , SUPSDC, SUPSDD	Yes
1.9E-4	2.6	SUPSDB , SUPSDC, SUPSDD	Yes
1.9E-4	2.6	SUPSDA , SUPSDB, SUPSDD	Yes
6.7E-5	0.9	RCK0302G, SUPRC	Yes
6.7E-5	0.9	RCK0712G, SUPRA	Yes
6.7E-5	0.9	RCK0712G, SUPRC	Yes
6.7E-5	0.9	RCK0071G, SUPRD	Yes
6.7E-5	0.9	RCK0571G, SUPRB	Yes
6.7E-5	0.9	RCK0071G, SUPRB	Yes
6.7E-5	0.9	RCK0571G, SUPRD	Yes
6.7E-5	0.9	RCK0302G, SUPRA	Yes
Cumulative importance	52.3		

* SUPSDA, SUPSDB, SUPSDC, SUPSDD--notation for the 4160 V shutdown board faults; SUPRA, SUPRB, SUPRC, SUPRD--notation for RHRSW interface faults.

2.3 High Pressure Coolant Injection (HPCI) System

Certain LOCAs will not depressurize the reactor vessel rapidly enough to allow successful reflooding of the vessel with the LPCI systems. Therefore, an HPCI system is necessary. In addition, there are times when the reactor vessel may be isolated and pressurized at or near operating pressure. Decay and residual heat will continue to generate steam in the vessel. Consequently, vessel water level will decrease as the water evolves into steam. In this case, some high-pressure source of makeup water must be provided. Both of these functions can be accomplished by the HPCI system.

2.3.1 Purpose

The HPCI system is one of the emergency core cooling systems at BFl.

The primary purpose of the HPCI system is to provide a supply of cooling water to reflood the reactor core in the event of a LOCA that does not result in rapid depressurization of the reactor vessel. The HPCI system is designed to provide this function, unassisted, for all liquid breaks less than 0.12 ft² in area, or approximately 5 inches in diameter; or all steam breaks that are less than 1.4 ft² in area, or approximately 16 inches in diameter.

The HPCI system can also be used to provide makeup water to the reactor during periods when the reactor is at or near normal operating pressure and is isolated from normal makeup sources.

2.3.2 System Configuration

Overall Configuration. The HPCI system consists of a steam turbine assembly that drives a constant-flow pump and includes the associated piping, valves, controls, and instrumentation. Figure B-8 is a simplified diagram of the system.

The HPCI turbine is driven by steam that is generated in the reactor vessel. The steam is extracted from main steam Line B upstream of the main steam isolation valves. The turbine exhaust is directed to the suppression pool. Rupture disks in the turbine exhaust line provide turbine protection should turbine exhaust line blockage occur.

The turbine-driven pump, which actually consists of a main pump and booster pump driven by the HPCI turbine through a speed reducer, is provided with two sources of water for injection into the reactor vessel. Initially, demineralized water from the CST is used instead of injecting the less desirable water from the suppression pool into the reactor. This provides reactor grade water to the reactor vessel for the case where the need for HPCI is rapidly satisfied. After the water in the CST is depleted, the tank's low level signal will automatically shift suction to the suppression pool. Water from either source is pumped into the reactor vessel via feed water Line A.

To prevent HPCI pump overheating during periods of reduced system flow, a minimum-flow bypass line is provided. This line routes a small volume of water from the pump discharge path to the suppression pool. Flow is controlled by the minimum-flow bypass valve (FCV-73-30).

Another line in the HPCI pump discharge path is used for full-flow operational testing of the HPCI system while the plant is operating. A 4-inch orifice in this line provides a discharge head to simulate reactor pressure. If, during testing, an HPCI initiation signal is received, the two test line isolation valves (FCV-73-35 and 36) will automatically shut. These valves will also shut if either of the suppression pool suction valves (FCV-73-26 and 27) is opened.

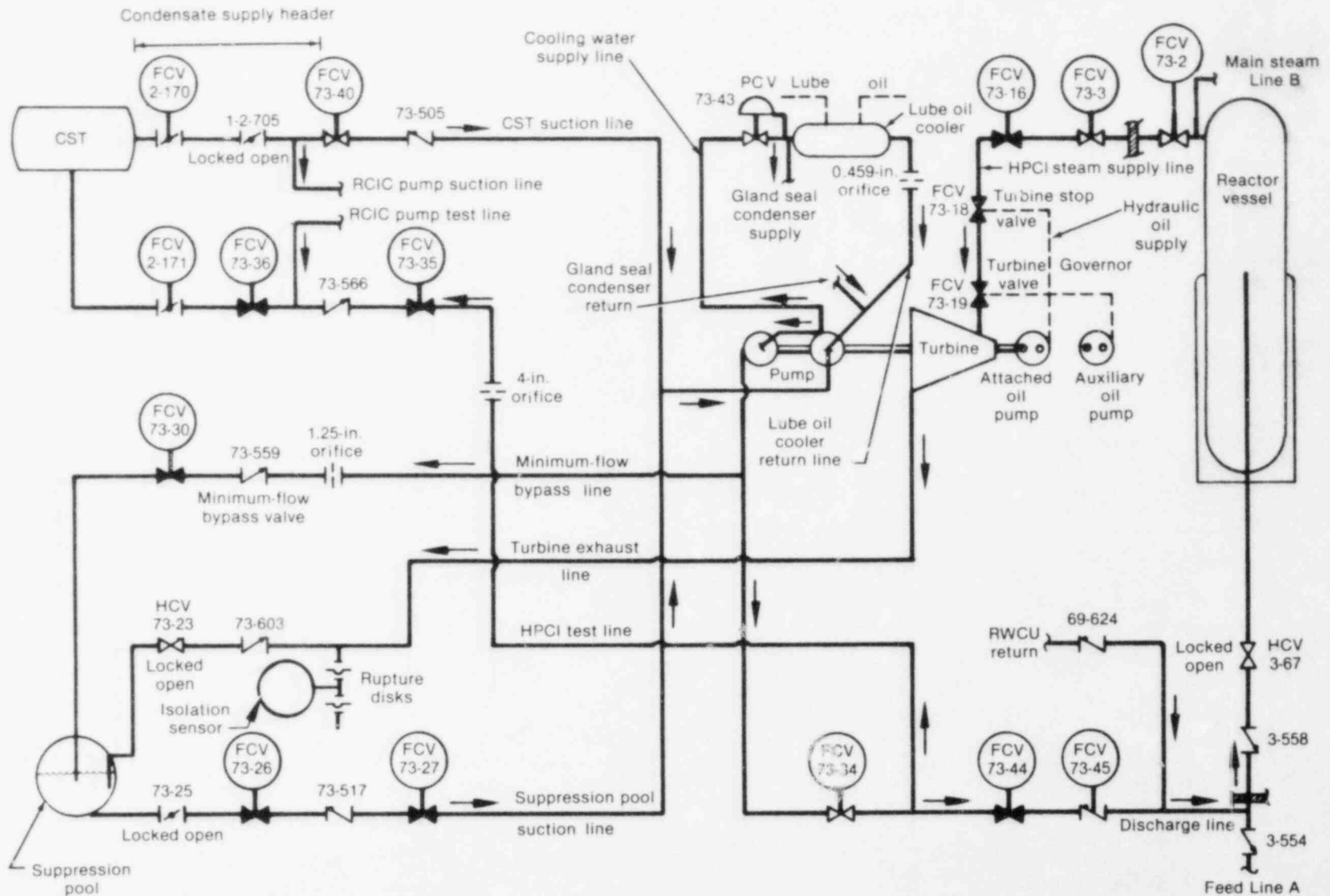


Figure B-8. HPCI system.

B-111

Some of the booster pump discharge flow is directed through a pressure regulator (CV-73-43) and is used as cooling water for the HPCI pump lubrication system lube oil cooler. In addition, this flow is directed to the HPCI system gland seal condenser and used to condense turbine gland seal leakoff and valve stem sealing steam. Heat from the HPCI turbine and pump lubricating oil is transferred to the cooling water and the water is directed to the suction side of the booster pump via a common cooling water return line. Here the water is mixed with the water flowing into the booster pump from the CST or suppression pool. The HPCI turbine and pump lubricating oil flows through the shell side of the lube oil cooler and provides lubrication to the turbine and pump components. Oil flow is accomplished by the DC motor-driven auxiliary oil pump or the attached lube oil pump.

The DC motor-driven auxiliary oil pump is required for initial operation of the turbine lubrication and hydraulic systems during turbine startup and provides a backup for the attached lube oil pump should the attached lube oil pump malfunction during turbine operation. The attached lube oil pump is designed to meet total oil requirements of the lubrication and hydraulic systems over the normal operating speed range (2000 to 4000 rpm).

The HPCI system gland seal condenser collects steam leakage from turbine gland seals, turbine control and stop valve stems, and turbine exhaust drainage. Coolant flow from the HPCI booster pump sprays into the condenser and aids in condensing the steam. A DC-powered gland seal condenser condensate pump maintains level in the gland seal condenser hotwell. Condensate is pumped from the hotwell to the suction side of the booster pump via the common cooling water return line. A DC-powered gland seal condenser gland exhauster removes noncondensables from the gland seal condenser via the standby gas treatment system. Startup of the condenser equipment is automatic, but condenser equipment failure does not prevent the HPCI system from fulfilling its core cooling objective.

The HPCI system controls automatically start the HPCI system and bring it to the design flow rate of 5000 gpm within 25 sec after receipt of a reactor vessel low-low water level signal or a primary containment (drywell) high pressure signal. The system is designed to deliver the design flow rate to the core at reactor vessel pressures ranging from 1120 to 150 psig. The HPCI system automatically stops when a high water level in the reactor is signaled, when steam supply pressure drops below 100 psig, or when other system parameters generate a trip signal.

HPCI system operation is designed to be completely independent of AC power although some HPCI components interface with AC power systems. Only DC power from the plant batteries and steam extracted from the reactor vessel are necessary for startup and operation of the system.

Support System Interfaces FMEA. The HPCI system components interface with various AC and DC electrical systems, the control air system, and the EAC system. HPCI pump lubrication and control system components are integral to the HPCI system. Component/supporting system interactions are given in Table B-26.

Instrumentation and Control. HPCI system initiation, trip, and isolation are automatically controlled by various plant and system parameters.

TABLE B-26. HPCI SYSTEM FMEA OF COMPONENT/SUPPORTING-SYSTEM INTERACTIONS

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
FCV-73-2	480 V AC RMOV-1A	Terminal 17E	No power to board; breaker open	No motive power to valve operator; valve remains in position	FCV-73-2 is a normally open containment isolation valve in the steam supply line to the turbine
	250 V DC RMOV Board-1A	Relays: 23A-K12 23A-K27	No signal from control logic	Valve remains in position unless manually activated	Because valve is normally open, it has auto-close capability; protective functions energize these relays to close the valve
	250 V DC RMOV Board-1B	Relay 23A-K37	--	--	--
FCV-73-3	250 V DC RMOV-1A	Terminal 11D2	No power to board; breaker open	No motive power to valve operator; valve remains in position	FCV-73-3 is a normally open containment isolation valve in series with FCV-73-2
	250 V DC RMOV Board-1A	Relays: 23A-K12 23A-K27	No signal from control logic	Valve remains in position unless manually activated	Because valve is normally open, it has auto-close capability; protective functions energize these relays to close the valve
	250 V DC RMOV Board-1B	Relay 23A-K37	--	--	--
LCV-73-5	Control air system	--	No air supply	Valve will not open	LCV-73-5 is a solenoid operated, air-actuated valve that opens on high level in the steam line condensate pot; if there is sufficient condensate in the steam line, failure of the steam line high pressure drain trap and coincident failure of LCV-73-5 to open, combined with operator failure to recognize associated valve position indication and alarms, may result in turbine damage
	250 V DC RMOV Board-1A	LS-73-5	No signal from LS-73-5	LCV-73-5 will not open; LS-73-5 is the high-level switch to automatically activate LCV-73-5	
FCV-73-16	250 V DC RMOV-1A	Terminal 3D	No power to board; breaker open	Valve remains closed; no steam to turbine; HPCI unavailable	FCV-73-16 is a normally closed valve in the steam supply line to the turbine
	250 V DC RMOV Board-1A	Relays: 23A-K1--low reactor level pressure 23A-K3--high drywell pressure	No signal from control logic	Valve will not open automatically	--
FCV-73-26	250 V DC RMOV-1A	Terminal 4D	No power to board; breaker open	Valve remains closed; isolation of suction flow path from torus to pump	FCV-73-26 is a normally closed valve in the HPCI pump suction line; the preferred source of water is the condensate storage tank

TABLE B-26. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
FCV-73-26 (continued)	250 V DC RMOV Board-1A	Relays to open valve: 23A-K15, 23A-K25	No signal from control logic	Valve will not automatically change position	System unavailable if condensate storage tank is empty; manual operation is possible
		Relays to close valve: 23A-K13, 23A-K28	--	--	--
FCV-73-27	250 V DC RMOV-1A	Terminal 9D	No power to board; breaker open	Valve will remain closed; isolation of suction flow path from torus to pump	FCV-73-27 is a normally closed valve in series with FCV-73-26
	250 V DC RMOV Board-1A	-----	-----	-Same relays and failure effects as FCV-73-26-	-----
FCV-73-30	250 V DC RMOV-1A	Terminal 8D	No power to board; breaker open	--	FCV-73-30 is the flow control valve in the minimum-flow bypass line
	250 V DC RMOV Board-1A	Relays to open valve: 23A-K24, 27A-K16	No signal from control logic	Valve remains in position unless manually activated	Condensate storage tank drains to suppression pool if valve remains open; suction is from CST and HPCI system trips
		Relay to close valve: 23A-K14	--	--	--
FCV-73-34	250 V DC RMOV-1A	Terminal 5A	No power to board; breaker open	Valve will remain in position	FCV-73-34 is a normally open valve in the pump discharge line to the reactor vessel; it is in series with FCV-73-44, which is normally closed
	250 V DC RMOV Board-1A	Relays: 23A-K2--reactor low level 23A-K4--high drywell pressure 23A-K43	No signal from control logic	Valve will not automatically change position; however, the normal position of the valve is its required operational position (i.e., open)	Valve receives a signal to open even though it is normally open
FCV-73-35	250 V DC RMOV-1A	Terminal 6A	No power to board; breaker open	Valve remains in position	FCV-73-35 is a normally closed valve in the 10-in. HPCI full-flow test line to the condensate storage tank; FCV-73-36 is a redundant valve in series; both valves must be inadvertently open to interfere with HPCI operation; failure of these valves to close could result in insufficient HPCI injection flow to the reactor vessel or contamination of the CST with suppression pool water

B-114

TABLE B-26. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
FCV-73-35 (continued)	250 V DC RMOV Board-1A	Relays: 23A-K1 23A-K2 23A-K4 23A-K21 23A-K22 23A-K43	No signal from control logic	Valve will not automatically activate to close as required	Manual operation is possible
FCV-73-36	250 V DC RMOV-1B	Terminal 4A	-----Same failure effects as FCV-73-35-----		
	250 V DC RMOV Boards		-----Same relays and failure effects as FCV-73-35-----		
FCV-73-40	250 V DC RMOV-1A	Terminal 1D2	No power to board; breaker open	Valve remains in position	FCV-73-40 is a normally open isolation valve in the pump suction line from the condensate storage tank; failure to change position could cause HPCI unavailability due to loss of suction when the CST is empty
	250 V DC RMOV Board-1A	Relays: 23A-K1--open valve 23A-K3--open valve 23A-K21--close valve 23A-K22--close valve	No signal from control logic	Valve will not automatically change position	Manual operation is possible
FCV-73-44	250 V DC RMOV-1A	Terminal 7A	No power to board; breaker open	Valve will remain closed; isolation of flow path from pump to reactor vessel	FCV-73-44 is a normally closed valve that isolates HPCI from the reactor vessel
				Failure of valve to reclose upon opening is not a serious failure because of redundant check valves and isolation valves in the line	
	250 V DC RMOV Board-1A	Relays: 23A-K1--reactor low level 23A-K3--high drywell pressure	No signal from control logic	Valve will not automatically open	Manual operation is possible
FCV-73-45	120 V AC I&C Bus A Control air system	Remote test switch and local test switch	No power to board; blown fuse	Valve will operate normally regardless of switch position, power availability, or control air pressure	FCV-73-45 is a testable check valve in the HPCI pump discharge line to the reactor vessel

TABLE B-26. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
Auxiliary oil pump	250 V DC RMOV-1A	Terminal 4A	No power to board; breaker open	Oil pump not operable; turbine inlet valves will not open; HPCI unavailable	The auxiliary oil pump provides hydraulic force to the turbine stop valve and turbine governor valve during startup of the turbine
	250 V DC RMOV Board-1A	Relay 23A-K24X	No signal from control logic	Pump will not automatically start	Can be started manually regardless of control logic signal if FCV-73-16 is open
Gland seal condensate pump	250 V DC RMOV-1A	Terminal 9B2	No power to board; breaker open	Gland seal condensate pump is inoperable	HPCI is functional with this pump inoperable
	250 V DC RMOV Board-1A	Relays: 23A-K19--start 23A-K10--stop	No signal from control logic	Pump will not auto-start or auto-stop	--
Gland seal exhauster	250 V DC RMOV-1A	Terminal 8B2	No power to board; breaker open	Gland seal exhauster is inoperable	HPCI is functional with this component inoperable
	250 V DC RMOV Board-1A	Relay 23A-K24	No signal from control logic	Exhauster will not auto-start	--
Turbine	Equipment area cooling	RHR Room A and C fan coolers	No heat removal by EECW	Turbine room will heat until turbine isolates at 194°F	Turbine can operate for a minimum of 8 hours without EAC when the suppression pool is the source of water for the system (worst case)
			No forced convection by HVAC	Design conditions for oil coolers are exceeded	--
Division II control logic	250 V DC RMOV-1A	--	No power to board; breaker open	Division II logic inoperable	LS-73-5 is the high level limit switch to auto- matically activate LCV-73-5
Division I control logic	250 V DC RMOV-1B	--	No power to board; breaker open	Division I logic inoperable	HPCI inoperable Initiation logic changes from one-out-of-two- twice to two-of-two for both drywell pressure and reactor vessel level signals

System Initiation--The HPCI system will automatically start and inject water into the reactor vessel when either of two signals are present. These signals are:

1. High drywell pressure (2 psig).
2. Low reactor vessel water level (476.5 inches above vessel zero).

Four pressure switches are used to sense drywell pressure. Relays associated with these switches are arranged in one-out-of-two-twice logic for the HPCI initiation signal.

Four level switches are used to sense reactor vessel level. In a similar arrangement, the relays associated with these switches are arranged in one-out-of-two-twice logic for HPCI initiation. Figure B-9 is a simplified diagram of the HPCI system initiation circuitry.

When the HPCI initiation signal is received, the HPCI steam supply valve (FCV-73-16) opens, the HPCI pump discharge valve (FCV-73-44) opens, and the minimum-flow bypass valve (FCV-73-30) opens. In addition, the auxiliary oil pump starts and causes the turbine stop valve (FCV-73-18) and the turbine governor valve (FCV-73-19) to open. Figure B-10 is a simplified diagram of the auxiliary oil pump starting circuit. These component responses will result in water being pumped from the CST to the reactor vessel via feed Line A.

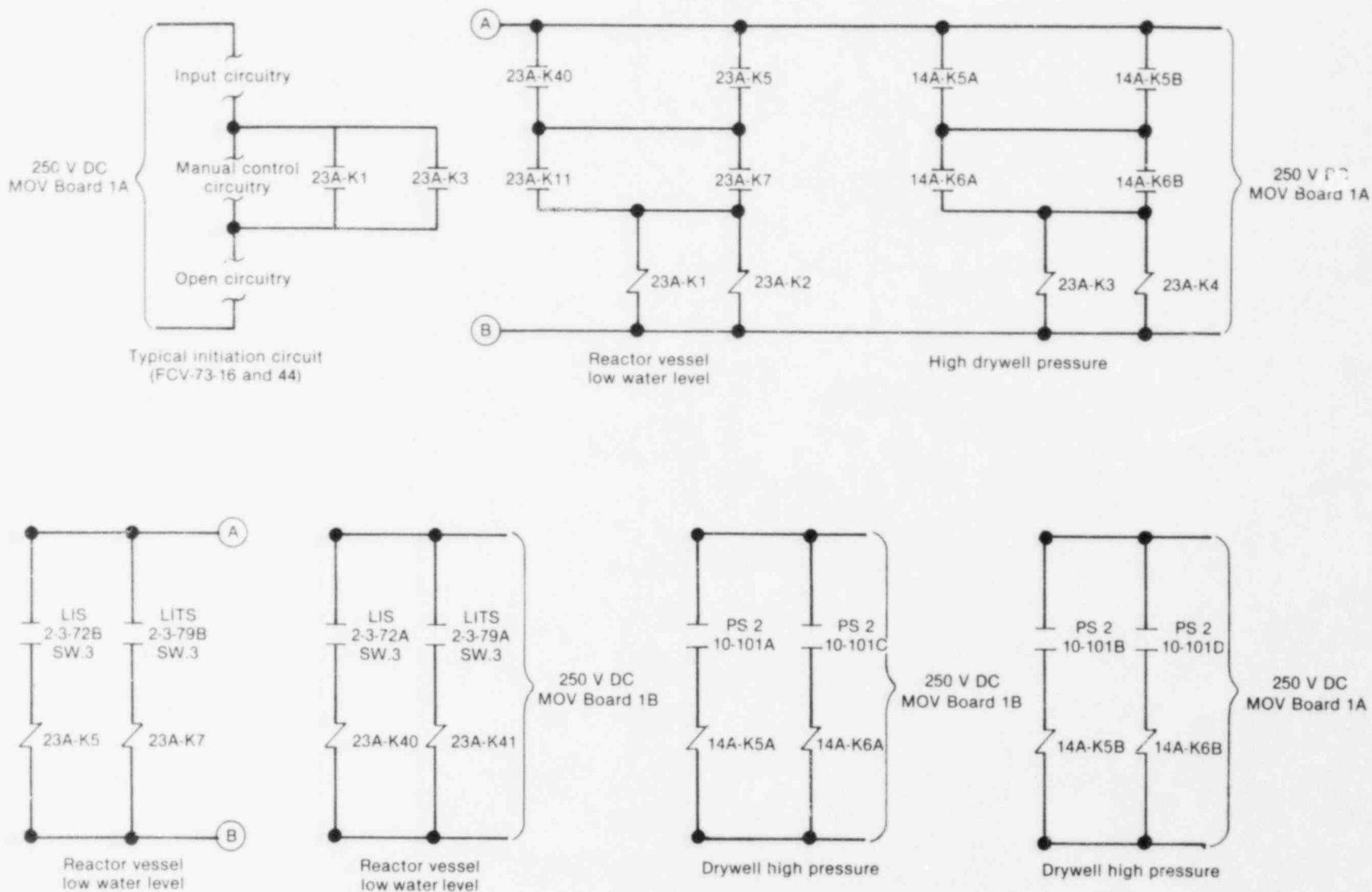
In addition, the initiation signal will cause the CST suction header isolation valve (FCV-73-40) to open if it is closed, unless the two suppression pool suction valves (FCV-73-26 and 27) are already open. The signal will close the two test line isolation valves (FCV-73-35 and 36) if they are open. The normally open discharge line isolation valve (FCV-73-34) will also open if it is closed.

The auxiliary oil pump will shut down when turbine speed reaches 1800 rpm. At this speed the attached oil pump output will meet the requirements of the turbine hydraulic and lubrication systems.

When system flow reaches 1200 gpm the minimum-flow bypass valve (FCV-73-30) will close.

Turbine Trip--Any of the following conditions will cause the HPCI turbine to trip:

1. High reactor vessel water level (582 inches above vessel zero).
2. High turbine exhaust pressure (150 psig).
3. Low booster pump suction pressure (15 inches Hg vacuum).
4. Turbine mechanical overspeed (5000 rpm).
5. Any HPCI isolation signal.



INEL 2 1480

Figure B-9. HPCI initiation circuitry.

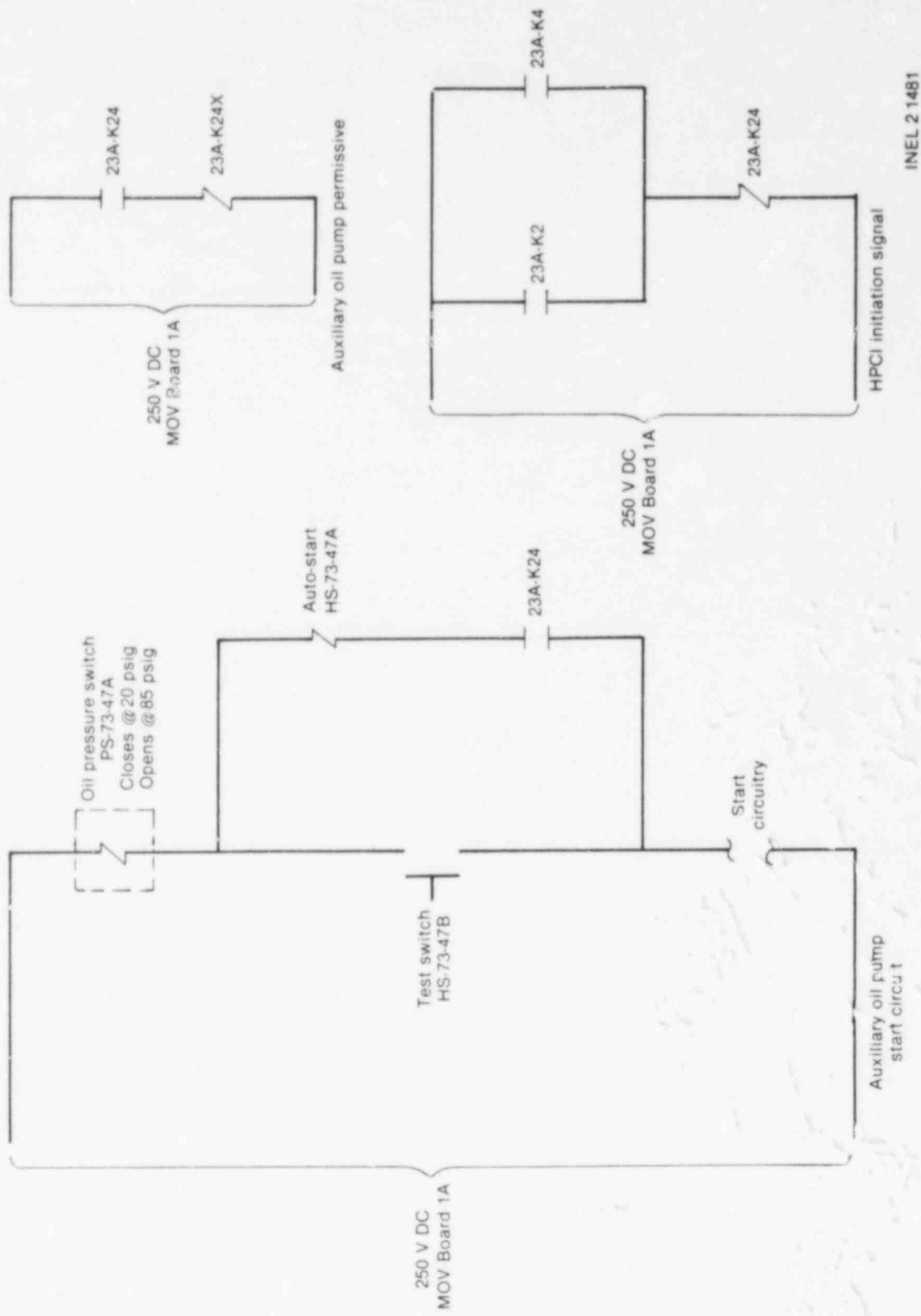


Figure B-10. Auxiliary oil pump starting circuitry.

6. Remote manual trip from control room.
7. Manual trip lever on the HPCI turbine.

A turbine trip will cause the following system effects:

1. Turbine stop valve (FCV-73-18) closes.
2. Minimum-flow bypass valve (FCV-73-30) closes.

The latter action is necessary to prevent drainage of the CST to the suppression pool.

All of the turbine trips except high water level and HPCI isolation will reset automatically when the initiating condition clears. High water level will reset when the low level initiation setpoint (476.5 inches above vessel zero) is reached or when the high level signal is manually reset. The HPCI isolation signal must always be manually reset.

System Isolation--Any of the following conditions will cause the HPCI system to be automatically isolated:

1. High temperature (194°F) of HPCI steam line space.
2. High differential pressure of HPCI steam line (steam line break; 225 inches of water or approximately 300% of design flow).
3. Low HPCI steam supply pressure (low reactor pressure) (100 psig).
4. High pressure of turbine exhaust line rupture disk (10 psig in the space between rupture disks). (The rupture disks are designed to rupture at 175 psig at 378°F.)
5. Manual isolation from the control room.

The HPCI isolation signal will cause the following system effects:

1. Turbine trip:
 - a. Turbine stop valve (FCV-73-18) closes.
 - b. Minimum-flow bypass valve (FCV-73-30) closes.
2. Inboard (AC) steam line isolation valve (FCV-73-2) closes.
3. Outboard (DC) steam line isolation valve (FCV-73-3) closes.
4. Suppression pool suction valves (FCV-73-26 and 27) close, if open.

The low HPCI steam supply pressure isolation signal will automatically reset when reactor pressure is restored. The remaining isolation signals seal in and must be manually reset when the isolation condition has cleared.

Testing. HPCI system testing requirements are summarized in Table B-27. When a test places any part of the HPCI system in a condition that would preclude proper system operation on demand, it is assumed that the test contributes to the overall system unavailability. Consequently, the test is coded as a basic event and included in the system fault tree.

Where applicable, the basic event code for each test is included in parentheses under the "Component Undergoing Test" column of Table B-27.

Maintenance. Upon reviewing the BFI maintenance schedules, only one maintenance act was identified that was assumed to contribute to the overall HPCI system unavailability. Once per quarter the HPCI turbine stop valve (FCV-73-18) hydraulic cylinder seals must be checked for leakage. The total time to perform this maintenance act is 2 hours. It is assumed that the HPCI system will be unavailable for the total duration of this maintenance act.

Table B-28 is a summary of the HPCI system maintenance acts identified as a result of the review mentioned above. When the maintenance act is considered to contribute to HPCI system unavailability, the act is coded as a basic event and included in the system fault tree. Where applicable, the basic event code associated with the corresponding maintenance act is included in parentheses under the "Maintenance Requirement" column.

Technical Specification Limitations

1. The HPCI system shall be operable:
 - a. Prior to startup from cold condition.
 - b. Whenever there is irradiated fuel in the reactor vessel and the reactor vessel pressure is greater than 122 psig, except if the HPCI system is inoperable the reactor may remain in operation for a period not to exceed 7 days provided ADS, core spray, LPCI mode of RHR, and RCIC are all operable.

If these conditions are not met, an orderly shutdown shall be initiated and the reactor vessel pressure reduced to 122 psig or less within 24 hours.

2. HPCI testing shall be performed as follows:
 - a. Simulated automatic actuation test (SI 4.5.E.1.a) once per operating cycle.
 - b. Pump operability (SI 4.5.E.1.b) once every month.
 - c. Motor-operated valve operability (SI 4.5.E.1.c) once every month.
 - d. Flow rate at normal reactor operating pressure (SI 4.5.E.1.d and e) once every 3 months.
 - e. Flow rate at 150 psig (SI 4.5.E.2.d and e or SI 4.5.E.1.d and e) once per operating cycle.

3. Whenever HPCI is required to be operable the piping from the pump discharge to the last flow-blocking valve shall be filled. Water flow from the high point vent must be observed monthly.
(SI 4.5.E.1.b, d and e or SI 4.5.E.2.d and e.)

2.3.3 System Operation

As discussed earlier, the HPCI system is designed to start and inject water into the reactor vessel without operator action. However, the system can be operated manually. Both of these methods of operation will be discussed below.

Automatic Operation. When reactor vessel level decreases to 476.5 inches above vessel zero or when drywell pressure increases to 2 psig, the HPCI logic circuitry sends an initiation signal to various HPCI components. Given a normal system lineup as depicted in Figure B-8, the following actions will take place. The turbine steam supply valve (FCV-73-18), the minimum-flow bypass valve (FCV-73-30), and the HPCI pump discharge valve (FCV-73-44) will open. The auxiliary oil pump will start, and this will cause the turbine stop valve (FCV-73-18) and the turbine governor valve (FCV-73-19) to open. The turbine will ramp up on the governor and settle out at an injection flow rate of 5000 gpm.

While the turbine is ramping up, the minimum-flow bypass valve will close when the HPCI pump discharge flow reaches 1200 gpm, and the auxiliary oil pump will trip off when turbine speed reaches 1800 rpm.

When CST level reaches 42 feet 10 inches of water (approximately 7,000 gallons) or when the suppression pool water level increases to 7 inches above normal level, the suppression pool suction valves (FCV-73-26 and 27) will open. When both valves are fully open, the CST suction valve (FCV-73-40) will close.

The turbine control system will maintain turbine speed to provide constant flow to the reactor vessel until a turbine trip signal or an isolation signal shuts the system down.

Manual Operation. The system is manually operated by starting the standby gas treatment system and the gland seal exhaustor. The flow controller is shifted to "manual" and set for 20% flow. The minimum-flow bypass valve (FCV-73-30) and the turbine steam supply valve (FCV-73-16) are opened. The auxiliary oil pump is started, and this will start the turbine. The HPCI pump discharge valve (FCV-73-44) is opened, and the flow controller is used to maintain desired reactor vessel water level.

2.3.4 Fault Tree

Figure B-11 is the HPCI system fault tree. The HPCI system is a single-train system. Consequently, many logical OR gates exist in the system fault tree. A reduced tree is depicted in Figure B-11. Many of these OR gates have been combined into one tabulation OR (TAB OR) gate in order to save space and make the tree easier to comprehend. The TAB OR gates were only used where system fault logic would not be compromised by

3. Whenever HPCI is required to be operable the piping from the pump discharge to the last flow-blocking valve shall be filled. Water flow from the high point vent must be observed monthly.
(SI 4.5.E.1.b, d and e or SI 4.5.E.2.d and e.)

2.3.3 System Operation

As discussed earlier, the HPCI system is designed to start and inject water into the reactor vessel without operator action. However, the system can be operated manually. Both of these methods of operation will be discussed below.

Automatic Operation. When reactor vessel level decreases to 476.5 inches above vessel zero or when drywell pressure increases to 2 psig, the HPCI logic circuitry sends an initiation signal to various HPCI components. Given a normal system lineup as depicted in Figure B-8, the following actions will take place. The turbine steam supply valve (FCV-73-18), the minimum-flow bypass valve (FCV-73-30), and the HPCI pump discharge valve (FCV-73-44) will open. The auxiliary oil pump will start, and this will cause the turbine stop valve (FCV-73-18) and the turbine governor valve (FCV-73-19) to open. The turbine will ramp up on the governor and settle out at an injection flow rate of 5000 gpm.

While the turbine is ramping up, the minimum-flow bypass valve will close when the HPCI pump discharge flow reaches 1200 gpm, and the auxiliary oil pump will trip off when turbine speed reaches 1800 rpm.

When CST level reaches 42 feet 10 inches of water (approximately 7,000 gallons) or when the suppression pool water level increases to 7 inches above normal level, the suppression pool suction valves (FCV-73-26 and 27) will open. When both valves are fully open, the CST suction valve (FCV-73-40) will close.

The turbine control system will maintain turbine speed to provide constant flow to the reactor vessel until a turbine trip signal or an isolation signal shuts the system down.

Manual Operation. The system is manually operated by starting the standby gas treatment system and the gland seal exhaustor. The flow controller is shifted to "manual" and set for 20% flow. The minimum-flow bypass valve (FCV-73-30) and the turbine steam supply valve (FCV-73-16) are opened. The auxiliary oil pump is started, and this will start the turbine. The HPCI pump discharge valve (FCV-73-44) is opened, and the flow controller is used to maintain desired reactor vessel water level.

2.3.4 Fault Tree

Figure B-11 is the HPCI system fault tree. The HPCI system is a single-train system. Consequently, many logical OR gates exist in the system fault tree. A reduced tree is depicted in Figure B-11. Many of these OR gates have been combined into one tabulation OR (TAB OR) gate in order to save space and make the tree easier to comprehend. The TAB OR gates were only used where system fault logic would not be compromised by

TABLE B-27. HPCI SYSTEM TEST REQUIREMENTS SUMMARY

Component Undergoing Test	Type of Test	Test Procedure Number	Components Aligned Away from Engineered Safeguards Position for Test	Expected Test Frequency	Expected Test Outage Time	Remarks
LS-23-94A LS-23-94B (MS42B26J)	CST level functional test	SI 4.2.B-26, Step 4.3	FCV-73-26 FCV-73-27 LS-23-94A LS-23-94B FCV-73-35* FCV-73-36*	Once every month	2 hr (see note in remarks below)	Power removed from 26 and 27 FCV-73-35 and 36 momentarily opened to test logic
Same as above	CST level calibration	SI 4.2.B-26, Step 4.2	Same as above	Once every 3 months	Same as above	Same as above (Steps 4.2 and 4.3 are essentially the same procedure)
LS-73-91A LS-73-91B (MS42B27J)	Suppression pool high level functional test and calibration	SI 4.2.B-27, Step 4.3	FCV-73-26 FCV-73-27	Once every 3 months	3 hr	(The channel calibration is run once every 3 months but the outage for these valves will remain the same; the functional test and the calibration procedures are essentially the same)
FCV-73-2 FCV-73-3 FCV-73-16 FCV-73-26 FCV-73-27 FCV-73-30 FCV-73-81 (MS42B36J)	HPCI turbine steam line high flow functional test and calibration	SI 4.2.B-36	FCV-73-16 FCV-73-30	Once every month	2 hr	Power removed from FCV-73-16 and 30
HPCI steam line temperature switches	Functional calibration	SI 4.2.B-37	FCV-73-16	Once every 3 months (Calibration)	--	Tagged out (FCV-73-16 is tagged out, but only if it is determined that temperature switch replacement is necessary)

B-123

TABLE B-27. (continued)

Component Undergoing Test	Type of Test	Test Procedure Number	Components Aligned Away from Engineered Safeguards Position for Test	Expected Test Frequency	Expected Test Outage Time	Remarks
FCV-73-2 FCV-73-3 FCV-73-16 FCV-73-26 FCV-73-27 FCV-73-30 FCV-73-34 FCV-73-35 FCV-73-36 FCV-73-40 FCV-73-44 FCV-73-81	HPCI system initiation and isolation logic functional test	SI 4.2.B-42A	FCV-73-16 FCV-73-30 FCV-73-44	Once every 6 months	Assume: 8 hr	Power removed from FCV-73-16, 30 and 44
Auxiliary oil pump (MS42B42J)	--	--	Auxiliary oil pump	--	--	Auxiliary oil pump locked out and circuit breaker open
HPCI system (MS45E1AJ)	Automatic actuation	SI 4.5.E.1.a	FCV-73-2* FCV-73-3* FCV-73-34* FCV-73-35* FCV-73-36* FCV-73-40* Auxiliary oil pump hand switch (HS-73-47A) pull-to-lock	Once every operating cycle	Assume: 1 hr	All valves repositioned to "normal" by test signal and procedure Renders entire system inoperable; repositioned to "auto" by procedure
HPCI pump (MS45E1BJ)	Operability	SI 4.5.E.1.b	Flow controller-- manual	Once every month	Assume: 5 min	System will not deliver design flow with controller in manual; repositioned when test complete

B-124

TABLE B-27. (continued)

Component Undergoing Test	Type of Test	Test Procedure Number	Components Aligned Away from Engineered Safeguards Position for Test	Expected Test Frequency	Expected Test Outage Time	Remarks
LCV-73-5 FCV-73-16	Stroke	SI 4.5.E.1.c	Auxiliary oil pump locked out for FCV-73-16 stroke	Once every month	20 sec (max)	Renders entire system inoperable
FCV-73-6A FCV-73-6B FCV-73-30 FCV-73-26 FCV-73-27					[Unavailability contribution considered insignificant compared to valve failure rate (1E-3D); each valve is stroked independently of the next]	All valves cycled from standby to engineered safeguards position and back
HPCI system (MS45E1DJ)	Flow (normal steam pressure)	SI 4.5.E.1.d and e	Flow controller-- manual FCV-73-18 (tripped) FCV-73-35* FCV-73-36*	Once every 3 months	Assume: 1 hr	System will not deliver design flow with controller in manual With FCV-73-18 tripped system is rendered inoperable (momentarily)
HPCI system	Flow (150 psig steam pressure)	SI 4.5.E.1.d and e	Same as above	Once every operating cycle	Same as above	Same as above; assume: this SI normally done when reactor is shut down (i.e., SI 4.5.E.2.d and e)

* Will reposition automatically if accident signal is present.

TABLE B-28. HPCI SYSTEM MAINTENANCE ACTS SUMMARY

<u>Maintenance Requirement</u>	<u>Instruction Number</u>	<u>Frequency</u>	<u>Duration</u>	<u>Remarks</u>
Perform quarterly inspection of HPCI system	MMI 23	Once every month	--	Visual inspection only
Check turbine stop valve (FCV-73-18) hydraulic cylinder seals for leakage (MM00181J)	--	Once every 3 months	2 hr	Assumed: system out of service
Inspect HPCI drain level switches (LS-73-5 and LS-73-8)	--	Once every 6 months	--	Assumed: system not taken out of service, because no duration time was given

B-126

B-127

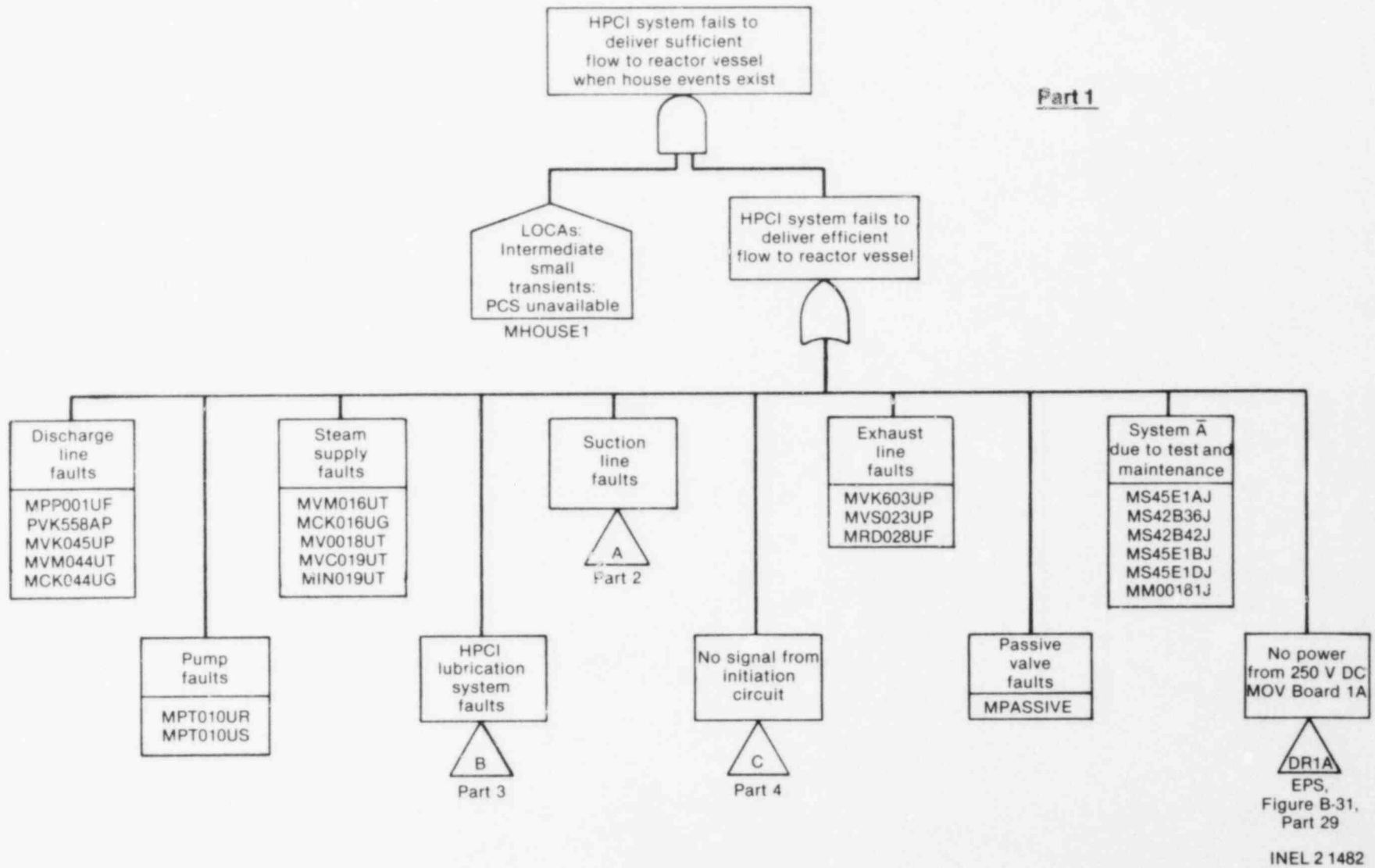
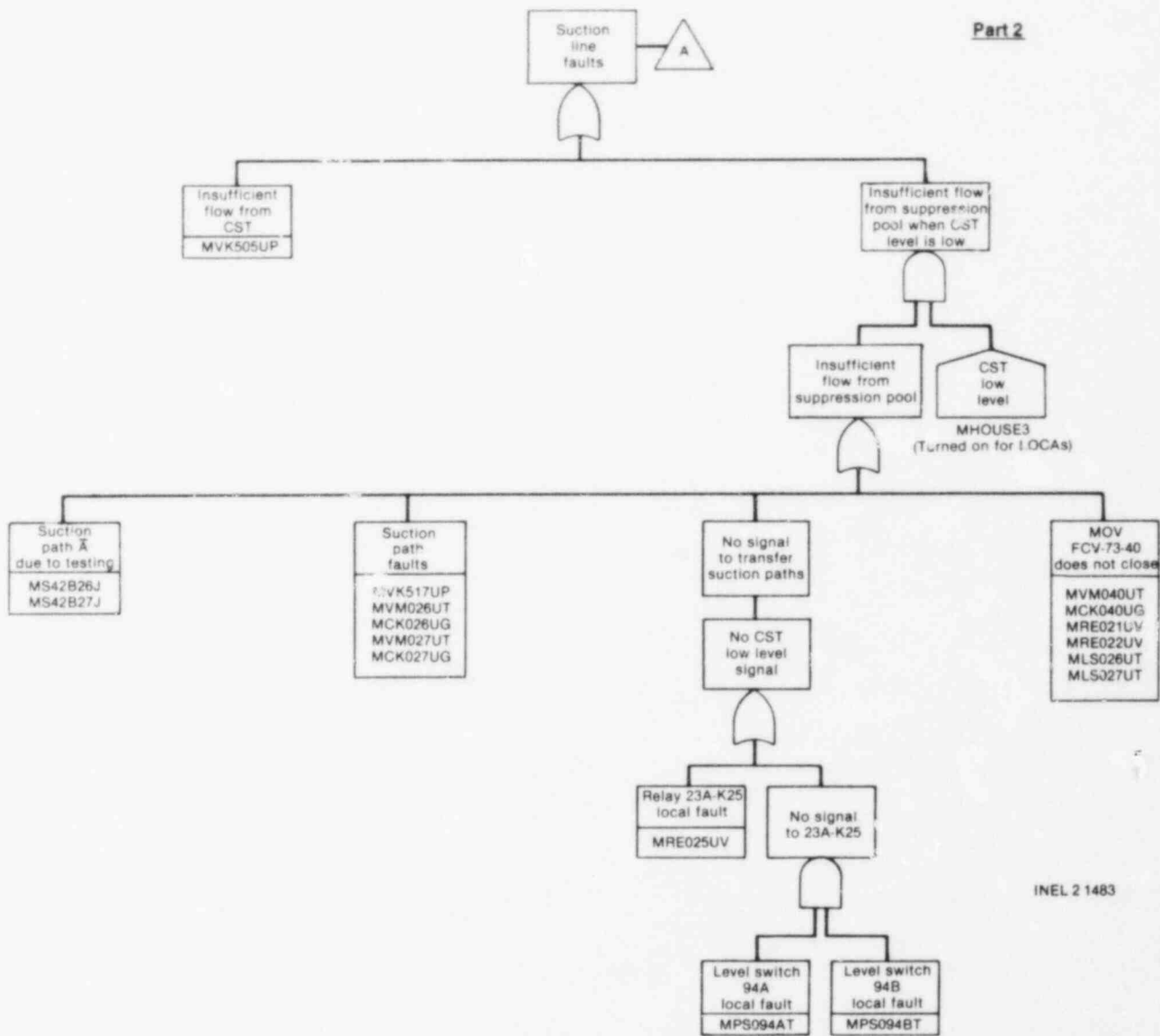


Figure B-11. HPCI fault tree.

B-1138



INEL 2 1483

Figure B-11. (continued).

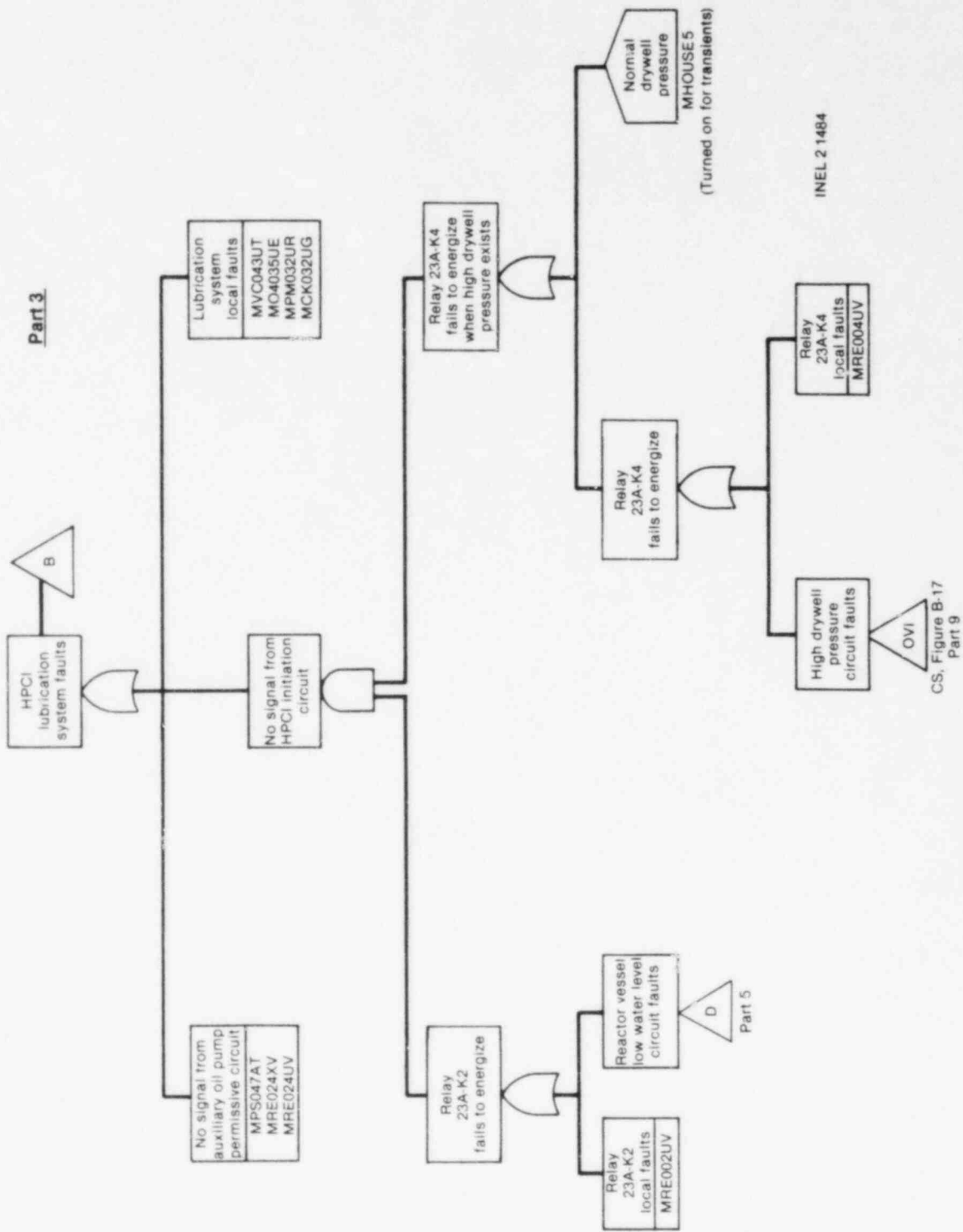
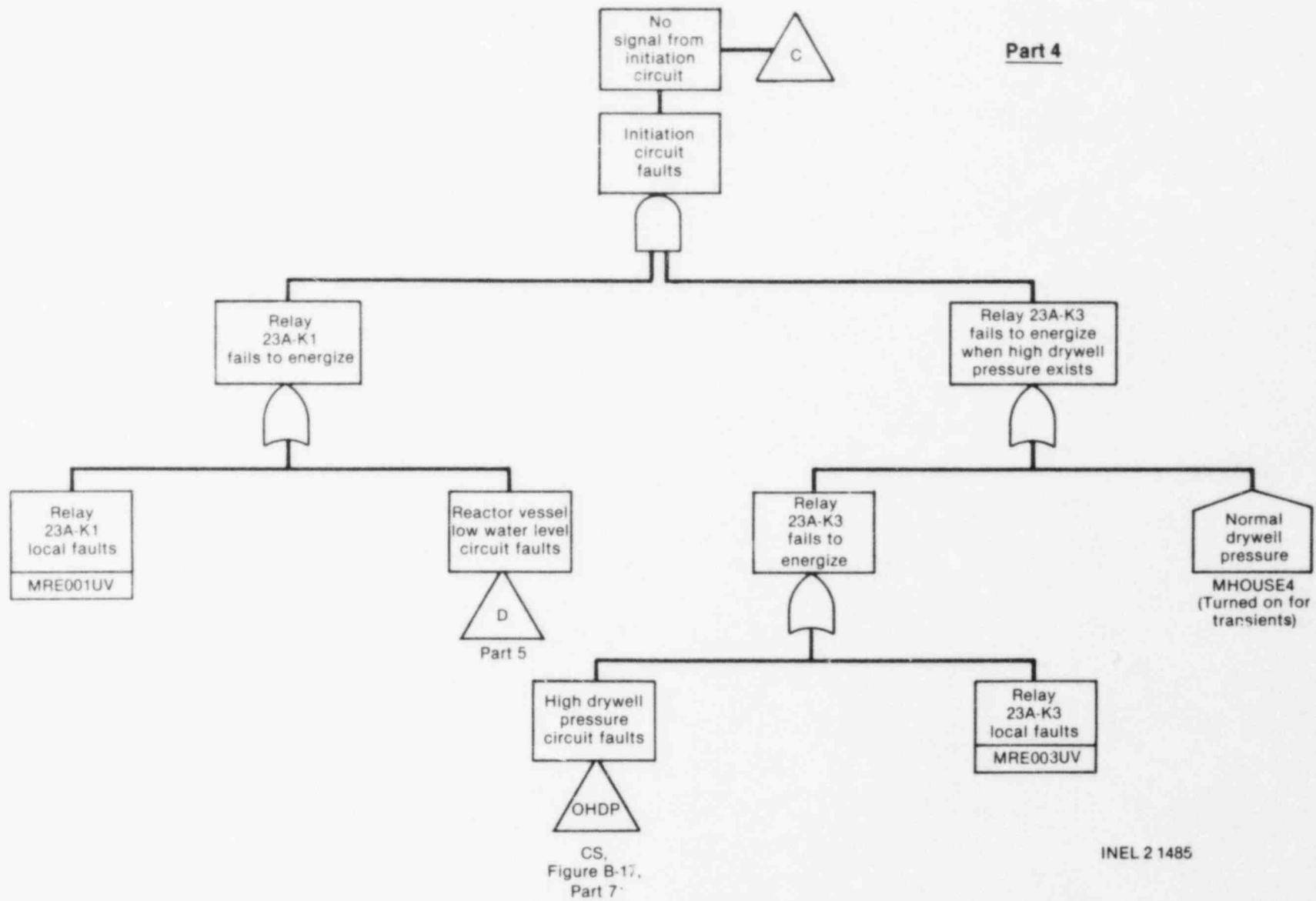


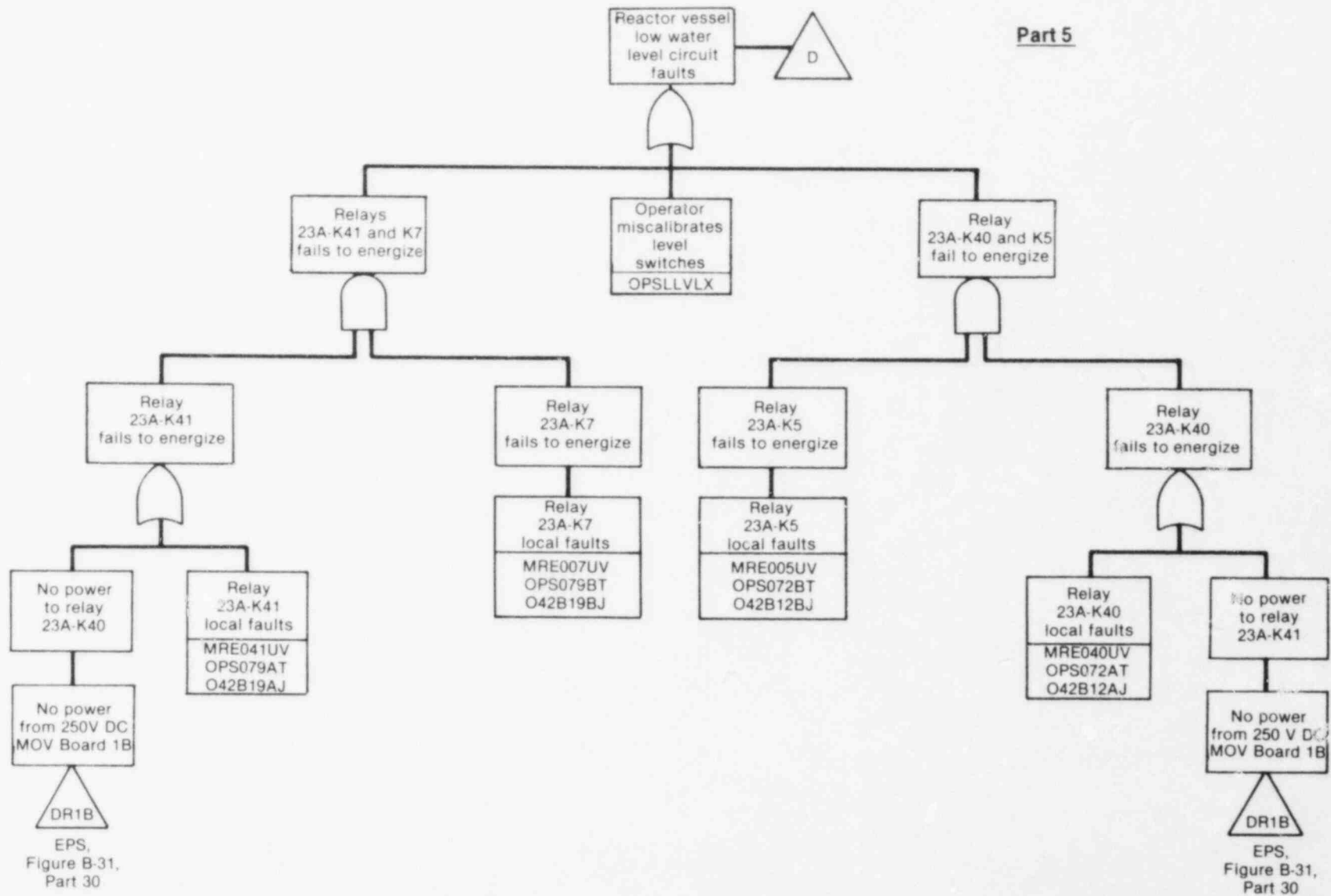
Figure B-11. (continued).

B-130



INEL 2 1485

Figure B-11. (continued).



B-131

Figure B-11. (continued).

compressing the appropriate gates and their corresponding basic events into one logic gate. Where this could not be accomplished, no reduction was attempted and the fault logic is fully developed.

The HPCI pump suction transfer fault logic is an example of fully-developed logic. In this case the house event, MHOUSE3, is used to model suction transfer faults when LOCA initiating events are being considered. It is assumed that when a LOCA exists, HPCI suction transfer will be necessary, otherwise the CST will provide adequate inventory. MHOUSE3 is used to turn on the suction transfer fault logic when appropriate.

HPCI initiation circuit faults largely involve one-out-of-two-twice logic and are relatively complicated to model. Consequently, the logic associated with these faults is also fully developed where necessary.

The house events MHOUSE4 and MHOUSE5 are used to control the portion of the tree that models drywell pressure signal faults. During transients fluid is not discharged into the containment drywell. Consequently, for transients, it would be incorrect to include faults of the high drywell pressure signal circuitry in the HPCI fault tree. Therefore, MHOUSE4 and MHOUSE5 are turned on for transients to allow for this consideration. Table B-29 lists the house events and shows when each is "on" or "off."

TABLE B-29. HPCI SYSTEM HOUSE EVENTS STATUS

<u>Initiators</u>	<u>MHOUSE1</u>	<u>MHOUSE3</u>	<u>MHOUSE4</u>	<u>MHOUSE5</u>
I _L , I _V , S	On	On	Off	Off
T _U , T _A , T _P	On	Off	On	On
T _P K, TK	On	On	On	On

In light of the major assumptions used to develop the tree, the remaining gates and system logic should be self-explanatory. These major assumptions will be discussed in the next following subsection.

Success/Failure Criteria. The top event in the HPCI system fault tree, representing the system failure definition, is "HPCI system fails to deliver sufficient flow to reactor vessel when house events exist." The house events are small and intermediate LOCAs, and transients where PCS is unavailable. Therefore, failure of the HPCI system occurs if the system cannot deliver sufficient flow to the reactor vessel during small or intermediate LOCAs or during transients when PCS is unavailable. For this analysis "sufficient flow" was considered to be the design flow of 5000 gpm. Any flow less than this amount was considered to be inadequate.

Major Assumptions. The following major assumptions were used for construction of the HPCI system fault tree:

1. The HPCI system can successfully respond to any liquid break that is less than 0.12 ft^2 or any steam break that is less than 1.4 ft^2 . Successful HPCI system operation will either result in reflooding of the core or depressurization of the reactor vessel, or both, depending upon the size of the break.
2. The system is initially aligned as shown in Figure B-8. This shows that, to achieve successful injection to the reactor vessel, the only valves required to change state are: the steam supply valve (FCV-73-16); the turbine stop valve (FCV-73-18); the turbine governor valve (FCV-73-19); and the pump discharge valve to the feedwater line (FCV-73-44).
3. Faults in the minimum-flow recirculation line downstream of the orifice are not considered in this tree. The HPCI pump is designed to maintain a constant discharge flow of 5000 gpm. Since the minimum-flow bypass line taps off of the discharge line upstream of the discharge flow sensor, any flow diversion through the bypass line will be detected by the flow sensor, and the pump output will be adjusted to maintain the 5000 gpm flow. The orifice will tend to reduce flow diversion to a minimum. Ruptures in the minimum-flow bypass line were not considered due to the size of the piping (see Assumption 4) and the fact that the HPCI system is a constant discharge flow system. It is further assumed that failure of the minimum-flow bypass to open will not significantly affect system operation unless a fault exists in the HPCI pump discharge path to the reactor vessel. However, if a discharge path fault causes a need for the minimum-flow bypass valve to be open, then this flow blockage will cause the HPCI system to be unavailable, by definition, regardless of the position of the minimum-flow bypass valve.
4. Faults in pipes, valves, or system connections of a 2-inch diameter or less are considered to have an insignificant effect on system operation. One exception to this assumption is the lubricating oil system. It is assumed that lube oil supply and cooling faults could significantly affect system operation. Many system components have a direct dependence on the proper operation of these systems. Therefore, these faults are considered in the fault model.
5. For LOCAs, it will be necessary to transfer the HPCI pump suction path from the CST to the suppression pool. For transients, it will not be necessary to shift the HPCI pump suction path.
6. Any faults in the turbine exhaust piping that cause turbine exhaust piping overpressure are assumed to actuate the turbine exhaust line pressure switches. This action sends a signal to the turbine control circuitry that will initiate a turbine trip. Turbine exhaust line rupture disk leakage will cause an isolation signal to be generated in the control circuitry, which also causes a turbine trip.

7. Faults in the condensate drain systems were analyzed and found to be insignificant relative to the dominant contributors to HPCI system unavailability. Essentially, in order for drain system faults to cause turbine damage, there must be either a flooded steam supply line or steam line drain system faults that would cause the condensate drain pots to fill. These faults must then be combined with condensate drain pot level switch failure in order for significant amounts of condensate to remain undetected in the steam supply line.
8. Passive failure of normally open valves that do not have to change state were considered if the failure would disable the whole system. There were eight such valves for this system, three CST suction valves (FCV-2-170, 1-2-705, and FCV-73-505), one suppression pool suction valve (HCV-73-25), two discharge valves (FCV-73-34 and HCV-3-67), and two steam valves (FCV-73-2 and 3).

Basic Events. The information associated with the various basic events listed in the fault tree is summarized in the HPCI fault summary short form, Table B-30. In addition, the failure data associated with these basic events is summarized in Table B-31. Tables B-32 and B-33 list the dominant cut sets for HPCI unavailability.

TABLE B-30. HPCI SYSTEM FAULT SUMMARY SHORT FORM

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
MPP001UF	Pipe break (anywhere)	Leakage/ rupture	1E-10/hr/ section	384	30
PVK558AP	Check Valve 3-558	Does not open	1E-4/D	--	3
MVK045UP	Testable check Valve FCV-73-45	Does not open	1E-4/D	--	3
MVM044UT	Discharge Valve FCV-73-44	Does not operate	1E-3/D	--	3
MCK044UG	FCV-73-44 control circuit	No output	3.2E-3	--	10
MPT010UR	HPCI pump	Does not start	3E-3/D	--	3
MPT010US	HPCI pump	Does not continue to run	3E-5/hr	37	3
MVM016UT	HPCI turbine steam supply Valve FCV-73-16	Does not operate	1E-3/D	--	3
MCK016UG	FCV-73-16 control circuit	No output	3.2E-3	--	10
MV0018UT	Turbine stop Valve FCV-73-18	Does not operate	3E-4/D	--	3

TABLE B-30. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
MVC019UT	Turbine govern control Valve FCV-73-19	Does not operate	3E-4/D	--	3
MIN019UT	FCV-73-19 control circuit instrument	Does not operate	1E-6/hr	367	10
MVK603UP	Turbine exhaust line check Valve 73-603	Does not open	1E-4/D	--	3
MVS023UP	Turbine exhaust line stop check Valve HCV-73-23	Does not open	1E-4/D	--	3
MRD028UF	Turbine exhaust line upstream rupture disk	Leakage/rupture	5.73E-5/hr	372	3
MS45E1AJ	HPCI system automatic actuation Test SI 4.5.E.1.a	Unavailable due to test or maintenance	7.7E-5	--	0
MS42B36J	HPCI steam line high flow functional test and calibration SI 4.2.B-36	↓	2.8E-3	--	↓
MS42B42J	Initiation and isolation logic functional Test SI 4.2.B-42A		1.9E-3	--	
MS45E1BJ	HPCI pump operability Test SI 4.5.E.1.b		1.2E-4	--	

TABLE B-30. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
MS45E1DJ	HPCI system flow Test SI 4.5.E.1.d and e	Unavailable due to test or maintenance	4.6E-4	--	0
MM00181J	Maintenance--check FCV-73-18 hydrocylinder seals for leakage	Unavailable due to test or maintenance	9.3E-4	--	0
MVK505UP	CST suction line check Valve 73-505	Does not open	1E-4/D	--	3
MS42B26J	CST level functional Test SI 4.2.B-26	Unavailable due to test or maintenance	2.8E-3	--	0
MS42B27J	Suppression pool high level functional Test SI 4.2.B-27	Unavailable due to test or maintenance	4.2E-3	--	0
MVK517UP	Suppression pool suction check Valve 73-517	Does not open	1E-4/D	--	3
MVM026UT	Suppression pool suction Valve FCV-73-26	Does not operate	1E-3/D	--	3
MCK026UG	FCV-73-26 control circuit	No output	3.2E-3	--	10
MVM027UT	Suppression pool suction Valve FCV-73-27	Does not operate	1E-3/D	--	3

TABLE B-30. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
MCK027UG	FCV-73-27 control circuit	No output	3.2E-3	--	10
MRE025UV	Relay 23A-K25	Does not energize	1E-4/D	--	3
MPS094AT	Level Switch LS-23-94A	Does not operate	↓	--	↓
MPS094BT	Level Switch LS-23-94B	Does not operate		--	
MVM040UT	CST suction isolation Valve FCV-73-40	Does not operate		--	
MCK040UG	FCV-73-40 control circuit	No output	3.2E-3	--	10
MRE021UV	Relay 23A-K21	Does not energize	1E-4/D	--	3
MRE022UV	Relay 23A-K22	Does not energize	1E-4/D	--	↓
MLS026UT	Valve open limit Switch LS-2 on FCV-73-26	Does not operate	3E-4/D	--	
MLS027UT	Valve open limit Switch LS-2 on FCV-73-27	Does not operate	3E-4/D	--	

TABLE B-30. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
MPS047AT	Oil pressure Switch PS-73-47A	Does not operate	1E-4/D	--	3
MRE024XV	Relay 23A-K24X	Does not energize	↓	--	↓
MRE024UV	Relay 23A-K24	Does not energize		--	
MRE002UV	Relay 23A-K2	Does not energize		--	
MVC043UT	Lube oil cooler inlet pressure control Valve PCV-73-43	Does not operate	3E-4/D	--	
MOR035UE	Lube oil cooler return line orifice	Plugged	3E-4/D	--	
MPM032UR	Auxiliary oil pump	Does not start	1E-3/D	--	
MCK032UC	Auxiliary control circuit	No output	2.2E-3	--	10
MRE004UV	Relay 23A-K4	Does not energize	1E-4/D	--	3
MRE001UV	Relay 23A-K1	Does not energize	1E-4/D	--	3

TABLE B-30. (continued)

B-140

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
MRE003UV	Relay 23A-K3	Does not energize	1E-4/D	--	3
MRE041UV	Relay 23A-K41	↓	↓	--	↓
MRE007UV	Relay 23A-K7			--	
MRE005UV	Relay 23A-K5			--	
MRE040UV	Relay 23A-K40			--	
OPS079AT	Level indicating transmitter Switch 3, LITS-2-3-79A	Does not operate		--	
OPS079BT	Level indicating transmitter Switch 3, LITS-2-3-79B	↓	↓	--	↓
OPS072BT	Level indicating Switch 3, LIS-2-3-72B			--	
OPS072AT	Level indicating Switch 3, LIS-2-3-72A			--	
042B19AJ	Reactor low water level 79A functional Test SI 4.2.B-1	Unavailable due to test or maintenance	1.4E-3	--	0
042B19BJ	Reactor low water level 79B functional Test SI 4.2.B-1	Unavailable due to test or maintenance	1.4E-3	--	0

TABLE B-30. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
042B12BJ	Reactor low water Level 72B functional Test SI 4.2.B-1	Unavailable due to test or maintenance	1.4E-3	--	0
042B12AJ	Reactor low water Level 72A functional Test SI 4.2.B-1	Unavailable due to test or maintenance	1.4E-3	--	0
MPASSIVE	Passive valve faults	Does not remain open	7E-4/D	(Transients)	3
			8E-4/D	(LOCAs)	3
OPSLVLX	Core spray reactor low level switches	Operator miscalibration	2.4E-6/D	--	10

TABLE B-31. HPCI SYSTEM FAILURE DATA SUMMARY

Component/Activity (Code)	Failure Mode (Code)	Time to Detect (T _D)	Time to Repair (T _R)	Fault Duration Time ^a (T = T _D + T _R)	Failure Probability	Unavailability (A)	Remarks
Auxiliary oil pump control circuit (CK)	No output (G)	360 hr	7 hr	367 hr	5.4E-6/hr + 2E-4/D	2.2E-3	T _D --based on HPCI pump operability check, once every month T _R --WASH-1400, Table III 5-2 A = 2E-4 + 5.4E-6T
Motor-operated valve control circuit (CK)	No output (G)	360 hr	7 hr	367 hr	7.7E-6/hr + 4.1E-4/D	3.2E-3	A = 4.1E-4 + 7.7E-6T T _R --WASH-1400, Table III 5-2 T _D = half test interval; based on pump operability test and stroke time test, once every month
Governor instrumentation (transmitter, amplifier, output devices) (IN)	Does not operate (T)	360 hr	7 hr	367 hr	1E-6/hr	3.7E-4	T _D --based on pump operability check, once every month T _R --WASH-1400, Table III 5-2
Limit switch (LS)	Does not operate (T)	--	--	--	3E-4/D	3E-4	--
Orifice (OR)	Plugged (E)	--	--	--	3E-10/D	3E-10	--
Auxiliary oil pump (PM)	Does not start (R)	--	--	--	1E-3/D	1E-3	--
Pipe (PP)	Leakage/rupture (F)	360 hr	24 hr	384 hr	1E-10/hr	3.8E-8	T _R = 24 hr, assumed time to cold shutdown T _D --based on pump operability test, once every month
Process switch (PS)	Does not operate (T)	--	--	--	1E-4/D	1E-4	--
HPCI pump (PT)	Does not start (R)	--	--	--	1E-3	1E-3	--
HPCI pump (PI)	Does not run (S)	0 hr	37 hr	8 hr	3E-5/hr	2.4E-4	T _R --WASH-1400, Table III 5-2
Rupture disk (RD)	Leakage/rupture (F)	360 hr	12 hr	372 hr	5.7E-5/hr	2E-2	T _D --based on HPCI pump operability check, once every month T _R --plant-specific data λ--based on plant-specific data
Relay (RE)	Does not energize (V)	--	--	--	1E-4/D	1E-4	--

B-142

TABLE B-31. (continued)

Component/Activity (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (A)	Remarks
Control valve (VC)	Does not operate (T)	--	--	--	3E-4/D	3E-4	Considered to be air-fluid operated
Check valve (VK)	Does not open (P)	--	--	--	1E-4/D	1E-4	--
Motor-operated valve (VM)	Does not operate (T)	--	--	--	1E-3/D	1E-3	--
Hydraulic operated valve (VO)	Does not operate (T)	--	--	--	3E-4/D	3E-4	Considered to be air-fluid operated
Stop check valve (VS)	Does not open (P)	--	--	--	1E-4/D	1E-4	Used same unavailability as that for check valve (VK)
CST level functional test (MS42B26J)	Unavailable due to test or maintenance (J)	--	--	--	--	2.8E-3	Performed once every month; duration, 2 hr
Suppression pool high level function test (MS42B27J)	Unavailable due to test or maintenance (J)	--	--	--	--	4.2E-3	Performed once every month; duration, 3 hr
Steam line high flow functional test (MS42B36J)	Unavailable due to test or maintenance (J)	--	--	--	--	2.8E-3	Performed once every month; duration, 2 hr
Initiation and isolation logic functional test (MS42B42J)	Unavailable due to test or maintenance (J)	--	--	--	--	1.9E-3	Performed once every 6 months; duration, 8 hr
HPCI automatic actuation test (MS45E1AJ)	Unavailable due to test or maintenance (J)	--	--	--	--	7.7E-5	Performed once every operating cycle; duration, 1 hr
HPCI pump operability (MS45E1BJ)	Unavailable due to test or maintenance (J)	--	--	--	--	1.2E-4	Performed once every month; duration, 5 min

TABLE B-31. (continued)

Component/Activity (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (A)	Remarks
System flow test (MS45E1DJ)	Unavailable due to test or maintenance (J)	--	--	--	--	4.6E-4	Performed once every 3 months; duration, 1 hr
FCV-73-18 maintenance (MM00181J)	Unavailable due to test or maintenance (J)	--	--	--	--	9.3E-4	Performed once every 3 months; duration, 2 hr
Core spray system process switches (042B---J)	Unavailable due to test or maintenance (J)	--	--	--	--	1.4E-3	See core spray system documentation
Core spray low level switches (OPSLVLX)	Operator miscalibration (X)	--	--	--	--	2.4E-6	--
Passive valve faults (MPASSIVE)	Does not remain open	--	--	--	1E-4/D	8E-4 7E-4	Eight valves for LOCAs, seven valves for transients; suppres- sion pool suction valve (HCV-73-25) not required

a. If $T_D = 0$, then $T = T_R$ if the mission time (8 hr) $> T_R$. If $T_D = 0$, then $T =$ mission time (8 hr) if mission time $\leq T_R$.

TABLE B-32. HPCI SYSTEM CUT SETS
(Transients)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
2.0E-2	45.2	MRD028UF	No
3.2E-3	7.2	MCK016UF	No
3.2E-3	7.2	MCK044UG	No
3.0E-3	6.8	MPT010UR	No
2.8E-3	6.3	MS42B36J	No
2.2E-3	5.0	MCK032UG	No
1.9E-3	4.3	MS42B42J	No
1.0E-3	2.3	MVM016UT	No
1.0E-3	2.3	MPM032UR	No
1.0E-3	2.3	MVM044UT	No
Cumulative importance	88.9		

TABLE B-33. HPCI SYSTEM CUT SETS
(LOCAs)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
2.0E-2	30.6	MRD028UF	No
4.2E-3	6.5	MS42B27J	No
3.2E-3	4.9	MCK016UG	No
3.2E-3	4.9	MCK044UG	No
3.2E-3	4.9	MCK040UG	No
3.2E-3	4.9	MCK027UG	No
3.2E-3	4.9	MCK026UG	No
3.0E-3	4.6	MPT010UR	No
2.8E-3	4.3	MS42B36J	No
2.8E-3	4.3	MS42B26J	No
2.2E-3	3.4	MCK032UG	No
1.9E-3	2.9	MS42B42J	No
1.0E-3	1.5	MVM016UT	No
1.0E-3	1.5	MPM032UR	No
1.0E-3	1.5	MVM026UT	No
1.0E-3	1.5	MVM027UT	No
1.0E-3	1.5	MVM044UT	No
1.0E-3	1.5	MVM040UT	No
Cumulative importance	90.3		

2.4 Automatic Depressurization System

2.4.1 Purpose

The ADS is provided to reduce reactor pressure whenever the high pressure makeup systems are unable to maintain reactor water level. This allows the core spray system and the LPCI system to function in order to maintain water level. The ADS will be used in a small break LOCA or a transient situation if HPCI and RCIC systems fail. The depressurization is accomplished automatically by the opening of four of six safety relief valves on the main steam lines to vent steam to the suppression pool.

2.4.2 System Configuration

Overall Configuration. ADS utilizes 6 of the 13 relief valves. Each valve is a Target Rock two-stage safety valve. Each valve is individually piped to the suppression pool. A vacuum breaker to the drywell equalizes water level between the discharge pipe and the suppression pool when the valve is closed. Each line also has a temperature detector.

Each valve relieves approximately 800,000 lb/hr at 1000 psi. ADS activation of a relief valve involves energizing a solenoid, which allows compressed air from the drywell control air system to pressurize a pneumatic actuator that opens the relief valve. The valve will remain open until closed by the operator. All ADS valves are equipped with an accumulator on the air line. A check valve is upstream of the accumulator. Drywell control air is isolated by a high drywell pressure signal. The accumulator/check valve provision is to ensure adequate pneumatic pressure for activation. A simplified diagram of ADS is shown in Figure B-12.

Depressurization will occur if three conditions exist. These are:

1. Reactor water level at Level 1 (-143 inches).
2. High drywell pressure (+2 psig).
3. Sufficient LPCI or core spray pumps are operating to ensure that makeup water is available after depressurization.

All relief valves are able to be manually activated from the control room. This serves as a backup to ADS should depressurization be required and the activation logic fails. Manual activation of the relief valves will be required for transients since the high drywell pressure signal will not be present.

System Interfaces. The major interfaces for the ADS are with control power (for the sensors and logic circuits), motive power (for the solenoids), and drywell control air (for the valve actuators). The interfaces are listed in Table B-34. This table also lists the interfaces for the other seven main steam relief valves.

Instrumentation Control. The ADS receives signals from drywell pressure, reactor vessel water level, RHR pump discharge pressure, and core spray pump discharge pressure. The ADS valves are controlled in two groups:

PSV-1-5, PSV-1-30, and PSV-1-34 are controlled by Relays 2E-K7, 2E-K9, 2E-K18, and 2E-K20; PSV-1-19, PSV-1-22, and PSV-1-31 are controlled by Relays 2E-K6, 2E-K9, 2E-K17, and 2E-K20. All of these relays are energized by the 250 V RMOV (reactor motor-operated valve) Board 1B.

The following signals must be present for ADS to be activated.

1. Coincident signals of low reactor water level (-143 inches) and high drywell pressure must be present. High drywell signal is sealed in, but low water level must exist for 120 sec.
2. Confirmatory low water level signal (+10 inches).
3. Appropriate permissives to indicate the RHR pumps or core spray pumps are operating. At least one RHR pump or two core spray pumps must be operating. This ensures availability of water after depressurization. Signals are derived from pressure switches in the pump discharge: 100 psi for RHR and 185 psi for core spray.
4. When all signals are present, a 120 sec timer is activated. When the timer runs out, ADS actuates. The valves remain open until reactor pressure is 50 psig. With the exception of high drywell, all signals must be present for 120 sec or else the timer is reset.

The ADS initiation logic is shown in Figure B-13.

Testing. No periodic testing of the relief valves is performed during reactor operation. The actuation logic is tested once every 6 months per SI 4.2.B-44. The valves are tested once every operating cycle, just before restart.

Maintenance. No scheduled maintenance of the ADS is performed during reactor operation. Unscheduled maintenance can be performed on the actuation logic during operation. Maintenance of the valves requires shutdown and depressurization of the reactor.

Technical Specification Limitations. Technical specifications allow reactor operation for 30 days with only four ADS valves operable. If three valves are known to be inoperable, the reactor must be shut down in 72 hours.

2.4.3 Operation

Operation of the system was described in the previous section, "Overall Configuration."

2.4.4 Fault Tree Description

The ADS function appears as Event E in the LOCA event trees in Appendix A.

Success/Failure Criteria. Success requires at least four of six valves to open for automatic depressurization. Opening of any four of the thirteen safety relief valves constitutes successful manual depressurization.

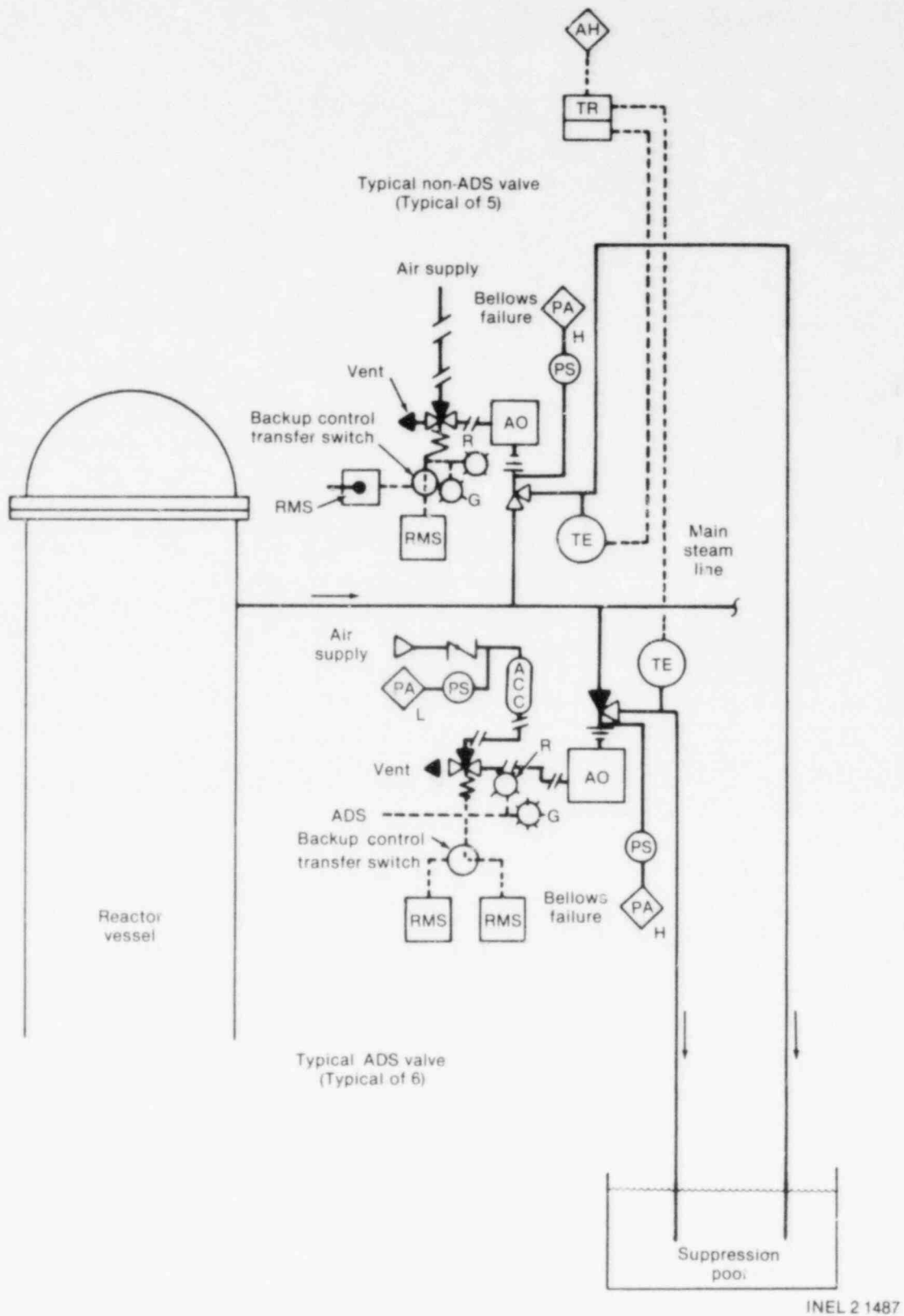


Figure B-12. Automatic depressurization system (ADS).

TABLE E-34. ADS FMEA OF COMPONENT/SUPPORTING-SYSTEM INTERACTIONS

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
PCV-1-41	Drywell control air	No accumulator	Air pressure low	Valve will not actuate except on high steam pressure	--
			Condensation in air line	Unknown	--
PSV-1-41	250 V RMOV-1A	Terminal 11C1	No power to board	Valve will not actuate except on high steam pressure	--
PCV-1-180 (manual valve)	Drywell control air	No accumulator	Air pressure low	Same as PCV-1-41	--
			Condensation in air line	Unknown	--
PSV-1-180	250 V RMOV-1C	Terminal 10B1	No power to board	Valve will not actuate except on high steam pressure	--
PCV-1-42	Drywell control air	No accumulator	Air pressure low	Same as PCV-1-41	--
			Condensation in air line	Unknown	--
PSV-1-42	250 V RMOV-1B	Terminal 8B2	No power to board	Valve will not actuate except on high steam pressure	--
PCV-1-30 (ADS valve)	Drywell control air	Accumulator downstream of CV-1-32-892	Air pressure low	Same as PCV-1-41	--
			Condensation in air line	Unknown	--
PSV-1-30	250 V RMOV-1A (normal source)	Terminal 9B1	No power to board	Valve will not actuate except on high steam pressure	--
	250 V RMOV-1C (alternate source)	Terminal 7A	--	--	--
PCV-1-31 (ADS valve)	Drywell control air	Accumulator downstream of CV-1-32-915	Air pressure low	Same as PCV-1-41	--
			Condensation in air line	Unknown	--
PSV-1-31	250 V RMOV-1B	Terminal 1C2	No power to board	Valve will not actuate except on high steam pressure	--
PCV-1-34 (ADS valve)	Drywell control air	Accumulator downstream of CV-1-32-919	Air pressure low	Same as PCV-1-41	--
			Condensation in air line	Unknown	--

B-149

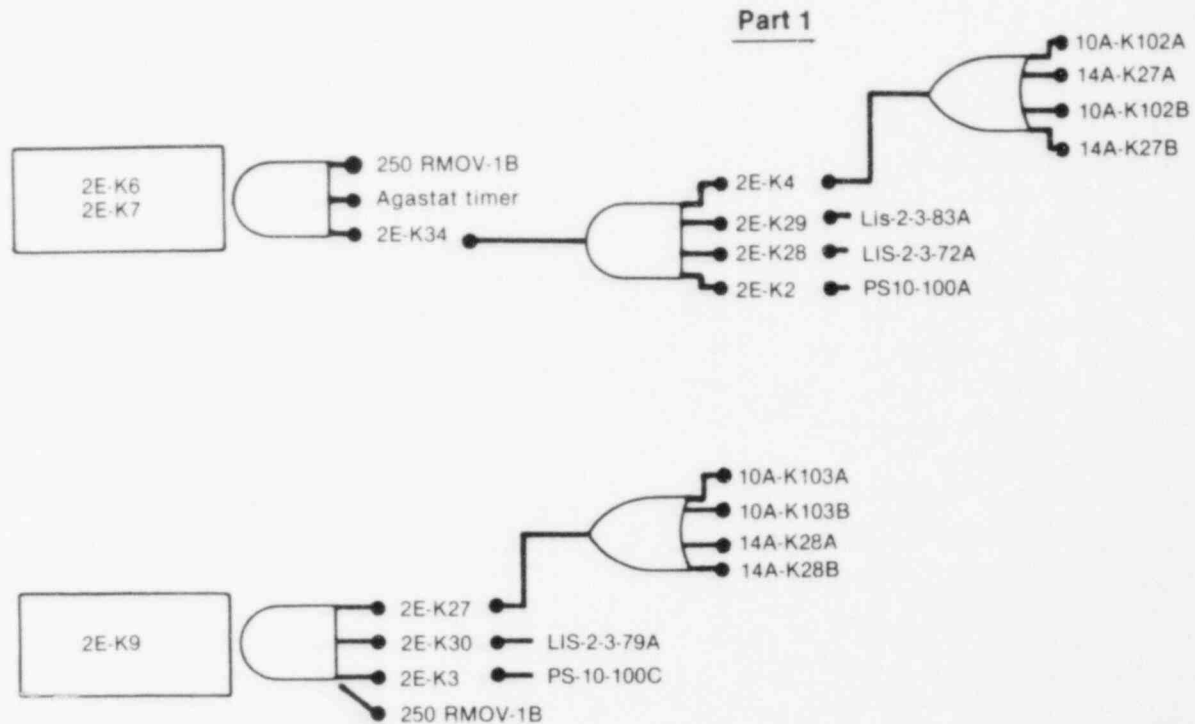
TABLE B-34. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
PSV-1-34	250 V RMOV-1C	Terminal 10A	No power to board	Valve will not actuate except on high steam pressure	--
PCV-1-18	Drywell control air	--	Air pressure low	Same as PCV-1-41	--
			Condensation in air line	Unknown	--
PSV-1-18	250 V RMOV-1B	Terminal 8C1	No power to board	Valve will not actuate except on high steam pressure	--
PCV-1-19 (ADS valve)	Drywell control air	--	Air pressure low	Same as PCV-1-41	--
			Condensation in air line	Unknown	--
PSV-1-19	250 V RMOV-1B	Terminal 1B2	No power to board	Valve will not actuate except on high steam pressure	--
PCV-1-22 (ADS valve)	Drywell control air	Accumulator downstream of CV-1-32-872	Air pressure low	Same as PCV-1-41	--
			Condensation in air line	Unknown	--
PSV-1-22	250 V RMOV-1A (normal source)	Terminal 11C2	No power to board	Valve will not actuate except on high steam pressure	--
	250 V RMOV-1B (alternate source)	Terminal 1C1	--	--	--
PCV-1-23	Drywell control air	No accumulator	Air pressure low	Same as PCV-1-41	--
			Condensation in air line	Unknown	--
PSV-1-23	250 V RMOV-1C	Terminal 1B1	No power to board	Valve will not actuate except on high steam pressure	--
PCV-1-4	Drywell control air	No accumulator	Air pressure low	Same as PCV-1-41	--
			Condensation in air line	Unknown	--
PSV-1-4	250 V RMOV-1A	Terminal 11B2	No power to board	Valve will not actuate except on high steam pressure	--

B-150

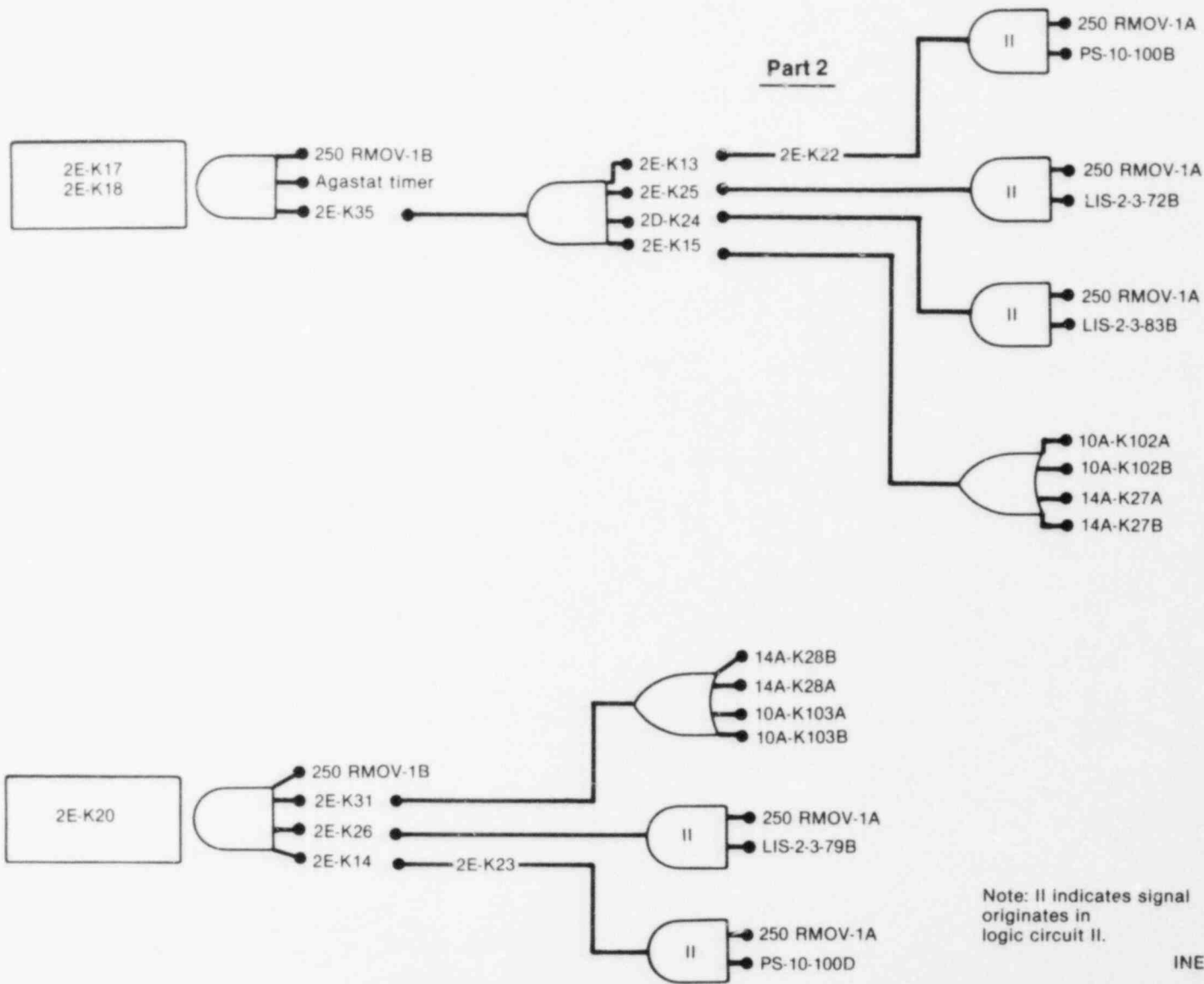
TABLE B-34. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
PCV-1-179 (manual valve)	Drywell control air	No accumulator	Air pressure low	Same as PCV-1-41	--
			Condensation in air line	Unknown	--
PSV-1-179	250 V RMOV-1B	Terminal 8C2	No power to board	Valve will not actuate except on high steam pressure	--
PCV-1-5 (ADS valve)	Drywell control air	Accumulator downstream of CV-1-32-869	Air pressure low	Same as PCV-1-41	--
			Condensation in air line	Unknown	--
PSV-1-5	250 V RMOV-1C	Terminal 7A	No power to board	Valve will actuate except on high steam pressure	--
Auto-blowdown logic, Division II	250 V RMOV-1A	Terminal 9A1	No power to board	Division II logic inoperable	--
Auto-blowdown logic, Bus A, Division I	250 V RMOV-1B	Terminal 1F1	No power to board	Division I, Bus A logic inoperable	--
Auto-blowdown logic, Bus B, Division I	250 V RMOV-1B	Terminal 8F2	No power to board	Division I, Bus B logic inoperable	--



INEL 2 1488

Figure B-13. ADS initiation circuitry.



INEL 2 1489

Figure B-13. (continued).

Major Assumptions. The following major assumptions were used for construction of the ADS fault tree:

1. Manual backup was not addressed in the initial analysis. Manual depressurization is dominated by operator error and is discussed further in Section 4. This action is depicted as Event V in the transient systemic event trees (see Appendix A).
2. Failure of the drywell control air system was not addressed on the fault tree. Each ADS valve is equipped with an accumulator that is rated for five cycles.
3. Failures of the initiation logic were only taken to the level of the relay; that is, the contacts were assumed to be operable if the relay was operable. All contacts of a given relay were assumed to have the same operability status; i.e., if a relay worked properly, all the contacts worked properly.
4. Control switches and transfer switches were assumed to be in the correct position prior to ADS demand. Misposition of these switches is indicated in the control room.
5. The vacuum relief valves that connect the ADS discharge piping to the drywell atmosphere were not considered important to the failure modes of ADS and, consequently, were eliminated from the fault tree analysis.
6. Failure of the 250 V RMOV Board 1A is inconsequential because both valves automatically switch to other RMOV boards.
7. Failure of 250 V RMOV Board 1B will fail ADS because it disables the control logic.
8. The switch to the alternate source of power for Valves PCV-1-30 and 22 is automatic. A single relay is provided to switch power from the normal RMOV to the alternate RMOV, identified as follows:

<u>Valve</u>	<u>Relay</u>	<u>Normal Power</u>	<u>Alternate Power</u>
PSV-1-30	2E-K33	RMOV A	RMOV C
PSV-1-22	2E-K32	RMOV A	RMOV B

These relays are energized by RMOV A. In the deenergized position, the relay closes the contacts to the alternate power source. To interrupt power from both sources, a failure mode would have to be postulated where the relay fails in neither the closed nor open position. This failure mode of the relay was not addressed. All failures of the RMOV boards were properly addressed.

9. Errors of commission on the part of the operator to mistakenly reset the Agastat timer were ignored. This is consistent with the general assumption that when there is no procedure calling for operator action, no action is taken.

10. Two faults were postulated for each relay: failure of the relay itself and failure to receive a signal.
11. Level switches and pressure switches associated with this system are mechanically activated and, as such, require no power sources.

Fault Tree. A reduced fault tree of the ADS is shown in Figure B-14. The ADS fault tree has been reduced to segregate valve failures, power failures, and initiation logic failures. The fault tree for the initiation logic is not in reduced form.

The following describes the derivation of the failure rate for relief valve fail to open (VREXXUNO). Event VREXXUNO is composed of random valve faults that are independent of other plant events. By doing this, the combinatorial OR gate can be quantified and input into the tree as a basic event.

Two possible common mode failures were identified but were not pursued because representative data is not available. The first was any common mode failure problems with the check valves in the air lines, and the second was multiple ADS valve failure due to secondary damage from equipment rupture.

Failure of each ADS valve can occur for three reasons: (a) faults in the accumulator line, (b) faults in the solenoid, and (c) faults in the valve itself. These are further elaborated:

Reason 1--All ADS valves are equipped with an accumulator on the air line. A check valve is upstream of the accumulator. Drywell control air is isolated on high drywell pressure. The accumulator/check valve provision is to ensure adequate pneumatic pressure for activation. This can be defeated in two ways; rupture downstream of the check valve or failure of the check valve. Should the check valve fail open or leak, it was assumed there will be sufficient leakage into the drywell control air system to prevent actuation. Failure of the check valve could only be detected during isolation of the drywell control air system. No surveillance procedure, performed during operation, for the check valves was identified.

Reasons 2 and 3--Faults in the solenoid and the valve itself were combined into a single failure probability, which was compatible with the IREP failure data.

Failure rates were assigned as follows:

Accumulator Rupture

$$\lambda = \epsilon \quad (\text{based on a failure rate of } 10^{-9}/\text{hr})$$

Check Valve Leak

$$q = \lambda t = 3 \times 10^{-7} \frac{1}{\text{hr}} \times \frac{8760}{2} \text{ hr}$$

$$q = 1.3 \times 10^{-3}$$

Solenoid and Valve Fail

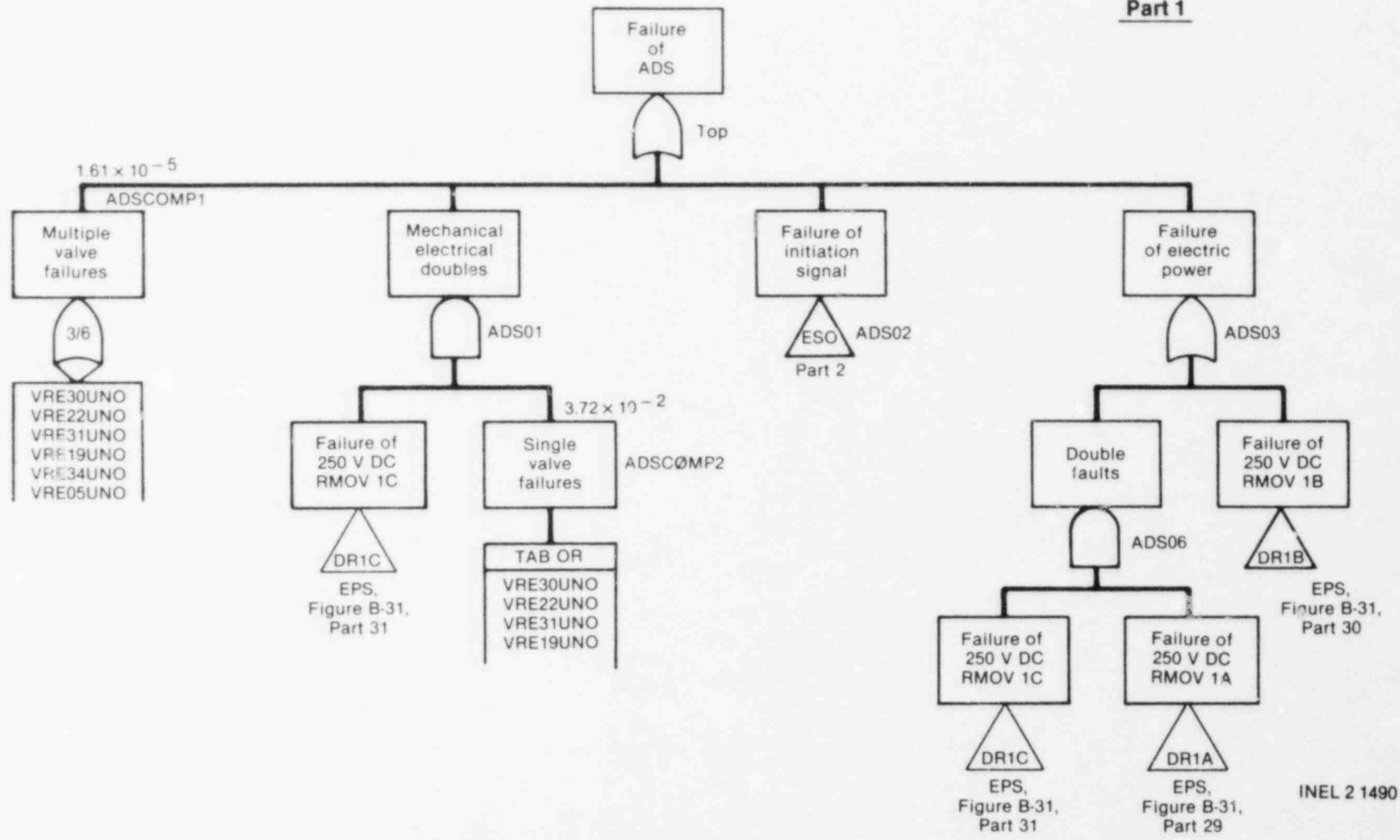
8×10^{-3} per demand (This value does not include command faults)

Total = 9.3×10^{-3}

VREXXUNO = 9.3×10^{-3} .

Basic Events. The information associated with the various basic events listed in the fault tree is summarized in the ADS fault summary short form, Table B-35. The failure associated with these basic events is summarized on Table B-36. Table B-37 lists the dominant cut sets for ADS unavailability.

Part 1

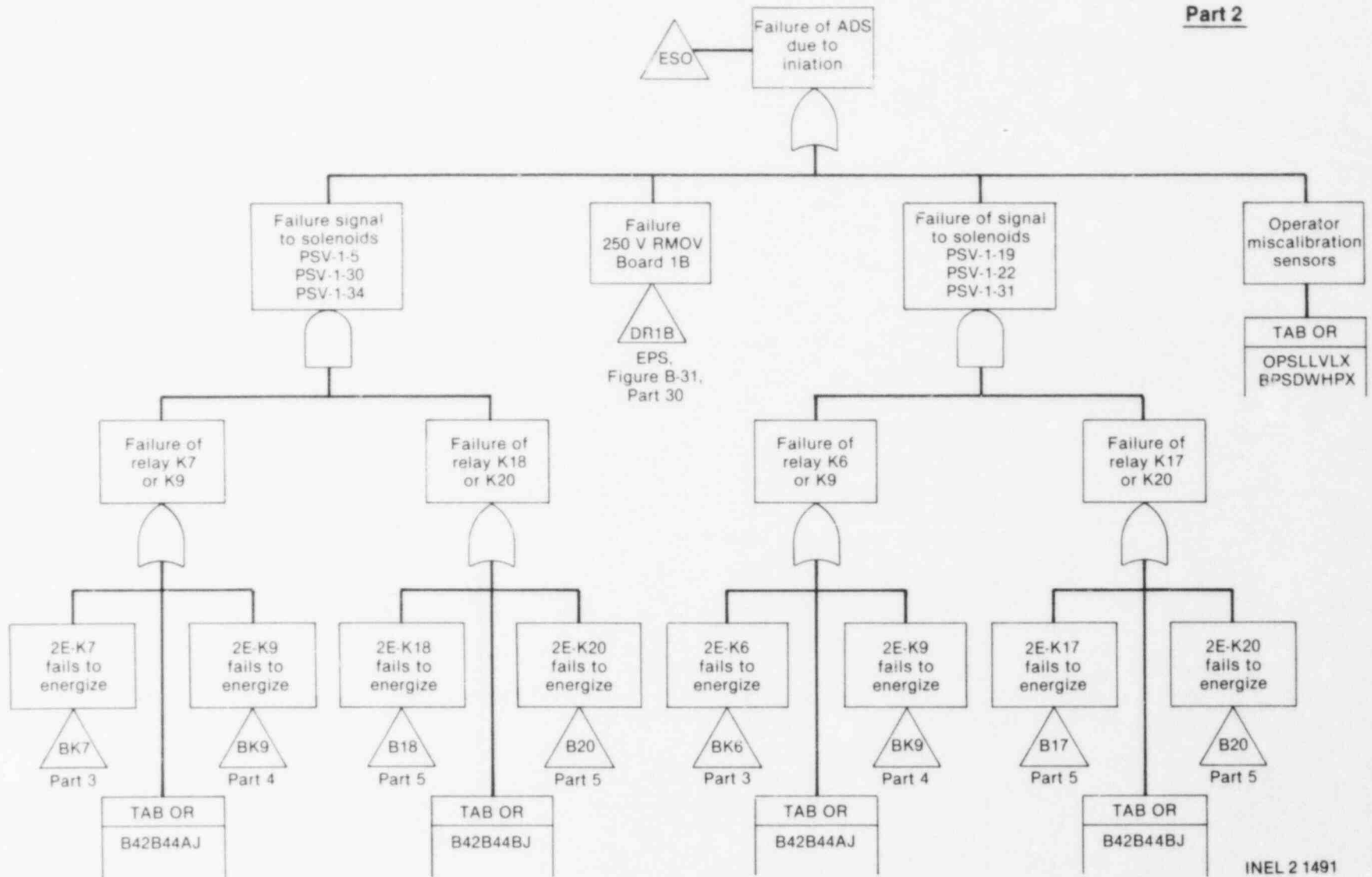


B-157

Figure B-14. ADS reduced fault tree.

INEL 2 1490

B-158



INEL 2 1491

Figure B-14. (continued).

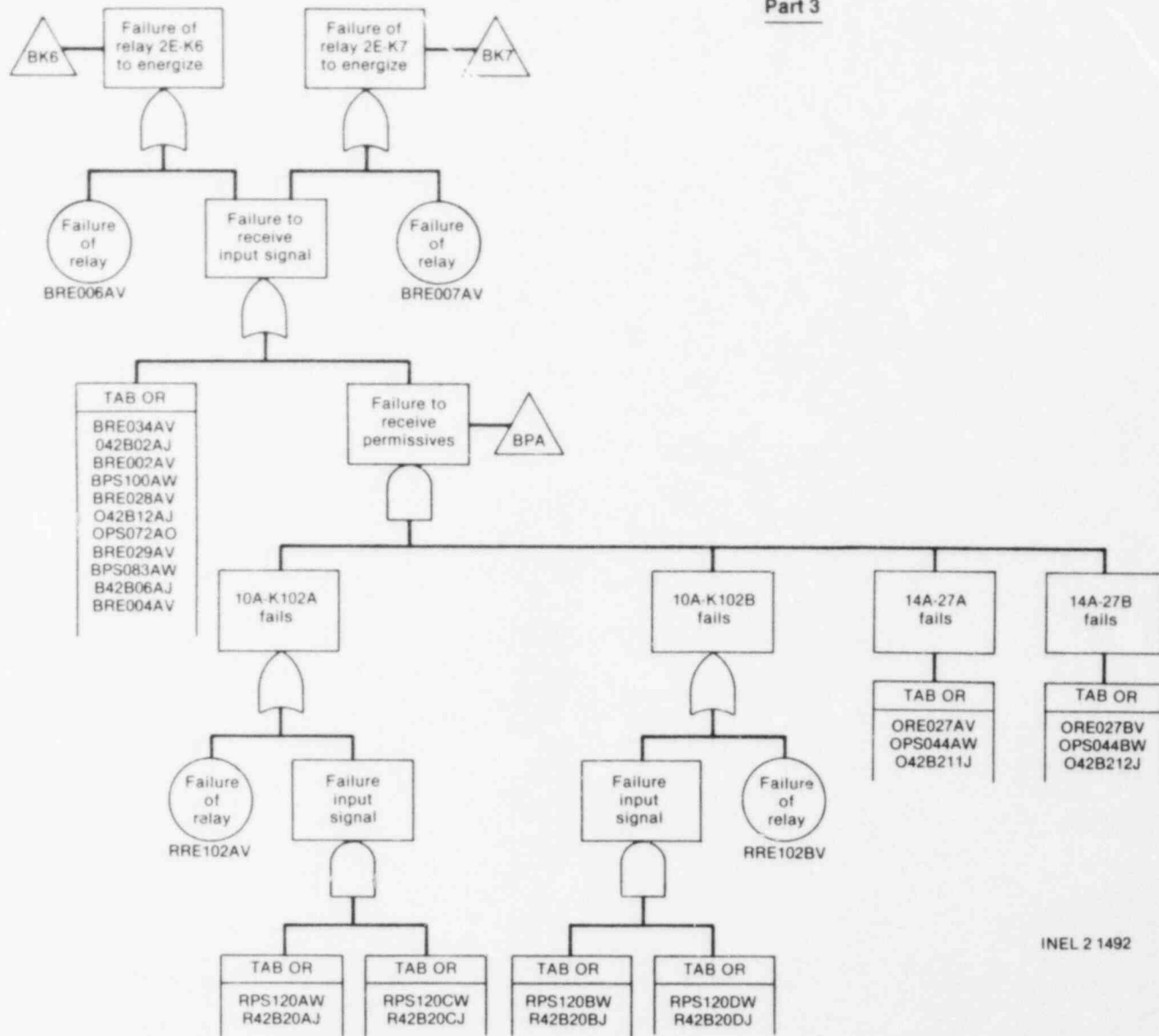
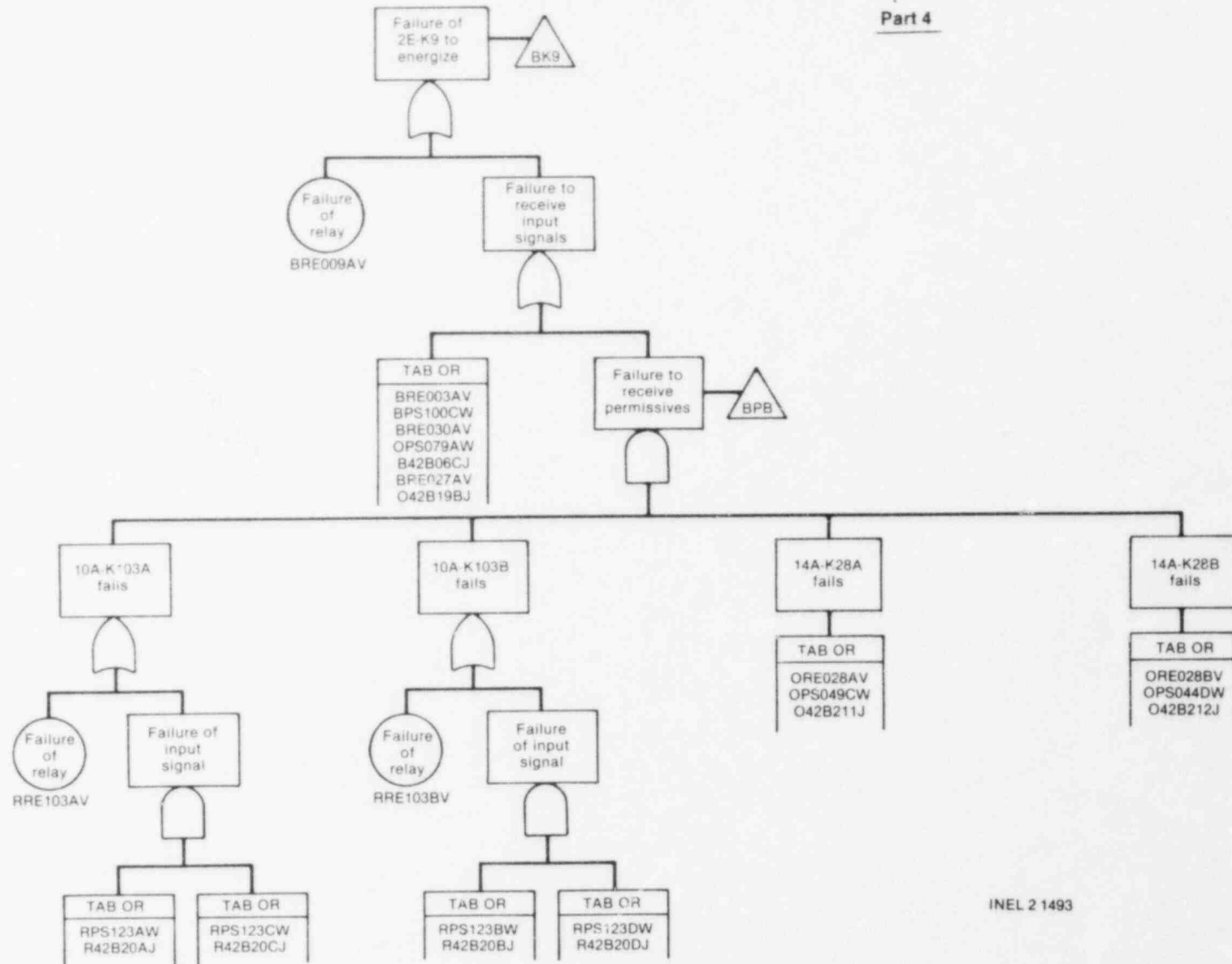


Figure B-14. (continued).

B-159

INEL 2 1492

B-160



INEL 2 1493

Figure B-14. (continued).

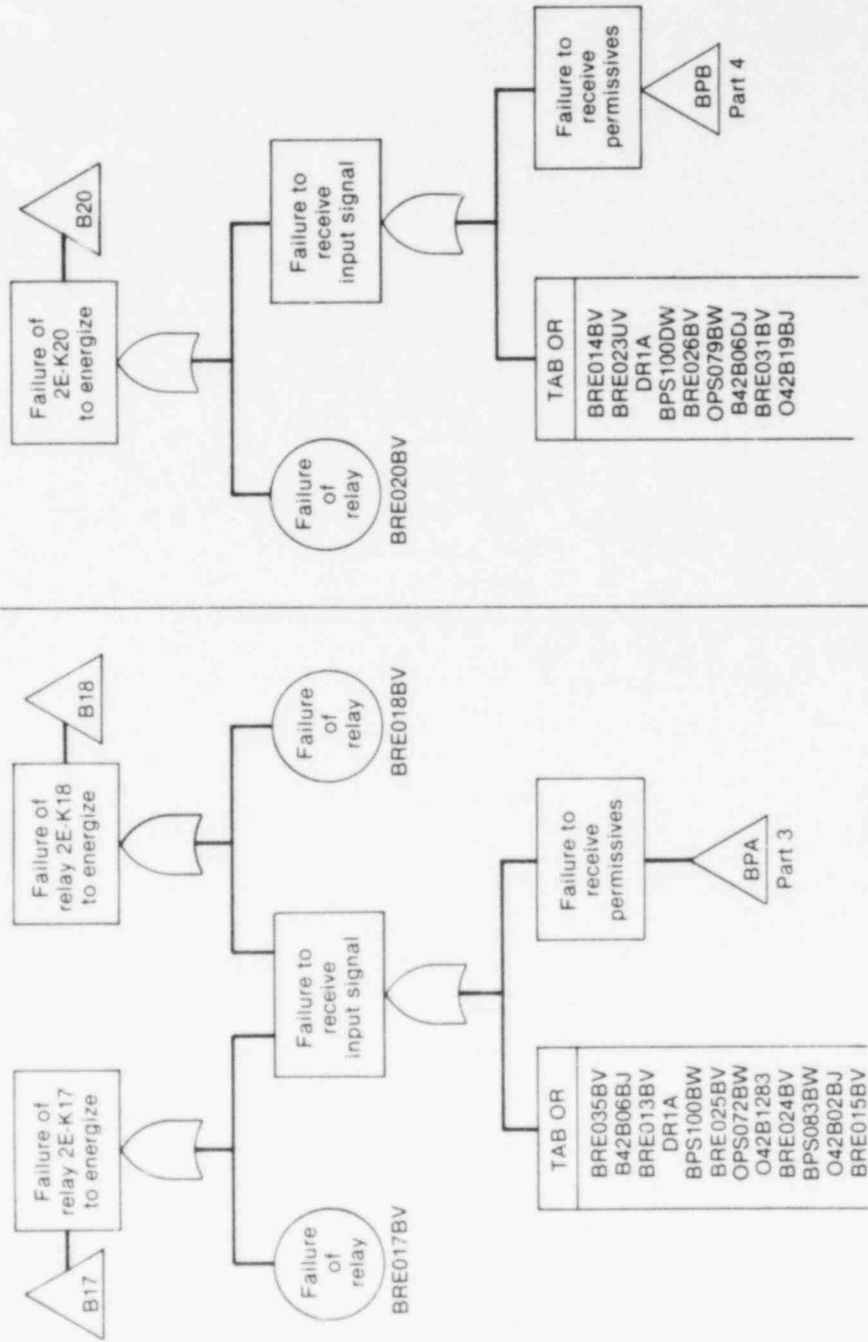


Figure B-14. (continued).

TABLE B-35. ADS FAULT SUMMARY SHORT FORM

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
BRE007AV	Relay 2E-K7	Does not energize	1E-4/D	--	3
BRE009AV	Relay 2E-K9	↓	↓	--	↓
BRE020BV	Relay 2E-K20			--	
BRE018AV	Relay 2E-K18			--	
BRE006AV	Relay 2E-K6			--	
BRE017AV	Relay 2E-K17			--	
BRE034AV	Relay 2E-K34			--	
BRE002AV	Relay 2E-K2			--	
BRE028AV	Relay 2E-K28			--	
BRE029AV	Relay 2E-K29			--	
BRE004AV	Relay 2E-K4			--	
BRE035BV	Relay 2E-K35			--	
BRE013BV	Relay 2E-K13			--	
BRE025BV	Relay 2E-K25	--			

B-162

TABLE B-35. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
BRE024BV	Relay 2E-K24	Does not energize	1E-4/D	--	3
BRE015BV	Relay 2E-K15	↓	↓	--	↓
BRE014BV	Relay 2E-K14			--	
BRE023UV	Relay 2E-K23			--	
BRE026BV	Relay 2E-K26			--	
BRE031BV	Relay 2E-K31			--	
BRE003AV	Relay 2E-K3			--	
BRE030AV	Relay 2E-K30			--	
BRE027AV	Relay 2E-K27			--	
RRE102AV	Relay 10A-K102A			--	
KRE102BV	Relay 10A-K102B			--	
ORE027AV	Relay 14A-K27A			--	
ORE027BV	Relay 14A-K27B			--	
RRE103AV	Relay 10A-K103A			--	

B-163

TABLE B-35. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RRE103BV	Relay 10A-K103B	Does not energize	1E-4/D	--	3
ORE028AV	Relay 14A-K28A	Does not energize	↓	--	↓
ORE028BV	Relay 14A-K28B	Does not energize		--	
BPS100AW	Pressure Switch 10-100A	Loss of function		--	
OPS072AW	Level Switch 2-3-72A	↓		--	
BPS083AW	Level Switch 2-3-83A			--	
BPS100BW	Pressure Switch 10-100B			--	
OPS072BW	Level Switch 2-3-72B			--	
BPS083BW	Level Switch 2-3-83B			--	
BPS100DW	Pressure Switch 10-100D			--	
OPS079BW	Level Switch 2-3-79B			--	
BPS100CW	Pressure Switch 10-100C			--	
OPS079AW	Level Switch 2-3-79A			--	
OPS044AW	Pressure Switch 14A-44A			--	

B-164

TABLE B-35. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
OPS044BW	Pressure Switch 14A-44B	Loss of function	1E-4/D	--	3
OPS044CW	Pressure Switch 14A-44C	↓	↓	--	↓
OPS044DW	Pressure Switch 14A-44D			--	
RPS120AW	Pressure Switch 10-120A			--	
RPS120CW	Pressure Switch 10-120C			--	
RPS120BW	Pressure Switch 10-120B			--	
RPS120DW	Pressure Switch 10-120D			--	
RPS123AW	Pressure Switch 10-123A			--	
RPS123BW	Pressure Switch 10-123B			--	
RPS123CW	Pressure Switch 10-123C			--	
042B02AJ	Level Switch LIS-3-184			Test	
042B12AJ	Level Switch LIS-3-58A	↓	1.4E-3	--	↓
B42B06AJ	Pressure Switch PS-64-57A		7E-4	--	
B42B06BJ	Pressure Switch PS-64-57B		7E-4	--	

B-165

TABLE B-35. (continued)

Event Name	Event Component	Failure Mode	Primary Failure			
			Failure Rate	Fault Duration (hr)	Error Factor	
042B12BJ	Level Switch LIS-3-58C	Loss of function	1.4E-3	--	0	
042B02BJ	Level Switch LIS-3-185	↓	2.8E-3	--	↓	
B42B44AJ	Pressure Switch Pump A and C discharge		9E-4	--		
B42B44BJ	Pressure Switch Pump B and D discharge		9E-4	--		
B42B06DJ	Pressure Switch PS-64-57D		7E-4	--		
042B19AJ	Level Switch LIS-3-58D		1.4E-3	--		
B42B06CJ	Pressure Switch PS-64-57C		7E-4	--		
042B19BJ	Level Switch LIS-3-58B		Test	1.4E-3		--
042B211J	Pressure Switch Pump A and C discharge		9E-4	--		
042B212J	Pressure Switch Pump B and D discharge		9E-4	--		
R42B20AJ	Pressure Switch PS-74-8 A and B		1.4E-3	--		
R42B20CJ	Pressure Switch PS-74-31 A and B	1.4E-3	--			

B-166

TABLE B-35. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
R42B20BJ	Pressure Switch PS-74-19 A and B	Test	1.4E-3	--	0
R42B20DJ	Pressure Switch PS-74-42 A and B	Test	1.4E-3	--	0
OPSLLVLX	Core spray reactor low level switches	Operator miscalibration	2.4E-6/D	--	10
BPSDWHPX	ADS drywell high pressure switches	Operator miscalibration	2.9E-4/D	--	10

B-167

TABLE B-36. ADS FAILURE DATA SUMMARY

Component/ Activity (Code)	Failure Mode (Code)	Failure Probability (λ)	Unavailability (A)	Remarks
Relief valve (VREXXUNO)	Does not open	--	9.3E-3	See ADS, Section 2.4.4, "Fault Tree" discussion
Relay (RE)	Does not energize (V)	1E-4/D	1E-4	--
Pressure or level switch (PS)	Loss of function (W)	1E-4/D	1E-4	--
Core spray level switches (042B12_J) (042B19_J)	Maintenance	--	2.8E-3 1.4E-3 1.4E-3	--
ADS pressure switch (B42B06_J)	Maintenance	--	7E-4	--
RHR pressure (R42B20_J)	Maintenance	--	1.4E-3	RHR pump discharge
Core spray pump discharge pres- sure switch (042B21_J)	Calibration	--	9E-4	See core spray, Table B-39
ADS logic bus test (B42B44_J)	Test	--	9E-4	See ADS, Section 2.4.2, "Testing" discussion
Core spray low level switches (OPSLVLX)	Operator miscalibrates	--	2.4E-6	See Section 4
ADS drywell pressure switches (BPSDWHPX)	Operator miscalibrates	--	2.9E-4	Similar to core spray drywell switch model in Section 4

TABLE B-37. ADS CUT SETS

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
2.9E-4	89.7	BPSDWHPX	No
1.6E-5	<u>4.9</u>	ADSCOMP1	No
Cumulative importance	94.6		

2.5 Safety Relief Valves

2.5.1 Purpose

The reactor and the steam system are protected from overpressure by 13 relief valves. The 13 valves are distributed among the four main steam lines, located upstream of the main steam isolation valves. Each valve is individually piped to release to the suppression pool. The safety valves are designed to maintain at all times primary system pressure below the emergency stress limit of 1350 psig.

This section describes the overpressure relief function of the valves. Automatic depressurization is discussed in Section 2.4. Manual depressurization is discussed in Section 2.6.

2.5.2 System Configuration

Overall Configuration. Bf1 has 13 identical Target Rock two-stage safety relief valves. When operating in the overpressure relief mode, the valves are pilot-operated by the self-contained pilot valve. The valves are set as follows: five valves at 1105 psig, four valves at 1115 psig, and four valves at 1125 psig.

At their rated setpoints, the 13 valves provide a total relief capacity of 74% of rated steam flow.

System Interface. The valves are entirely self-actuated in the overpressure relief mode. Interfaces for these valves are shown in Table B-34.

Instrumentation and Control. The valves are self-actuated and have no control system. There is no instrumentation essential to their operation.

Testing. Valves cannot be tested during plant operation. Valves are tested for setpoint accuracy at each refueling outage.

Maintenance. Valves cannot be maintained during plant operation.

Technical Specification Limitations. Technical specifications require that the plant be shut down and depressurized within 24 hours if just one safety relief valve is known to be inoperable in the overpressure relief mode.

2.5.3 Operation

Operation is totally automatic in the overpressure relief mode. Valves will open at their setpoint and remain open until pressure is 100 psi below the setpoint.

2.5.4 Fault Tree

The relief valves appear in two events on the event trees (see Appendix A): Events J and K.

Success/Failure Criteria. The success criteria for the valves are derived from Appendix U of the FSAR and are:

Event J

With turbine bypass available:

Direct Scram	No valves needed
Flux scram	No valves needed
Pressure scram	No valves needed

With turbine bypass unavailable:

Direct Scram	2 of 13 valves
Flux scram	7 of 13 valves
Pressure scram	10 of 13 valves

Event K

All valves that open must close. Due to the proximity of the valve setpoints, it was assumed that, if the pressure reaches the setpoint of any valve, all valves will open, although fewer than 13 valves are required to limit the pressure to less than 1350 psig. Therefore, all 13 valves must reclose for all transients in which the pressure reaches the relief valve setpoint. In addition, for transients where the PCS is unavailable, some relief valves may reopen after the first pressure surge has been relieved. It is estimated, based on the transient analysis of the main steam isolation valve closure in Chapter 14 of the FSAR, that pressure relief from six more valve openings may occur (in stages of three then two then one). Therefore, the total number of valve reclosures for this event when the PCS is unavailable is 19.

Major Assumptions. The following major assumptions were used in the analysis of the relief valves.

1. Operation of the safety valves is entirely automatic in the overpressure relief mode. No time is available for operator action.
2. When PCS is available, the valves have an initial demand at the time of scram. If heat can be removed by the PCS and, consequently, pressure can be controlled, there are no subsequent demands on the relief valves.
3. When PCS is unavailable, there are demands on the relief valves subsequent to the initial demand at scram. As steam is continually generated by decay heat, the increasing pressure will require periodic release to the suppression pool. One valve has sufficient capacity to provide this function. During this mode of operation, it is likely the operator will manually activate the valves per Browns Ferry EOI-4. This Emergency Operating Instruction (EOI) directs the operator to relieve vessel pressure to 850 psi. In so doing, the operator depressurizes the vessel to a point low enough that the valves will not continually cycle in the self-actuation mode. Based on transient analysis contained in FSAR Chapter 14, a demand of six openings in 8 hours was derived.

Fault Tree. Because operation of the relief valves is totally self-contained, it is not necessary to construct a fault tree. Operation of each valve is independent of the other valves and all other plant components. The probability of Event J is determined by the binomial expression for x successes in 13 trials, where x is the number of valves required. Event K is the number-of-open-valves times the valve-fail-to-close-rate.

For transients where the PCS is unavailable there are three criteria for overpressure protection failure (J) depending upon which type of scram occurred. For direct scrams, 12 of 13 valves must fail. There are 13 combinations of valves for this case. If the direct scram fails then 7 of 13 valves must fail after a flux scram occurs: there are 1716 combinations of valves for this case. If both the flux and direct scrams fail but the pressure scram succeeds, then 4 of 13 valves must fail; there are 715 combinations of valves for this case. The value for independent valve failure rate is 1×10^{-2} per demand. The value for the conditional probabilities of direct, flux, or pressure scrams, given that a successful scram occurs, are 0.95 for direct, 0.049 for flux, and 0.001 for pressure scrams. These values are based on engineering judgement taking in to account the plant response to the initiators for transient where the PCS is unavailable. Therefore, the unavailability of overpressure protection is equal to the sum of the conditional probabilities given above:

$$\begin{aligned}
 Q(J) &= Q(\text{direct}) + Q(\text{flux}) + Q(\text{pressure}) \\
 &= 13(0.95)(1 \times 10^{-2})^{12} + (0.049)(1716)(1 \times 10^{-2})^7 \\
 &\quad + (1 \times 10^{-3})(715)(1 \times 10^{-2})^4
 \end{aligned}$$

$$Q(J) = \epsilon + \epsilon + 7.2 \times 10^{-9}$$

$$Q(J) = 7.2 \times 10^{-9}.$$

For overpressure protection failure (K), the unavailability is merely the individual valve-failure-to-reclose-rate (3×10^{-3} per demand) times the number-of-valves-that-must-close:

$$Q(K) = 13(3 \times 10^{-3})$$

$$= 3.9 \times 10^{-2} \quad \text{for } T_A \text{ initiator}$$

$$Q(K) = 19(3 \times 10^{-3})$$

$$= 5.7 \times 10^{-2} \quad \text{for } T_U \text{ and } T_P \text{ initiators.}$$

For transients with PCS available, this number is 13; for others, it is 19.

2.6 Manual Depressurization

2.6.1 Purpose

Manual depressurization of the reactor is accomplished by the operator opening the safety relief valves whenever the high pressure makeup systems are unable to maintain reactor water level following a transient.

2.6.2 System Configuration

Overall Configuration. BFl has 13 two-stage Target Rock relief valves. As previously described, six of these valves are designed for automatic operation upon coincident signals of low reactor water level, high drywell pressure, and LPCI/core spray pumps operating. However, manual activation of the relief valves will be required for transients since the high drywell pressure condition will not be present. All 13 relief valves have the capability of being actuated from the control room.

System Interface. The system interfaces for the 13 relief valves are contained in Table 34.

2.6.3 Fault Tree

The manual depressurization action is depicted as Event V in the transient systemic event trees (see Appendix A).

Success/Failure Criteria. Opening of any 4 of the 13 safety relief valves constitutes successful depressurization of the reactor.

Major Assumptions. Manual depressurization failure analysis was developed from human error considerations only. Mechanical and electrical faults associated with the safety relief valves opening was not considered to be a significant contributor to system failure.

Fault Tree. The human error model for manual depressurization via the relief valves is addressed in Section 4.2. Assumptions and results of failing to manually depressurize are also contained in Section 4.2.

2.7 Core Spray System

During a postulated accident, steam is generated by residual and decay heat. For a small break, if the feedwater system does not operate, the reactor vessel depressurizes slowly, and the HPCI system or the RCIC system is designed to inject sufficient coolant in time to prevent uncovering the core. When the pressure in the reactor vessel decreases to 500 psig, the core spray system is designed to begin pumping water from the suppression pool into the core region of the reactor vessel, with rated flow delivered at reactor pressure less than 350 psig.

For large breaks, the reactor will depressurize very quickly and the core spray system is designed to spray the core at full flow within 12 sec after reactor pressure drops below 500 psig.

2.7.1 Purpose

The core spray system along with its control and instrumentation is one of several emergency core cooling systems (ECCS) used to inject coolant onto the reactor core following an accident (pipe break) or an operational transient. The core spray system is designed to prevent excessive fuel cladding temperature for a pipe break of up to 4 ft² by spraying water onto the reactor core. The core spray system is to function with a complete loss of offsite power (LOSP).

2.7.2 System Configuration

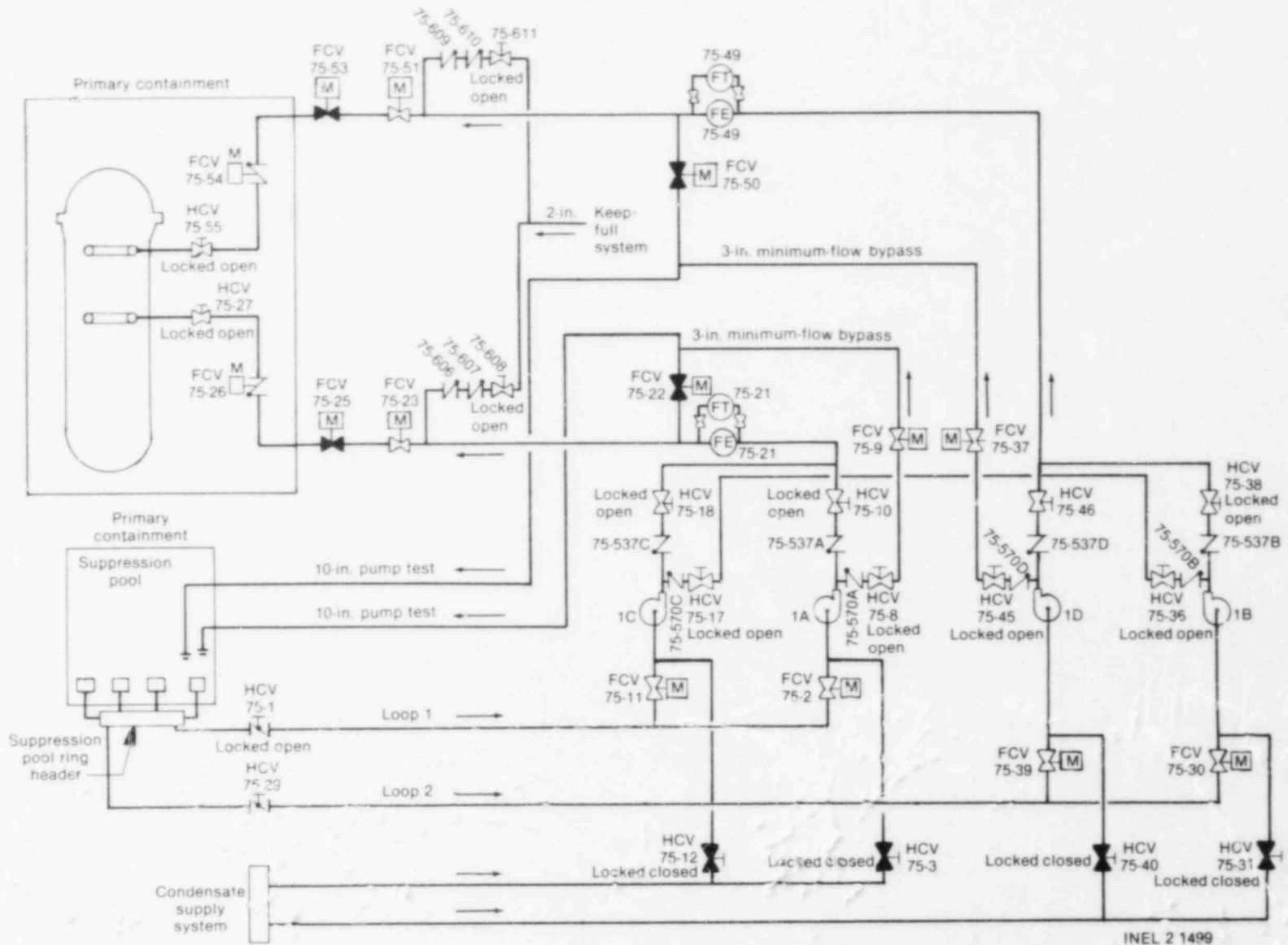
Overall Configuration. The core spray system consists of four pumps divided into two parallel systems that are identical and are physically and electrically independent from each other. Each system contains two 50%-capacity, AC-motor-driven centrifugal pumps; core spray sparger; and interconnecting pipes and valves.

The pump configuration for the core spray systems is:

<u>Core Spray System</u>	<u>Pumps</u>
Loop I	1A and 1C
Loop II	1B and 1D

The pumps are connected in parallel. With only one pump operating in a loop, the core spray system will not deliver the required flow to those fuel assemblies located near the vertical centerline of the core. The core spray system is shown in Figure B-15.

B-174



INEL 2 1499

Figure B-15. Core spray system.

Except where otherwise specified, the remainder of the description of the core spray system refers to one spray loop; the remaining spray loop is identical. All equipment is located outside of primary containment in the reactor building, with the exception of the testable check valve and a locked-open manual isolation valve. The 360 deg spray sparger is located within the core shroud and is split into two 180 deg segments. Nozzles on the spray sparger direct the water onto the core. The testable check valve inside the drywell is air operated, providing periodic testing capability from Panel 9-3 in the main control room (MCR). The check valve is designed with a free-floating disk to ensure that the valve will open in the event of emergency injection regardless of the position of the air operator. The locked-open manual isolation valve located in the drywell has position indication displayed on Panel 9-3 in the MCR. This valve is used for maintenance purposes only.

Two AC-motor-operated injection valves, inboard and outboard, allow testing of the injection valves. The inboard injection valve (FCV-75-25 for Loop I and FCV-75-53 for Loop II) is a normally closed valve. The inboard injection valve automatically opens on receipt of an initiation signal and reactor vessel pressure less than, or equal to, 450 psig. The valve cannot be opened from the MCR unless reactor vessel pressure is less than 450 psig, or the outboard injection valve is shut. The outboard injection valve (FCV-75-23 for Loop I and FCV-75-51 for Loop II) is a normally open valve and (a) automatically opens if closed upon receipt of an initiation signal and reactor vessel pressure less than 450 psig, and (b) is interlocked open until the logic is reset.

An AC-motor-operated test valve (FCV-75-22 for Loop I and FCV-75-50 for Loop II) is provided to allow for full-flow testing of the spray loop. The test valve automatically closes and is interlocked closed upon receipt of an initiation signal. The minimum-flow bypass line diverts discharge water from the core spray loop pumps back to the suppression pool to protect the pumps from operating at full shutoff head. The AC-motor-operated valve (FCV-75-9 for Loop I and FCV-75-37 for Loop II) in the bypass line is a normally open valve that closes when discharge flow from the pumps increases to at least 1250 gpm and reopens on decreasing flow of less than 600 gpm. The flow signal for opening and closing of the minimum-flow bypass valve comes from a flow transmitter located in the common injection path from the discharge of both loop pumps.

The core spray pumps are vertical, single-stage pumps. Each pump is rated at 50% capacity (3125 gpm) and is driven by a 600 hp motor. The pumps are located in the basement of the reactor building to ensure that water from the suppression pool maintains the net positive-suction-head requirements. Core spray system Loop I pumps are located in the northwest quadrant of the reactor building, while core spray Loop II pumps are located in the northeast quadrant.

The pump suction valve (FCV-75-30 for Pump 1B, FCV-75-39 for Pump 1D, FCV-75-2 for Pump 1A, FCV-75-11 for Pump 1C) is an AC-motor-operated valve that is normally open and alarms in the MCR if the valve is closed. The common suction header to both loop pumps contains a locked-open manual isolation valve (HCV-75-1 for Loop I and HCV-75-29 for Loop II). Position indication of this valve is displayed in the MCR. Normal suction for the

core spray loop pumps is from the suppression pool via the ECCS suction header. There are four suction lines from the suppression pool to the ECCS suction header.

Stainless-steel screens are provided on each line from the suppression pool to the ECCS suction header to prevent plugging of the core spray sparger nozzles. The screens are also located above the bottom of the suppression pool to minimize plugging. The flow area of the four suction lines are sized for combined, simultaneous, full-flow requirements of HPCI, LPCI, and core spray with one suction screen completely plugged. Alternate suction for the core spray loop pumps is from the CST through locked-closed manual isolation valves.

System Interfaces. The core spray system interfaces with the EPS, EECW system, EAC system, and the keep-full system. Lubrication and cooling are integral to the core spray motor and pump bearings. System interactions that could affect availability are shown in Table B-38. The core spray pump motors receive power from the 4160 V AC shutdown buses, while the motor-operated valves receive power from the 480 V AC reactor MOV buses.

The EECW system provides cooling water to room air coolers located in the pump rooms. The EAC system consists of fans located in the respective pump rooms that circulate room air to cool the core spray pump motors. The keep-full system is designed to keep full of water the discharge piping from the pump check valve to the normally closed inboard injection valve.

Instrumentation and Control. The controls and instrumentation for the core spray system include the sensors, relays, wiring, and valve-operating mechanisms used to start, test, and operate the system. Except for the testable check valve in each spray loop, the sensors and valve-closing mechanisms for the core spray system are located in the reactor building. Logic control power for each of the core spray loops comes from separate 250 V DC reactor MOV buses. Figure B-16 is a diagram of the core spray initiation circuitry.

The signals used to initiate the core spray system are: (a) low-low reactor water level (470 inches), or (b) high drywell pressure (+2 psig) concurrent with low reactor vessel pressure (less than, or equal to, 450 psig).

These signals are sealed in and have to be manually reset when the initiating condition has cleared.

Upon receipt of a low reactor water level initiation signal, the following events occur:

1. The test valves (FCV-75-22 for Loop I, and FCV-75-50 for Loop II) are closed, if open, and are interlocked closed to prevent opening.

2. If normal AC power is available, the four core spray pumps start one at a time in the following order:

<u>Pump</u>	<u>Time (sec)</u>
1A	0
1B	7
1C	14
1D	21

3. If normal AC power is not available, all four core spray pumps start immediately 7 sec after standby power (diesel generators) becomes available. (The LPCI pumps start as soon as standby power is available.)
4. When reactor pressure drops to 450 psig, the inboard injection valves open and water is sprayed on the core.
5. When core spray loop flow increases to 1250 gpm, the minimum-flow bypass valve closes, directing full loop flow to the core.
6. The core spray pumps are stopped by placing the control room switch in the "stop" position. The pumps will not start automatically unless the logic is reset.

The same sensors that initiate core spray also initiate the LPCI system.

Testing. Surveillance testing of the core spray components is performed on a scheduled basis. Only those tests that are done while the reactor is critical are considered for this analysis. Table B-39 is a summary of the surveillance testing done on the core spray system while the reactor is critical.

The simulated automatic actuation test provides verification that a simulated actuation signal will automatically start the system and correctly position the proper valves for injecting water into the reactor vessel. The system flow test is conducted to insure the capability of the core spray loops to pump ≥ 6250 gpm at a system head pressure corresponding to a 105 psig differential between the reactor vessel and the primary containment. The pump operability test consists of starting the pumps through the minimum-flow line. The motor-operated valve operability test consists of cycling and timing the valves in the system.

The system flow test, pump operability test, and the motor operated valve operability were excluded from the core spray system analysis since these tests do not result in the system being unavailable if an initiation signal is received.

Maintenance. Maintenance is performed on the core spray system only on an as-needed basis while the reactor is critical. Maintenance on the pumps is the only activity done on a scheduled routine. Once every 2 years the oil is changed on each pump. Table B-40 summarizes this maintenance activity.

TABLE B-38. CORE SPRAY SYSTEM FMEA OF COMPONENT/SUPPORTING-SYSTEM INTERACTIONS

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
CS Division II system logic	250 V DC	RMOV Board-1A	No power to board; breaker open	No FC power to CS Division II	No auto-initiation of CS Loop II
FCV-75-53 (inboard MOV)	480 V AC	RMOV Board-1B	No power to board; breaker open	Valve fails to open as required	No flow through Loop II
	Control signal	Relay 14A-K13B	No signal	Valve remains closed unless manually opened	No flow through Loop II
FCV-75-51 (outboard MOV)	480 V AC	RMOV Board-1B	No power to board; breaker open	Valve remains in normal position	Valve is normally open and need not change position for successful CS
	Control signal	Relay 14A-K13B	No signal	Valve remains in normal position	Valve is normally open and need not change position for successful CS
FCV-75-39	480 V AC	RMOV Board-1B	No power to board; breaker open	Valve remains in normal position	Valve is normally open and need not change position for successful CS
	Control signal	Manually controlled HS-75-39	No signal	Valve remains in normal position	Valve is normally open and need not change position for successful CS
FCV-75-30	480 V AC	RMOV Board-1B	No power to board; breaker open	Valve remains in normal position	Valve is normally open and need not change position for successful CS
	Control signal	Manually controlled HS-75-30	No signal	Valve remains in normal position	Valve is normally open and need not change position for successful CS
CS Division I system logic	250 V DC	RMOV Board-1B	No power to board; breaker open	No DC power to CS Division I	No auto-initiation of CS Loop I
FCV-75-25 (inboard MOV)	480 V AC	RMOV Board-1A	No power to board; breaker open	Valve fails to open as required	No flow through Loop I
	Control signal	Relay 14A-K13A	No signal	Valve remains closed unless manually opened	No flow through Loop I
FCV-75-23 (outboard MOV)	480 V AC	RMOV Board-1A	No power to board; breaker open	Valve remains in normal position	Valve is normally open and need not change position for successful CS
	Control signal	Relay 14A-K13A	No signal breaker open	Valve remains in normal position	Valve is normally open and need not change position for successful CS
FCV-75-11	480 V AC	RMOV Board-1A	No power to board; breaker open	Valve remains in normal position	Valve is normally open and need not change position for successful CS

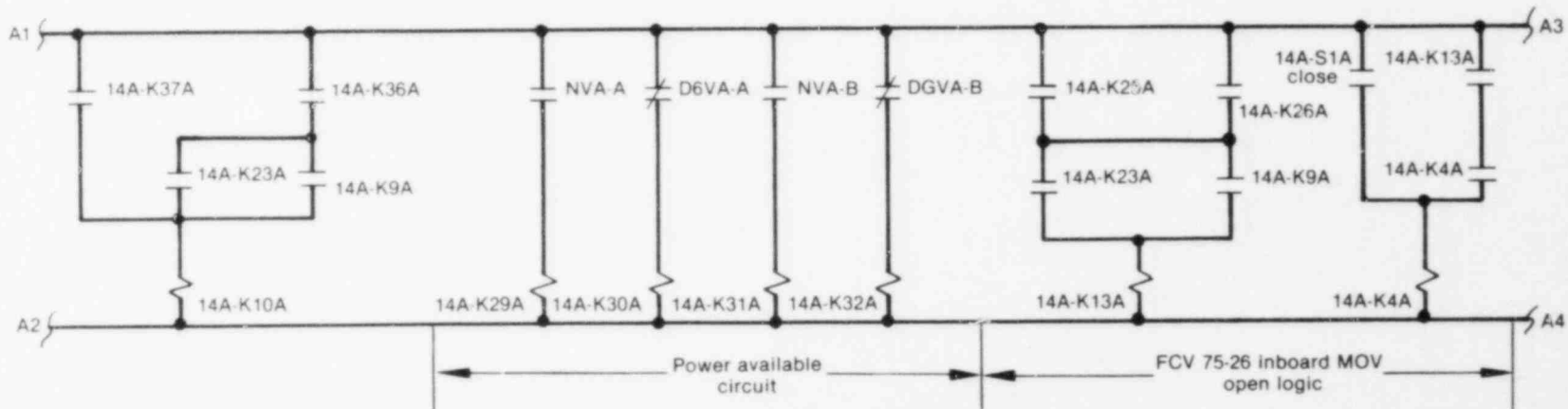
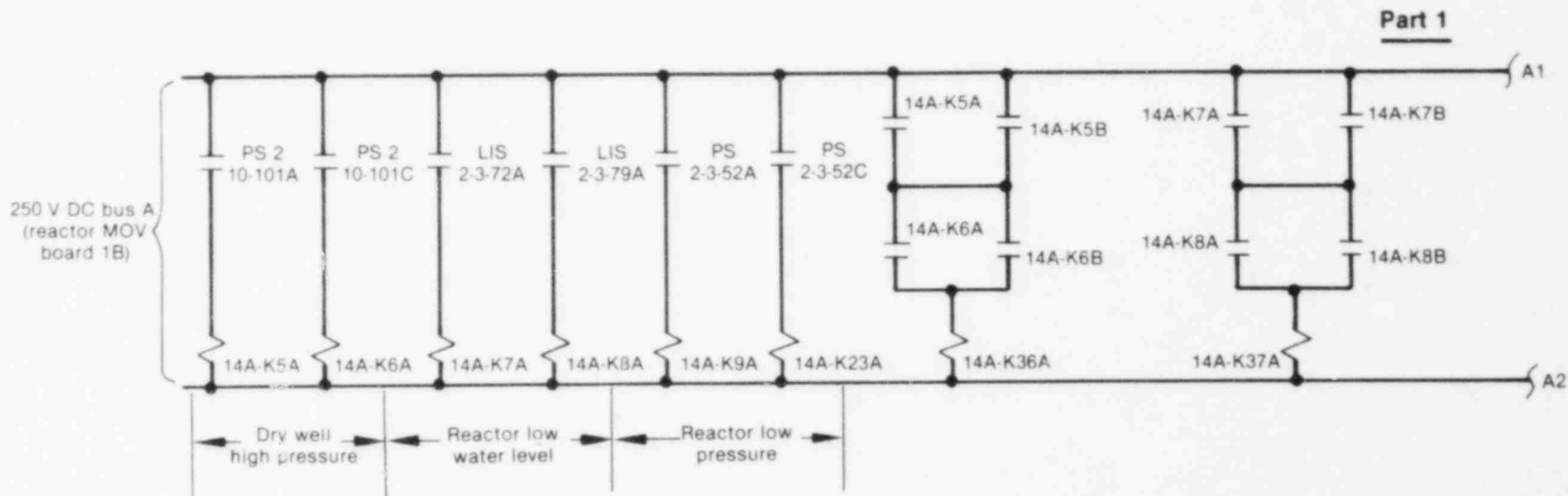
B-178

TABLE B-38. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
FCV-75-2	Control signal	Manually controlled HS-75-11	No signal	Valve remains in normal position	Valve is normally open and need not change position for successful CS
	480 V AC	RMOV Board-1A	No power to board breaker open	Valve remains in normal position	Valve is normally open and need not change position for successful CS
CS Pump B	Control signal	Manually controlled HS-75-2	No signal	Valve remains in normal position	Valve is normally open and need not change position for successful CS
	4160 V AC	SD-BD-C	No power to board breaker open	Pump will not start as required	Insufficient CS from CS Loop II
	250 V DC control	Distribution Panel SB-B	No power to board	Pump circuit breaker will not close	Insufficient CS from CS Loop II
	Control signal	Relay 14A-K12B	No signal	Pump will not auto-start as required	Pump can be manually started
CS Pump D	EECW	CS room cooler heat Exchanger B and D	Rupture Plug	Once started, pump may fail to run for long duration	Pump may overheat if run for extended time
	EAC	CS cooler Fan B and D	Fails to run	Once started; pump may fail to run for long duration	Pump may overheat if run for extended time
	4160 V AC	SD-BD-D	No power to board; breaker open	Pump will not start as required	Insufficient CS from CS Loop II
CS Pump A	250 V DC control	Distribution Panel SB-D	No power to board	Pump circuit breaker will not close	Insufficient CS from CS Loop II
	Control signal	Relay 14A-K14B	No signal	Pump will not auto-start as required	Pump can be manually started
	EECW	CS room cooler heat Exchanger B and D	Rupture Plug	Once started, pump may fail to run for long duration	Pump may overheat if run for extended time
	EAC	CS cooler Fan B and D	Fails to run	Once started, pump may fail to run for long duration	Pump may overheat if run for extended time
CS Pump A	4160 V AC	SD-BD-A	No power to board; breaker open	Pump will not start as required	Insufficient CS from CS Loop I
	250 V DC control	Distribution Panel SB-A	No power to board	Pump circuit breaker will not close	Insufficient CS from CS Loop I

TABLE B-38. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
CS Pump C	Control signal	Relay 14A-K12A	No signal	Pump will not auto-start as required	Pump can be manually started
	EECW	CS room cooler heat Exchanger A and C	Rupture Plug	Once started, pump may fail to run for long duration	Pump may overheat if run for extended time
	EAC	CS cooler Fan A and C	Fails to run	Once started, pump may fail to run for long duration	Pump may overheat if run for extended time
	4160 V AC	SD-BD-B	No power to board breaker open	Pump will not start as required	Insufficient CS from CS Loop I
	250 V DC control	Distribution Panel SB-C	No power to board	Pump circuit breaker will not close	Insufficient CS from CS Loop I
	Control signal	Relay 14A-K14A	No signal	Pump will not auto-start as required	Pump can be manually started
	EECW	CS room cooler heat Exchanger A and C	Rupture Plug	Once started, pump may fail to run for long duration	Pump may overheat if run for extended time
	EAC	CS cooler Fan A and C	Fails to run	Once started, pump may fail to run for long duration	Pump may overheat if run for extended time

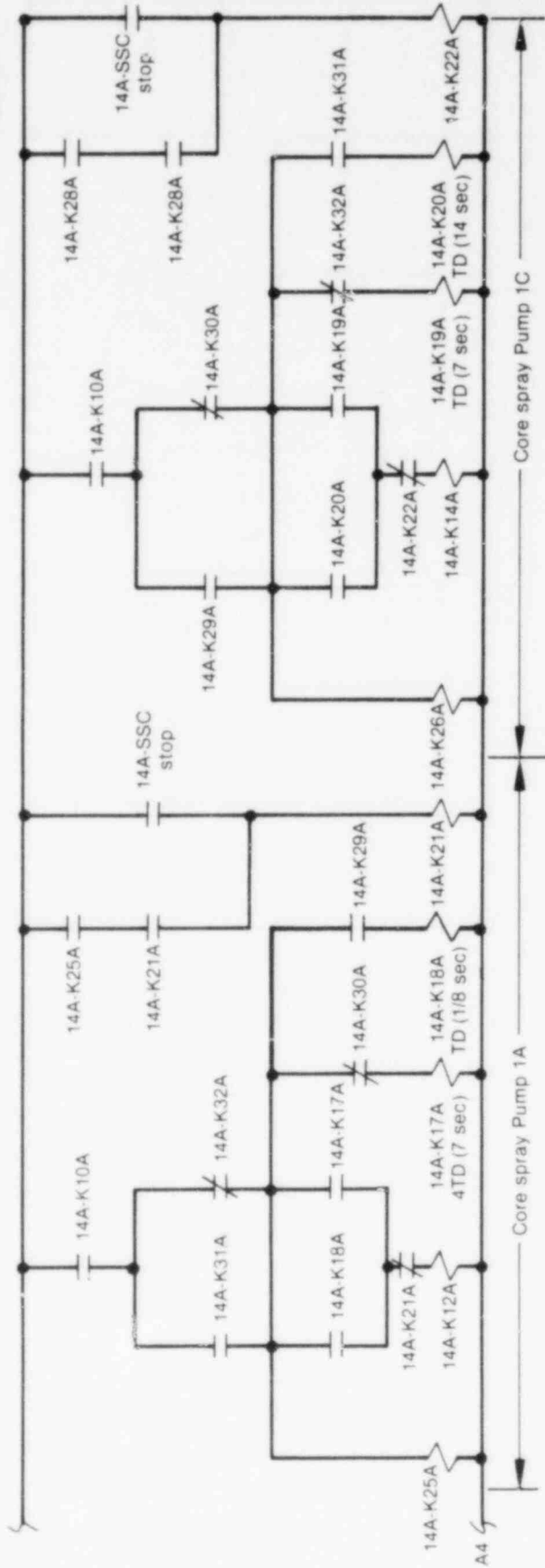


NVA-A closed when normal auxiliary power available at Bus A
 NVA-B closed when normal auxiliary power available at Bus B
 DGVA-A open when diesel generator power available at Bus A
 DGVA-B open when diesel generator power available at Bus B

INEL 2 1522

Figure B-16. Core spray initiation circuitry.

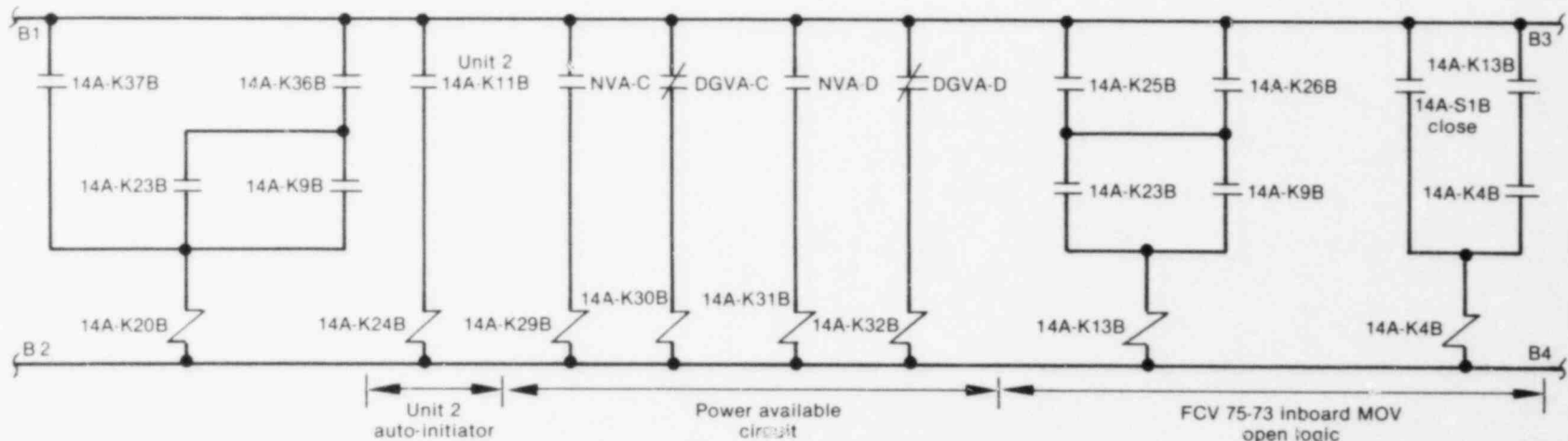
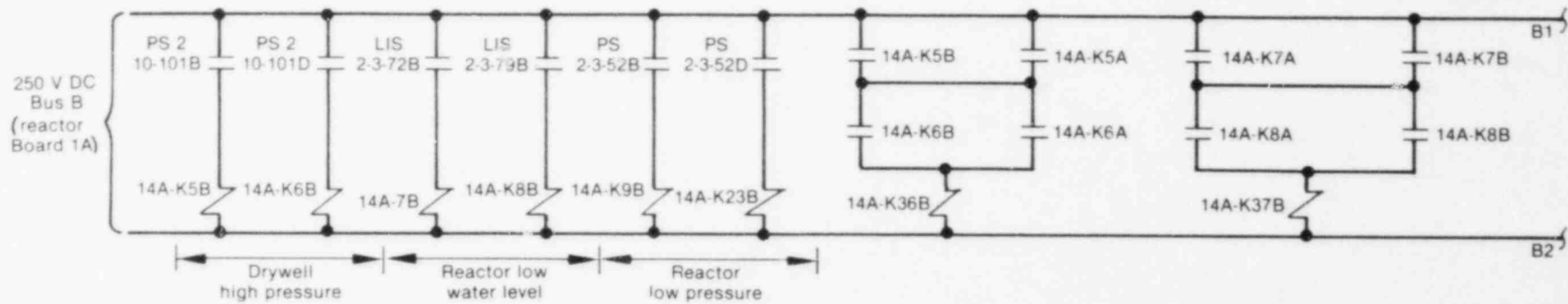
Part 2



INEL 2 1523

Figure B-16. (continued).

Part 3

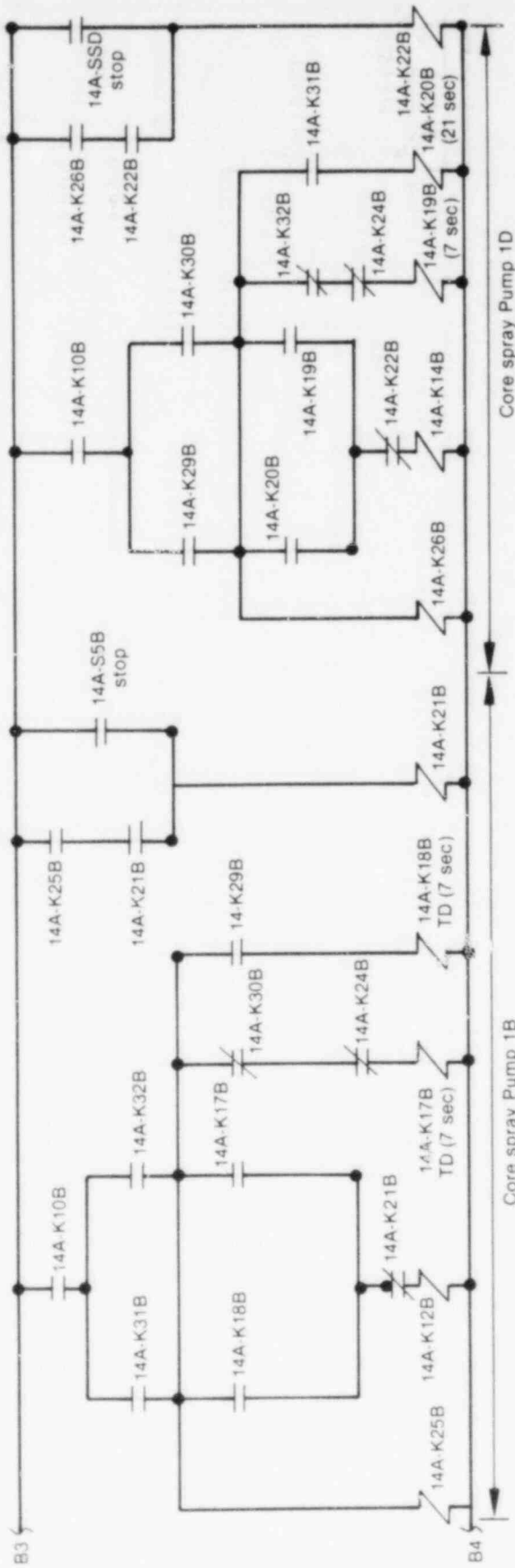


NVA-C closed when normal auxiliary power available at Bus C
 NVA-D closed when normal auxiliary power available at Bus D
 DGVA-C open when diesel generator power available at Bus C
 DGVA-D open when diesel generator power available at Bus D

B-183

Figure B-16. (continued).

Part 4



INEL 2 1525

Figure B-16. (continued).

TABLE B-39. CORE SPRAY SYSTEM TEST REQUIREMENTS SUMMARY

Component Undergoing Test	Type of Test	Test Procedure Number	Components Aligned Away from Engineered Safeguards Position for Test	Expected Test Frequency	Expected Test Outage Time	Remarks
Core spray Loop I simulated automatic actuation test (0S45A11J)	Functional	SI 4.5.A.1.a	FCV-75-25 breaker opened FCV-75-23 closed (FCV-75-23 breaker opened later on in test to verify FCV-75-25 operability)	Once every operating cycle ^a	4 hr	A technician is in continuous communication with control room and observer stationed at FCV-75-25; with FCV-75-25 inoperable, all core spray protection is lost in event of simultaneous Unit 2 core spray initiation and loss of normal auxiliary power
Core spray Loop II simulated automatic actuation test (0S45A12J)	Functional	SI 4.5.A.1.a	FCV-75-53 Same as FCV-75-51 above	Once every operating cycle ^a	4 hr	Same as above
Core spray Loop I logic (0142B39J)	Functional	SI 4.2.B-39	Pump 1A and 1C breakers in test position FCV-25 shut with breaker open	Once every 6 months	4 hr	--
Core spray Loop II logic (0242B39J)	Functional	SI 4.2.B-39	Pump 1B and 1D Same as FCV-75-53 above	Once every 6 months	4 hr	--
Core spray Loop I pump time delay relays (042B391J)	Calibration	SI 4.2.B-39, Step 4.5	Same as for Loop I logic test	Once every operating cycle ^a	2 hr	--
Core spray Loop II pump time delay relays (042B392J)	Calibration	SI 4.2.B-39, Step 4.5	Same as for Loop II logic test	Once every operating cycle ^a	2 hr	--
Loop I core spray sparger to reactor pressure vessel differential pressure PdIS 75-28 (042B241J)	Calibration	SI 4.2.B-24	Pumps not allowed to be running unless absolutely necessary	Once every 3 months	2 hr	Core spray not in service (Page 5, IMI-75)
Loop II core spray sparger to reactor pressure vessel differential pressure PdIS 75-56 (042B242J)	Calibration	SI 4.2.B-24	Same as above	Once every 3 months	2 hr	Same as above
Core spray pump discharge pressure Loop I PS-75-7 and 16 (042B211J)	Calibration	SI 4.2.B-21	Core spray not in service (Page 5, IMI-75)	Once every 3 months	2 hr	Core spray auto-blowdown permissives
Core spray pump discharge pressure Loop II PS-75-35 and 44 (042B212J)	Calibration	SI 4.2.B-21	Same as above	Once every 3 months	2 hr	Core spray auto-blowdown

TABLE B-39. (continued)

Component Undergoing Test	Type of Test	Test Procedure Number	Components Aligned Away from Engineered Safeguards Position for Test	Expected Test Frequency	Expected Test Outage Time	Remarks
Loop I discharge pressure PI-75-20 PT-75-20 PX-75-20 (0S42B52J)	Calibration	SI 4.2.B-52	Core spray not in service (Page 5, IMI-75)	Once every 6 months	3 hr	--
Loop II discharge pressure PI-75-48 PT-75-48 PX-75-48 (0S42B53J)	Calibration	SI 4.2.B-53	Same as above	Once every 6 months	3 hr	--
CSS auto-initiation Inhibit (Loop II) (0S42B48J)	Functional	SI 4.2.B-48	--	Once every 6 months	1 hr	--
Loop I core spray sparger to reactor pressure vessel differential pressure PdIS-75-28 (0142B24J)	Functional	SI 4.2.B-24	Core spray system not in service (Page 5, IMI-75)	Once every month	1 hr	--
Loop II core spray sparger to reactor pressure vessel differential pressure PdIS-75-56 (0242B24J)	Functional	SI 4.2.B-24	Same as above	Once every month	1 hr	--
Loop I flow detector FI-75-21 (0IMI751J)	Calibration	IMI-75	Core spray system not in service	Yearly	2 hr	Table 5.1.6, IMI-75
Loop II flow detector FI-75-49 (0IMI752J)	Calibration	IMI-75	Same as above	Yearly	2 hr	Same as above
Reactor low water level LIS-3-58A (042B12AJ)	Functional	SI 4.2.B-1	Level yarway removed from service	Once every month	1 hr per instrument	Switch 1, RHR/RCIC Switch 2, HPCI
LIS-3-58C (042B12BJ)	Functional	SI 4.2.B-1	Same as above	Same as above	Same as above	Switch 3, ADS
LITS-3-58B (042B19AJ)	Functional	SI 4.2.B-1	Same as above	Same as above	Same as above	Switch 4, core spray
LITS-3-58D (042B19BJ)	Functional	SI 4.2.B-1	Same as above	Same as above	Same as above	--
High drywell pressure PS-64-58A and C (0S42B5AJ)	Functional	SI 4.2.B-5	Sensor valved out	Once every month	1 hr	Initiates trips in core spray, HPCI, and LPCI systems
PS-64-58B and D (0S42B5BJ)	Functional	SI 4.2.B-5	Same as above	Same as above	Same as above	--

TABLE B-39. (continued)

Component Undergoing Test	Type of Test	Test Procedure Number	Components Aligned Away from Engineered Safeguards Position for Test	Expected Test Frequency	Expected Test Outage Time	Remarks
Reactor low pressure PS-3-74A and B (042B7CAJ)	Calibration	SI 4.2.B-7	Sensor valved out	Once every 3 months	1-1/2 hr	Switch 1, RHR Switch 2, core spray
PS-68-95 and 96 (042B7CBJ)	Calibration	SI 4.2.B-7	Same as above	Same as above	Same as above	--
Reactor low pressure PS-3-74A and B (042B7FAJ)	Functional	SI 4.2.B-7	Sensor valved out	Once every month	1/2 hr	Switch 1, RHR Switch 2, core spray
PS-68-95 and 96 (042B7FBJ)	Functional	SI 4.2.B-7	Same as above	Same as above	Same as above	--

a. Operating cycle is presently 18 months (i.e., time between refuelings).

TABLE B-40. CORE SPRAY SYSTEM MAINTENANCE ACTS SUMMARY

<u>Component Undergoing Maintenance</u>	<u>Type of Maintenance</u>	<u>Maintenance Procedure Number</u>	<u>Components That Must Be Aligned Away from Engineered Safeguards Position</u>	<u>Expected Frequency of Maintenance</u>	<u>Expected Outage Time Maintenance</u>
Pump 1A	Oil change	157G015	Pump prevented from starting	Once every 2 years	8 hr
Pump 1B	Oil change	157G015	Same as above	Same as above	8 hr
Pump 1C	Oil change	157G015	Same as above	Same as above	8 hr
Pump 1D	Oil change	157G015	Same as above	Same as above	8 hr

Technical Specification Limitations

1. The core spray system shall be operable: prior to reactor startup from a cold condition, or when there is irradiated fuel in the vessel and when the reactor vessel pressure is greater than atmospheric pressure.
2. If one core spray system loop is inoperable, the reactor may remain in operation for a period not to exceed 7 days, provided all active components in the other core spray loop and the RHR system (LPCI mode) and the diesel generators are operable.
3. If the above specifications cannot be met, the reactor shall be shut down in the cold condition within 24 hours.
4. When the reactor vessel pressure is atmospheric and irradiated fuel is in the reactor vessel, at least one core spray loop with one operable pump and associated diesel generator shall be operable, except with the reactor vessel head removed as specified in Item 5 below or prior to reactor startup as specified in Item 1 above.
5. When irradiated fuel is in the reactor vessel and the reactor vessel head is removed, core spray is not required provided work is not in progress that has the potential to drain the vessel, provided (a) the fuel pool gates are open and the fuel pool is maintained above the low level alarm point, and (b) one RHRSW pump and associated valves supplying the standby coolant supply are operable.
6. When one of the 4-kV shutdown boards for Units 1 and 2 is inoperable, continued reactor operation is permissible for a period not to exceed 5 days, provided that both offsite 161-kV transmission lines and both common station transformers and one cooling tower transformer (not parallel with the energized common transformer) are available, and the remaining 5-kV shutdown boards and associated diesel generators, core spray, RHR (LPCI and containment cooling) systems, and all 480-V emergency power boards are operable. If this requirement cannot be met, an orderly shutdown shall be initiated and both reactors will be shut down and in the cold condition within 24 hours.

2.7.3 System Operation

The core spray system is designed to spray water onto the fuel bundle upon receipt of an initiation signal without any operator action. However the system must be manually shut down following an automatic start.

Automatic Start. When on diesel power, if an accident signal on Unit 2 is automatically initiated and has not been reset, Unit 1 core spray Pumps 1B and 1D (Loop II) are prohibited from starting and, if running, will trip. Upon receiving an initiation signal, all operable diesel generators start. The core spray system test valves (FCV-75-22 and 50) close if open. All four core spray pumps will stagger start, unless the 4160 V AC shutdown

boards are being powered from the diesel generators. At approximately 450 psig reactor pressure, the inboard injection valves (FCV-75-25 and 53) open. All the RHRSW pumps that supply the EECW system start.

The operator action upon system startup is to verify the initiating signals, verify the core spray system actuated, and check that flow to reactor vessel increases to design flow of 6250 gpm (FI-75-21 and 49) for each loop as reactor pressure decreases.

If the core spray pumps are tripped manually after auto-initiation, they will not restart automatically until the initiating condition is cleared and the initiating logic is reset. Similarly, if the inboard injection valves are manually closed after auto-initiation, they will not reopen automatically until the initiating condition is cleared and the initiating logic is reset.

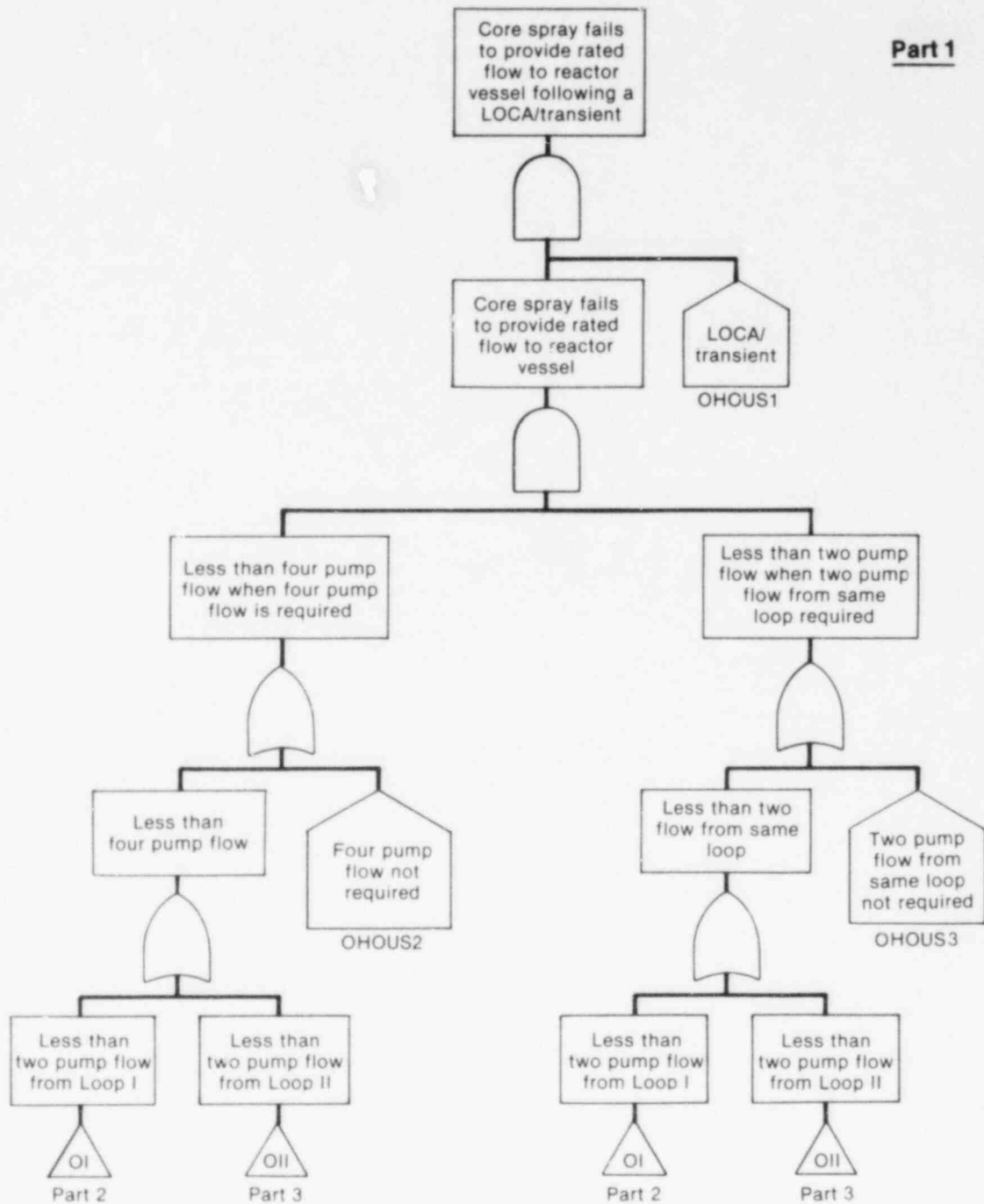
2.7.4 Fault Tree

A fault tree was constructed for the two independent core spray loops in the core spray system based on information contained in the FSAR, P and ID diagrams, and the Hot License Training Program at Browns Ferry Station. The fault tree begins with the undesired top event and structures back through the system from the reactor core to the core spray pumps and suction from the suppression pool. Events shown include faults in the core spray system as well as faults at interfaces with other systems, such as electric power. Figure B-17 displays the core spray fault tree. The two independent loops of the core spray system are designated as Loop I (contains core spray Pumps 1A and 1C) and Loop II (contains core spray Pumps 1B and 1D).

There are eight house events in the core spray tree. The first three (OHOUS1, OHOUS2, and OHOUS3) establish whether the fault tree will be analyzed for one of two loop success (F_B) or two of two loop success (F_A). The next two house events (OHOUS4 and OHOUS5) allow the analyst to account for minimum-flow bypass valve failures causing loop failure due to flow diversion. The initiation circuitry model contains three house events. Two of these (HOUSENVA and HOUSENVL) are mutually exclusive and account for whether the shutdown boards supplying power to the core spray pumps are supplied by normal power or the diesel generators. The HOUSTRAN event prevents taking credit for drywell pressure initiation during transients since high drywell pressure is not a normal result of transients. Table B-41 lists the house events and the initiators for which core spray operation is required.

Success/Failure Criteria. The top event of the core spray system fault tree is defined as "core spray fails to provide rated flow to the reactor vessel." Due to multiple ECCS systems employed at Browns Ferry Station to mitigate accidents and abnormal transients, successful emergency coolant injection is dictated by the various ECCS system availabilities. Refer to Tables B-42 and B-43 for core spray success criteria.)

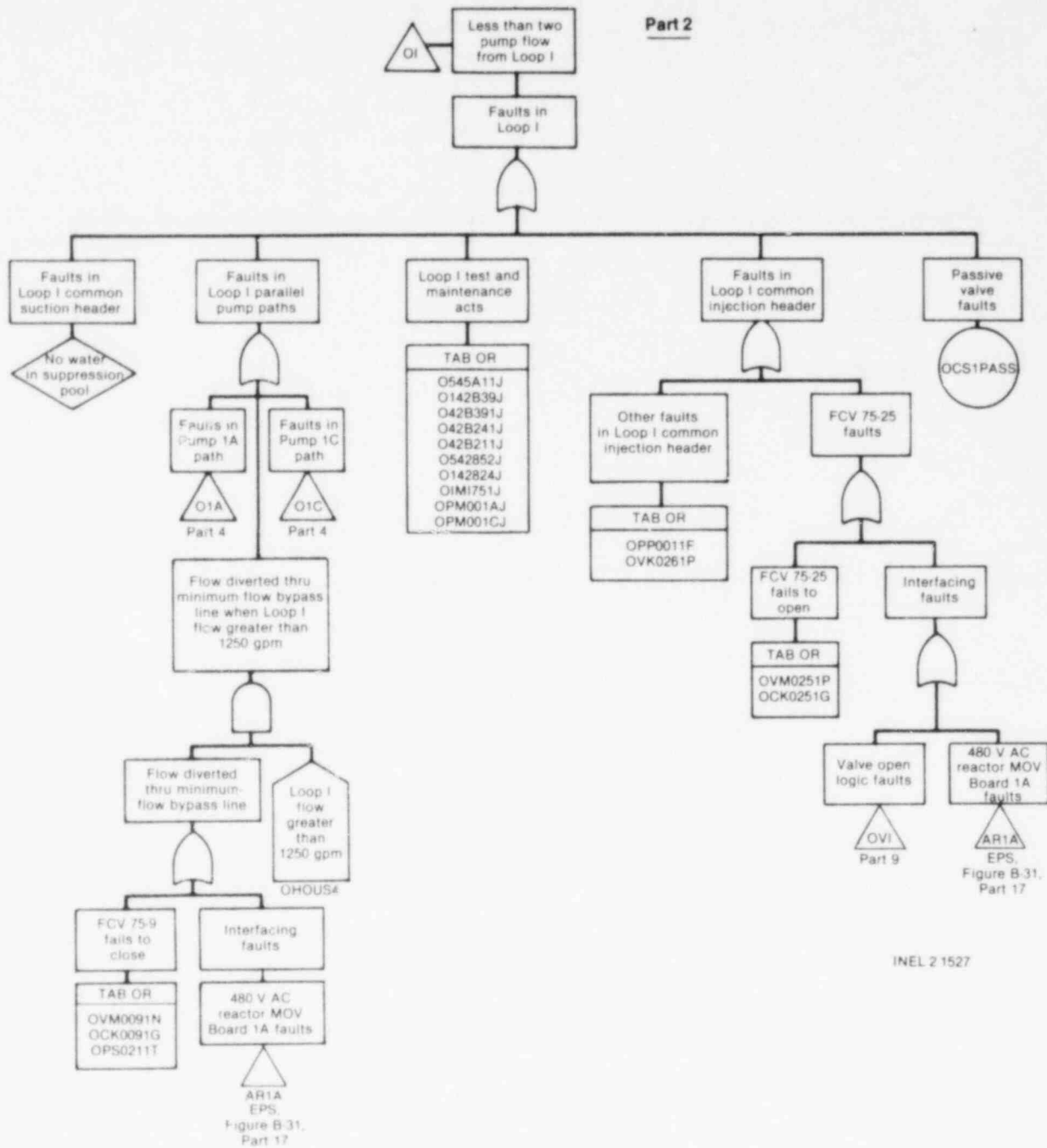
Only the success criteria stated in Table B-42 are considered in the core spray analysis. This criteria defines the requirements for core spray through the full spectrum of break sizes.



INEL 2 1526

Figure B-17. Core spray fault tree.

Part 2

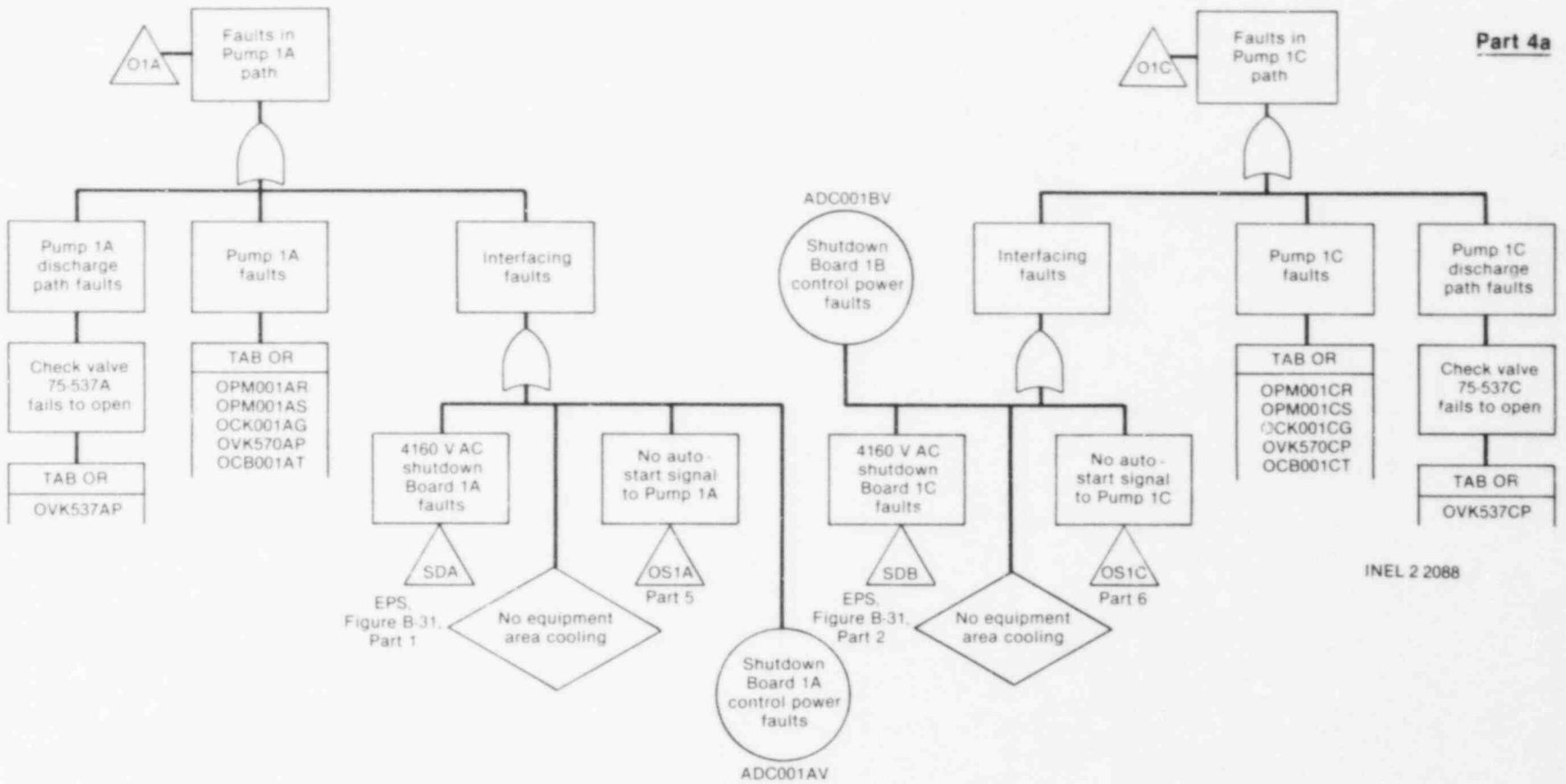


INEL 2 1527

Figure B-17. (continued).



Figure B-17. (continued).



INEL 2 2088

Figure B-17. (continued)

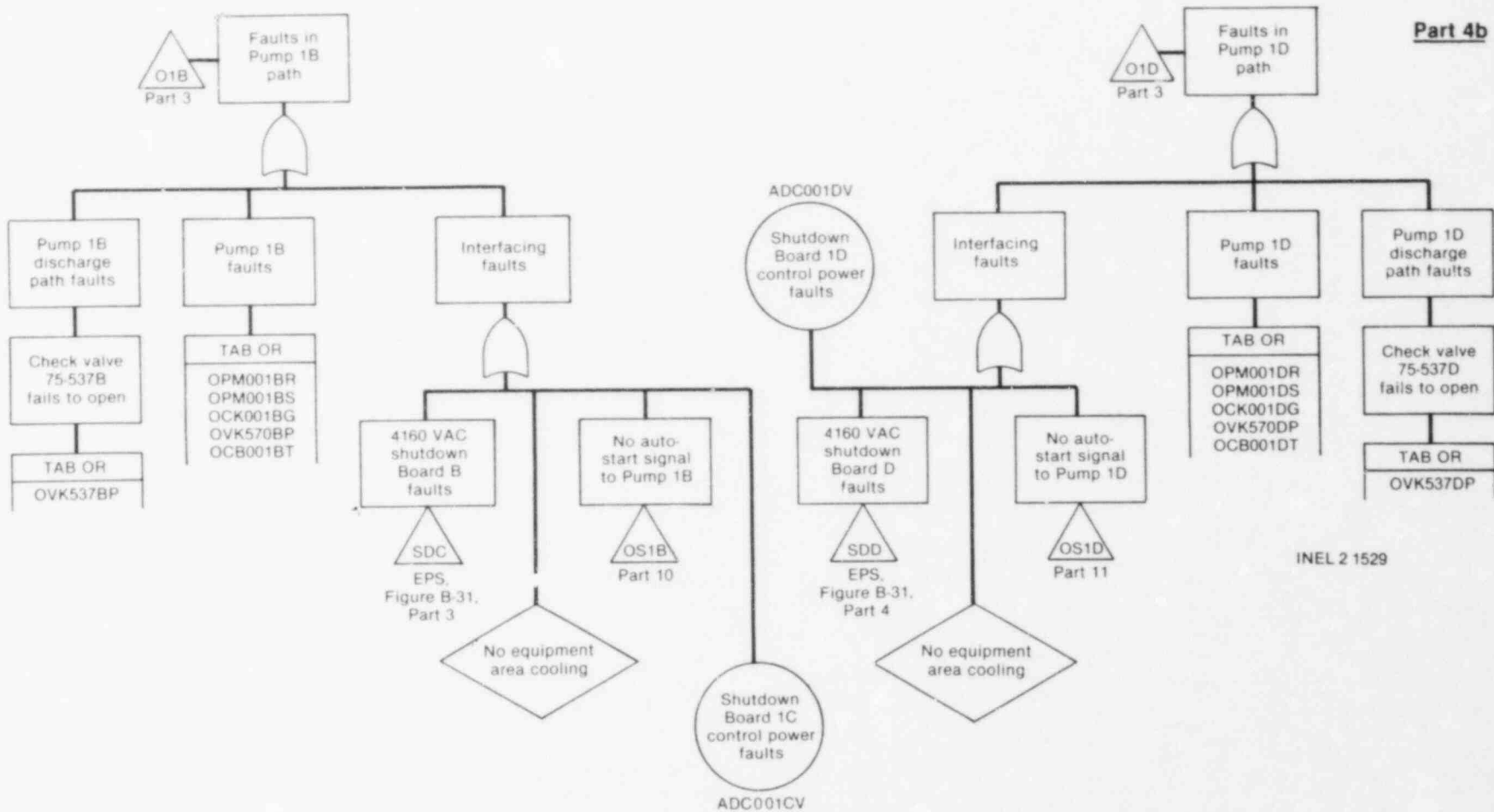


Figure B-17. (continued)

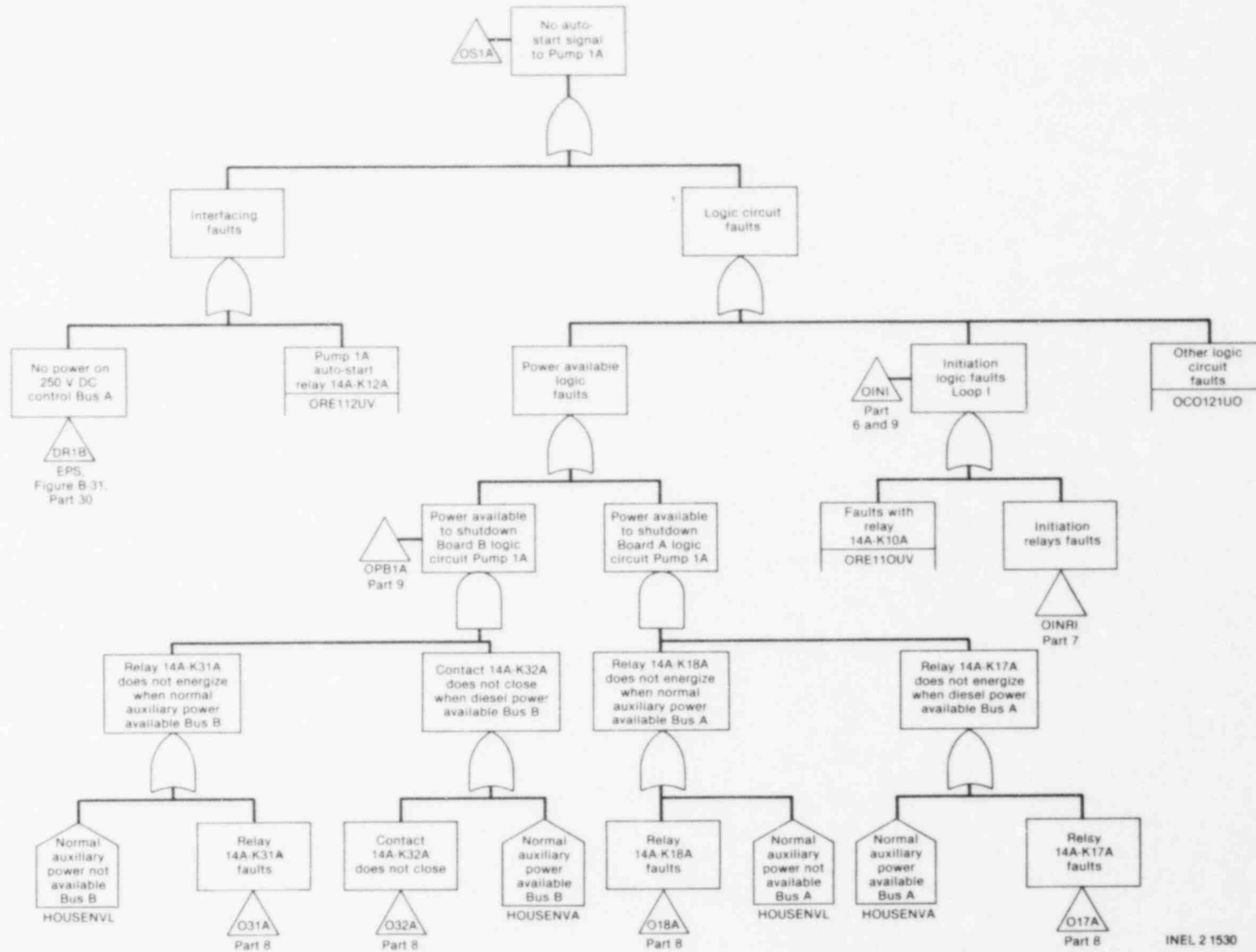


Figure B-17. (continued).

Part 6

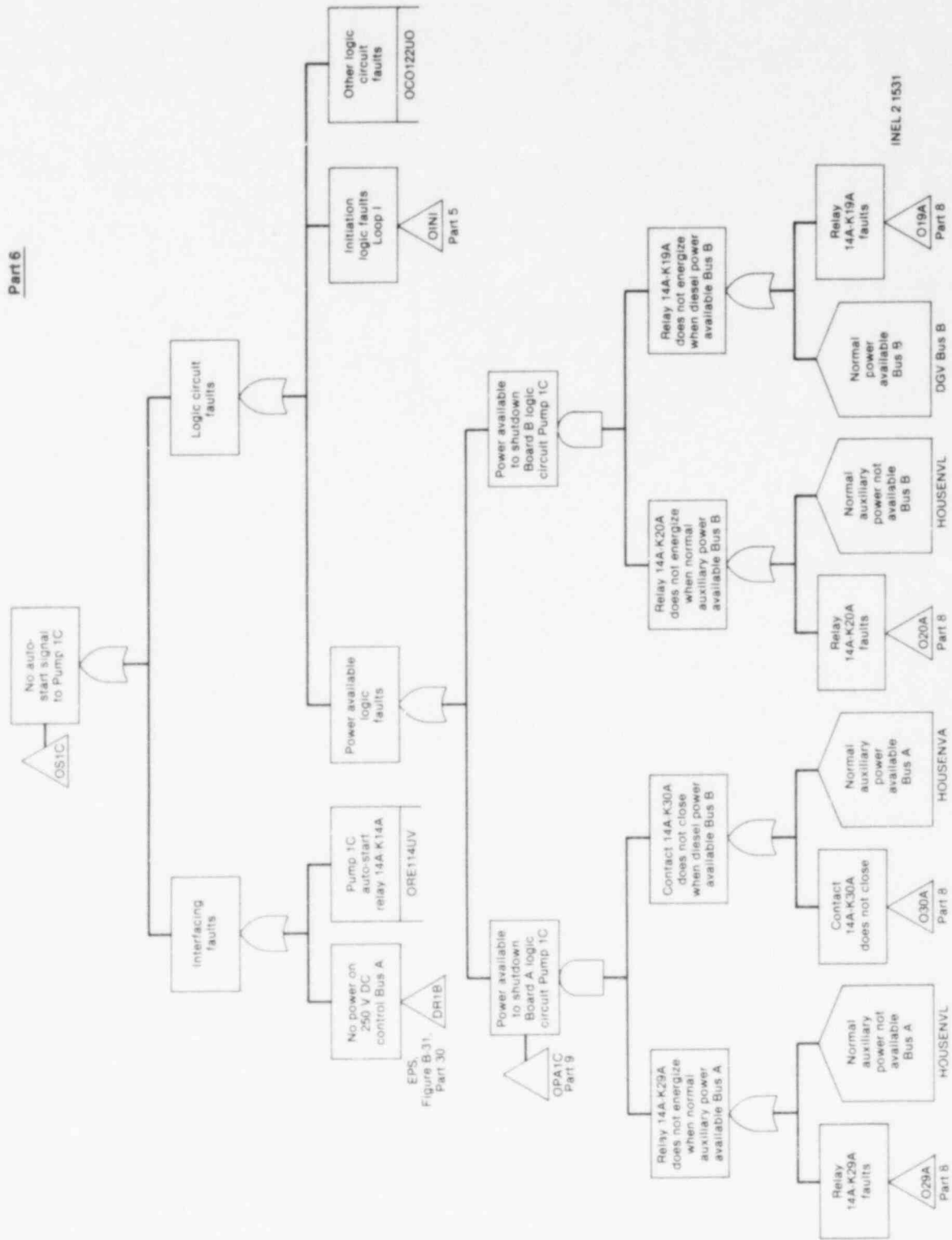
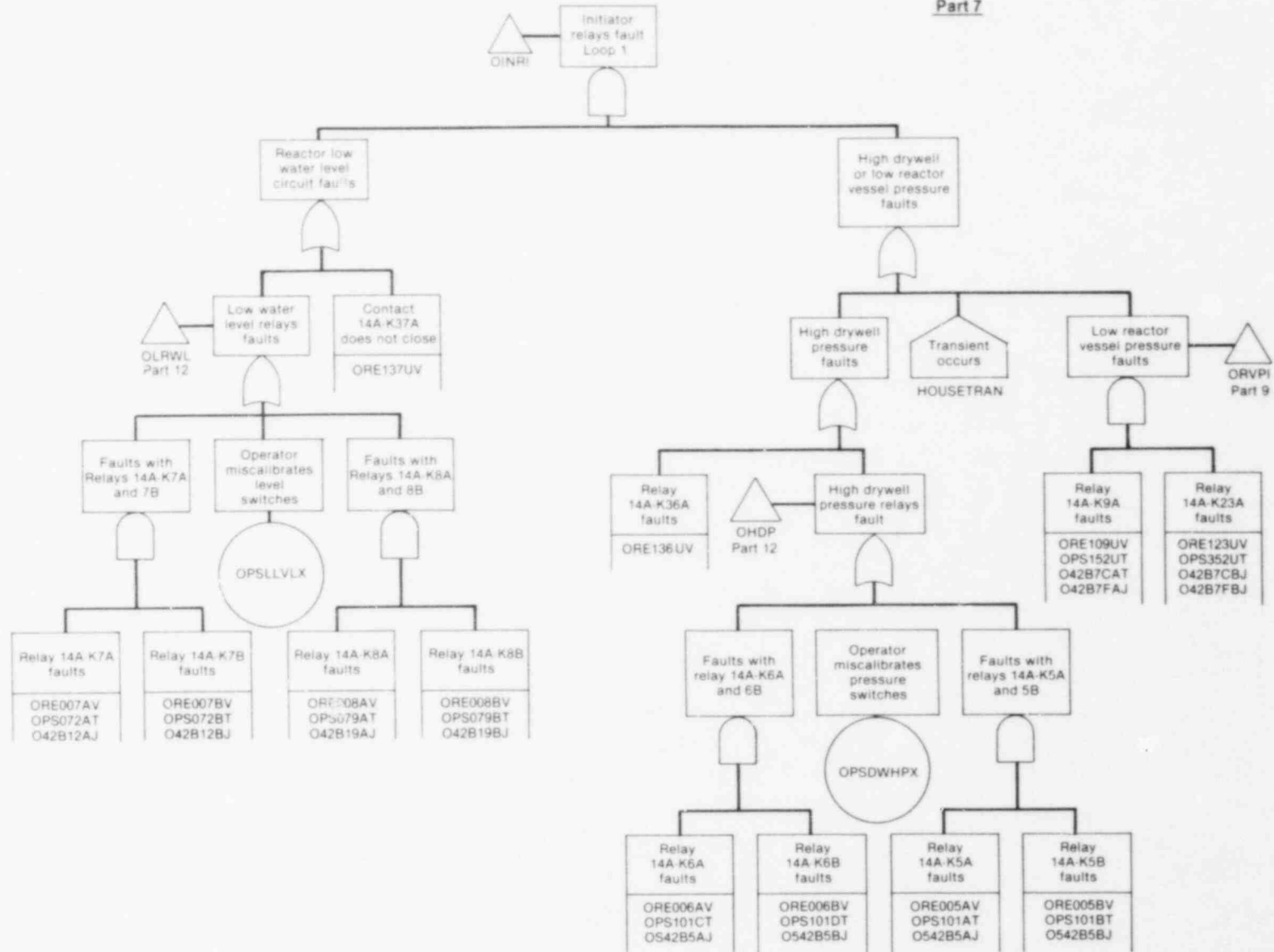


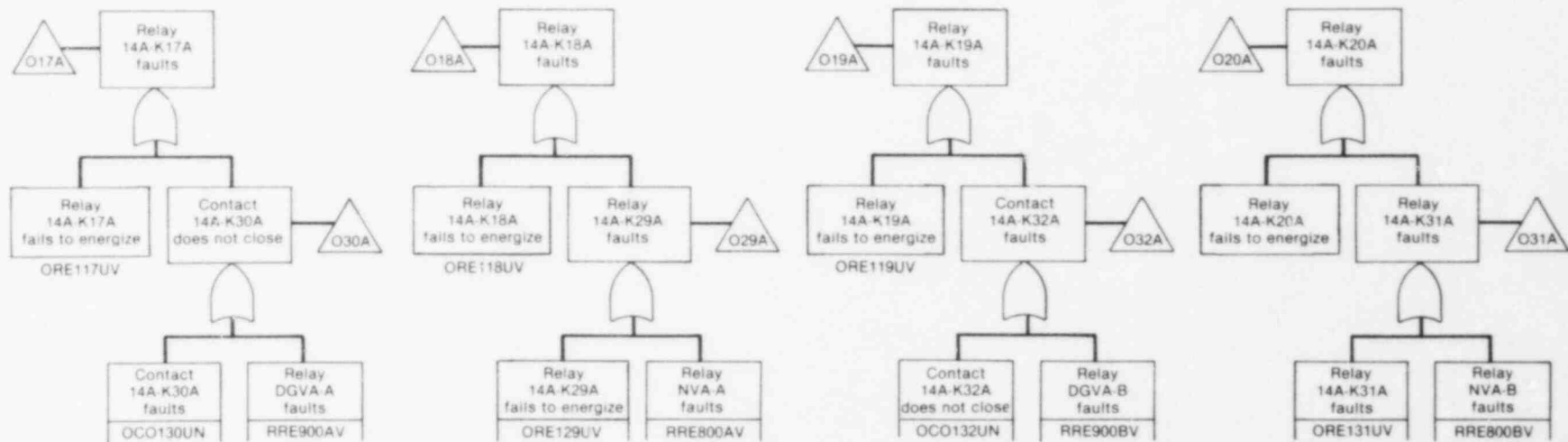
Figure B-17. (continued).



INEL 2 1532

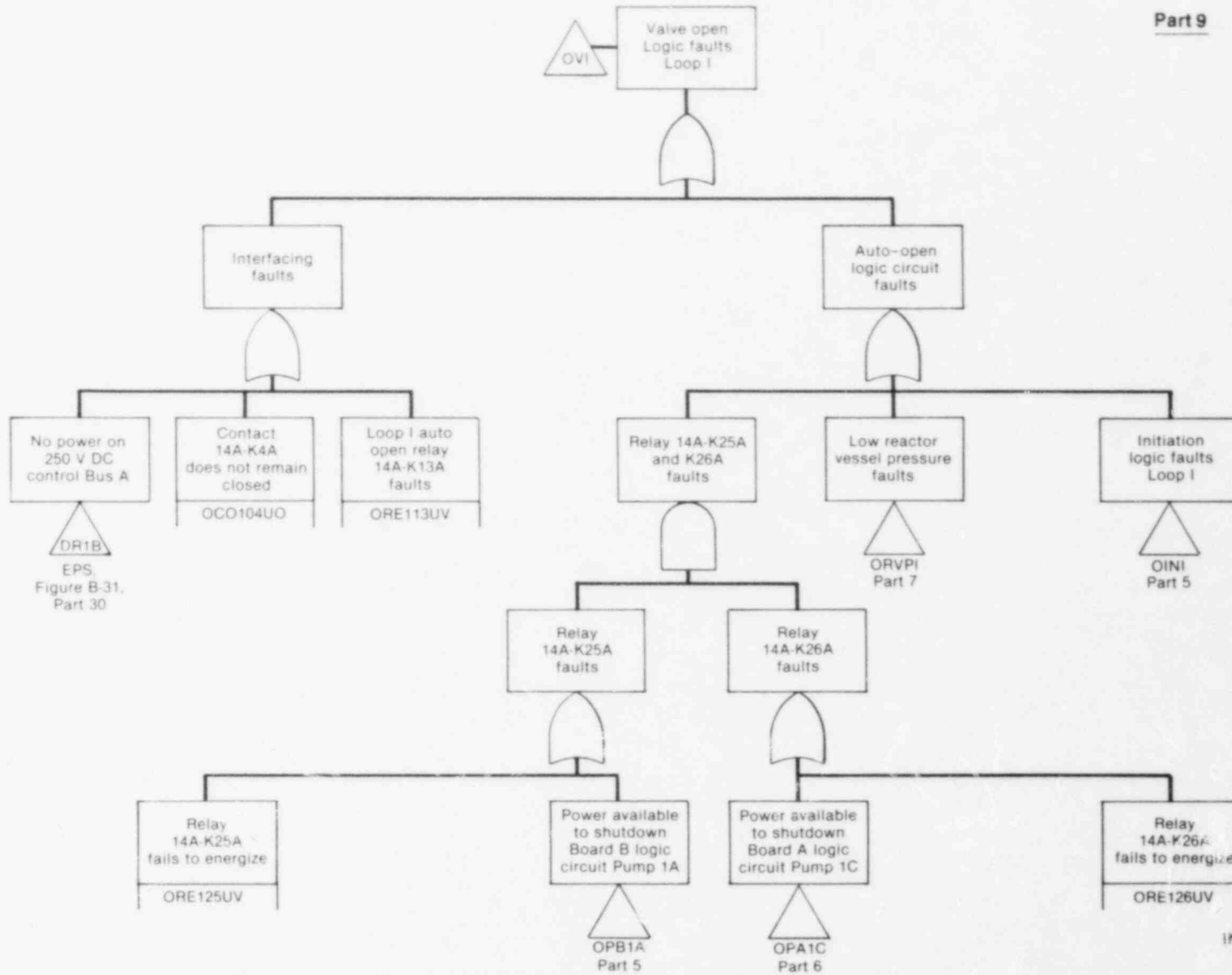
Figure B-17. (continued).

B-199



INEL 2 1533

Figure B-17. (continued).



B-200

INEL 2 1534

Figure B-17. (continued).

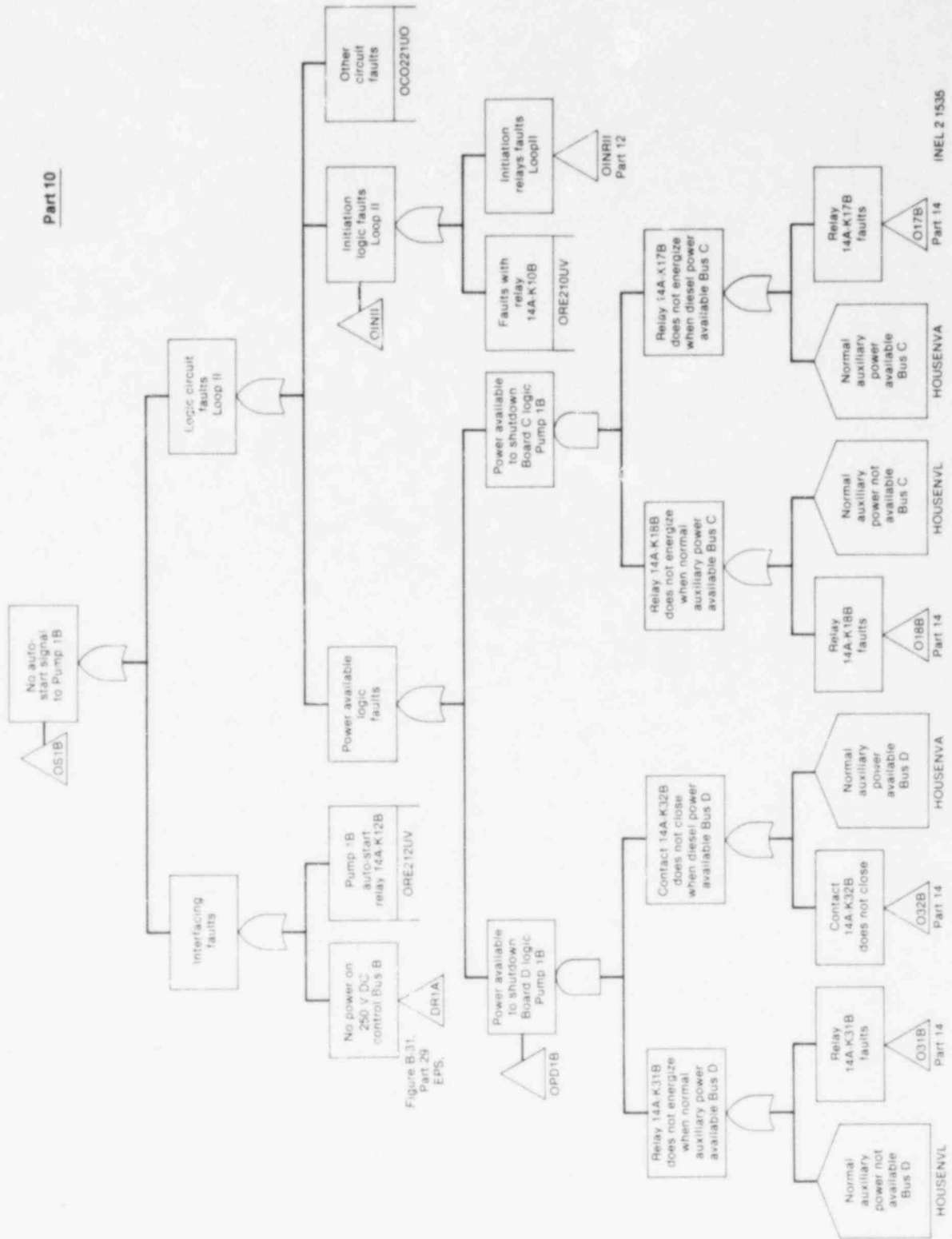


Figure B.31.
Part 29
EPS.

Figure B-17. (continued).

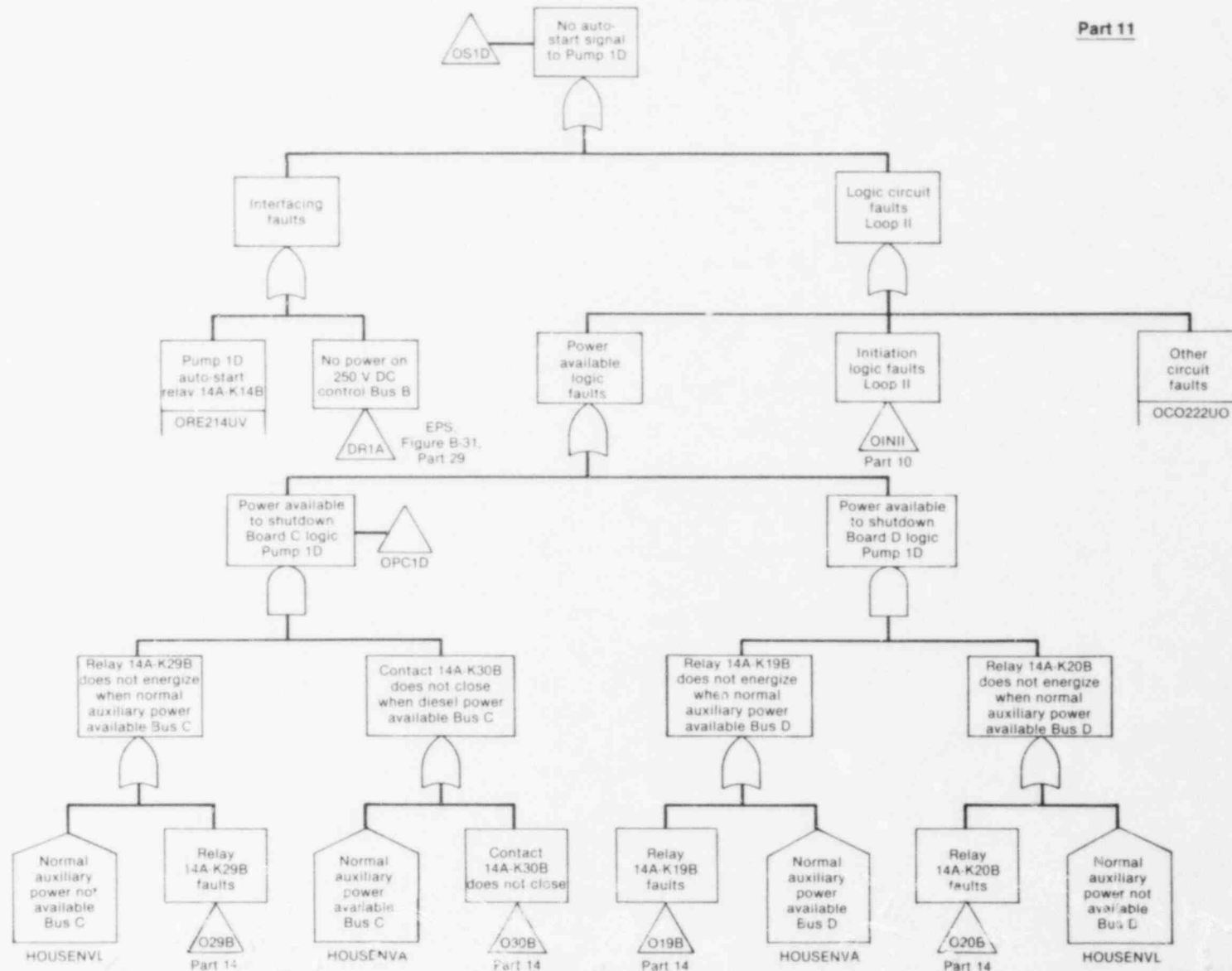
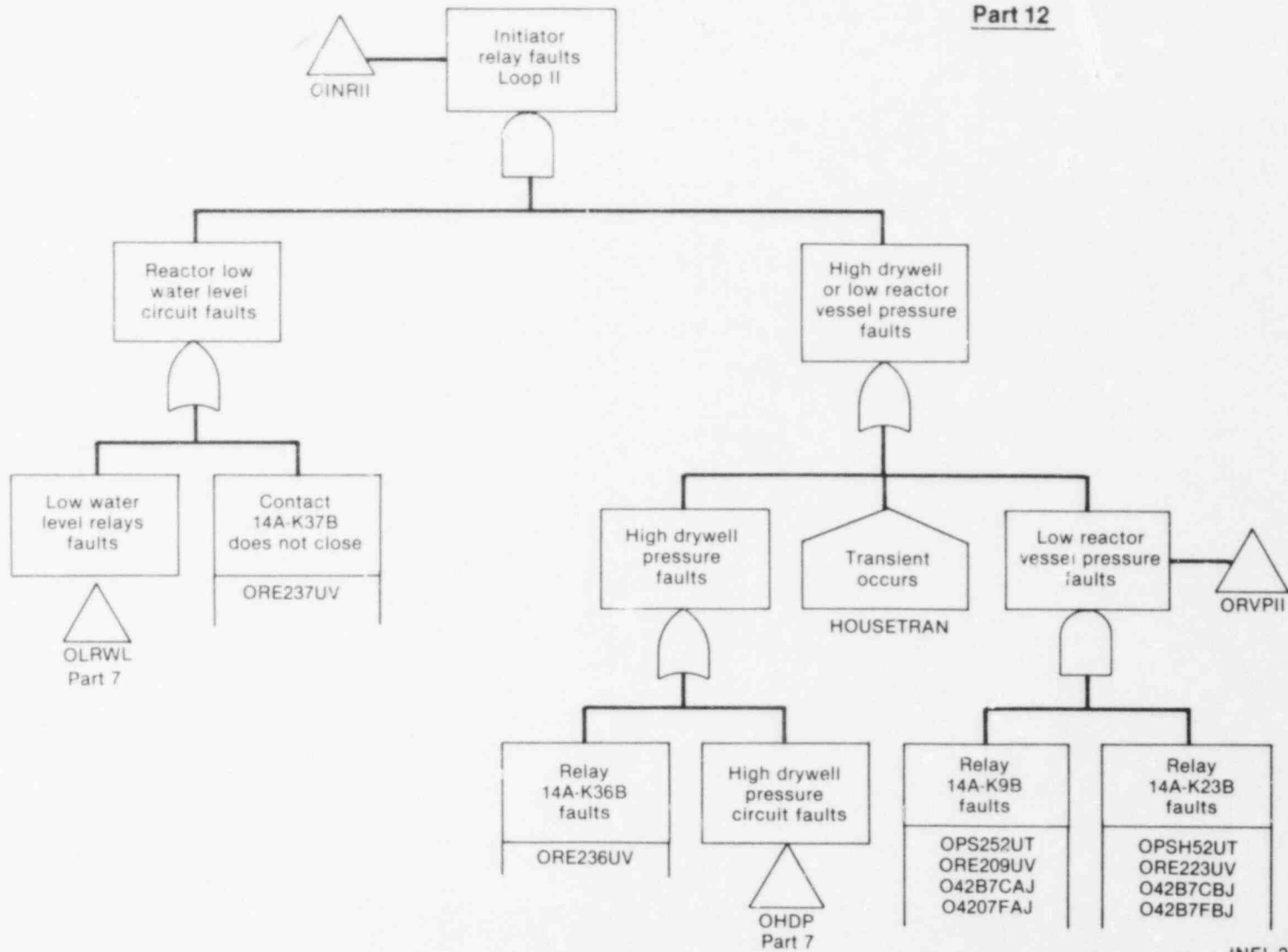


Figure B-17. (continued).

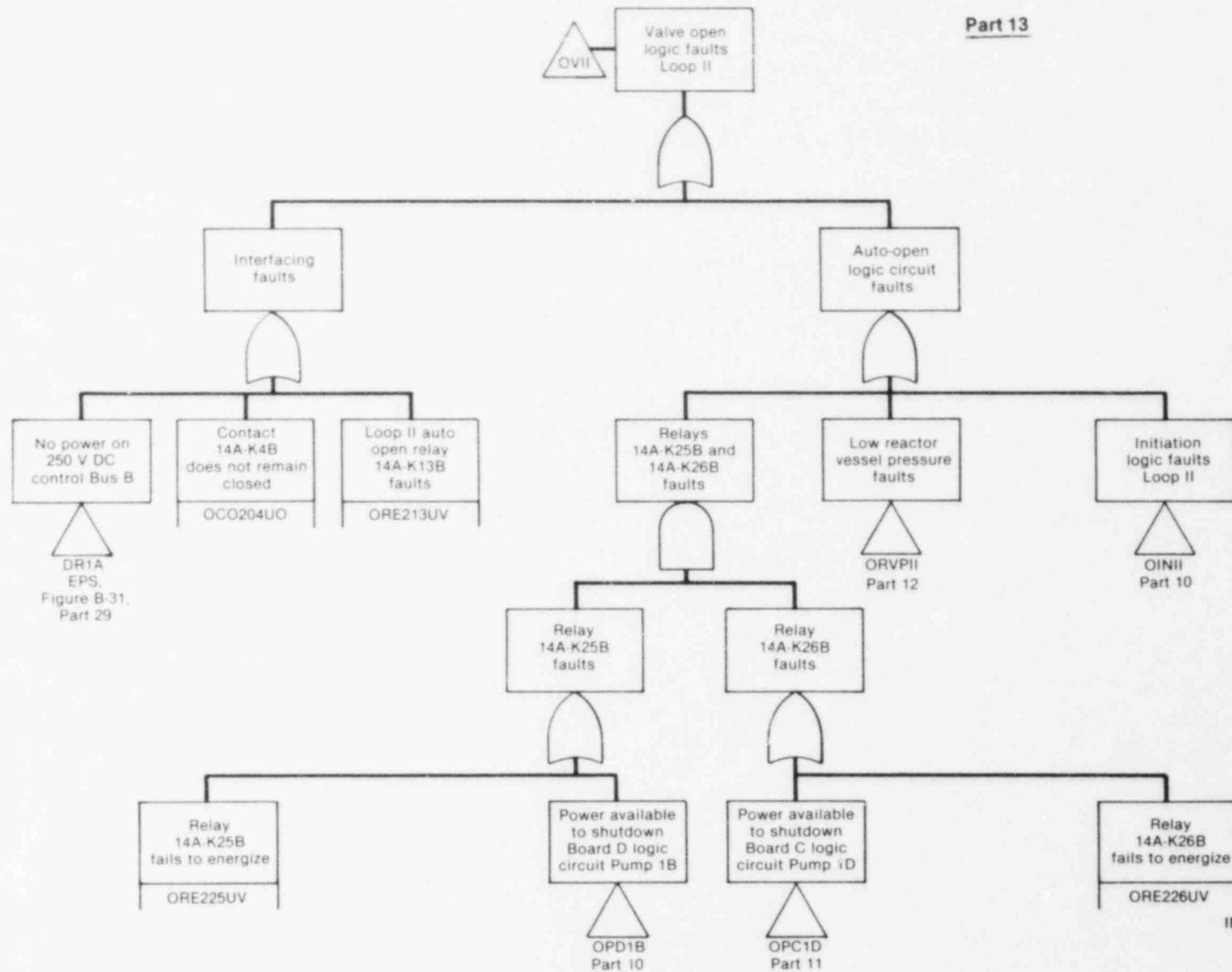
B-202



B-203

INEL 2 1537

Figure B-17. (continued).



INEL 2 1538

Figure B-17. (continued).

B-204

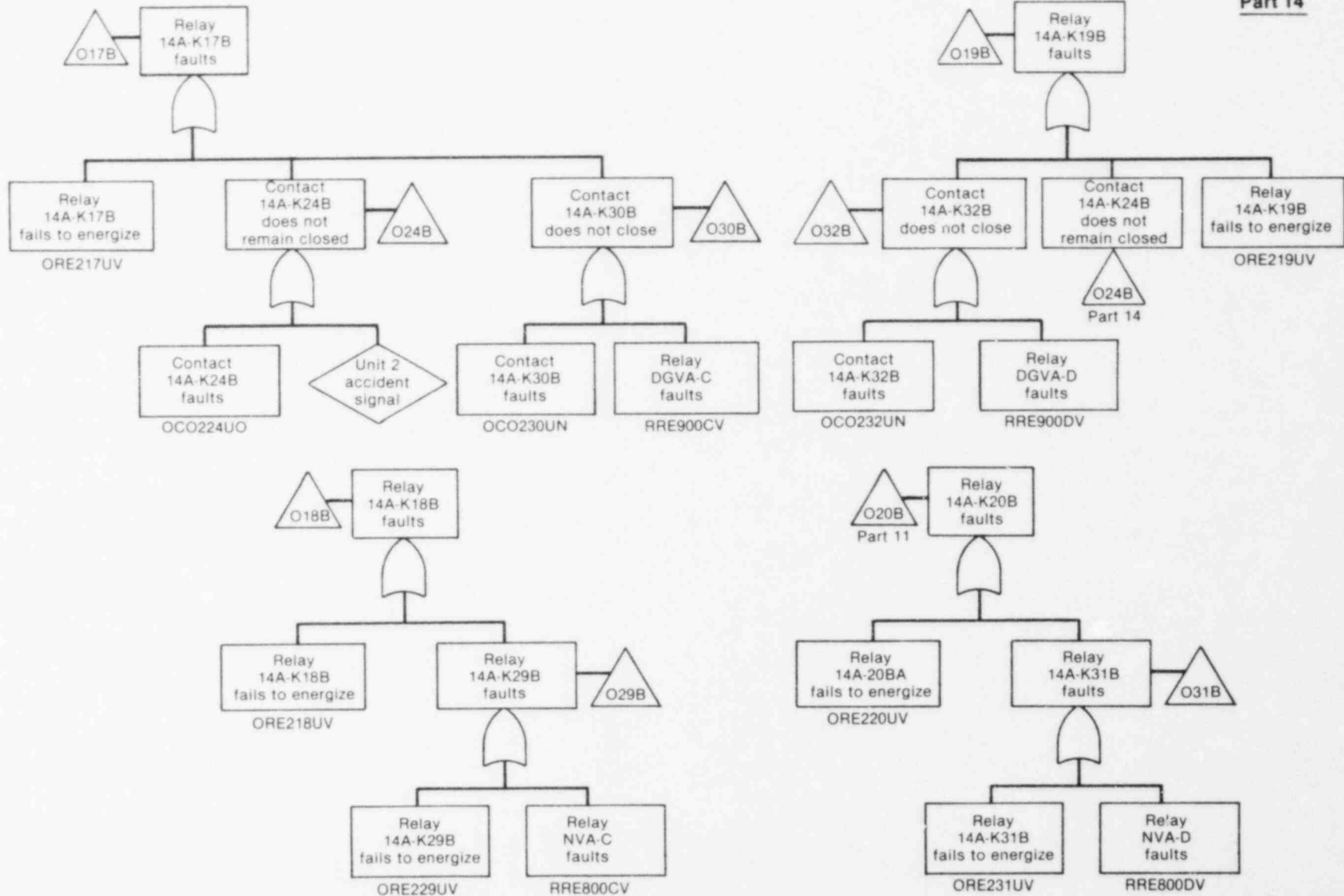


Figure B-17. (continued).

B-205

TABLE B-41. CORE SPRAY SYSTEM HOUSE EVENTS STATUS

<u>Initiator</u>	<u>OHOUS1</u>	<u>OHOUS2</u>	<u>OHOUS3</u>	<u>OHOUS4</u>	<u>OHOUS5</u>	<u>HOUSENVA</u>	<u>HOUSENVL</u>	<u>HOUSSTRAN</u>
L _S *	On	On/Off	Off/On	On	On	On	Off	Off
L _D *	On	On/Off	Off/On	On	On	On	Off	Off
L _V *	On	On/Off	Off/On	On	On	On	Off	Off
I _L , I _V , S	On	Off	On	On	On	On	Off	Off
T _U , T _A	On	Off	On	On	On	On	Off	On
T _p	On	Off	On	On	On	Off	On	On
TK	On	Off	On	On	On	On	Off	On
T _p K	On	Off	On	On	On	Off	On	On

* For these initiators, both the F_A and F_B modes are required depending on the sequence. OHOUS2 "on" with OHOUS3 "off" gives F_A. OHOUS2 "off" with OHOUS3 "on" yields F_B.

TABLE B-42. CORE SPRAY SYSTEM LOCA MITIGATION SUCCESS CRITERIA

<u>Reactor Subcriticality</u>	<u>Short-Term Containment Integrity</u>	<u>Emergency Coolant Injection</u>	<u>Decay Heat Removal</u>
Large Break--Liquid Line--0.3 to 4.3 ft ² --Suction			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	Two core spray loops and two of four LPCI pumps or Four of four LPCI pumps	Two of four RHR pumps with associated heat exchangers in torus cooling mode or One of four RHR pumps with associated heat exchangers in shutdown cooling mode
or		One of two core spray loops and two of four LPCI pumps (one LPCI pump per injection loop)	
No more than five adjacent rods not fully inserted			
Large Break--Liquid Line--0.3 to 4.3 ft ² --Discharge			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	Two core spray loops or One of two core spray loops and one of two LPCI pumps on unaffected side	Two of four RHR pumps with associated heat exchangers in torus cooling mode or One of four RHR pumps with associated heat exchangers in shutdown cooling mode
or			
No more than five adjacent rods not fully inserted			

TABLE B-42. (continued)

Reactor Subcriticality	Short-Term Containment Integrity	Emergency Coolant Injection	Decay Heat Removal
Large Break--Steam Line--1.4 to 4.1 ft ²			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	Two core spray loops	Two of four RHR pumps with associated heat exchangers in torus cooling mode
or		or	or
No more than five adjacent rods not fully inserted		Four of four LPCI pumps	
		or	
		One of two core spray loops and one of four LPCI pumps	One of four RHR pumps with associated heat exchangers in shutdown cooling mode
Intermediate Break--Liquid Line--0.12 to 0.3 ft ²			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	One of one HPCI pump	Two of four RHR pumps with associated heat exchangers in torus cooling mode
or		or	or
No more than five adjacent rods not fully inserted		Four of six ADS relief valves	
		and	
		One of four LPCI pumps	One of four RHR pumps with associated heat exchangers in shutdown cooling mode
		or	
		One of two core spray loops	

B-208

TABLE B-42. (continued)

<u>Reactor Subcriticality</u>	<u>Short-Term Containment Integrity</u>	<u>Emergency Coolant Injection</u>	<u>Decay Heat Removal</u>
Intermediate Break--Steam Line--0.12 to 1.4 ft ²			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	One of one HPCI pump or One of four LPCI pumps	Two of four RHR pumps with associated heat exchangers in torus cooling mode
or		or	or
No more than five adjacent rods not fully inserted		One of two core spray loops	One of four RHR pumps with associated heat exchangers in shutdown cooling mode
Small Break--Liquid or Steam--Up to 0.12 ft ²			
No more than 30 rods scattered throughout the core not fully inserted	Adequate suppression pool level and no bypass leakage from drywell to wetwell	One of one HPCI pump or Four of six ADS relief valves and one of four LPCI pumps	Two of four RHR pumps with associated heat exchangers in torus cooling mode
or		or	or
No more than five adjacent rods not fully inserted		Four of six ADS relief valves and one of two core spray loops	One of four RHR pumps with associated heat exchangers in shutdown cooling mode

TABLE B-43. CORE SPRAY SYSTEM TRANSIENT MITIGATION SUCCESS CRITERIA

Anticipated Transient	Reactor Shutdown		Overpressure Protection			Vessel Water Inventory				DHR
	CRD	RPT	OP(O) ^a	OP(C) ^b	PCS	MSI	HPCI	DEP	INJ	RHR
Transients where PCS is available	No more than 30 rods fail to insert	Both recirculation pumps trip ^b	NA	All relief valves reclose ^c	Condenser available and Feed system providing makeup	MSIVs shut ^d or Turbine valves ^d and bypass valves shut	HPCI or RCIC	Manual operation of at least four relief valves	One LPCI pump or One core spray loop	Two RHR pumps and two heat exchangers in torus cooling mode or One RHR pump and one heat exchanger in shutdown cooling mode
	or No more than five adjacent rods fail to insert								or One booster and one condensate pump or One RHRSW pump in SBCS mode	
Transients where PCS is unavailable	No more than 30 rods fail to insert		Direct scram 2 of 13 valves	All relief valves reclose	NA	MSIVs shut or Turbine valves and bypass valves shut	HPCI or RCIC	Manual operation of at least four relief valves	One LPCI pump or One core spray loop	Two RHR pumps and two heat exchangers in torus cooling mode or One RHR pump and one heat exchanger in shutdown cooling mode
	or No more than five adjacent rods fail to insert		Flux scram 7 of 13 valves						or One booster and one condensate pump ^e or One RHRSW pump in SBCS mode	
			Pressure scram 10 of 13 valves							

a. Relief valves open OP(O) and reclose OP(C).

b. If both recirculation pumps trip and PCS remains available, the resulting power level is such that the capacity of the bypass valves is adequate to remove the heat being generated.

c. Even though relief valve action is not required some relief valves will open.

d. MSI only necessary if PCS fails.

e. Although PCS is unavailable, the condensate system may still be operable.

Major Assumptions. The fault tree analysis of the core spray system was based on the following assumptions:

1. System valves are aligned prior to LOCA as shown in Figure B-15. A successful response will be for the core spray loop pumps to start, the inboard injection valves to open, and the minimum-flow bypass valves to close.
2. Passive failures of normally open valves that are not required to change state are considered if the passive fault could disable an entire loop. There are seven such valves in each loop: a torus suction valve (HCV-75-1 and 29), two pump suction valves (FCV-75-11 and 2, and FCV-75-30 and 39), two pump discharge valves (HCV-75-10 and 18, and HCV-75-38 and 46), and two loop discharge valves (FCV-75-23, HCV-75-27 and FCV-75-55). Passive failures of active components are insignificant compared to the active failure rates.
3. No credit is given to manual intervention as a means of producing successful operation.
4. The suppression pool is common to core spray, LPCI, and primary containment. Faults associated with the suppression pool, including torus rupture and low water, were considered to be insignificant contributors to core spray unavailability.
5. Each of the core spray loop pump suction lines has an interface with the CST through a locked-closed manual isolation valve. This alternate source of water is not considered as an alternative source because of Assumptions 1 and 3.
6. Piping less than or equal to 2-inch diameter for diverting flow, was considered to be insignificant contributors to system performance.
7. Pipe rupture due to water hammer is considered to be insignificant since the core spray piping is maintained full of water by the keep-full system.

Basic Events. The information associated with the various basic events listed in the fault tree is summarized in the core spray fault summary short form, Table B-44. In addition, the failure data associated with these basic events is summarized in Table B-45. Tables B-46 through B-48 list the dominant cut sets for core spray unavailabilities.

TABLE B-44. CORE SPARY SYSTEM FAULT SUMMARY SHORT FORM

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
0H0US1	LOCA/transient	On/off	--	--	--
0H0US2	Four-pump flow not required	↓	--	--	--
0H0US3	Two-pump flow from same loop not required		--	--	--
0H0US4	Loop I flow greater than 1250 gpm		--	--	--
0PP0011F	Loop I injection header down stream of FCV-75-25		Rupture	1E-10/hr/section	25
0VK0261P	FCV-75-25 Loop I	Does not open	1E-4/D	--	3
0S45A11J	Loop I simulated automatic actuation test	Out of service	3E-4	--	0
0142B39J	Loop I logic test	↓	9E-4	--	↓
042B241J	Loop I sparger to reactor pressure vessel differential pressure calibration		9E-4	--	
042B391J	Loop I pump time delay calibration		1.5E-4	--	
042B211J	Loop I pump discharge calibration		1.4E-3	--	

B-212

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
0S42B52J	Loop I discharge pressure calibration	Out of service	6.9E-4	--	0
0142B24J	Loop I sparger to reactor pressure vessel differential pressure test	Out of service	1.4E-3	--	0
01M1751J	Loop I flow detector	Out of service	2.3E-4	--	0
0PP0012F	Loop 2 injection header down stream of FCV-75-53	Rupture	1E-10/hr/section	25	30
0VK0542P	FCV-75-54 Loop 2	Does not open	1E-4/D	--	3
0H0US5	Loop II flow greater than 1250 gpm	On/off	--	--	--
0S45A12J	Loop II simulated automatic actuation test	Out of service	3E-4	--	0
0242B39J	Loop II logic test	Out of service	9E-4	--	0
042B392J	Loop II pump time delay relays calibration	Out of service	1.5E-4	--	0

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
042B242J	Loop II sparger to reactor pressure vessel differential pressure calibration	Out of service	9E-4	--	0
042B212J	Loop II pump discharge pressure calibration	↓	1.4E-3	--	↓
0S42B53J	Loop II discharge pressure calibration		6.9E-4	--	
0S42B48J	Loop II auto-initiation inhibit test		2.3E-4	--	
0242B24J	Loop II sparger to reactor pressure vessel differential pressure test		1.4E-3	--	
0IMI752J	Loop II flow detector		2.3E-4	--	
0VM0251P	Loop I inboard injection Valve FCV-75-25	Does not open	1E-3/D	--	3

B-214

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
OCK0251G	Control circuit for Loop I inboard injection valve	No output	3.2E-3	--	10
OVM0532P	Loop II inboard injection Valve FCV-75-53	Does not open	1E-3/D	--	3
OCK0532G	Control circuit for Loop II inboard injection valve	No output	3.2E-3	--	10
OVK537CP	Pump 1C discharge check Valve 75-537C	Does not open	1E-4/D	--	3
OVM0091N	Loop I miniflow bypass FCV-75-9	Does not close	1E-3/D	--	3
OCK0091G	Loop I miniflow bypass control circuit	No output	3.2E-3	--	10
OPS0211T	Loop I miniflow bypass flow sensor	Does not operate	1E-4/D	--	3
ADCO01BV	Shutdown Board 1B control power	Does not energize	1E-6/hr	7	10
OPM001CR	Pump 1C	Does not start	1E-3/D	--	3

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
OPMO01CS	Pump 1C	Stops running	3E-5/hr	8	10
OCK001CG	Pump 1C motor control circuit	No output	2.9E-3	--	10
OVK570CP	Pump 1C miniflow bypass check Valve 75-570C	Does not open	1E-4/D	--	3
GCB001CT	Pump 1C circuit breaker	Does not operate	1E-3/D	--	3
OPMO01CJ	Pump 1C maintenance	Out of service	4.6E-4	--	0
OVK537AP	Pump 1A discharge check Valve 75-537A	Does not open	1E-4/D	--	3
ADCO01AV	Shutdown Board 1A control power	Does not energize	1E-6/hr	7	10
OPMO01AR	Pump 1A	Does not start	1E-3/D	--	3
OPMO01AS	Pump 1A	Stops running	3E-5/hr	8	10
OCK001AG	Pump 1A motor control circuit	No output	2.9E-3	--	10

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
OVK570AP	Pump 1A miniflow bypass check Valve 75-570A	Does not open	1E-4/D	--	3
OCB001AT	Pump 1A circuit breaker	Does not operate	1E-3/D	--	3
OPM001AJ	Pump 1A maintenance	Out of service	4.6E-4	--	0
OVK537BP	Pump 1B discharge check Valve 75-537B	Does not open	1E-4/D	--	3
OVM0372N	Loop II miniflow bypass FCV-75-37	Fails to close	1E-3/D	--	3
OPS0492T	Loop II miniflow bypass flow sensor	Does not operate	1E-4/D	--	3
OCK0372G	Loop II miniflow bypass valve control circuit	No output	3.2E-3	--	10
ADC001CV	Shutdown Board 1C control power	Does not energize	1E-6/hr	7	10
OPM001BR	Pump 1B	Does not start	1E-3/D	--	3

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
OPM001BS	Pump 1B	Stops running	3E-5/hr	8	10
OCK001BG	Pump 1B motor control circuit	No output	2.9E-3	--	10
OVK570BP	Pump 1B miniflow bypass check Valve 75-570B	Does not open	1E-4/D	--	3
OCB001BT	Pump 1B circuit breaker	Does not operate	1E-3/D	--	3
OPM001BJ	Pump 1B maintenance	Out of service	4.6E-4	--	0
OVK537DP	Pump 1D discharge check Valve 75-537D	Does not open	1E-4/D	--	3
ADCO01DV	Shutdown Board 1D control power	Does not energize	1E-6/hr	7	10
OPM001DR	Pump 1D	Does not start	1E-3/D	--	3
OPM001DS	Pump 1D	Stops running	3E-5/hr	8	10
OCK001DG	Pump 1D motor control circuit	No output	2.9E-3	--	10

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
OVK570DP	Pump 1D miniflow bypass check Valve 75-570D	Does not open	1E-4/D	--	3
OCB001DT	Pump 1D circuit breaker	Does not operate	1E-3/D	--	3
OPM001DJ	Pump 1D maintenance	Out of service	4.6E-4	--	0
ORE112UV	Relay 14A-K12A	Does not energize	1E-4/D	--	3
OC0121U0	Contact 14A-K21A	Does not remain closed	1E-7/hr	367	3
ORE110UV	Relay 14A-K10A	Does not energize	1E-4/D	--	3
HOUSENVL	Normal auxiliary power not available, Bus B	On/off	--	--	--
HOUSENVA	Diesel power not available, Bus B	On/off	--	--	--

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
HOUSENVL	Normal auxiliary power not available, Bus A	On/off	--	--	--
HOUSENVA	Diesel power not available, Bus A	On/off	--	--	--
ORE120UV	Relay 14A-K20A	Does not energize	1E-4/D	--	3
ORE119UV	Relay 14A-K19A	↓	↓	--	↓
ORE118UV	Relay 14A-K18A			--	
ORE117UV	Relay 14A-K17A			--	
ORE131UV	Relay 14A-K31A			--	
RRE800BV	Relay NVA-B			--	
GC0132UN	Contact 14A-K32A	Does not close	3E-7/hr	2167	↓
RRE900BV	Relay DGVA-B	Does not energize	1E-4/D	--	

B-220

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ORE129UV	Relay 14A-K29A	Does not energize	1E-4/D	--	3
RRE800AV	Relay NVA-A	Does not energize	1E-4/D	--	↓
OC0130UN	Contact 14A-K30A	Does not close	3E-7/hr	2167	
RRE900AV	Relay DGVA-A	Does not energize	1E-4/D	--	
ORE137UV	Relay 14A-K37A	Does not energize	↓	--	
ORE136UV	Relay 14A-K36A	Does not energize		--	
OPS101CT	Pressure Switch 2-10-101C	Does not operate		--	
OS42B5AJ	Functional Test PS-64-58 A and C	Out of service		1.4E-3	
ORE005AV	Relay 14A-K5A	Does not energize	1E-4/D	--	3

B-221

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
OPSI01AT	Pressure Switch 2-10-101A	Does not operate	1E-4/D	--	3
OS42B5BJ	Functional Test PS-64-58 B and D	Out of service	1.4E-3	--	0
ORE006BV	Relay 14A-K6B	Does not energize	1E-4/D	--	3
OPSI01DT	Pressure Switch 2-10-101D	Does not operate	↓	--	↓
ORE005BV	Relay 14A-K5B	Does not energize		--	
OPSI01BT	Pressure Switch 2-10-101B	Does not operate		--	
ORE114UV	Relay 14A-K14A	Does not energize		--	
OC0122U0	Contact 14A-K22A	Does not remain closed	1E-7/hr	367	
OC0104U0	Contact 14A-K4A	Does not remain closed	1E-7/hr	367	

B-222

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ORE113UV	Relay 14A-K13A	Does not energize	1E-4/D	--	3
ORE125UV	Relay 14A-K25A	↓	↓	--	↓
ORE126UV	Relay 14A-K26A			--	
ORE212UV	Relay 14A-K12B			--	
OC0221U0	Contact 14A-K21B	Does not remain closed	1E-7	367	
ORE210UV	Relay 14A-K10B	Does not energize	1E-4/D	--	
HOUSENVL	Normal auxiliary power not available, Bus D	On/off	--	--	--
HOUSENVA	Diesel power not available, Bus D	On/off	--	--	--
HOUSENVL	Normal auxiliary power not available, Bus C	On/off	--	--	--

B-223

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
HOUSENVA	Diesel power not available, Bus C	On/off	--	--	--
ORE237UV	Relay 14A-K37B	Does not energize	1E-4/D	--	3
ORE236UV	Relay 14A-K36B	Does not energize	↓	--	3
ORE223UV	Relay 14A-K23B	Does not energize		--	3
OPS452UT	Pressure Switch 2-3-52D	Does not operate		--	↓
OPS252UT	Pressure Switch 2-3-52B	Does not operate		--	
ORE209UV	Relay 14A-K9B	Does not energize		--	
ORE220UV	Relay 14A-K20B	↓		--	
ORE219UV	Relay 14A-K19B			--	
ORE231UV	Relay 14A-K31B			--	
RRE800DV	Relay NVA-D			--	

B-224

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
OC0224U0	Contact 14A-K24B	Does not remain closed	1E-7/hr	2167	3
RRE900DV	Relay DGVA-D	Does not energize	1E-4/D	--	↓
OC0232UN	Contact 14A-K32B	Does not close	3E-7/hr	2167	
ORE218UV	Relay 14A-K18B	Does not energize	1E-4/D	--	
ORE217UV	Relay 14A-K17B	↓	↓	--	
ORE229UV	Relay 14A-K29B	↓	↓	--	
RRE800CV	Relay NVA-C	↓	↓	--	
RRE900CV	Relay DGVA-C	↓	↓	--	
OC0230UN	Contact 14A-K30B	Does not close	3E-7/hr	2167	

B-225

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ORE214UV	Relay 14A-K14B	Does not energize	1E-4/D	--	3
ORE007AV	Relay 14A-K7A	Does not energize	1E-4/D	--	3
OPSO72AT	Level Switch 2-3-72B	Does not operate	1E-4/D	--	3
042B12AJ	Functional Test LIS-3-58A	Out of service	1.4E-3	--	0
ORE008AV	Relay 14A-K8A	Does not energize	1E-4/D	--	3
OPSO79AT	Level Switch 2-3-79A	Does not operate	1E-4/D	--	3
042B19AJ	Functional Test LITS-3-58B	Out of service	1.4E-3	--	0
ORE123AV	Relay 14A-K23A	Does not energize	1E-4/D	--	3
OPSO352UT	Pressure Switch 2-3-52C	Does not operate	1E-4/D	--	3

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
042B7CAJ	Calibration PS-3-74 A and B	Out of service	6.9E-4	--	0
042B7FAJ	Functional Test PS-3-74 A and B	Out of service	6.9E-4	--	0
OPS152UT	Pressure Switch 2-3-52A	Does not operate	1E-4/D	--	3
ORE109UV	Relay 14A-K9A	Does not energize	1E-4/D	--	3
042B7CBJ	Calibration PS-68-95 and 96	Out of service	6.9E-4	--	0
042B7FBJ	Functional Test PS-68-95 and 96	Out of service	6.9E-4	--	0
ORE007BV	Relay 14A-K9B	Does not energize	1E-4/D	--	3
OPSO72BT	Level Switch 2-3-72B	Does not operate	1E-4/D	--	3
042B12BJ	Functional Test LIS-3-58C	Out of service	1.4E-3	--	0

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ORE008BV	Relay 14A-K8B	Does not energize	1E-4/D	--	3
OPSO79BT	Level Switch 2-3-79B	Does not operate	1E-4/D	--	3
042B19BJ	Functional Test LITS-3-58D	Out of service	1.4E-3	--	0
ORE006AV	Relay 14A-K6A	Does not energize	1E-4/D	--	3
OC0222U0	Contact 14A-K22B	Does not remain closed	1E-7/hr	367	↓
OC0204U0	Contact 14A-K4B	Does not remain closed	1E-7/hr	367	
ORE213UV	Relay 14A-K13B	Does not energize	1E-4/D	--	
ORE225UV	Relay 14A-K25B	Does not energize	1E-4/D	--	

B-228

TABLE B-44. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ORE226UV	Relay 14A-K26B	Does not energize	1E-4/D	--	3
HOUSTRAN	Transient initiator	On/off	--	--	--
OPSDWHPX	Drywell pressure switches	Operator miscalibration	2.9E-4	--	--
OPSLVLX	Low water level switches	Operator miscalibration	2.4E-6	--	--

B-229

TABLE B-45. CORE SPARY SYSTEM FAILURE DATA SUMMARY

Component/Activity	Failure Mode	Time to Detect (T _D)	Time to Repair (T _R)	Fault Duration Time ^a (T = T _D + T _R)	Failure Probability	Unavailability (A)	Remarks
Check valve	Does not open	--	--	--	1E-4/D	1E-4	--
Motor-operated valve	Does not open	--	--	--	1E-3/D	1E-3	--
Motor-operated valve control circuit	No output	360 hr	7 hr	367 hr	7.7E-6/hr + 4.1E-4/D	3.2E-3	$\bar{A} = 4.1E-4 + 7.7E-6T$ $T = T_D + T_R$ T_R --WASH-1400 value T_D = half test interval
Pipe	Rupture	1 hr	24 hr	25 hr	1E-10/hr	2.5E-9	$T_R = 24$ hr, assumed time to shut down plant $T_D = 1$ hr, assumed since keep-full should alarm by then to indicate a ruptured pipe
Pump	Does not start	--	--	--	1E-3/D	1E-3	--
Pump	Does not run	0 hr	37 hr	8 hr	3E-5/hr	2.4E-4	--
Pump motor-control circuit	No output	360 hr	7 hr	367 hr	7.6E-6/hr + 4.1E-4/D	2.9E-3	$\bar{A} = 4.1E-4 + 7.6E-6T$ $T = T_D + T_R$ T_R --WASH-1400 value T_D = half test interval
Pump circuit breaker	Does not close	--	--	--	1E-3/D	1E-3	--
Pressure switch	Does not operate	--	--	--	1E-4/D	1E-4	--
Relay	Does not energize	--	--	--	1E-4/D	1E-4	--
Contact remain closed	Does not	2160 hr	7 hr	2167 hr	3E-7/hr	6.2E-4	T_D = half test interval
Simulated automatic actuation test	Inoperable	--	--	--	--	3E-4	From Table B-39
Core spray logic test	Inoperable	--	--	--	--	9E-4	From Table B-39
Core spray pump time delay relay calibration	Inoperable	--	--	--	--	1.5E-4	From Table B-39

B-230

TABLE B-45. (continued)

Component/Activity	Failure Mode	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (A)	Remarks
Core spray sparger to reactor pressure vessel differential pressure calibration	Inoperable	--	--	--	--	9E-4	From Table B-39
Core spray pump discharge pressure calibration	Inoperable	--	--	--	--	9E-4	From Table B-39
Core spray loop discharge pressure calibration	Inoperable	--	--	--	--	6.9E-4	From Table B-39
Core spray auto-initiation inhibit test	Inoperable	--	--	--	--	2.3E-4	From Table B-39
Core spray sparger to reactor pressure vessel differential pressure test	Inoperable	--	--	--	--	1.4E-3	From Table B-39
Flow instrument calibration	Inoperable	--	--	--	--	2.3E-4	From Table B-39
Reactor low water level instrument functional test	Inoperable	--	--	--	--	1.4E-3	From Table B-39
High drywell pressure instrument functional test	Inoperable	--	--	--	--	1.4E-3	From Table B-39
Reactor low pressure instrument calibration	Inoperable	--	--	--	--	6.9E-4	From Table B-39
Reactor low pressure instrument functional test	Inoperable	--	--	--	--	6.9E-4	From Table B-39
Pump oil change	Inoperable	--	--	--	--	4.6E-4	From Table B-40
Core spray reactor low level switch (OPSLLVLX)	Operator miscalibration	--	--	--	--	2.4E-6	See Section 4
Core spray drywell pressure switches (OPSDWHPX)	Operator miscalibration	--	--	--	--	2.9E-4	See Section 4
Passive valve faults	Fail to remain open	--	--	--	1E-4/D	7E-4	Seven valves per loop

a. If $T_D = 0$, then $T = T_R$ if the mission time (8 hr) $> T_R$. If $T_D = 0$, $T =$ mission time (8 hr) if mission time $\leq T_R$.

TABLE B-46. CORE SPRAY SYSTEM CUT SETS
(F_A)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
3.2E-3	5.9	OCK0532G	No
3.2E-3	5.9	OCKC372G	No
3.2E-3	5.9	OCK0091G	No
3.2E-3	5.9	OCK0251G	No
2.9E-3	5.3	OCK001CG	No
2.9E-3	5.3	OCK001DG	No
2.9E-3	5.3	OCK001BG	No
2.9E-3	5.3	OCK001AG	No
1.4E-3	2.6	0142B24J	No
1.4E-3	2.6	0242B24J	No
1.4E-3	2.6	042B211J	No
1.4E-3	2.6	042B212J	No
1.0E-3	1.8	OPM001DR	No
1.0E-3	1.8	OPM001BR	No
1.0E-3	1.8	OCB001AT	No
1.0E-3	1.8	OPM001CR	No
1.0E-3	1.8	OCB001BT	No
1.0E-3	1.8	OCB001DT	No
1.0E-3	1.8	OPM001AR	No
1.0E-3	1.8	OCB001CT	No
1.0E-3	1.8	OVM0372N	No
1.0E-3	1.8	OVM0532P	No
1.0E-3	1.8	OVM0251P	No
1.0E-3	1.8	OVM0091N	No
9.0E-4	1.6	042B241J	No
9.0E-4	1.6	042B242J	No
9.0E-4	1.6	0242B39J	No
9.0E-4	1.6	0142B39J	No
6.9E-4	1.3	0542B53J	No
6.9E-4	1.3	0542B53J	No
4.6E-4	0.8	OPM001AJ	No
4.6E-4	0.8	OPM001BJ	No
4.6E-4	0.8	OPM001CJ	No
4.6E-4	0.8	OPM001DJ	No
Cumulative importance	89.0		

TABLE B-47. CORE SPRAY SYSTEM CUT SETS
(F_B)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
1.0E-5	1.5	OCK0091G,OCK0532G	No
1.0E-5	1.5	OCK0251G,OCK0372G	No
1.0E-5	1.5	OCK0091G,OCK0372G	No
1.0E-5	1.5	OCK0251G,OCK0532G	No
9.3E-6	1.3	OCK001AG,OCK0532G	No
9.3E-6	1.3	OCK001CG,OCK0532G	No
9.3E-6	1.3	OCK0251G,OCK001BG	No
9.3E-6	1.3	OCK001AG,OCK0372G	No
9.3E-6	1.3	OCK0091G,OCK001DG	No
9.3E-6	1.3	OCK0251G,OCK001DG	No
9.3E-6	1.3	OCK001CG,OCK0372G	No
9.3E-6	1.3	OCK0091G,OCK001BG	No
8.4E-6	1.2	OCK001AG,OCK001BG	No
8.4E-6	1.2	OCK001CG,OCK001BG	No
8.4E-6	1.2	OCK001AG,OCK001DG	No
8.4E-6	1.2	OCK001CG,OCK001DG	No
4.5E-6	0.6	042B211J,OCK0532G	No
4.5E-6	0.6	0412B24J,OCK0372G	No
4.5E-6	0.6	0242B24J,OCK0091G	No
4.5E-6	0.6	0142B24J,OCK0532G	No
4.5E-6	0.6	042B212J,OCK0251G	No
4.5E-6	0.6	042B211J,OCK0372G	No
4.5E-6	0.6	042B212J,OCK0091G	No
4.5E-6	0.6	0242B24J,OCK0251G	No
4.1E-6	0.6	0142B24J,OCK001DG	No
4.1E-6	0.6	0242B24J,OCK001AG	No
4.1E-6	0.6	042B211J,OCK001BG	No
4.1E-6	0.6	0242B24J,OCK001CG	No
4.1E-6	0.6	042B211J,OCK001DG	No
4.1E-6	0.6	042B212J,OCK001CG	No
4.1E-6	0.6	0142B24J,OCK001BG	No
4.1E-6	0.6	042B212J,OCK001AG	No
Cumulative importance	30.8		

TABLE B-48. CORE SPRAY SYSTEM CUT SETS
(F_B with LOSP)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
9.0E-4	9.3	ADL001BR,ADL001CR	No
9.0E-4	9.3	ADL001BR,ADL001DR	No
9.0E-4	9.3	ADL001AR,ADL001DR	No
9.0E-4	9.3	ADL001AR,ADL001CR	No
9.6E-5	1.0	ADL001AR,OCK0532G	No
9.6E-5	1.0	ADL001AR,OCK0372G	No
9.6E-5	1.0	ADL001BR,OCK0532G	No
9.6E-5	1.0	OCK0251G,ADL001DR	No
9.6E-5	1.0	OCK0251G,ADL001CR	No
9.6E-5	1.0	ADL001BR,OCK0372G	No
9.6E-5	1.0	OCK0091G,ADL001DR	No
9.6E-5	1.0	OCK0091G,ADL001CR	No
8.9E-5	0.9	ADL001BR,ADL001CJ	No
8.9E-5	0.9	ADL001BJ,ADL001CR	No
8.9E-5	0.9	ADL001AJ,ADL001CR	No
8.9E-5	0.9	ADL001BJ,ADL001DR	No
8.9E-5	0.9	ADL001AR,ADL001CJ	No
8.9E-5	0.9	ADL001AJ,ADL001DR	No
8.9E-5	0.9	ADL001AR,ADL001DJ	No
8.9E-5	0.9	ADL001BR,ADL001DJ	No
Cumulative importance	52.5		

2.8 Vapor Suppression System

In the event of a LOCA within the drywell, reactor water and steam would be released into the drywell air space. The resulting increased drywell pressure would then force a mixture of steam and water through the connecting vent system between the drywell and the pool of water in the pressure suppression chamber (torus). The steam would rapidly condense in the suppression pool resulting in a rapid pressure reduction in the drywell.

2.8.1 Purpose

The vapor suppression system is designed to direct the LOCA effluents to the pressure suppression chamber to prevent containment over-pressurization following a postulated pipe rupture in the drywell. The suppression chamber receives this flow, condenses the steam portion of this flow, and contains noncondensable gases and fission products driven into the chamber. The suppression-chamber-to-drywell vacuum breakers limit the pressure differential between the drywell and suppression chamber.

2.8.2 System Configuration

Overall Configuration. Figure B-18 represents the basic configuration of the vapor suppression system as part of the primary containment. Large vent pipes form a connection between the drywell and the pressure chamber. A total of eight circular vent pipes are provided, each having a diameter of 81 inches. The pressure suppression chamber is a steel pressure vessel in the shape of a torus below, and encircling the drywell, with a centerline diameter of approximately 111 ft and a cross-sectional diameter of 31 ft. It contains approximately 135,000 ft² of water as a maximum and has a net air volume above the water pool of approximately 119,000 ft². The eight drywell vents are connected to a 57-inch diameter vent header in the form of a torus, which is contained within the airspace of the suppression chamber. Projecting downward from the header are 96 downcomer pipes, 24 inches in diameter and terminating approximately 4 ft below the water surface of the pool. Vacuum breakers (18 inches) discharge from the suppression chamber into the drywell to equalize the pressure differential and to prevent a backflow of water from the suppression pool into the vent header system.

Support System Interfaces FMEA. Component/support-system interactions are shown in Table B-49. Support system interfaces include control air and 120 V AC buses for the vacuum relief valves and heating/ventilation/airconditioning interfaces for the drywell and suppression pool.

Instrumentation and Control. No instrumentation and control is required for the vapor suppression function. Lights are provided in the main control room to indicate if vacuum breakers are off their seats.

Testing. Drywell to pressure suppression chamber vacuum breakers are exercised periodically. These requirements are summarized below in Table B-50.

Maintenance. No scheduled maintenance acts were identified from the BFI maintenance schedules for components of the vapor suppression system.

Technical Specification Limitations. The technical specifications require that: when it is determined that two vacuum breakers are inoperable, all other vacuum breaker valves shall be exercised immediately and every 15 days thereafter until the inoperable valves have been returned to normal service.

2.8.3 System Operation

Operation of the vapor suppression system is described in the previous section, "Overall Configuration."

2.8.4 Fault Tree

Other than failure of the primary containment (torus rupture), all of the faults represented on the vapor suppression system fault tree (Figure B-19) would result in bypass leakage from the drywell to the airspace of the wetwell. This leakage could conceivably pressurize the wetwell airspace to the same pressure as the drywell, preventing the required 2 psi differential pressure between the drywell and wetwell airspace to expel

water from the downcomer pipes. Appendix U of the Browns Ferry FSAR indicates the maximum allowable leakage area is approximately 0.3 ft² (8-inch diameter pipe) for a primary system break area range that encompasses the small, intermediate, and lower-end range of the large LOCA break sizes considered in the BFl risk assessment. The house event VSSHOUSE is "on" for LOCAs and "off" for transients.

Success/Failure Criteria. Success criteria for the vapor suppression system is defined as adequate suppression pool level and no bypass leakage from drywell to wetwell.

Major Assumptions. Thus, it is conservatively assumed that any of the faults identified (i.e., pipe ruptures or any vacuum breaker failed open) would result in failure of the vapor suppression system to perform its function following a LOCA of any size. The diamond event for operational faults regarding wetwell water level being too high, too low, or too hot are assumed to be insignificant contributors to vapor suppression system failure because of the instrumentation redundancy and frequency of operator observance of this instrumentation.

Basic Events. The information associated with the various basic events listed in the fault tree is summarized in the vapor suppression system fault summary short form, Table B-51. In addition, the failure data associated with these basic events is summarized in Table B-52. Table B-53 lists the dominant contributors to vapor suppression system unavailability.

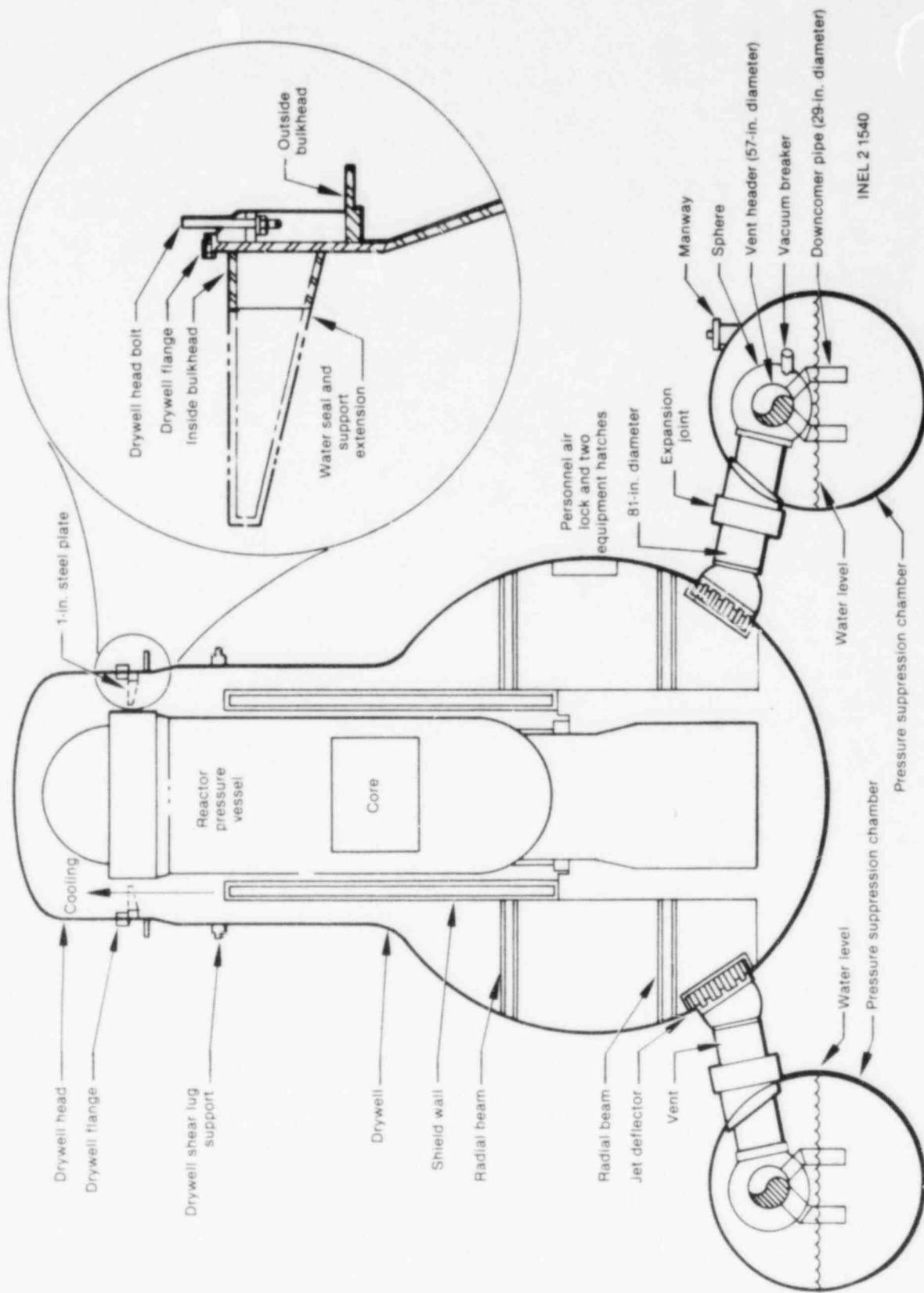


Figure B-18. Vapor suppression part of the primary containment system.

TABLE B-49. VAPOR SUPPRESSION SYSTEM FMEA OF COMPONENT/SUPPORTING-SYSTEM INTERACTIONS

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
FCV-64-28A thru M (12 vacuum relief valves)	Control air	Corresponding actuator FSV-64-28A thru M	Insufficient air pressure	Valves cannot be tested	Does not interfere with vapor suppression phenomena
	120 V AC Bus B	HS-64-28A thru M	No power to board	No power to valve indicating lights	Does not interfere with vapor suppression phenomena
Drywell	HVAC	FCV-64-18 FCV-64-29 FCV-64-31	Valve fails to close on high drywell pressure	None	Failure of a single valve to close is not serious; however, failure of two or more valves to close may create a flow path between the drywell and suppression pool, thereby interfering with the vapor suppression ability of the containment
Suppression pool	HVAC	FCV-64-19 FCV-64-32 FCV-64-34	--	--	--

B-238

TABLE B-50. VAPOR SUPPRESSION SYSTEM TEST REQUIREMENTS SUMMARY

<u>Component Undergoing Test</u>	<u>Type of Test</u>	<u>Test Procedure Number</u>	<u>Components Aligned Away from Engineered Safeguards Position for Test</u>	<u>Expected Test Frequency</u>	<u>Expected Test Outage Time</u>	<u>Remarks</u>
FCV-64-28A thru FCV-64-28M (12 valves)	Open-close cycle	SI 4.7.A.4.a	Yes	Once every month	12 min	Only one valve is tested at a time

B-239

B-240

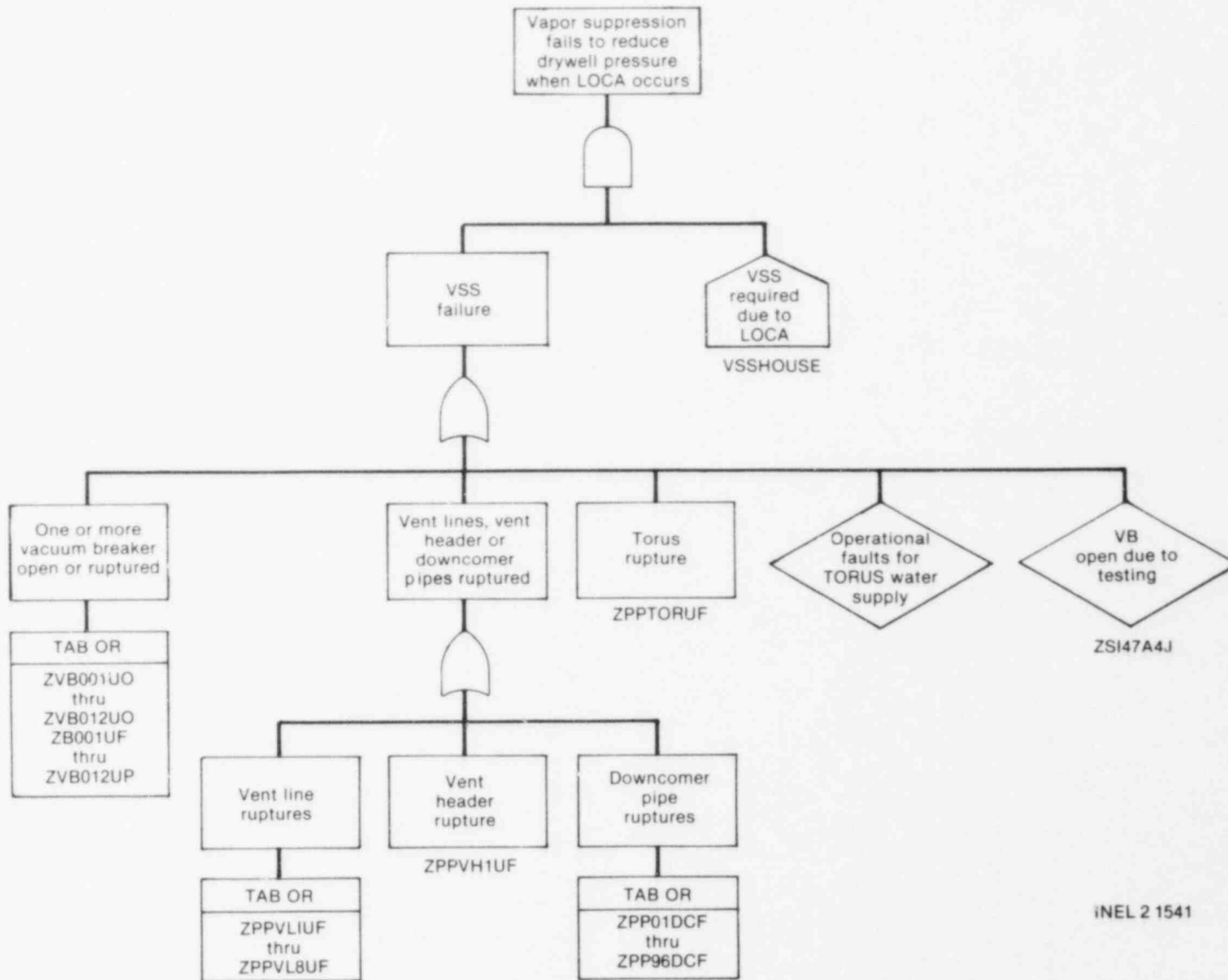


Figure B-19. Vapor suppression fault tree.

TABLE B-51. VAPOR SUPPRESSION SYSTEM FAULT SUMMARY SHORT FORM

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ZVBO01U0 thru ZVBO12U0	Vacuum breaker Valve FCV-64-28A thru FCV-64-28M	Premature open	1E-6/hr	--	3
ZVBO01UF thru ZVBO12UF	FCV-64-28A thru FCV-64-28M	Rupture	1E-8/hr	--	10
ZPPVLIUF thru ZPPVL8UF	Vent Line 1 thru 8	↓	1E-10/hr/ section	--	30
ZPPTORUF	Torus		1E-10/hr/ section	--	30
ZPPVH1UF	Vent header				
ZPP01DCF thru ZPP96DCF	Downcomer Pipe 1 thru 96		1E-10/hr/ section	--	30
ZSI47A4J	Vacuum breaker test	Open due to test	2.7E-4	--	0

B-241

TABLE B-52. VAPOR SUPPRESSION SYSTEM FAILURE DATA SUMMARY

Component/Activity (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (A)	Remarks
Vacuum breaker valve (VB)	Premature open (O)	0 hr	24 hr	8 hr	1E-6/hr	8E-6	Used primary safety valve rate
	Leakage/ rupture (F)	360 hr	24 hr	384 hr	1E-8/hr	3.8E-6	Used solenoid valve rate
Downcomers, vent lines, headers (PP)	Rupture (F)	6480 hr	--	6480 hr	1E-10/hr/section	6.5E-7	Used pipe >3 inch; rate detection time based on 18 month operating cycle
Torus (PP)	Rupture (F)	0 hr	24 hr	8 hr	1E-10/hr	8E-10	Torus failure would be immediately detectable based on instrumentation
Vacuum breakers (ZSI47A4J)	Open due to test	--	--	--	--	2.7E-4	From Table B-50

a. If $T_D = 0$, then $T = T_R$ if the mission time (8 hr) $> T_R$. If $T_D = 0$, then $T =$ mission time (8 hr) if mission time $\leq T_R$.

B-242

TABLE B-53. VAPOR SUPPRESSION SYSTEM CUT SETS

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
2.7E-4	73.6	ZS147A4J	No
9.6E-5	<u>26.2</u>	ZVB012UO	No
Cumulative importance	99.8		

2.9 Control Rod Drive Hydraulic System

2.9.1 Purpose

The CRDH system is designed to supply and control hydraulic pressure and flow requirements to the control rod drive mechanisms. Water is supplied to the hydraulic control units (HCUs). Each HCU controls the flow to and from an individual drive. Water that is discharged from the drives during a scram flows through the HCUs to the scram discharge volume. During normal operation rod positioning, this discharge flows through its HCU and exhaust header to the reactor vessel.

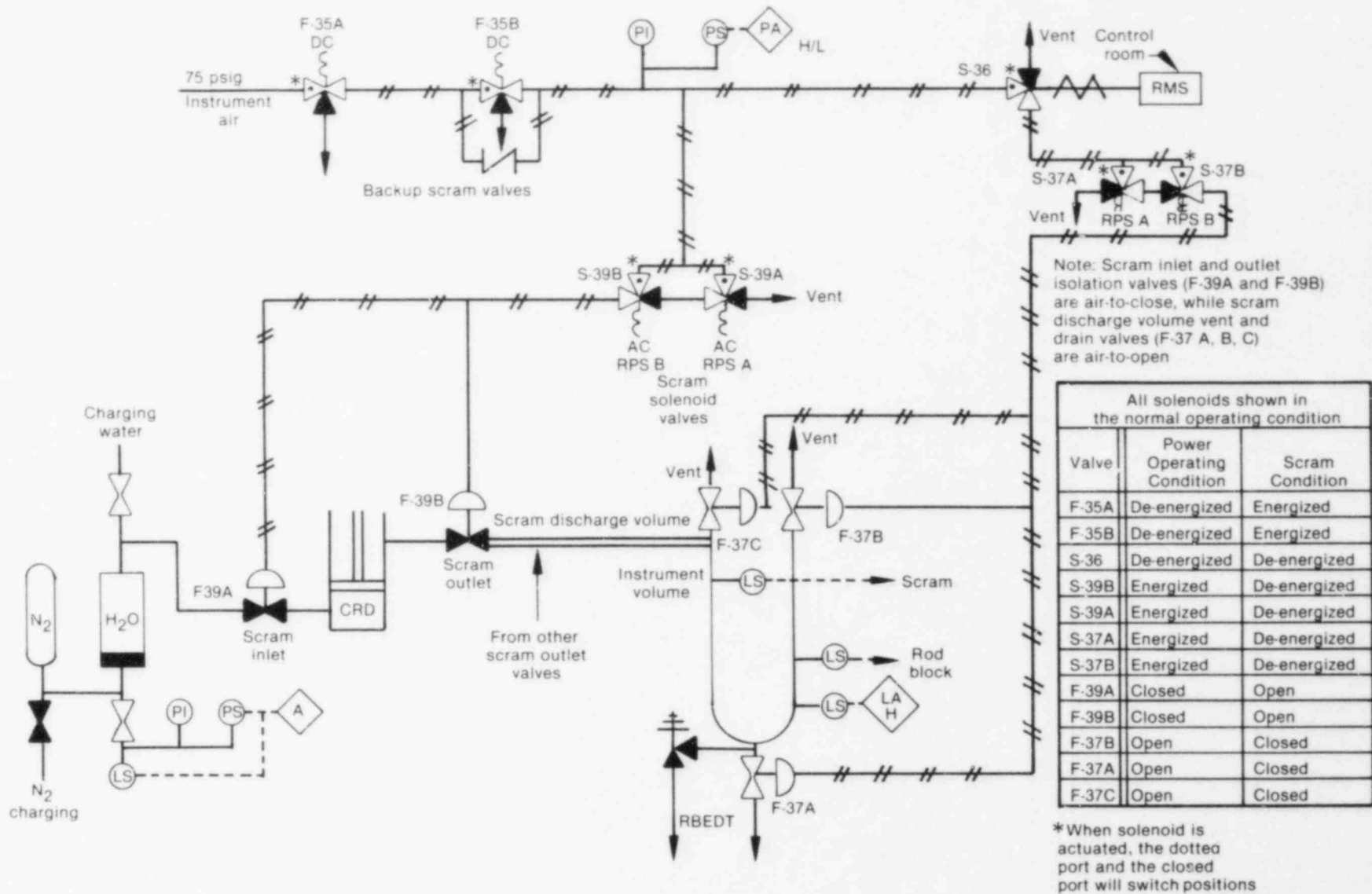
2.9.2 System Configuration

Overall Configuration. A simplified schematic of the CRDH system is shown in Figure B-20. This figure shows one of the 185 HCUs and scram arrangements and is typical of all 185 units. During a reactor scram, the scram inlet valves and scram discharge outlet valves open, allowing water from the CRDH system to flow into the drives, thereby inserting the control rods. Operation of the scram inlet valves and the scram discharge outlet valves is controlled by the scram pilot solenoid valves.

The pilot solenoid valves are operated by signals received from the RPS. Two scram pilot solenoid valves for each HCU control both the scram inlet valve and scram discharge outlet valve for that HCU. The scram inlet and discharge outlet valves are designed to open on loss of air pressure. The pilot solenoid valves are normally energized and are aligned to provide air pressure to the scram inlet and discharge valves, thus keeping them closed. Upon loss of electrical signal, the pilot solenoid valve inlet ports are closed and the exhaust ports are opened, which depressurizes the scram inlet and discharge outlet valves. This opens the valves (inserting the rods) and trips the reactor.

The scram accumulators store sufficient energy to insert a rod during scram independently of any other energy source. The accumulator is a water volume stored under nitrogen pressure. Loss of accumulator pressure is alarmed in the control room. Although accumulator pressure provides the energy for initial rod acceleration, once accumulator pressure has equalized with vessel pressure, the primary driving force for control rod

B-244



INEL 2 1542

Figure B-20. CRDH system.

insertion is the reactor vessel pressure. The accumulators are required for successful rod insertion only when the reactor vessel pressure is less than 400 psi.

The scram discharge volume, which is provided by the instrument volume and the scram discharge headers, is designed to contain water from all the drives during a scram. During normal plant operation, the volume is empty with both its drain valve and its two vent valves open. These valves close upon receipt of a scram signal. During a scram, the scram discharge volume is partly filled with water, which is discharged from above the drive pistons. An isometric view of the scram discharge volume equipment is shown in Figure B-21.

The CRDH system also performs rod insertion and withdrawal during normal plant operation. Components other than those described above may be used during normal operation. However, the scope of this analysis does not extend beyond the scram function and those components necessary to achieve successful scram.

System Interfaces. The CRDH system has, as its primary interfaces, the RPS and the offsite AC power system. The most important interface is that with the RPS. The RPS provides the A and B reactor trip signals that are necessary to open the scram inlet and discharge outlet valves, thus inserting the control rods and scrambling the reactor.

The CRDH system interface with electrical power is less important in terms of CRDH reliability, because the CRDH system is designed to scram the reactor upon loss of electricity to the scram pilot solenoid valves. Upon loss of electrical signal, the pilot solenoid valves depressurize the scram inlet and discharge outlet valves, inserting the control rods.

Instrumentation and Control. Discharge volume instrumentation, alarms, and interlocks guard against reactor operation when, in the event of a scram, there is not sufficient free volume in the discharge volume to receive discharge water. Three different water levels in the discharge volume are monitored. The first level is at 3 gallons above reference zero. At the first level, an alarm is activated. The second level is 25 gallons above reference zero. At the second level, a rod withdrawal block is initiated that prevents any further rod withdrawal. The third level is 50 gallons above reference zero. At the third level, a scram is initiated while sufficient free volume is still available to receive the scram discharge.

Testing. The CRDH system is not subject to any periodic testing procedures that contribute to system unavailability during power operation.

Maintenance. The CRDH system is not subject to any unscheduled maintenance procedures that contribute to system unavailability during power operation.

Technical Specification Limitations. System technical specifications require that the control rod accumulators be determined operable at least once per week by verifying that the pressure and level detectors are not in the alarmed condition. Control rods are considered to be inoperable if

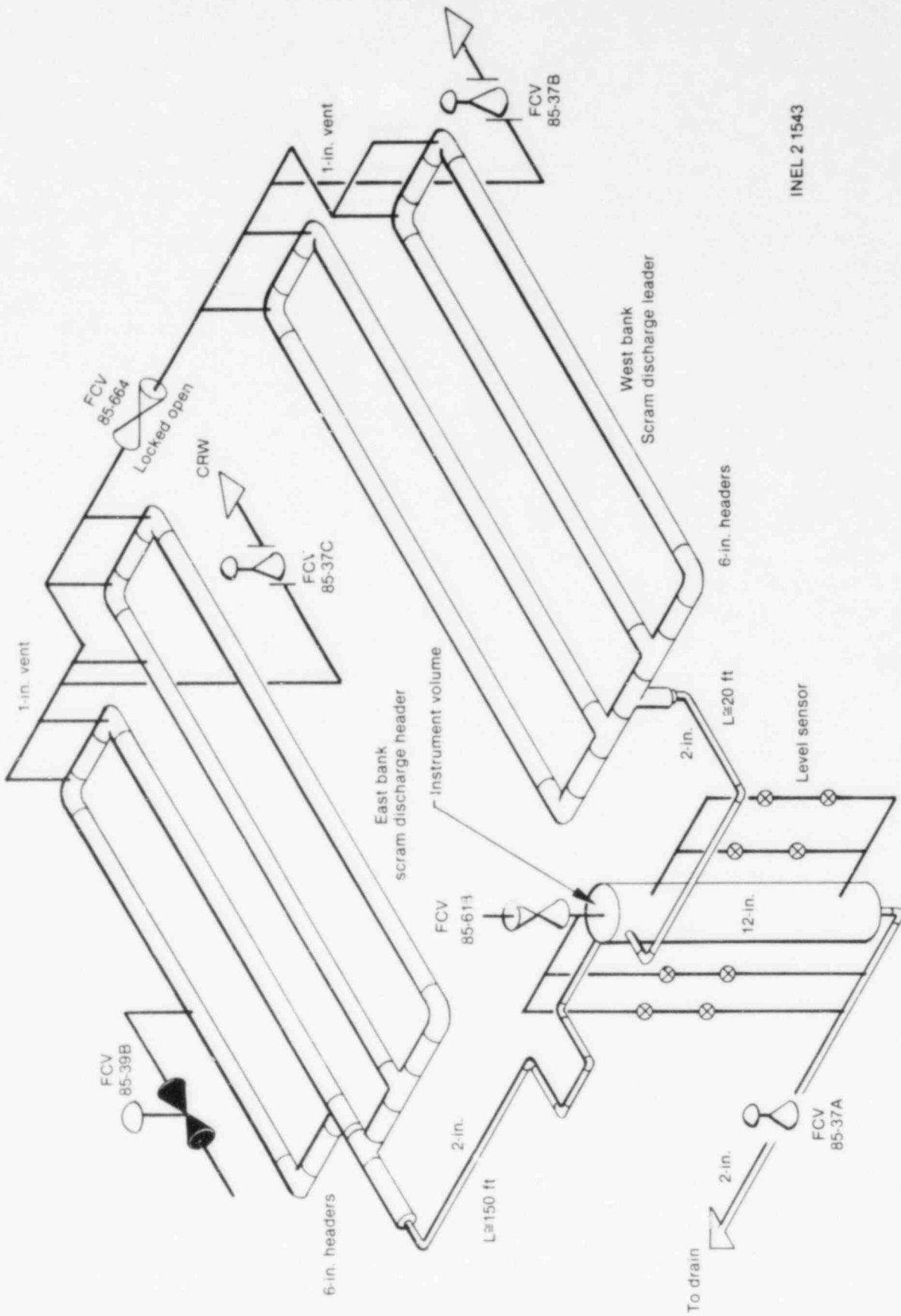


Figure B-21. Scram discharge volume equipment.

they have inoperable accumulators or if their position cannot be positively determined. The specifications further require that when a partially or fully withdrawn control rod is determined to be inoperable, the reactor shall be brought to the cold shutdown condition within 24 hours and not restarted unless: (a) investigation demonstrates that the cause of failure is not a failed rod drive mechanism collet housing, and (b) adequate shutdown margin has been demonstrated for all control rods capable of being withdrawn and all inoperable control rods.

2.9.3 System Operation

CRDH operation is discussed in the previous section, "Overall Configuration."

2.9.4 Fault Tree

The CRDH system is currently subject to the close scrutiny by a number of parties concerned with questions of nuclear safety.³ Although a number of problems⁴ and potential failure modes of the CRDH system have been identified and described, these potential failure modes do not lend themselves well to the binary fault modeling that characterizes the fault tree analysis technique. Therefore, rather than attempting to analyze the CRDH system with fault tree techniques, it is more appropriate to provide a qualitative, phenomenological discussion of the potential failure modes that have been identified for the CRDH system. A CRDH system fault tree is given in Figure B-22.⁵ This fault tree is not a representation of a fault tree analysis. Rather, it represents a graphical depiction from a phenomenological analysis of CRDH system failure of the minimum and sufficient failure modes that are necessary to cause failure of the CRDH system to provide adequate reactor trip protection. No attempt has been made to quantify this fault tree.

As is shown in Figure B-22, the CRDH system fails to provide a reactor trip if either of two RPS trip signals are not received by the scram discharge valves or if either of the east or west trip discharge headers are filled with water. The trip discharge headers may be filled with water only if water is introduced into a header and if the header does not drain properly.

The most likely way in which water may enter a discharge header is via leakage past any of the scram discharge valves that discharge into that header. The question arises as to how many of the discharge valves must leak into the header in order to fail the system. This is best addressed by stating that the point of interest is the rate at which water is introduced into the header rather than how many valves that leak. At a minimum, leakage past one scram discharge valve may be sufficient to fail the system if the leak rate is such that water is entering the header faster than the header is draining to the scram instrument volume. A number of phenomenological considerations affect the rate at which the discharge headers drain to the instrument volume.

The first consideration is that both the east and west discharge headers consist of four 6-inch pipes that connect with a single 2-inch line that drains the contents of the headers to the scram instrument volume.

B-248

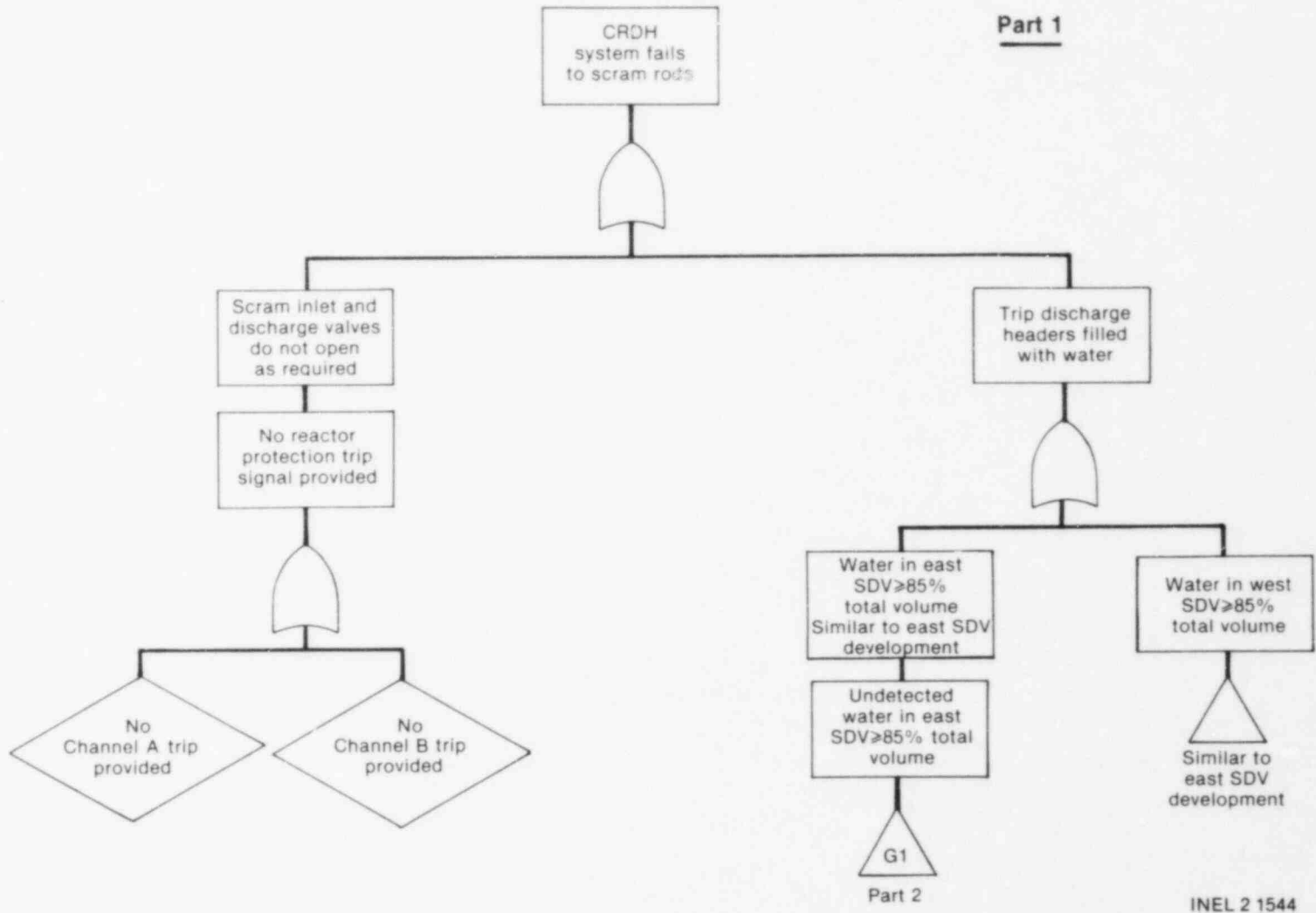


Figure B-22. CRDH fault tree.

2.10 Power Conversion System, Including Condensate/Booster Pumps

2.10.1 Purpose

The PCS provides a means of bringing the reactor to a stable shutdown condition following a transient event that does not preclude PCS availability. The PCS can provide both the vessel water inventory and decay heat removal functions by removing steam from the reactor, condensing the steam, and returning the water to the reactor via the condensate and feedwater systems. Successful PCS operation requires that the condenser be available and the feed system provide makeup water to the reactor vessel.

2.10.2 System Configuration

Overall Configuration. The PCS consists primarily of the main steam, condensate, and feedwater systems. Simplified flow diagrams for these systems are provided by Figures B-23 and B-24.

During normal operation, steam from the reactor flows directly to the main turbine generator via the main steam lines. Condensed extraction steam is cascaded through the feedwater heaters to the main condenser where it is deaerated and collected in the condenser hotwell along with condensed steam from the turbine exhaust and miscellaneous drains from the turbine cycle. Condensate pumps, taking suction from the hotwell, pump the condensate through the air ejector condensers, gland exhaust condensers, and filter/demineralizers to the condensate booster pumps, which increase the condensate pressure and discharge through the low pressure heaters to the reactor feed pump suctions. The reactor feed pumps discharge through the high pressure heaters to the reactor.

Under abnormal conditions requiring an emergency shutdown from power, and if the PCS is not rendered unavailable by the initiating event, the following actions occur. The main turbine is tripped and is isolated from the main steam system by the turbine stop valves and turbine control valves. There are nine turbine bypass valves that open to take steam from ahead of the turbine stop valves and discharge to the condenser. The bypass valves are sized to pass up to 30% of maximum turbine design flow. The condensed steam drops to the lower section of the condenser, called the condenser hotwell. The operator manually trips all but one of the operating condensate pumps taking suction from the condenser hotwell. The condensate discharge passes through filter/demineralizers to the suction header for the condensate booster pumps. The operator manually trips all but one of the operating condensate booster pumps. The remaining condensate booster pump discharges through a series of heaters to raise the condensate water temperature.

The feedwater system is actually an extension of the condensate system, which receives water from the condensate system at booster pump discharge pressure and increases the pressure via a steam-driven reactor feed pump in order to feed the reactor through the high pressure heaters, which further raises the temperature of the feedwater. The feedwater flow is combined into a 30-inch mixing header and then is divided into two 24-inch lines to feed the reactor through the feed sparger rings. The operator trips all but one of the operating reactor feedwater pumps.

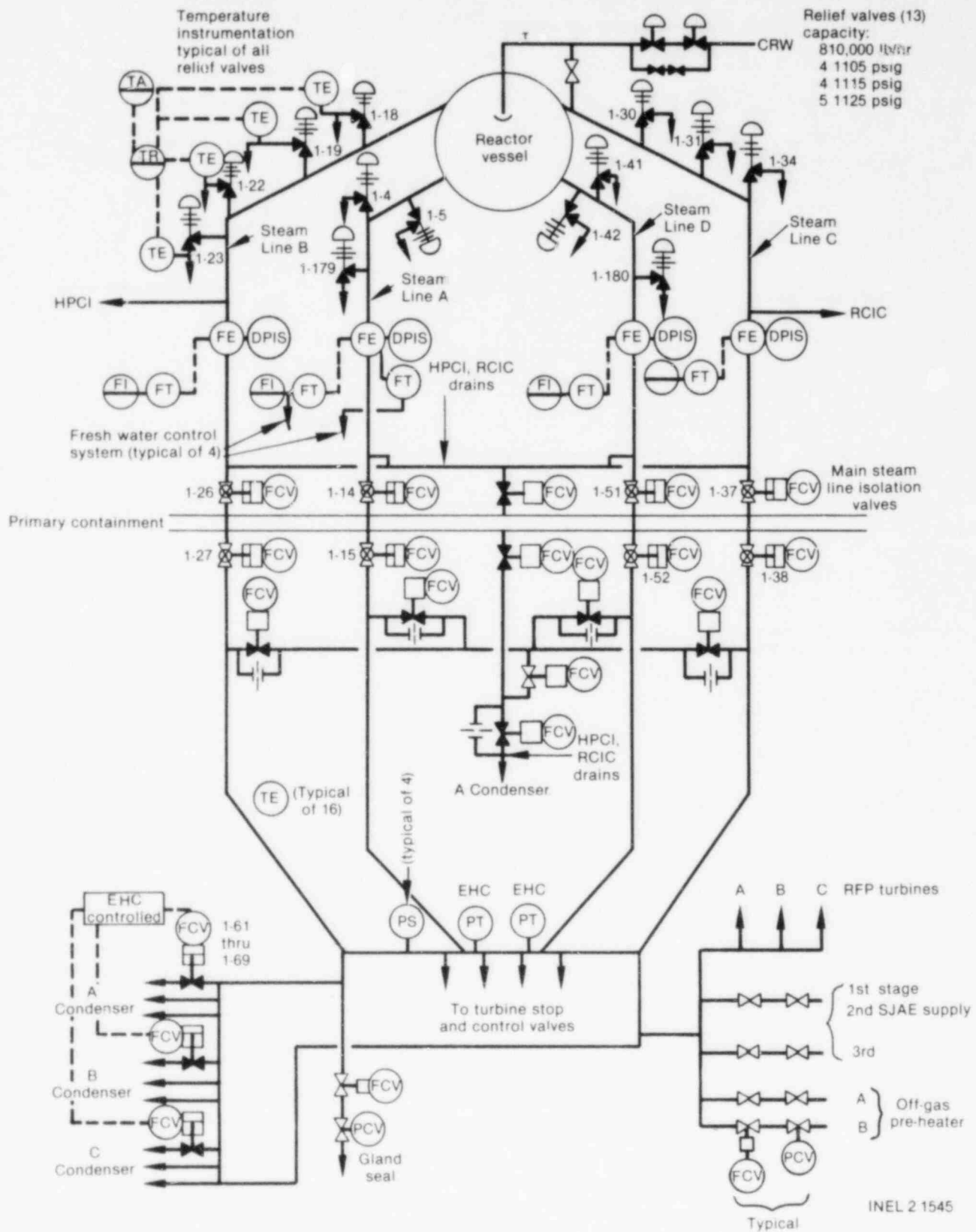


Figure B-23. Main steam system.

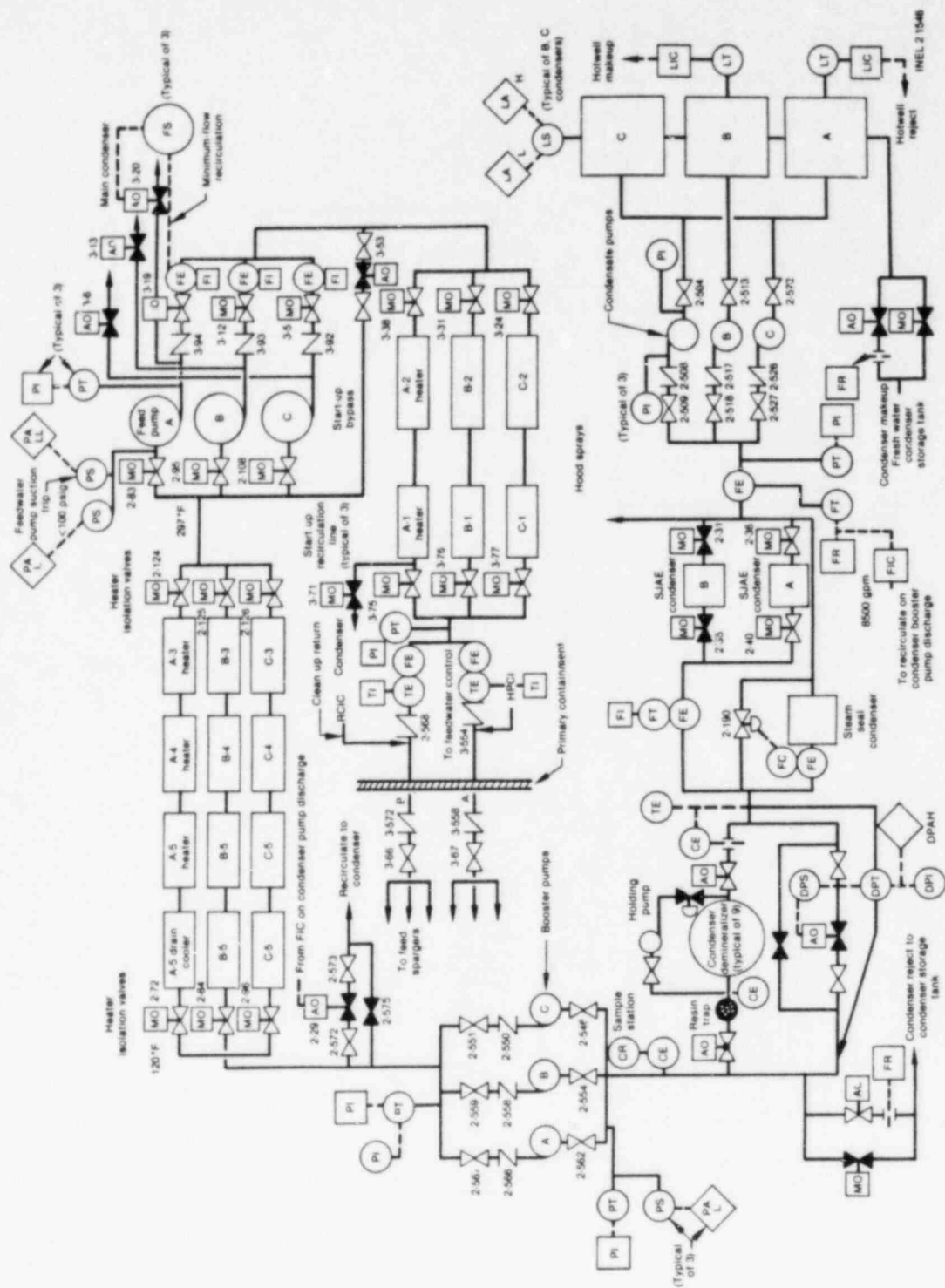


Figure B-24. Condensate and feedwater systems.

Low Pressure Injection via the Condensate System. Under abnormal conditions following a transient and given the high pressure makeup systems have failed to maintain vessel water inventory, the condensate portion of the PCS may be used as an alternative for providing low pressure makeup capability. After having successfully manually depressurized the reactor, one condensate pump and one condensate booster pump can provide sufficient makeup capability at low pressure. The low pressure injection path of makeup water would be the same as described for the PCS, with the exception that the feed pumps are bypassed. Makeup water would bypass the feed pumps through the startup bypass portion of the feed system. This method of injection can only be provided where reactor pressure is less than 350 psig. Event W on the transient systemic event tree (Appendix A) depicts this method of low pressure injection. This method is described in EOI-41, Water Makeup Methods to Reactor Vessel.

2.10.3 Fault Tree

As discussed in Section 1 of Appendix A, many of the transient initiators and accidents considered in the Browns Ferry Risk Assessment cause the PCS to be unavailable. In most of these cases, PCS is rendered inoperable due to subsequent closure of the MSIVs from low reactor vessel level or faults that directly disable PCS, such as a loss of offsite power.

For those transients where the PCS remains available following the initiator, the PCS can provide both the vessel water inventory and decay heat removal functions by removing steam from the reactor, condensing the steam, and returning the water to the reactor via the condensate and reactor feedwater pumps.

A fault model was developed for the PCS as it would be configured for long term decay heat removal. This model essentially consists of passive hardware faults, since the PCS is in normal operation at the time an accident or transient occurs. That is, other than turbine bypass valves having to open, there are essentially no components that have to change state. Rather, the operator is instructed to take components out of service (GOI 100-1, Step VI-Emergency Shutdown from Power). For example, only one condensate, condensate booster, and reactor feedwater pump are required for post-accident conditions, although three of each may have initially been available. The quantification of this fault model based on these redundant features yields an unavailability value of 5.1×10^{-5} . However, this fault model does not include the multiple interfaces of the PCS with the balance-of-plant control system, the electro-hydraulic control system.

The electro-hydraulic control system for Browns Ferry is an extremely large and complex integrated system and was considered beyond the scope of this study. As a result, without the electro-hydraulic control system fault contributions to the PCS model, it was felt that this PCS unavailability calculation would be nonconservative. Therefore, the PCS failure probability from WASH-1400 was used for accident sequence screening purposes in the event trees. The WASH-1400 PCS value is 7×10^{-3} and was based on actual operating experience of U.S. power reactors (WASH-1400, Appendix V, Page V-41) for failure to remove long-term decay heat. No sequences on the PCS available event tree were found to be significant ($>10^{-6}$) for those involving subsequent PCS failure.

For those transient initiators that result in the PCS being initially unavailable for accident mitigation, there is still some probability that the condensate system may remain operable or be restored in a time frame that allows these low pressure pumps to be used to provide makeup water to the reactor for successful vessel water inventory. The probability of the loss of feedwater for greater than about 1/2 hour has been estimated, based on U.S. power reactor operating experience, to be 10^{-2} (WASH-1400, Appendix V, Page V-40). No credit was taken for condensate system restoration following a loss of offsite power transient event.

2.11 Standby Coolant Supply System

The SBCS system is a special mode of alignment of the RHRSW system to the RHR system to provide a standby source of coolant to the reactor. The D supply header of the RHRSW system contains piping and valves that cross-connect the RHRSW system with the RHR system. The purpose of this crosstie is to inject RHR service water into the reactor vessel or containment, via the RHR piping, for final flooding if all other sources of coolant are expended. This mode of coolant injection to the reactor is included in the description RHRSW system (see Section 3.2). SBCS system cut sets are given in Tables B-54 and B-55.

2.12 Recirculation Pump Trip System

2.12.1 Purpose

During normal operation, the recirculation pumps are used to vary reactor power over a portion of the power range by varying pump flow. During transient conditions that cause sharp increases in reactor pressure, the recirculation pumps are tripped to rapidly reduce flow through the core and consequently to reduce reactor power level very quickly.

2.12.2 System Configuration

Overall Configuration. The RPT is accomplished by opening the breakers for the recirculation pumps. The RPS provides the signal to the breaker control circuit to trip the breaker. Opening the breaker causes a rapid decrease in pump flow, which in turn reduces reactor power. The reduction in reactor power also limits the pressure rise in the reactor to acceptable limits. Figure B-25 shows the RPT trip circuit.

System Interfaces. The RPT receives actuation signals from the RPS. Control power for recirculation Pump 1A comes from 250 V DC RMOV Board 1A with alternate supply from 250 V DC battery Board 3. Recirculation Pump 1B normally receives control power from 250 V DC RMOV Board 1B. The alternate supply is 250 V DC battery Board 1.

Testing and Maintenance. Technical specifications require both recirculation pumps be operating during a reactor operation. Therefore, no testing or maintenance is performed during this time.

TABLE B-54. SBCS SYSTEM CUT SETS
(Normal Power)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
8.8×10^{-3}	21.0	XCK057DG	No
8.8×10^{-3}	21.0	XCK052DG	No
8.8×10^{-3}	21.0	XCK1012G	No
8.0×10^{-3}	19.0	XEOI041D	Yes
3.3×10^{-3}	7.9	RCK067AG	No
1.0×10^{-3}	2.4	RVM0672P	No
1.0×10^{-3}	2.4	XVM1012T	No
1.0×10^{-3}	2.4	XVM057DT	No
1.0×10^{-3}	<u>2.4</u>	XVM052DT	No
Cumulative importance	99.3		

TABLE B-55. SBCS SYSTEM CUT SETS
(with LOSP)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
8.8×10^{-3}	19.1	XCK057DG	No
8.8×10^{-3}	19.1	XCK052DG	No
8.8×10^{-3}	19.1	XCK1012G	No
8.0×10^{-3}	17.4	XEOI041D	Yes
3.3×10^{-3}	7.2	RCK067AG	No
1.0×10^{-3}	2.2	RVM0672P	No
1.0×10^{-3}	2.2	XVM1012T	No
1.0×10^{-3}	2.2	XVM057DT	No
1.0×10^{-3}	<u>2.2</u>	XVM052DT	No
Cumulative importance	90.1		

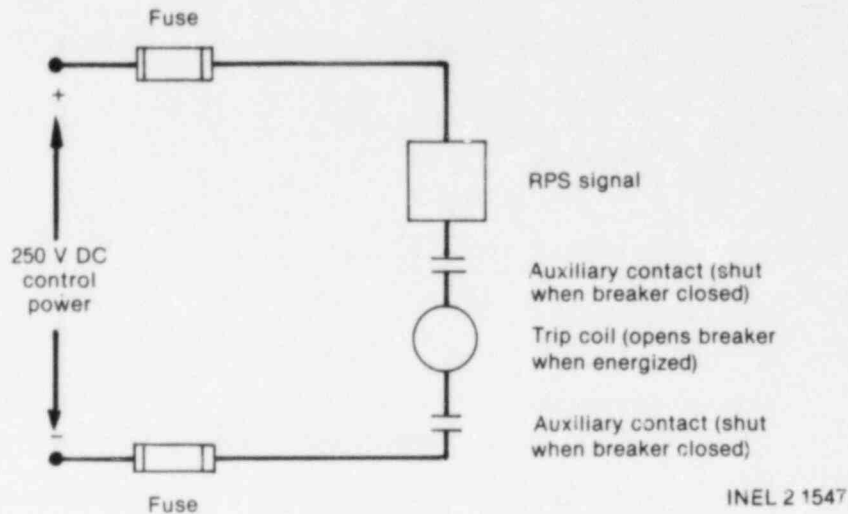


Figure B-25. Recirculation-pump trip circuit.

2.12.3 System Operation

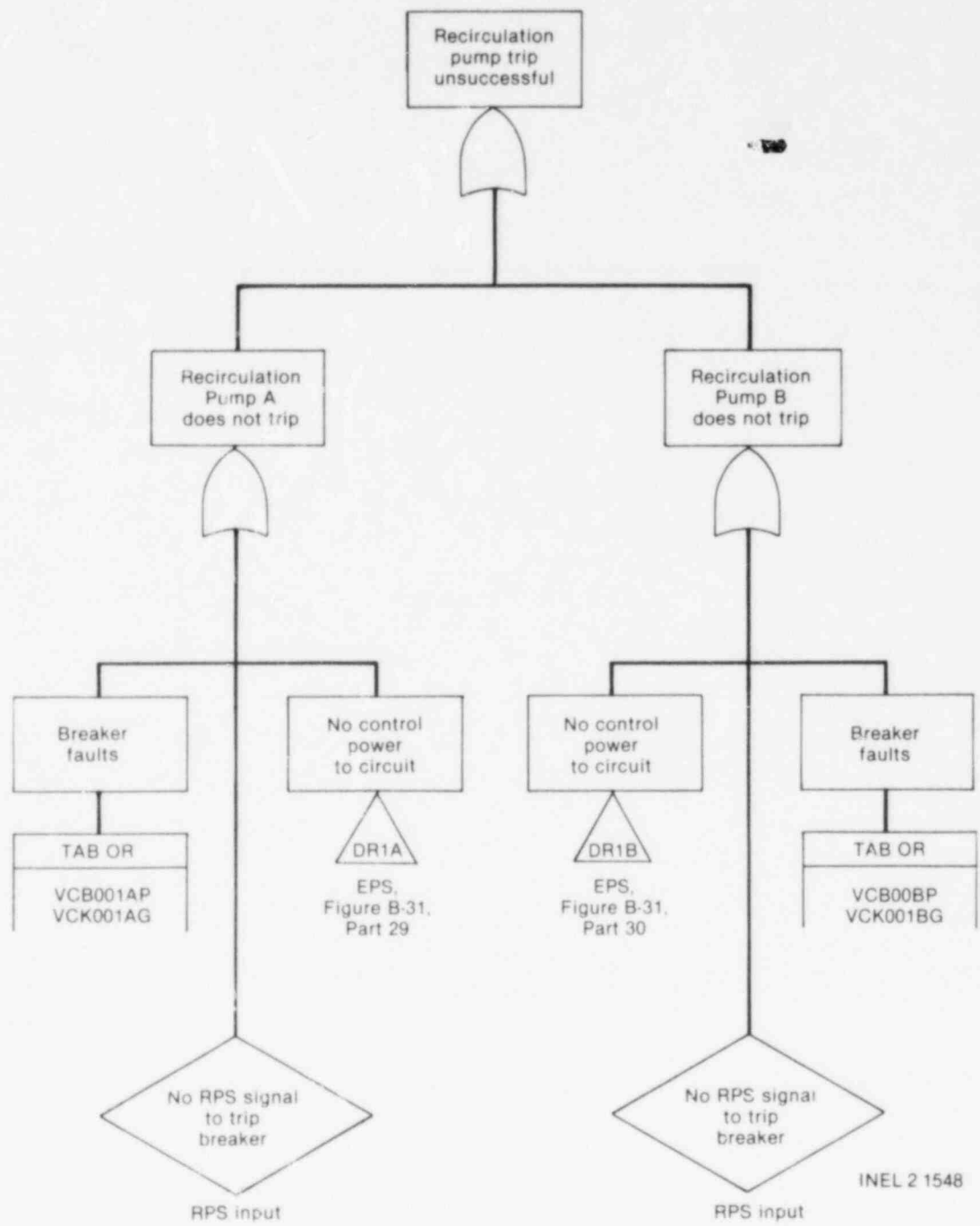
Operation of the RPT circuitry is automatic and is described in the previous section, "Overall Configuration."

2.12.4 Fault Tree

Figure B-26 is the RPT fault tree. Failure of either recirculation pump to trip constitutes failure of the RPT. Rather than modeling the RPS, a single event is used to represent failure of the RPS to initiate the RPT. The WASH-1400 value for common mode failures of the RPS is used for RPS failure in this fault tree.

Major Assumptions. The only major assumption made during RPT fault tree construction was that insufficient time exists for the operator to manually initiate RPS or manually trip the recirculation pump circuit breakers.

Basic Events. The information associated with the various events listed in the fault tree, along with the failure data, is provided in the RPT fault summary short form, Table B-56. Table B-57 lists the dominant contributors to RPT unavailability.



INEL 2 1548

Figure B-26. Recirculation-pump trip-circuit fault tree.

TABLE B-56. RPT 89.1. SUMMARY SHORT FORM

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
VCBO01AP	Recirculation Pump 1A circuit breaker	Fails to open	1E-3/D	--	3
VCBO01BP	Recirculation Pump 1B circuit breaker	Fails to open	1E-3/D	--	3
RPSINPUT	No signal from reactor pressure vessel to initiate reactor pump trip	Fails to initiate	1.9E-6	--	10
VCK001AG	Recirculation Pump 1A control circuit	No output	3.3E-3	--	10
VCK001BG	Recirculation Pump 1B control circuit	No output	3.3E-3	--	10

B-259

TABLE B-57. RPT SYSTEM CUT SETS

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
3.3 E-3	38.4	VCK001AG	No
3.3 E-3	38.4	VCK001BG	No
1.0 E-3	11.6	VCB001AP	No
1.0 E-3	11.6	VCB001BP	No
Cumulative importance	100.0		

2.13 Main Steam Isolation Valves

2.13.1 Purpose

The purpose of the MSIVs are to provide isolation of the main condenser from the reactor vessel when the PCS is unavailable so that the high or low pressure injection safety systems can maintain vessel water inventory.

2.13.2 System Configuration

Overall Configuration. The main steam isolation system consists of four main steam lines, eight main steam isolation valves (MSIVs), 13 steam relief valves (of which six are utilized for the automatic depressurization system), and steam line flow restrictors located between the relief valves and inboard MSIVs of each main steam line. There are two MSIVs per steam line, one located inside the primary containment (inboard) and one located outside the primary containment (outboard) as shown by Figure B-27. The four main steam lines connect to a common manifold in the turbine building. The common manifold supplies steam to the gland seal steam system, the feed pump turbines, the steam jet air ejectors, and nine turbine bypass valves. Four main steam lines continue from the common manifold to the main turbine; each of these lines has a turbine stop valve upstream of the turbine control valve.

The MSIVs are designed to close automatically when the reactor vessel water level falls below preset values. These valves are air-piston operated with a spring to close then upon loss of operating air. Redundant level switches deenergize both the DC and AC solenoid control valves, which allows air to escape beneath the piston resulting in rapid closure of the valve.

System Interfaces. Closure of the MSIVs does not depend on any support system interfaces other than its associated redundant instrumentation.

Instrumentation and Control. Four reactor low level indicating switches are utilized in a one-out-of-two-twice logic scheme to deenergize the AC and DC solenoid control valves when reactor vessel water level falls

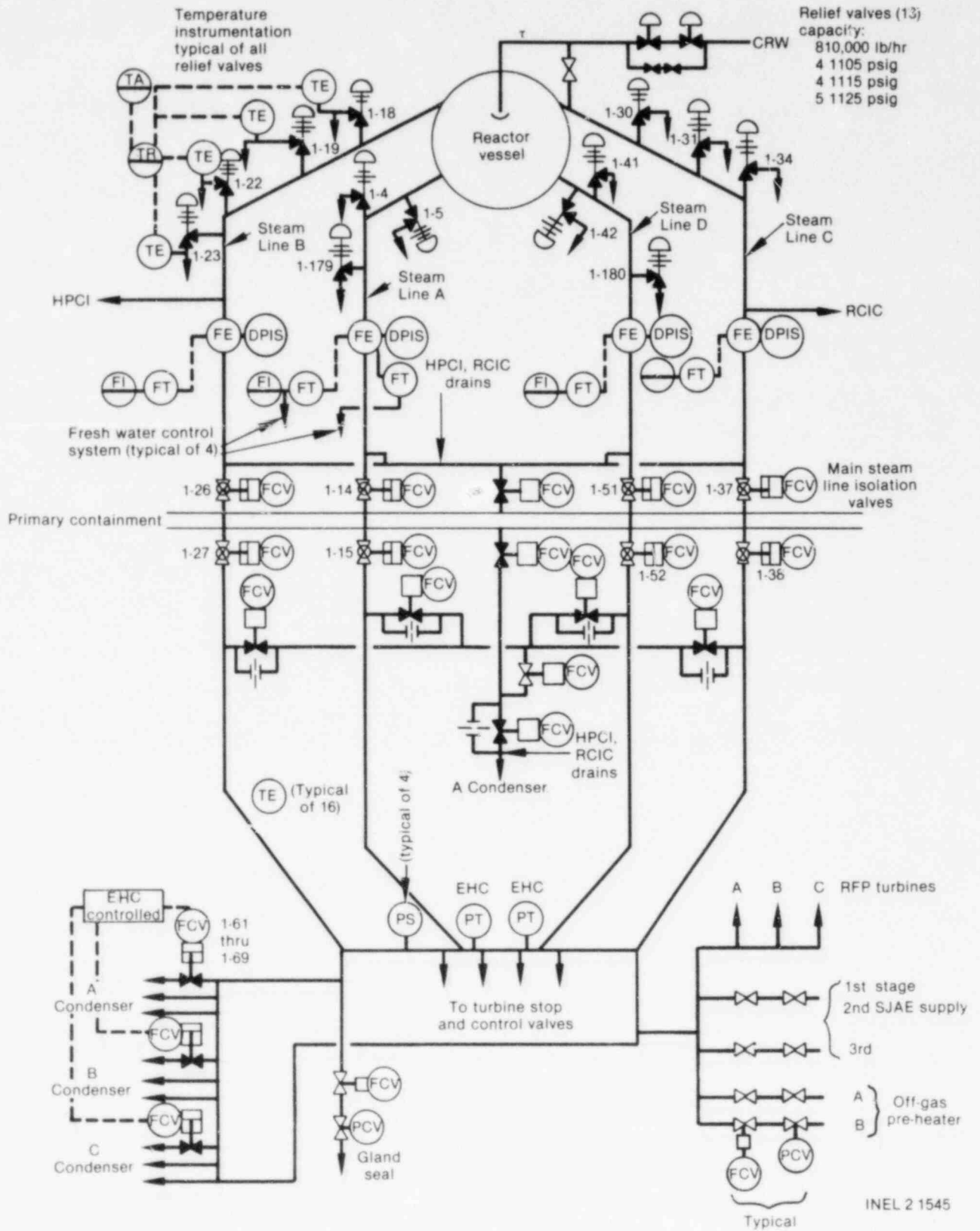


Figure B-27. Main steam isolation system.

below preset limits. The operator can also control each MSIV position by handswitches located in the main control room. Figure B-28 provides a logic diagram for closure of one MSIV.

The electro-hydraulic control system also provides signals to close the turbine bypass and turbine stop valves to provide further isolation of the main steam system.

Testing. Two tests are performed on the MSIVs during normal operation:

1. With the reactor power less than 75%, each MSIV is tripped individually to verify closure time.
2. At least twice per week, the MSIVs are exercised one at a time by partial closure (less than 10% closed) and subsequent reopening.

Neither of these tests contribute to MSIV unavailability since the valves are not aligned from their engineered safeguard position.

Maintenance. Maintenance of the MSIVs is not permitted during normal operations due to high radiation fields and the inherent hazards associated with maintenance of high energy systems.

Technical Specification Limitations. In the event any MSIV becomes inoperable, reactor power operation may be continued provided the inoperable MSIV is in the closed position.

2.13.3 System Operation

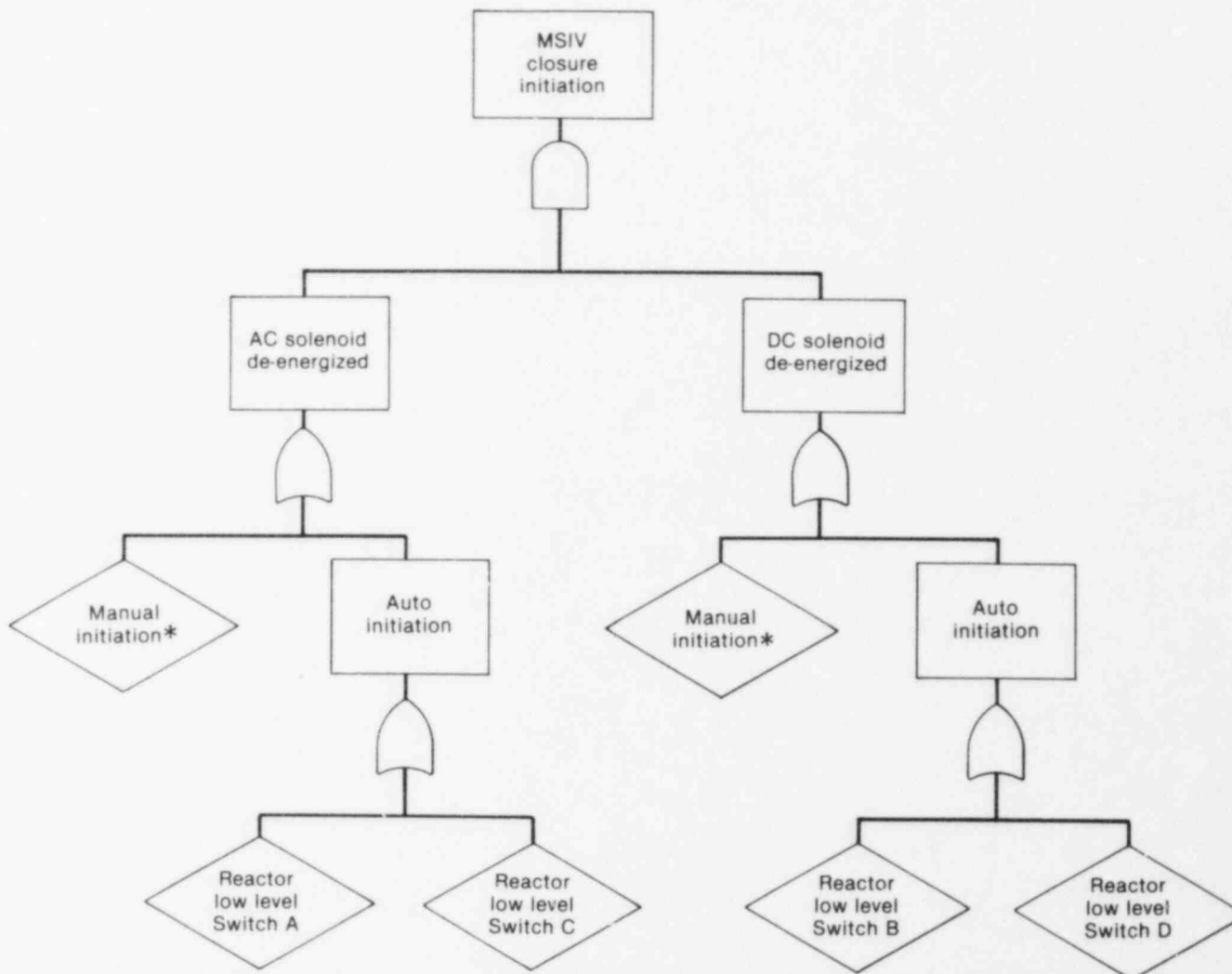
Automatic and manual operation of the MSIVs was discussed in the previous section, "Instrumentation and Control." For transients where PCS is unavailable (e.g., loss of main feedwater), EOI-2 specifies that one set of the automatic actions that should occur is: RCIC and HPCI will be initiated, reactor recirculation pumps will trip, and MSIVs will close when reactor vessel water level drops to a predetermined setpoint. Step III of EOI-2, Immediate Operator Action, requires the operator to verify the automatic actions have occurred and, if not, place controls on manual and take corrective actions.

2.13.4 Fault Tree

Figure B-29 is the MSIV closure fault tree for main steam Line A. The model would be similar for each of the four main steam lines.

As shown by Figure B-29, main steam isolation can be accomplished by closure of either the inboard or outboard MSIV, or by closure of the turbine bypass valves and stop valves. These latter two categories of valves require an input from the electro-hydraulic control system to close. It was considered beyond the scope of this analysis to analyze this balance-of-plant system. Therefore, no credit is taken for this means of providing the main steam isolation function from this portion of the model.

Only the faults associated with the air-operated valves failing to operate on demand ($3 \times 10^{-4}/D$) and initiation circuitry are considered.



*Same hand switch controls both solenoids.

INEL 2 1550

Figure B-28. Logic diagram for closure of a MSIV.

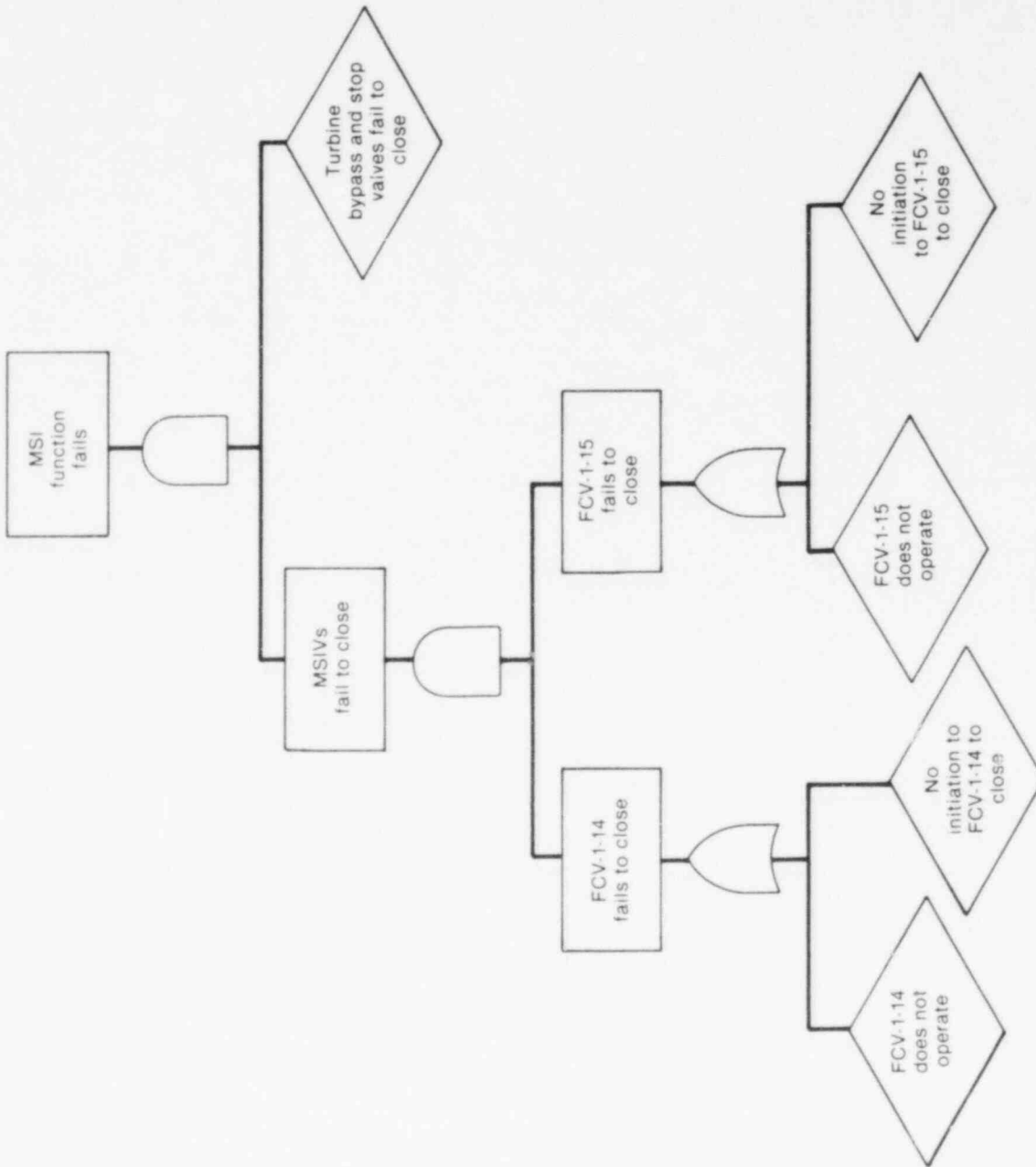


Figure B-29. MSI fault tree.

INEL 2 1551

As shown previously in Figure B-28, failure of the valve to auto-initiate would require the simultaneous failure of two level switches. Even considering the possibility of miscalibration of these switches, the operator is instructed by emergency operating procedures to manually initiate MSIV closure if auto-initiation fails. As is discussed in Section 4, a human error model for miscalibration of four level switches yielded a human error probability of 2.4×10^{-6} . Failure of the operator to follow the EOI procedures is similar to the human error model for failure to manually depressurize the reactor (9×10^{-3}), which is also presented in Section 4. Therefore, failure to initiate MSIV closure from either automatic or manual actions is:

$$(2.4 \times 10^{-6})(9 \times 10^{-3}) = 2.2 \times 10^{-8}.$$

Thus, failure of at least one MSIV to close in a given steam line is:

$$\begin{aligned} (3 \times 10^{-4}/D)(3 \times 10^{-4}/D) &= 9 \times 10^{-8} \text{ plus } 2.2 \times 10^{-8} \text{ for failure} \\ &\text{to initiate closure} \\ &= 1.1 \times 10^{-7}. \end{aligned}$$

Since there are four similar main steam lines, failure to achieve successful main steam isolation (Event N on the transient systemic event trees--Appendix A) is 4.4×10^{-7} .

3. SUPPORT SYSTEM FAULT ANALYSES

3.1 Electrical Power System

3.1.1 Purpose

The Browns Ferry Nuclear Station EPS is a complex arrangement of switching equipment, transformers, generators, batteries, and other devices needed to provide power to the various pumps, valves, and control circuits. In general, the system consists of two parts; an AC and a DC distribution system. The AC system consists of two parts, those buses powered only by offsite power and those buses powered by either offsite power or emergency onsite diesel generators.

3.1.2 System Configuration

Overall Configuration

AC Power Distribution System--The AC system consists of a distribution system powered by offsite power and a distribution system powered by either offsite power or emergency onsite diesel generators. Figure B-30 is a simplified drawing of the AC power system that shows those buses directly associated with Unit 1 that receive power from offsite power or the diesel generators. Breakers shown shaded are normally closed.

Each 4160 V shutdown board has two offsite power supplies. Automatic transfer from one to the other offsite supply occurs if one is lost. If both offsite sources are lost, the diesel generator for that bus automatically receives a start signal. When the diesel is running, the output breaker will automatically close to supply power to the shutdown board if there is no offsite supply. Supplying a shutdown board from its corresponding Unit 3 shutdown board (or vice versa) is done manually.

The 480 V shutdown boards each receive power from a principal and alternate transformer powered by the 4160 V shutdown boards. Transfer from one power source to the other is done manually.

Each 480 V RMOV board has two power sources. RMOV Boards 1D and 1E have AC motor generators providing power from the 480 V shutdown boards. RMOV Boards 1D and 1E automatically transfer from one power supply to the other on undervoltage. Transfers for RMOV Boards 1A, 1B, and 1C are done manually.

DC Power Distribution System--There are four DC systems at Browns Ferry Nuclear Station. The 48 and 24 V DC systems do not directly supply any of the loads necessary for accident or transient mitigation. Figure B-30 also provides a simplified drawing of the 250 V DC system as it applies to accident and transient mitigation loads. Breakers shown shaded are normally closed. Each battery board is supplied by a battery and a principal and alternate battery charger. The alternate charger for each board is shared by all three battery boards. Each battery charger has two sources of AC power. Each DC RMOV board receives power from one of two of the battery boards. All transfers of power supplies in this system are done manually. The 125 V DC system consists of the batteries and chargers

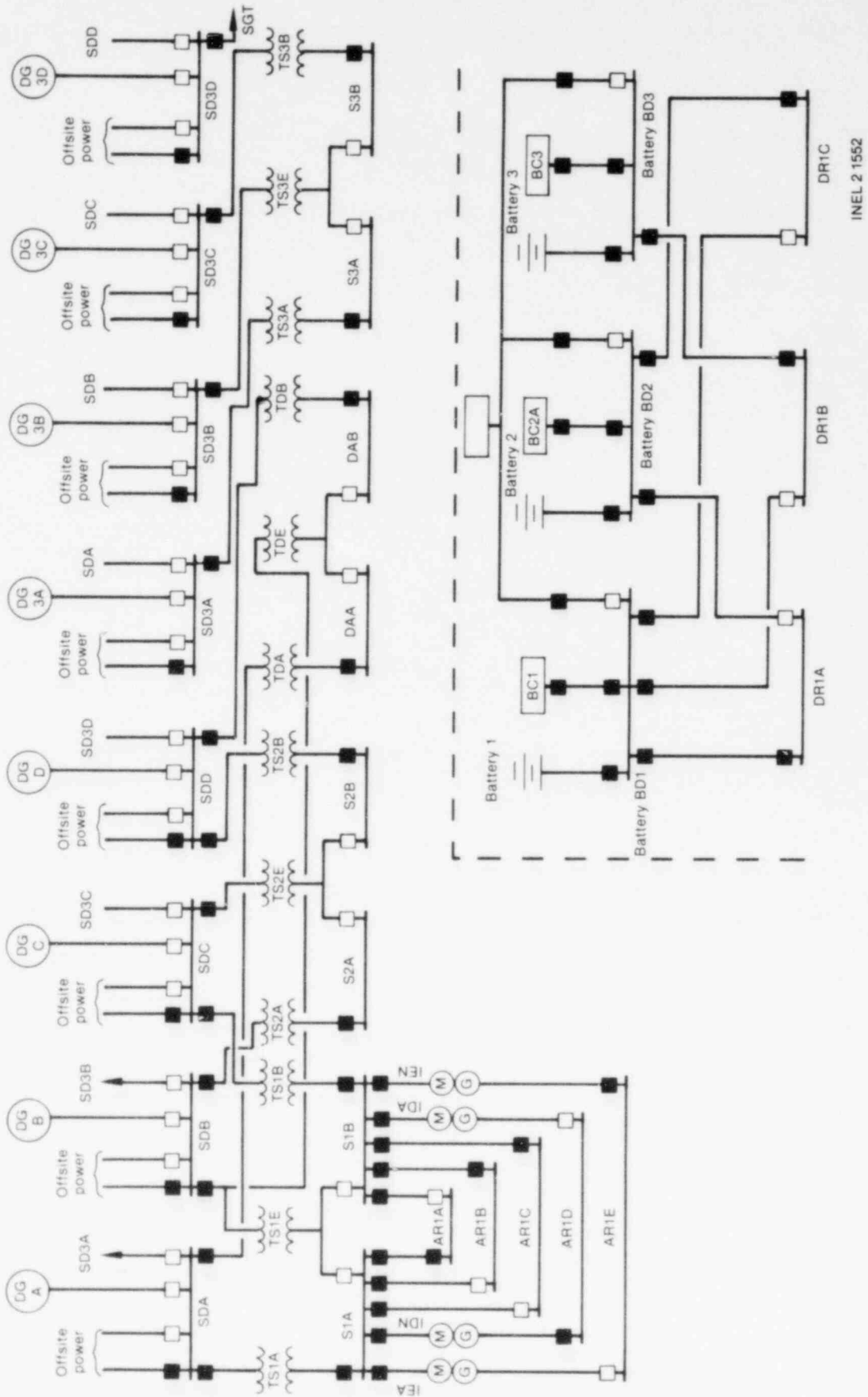


Figure B-30. EPS diagram showing AC and DC systems.

associated with starting and controlling the diesel generators. Each diesel has its own 125 V DC system that is independent of the other diesels' 125 V DC system.

System Interfaces. The EECW system is the only support system interface with the EPS considered in the analysis. It provides cooling to the diesel generator lube oil and engine coolers. There are several diesel support systems, such as lube oil, control power, fuel oil, etc., that were not considered separately, since each diesel's support systems are independent of the support systems of the other diesels. Table B-58 is the FMEA for EPSs.

Instrumentation and Control. The breakers in the EPS have many different instrumentation and control schemes. In general, these include fault protection, undervoltage transfers, and interlocks with other breakers. Table B-59 lists each breaker shown on the EPS drawing (Figure 30) and describes the interlocks and controls associated with each breaker.

The diesel generator control circuit provides start signals to the diesel generator on loss of voltage to its shutdown board, loss of voltage to the bus providing offsite power to its shutdown board, high drywell pressure, or low reactor water level. The accident signals are provided by the core spray logic. The undervoltage sensors are powered by the 250 V DC control power bus for the diesel's shutdown board.

Testing. Technical specifications require periodic testing of components in the EPSs. Table B-60 lists those tests that render components inoperable. It also lists the frequency, duration, and calculated unavailabilities for these tests.

The only contribution to unavailability for all of the diesel generator tests is the requirement that the diesels be manually started and warmed up prior to any auto-start or load tests. This action limits wear on the diesels from repetitive fast starts from a cold condition. During manual startup, the operator opens the breaker to the diesel output breaker logic prevents cabinet, disabling the auto-initiation circuitry, which prevents automatic starting and loading of the diesel for the 15 min. After warmup, the diesel is either loaded for the monthly load test or shut down prior to testing the auto-start logic. At this point the operator recloses the breaker on the logic cabinet and auto-initiation is again available.

The unavailability calculation for the diesel tests does not take credit for operator action to reclose the logic breaker and allow the diesel to function normally should the need arise during the warmup period. Since the operator is in communication with the control room during this procedure and the other diesel generators nearby would start if normal power was lost, it is likely that the operator would be able to return the diesel being warmed up to standby readiness almost immediately. However, the unavailability due to testing does not consider this recovery action.

Each month, each diesel must be manually warmed up, paralleled onto its shutdown board and loaded to at least 75% design rating for 1 hour. Automatic operation is inhibited, as previously discussed, for 15 min during this procedure. Only one diesel may be tested at a time during reactor operation.

TABLE B-58. EPS FMEA OF COMPONENT/SUPPORTING-SYSTEM INTERACTIONS

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
Standby AC Power--Diesel Generator A					
4160 V SD-BD-A	Offsite power	Shutdown Bus 1 or 2	Offsite power unavailable	Board is temporarily dead until diesels come on line	--
	Diesel Generator A	--	--	--	Diesel Generator A is the primary source of onsite power for 4 kV SD-BD-A
	Diesel Generator 3A	--	--	--	Diesel Generator 3A is second source of onsite power
4160 V SD-BD-B	250 V DC power	Control Bus A	No power to bus	Switchgear on board is inoperative	--
	Offsite power	Shutdown Bus 1 or 2	Offsite power unavailable	Board is temporarily dead until diesels come on line	--
	Diesel Generator B	--	--	--	Primary source of onsite power
4160 V SD-BD-C	Diesel Generator 3B	--	--	--	Secondary source of onsite power
	250 V DC power	Control Bus B	No power to bus	Switchgear on bus is inoperative	--
	Offsite power	Shutdown Bus 2 or 1	Offsite power unavailable	Board is temporarily dead until diesels come on line	--
4160 V SD-BD-D	Diesel Generator C	--	--	--	Primary source of onsite power
	Diesel Generator 3C	--	--	--	Secondary source of onsite power
	250 V DC power	Control Bus C	No power to bus	Switchgear associated with the 4 kV shutdown board	--
4160 V SD-BD-D	Offsite power	Shutdown Bus 2 or 1	Offsite power unavailable	Board is temporarily dead until diesels come on line	--
	Diesel Generator D	--	--	--	Primary source of onsite power
	Diesel Generator 3D	--	--	--	Secondary source of onsite power
480 V SD-BD-1A	250 V DC power	Control Bus D	No power to board	Switchgear on bus is inoperable	--
	250 V DC power	Control Bus A	Bus dead	Switchgear on 480 V board is inoperable	--
480 V SD-BD-1B	250 V DC power	Control Bus B	Bus dead	Switchgear on 480 V board in inoperable	--

B-269

TABLE B-58. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
Standby AC Power--Diesel Generator A (continued)					
125 V DC battery	480 V AC Board A	Battery Charger A	No power to board; circuit open	Loss of diesel Generator A control power only if both 480 V AC support systems and the battery are unavailable	--
	480 V AC Board B	Battery Charger B	No power to board; circuit open	--	--
Start air Compressor A	480 V AC	Diesel auxiliary Board A	No power to board; circuit open	Compressor A cannot be used to start diesel Generator A	Does not fail; the diesel Generator B compressor or air flasks may be used to start diesel generator
Engine cooler	EECW	--	Insufficient EECW	Diesel Generator A not cooled and will not continue to run	--
Auxiliary oil pump	480 V AC	Diesel auxiliary Board A	No power; circuit open	Increased probability that diesel Generator A will not start as required	--
Lube oil heater	480 V AC	Diesel auxiliary Board A	No power to board; circuit open	Increased probability that diesel Generator A will not start as required	--
Start air Compressor B	480 V AC	Diesel auxiliary Board B	No power to board; circuit open	If both AC and DC sources to Compressor B fail, the compressor cannot start the diesel	If both A and B compressors fail and the air flasks are empty, the diesel generator will not start
	125 V DC	--	No power; circuit open	--	--
Standby AC Power--Diesel Generator B					
125 V DC battery	480 V AC Board A	Battery Charger A	No power to board; circuit open	Loss of diesel Generator B control power only if both 480 V AC support systems and the battery are unavailable	--
	480 V AC Board B	Battery Charger B	No power to board; circuit open	--	--
Start air Compressor A	480 V AC	Diesel auxiliary Board A	No power to board; circuit open	Compressor A cannot be used to start diesel Generator B	Does not fail; the diesel Generator B compressor or air flasks may be used to start diesel generator

TABLE B-58. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
Standby AC Power--Diesel Generator B (continued)					
Engine cooler	EECW	--	Insufficient EECW	Diesel Generator B not cooled and will not continue to run	--
Auxiliary oil pump	480 V AC	Diesel auxiliary Board A	No power; circuit open	Increased probability that diesel Generator B will not start as required	--
Lube oil heater	480 V AC	Diesel auxiliary Board A	No power to board; circuit open	Increased probability that diesel Generator B will not start as required	--
Start air Compressor B	480 V AC	Diesel auxiliary Board B	No power to board; circuit open	If both AC and DC sources to Compressor B fail, the compressor cannot start the diesel	If both A and B compressors fail and the air flasks are empty, the diesel generator will not start
	125 V DC	--	No power; circuit open		
Standby Power--Diesel Generator C					
125 V DC battery	480 V AC Board A	Battery Charger A	No power to board; circuit open	Loss of diesel Generator C control power only if both 480 V AC support systems and the battery are unavailable	--
	480 V AC Board B	Battery Charger B	No power to board; circuit open	--	--
Start air Compressor A	480 V AC	Diesel auxiliary Board A	No power to board; circuit open	Compressor A cannot be used to start diesel Generator C	Does not fail; the diesel Generator B compressor or air flasks may be used to start diesel generator
Engine cooler	EECW	--	Insufficient EECW	Diesel Generator C not cooled and will not continue to run	--
Auxiliary oil pump	480 V AC	Diesel auxiliary Board B	No power; circuit open	Increased probability that diesel Generator C will not start as required	--
Lube oil heater	480 V AC	Diesel auxiliary Board B	No power to board; circuit open	Increased probability that diesel Generator B will not start as required	--

TABLE B-58. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
Standby AC Power--Diesel Generator C (continued)					
Start air Compressor B	480 V AC	Diesel auxiliary Board B	No power to board; circuit open	If both AC and DC sources to Compressor B fail, the compressor cannot start the diesel	If both A and B compressors fail and the air flasks are empty, the diesel generator will not start
	125 V DC	--	No power; circuit open	--	--
Standby AC Power--Diesel Generator D					
125 V DC battery	480 V AC Board A	Battery Charger A	No power to board; circuit open	Loss of diesel Generator D control power only if both 480 V AC support systems and the battery are unavailable	--
	480 V AC Board B	Battery Charger B	No power to board; circuit open	--	--
Start air Compressor A	480 V AC	Diesel auxiliary Board A	No power to board; circuit open	Compressor A cannot be used to start diesel Generator D	Does not fail; the diesel Generator B compressor or air flasks may be used to start diesel generator
Engine cooler	EECW	--	Insufficient EECW	Diesel Generator D not cooled and will not continue to run	--
Auxiliary oil pump	480 V AC	Diesel auxiliary Board B	No power; circuit open	Increased probability that diesel Generator D will not start as required	--
Lube oil heater	480 V AC	Diesel auxiliary Board B	No power to board; circuit open	Increased probability that diesel Generator A will not start as required	--
Start air Compressor B	480 V AC	Diesel auxiliary Board B	No power to board; circuit open	If both AC and DC sources to Compressor B fail, the compressor cannot start the diesel	If both A and B compressors fail and the air flasks are empty, the diesel generator will not start
	125 V DC	--	No power; circuit open	--	--

TABLE B-58. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
Standby AC Power--Diesel Generator 3A					
125 V DC battery	480 V AC Board 3EA	Battery Charger A	No power to board; circuit open	Loss of diesel Generator 3A control power only if both 480 V AC support systems and the battery are unavailable	--
	480 V AC Board 3FB	Battery Charger B	No power to board; circuit open	--	--
Start air Compressor A	480 V AC	Diesel auxiliary Board 3EA	No power to board; circuit open	Compressor A cannot be used to start diesel Generator 3A	Does not fail; the diesel Generator B compressor or air flasks may be used to start diesel generator
Engine cooler	EECW	--	Insufficient EECW	Diesel Generator 3A not cooled and will not continue to run	--
Auxiliary oil pump	480 V AC	Diesel auxiliary Board 3EA	No power; circuit open	Increased probability that diesel Generator 3A will not start as required	--
Lube oil heater	480 V AC	Diesel auxiliary Board 3EA	No power to board; circuit open	Increased probability that diesel Generator 3A will not start as required	--
Start air Compressor B	480 V AC	Diesel auxiliary Board 3EB	No power to board; circuit open	If both AC and DC sources to Compressor B fail, the compressor cannot start the diesel	If both A and B compressors fail and the air flasks are empty, the diesel generator will not start
	125 V DC	--	No power; circuit open	--	--
Standby AC Power--Diesel Generator 3B					
125 V DC battery	480 V AC Board 3EA	Battery Charger A	No power to board; circuit open	Loss of diesel Generator 3B control power only if both 480 V AC support systems and the battery are unavailable	--
	480 V AC Board 3EB	Battery Charger B	No power to board; circuit open	--	--

B-273

TABLE B-58. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
Standby AC Power--Diesel Generator 3B (continued)					
Start air Compressor A	480 V AC	Diesel auxiliary Board 3EA	No power to board; circuit open	Compressor A cannot be used to start diesel Generator 3B	Does not fail; the diesel Generator B compressor or air flasks may be used to start diesel generator
Engine cooler	EECW	--	Insufficient EECW	Diesel Generator 3B not cooled and will not continue to run	--
Auxiliary oil pump	480 V AC	Diesel auxiliary Board 3EA	No power; circuit open	Increased probability that diesel Generator 3B will not start as required	--
Lube oil heater	480 V AC	Diesel auxiliary Board 3EA	No power to board; circuit open	Increased probability that diesel Generator 3B will not start as required	--
Start air Compressor B	480 V AC	Diesel auxiliary Board 3EB	No power to board; circuit open	If both AC and DC sources to Compressor B fail, the compressor cannot start the diesel	If both A and B compressors fail and the air flasks are empty, the diesel generator will not start
	125 V DC	--	No power; circuit open	--	--
Standby AC Power--Diesel Generator 3C					
125 V DC battery	480 V AC Board 3EA	Battery Charger A	No power to board; circuit open	Loss of diesel Generator 3C control power only if both 480 V AC support systems and the battery are unavailable	--
	480 V AC Board 3BA	Battery Charger B	No power to board; circuit open	--	--
Start air Compressor A	480 V AC	Diesel auxiliary Board 3EA	No power to board; circuit open	Compressor A cannot be used to start diesel Generator 3C	Does not fail; the diesel Generator B compressor or air flasks may be used to start diesel generator
Engine cooler	EECW	--	Insufficient EECW	Diesel Generator 3C not cooled and will not continue to run	--
Auxiliary oil pump	480 V AC	Diesel auxiliary Board 3EB	No power; circuit open	Increased probability that diesel Generator 3C will not start as required	--

TABLE B-58. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
Standby AC Power--Diesel Generator 3C (continued)					
Lube oil heater	480 V AC	Diesel auxiliary Board 3EB	No power to board; circuit open	Increased probability that diesel Generator 3C will not start as required	--
Start air Compressor B	480 V AC	Diesel auxiliary Board 3EB	No power to board; circuit open	If both AC and DC sources to Compressor B fail, the compressor cannot start the diesel	If both A and B compressors fail and the air flasks are empty, the diesel generator will not start
	125 V DC	--	No power; circuit open	--	--
Standby AC Power--Diesel Generator 3D					
125 V DC battery	480 V AC Board 3EA	Battery Charger A	No power to board; circuit open	Loss of diesel Generator 3C control power only if both 480 V AC support systems and the battery are unavailable	--
	480 V AC Board 3EB	Battery Charger B	No power to board; circuit open	--	--
Start air Compressor A	480 V AC	Diesel auxiliary Board 3EA	No power to board; circuit open	Compressor A cannot be used to start diesel Generator 3C	Does not fail; the diesel Generator B compressor or air flasks may be used to start diesel generator
Engine cooler	EECW	--	Insufficient EECW	Diesel Generator 3D not cooled and will not continue to run	--
Auxiliary oil pump	480 V AC	Diesel auxiliary Board 3EB	No power; circuit open	Increased probability that diesel Generator 3D will not start as required	--
Lube oil heater	480 V AC	Diesel auxiliary Board 3EB	No power to board; circuit open	Increased probability that diesel Generator 3D will not start as required	--
Start air Compressor B	480 V AC	Diesel auxiliary Board 3EB	No power to board; circuit open	If both AC and DC sources to Compressor B fail, the compressor cannot start the diesel	If both A and B compressors fail and the air flasks are empty, the diesel generator will not start
	125 V DC	--	No power; circuit open	--	--

TABLE B-58. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
250 V DC System					
Plant Battery 1	480 V SD-BD-1A	Battery Charger 1	--	Battery Chargers 1 and 2B can charge Battery 1; should both of these fail, the loads on battery Board 1 will be powered by the battery	--
	480 V SD-BD-2B	Battery Charger 2B	--		
Plant Battery 2	480 V SD-BD-2A	Battery Charger 2A	--	Battery Chargers 2A and 2B can charge Battery 1; should both of these fail, the loads on battery Board 2 will be powered by the battery	--
	480 V SD-BD-2B	Battery Charger 2B	--		
Plant Battery 3	480 V SD-BD-3A	Battery Charger 3	--	Battery Chargers 3A and 2B can charge Battery 1; should both of these fail, the loads on battery Board 3 will be powered by the battery	--
	480 V SD-BD-2B	Battery Charger 2B	--		
Plant Battery 4	480 V SD-BD-3B	Battery Charger 3B	--	Battery Chargers 3B and 2B can charge Battery 1; should both of these fail, the loads on battery Board 4 will be powered by the battery	--
	480 V SD-BD-2B	Battery Charger 2B	--		
Control Battery A	480 V RMOV-1A	Battery Charger SB-A	480 V BD unavailable	Battery will not recharge; the battery is rated for 3 hours	Battery Board 2 is alternate source of power
Control Battery B	480 V RMOV-2A	Battery Charger SB-B	Same as above	Same as above	Battery Board 2 is alternate source of power
Control Battery C	480 V RMOV-1B	Battery Charger SB-C	Same as above	Same as above	Battery Board 1 is alternate source of power
Control Battery D	480 V RMOV-2B	Battery Charger SB-D	Same as above	Same as above	Battery Board 3 is alternate source of power
Room exhaust Fan 1A	480 V RMOV-1A	--	No power to board	The effects and the time needed to affect the effects of fan failure, or combinations thereof, is not known	--
Room exhaust Fan 1B	480 V RMOV-1B	--	Same as above	Same as above	--
Room supply Fan 1A	480 V RMOV-1A	--	Same as above	Same as above	--
Room supply Fan 1B	480 V RMOV-1B	--	Same as above	Same as above	--

TABLE B-59. EPS BREAKER INTERLOCK AND CONTROL DESCRIPTION

Breaker Number	Description	Control Features
1614	Offsite power to Shutdown Board A	Normally closed breaker; if open, will close if other off-site power source lost and power is available to 1614 (1716 must be open)
1716	Offsite power to Shutdown Board A	Normally open breaker; shuts if normal offsite power lost and power is available to 1716 (1614 must be open)
1818	Diesel Generator A to Shutdown Board A	Closes on loss of voltage on Shutdown Board A if diesel is running and all other supply breakers to Shutdown Board A are open (1614, 1716, and 1824)
1824	Shutdown Boards 3EA to A	Manually operated; must have all other supply breakers to Shutdown Board A open
1616	Offsite power to Shutdown Board B	Similar to 1614
1714	Offsite power to Shutdown Board B	Similar to 1716
1822	Diesel Generator B to Shutdown Board B	Similar to 1818
1828	Shutdown Boards 3EB to B	Similar to 1824
1624	Offsite power to Shutdown Board C	Similar to 1614
1718	Offsite power to Shutdown Board C	Similar to 1716
1812	Diesel Generator C to Shutdown Board C	Similar to 1818
1814	Shutdown Boards 3EC to C	Similar to 1824
1618	Offsite power to Shutdown Board D	Similar to 1614
1724	Offsite power to Shutdown Board D	Similar to 1716

TABLE B-59. (continued)

Breaker Number	Description	Control Features
1816	Diesel Generator D to Shutdown Board D	Similar to 1818
1826	Shutdown Boards 3ED to D	Similar to 1824
1334	Offsite power to Shutdown Board 3EA	Similar to 1614
1726	Offsite power to Shutdown Board 3EA	Similar to 1716
1844	Diesel Generator 3A to Shutdown Board 3EA	Similar to 1818
1838	Shutdown Boards 3EA to A	Similar to 1824
1336	Offsite power to Shutdown Board 3EB	Similar to 1614
1728	Offsite power to Shutdown Board 3EB	Similar to 1716
1848	Diesel Generator 3B to Shutdown Board 3EB	Similar to 1818
1842	Shutdown Boards 3B to 3EC	Similar to 1824
1338	Offsite power to Shutdown Board 3EC	Similar to 1614
1626	Offsite power to Shutdown Board 3EC	Similar to 1716
1834	Diesel Generator 3C to Shutdown Board 3EC	Similar to 1818
1832	Shutdown Boards 3C to 3EC	Similar to 1824
1342	Offsite power to Shutdown Board 3ED	Similar to 1614
1628	Offsite power to Shutdown Board 3ED	Similar to 1716
1846	Diesel Generator 3D to Shutdown Board 3ED	Similar to 1818
1836	Shutdown Boards 3ED to D	Similar to 1824

TABLE B-59. (continued)

Breaker Number	Description	Control Features
001A	Shutdown Board A to Transformer TS1A	Normally closed breaker
002A	Transformer TS1A to Shutdown Board S1A	Normally closed; interlocked with 003A so that both cannot be closed at same time
003A	Transformer TS1E to Shutdown Board S1A	Normally open; interlocked with 002A
001B	Shutdown Board B to Transformer TS1E	Similar to 001A
001C	Shutdown Board C to Transformer TS1B	Similar to 001A
002B	Transformer TS1B to Shutdown Board S1B	Similar to 002A
003B	Transformer TS1E to Shutdown Board S1B	Similar to 003A
061B	Shutdown Board 2 to Transformer TS2A	Similar to 001A
062A	Transformer TS2A to Shutdown Board S2A	Similar to 002A
063A	Transformer TS2E to Shutdown Board S2A	Similar to 003A
061D	Shutdown Board D to Transformer TS2B	Similar to 001A
062B	Transformer TS2B to Shutdown Board S2B	Similar to 002A
063B	Transformer TS2E to Shutdown Board S2B	Similar to 003A
061C	Shutdown Board C to Transformer TS2E	Similar to 001B
071A	Shutdown Board 3EA to Transformer TS3A	Similar to 001A
072A	Transformer TS3A to Shutdown Board S3A	Similar to 002A

TABLE B-59. (continued)

Breaker Number	Description	Control Features
073A	Transformer TS3E to Shutdown Board S3A	Similar to 003A
071B	Shutdown Board 3EB to Transformer TS3E	Similar to 001B
071C	Shutdown Board 3EC to Transformer TS3B	Similar to 001A
072B	Transformer TS3B to Shutdown Board S3B	Similar to 002A
073B	Transformer TS3E to Shutdown Board S3B	Similar to 003A
081A	Shutdown Board A to Transformer TDA	Similar to 001A
082A	Transformer TDA to Diesel Auxiliary A	Similar to 002A
083A	Transformer TDE to Diesel Auxiliary A	Similar to 003A
081D	Shutdown Board D to Transformer TDB	Similar to 001A
082D	Transformer TDB to Diesel Auxiliary B	Similar to 002A
083B	Transformer TDE to Diesel Auxiliary B	Similar to 003A
004A	Shutdown Board A to AC RMOV 1A	Normally closed breaker
011A	AC RMOV 1A normal input	Normally closed; interlocked with 012A
004B	Shutdown Board S1B to AC RMOV 1A	Similar to 004A
012A	AC RMOV 1A alternate source	Normally open; interlocked with 011A
005B	Shutdown Board S1B to AC RMOV 1B	Similar to 004A
011B	AC RMOV 1B normal source	Similar to 011A

TABLE B-59. (continued)

Breaker Number	Description	Control Features
005A	Shutdown Board S1A to AC RMOV 1B	Similar to 004A
012B	AC RMOV S1B to alternate source	Similar to 012A
006B	Shutdown Board S1B to AC RMOV 1C	Similar to 004A
011C	AC RMOV 1C normal source	Similar to 011A
006A	Shutdown Board S1A to AC RMOV 1C	Similar to 004A
012C	AC RMOV 1C alternate source	Similar to 012A
007A	Shutdown Board S1A to Motor Generator 1DN	Similar to 004A
011D	Motor Generator 1DN to AC RMOV 1D	Normally closed; if open will auto-close on loss of voltage on RMOV 1D if 012D open Automatic return to normal supply provided 012D opens
007B	Shutdown Board S1B to Motor Generator 1DA	Similar to 004A
012D	Motor Generator 1DA to AC RMOV 1D	Normally open; auto-close on loss of voltage on RMOV 1D and 011D open, auto-opens when normal power (Motor Generator 1DN) available
008B	Shutdown Board S1B to Motor Generator 1EN	Similar to 004A
011E	Motor Generator 1EN to AC RMOV 1E	Similar to 011D
008A	Shutdown Board S1A to Motor Generator 1EA	Similar to 004A
012E	Motor Generator 1EA to AC RMOV 1E	Similar to 012D
041A	Shutdown Board 1A to Battery Charger 1	Normally closed; interlock with 0511

TABLE B-59. (continued)

Breaker Number	Description	Control Features
0511	Offsite power to Battery Charger 1	Normally open; interlock with 041A
042A	Shutdown Board 1A to Battery Charger 2A	Similar to 041A
052A	Offsite power to Battery Charger 2A	Similar to 0511
042B	Shutdown Board 2B to Battery Charger 2B	Similar to 041A
052B	Offsite power to Battery Charger 2B	Similar to 0511
043A	Shutdown Board 3A to Battery Charger 3	Similar to 041A
0531	Offsite power to Battery Charger 3	Similar to 0511
0211	Battery 1 to Battery Board 1	Normally closed; manual breaker
0221	Battery Board 1 normal source	Similar to 0211
0241	Battery Charger 1 to Battery Board 1	Similar to 0211
0231	Battery Board 1 alternate source	Normally open; manual breaker
0251	Battery Charger 2B to Battery Board 1	Similar to 0211
0212	Battery 2 to Battery Board 2	Similar to 0211
0222	Battery Board 2 normal source	Similar to 0211
0242	Battery Charger 2A to Battery Board 2	Similar to 0211
0232	Battery Board 2 alternate source	Similar to 0231
0252	Battery Charger 2B to Battery Board 2	Similar to 0211
0213	Battery 3 to Battery Board 3	Similar to 0211

TABLE B-59. (continued)

Breaker Number	Description	Control Features
0223	Battery Board 3 normal source	Similar to 0211
0243	Battery Charger 3 to Battery Board 3	Similar to 0211
0233	Battery Board 3 alternate source	Similar to 0231
0253	Battery Charger 2B to Battery Board 3	Similar to 0211
0261	Battery Board 1 to DC RMOV 1A	Similar to 0211
0272	Battery Board 2 to DC RMOV 1A	Similar to 0211
031A	DC RMOV 1A normal source	Normally closed; interlock with 032A
032A	DC RMOV 1A alternate source	Normally open; interlock with 031A
0263	Battery Board 3 to DC RMOV 1B	Similar to 0211
0271	Battery Board 1 to DC RMOV 1B	Similar to 0211
031B	DC RMOV 1B normal source	Similar to 031A
032B	DC RMOV 1B alternate source	Similar to 032A
0262	Battery Board 2 to DC RMOV 1C	Similar to 0211
0281	Battery Board 1 to DC RMOV 1C	Similar to 0211
031C	DC RMOV 1C normal source	Similar to 031A
032C	DC RMOV 1C alternate source	Similar to 032A

TABLE B-60. EPS TEST REQUIREMENTS SUMMARY

Component Undergoing Test	Type of Test	Test Procedure Number	Components Aligned Away from Engineered Safeguards Position for Test	Expected Test Frequency	Expected Test Outage Time	Remarks
<u>Diesel Generators</u>						
Coded ADLS11AJ	Manual start and load	SI 4.9.A.1.a	In each of these tests the auto-start logic (output breaker auto-close) is overridden and the diesel is started and warmed up manually (requires 15 min); then the auto-start logic is reset and the test is performed	Once every month	15 min	$\bar{A} = \frac{15 \text{ min}}{43200 \text{ min}}$ was used in trees (ADLS11AJ, etc.) even though the operator is at the diesel and in communication with the control room so that auto-start could be immediately restored if required
•	Auto-start	SI 4.9.A.1.b		Once every operating cycle	15 min	
•	and load					
ADLS13DJ in fault trees	Common accident signal	SI 4.9.A.3.a		Once every 6 months	15 min	
	Undervoltage start	SI 4.9.A.4.a SI 4.9.A.4.b		Once every 6 months	15 min	
				Once every 6 months	15 min	
<u>Station Batteries</u>						
Coded BBY0011J BBY0012J BBY0013J in fault trees	Discharge test	SI 4.9.A.2.c	All loads on the battery board associated with the tested battery are first transferred to the alternate supply, they are transferred back after the test	Once every 2 years	7 days	Outage based on maximum allowable reactor operating time with battery OOC per technical specifications $\bar{A} = \frac{7 \text{ days}}{(365 \text{ day/yr})(2 \text{ yr})}$ $\bar{A} = 0.0096$

B-284

Every 6 months the common accident signal and undervoltage signal start tests are performed. As before, the diesel auto-initiation is bypassed for 15 min. Then the auto-start circuitry is tested by manually actuating various relays to cause the diesel to automatically start. Only one diesel is tested at a time during reactor operation.

Once every operating cycle (18 months) the diesel is tested for automatic starting and load acceptance of normal emergency loads. As before, the diesel is manually warmed up for 15 min during this test. Although this test is usually performed during shutdown periods, there are no procedural requirements prohibiting performance when the reactor is operating. The calculated unavailability assumes the test is done during reactor operation.

The station batteries undergo discharge testing biannually. Only one battery may be made inoperable at a time. All loads on the battery board served by the tested battery are shifted to their alternate supply. A test resistor bank is installed on the battery board and the discharge test is run. Upon completion of the test, the operator returns the normal loads to their preferred supply. Although this test is normally conducted during shutdown periods, there are no procedures prohibiting testing during reactor operation. The technical specifications allow one battery board to be inoperable for no more than 7 days. The calculated unavailability is based on an outage time of 7 days every 2 years.

Maintenance. Table B-61 lists those scheduled maintenance items that cause components of the EPS to be inoperable. It also shows the frequency and duration, for these items.

Once every year, each diesel generator undergoes an inspection that requires 8 to 12 hours to complete. The diesel is made unavailable due to partial disassembly necessary to make the inspection. Only one diesel at a

TABLE B-61. EPS MAINTENANCE ACTS SUMMARY

<u>Maintenance Requirement</u>	<u>Instruction Number</u>	<u>Frequency</u>	<u>Duration</u>	<u>Remarks</u>
Diesel generator inspection	SI 4.9.A.1.d	Every year	8 to 12 hr	One diesel generator at a time
Clean diesel generator coolers		Every year	8 to 12 hr	One diesel generator at a time
Change diesel generator governor oil		Every year	1 to 2 hr	One diesel generator at a time

time may be inoperable if the reactor is operating. This maintenance is usually done during shutdown periods, but the calculated unavailability assumes the reactor is operating during performance of the maintenance.

Once every year, the diesel engine coolers are disassembled and cleaned. This action requires 8 to 12 hours to complete. Only one diesel may be inoperable during reactor operation. The calculated unavailability assumes the maintenance is done during reactor operation as previously discussed.

Once every year, the diesel governor oil is changed. This change requires 1 to 2 hours. Only one diesel is made inoperable at a time. The calculated unavailability assumptions are the same as noted before.

The unavailability number used in the fault trees assumes that these tests are done separately and that the maximum duration is required. Therefore, the outage time is 26 hours out of every 8760 hours, or an unavailability equal to 0.00297.

Technical Specification Limitations. The reactor cannot be started unless all four diesel generators for Units 1 and 2 are operable. Under certain conditions, the reactor may be started if only three diesels are operable. In that case, the reactor must already be in hot shutdown condition; an additional 161-kV line and transformer must be available to supply the shutdown buses; and at least one 500-kV line backfeeding through the Unit 2 main and station transformers must be available to provide auxiliary power to the shutdown buses.

If one diesel is inoperable, reactor operation may continue for 7 days, provided that both offsite 161-kV lines and both common station transformers are available and that all of the core spray, RHR, and remaining three diesels are operable. Otherwise, the reactor must be in cold shutdown condition within 24 hours.

3.1.3 System Operation

Normal operation of the EPS requires no operator action to supply power for the normal or emergency loads. During abnormal conditions, operator action may or may not be required, depending on which bus was affected.

The 4160 V shutdown boards automatically transfer from one offsite source to their alternate on loss of voltage. Loss of voltage on both sources causes an automatic starting and loading of the diesel for that bus.

The 480 V shutdown boards, 480 V RMOV Boards 1A, 1B, and 1C, and 480 V diesel auxiliary Boards A and B do not automatically transfer from their normal to their alternate supplies. The buses are alarmed and the operator transfers these buses to their alternate source. The 480 V RMOV Boards 1E and 1D automatically transfer from their principal to their alternate supplies.

The 250 V DC system has no automatic transfers of buses from one supply to another. However, the battery board and 250 V DC RMOV boards are alarmed and the operator transfers power supplies to these buses.

Each battery board normally operates with power from a battery charger. Each board also has a battery for automatic operation in the event of AC failure or battery charger faults. Each battery board may also be supplied from a spare charger shared by all three boards. All battery charger operations are done manually.

The diesel generators automatically start on an accident signal or upon loss of voltage on the shutdown boards. However, the diesel output breaker will not shut automatically unless the shutdown board has an undervoltage condition, the normal supply breakers are open, and the diesel is running.

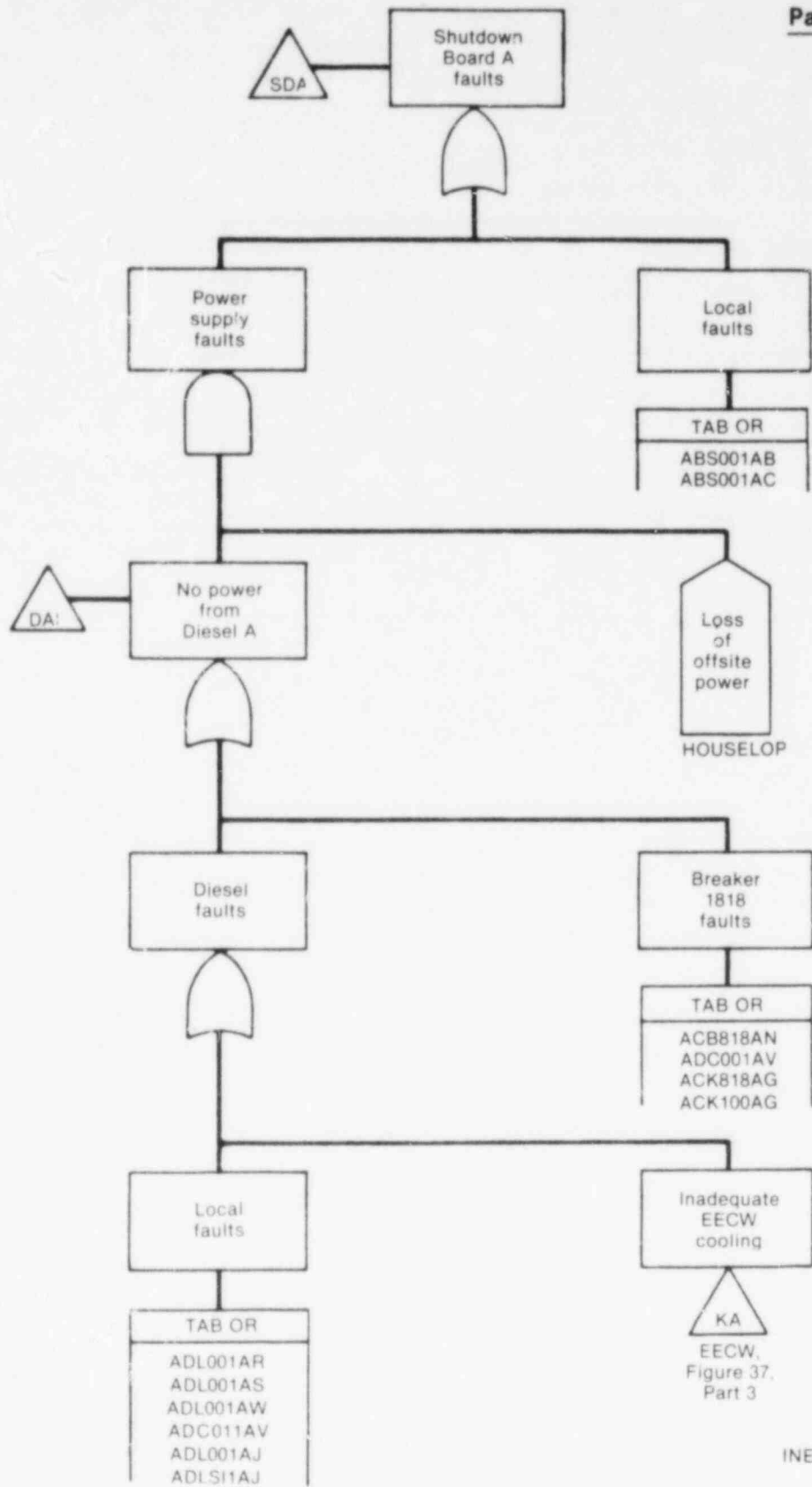
3.1.4 Fault Tree

Figure B-31 shows the fault trees for the EPSs. Each bus that interfaces with a front-line or support system has a fault tree. Parts 1 through 21 of Figure B-31 show the fault trees for various AC buses, while Parts 22 through 31 show fault trees for the DC system components. The 4160 V shutdown boards appear in Parts 1 through 8, while the 480 V shutdown boards appear in Parts 9 through 14. The remaining 480 V AC boards are shown in Parts 15 through 21. Parts 22 through 25 are fault trees for the battery chargers. Battery board fault trees appear in Parts 26 through 28, while DC RMOV board fault trees are in Parts 29 through 31.

In general, each fault tree has two parts. One part lists the local faults for the bus such as shorts or grounds. The remainder of the tree deals with faults in buses on components supplying that bus. For transfers from within the EPSs, the transfer device has an alphanumeric code and a part number. For transfers from other systems, the transfer device has an alphanumeric code and the figure number and figure-part number of the other system.

For AC breakers using 250 V DC control power, a single event appears in the fault tree for control power faults. Each shutdown board uses a 250 V DC control power bus for control of all breakers associated with that board. The control power bus is supplied from one of two 250 V DC buses, both of which are supplied by a battery and one of two battery chargers. Since faults of the control power bus of any shutdown board are orders of magnitude more probable than the loss of all the supplies to the bus and since there are no common mode failures of significance between control power buses for different boards, no fault tree appears for the loss of control power to these breakers. Instead, a single event is used to designate loss of control power. All breakers on a shutdown board share this event.

Each diesel has a separate and independent control circuit from the other diesels. However, in the fault tree summary sheet, no accident signals appear under the initiation faults. As mentioned before in the previous section, "System Operation," the output breaker for the diesel will not close unless its shutdown board has an undervoltage condition. Since this same signal also starts the diesel, any other start signals, such as accident signals, are repetitive. When reduced in a Boolean manner, these other signals, provide no contribution to the diesel unavailability



INEL 2 1553

Figure B-31. EPS fault tree.

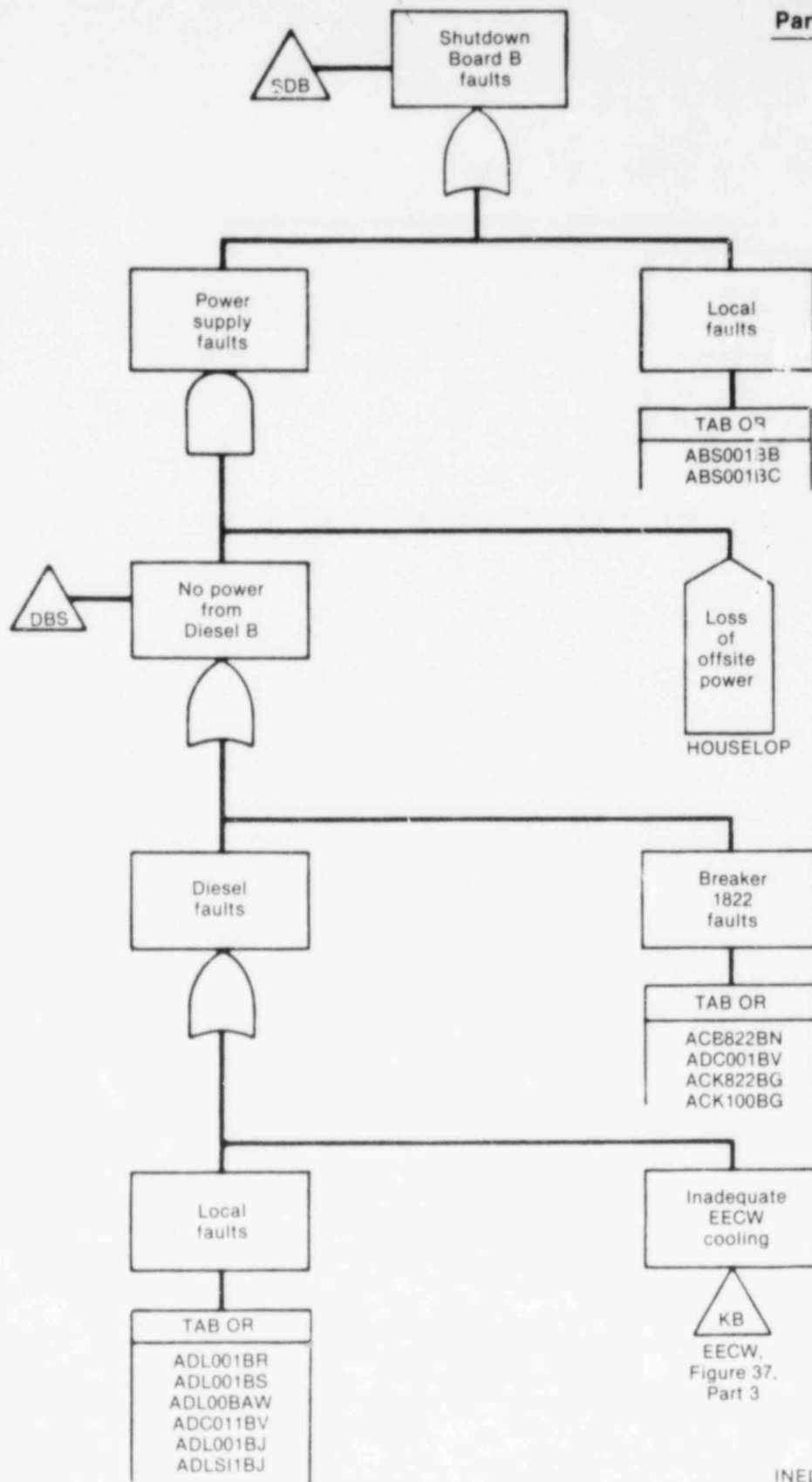
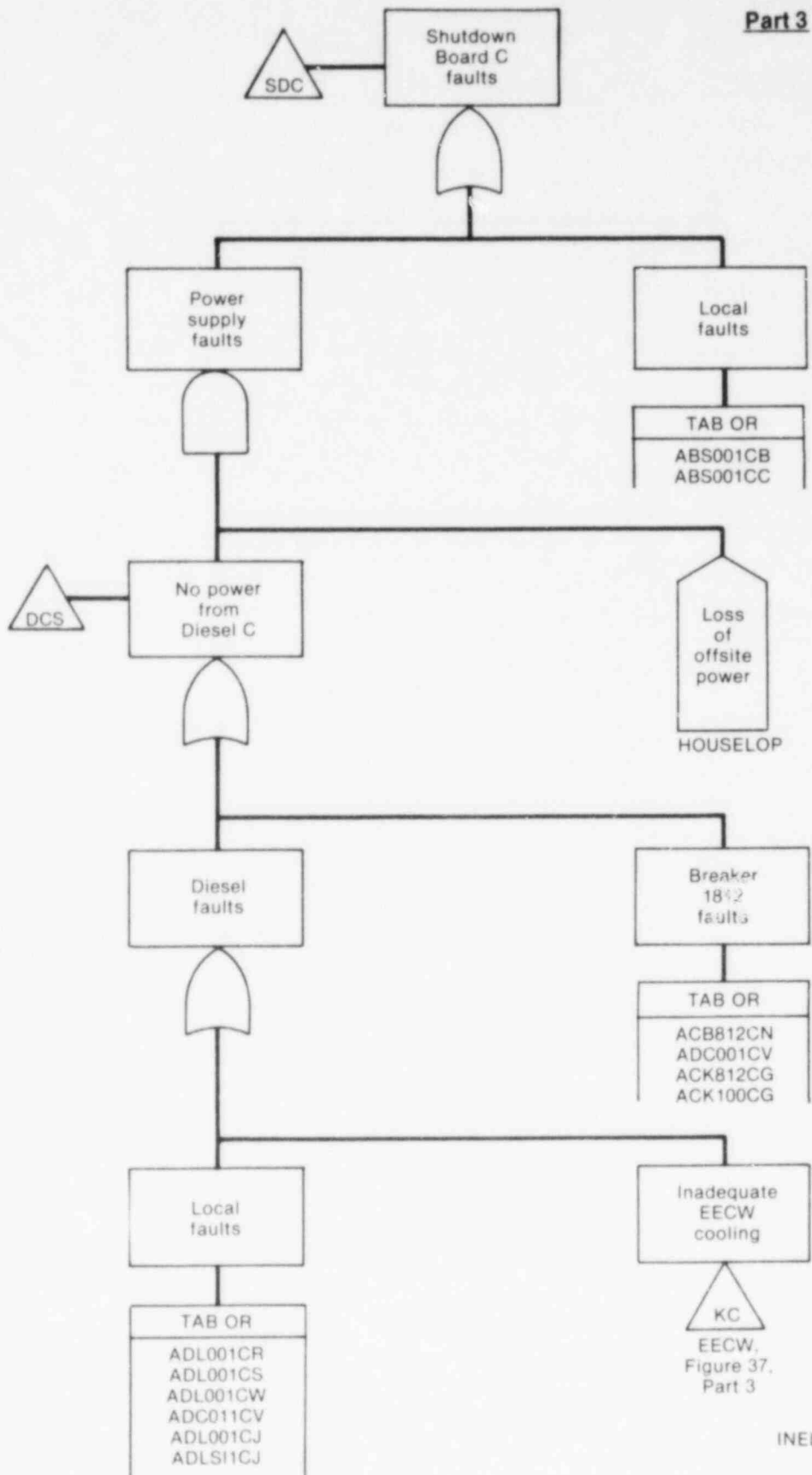
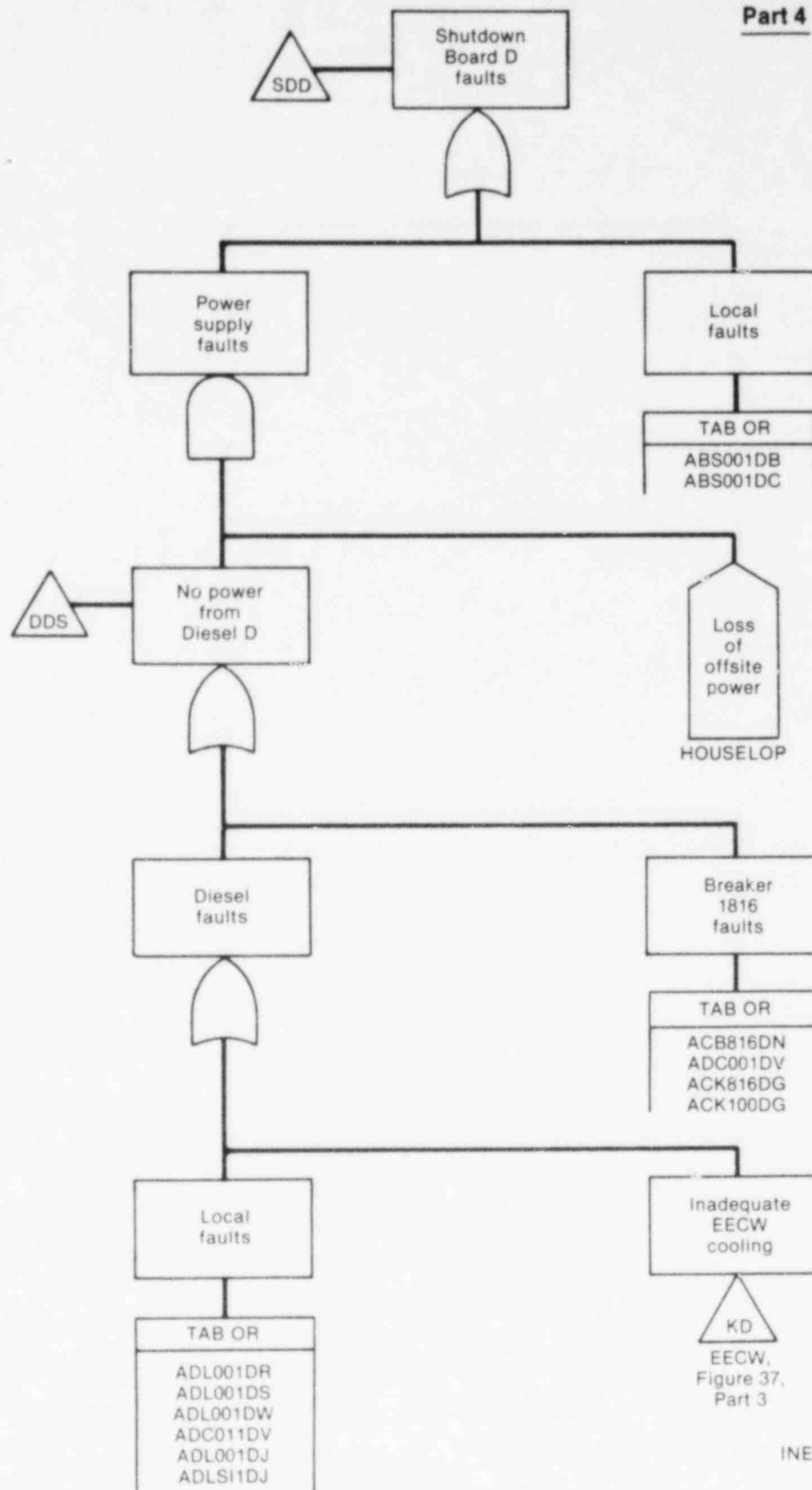


Figure B-31. (continued)



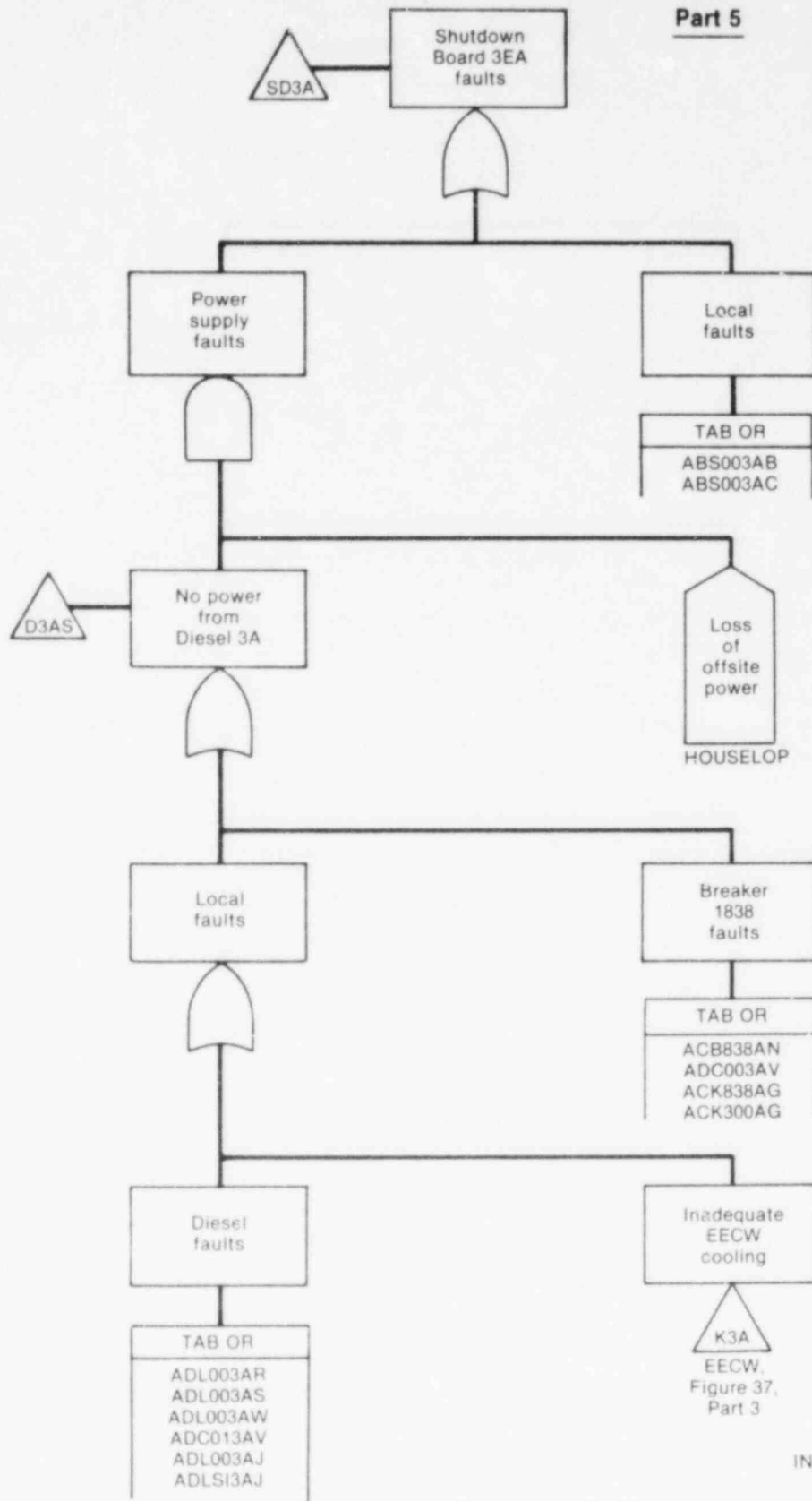
INEL 2 1555

Figure B-31. (continued)



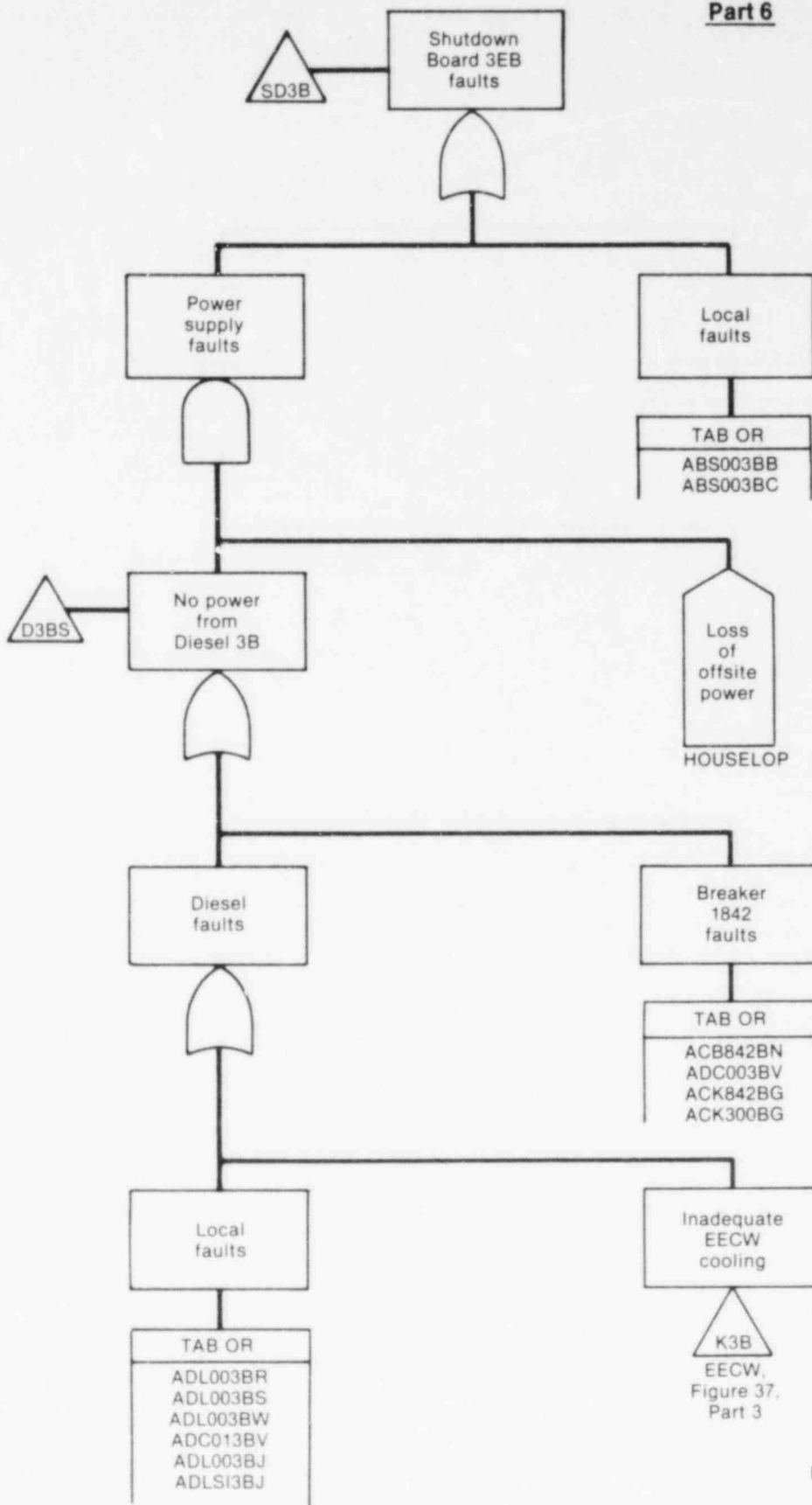
INEL 2 1556

Figure B-31. (continued)



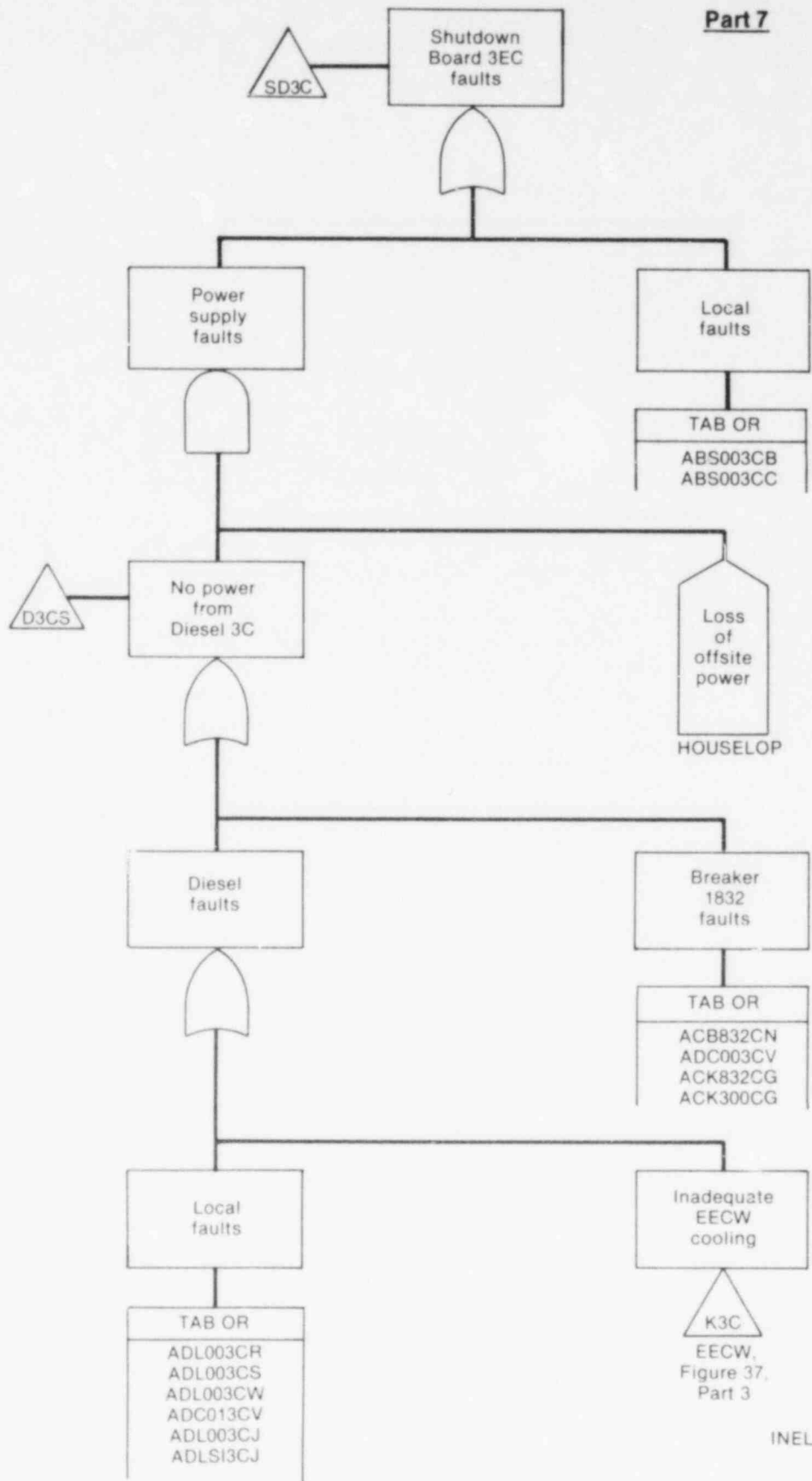
INEL 2 1557

Figure B-31. (continued)



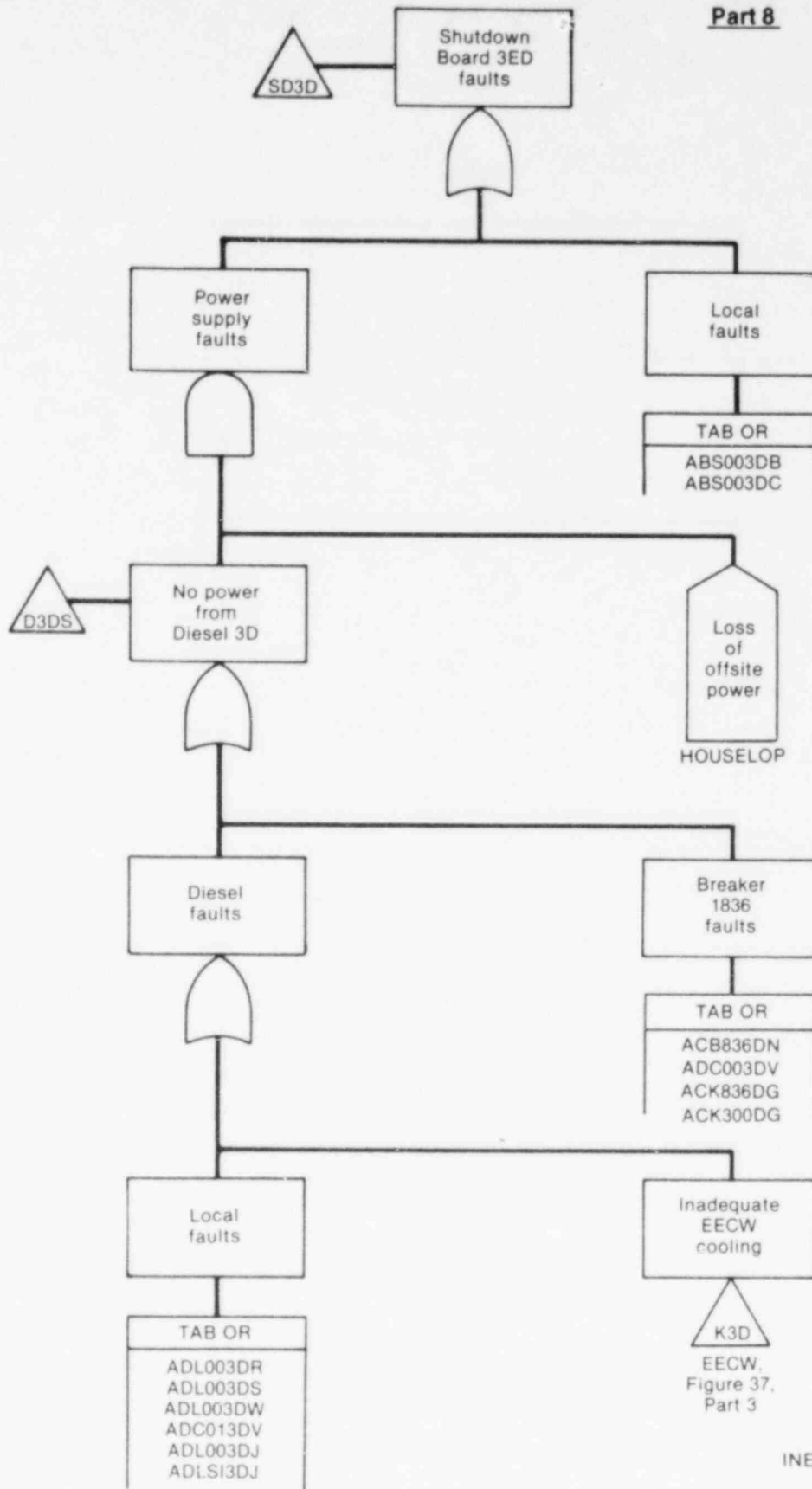
INEL 2 1558

Figure B-31. (continued)



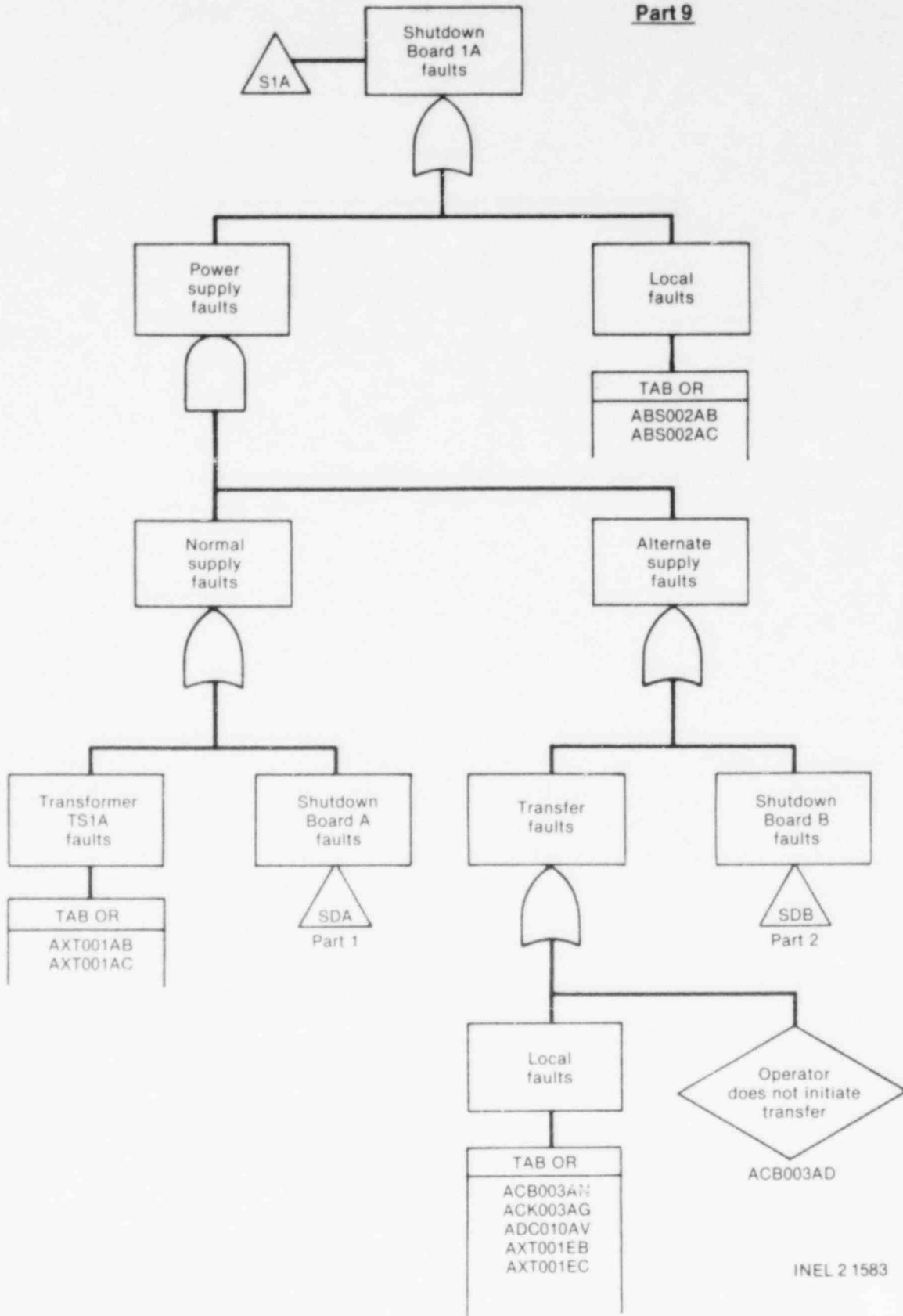
INEL 2 1559

Figure B-31. (continued)



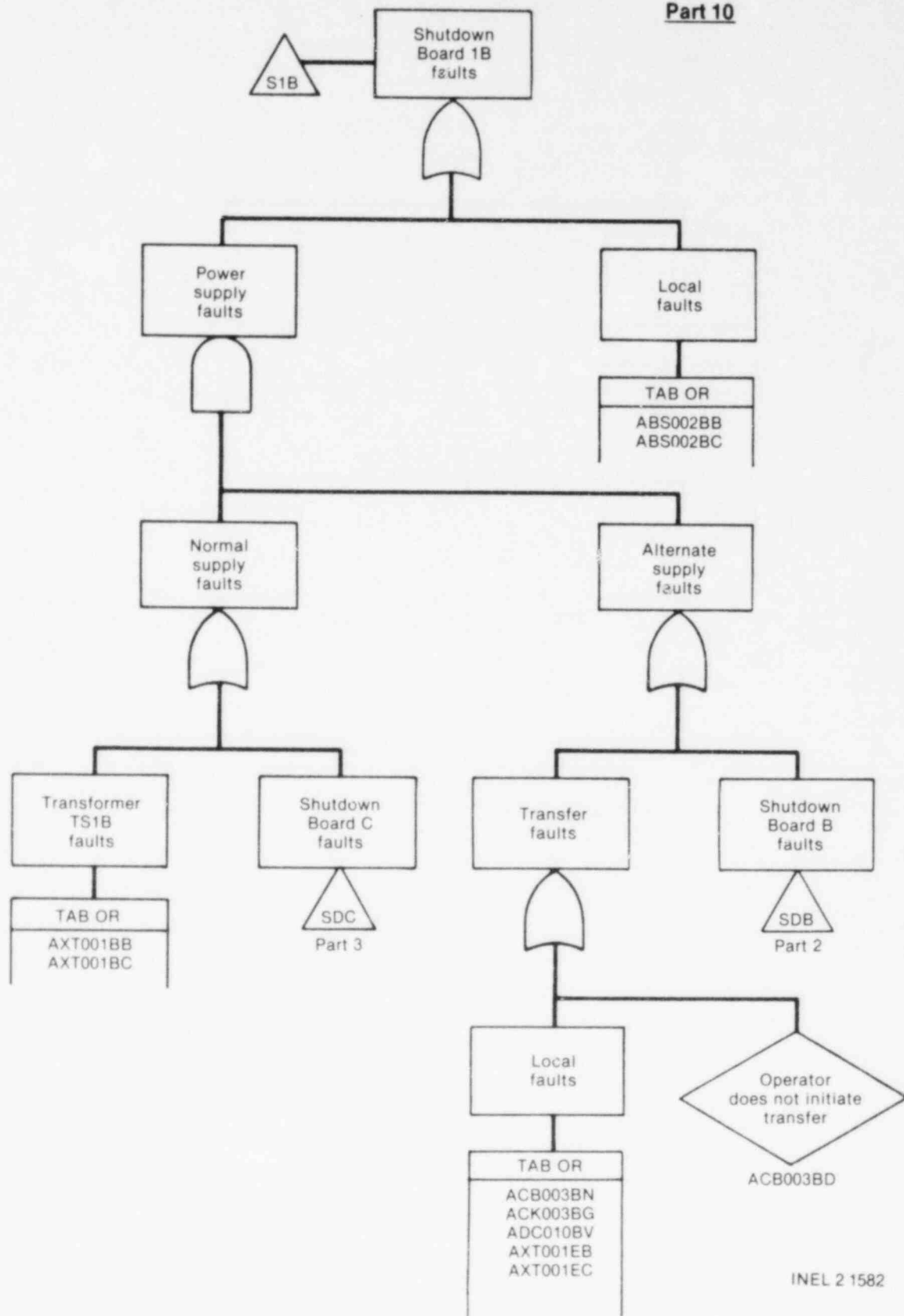
INEL 21560

Figure B-31. (continued)



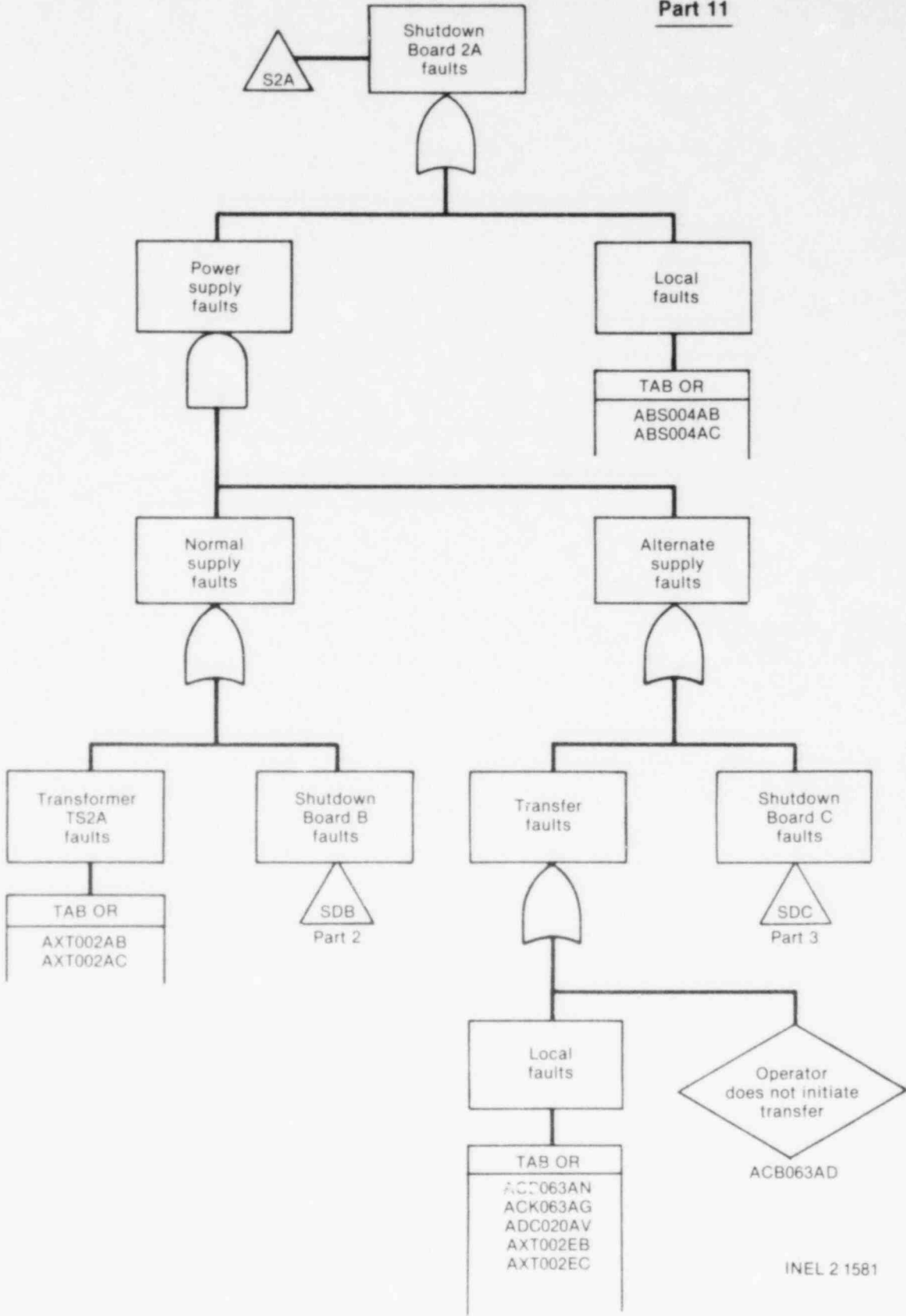
INEL 2 1583

Figure B-31. (continued)



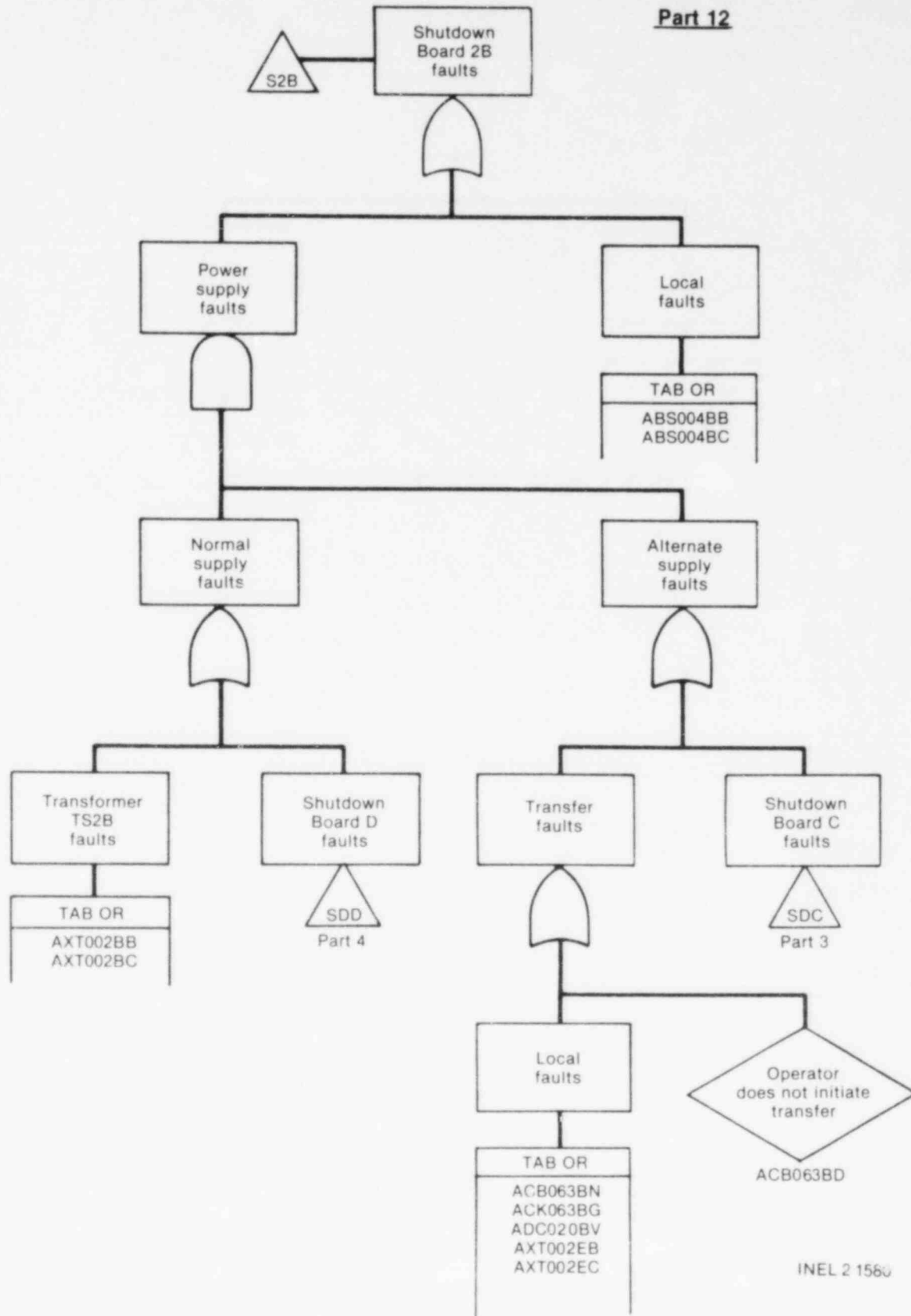
INEL 2 1582

Figure B-31. (continued)



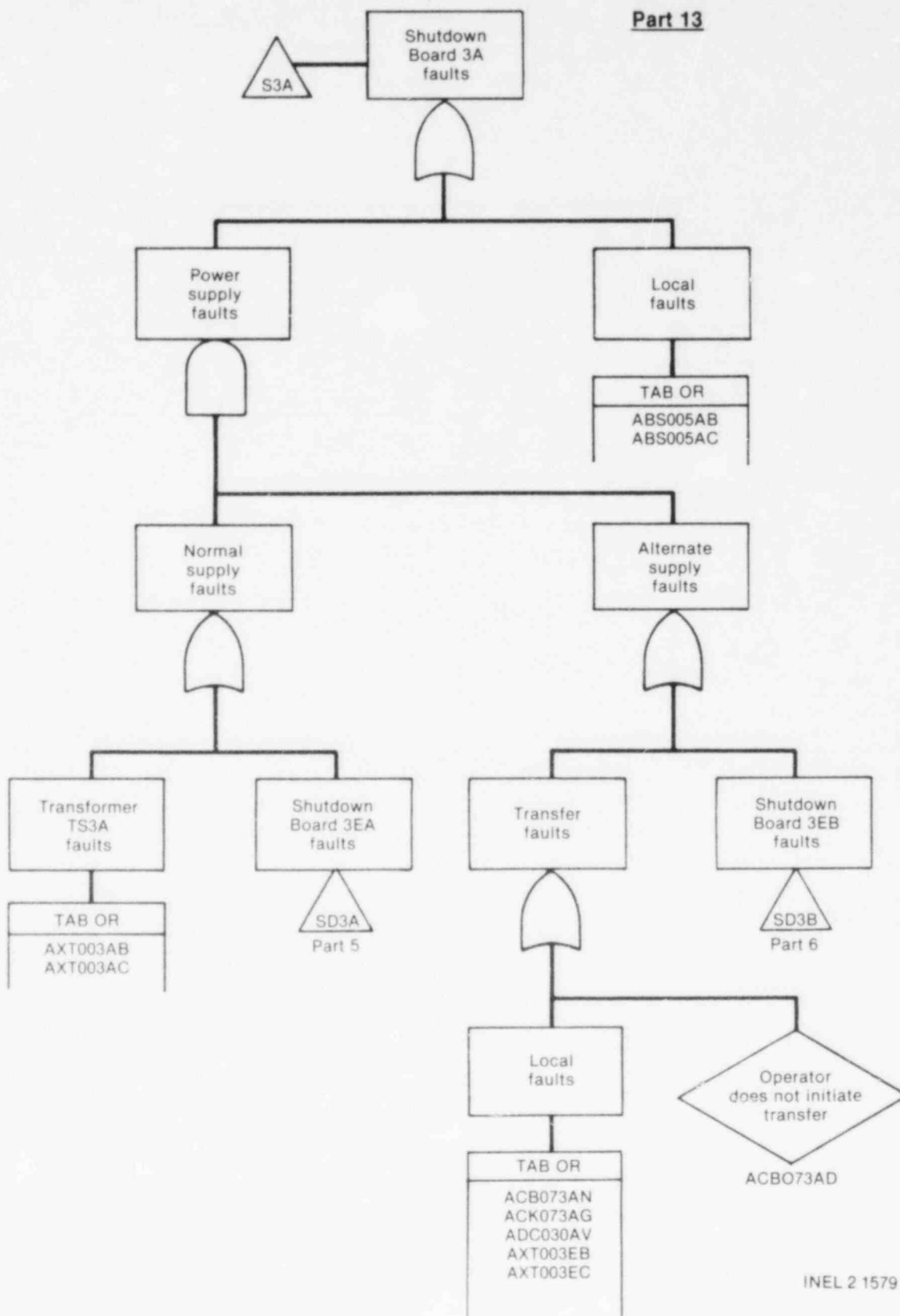
INEL 2 1581

Figure B-31. (continued)



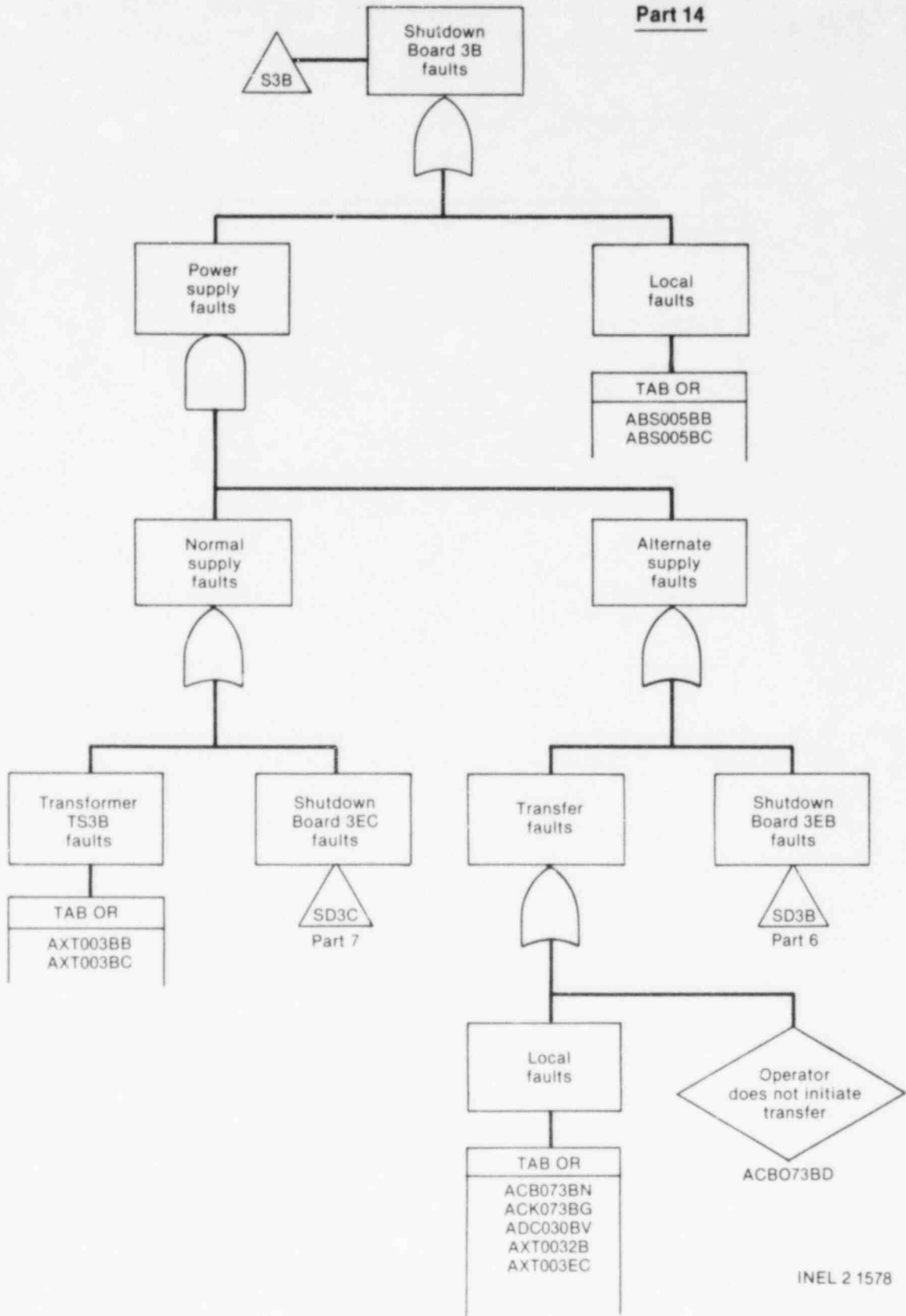
INEL 2 1560

Figure B-31. (continued)



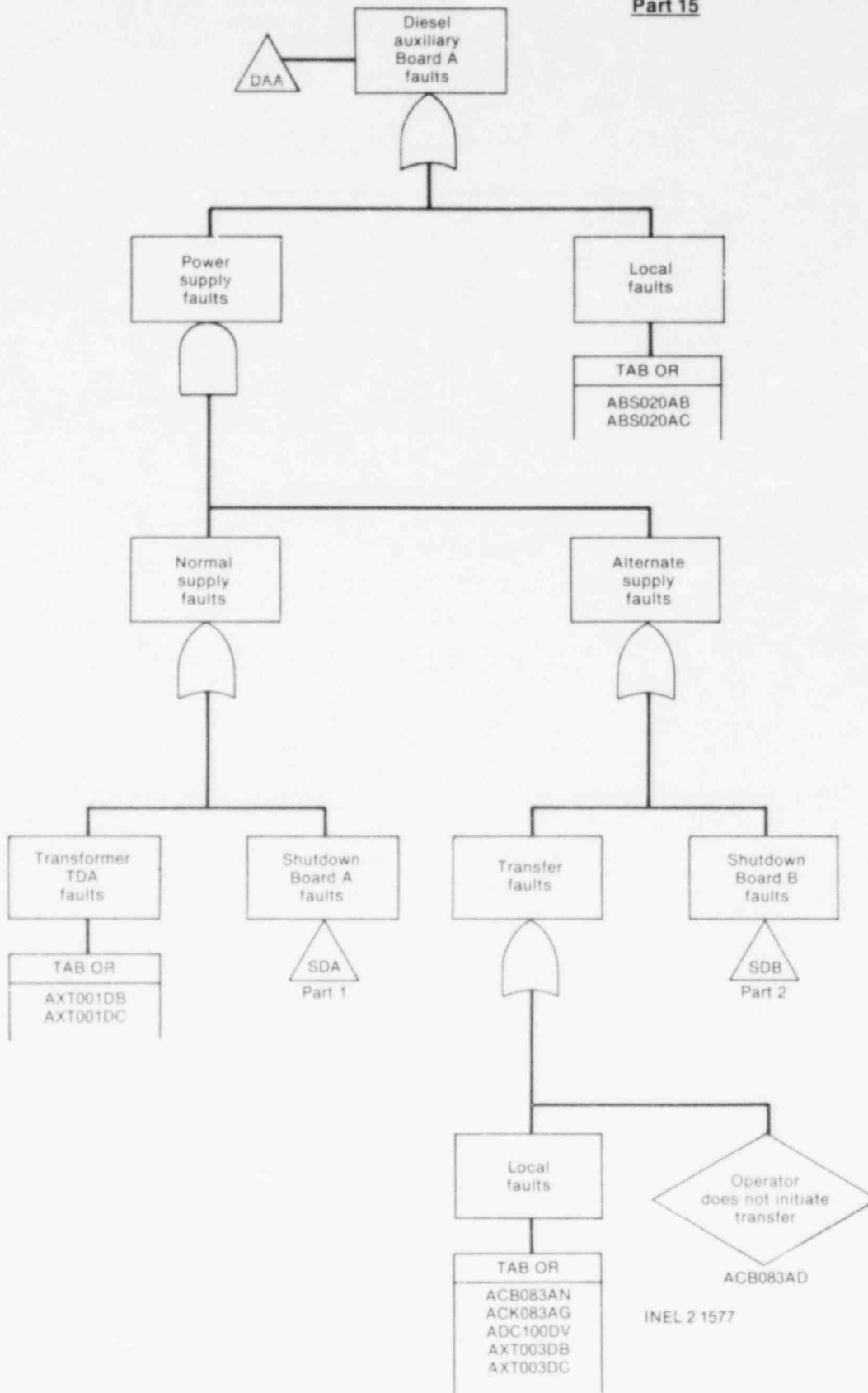
INEL 2 1579

Figure B-31. (continued)



INEL 2 1578

Figure B-31. (continued)



INEL 2 1577

Figure B-31. (continued)

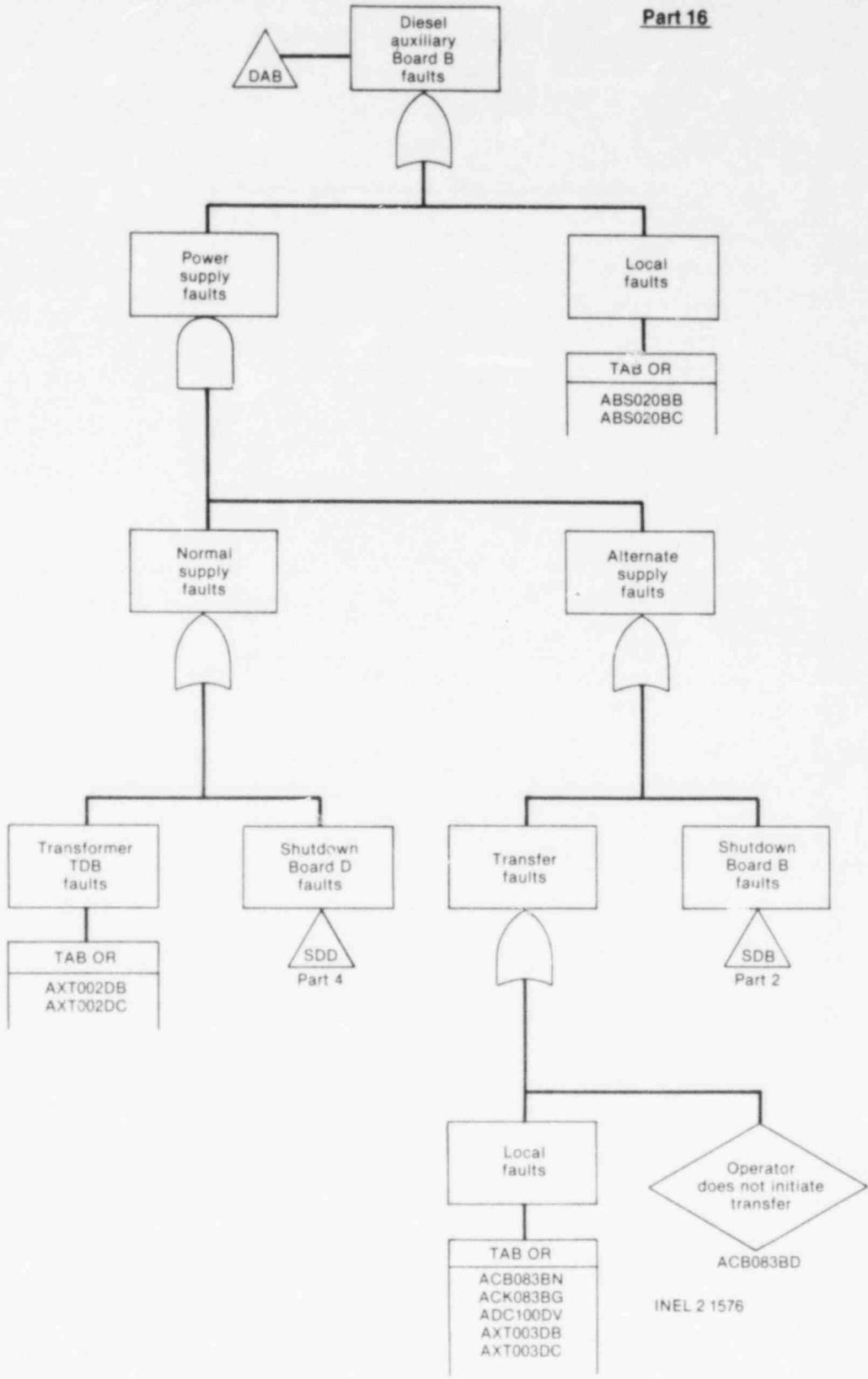
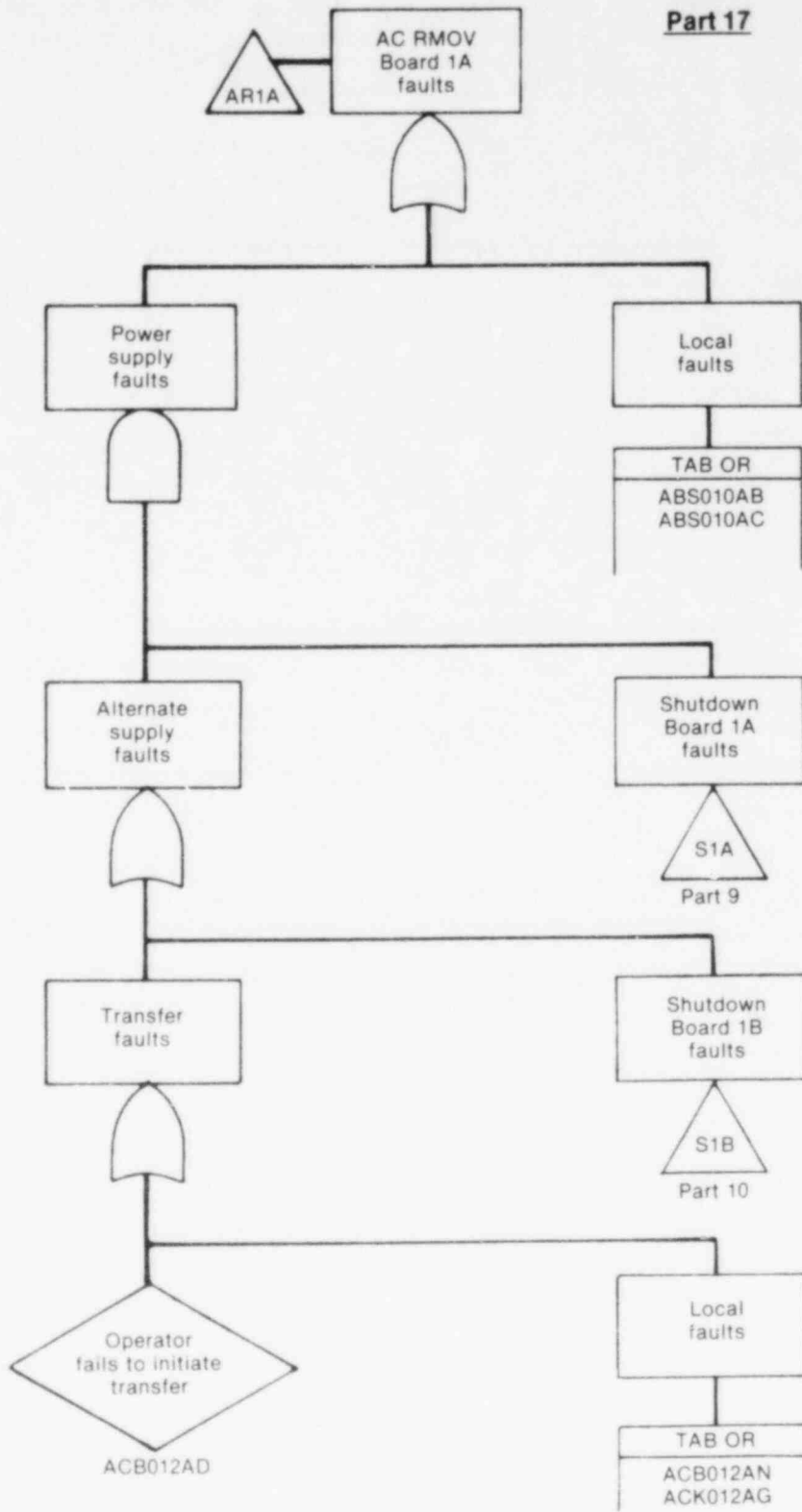


Figure B-31. (continued)



INEL 2 1575

Figure B-31. (continued)

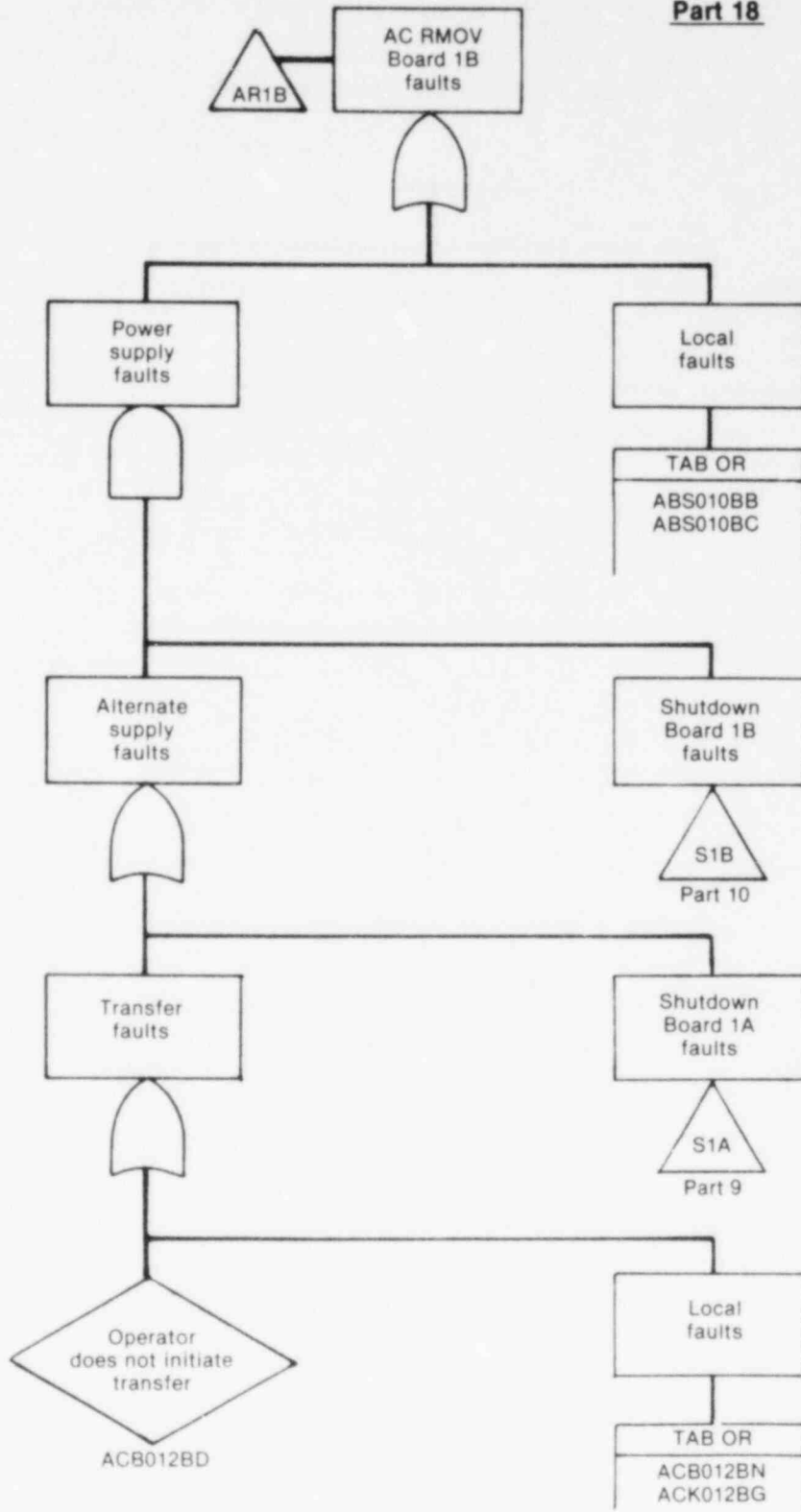
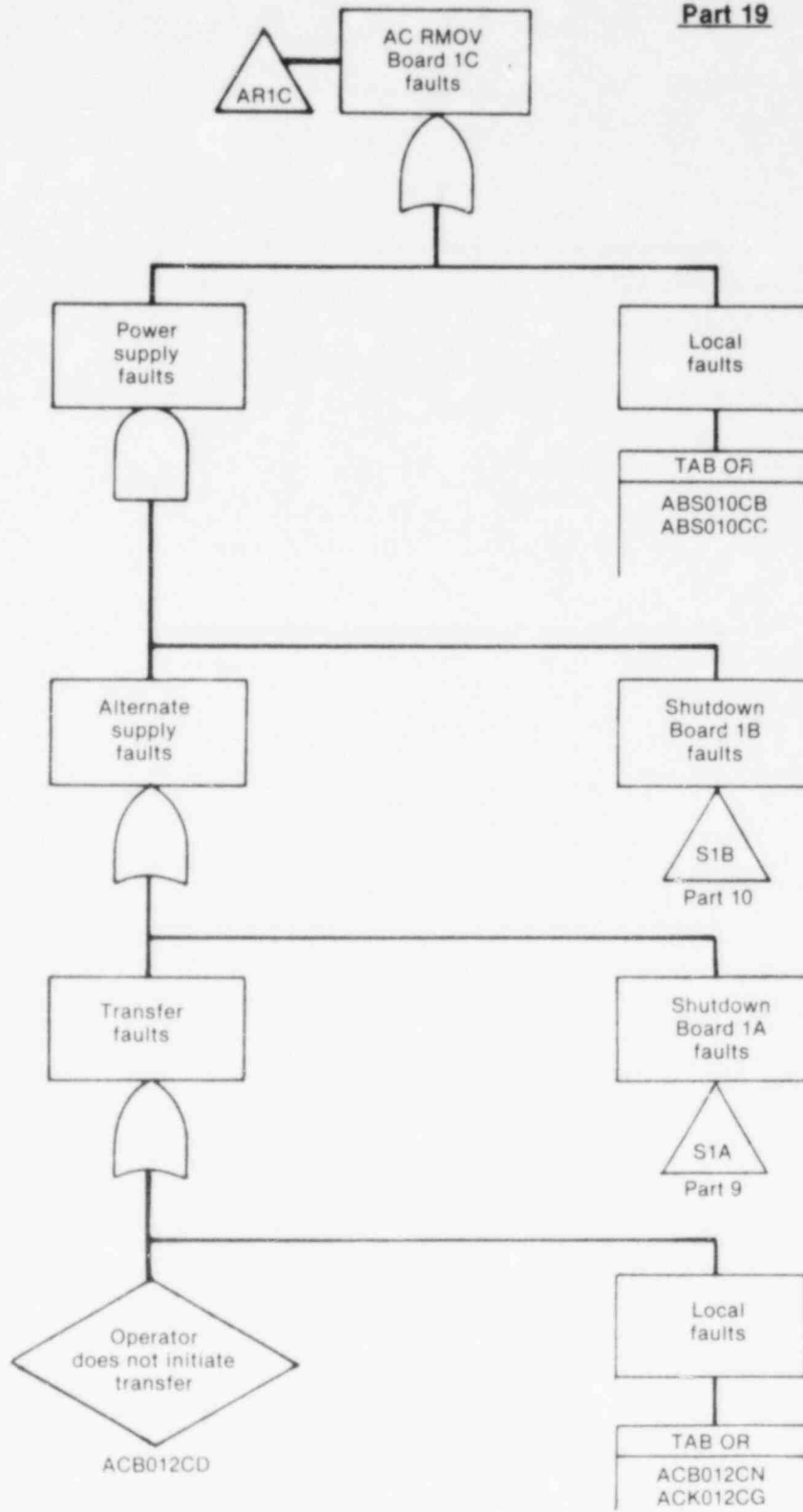
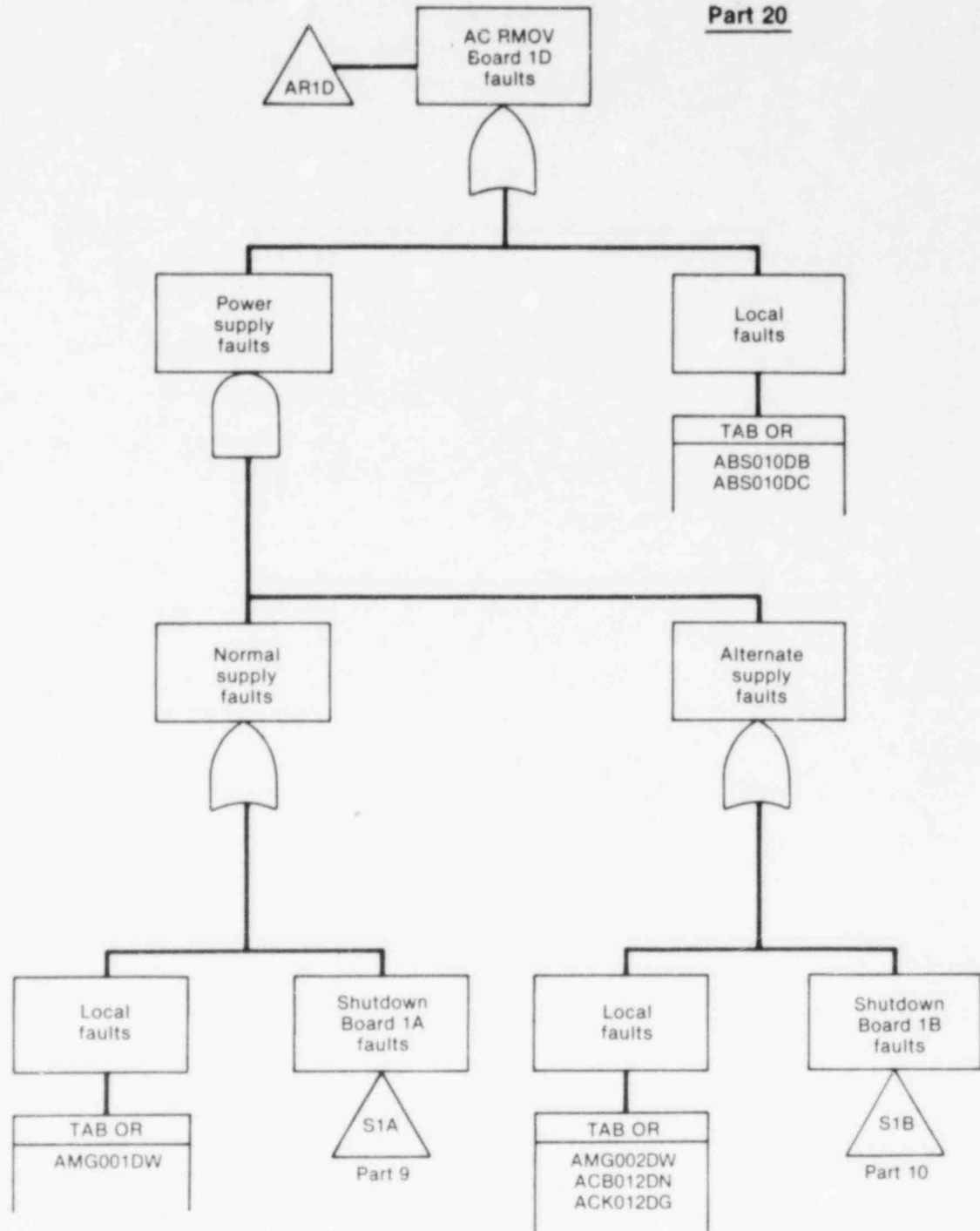


Figure B-31. (continued)



INEL 2 1573

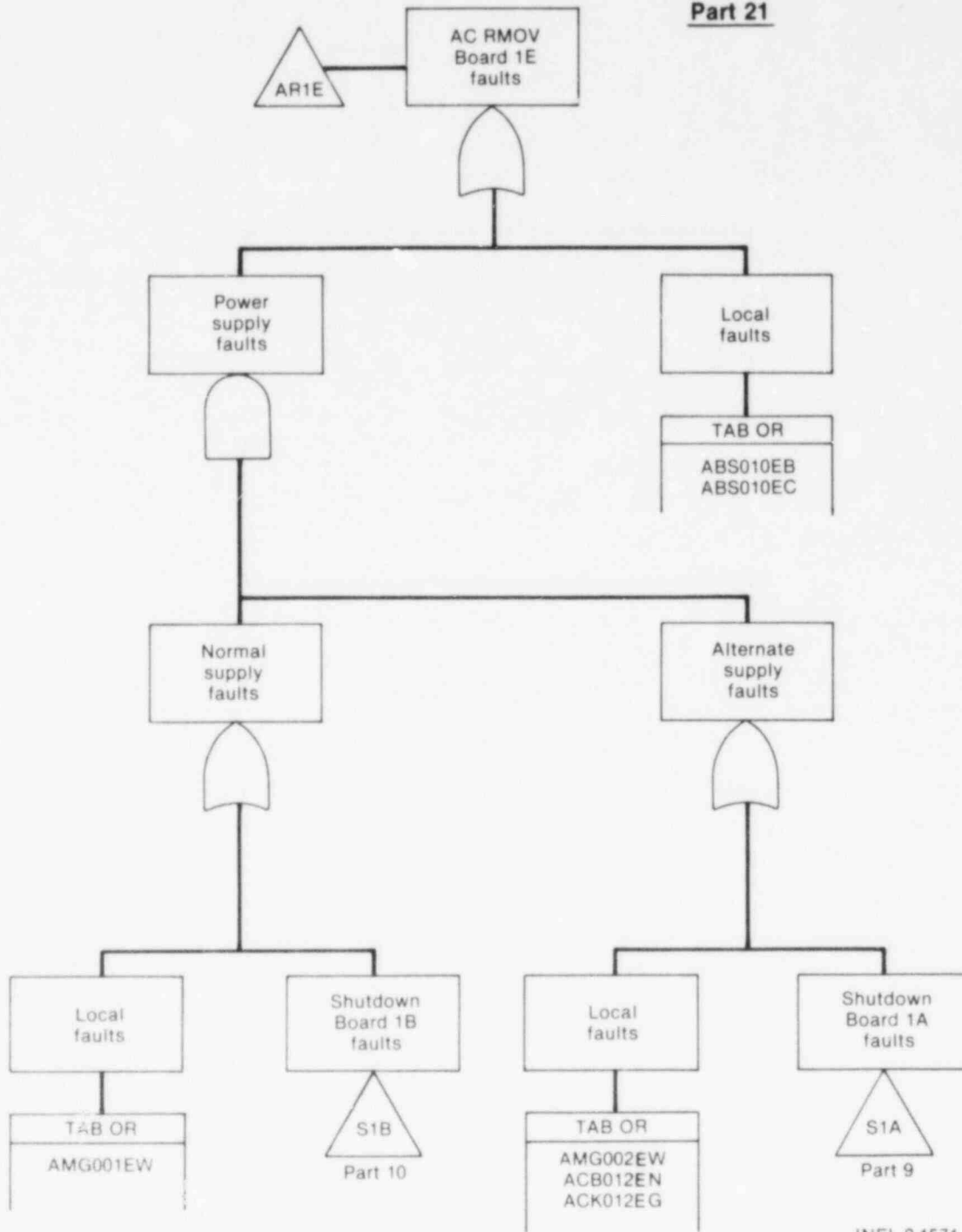
Figure B-31. (continued)



INEL 2 1572

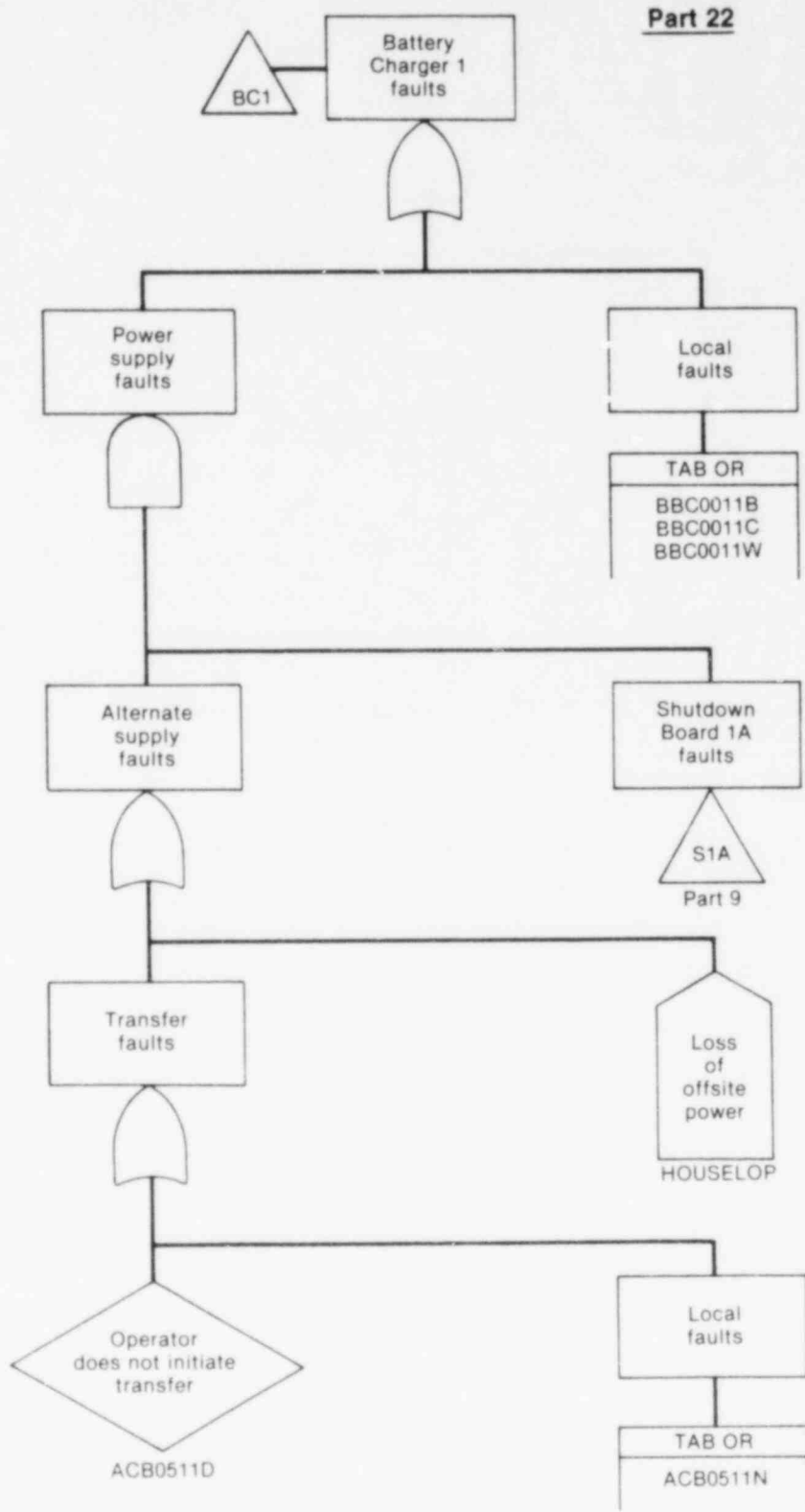
Figure B-31. (continued)

Part 21



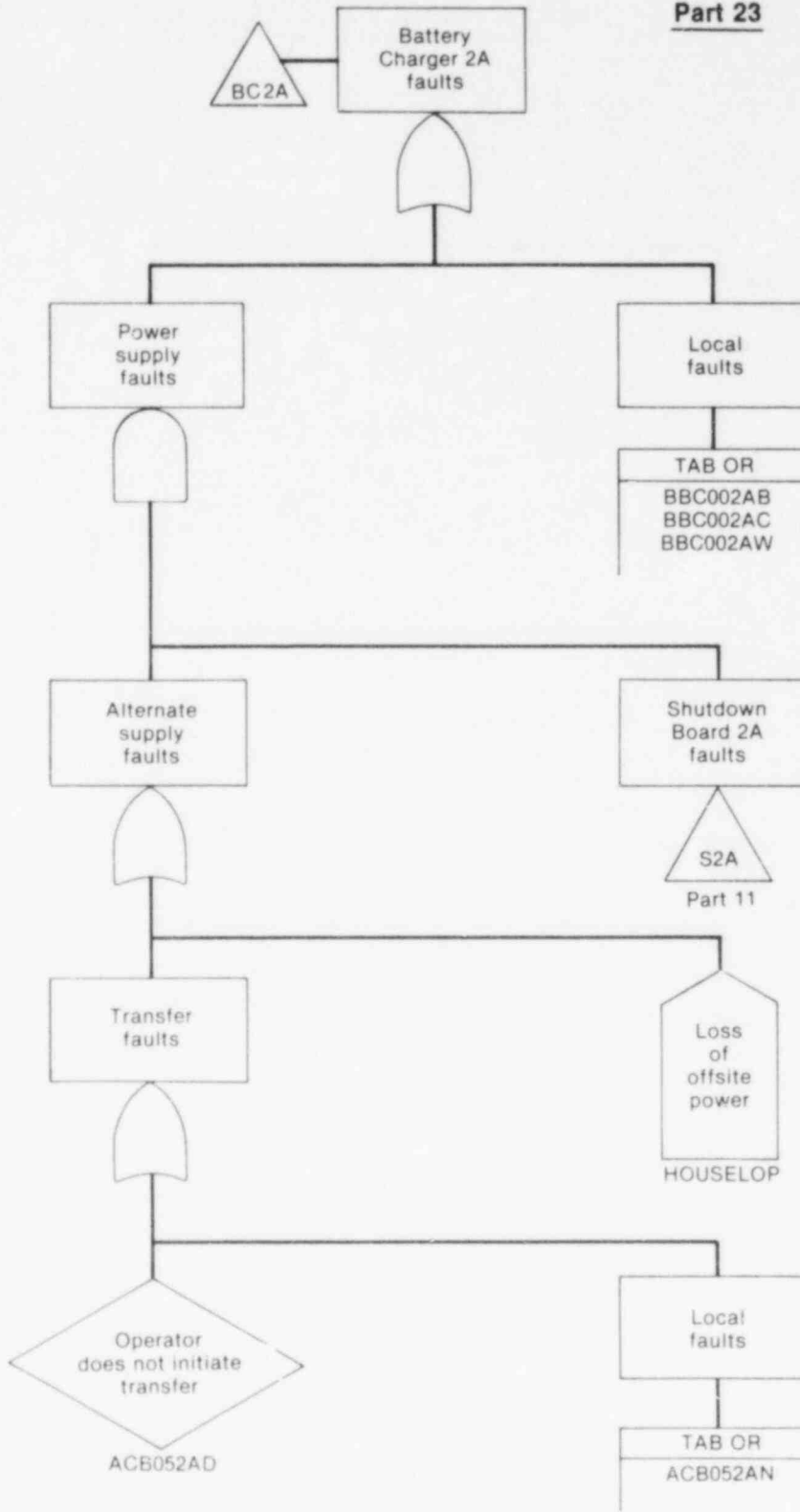
INEL 2 1571

Figure B-31. (continued).



INEL 2 1570

Figure B-31. (continued)



INEL 2 1569

Figure B-31. (continued)

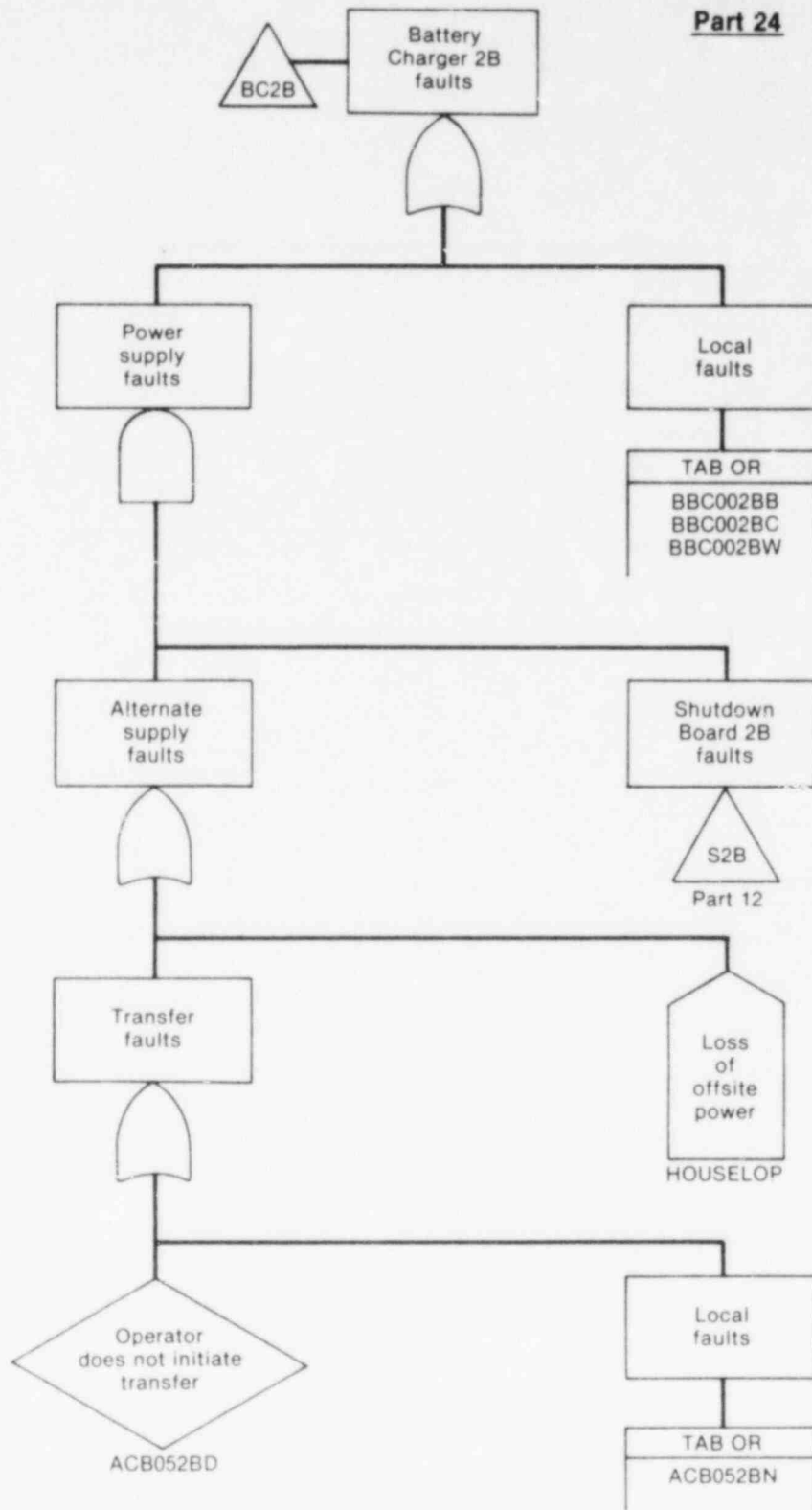
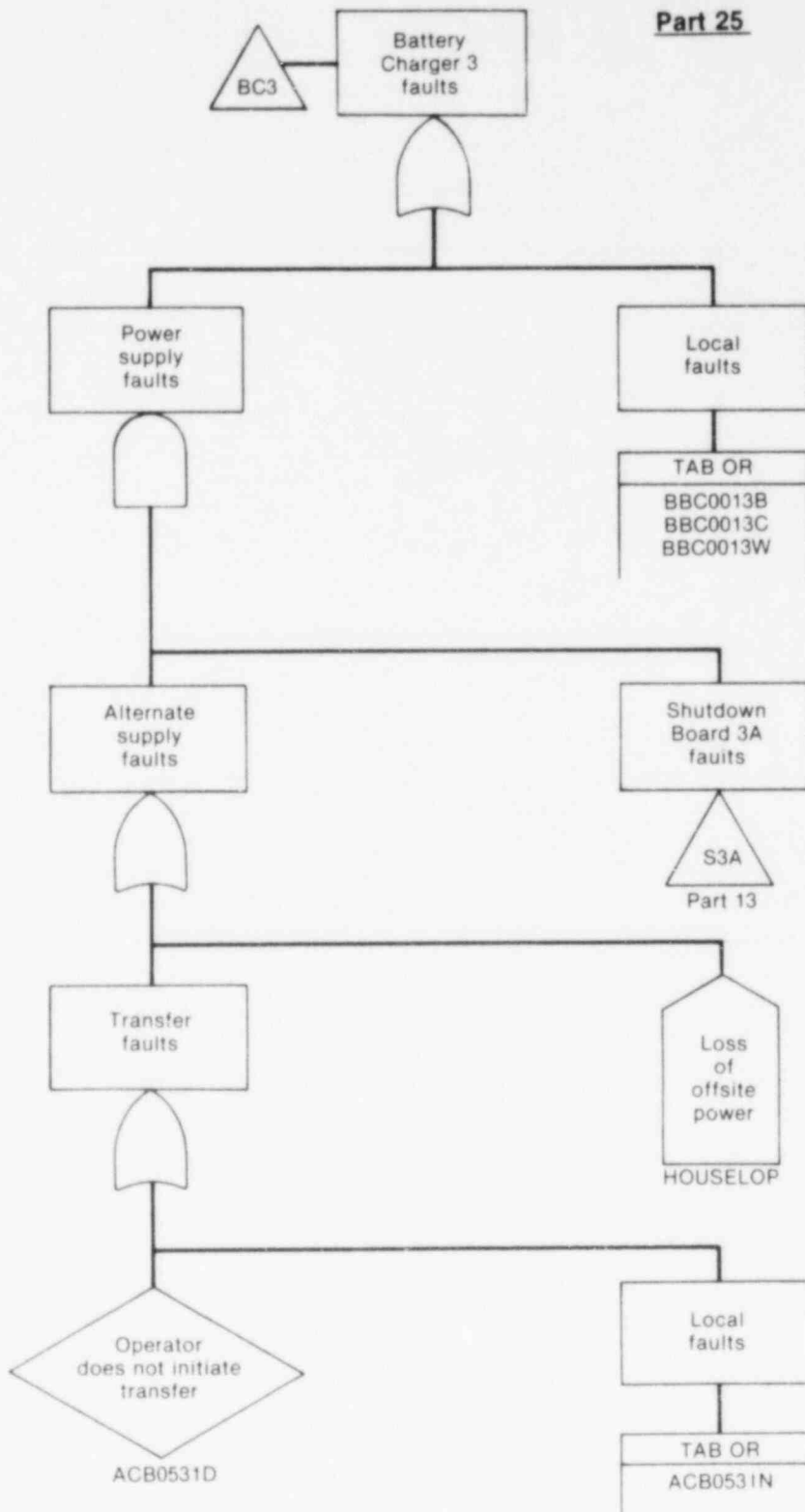


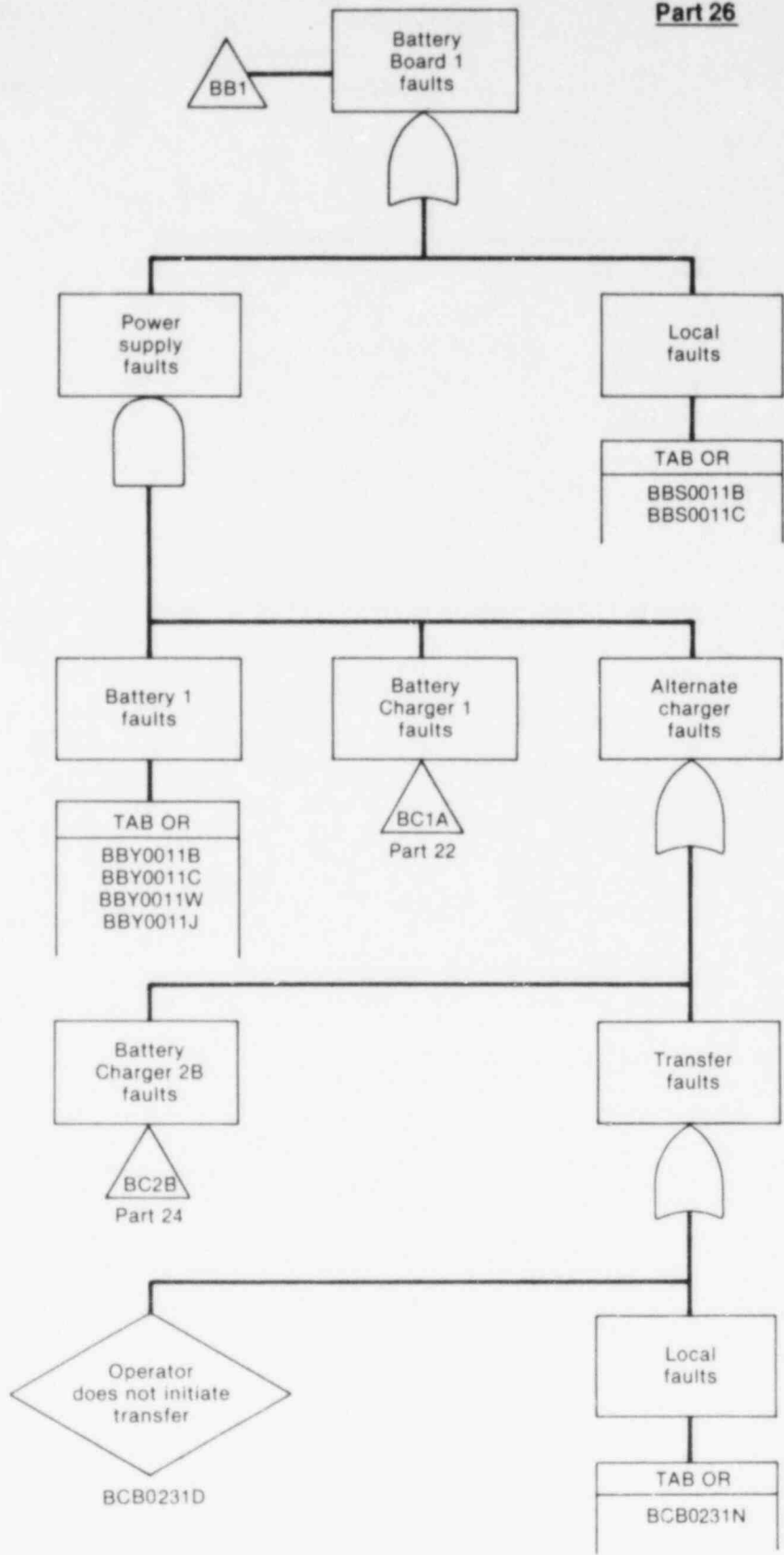
Figure B-31. (continued)

Part 25



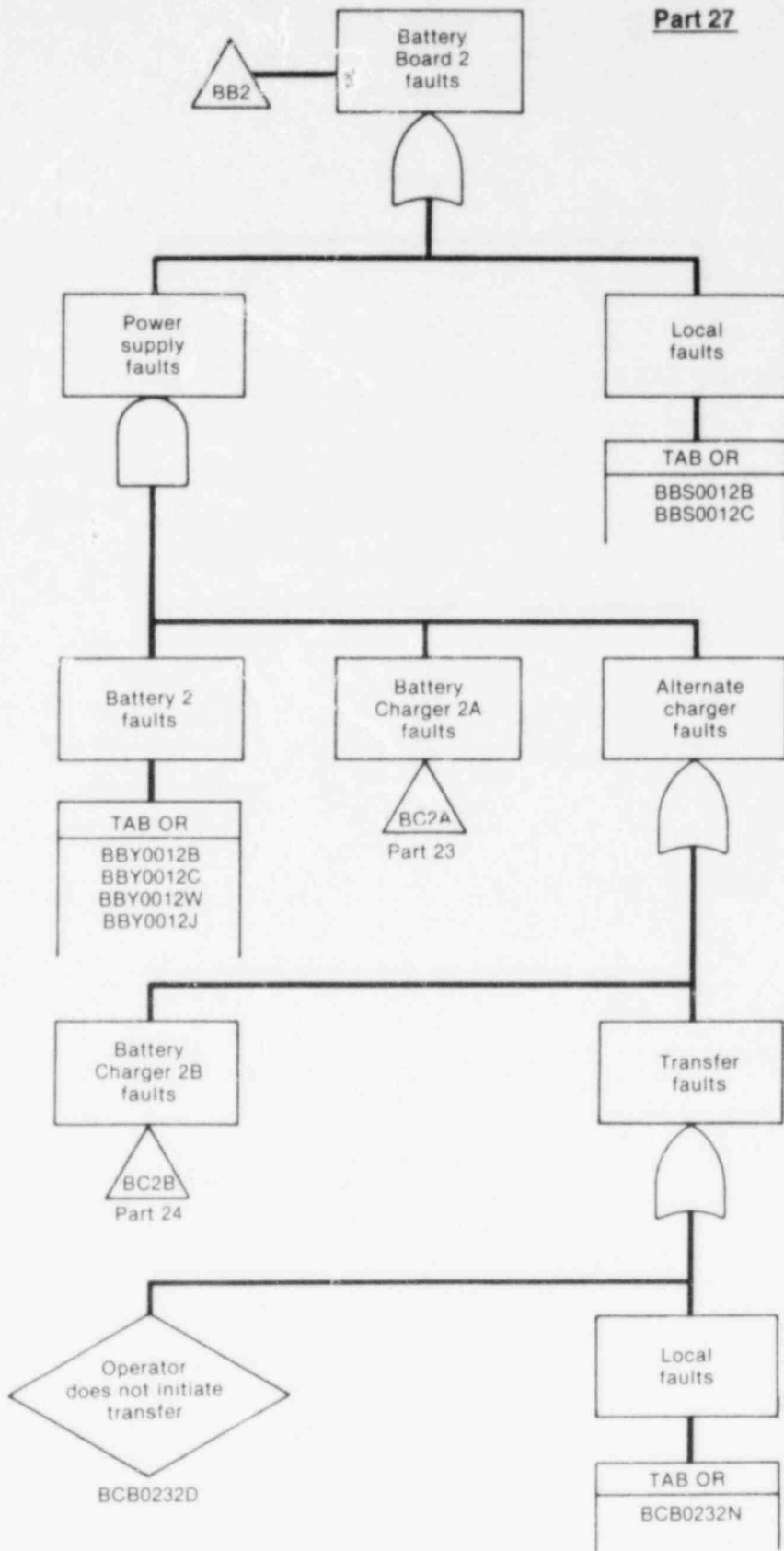
INEL 2 1567

Figure B-31. (continued)



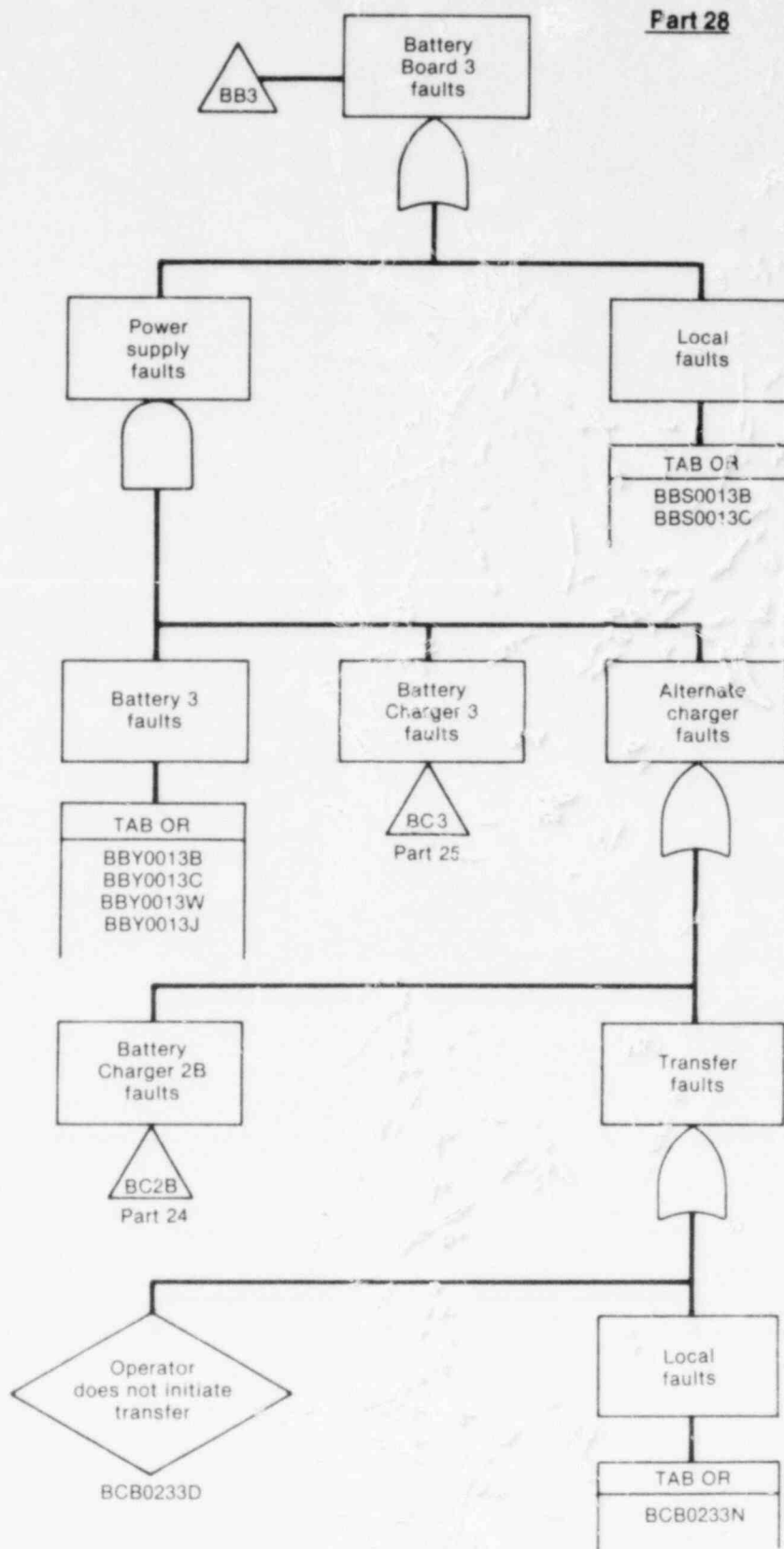
INEL 2 1566

Figure B-31. (continued)



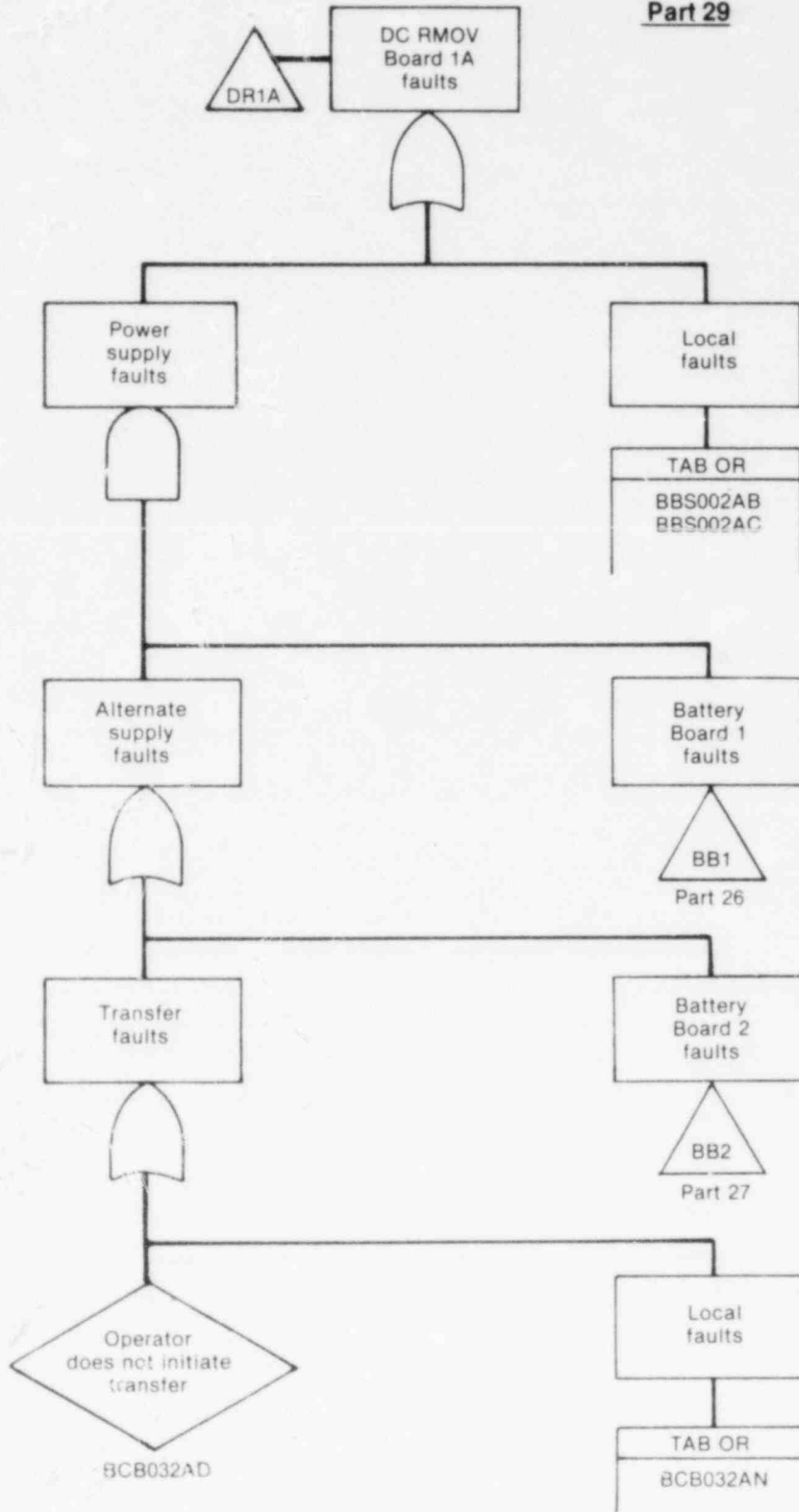
INEL 2 1565

Figure B-31. (continued)



INEL 2 1564

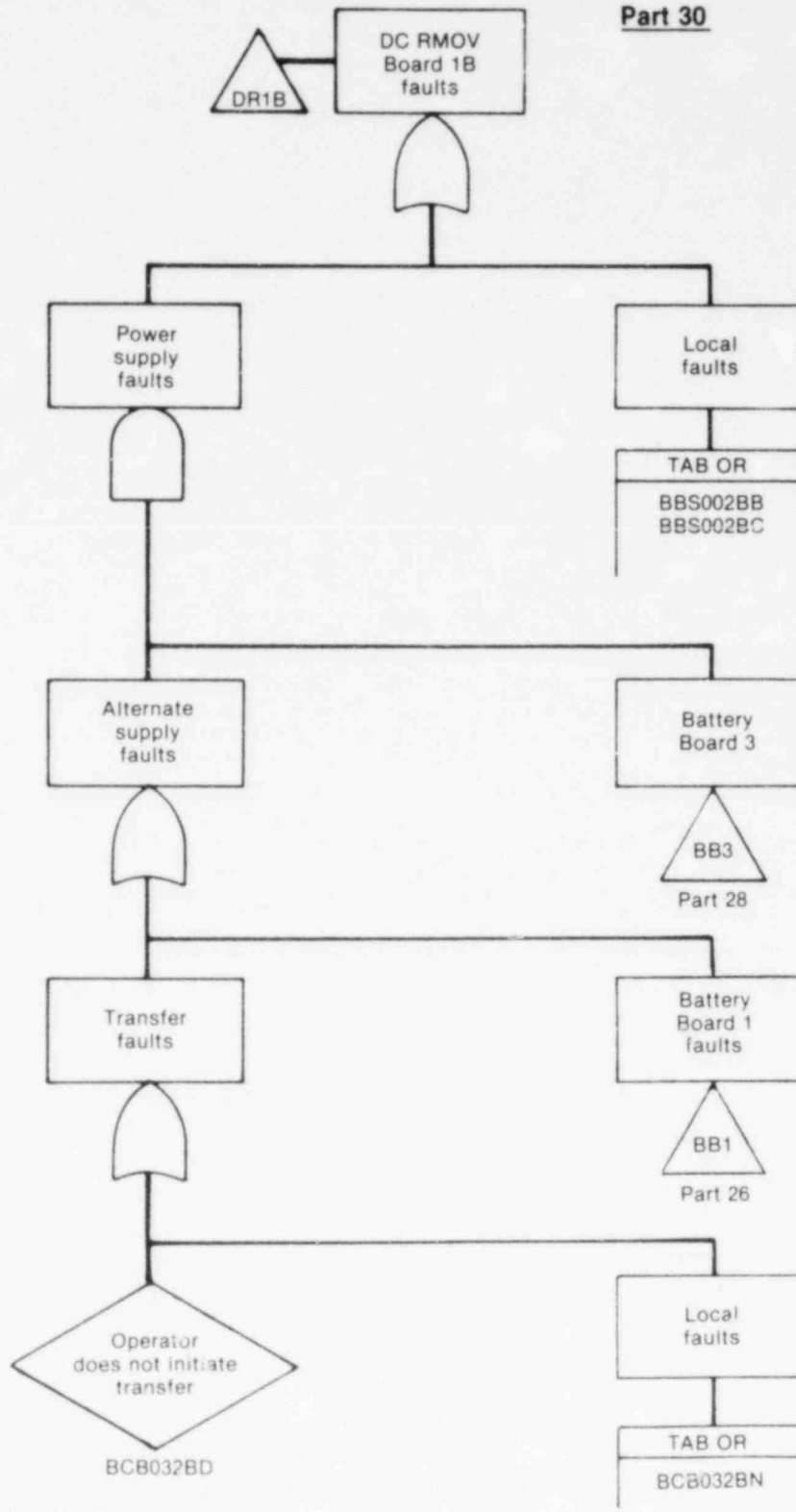
Figure B-31. (continued)



INEL 2 1563

Figure B-31. (continued)

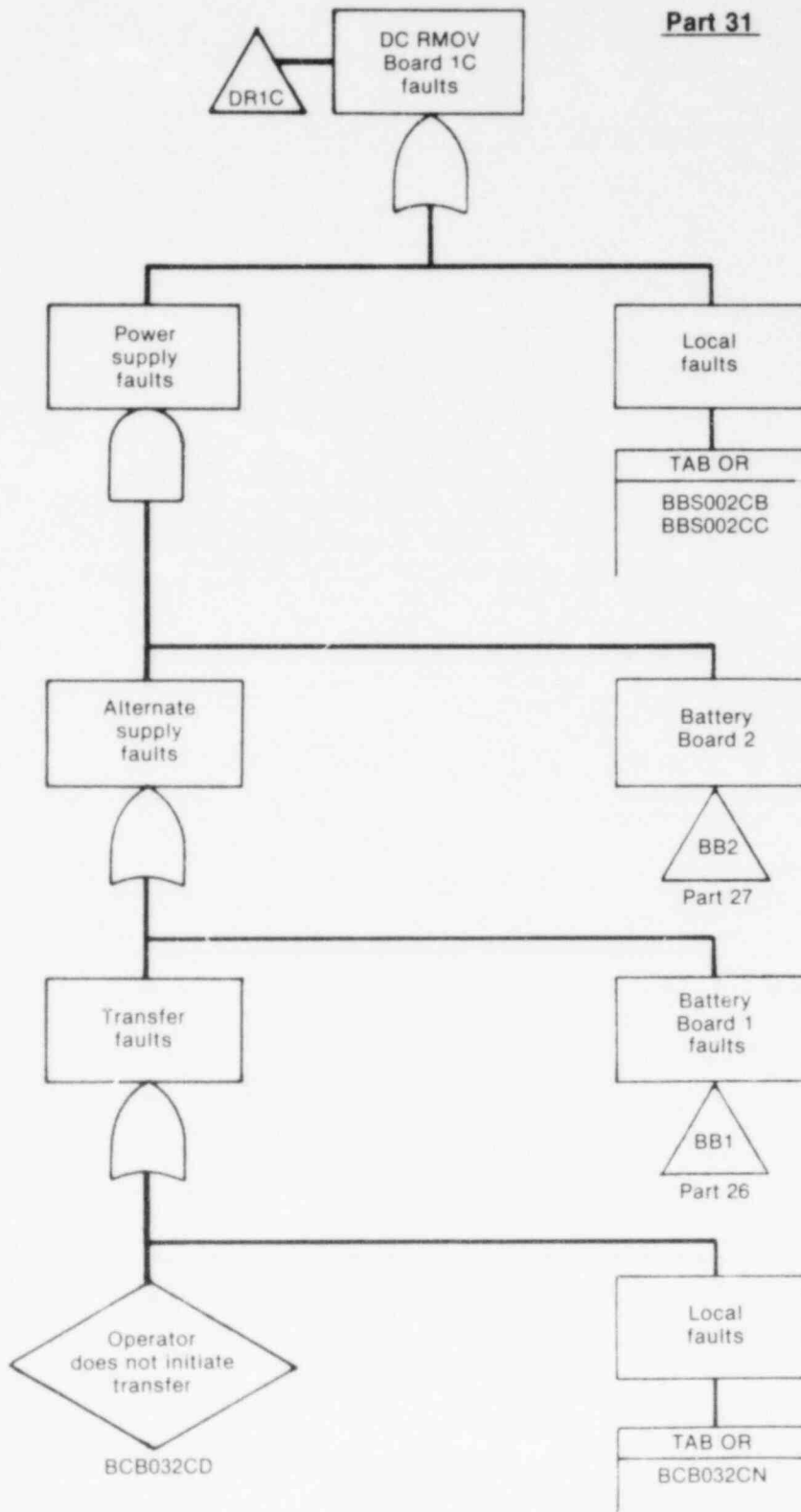
Part 30



INEL 2 1562

Figure B-31. (continued)

Part 31



INEL 2 1561

Figure B-31. (continued)

since they are not members of a minimal cut set; therefore, they do not appear in the fault tree. The undervoltage signal does appear separately from other control circuit faults.

Success/Failure Criteria. There are no success/failure criteria for the EPS as a whole. Instead, each bus that interfaces with a front-line or support system appears in the fault trees. Failure is defined as insufficient power at the bus to supply its loads. In general, this criteria divides into two parts: local bus faults and power supply faults.

Only those buses that interface with mitigating systems appear in the fault trees. Additionally, those buses that can only be supplied from off-site power (i.e., have no diesel generator backup) are not modeled. The event "No offsite power" appears in the front-line and support system trees for those buses. For non-loss-of-offsite-power initiators the probability of losing offsite power subsequently appears in the trees. For the loss-of-offsite-power transient, the value for this event is 1.0.

Major Assumptions. The following major assumptions were used in the construction of the EPS fault trees.

1. Only those breakers that are required to operate (change position) appear in the tree. Normally closed or open breakers that do not need to operate, and/or are not caused to operate by their control circuitry, do not appear in the fault trees.
2. Operator interfaces in the fault trees differ depending on the nature of the control circuitry. If manual operation is required, the operator is included only if there exists a procedure directing him to take some action. Otherwise, no credit for operator action appears.

Basic Events. The information associated with the various basic events listed in the fault tree is summarized in the EPS fault summary short form, Table B-62. In addition, the failure data associated with these basic events is summarized in Table B-63. Tables B-64 through B-69 list the dominant contributors to the various EPS bus unavailabilities.

TABLE B-62. EPS FAULT SUMMARY SHORT FORM

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ABS001AB	Shutdown Board A	Open circuit	3E-8/hr	7	10
ABS001AC	Shutdown Board A	Short to ground	3E-7/hr	7	10
ACB818AN	Circuit Breaker 1818 Diesel A to shutdown Board A	Does not close	1E-3/D	--	3
ADCO01AV	Shutdown Board A DC continuous power	Does not energize	1E-6/hr	7	3
ACK818AG	Circuit Breaker 1818 continuous circuit	No output	2.9E-3	--	10
ACK100AG	Shutdown Board A undervoltage circuit	No output	2.9E-3	--	10
ADL001AR	Diesel A	Does not start	3E-2/D	--	3
ADL001AS	Diesel A	Does not run	3E-4/hr	8	10
ADL001AW	Diesel A	Loss of function	1E-6/hr	8	10
ADCO11AV	Diesel A continuous power	Does not energize	1E-6/hr	7	3

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ADL001AJ	Diesel A	Maintenance	2.9E-3	--	0
ADLS11AJ	Diesel A	Test	3.5E-4	--	0
ABSO01BB	Shutdown Board B	Open circuit	3E-8/hr	7	10
ABSO01BC	Shutdown Board B	Short to ground	3E-7/hr	7	10
ACB822BN	Circuit Breaker 1822 Diesel B to shutdown Board B	Does not close	1E-3/D	--	3
ADC001BV	Shutdown Board B continuous power	Does not energize	1E-6/hr	7	3
ACK822BG	Circuit Breaker 1822 continuous circuit	No output	2.9E-3	--	10
ACK100BG	Shutdown Board B undervoltage circuit	No output	2.9E-3	--	10
ADL001BR	Diesel B	Does not start	3E-2/D	--	3
ADL001BS	Diesel B	Does not run	3E-4/hr	8	10

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ADL001BW	Diesel B	Loss of function	1E-6/hr	8	10
ADC011BV	Diesel B continuous power	Does not energize	1E-6/hr	7	3
ADL001BJ	Diesel B	Maintenance	2.9E-3	--	0
ADLS11BJ	Diesel B	Test	3.5E-4	--	0
ABS001CB	Shutdown Board C	Open circuit	3E-8/hr	7	10
ABS001CC	Shutdown Board C	Short to ground	3E-7/hr	7	10
ACB812CN	Circuit Breaker 1812 Diesel C to shutdown Board C	Does not close	1E-3/D	--	3
ADC001CV	Shutdown Board C continuous power	Does not energize	1E-6/hr	7	3
ACK812CG	Circuit Breaker 1812 continuous circuit	No output	2.9E-3	--	10
ACK100CG	Shutdown Board C undervoltage circuit	No output	2.9E-3	--	10

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ADL001CR	Diesel C	Does not start	3E-2/D	--	3
ADL001CS	↓	Does not run	3E-4/hr	8	10
ADL001CW		Loss of function	1E-6/hr	8	10
ADL001CJ		Maintenance	2.9E-3	--	0
ADLS11CJ		Test	3.5E-4	--	0
ADC011CV	Diesel C continuous power	Does not energize	1E-6/hr	7	3
ABS001DB	Shutdown Board D	Open circuit	3E-8/hr	7	10
ABS001DC	Shutdown Board D	Short to ground	3E-7/hr	7	10
ACB816DN	Circuit Breaker 1816 Diesel D to shutdown Board D	Does not close	1E-3/D	--	3
ADC001DV	Shutdown Board D continuous power	Does not energize	1E-6/hr	7	3

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ACK816DG	Circuit Breaker 1816 continuous circuit	No output	2.9E-3	--	10
ACK100DG	Shutdown Board D undervoltage circuit	No output	2.9E-3	--	10
ADL001DR	Diesel D	Does not start	3E-2/D	--	3
ADL001DS	Diesel D	Does not run	3E-4/hr	8	10
ADL001DW	Diesel D	Loss of function	1E-6/hr	8	10
ADC011DV	Diesel D continuous power	Does not energize	1E-6/hr	7	3
ADL001DJ	Diesel D	Maintenance	2.9E-3	--	0
ADLS11DJ	Diesel D	Test	3.5E-4	--	0
ABS003AB	Shutdown Board 3EA	Open circuit	3E-8/hr	7	10
ABS003AC	Shutdown Board 3EA	Short to ground	3E-7/hr	7	10

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ACB838AN	Circuit Breaker 1838 Diesel 3A to shutdown Board 3EA	Does not close	1E-3/D	--	3
ADC003AV	Shutdown Board 3EA continuous power	Does not energize	1E-6/hr	7	3
ACK838AG	Circuit Breaker 1838 continuous circuit	No output	2.9E-3	--	10
ACK300AG	Shutdown Board 3EA undervoltage circuit	No output	2.9E-3	--	10
ADL003AR	Diesel 3A	Does not start	3E-2/D	--	3
ADL003AS	Diesel 3A	Does not run	3E-4/hr	8	10
ADL003AW	Diesel 3A	Loss of function	1E-6/hr	8	10
ADC013AV	Diesel 3A continuous power	Does not energize	1E-6/hr	7	3
ADL003AJ	Diesel 3A	Maintenance	2.9E-3	--	0
ADLS13AJ	Diesel 3A	Test	3.5E-4	--	0

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ABS003BB	Shutdown Board 3EB	Open circuit	3E-8/hr	7	10
ABS003BC	Shutdown Board 3EB	Short to ground	3E-7/hr	7	10
ACB842BN	Circuit Breaker 1842 Diesel 3B to shutdown Board 3EB	Does not close	1E-3/D	--	3
ADC003BV	Shutdown Board 3EB continuous power	Does not energize	1E-6/hr	7	3
ACK842BG	Circuit Breaker 1842 continuous circuit	No output	2.9E-3	--	10
ACK300BG	Shutdown Board 3EB undervoltage circuit	No output	2.9E-3	--	10
ADL003BR	Diesel 3B	Does not start	3E-2/D	--	3
ADL003BS	Diesel 3B	Does not run	3E-4/hr	8	10
ADL003BW	Diesel 3B	Loss of function	1E-6/hr	8	10

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ADC013BV	Diesel 3B continuous power	Does not energize	1E-6/hr	7	3
ADL003BJ	Diesel 3B	Maintenance	2.9E-3	--	0
ADLS13BJ	Diesel 3B	Test	3.5E-4	--	0
ABS003CB	Shutdown Board 3EC	Open circuit	3E-8/hr	7	10
ABS003CC	Shutdown Board 3EC	Short to ground	3E-7/hr	7	10
ACB832CN	Circuit Breaker 1832 Diesel 3C to shutdown Board 3EC	Does not close	1E-3/D	--	3
ADC003CV	Shutdown Board 3EC continuous power	Does not energize	1E-6/hr	7	3
ACK832CG	Circuit Breaker 1832 continuous circuit	No output	2.9E-3	--	10
ACK300CG	Shutdown Board 3EC undervoltage circuit	No output	2.9E-3	--	10
ADL003CR	Diesel 3C	Does not start	3E-2/D	--	3

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ADL003CS	Diesel 3C	Does not run	3E-4/hr	8	10
ADL003CW	Diesel 3C	Loss of function	1E-6/hr	8	10
ADC013CV	Diesel 3C continuous power	Does not energize	1E-6/hr	7	3
ADL003CJ	Diesel 3C	Maintenance	2.9E-3	--	0
ADLSI3CJ	Diesel 3C	Test	3.5E-4	--	0
ABS003DB	Shutdown Board 3ED	Open circuit	3E-8/hr	7	10
ABS003DC	Shutdown Board 3ED	Short to ground	3E-7/hr	7	10
ACB836DN	Circuit Breaker 1836 Diesel 3D to shutdown Board 3ED	Does not close	1E-3/D	--	3
ADC003DV	Shutdown Board 3ED continuous power	Does not energize	1E-6/hr	7	3
ACK836DG	Circuit Breaker 1836 continuous circuit	No output	2.9E-3	--	10

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ACK300DG	Shutdown Board 3ED undervoltage circuit	No output	2.9E-3	--	10
ADL003DR	Diesel 3D	Does not start	3E-2/D	--	3
ADL003DS	Diesel 3D	Does not run	3E-4/hr	8	10
ADL003DW	Diesel 3D	Loss of function	1E-6/hr	8	10
ADC013DV	Diesel 3D continuous power	Does not energize	1E-6/hr	7	3
ADL003DJ	Diesel 3D	Maintenance	2.9E-3	--	0
ADLSI3DJ	Diesel 3D	Test	3.5E-4	--	0
HOUSELOP	Loss of offsite power	Offsite power lost	2.7E-5/hr	8	3
ABS002AB	Shutdown Board 1A	Open circuit	3E-8/hr	7	10
ABS002AC	Shutdown Board 1A	Short to ground	3E-7/hr	7	10

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
AXT001AB	Transformer TSIA	Open circuit	1E-6/hr	7	3
AXT001AC	Transformer TSIA	Short to ground	↓	↓	↓
AXT001EB	Transformer TSIE	Open circuit			
AXT001EC	Transformer TSIE	Short to ground			
ACB003AN	Circuit Breaker 0003A Transformer TSIE to shutdown Board 1A	Does not close	1E-3/D	--	↓
ACB003AD	Circuit Breaker 0003A Transformer TSIE to shutdown Board 1A	Operator error	1E-3/D	--	10
ACK003AG	Circuit Breaker 003A continuous circuit	No output	2.9E-3	--	10
ADC010AV	Shutdown Board 1A continuous power	Does not energize	1E-6/hr	7	3
ABS002BB	Shutdown Board 1B	Open circuit	3E-8/hr	7	10

B-330

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure			
			Failure Rate	Fault Duration (hr)	Error Factor	
ABS002BC	Shutdown Board 1B	Short to ground	3E-7/hr	7	10	
AXT001BB	Transformer TS1B	Open circuit	1E-6/hr	↓	3	
AXT001BC	Transformer TS1B	Short to ground	↓		↓	↓
AXT001EB	Transformer TS1E	Open circuit	↓		↓	↓
AXT001EC	Transformer TS1E	Short to ground	↓		↓	↓
ACB003BN	Circuit Breaker 0038 Transformer TS1E to shutdown Board 1B	Does not close	1E-3/D	--	↓	
ACB003BD	Circuit Breaker 0038 Transformer TS1E to shutdown Board 1B	Operator error	1E-3/D	--	10	
ACK003BG	Circuit Breaker 003B continuous circuit	No output	2.9E-3	--	10	
ADC010BV	Shutdown Board 1B continuous power	Does not energize	1E-6/hr	7	3	

B-331

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ABS004AB	Shutdown Board 2A	Open circuit	3E-8/hr	7	10
ABS004AC	Shutdown Board 2A	Short to ground	3E-7/hr	↓	10
AXT002AB	Transformer TS2A	Open circuit	1E-6/hr		3
AXT002AC	Transformer TS2A	Short to ground	↓		↓
AXT002EB	Transformer TS2E	Open circuit	↓	↓	↓
AXT002EC	Transformer TS2E	Short to ground	↓	↓	↓
ACB063AN	Circuit Breaker 063A Transformer TS2E to shutdown Board 2A	Does not close	1E-3/D	--	↓
ACB063AD	Circuit Breaker 063A Transformer TS2E to shutdown Board 2A	Operator error	1E-3/D	--	10
ACK063AG	Circuit Breaker 063A continuous circuit	No output	2.9E-3	--	10

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ADC020AV	Shutdown Board 2A continuous power	Does not energize	1E-6/hr	7	3
ABS004BB	Shutdown Board 2B	Open circuit	3E-8/hr	↓	10
ABS004BC	Shutdown Board 2B	Short to ground	3E-7/hr		10
AXT002BB	Transformer TS2B	Open circuit	1E-6/hr		3
AXT002BC	Transformer TS2B	Short to ground	↓		↓
AXT002EB	Transformer TS2E	Open circuit			
AXT002EC	Transformer TS2E	Short to ground			
ACB063BN	Circuit Breaker 063B Transformer TS2E to shutdown Board 2B	Does not close	1E-3/D		--
ACB063BD	Circuit Breaker 063B Transformer TS2E to shutdown Board 2B	Operator error	1E-3/D	--	10

B-333

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ACK063BG	Circuit Breaker 063B continuous circuit	No output	2.9E-3	--	10
ADC020BV	Shutdown Board 2B continuous power	Does not energize	1E-6/hr	7	3
ABS005AB	Shutdown Board 3A	Open circuit	3E-8/hr	↓	10
ABS005AC	Shutdown Board 3A	Short to ground	3E-7/hr		10
AXT003AB	Transformer TS3A	Open circuit	1E-6/hr		3
AXT003AC	Transformer TS3A	Short to ground	↓		↓
AXT003EB	Transformer TS3E	Open circuit	↓	↓	↓
AXT003EC	Transformer TS3E	Short to ground			
ACB073AN	Circuit Breaker 073A Transformer TS2E to shutdown Board 3A	Does not close	1E-3/D	--	↓

B-334

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ACB073AD	Circuit Breaker 073A Transformer TS2E to shutdown Board 3A	Operator error	1E-3/D	--	10
ACK073AG	Circuit Breaker 073A continuous circuit	No output	2.9E-3	--	10
ADC030AV	Shutdown Board 3A continuous power	Does not energize	1E-6/hr	7	3
ABS005BE	Shutdown Board 3B	Open circuit	3E-8/hr	↓	10
ABS005BC	Shutdown Board 3B	Short to ground	3E-7/hr		10
AXT003BB	Transformer TS3B	Open circuit	1E-6/hr		3
AXT003BC	Transformer TS3B	Short to ground	↓		↓
AXT003EB	Transformer TS3E	Open circuit	↓		↓
AXT003EC	Transformer TS3E	Short to ground	↓		↓

B-335

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ACB073BN	Circuit Breaker 073B Transformer TS3E to shutdown Board 3B	Does not close	1E-3/D	--	3
ACB073BD	Circuit Breaker 073B Transformer TS3E to shutdown Board 3B	Operator error	1E-3/D	--	10
ACK073BG	Circuit Breaker 073B continuous circuit	No output	2.9E-3	--	10
ADC030BV	Shutdown Board 3B continuous power	Does not energize	1E-6/hr	7	3
ABS020AB	Diesel auxiliary Board A	Open circuit	3E-8/hr	↓	10
ABS020AC	Diesel auxiliary Board A	Short to ground	3E-7/hr		10
AXT001DB	Transformer TDA	Open circuit	1E-6/hr		3
AXT001DC	Transformer TDA	Short to ground	1E-6/hr		3
AXT003DB	Transformer TDE	Open circuit	1E-6/hr		3

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
AXT003DC	Transformer TDE	Short to ground	1E-6/hr	7	3
ACB083AN	Circuit Breaker 083A Transformer TDE to diesel auxiliary Board A	Does not close	1E-3/D	--	3
ACB083AD	Circuit Breaker 083A Transformer TDE to diesel auxiliary Board A	Operator error	1E-3/D	--	10
ACK083AG	Circuit Breaker 083A continuous circuit	No output	2.9E-3	--	10
ADC100DV	Diesel auxiliary Board A continuous power	Does not energize	1E-6/hr	7	3
ABS020BB	Diesel auxiliary Board B	Open circuit	3E-8/hr	↓	10
ABS020BC	Diesel auxiliary Board B	Short to ground	3E-7/hr		10
AXT002DB	Transformer TDB	Open circuit	1E-6/hr		3
AXT002DC	Transformer TDB	Short to ground	1E-6/hr		3

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
AXT003DB	Transformer TDE	Open circuit	1E-6/hr	7	3
AXT003DC	Transformer TDE	Short to ground	1E-6/hr	7	3
ACB083BN	Circuit Breaker 083B Transformer TDE to diesel auxiliary Board B	Does not close	1E-3/D	--	3
ACB083BD	Circuit Breaker 083B Transformer TDE to diesel auxiliary Board B	Operator error	1E-3/D	--	10
ACK083BG	Circuit Breaker 083B continuous circuit	No output	2.9E-3	--	10
ADC100DV	Diesel auxiliary Board B control power	Does not energize	1E-6/hr	7	3
ABS010AB	AC RMOV Board 1A	Open circuit	3E-8/hr	7	10
ABS010AC	AC RMOV Board 1A	Short to ground	3E-7/hr	7	10
ACB012AN	Circuit Breaker 012A	Does not close	1E-3/D	--	3

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ACB012AD	Circuit Breaker 012A	Operator error	1E-3/D	--	10
ACK012AG	Circuit Breaker 012A continuous circuit	No output	2.9E-3	--	↓
ABS010BB	AC RMOV Board 1B	Open circuit	3E-8/hr	7	
ABS010BC	AC RMOV Board 1B	Short to ground	3E-7/hr	7	
ACB012BN	Circuit Breaker 012B	Does not close	1E-3/D	--	3
ACB012BD	Circuit Breaker 012B	Operator error	1E-3/D	--	10
ACK012BG	Circuit Breaker 012B continuous circuit	No output	2.9E-3	--	↓
ABS010CB	AC RMOV Board 1C	Open circuit	3E-8/hr	7	
ABS010CC	AC RMOV Board 1C	Short to ground	3E-7/hr	7	
ACB012CN	Circuit Breaker 012C	Does not close	1E-3/D	--	3

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ACB012CD	Circuit Breaker 012C	Operator error	1E-3/D	--	10
ACK012CG	Circuit Breaker 012C continuous circuit	No output	2.9E-3	--	↓
ABS010DB	AC RMOV Board 1D	Open circuit	3E-8/hr	7	
ABS010DC	AC RMOV Board 1D	Short to ground	3E-7/hr	↓	3
AMG001DW	Motor Generator IDN	Loss of function	1E-5/hr		
AMG002DW	Motor Generator IDA	Loss of function	1E-5/hr	↓	3
ACB012DN	Circuit Breaker 012D	Does not close	1E-3/D	--	10
ACK012DG	Circuit Breaker 012D continuous circuit	No output	2.9E-3	--	↓
ABS010EB	AC RMOV Board 1E	Open circuit	3E-8/hr	7	
ABS010EC	AC RMOV Board 1E	Short to ground	3E-7/hr	7	↓

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
AMG001EW	Motor Generator 1EN	Loss of function	1E-5/hr	7	3
AMG002EW	Motor Generator 1EA	Loss of function	1E-5/hr	7	3
ACB012EN	Circuit Breaker 012E	Does not close	1E-3/D	--	3
ACK012EG	Circuit Breaker 012E continuous circuit	No output	2.9E-3	--	10
BBC0011B	Battery Charger 1	Open circuit	3E-8/hr	7	↓
BBC0011C	Battery Charger 1	Short to ground	3E-7/hr	7	
BBC0011W	Battery Charger 1	Loss of function	3E-6/hr	7	
ACB0511N	Circuit Breaker 0511	Does not close	1E-3/D	--	3
ACK0511D	Circuit Breaker 0511	Operator error	1E-3/D	--	10
BBC002AB	Battery Charger 2A	Open circuit	3E-8/hr	7	10

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
BEC002AC	Battery Charger 2A	Short to ground	3E-7/hr	7	10
BBC002AW	Battery Charger 2A	Loss of function	3E-6/hr	7	10
ACB052AN	Circuit Breaker 052A	Does not close	1E-3/D	--	3
ACB052AD	Circuit Breaker 052A	Operator error	1E-3	--	10
BBC002BB	Battery Charger 2B	Open circuit	3E-8/hr	7	10
BBC002BC	Battery Charger 2B	Short to ground	3E-7/hr	7	10
ACB052BN	Circuit Breaker 052B	Does not close	1E-3/D	--	3
ACB052BD	Circuit Breaker 052B	Operator error	1E-3/D	--	10
BBC002BW	Battery Charger 2B	Loss of function	3E-6/hr	7	10
BBC0013B	Battery Charger 3	Open circuit	3E-8/hr	7	10

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
BBC0013C	Battery Charger 3	Short to ground	3E-7/hr	7	10
ACB0531N	Circuit Breaker 0531	Does not close	1E-3/D	--	3
ACB0531D	Circuit Breaker 0531	Operator error	1E-3/D	--	10
BBC0013W	Battery Charger 3	Loss of function	3E-6/hr	7	↓
BBS0011B	Battery Board 1	Open circuit	3E-8/hr	↓	
BBS0011C	Battery Board 1	Short to ground	3E-7/hr		↓
BBY0011B	Battery 1	Open circuit	3E-8/hr	↓	
BBY0011C	↓	Short to ground	3E-7/hr		↓
BBY0011W		Loss of function	3E-6/hr	3	
EBY0011J		Test	9.6E-3	--	0

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
BCB0231N	Circuit Breaker 0231	Does not close	1E-3/D	--	3
BCB0231D	Circuit Breaker 0231	Operator error	1E-3/D	--	10
BBS0012B	Battery Board 2	Open circuit	3E-8/hr	7	↓
BBS0012C	Battery Board 2	Short to ground	3E-7/hr	↓	
BBY0012B	Battery 2	Open circuit	3E-8/hr		
BBY0012C		Short to ground	3E-7/hr		
BEY0012W		Loss of function	3E-6/hr		
BBY0012J		Test	9.6E-3		--
BCB0232N	Circuit Breaker 0232	Does not close	1E-3/D	--	3
BCB0232D	Circuit Breaker 0232	Operator error	1E-3/D	--	10

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
BBS0013B	Battery Board 3	Open circuit	3E-8/hr	7	10
BBS0013C	Battery Board 3	Short to ground	3E-7/hr	↓	↓
BBY0013B	Battery 3	Open circuit	3E-8/hr		
BBY0013C	↓	Short to ground	3E-7/hr		
BBY0013W		Loss of function	3E-6/hr		
BBY0013J	↓	Test	9.6E-3	--	0
BCE0233N	Circuit Breaker 0233	Does not close	1E-3/D	--	3
BCE0233D	Circuit Breaker 0233	Operator error	1E-3/D	--	10
BBS002AB	DC RMOV Board 1A	Open circuit	3E-8/hr	7	10
BBS002AC	DC RMOV Board 1A	Short to ground	3E-7/hr	7	10

B-345

TABLE B-62. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
BCB032AN	Circuit Breaker 032A	Does not close	1E-3/D	--	3
BCB032AD	Circuit Breaker 032A	Operator error	1E-3/D	--	10
BBS002BB	DC RMOV Board 1B	Open circuit	3E-9/hr	7	10
BBS002BC	DC RMOV Board 1B	Short to ground	3E-7/hr	7	10
BCB032BN	Circuit Breaker 032B	Does not close	1E-3/D	--	3
BCB032BD	Circuit Breaker 032B	Operator error	1E-3/D	--	10
BBS002CB	DC RMOV Board 1C	Open circuit	3E-8/hr	7	10
BBS002CC	DC RMOV Board 1C	Short to ground	3E-7/hr	7	10
BCB032CN	Circuit Breaker 032C	Does not close	1E-3/D	--	3
BCB032CD	Circuit Breaker 032C	Operator error	1E-3/D	--	10

TABLE B-63. EPS FAILURE DATA SUMMARY

Component (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (\bar{A})	Remarks
Bus fault (BS)	Open circuit (B)	0	7	7	3E-8/hr	2.1E-7	Assumed one tenth of bus short rate
Bus fault (BS)	Short (C)	0	7	7	3E-7/hr	2.1E-6	Assumed same as wire rate from Table C-4
Circuit breaker (CB)	Does not close (N)	--	--	--	1E-3/D	1E-3	From Table C-4
Control circuit (CK)	No output (G)	--	--	--	--	2.9E-3	Calculated from generic control circuit model
Diesel generator (DL)	Does not start (R)	--	--	--	3E-2/D	3E-2	From Table C-4
Diesel generator (DL)	Does not run (S)	0	21	8	3E-4/hr	2.4E-3	From Table C-4 (engine only)
Diesel generator (DL)	Loss of function (W)	0	21	8	1E-6/hr	8E-6	Estimate for generator electrical failure rate
DC control power	Does not energize (V)	0	7	7	1E-6/hr	7E-6	From analysis of control power scheme
Diesel generator (DL)	Maintenance (J)	--	--	--	--	2.9E-3	From Table B-61
Diesel generator (DL)	Test (J)	--	--	--	--	3.5E-4	From Table B-60
Loss of offsite power (HOUSELOP)	Offsite power lost	--	--	--	--	1 or 2.7E-5/hr	Used as a house event when $A = 1$; otherwise $\lambda = 2.7E-5/hr$ based on EPRI NP-801 data of 3×10^{-2} per year and 8-hr mission time
Transformer (XT)	Open circuit (B)	0	7	7	1E-6/hr	7E-6	From Table C-4
Transformer (XT)	Short (C)	0	7	7	1E-6/hr	7E-6	From Table C-4
Motor-generator (MG)	Loss of function (W)	0	7	7	1E-5/hr	7E-5	Assumed approximately equal to motor failure rate of Table C-4
Battery charger	Open circuit (B)	0	7	7	3E-8/hr	2.1E-7	Assumed same as bus faults

TABLE B-63. (continued)

Component (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (A)	Remarks
Battery charger	Short (C)	0	7	7	3E-7/hr	2.1E-6	Assumed same as bus faults
Battery charger	Loss of function (W)	0	7	7	3E-6/hr	2.1E-5	From Table C-4
Battery	Open circuit (B)	0	7	7	3E-8/hr	2.1E-7	Assumed same as bus faults
	Short (C)	0	7	7	3E-7/hr	2.1E-6	Assumed same as bus faults
	Loss of function (W)	0	7	7	3E-6/hr	2.1E-5	From Table C-4 solid state device high power application
	Test (J)	--	--	--	--	9.6E-3	From Table B-60
Operator fails to initiate breaker transfer	Operator error (D)	--	--	--	1E-3/D	1E-3	Estimated based on similar actions modeled in other systems

a. If $T_D = 0$, then $T = T_R$ if the mission time (8 hr) $> T_R$. If $T_D = 0$, then $T =$ mission time (8 hr) if mission time $\leq T_R$.

TABLE B-64. EPS CUT SETS
(4160 V Shutdown Board A)(Gate SDA)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
2.1E-6	53.7	ABSO01AC	No
8.2E-7	21.0	HOUSELOP,ADLO01AR	No
5.2E-7	13.5	HOUSELOP,ADLO01AJ	No
2.1E-7	<u>5.3</u>	ABSO01AB	No
Cumulative importance	93.5		

TABLE B-65. EPS CUT SETS
(480 V AC RMOV Board 1A)(Gate AR1A)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
2.1E-6	90.9	ABS010AC	No
2.1E-7	<u>9.1</u>	ABS010AB	No
Cumulative importance	100.0		

TABLE B-66. EPS CUT SETS
(480 V AC RMOV Board 1D)(Gate AR1D)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
2.1E-6	81.3	ABS010DC	No
2.1E-7	8.1	ABS010DB	No
2.0E-7	<u>7.9</u>	ACK012DG,AMGO01DW	No
Cumulative importance	7.3		

TABLE B-67. EPS CUT SETS
(250 V DC RMOV Board 1A)(Gate DR1A)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
2.1E-6	90.9	BBS002AC	No
2.1E-7	<u>9.1</u>	BBS002AB	No
Cumulative importance	100.0		

TABLE B-68. EPS CUT SETS
(Diesel Auxiliary Board A)(Gate DA)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
2.1E-6	87.2	ABS020AC	No
2.1E-7	<u>8.7</u>	ABS020BC	No
Cumulative importance	95.9		

TABLE B-69. EPS CUT SETS
(Shutdown Board A with LOSP)(Gate SDA with LOSP)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
3.0E-2	51.0	ADL001AR	No
1.9E-2	32.6	ADL001AJ	No
2.9E-3	5.0	ACK818AG	No
2.9E-3	<u>5.0</u>	ACK100AG	No
Cumulative importance	93.6		

3.2 Residual Heat Removal Service Water System

3.2.1 Purpose

When the reactor has been shut down, either as the result of a scram or a normal reactor shutdown, a significant amount of heat will still be generated in the reactor vessel. Residual heat in the vessel structural materials and decay heat from fission daughter product decay are the principal sources of this heat. Since there are times when the power conversion system may not be available or cannot be used to remove this heat, another system must be available to perform this function. The RHR system is designed for this purpose. It circulates the reactor coolant or torus water through the RHR heat exchangers to remove the heat from the coolant or torus water. The main function of the RHRSW system is to provide adequate cooling water flow to the RHR heat exchangers, thus providing an adequate heat sink for the coolant or torus water being pumped through the RHR heat exchangers.

A second purpose of the RHRSW system is to provide a supply of water for the EECW system. This system supplies cooling water for various auxiliary systems and for items of equipment that support shutdown operations. The EECW system is discussed in Section 3.3.

Finally, the RHRSW system-to-RHR system cross-connection provides added long-term redundancy to other emergency core cooling and containment cooling methods. This crosstie can provide long-term reactor core cooling and primary containment cooling capability irrespective of primary containment integrity or RHR system operability, so long as a cooling water flow path exists.

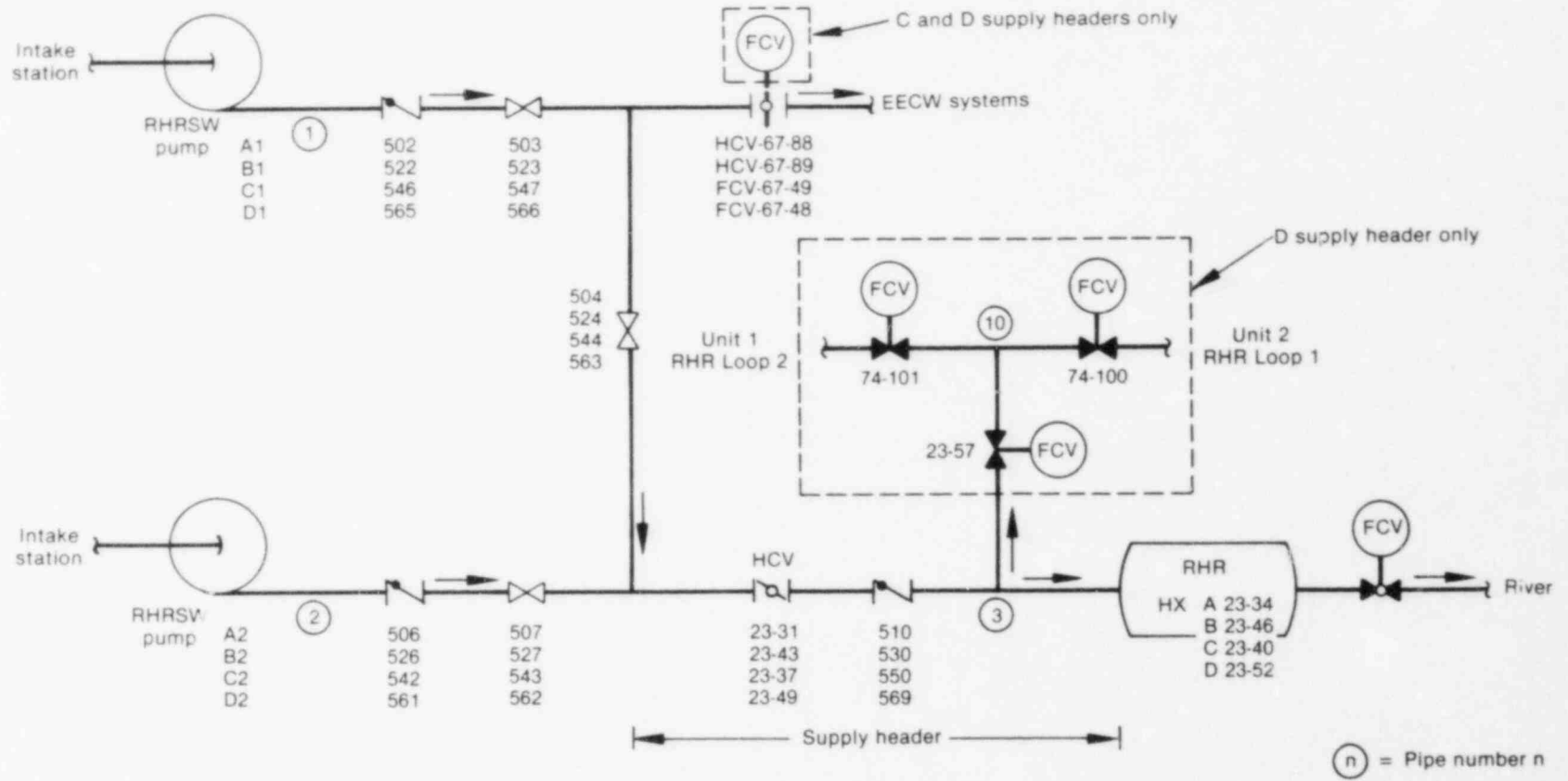
3.2.2 System Configuration

Overall Configuration. The RHRSW system, as considered for this analysis, consists of eight service water pumps, four service water headers, four service water heat exchangers, and the associated piping, valves, controls, and instrumentation.

Figure B-32 is a simplified composite diagram of the RHRSW system. Since the system consists of four nearly symmetric trains, Figure B-32 illustrates only one of the trains. Each train is identified alphabetically by the letters A through D, from top to bottom. The component identification numbers also use a similar convention. That is, for a specific component, the top number represents that component's identification number in Train A, while each successive identification number, downward, represents the component's identification number in Trains B, C, and D, respectively. Where the trains are not symmetric a dashed line is used to bound the asymmetric portion of the train, and an explanation is provided.

There are eight service water pumps associated with the RHRSW system. Four pair of pumps are connected to the four RHRSW headers. Each pair is designed to supply only one header according to the following configuration:

B-352



INEL 2 1584

Figure B-32. RHRSW system.

<u>Pump Pair</u>	<u>Header</u>
A1, A2	A
B1, B2	B
C1, C2	C
D1, D2	D

As Figure B-32 shows, each pump pair supplies only one supply header and, in turn, each supply header supplies only one Unit 1 RHR heat exchanger. Each service water pump has the capacity to supply 100% of the cooling water required by one RHR heat exchanger. No cross-connections exist between service water supply headers, but there is a cross-connection to the EECW system on each train. However, for reasons to be discussed in the following fault tree major assumptions section, this crosstie capability is only considered during EECW recovery considerations. Pumps and headers are shared among Units 1, 2, and 3. However, faults in Units 2 and 3 were not considered for this report.

The D supply header contains piping and valves that cross-connect the RHRSW system with the RHR system. Although it is only used as a last resort, this crosstie provides a method of injecting river water directly into the reactor vessel or primary containment via the RHRSW system and the residual heat removal piping. In the highly unlikely event that all other sources of injection water were unavailable, this source could be used to keep the reactor core covered and the containment cooled. When the RHRSW system is cross-connected to the RHR system in this manner, the resulting configuration is referred to as the SBCS system.

The RHRSW pumps are located at the station intake structure. They are vertical, single stage, turbine-type centrifugal pumps powered by a 400 hp electric motor. Each pump has a capacity of 4500 gpm at a head of 275 feet. The RHRSW pumps are powered from the following 4160 V shutdown boards:

<u>Pump</u>	<u>Shutdown Board</u>
A1	A
A2	A
B1	3EC
B2	C
C1	B
C2	B
D1	3ED
D2	D

The control circuits for the pumps are powered by the following DC control power sources:

<u>Pump</u>	<u>250 V DC Control Shutdown Board for Bus</u>	<u>Basic Event Name in System Fault Tree</u>
A1	A	ADCO01AV
A2	A	ADCO01AV
B1	3EC	ADCO03CV
B2	C	ADCO01CV

<u>Pump</u>	<u>250 V DC Control Shutdown Board for Bus</u>	<u>Basic Event Name in System Fault Tree</u>
C1	B	ADCOOLBV
C2	B	ADCOOLBV
D1	3EC	ADCOO3DV
D2	D	ADCOOLDV

Figure B-33 is a simplified diagram that further illustrates the RHRSW/EECW system power dependencies. The RHR heat exchanger service water outlet valves are powered from the following 480 V RMOV boards:

<u>Supply Header</u>	<u>Valve</u>	<u>480 V RMOV Board</u>
A	FCV-23-34	1A
B	FCV-23-46	1B
C	FCV-23-40	1A
D	FCV-23-52	1B

Support System Interfaces FMEA. The RHR service water system components interface with the 4160 V AC shutdown boards, the 480 V AC RMOV boards, and the 250 V DC control power buses. Component/supporting system interactions are listed in Table B-70.

Instrumentation and Control. The RHRSW system is essentially a manually operated system. However, Pumps A1, B1, C1, and D1 are capable of being crosstied to the EECW system via valves (HCV-67-88 and 89, and FCV-67-49 and 48), respectively. When these valves are open, the corresponding pumps have auto-start capabilities similar to the EECW pumps. But these valves are normally closed, and, as such, the auto-start of Pumps A1, B1, C1, and D1 is not considered in this report.

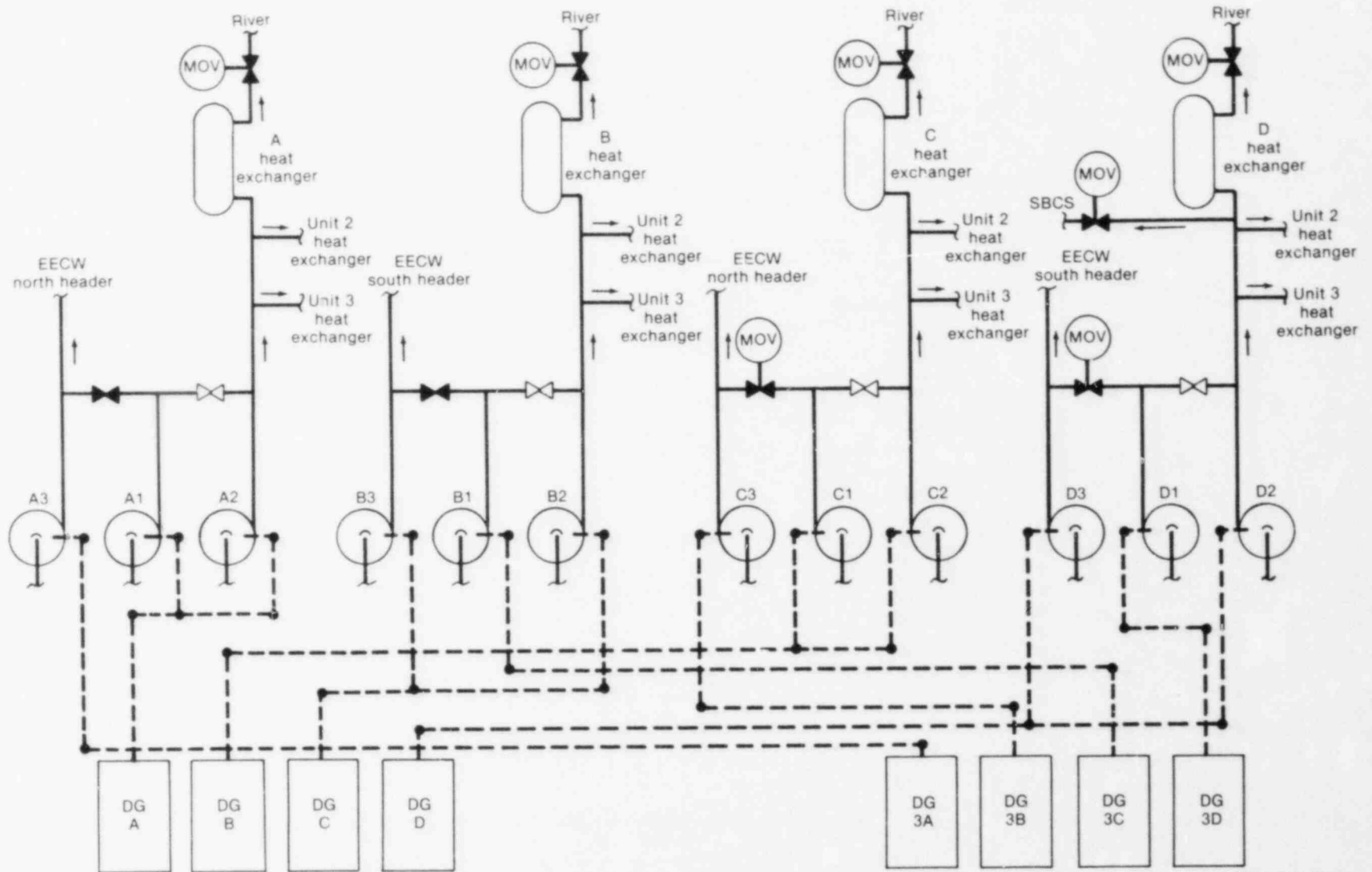
There is an interlock between the RHR heat exchanger service water outlet valves (FCV-23-34, 46, 40, and 52) and their associated pumps. One of the two pumps associated with the header must be running before the heat exchanger outlet valve can be opened. If the valve is open and both pumps are deenergized, the valve will automatically close. This prevents a siphon effect from creating a vacuum in the associated heat exchanger.

Normally, the RHRSW headers will have continuous charging from four RCW system lines located in Unit 2 (one line for each header). The purpose of these charging lines is to keep the RHRSW system charged and vented, thereby, preventing system water hammer on startup. System charging is verified by individual header pressure indicators located in the control room.

In addition, the following instrumentation and controls associated with the RHRSW system are located in the control room:

- RHRSW pump motor current.
- RHRSW pump motor control switches and status lights.

B-355



INEL 2 1585

Figure B-33. RHRSW/EECW systems power dependencies.

TABLE B-70. RHR SW SYSTEM FMEA OF COMPONENT/SUPPORTING-SYSTEM INTERACTIONS

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
Pump A1	4160 V SD-BD-1A	Terminal A10	No power to board	Pump unavailable	Both Pumps A1 and A2 must fail before RHR heat Exchanger A will be unavailable
	250 V DC control power	SD-BD-1A control power bus	No power to board	Breaker will not close; pump will not energize	--
Pump A2	4160 V SD-BD-1A	Terminal A17	-----Same failure modes and effects as Pump A1-----		
	250 V DC control power	SD-BD-1A control power bus			
FCV-23-34	480 V RMOV-1A	Terminal 4D	No power to board; breaker open	Valve will not actuate (open)	FCV-23-34 is the RHR heat Exchanger A service water outlet valve
Pump B1	4160 V SD-BD-3EC	Terminal C8	No power to board	Pump unavailable	Both Pumps B1 and B2 must fail before RHR heat Exchanger B will be unavailable
	250 V DC control power	SD-BD-3EC control power bus	No power to board	Breaker will not close; pump will not energize	--
Pump B2	4160 V SD-BD-1C	Terminal C16	-----Same failure modes and effects as Pump B1-----		
	250 V DC control power	SD-BD-1C control power bus			
FCV-23-46	480 V RMOV-1B	Terminal 14C2	No power to board; breaker open	Valve will not actuate (open)	FCV-23-46 is the RHR heat Exchanger B service water outlet valve
Pump C1	4160 V SD-BD-1B	Terminal B10	No power to board	Pump unavailable	Both Pumps C1 and C2 must fail before RHR heat Exchanger C will be unavailable
	250 V DC control power	SD-BD-1B control power bus	No power to board	Breaker will not close; pump will not energize	--
Pump C2	4160 V SD-BD-1B	Terminal B15	-----Same failure modes and effects as Pump C1-----		
	250 V DC control power	SD-BD-1B control power bus			
FCV-23-40	480 V RMOV-1A	Terminal 5D	No power to board; breaker open	Valve will not actuate (open)	FCV-23-40 is the RHR heat Exchanger C service water outlet valve
Pump D1	4160 V SD-BD-3ED	Terminal D6	No power to board	Pump unavailable	Both Pumps D1 and D2 must fail before RHR heat Exchanger D will be unavailable
	250 V DC control power	SD-BD-3ED control power bus	No power to board	Breaker will not close; pump will not energize	--

B-356

TABLE B-70. (continued)

Component	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
Pump D2	4160 V SD-BD-1D	Terminal D15			-----Same failure modes and effects as Pump D1-----
	250 V DC control power	SD-BD-1D control power bus	No power to board	Breaker will not close; pump will not energize	--
FCV-23-52	480 V RMOV-1B	Terminal 15C	No power to board; breaker open	Valve will not actuate (open)	FCV-23-52 is the RHR heat Exchanger D service water outlet valve
FCV-23-52	480 V RMOV-1B	Terminal 15C	No power to board; breaker open	Valve will not actuate (close)	Will divert some or all service water flow to river instead of RHR system; may allow reactor coolant in RHR system to discharge to river
FCV-23-57	480 V RMOV-1B	Terminal 17C	No power to board; breaker open	Valve will not actuate (open)	No flow to RHR system
FCV-74-101	480 V RMOV-1B	Terminal 19C	No power to board; breaker open	Valve will not actuate (open)	No flow to RHR system

B-357

- RHR heat exchanger service water outlet valve control switches and status lights.
- SBCS valve control switches and status lights.
- RHRSW header low pressure alarms (four) (<50 psig).

Testing. Only two RHRSW system test requirements were identified. These are summarized in Table B-71. Neither test contributes to RHRSW system unavailability, because neither of them degrade the system operability and because of their short outage time.

Maintenance. Upon reviewing the BFI maintenance schedules, only one maintenance act was identified that was assumed to contribute to the overall RHRSW system unavailability: the RHRSW electric motor oil is changed annually. This requires that the associated pump be taken out of service for approximately 4 hours. It was assumed that only one pump is taken out of service, the oil in its motor changed, and then the pump is returned to service before the next pump is taken out of service.

Table B-72 is a summary of the RHRSW system maintenance actions identified as a result of the review mentioned above. When the maintenance act is considered to contribute to RHRSW system unavailability, the act is coded as a basic event and included in the system fault tree. Where applicable, the basic event code associated with the corresponding maintenance act is included in parentheses under the "Maintenance Requirement" column of the table.

Technical Specification Limitations. The following limitations apply to both the RHRSW and the EECW systems. Due to the relatively complicated nature of these specifications with respect to the two system interrelationships, no attempt was made to discriminate between the requirements for the two systems. Again, for the purposes of this analysis, only 8 of the 12 RHRSW pumps were considered for the RHRSW system analysis. The remaining four pumps were considered to be used exclusively for EECW system requirements. Since there is a crosstie capability between the two systems, the following technical specifications, unlike our analysis, includes this capability.

Limiting Conditions for Operation--Prior to reactor startup from a cold condition, nine RHRSW pumps must be operable, with seven pumps (including Pump D1 or D2) assigned to RHRSW service and two auto-start pumps assigned to EECW service.

During power operation, RHRSW pumps must be operable and assigned to service for the time limits specified in Table B-73.

During power operation, both RHRSW Pumps D1 and D2 (normally or alternately assigned to the RHR heat exchanger header supplying the standby coolant supply connection) must be operable. However, one of the D1 or D2 RHRSW pumps may be inoperable for a period not to exceed 30 days, provided the operable pump is aligned to supply the RHR heat exchanger, and the associated diesel generator and the essential control valves are operable.

TABLE B-71. RHRSW SYSTEM TEST REQUIREMENTS SUMMARY

<u>Component Undergoing Test</u>	<u>Type of Test</u>	<u>Test Procedure Number</u>	<u>Components Aligned Away from Engineered Safeguards Position for Test</u>	<u>Expected Test Frequency</u>	<u>Expected Test Outage Time</u>	<u>Remarks</u>
FCV-23-57 FCV-67-48 FCV-67-49	Stroke	SI 4.5.C.1	FCV-23-57	Once every 3 months	90 sec (max) 90 sec (max) 90 sec (max)	Ran three times from each unit; no system degradation will result from running this test
RHRSW system	Pump and header operability and flow test	SI 4.5.C.3	None	Once every 3 months	--	No system degradation will result from running this test

B-359

TABLE B-72. RHRSW SYSTEM MAINTENANCE ACTS SUMMARY

<u>Maintenance Requirement</u>	<u>Instruction</u>	<u>Frequency</u>	<u>Duration</u>	<u>Remarks</u>
Inspect RHRSW pump pit to determine if cleaning is needed	--	Once every 5 years	--	Assumed: does not take system out of service
Change oil in RHRSW pump motor (SMOIL--J)	--	Once every year	4 hr/pump	Assumed: pump out of service only one pump down at a time

TABLE B-73. SERVICE ASSIGNMENTS FOR RHRSW PUMPS

<u>Time Limit (days)</u>	<u>Minimum Service Assignment</u>	
	<u>RHRSW</u>	<u>EECW^a</u>
Indefinite	7 ^b	3 ^b
30	7 ^b or 6 ^c	2 ^b or 3 ^c
7	6 ^b	2 ^b

- a. Only auto-start pumps may be assigned to EECW header service.
- b. At least one operable pump must be assigned to each header.
- c. Nine pumps must be operable. Either configuration is acceptable: 7 and 2, or 6 and 3.

If the above conditions cannot be met, an orderly shutdown of Unit 1 will be initiated, and the unit placed in cold shutdown condition within 24 hours.

Surveillance Requirements--Each of the RHRSW pumps normally assigned to automatic service on the EECW headers will be tested automatically each time the diesel generators are tested. Each of the RHRSW pumps and all associated essential control valves for the EECW headers and RHR heat exchanger headers will be demonstrated to be operable once every three months. Annually each RHRSW pump will be flow-rate tested. To be considered operable, each pump will pump at least 4500 gpm through its normally assigned flow path.

If not more than two RHRSW pumps are inoperable, increased surveillance is not required. When three RHRSW pumps are inoperable, the remaining pumps, associated essential control valves, and associated diesel generators will be operated weekly. When four RHRSW pumps are inoperable, the remaining pumps, associated essential control valves, and associated diesel generators will be operated daily.

When it is determined that one of the RHRSW pumps supplying standby coolant is inoperable at a time when operability is required, the operable RHRSW pump on the same header and its associated diesel generator and the RHR heat exchanger header and associated essential control valves shall be demonstrated to be operable immediately and every 15 days thereafter.

3.2.3 System Operation

The RHRSW system is manually operated. Prior to operation, the operator completes the RHRSW system valve checklist, instrument checklist, and panel checklist. The system is then verified to be charged and vented. This is accomplished by opening the high point vents on top of each RHR heat exchanger. Additional verification of system charging is indicated by header pressure, which is registered on pressure indicators in the control room. After further verification of component power supply availabilities and instrument readiness, the system is ready for startup.

When it is determined by the operator that a RHRSW pump is needed and which one is to be used, the appropriate pump is started. After the pump is running, the service water discharge valve for the associated heat exchanger is opened until the desired flow is reached. Flow is controlled in this manner in order to maintain the desired cooldown rate.

To shut down the RHRSW system, the appropriate heat exchanger service water outlet valve is closed and the associated RHRSW pump is stopped. If the heat exchanger is to be returned to standby condition, the raw water is drained from the heat exchanger, and it is refilled with demineralized water. This is done to inhibit the growth of marine organisms in the heat exchanger, thereby reducing subsequent fouling and plugging problems during system operation.

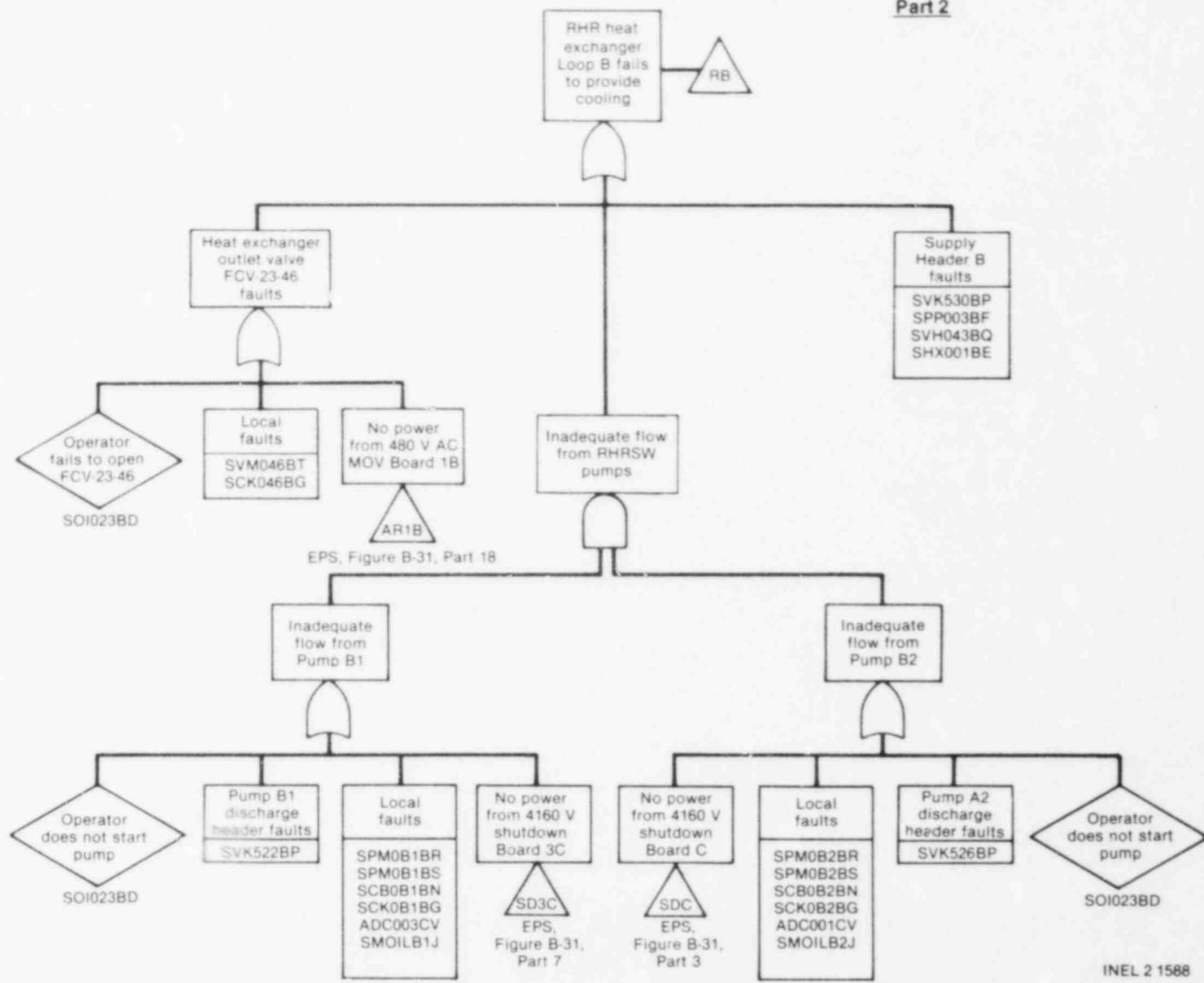
When the system is to be configured for SBCS system operation, the operator must initially verify that one of the two D header pumps, D1 and D2, is running. Then the cross-connect valves (FCV-23-57 and FCV-74-101) are opened and the D heat exchanger outlet valve (FCV-23-52) is closed. This provides a flow path for river water into the RHR system. The RHR system valves are then aligned to direct the flow to the appropriate location.

3.2.4 Fault Tree

Figure B-34 is the RHRSW system fault tree. Since a reduced tree is depicted in Figure B-34, many of the logical OR gates have been combined into one tabulation OR (TAB OR) gate to save space and make the tree easier to comprehend. The TAB OR gates were only used where system fault logic would not be compromised by compressing the appropriate gates and their

B-363

Part 2



INEL 2 1588

Figure B-34. (continued).

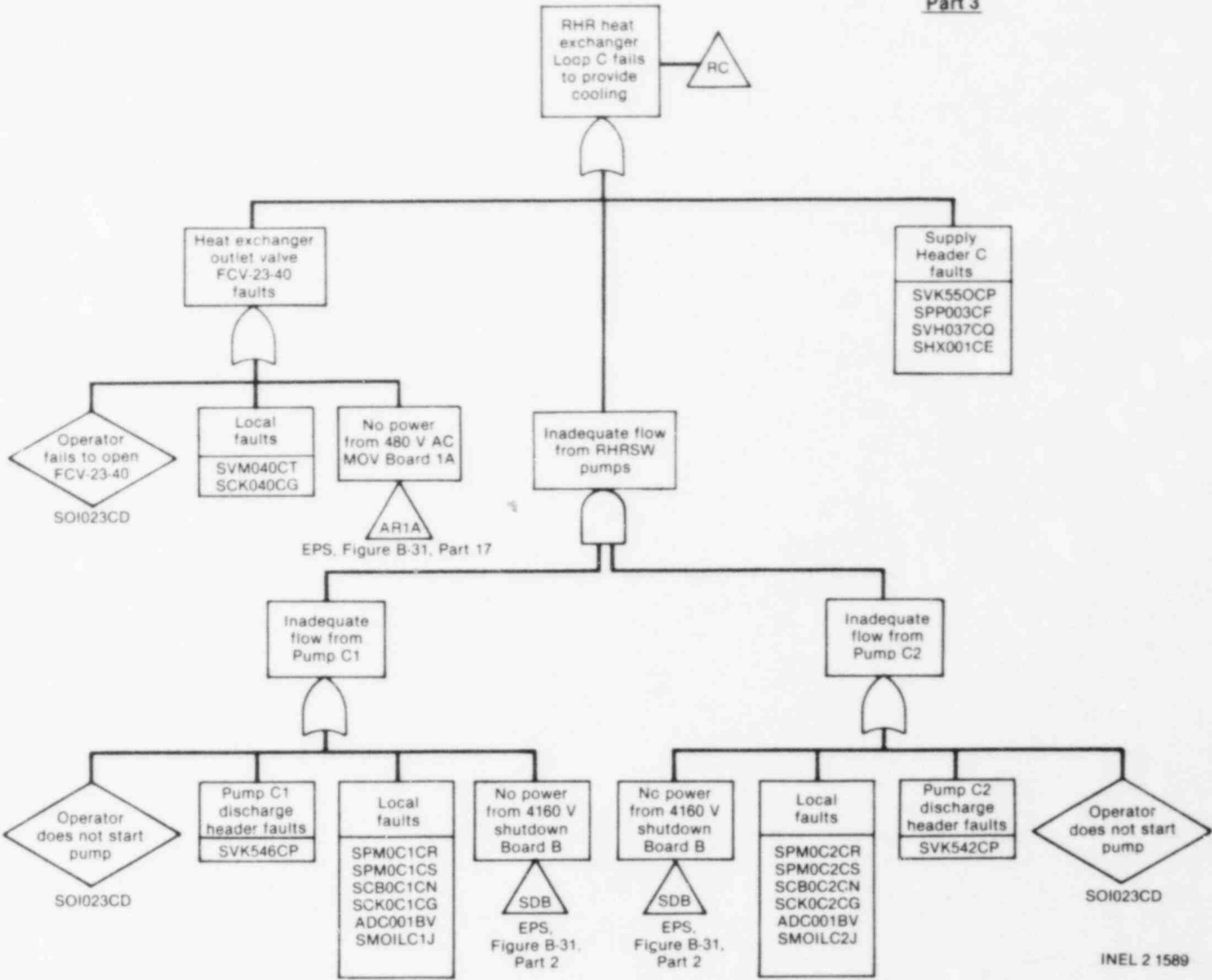
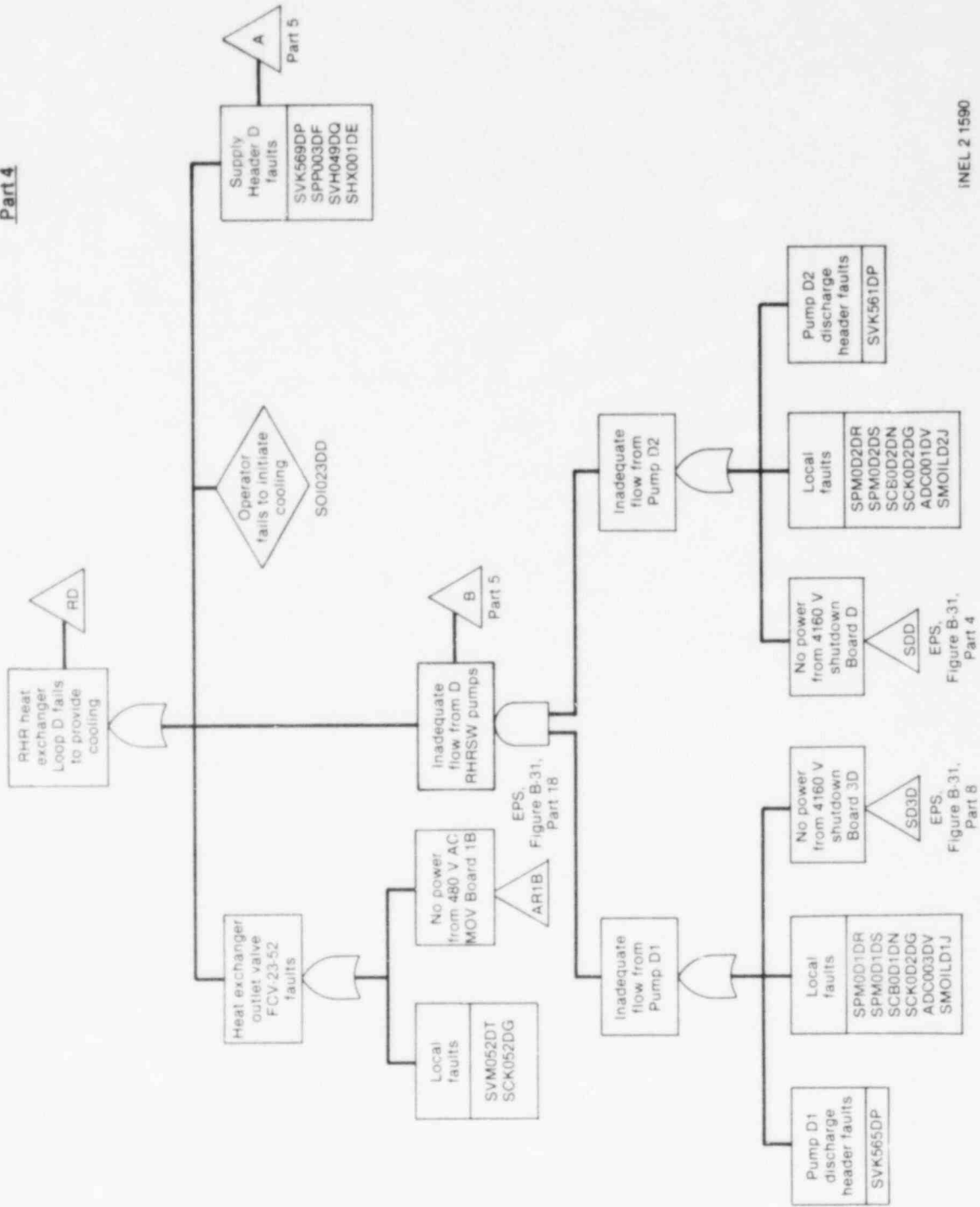


Figure B-34. (continued).

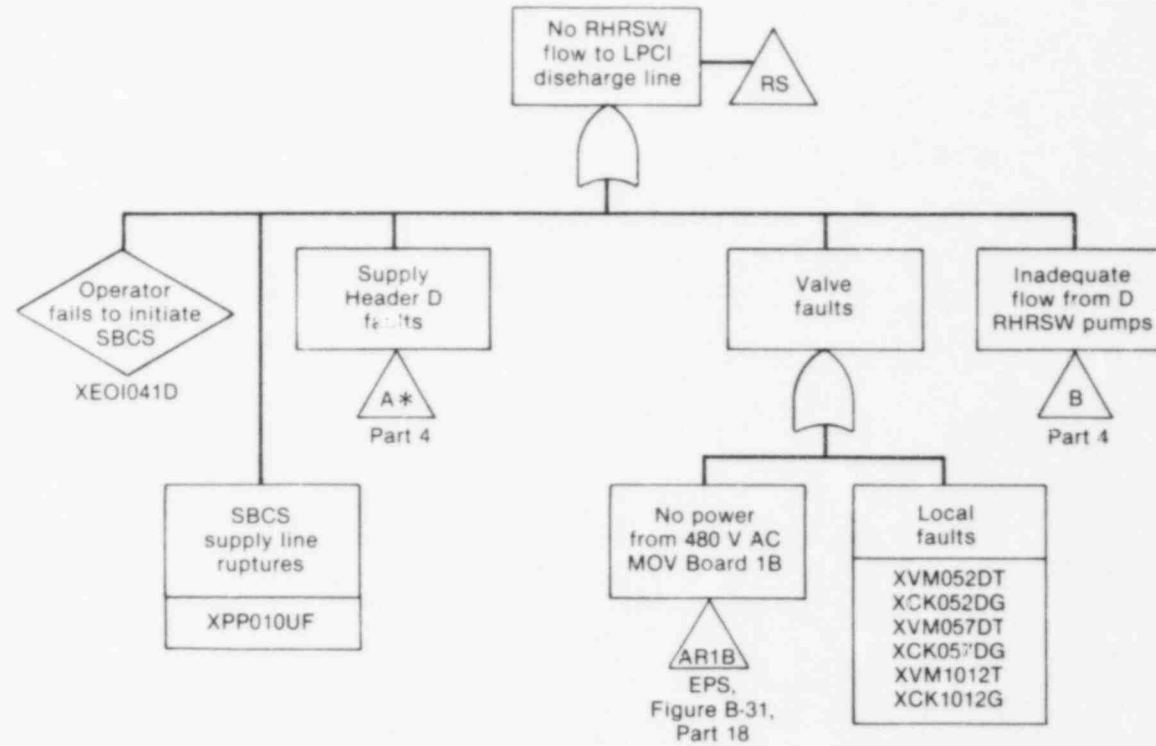
B-364

Part 4



INEL 2 1590

Figure B-34. (continued).



* Does not include fault event SHX001DE for this case.

INEL 2 1591

Figure B-34. (continued).

corresponding basic events into one logic gate. Where this could not be accomplished, no reduction was attempted and the fault logic is fully developed.

Each of the first four parts of the fault tree represents the fault logic associated with each of the four RHRSW headers. Part 1 represents the logic associated with faults in Header A, Part 2 represents fault logic for Header B, and so on. The part of the fault tree shows the fault logic associated with the SBCS.

Since the operator must follow one set of procedures to operate the RHRSW system and a different set of procedures to operate the SBCS system, the event "Operator Fails to Initiate Cooling" (SOIO23DD) was created for the D header logic. This prevents the logical error of including the SBCS tree in the operator response error associated with normal operation (SOIO23DD) with the operator response error associated with SBCS operation (XEOIO41D). This would be the case if the D header tree were constructed similar to the other header trees. Logically, all four header trees are the same although the D header tree looks different.

In light of the major assumptions used to develop the tree, the remaining gates and system logic should be self-explanatory.

Success/Failure Criteria. The top event description in the four header fault trees and in the SBCS fault tree (each of which represents the corresponding system failure definition) is ". . . fails to provide cooling" and "No RHRSW flow . . .," respectively. Either of these top event descriptions is interpreted to mean that failure of the RHRSW system occurs if adequate flow cannot be delivered through the component or system of interest. Adequate flow is defined as the flow delivered by one of the two RHRSW pumps that is available for a specific heat exchanger or, in the case of SBCS, that is available for discharge into the RHR system. In simpler terms, system success is the effective flow of one-out-of-two RHRSW pumps through the system. Any flow that is significantly less than this amount (4500 gpm) is considered to be a RHRSW system failure.

Major Assumptions. The RHRSW system fault tree was constructed based on the following major assumptions:

1. The RHRSW system is initially aligned as shown in Figure B-32. This implies that, to achieve successful RHRSW system operation, the associated RHR heat exchanger service water outlet valve must change state. This is done manually from the control room by the operator. In addition, the operator must start one of the two RHRSW pumps associated with the desired heat exchanger (see Assumption 2).
2. Only one of the two RHRSW pumps needs to operate successfully in order to have adequate service water flow through the associated RHR heat exchanger.
3. For successful SBCS operation, three components must change state. The crosstie valves (FCV-23-57 and FCV-74-101) must open. The

D heat exchanger outlet valve (FCV-23-52) must close. In addition, one of the two D header RHRSW pumps, D1 and D2, must be operating. Flow diversion, which would result if the 3/4-inch crosstie drain line isolation valve failed to close upon SBCS initiation, was considered inadequate to cause SBCS system failure.

4. Since the manually operated cross-connection valves (504, 524, 544, and 563) must be closed and two manually-operated EECW system cross-connection valves (HCV-67-88 and 89) must be opened for successful RHRSW supply to the EECW system, allowance was not made for this capability except where the amount of time for EECW recovery was greater than 1 hour. These valves are located in the intake station, which is a considerable distance from the control room. In addition, these unusual system lineups are only used for maintenance actions and are generally not considered as part of an accident mitigation scheme.
5. Since the operator must verify that the RHRSW system is charged and vented prior to system operation, faults in the RCW system charging supply, which would cause RHRSW system water hammer upon RHRSW system startup, were not considered except for inclusion of the operator response error of failure to follow the appropriate procedure (OI 23) in the fault tree.
6. Detailed information necessary for the analysis of intake station faults was not available for this report. Discussions with TVA personnel concluded that most intake station faults resulted in high intake temperatures for the RHRSW system. This closely resembles an external event--fire, flood, earthquake--and the IREP procedural guidelines dictated that external events should not be considered in our analysis. Therefore, as a result of both of these considerations, intake station faults were not developed in this analysis.
7. Faults in the chemical addition system and with system chemistry are considered to have an insignificant effect on system operation.
8. Pump discharge piping air release valve faults are considered to be insignificant.

Basic Events. The information associated with the various basic events listed in the fault tree is summarized in the RHRSW fault summary short form, Table B-74. In addition, the failure data associated with these basic events is summarized in Table B-75. Table B-76 lists the dominant contributors to RHRSW Train A unavailability. The other trains are similar.

TABLE B-74. RHRSW SYSTEM FAULT SUMMARY SHORT FORM

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
S0I023AD	Operator fails to initiate cooling per 01-23 (Header A)	Operator response error	5.5E-4/D	--	10
SUM034AT	Heat Exchanger A outlet Valve FCV-23-34	Does not operate	1E-3/D	--	3
SCK034AG	FCV-23-34 control circuit	No output	8.8E-3	--	10
SVK510AP	RHR heat Exchanger A inlet check Valve 510	Does not open	1E-4/D	--	3
SPP003AF	Supply Header A	Leakage/rupture	1E-10/hr/section	1104	30
SVK502AP	RHRSW Pump A1 discharge check Valve 502	Does not open	1E-4/D	--	3
SPMOA1AR	RHRSW Pump A1	Does not start	1E-3/D	--	3
SPMOA1AS	RHRSW Pump A1	Does not continue to run	3E-5/hr	37	10
SCB0A1AN	RHRSW Pump A1 circuit breaker	Does not close	1E-3/D	--	3
SCK0A1AG	RHRSW Pump A1 control circuit	No output	8.4E-3	--	10

TABLE B-74. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ADC001AV	RHRSW Pump A1 DC control power (4160 V AC shutdown Board A)	Does not energize	1E-6/hr	8	3
SMOILA1J	RHRSW Pump A1 oil change (motor)	Unavailable due to test or maintenance	5E-4	--	0
SPMOA2AR	RHRSW Pump A2	Does not start	1E-3/D	--	3
SPMOA2AS	RHRSW Pump A2	Does not continue to run	3E-5/hr	37	10
SCBOA2AN	RHRSW Pump A2 circuit breaker	Does not close	1E-3/D	--	3
SCKOA2AG	RHRSW Pump A2 control circuit	No output	8.4E-3	--	10
SMOILA2J	RHRSW Pump A2 motor oil change	Unavailable due to test or maintenance	5E-4	--	0
SVK506AP	RHRSW Pump A2 discharge check Valve 506	Does not open	1E-4/D	--	3

TABLE B-74. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
SO1023BD	Operator fails to initiate cooling per 01-23 (Header B)	Operator response error	5.5E-4/D	--	10
SVM046BT	Heat Exchanger B outlet Valve FCV-23-46	Does not operate	1E-3/D	--	3
SCK046BG	FCV-23-46 control circuit	No output	8.8E-3	--	10
SVK530BP	RHR heat Exchanger B inlet check Valve 530	Does not open	1E-4/D	--	3
SPP003BF	Supply Header B	Leakage/rupture	1E-10/hr/section	1104	30
SVK522BP	RHR SW Pump B1 discharge check Valve 522	Does not open	1E-4/D	--	3
SPMOB1BR	RHR SW Pump B1	Does not start	1E-3/D	--	3
SPMOB1BS	RHR SW Pump B1	Does not continue to run	3E-5/hr	37	10
SCBOB1BN	RHR SW Pump B1 circuit breaker	Does not close	1E-3/D	--	3
SCKOB1BG	RHR SW Pump B1 control circuit	No output	8.4E-3	--	10

TABLE B-74, (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ADC003CV	RHRWS Pump B1 DC control power (4160 V AC shutdown Board 3EC)	Does not energize	1E-6/hr	8	3
SMOILB1J	RHRWS Pump B1 oil change (motor)	Unavailable due to test or maintenance	5E-4	--	0
SPMOB2BR	RHRWS Pump B2	Does not start	1E-3/D	--	3
SPMOB2BS	RHRWS Pump B2	Does not continue to run	3E-5/hr	37	10
SCB0B2BN	RHRWS Pump B2 circuit breaker	Does not close	1E-3/D	--	3
SCK0B2BC	RHRWS Pump B2 control circuit	No output	8.4E-3	--	10
ADC001CV	RHRWS Pump B2 DC control power (4160 V AC shutdown Board C)	Does not energize	1E-6/hr	8	3
SMOILB2J	RHRWS Pump B2 oil change (motor)	Unavailable due to test or maintenance	5E-4	--	0

TABLE B-74. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
SVK526BP	RHR SW Pump B2 discharge check Valve 526	Does not open	1E-4/D	--	3
S0I023CD	Operator fails to initiate cooling per 01-23 (Header C)	Operator response error	5.5E-4/D	--	10
SVM040CT	Heat Exchanger C outlet Valve FCV-23-40	Does not operate	1E-3/D	--	3
SCK040CG	FCV-23-40 control circuit	No output	8.8E-3	--	10
SVK550CP	RHR heat Exchanger C inlet check Valve 550	Does not open	1E-4/D	--	3
SPP003CF	Supply Header C	Leakage/rupture	1E-10/hr/section	1104	30
SVK546CP	RHR SW Pump C1 discharge check Valve 546	Does not open	1E-4/D	--	3
SPMOC1CR	RHR SW Pump C1	Does not start	1E-3/D	--	3
SPMOC1CS	RHR SW Pump C1	Does not continue to run	3E-5/hr	37	10
SCBOC1CN	RHR SW Pump C1 circuit breaker	Does not close	1E-3/D	--	3

TABLE B-74. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
SCK0C1CG	RHRSW Pump C1 control circuit	No output	8.4E-3	--	10
ADC001BV	RHRSW Pump C1 DC control power (4160 V AC shutdown Board B)	Does not energize	1E-6/hr	8	3
SM0ILC1J	RHRSW Pump C1 oil change (motor)	Unavailable due to test or maintenance	5E-4	--	0
SPM0C2CR	RHRSW Pump C2	Does not start	1E-3/D	--	3
SPM0C2CS	RHRSW Pump C2	Does not continue to run	3E-5/hr	37	10
SCB0C2CN	RHRSW Pump C2 circuit breaker	Does not close	1E-3/D	--	3
SCK0C2CG	RHRSW Pump C2 control circuit	No output	8.4E-3	--	10
SM0ILC2J	RHRSW Pump C2 oil change (motor)	Unavailable due to test or maintenance	5E-4	--	0
SVK542CP	RHRSW Pump C2 discharge check Valve 542	Does not open	1E-4/D	--	3

TABLE B-74. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
S01023DD	Operator fails to initiate cooling per OI-23 (Header D)	Operator response error	5.5E-4/D	--	10
SVM052DT	Heat Exchanger D outlet Valve FCV-23-52	Does not operate	1E-3/D	--	3
SCK052DG	FCV-23-52 control circuit	No output	8.8E-3	--	10
SVK569DP	RHR heat Exchanger D inlet check Valve 569	Does not open	1E-4/D	--	3
SPP003DF	Supply Header D	Leakage/rupture	1E-10/hr/section	1104	30
SVK565DP	RHR SW Pump D1 discharge check Valve 565	Does not open	1E-4/D	--	3
SPMOD1DR	RHR SW Pump D1	Does not start	1E-3/D	--	3
SPMOD1DS	RHR SW Pump D1	Does not continue to run	3E-5/hr	37	10
SCB0D1DN	RHR SW Pump D1 circuit breaker	Does not close	1E-3/D	--	3
SCK0D1DG	RHR SW Pump D1 control circuit	No output	8.4E-3	--	10

TABLE B-74. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
ADC003DV	RHRSW Pump D1 DC control power (4160 V AC shutdown Board 3ED)	Does not energize	1E-6/hr	8	3
SMOILD1J	RHRSW Pump D1 oil change (motor)	Unavailable due to test or maintenance	5E-4	--	0
SPMOD2DR	RHRSW Pump D2	Does not start	1E-3/D	--	3
SPMOD2DS	RHRSW Pump D2	Does not continue to run	3E-5/hr	37	10
SCBOD2DN	RHRSW Pump D2 circuit breaker	Does not close	1E-3/D	--	3
SCKOD2DG	RHRSW Pump D2 control circuit	No output	8.4E-3	--	10
ADC001DV	RHRSW Pump D2 DC control power (4160 V AC shutdown Board D)	Does not energize	1E-6/hr	8	3
SMOILD2J	RHRSW Pump D2 oil change (motor)	Unavailable due to test or maintenance	5E-4	--	0

TABLE B-74. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
SVK561DP	RHR SW Pump D2 discharge check Valve 561	Does not open	1E-4/D	--	3
XEO1041D	Operator fails to initiate SBCS per OI-41	Operator response error	8E-3/D	--	10
XPP010UF	SBCS piping	Leakage/rupture	1E-10/hr/section	1104	10
XVM052DT	RHR heat Exchanger D outlet Valve FCV-23-52	Does not operate	1E-3/D	--	3
XCK052DG	FCV-23-52 control circuit	No output	8.8E-3	--	10
XVM057DT	SBCS Valve FCV-23-57	Does not operate	1E-3/D	--	3
XCK057DG	FCV-23-57 control circuit	No output	8.8E-3	--	10
XVM1012T	Unit 1 RHR cross-connect Valve FCV-74-101	Does not operate	1E-3/D	--	3
XVM1012G	FCV-74-101 control circuit	No output	8.8E-3	--	10
SVH031AQ	Manual Valve 23-31	Does not remain open	1E-4/D	--	3

TABLE B-74. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
SVH043BQ	Manual Valve 23-43	Does not remain open	1E-4/D	--	3
SVH037CQ	Manual Valve 23-37	Does not remain open	1E-4/D	--	3
SVH049DQ	Manual Valve 23-49	Does not remain open	1E-4/D	--	3
SHX001AE	RHR heat Exchanger A	Plugged	1E-6/hr	384	10
SHX001BE	RHR heat Exchanger B	↓	↓	↓	↓
SHX001CE	RHR heat Exchanger C				
SHX001DE	RHR heat Exchanger D				

B-378

TABLE B-75. RHRSW SYSTEM FAILURE DATA SUMMARY

Component/Activity (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (A)	Remarks
Circuit breaker (CB)	Does not close (N)	--	--	--	1E-3/D	1E-3	--
Motor-driven pump control circuit (CK)	No output (G)	1080 hr	7 hr	1087 hr	7.6E-6/hr + 1E-4/D	8.4E-3	$\bar{A} = 1E-4 + 7.6E-6T$ T_R --WASH-1400, Table III 5-2 T_D = half test interval; based on pump operability test and stroke time test, once every 3 months
Motor-operated valve control circuit (CK)	No output (G)	1080 hr	7 hr	1087 hr	7.7E-6/hr + 4.1E-4/D	8.8E-3	$\bar{A} = 4.1E-4 + 7.7E-6T$ T_R --WASH-1400, Table III 5-2 T_D = half test interval; based on pump operability test and stroke time test, once every 3 months
Motor-driven pump (PM)	Does not start (R)	--	--	--	1E-3/D	1E-3	--
Motor-driven pump (PM)	Does not run (S)	0 hr	37 hr	8 hr	3E-5/hr	2.4E-4	T_R --WASH-1400, Table III 5-2
Pipe (PP)	Leakage/ rupture (F)	1080 hr	24 hr	1104 hr	1E-10/hr	1.1E-7	T_R = 24 hr, assumed time to shut down plant T_D = based on pump operability test, once every 3 months
Check valve (VK)	Does not open (P)	--	--	--	1E-4/D	1E-4	--
Motor-operated valve (VM)	Does not operate (T)	--	--	--	1E-3/D	1E-3	--
Pump DC control	Does not energize (V)	0	7 hr	7 hr	1E-6/hr	7E-6	γ --developed by analysis T_R --WASH 1400, Table III 5-2
Operator does not follow normal operating procedure (S01023-D)	Operator response error (D)	--	--	--	5.5E-4/D	5.5E-4	A--used plant-specific human error model
Change oil in RHRSW pump motor (SMOIL--J)	Unavailability due to test or maintenance (J)	--	--	--	--	5E-4	Performed once every year; duration, 4 hr

B-379

TABLE B-75. (continued)

Component/Activity (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (\bar{A})	Remarks
Operator does not follow emergency operating procedure (XE01041D)	Operator response error (D)	--	--	--	--	8E-3	^A --used plant-specific human error model
Normally open manual valve (SVH__Q)	Does not remain open (Q)	--	--	--	1E-4/D	1E-4	One valve per loop that can disable entire loop
Heat exchanger (SHX__Q)	Plugged (Q)	360 hr	24 hr	384 hr	1E-6/hr	3.8E-4	Estimated failure and repair rates

a. If $T_D = 0$, then $T = T_R$ if the mission time (8 hr) $> T_R$. If $T_D = 0$, then $T =$ mission time (8 hr) if mission time $\leq T_R$.

TABLE B-76. RHRSW SYSTEM CUT SETS
(RHRSW Header A)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
8.8E-3	83.1	SCK034AG	Yes
1.0E-3	9.4	SVM034AT	No
Cumulative Importance	92.5		

3.3 Emergency Equipment Cooling Water System

The EECW system provides both direct and indirect cooling to safety-related components in systems that are required to operate when a transient or accident has occurred. In addition, the EECW serves as a backup supply to the RCW system.

Under a LOSP condition, failure of EECW could result in a station blackout at all three units. However, adequate time is available for EECW recovery considerations.

3.3.1 Purpose

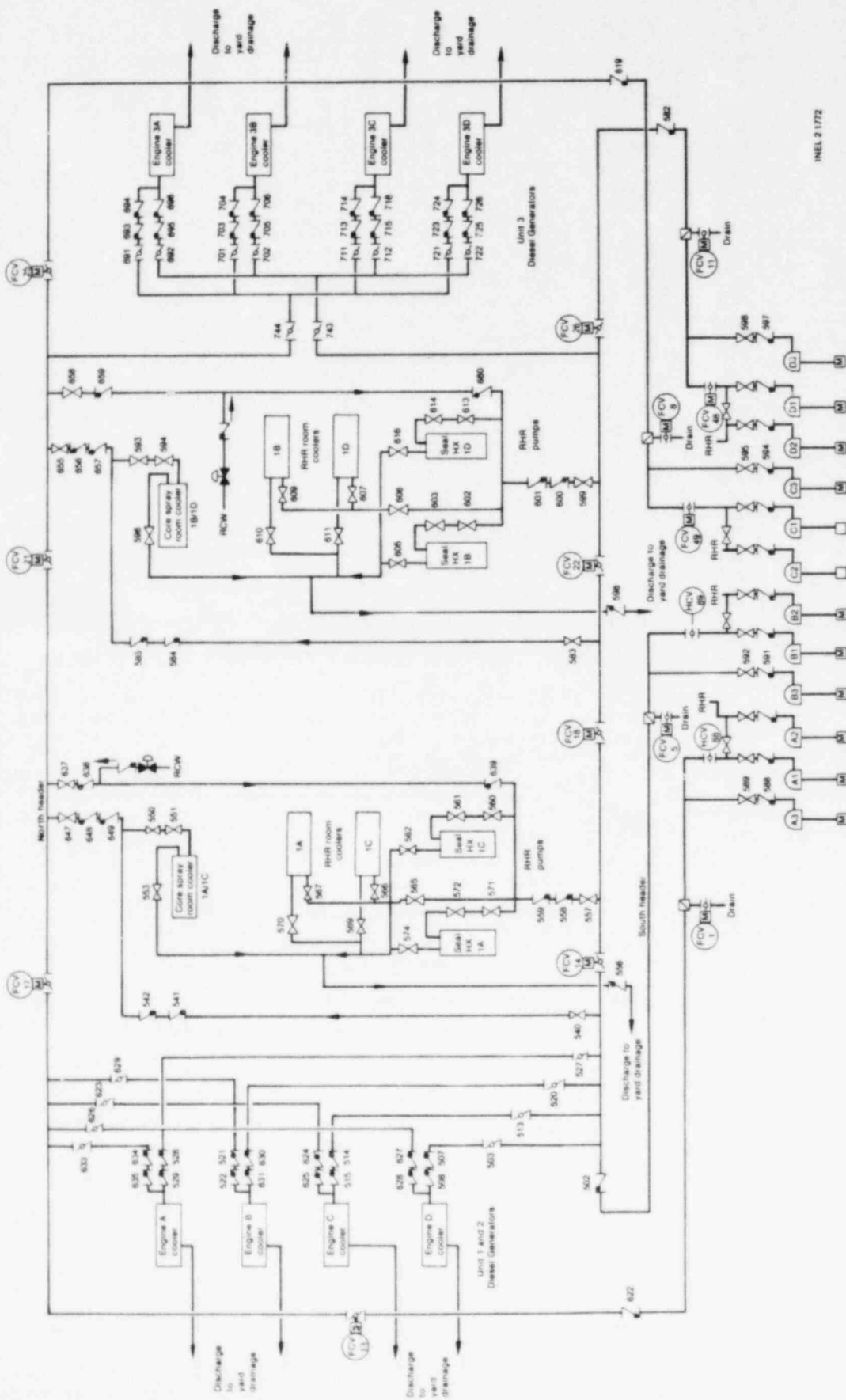
The purpose of the EECW is to supply cooling water to safety-related components in the core spray, RHR, and diesel generator systems. The EECW performs this function by supplying water from the intake station to heat exchangers in the previously mentioned safety systems. This cooling water then flows through the heat exchangers and discharges back to Wheeler Reservoir through yard drainage.

3.3.2 System Configuration

Overall Configuration. A simplified diagram of the EECW is provided by Figure B-35. The EECW is a Class I safety-related system that serves all three of the Browns Ferry units. Either of two independent piping headers (north and south headers) can supply the safety-related cooling loads. The EECW system uses 4 of the 12 RHRSW pumps to supply the 2 EECW headers (2 pumps per header) according to the following configuration:

<u>Header</u>	<u>Pump Pair</u>
North	A3, C3
South	B3, D3

The remaining eight pumps serve the RHRSW system. Four of these eight pumps may be valved into the EECW system if needed; however, the RHRSW is considered to be a separate support system.



INEL 2 1772

Figure B-35. EECW system.

Maximum design flow for each unit required approximately 3300 gpm, which includes 1500 gpm for nonsafety-related backup loads, such as reactor building closed cooling water heat exchangers, control and station service air compressors, and control room air conditioners. Under worst case conditions, such as exist following a LOSP transient, maximum design flow rates are required at all three units, resulting in total station flow requirement of 9900 gpm. Since each pump is designed to deliver approximately 4500 gpm, three of four pumps assigned to EECW are necessary to supply the EECW system design requirements.

Each EECW supply header from the intake station has a continuous self-cleaning strainer with a screen size of 1/8 inch to prevent clogging of the various coolers. The strainer automatically starts its cleaning cycle whenever its associated pump is started. Other than starting the pumps and strainers and opening check valves, no dynamic devices are required to operate the system.

System Interfaces. The EECW system provides cooling to the RHR pump seal heat exchangers, RHR room coolers, and diesel generator engine coolers. The EECW system also provides cooling to the core spray room coolers, although subsequent testing by General Electric has shown that the core spray pumps can run for up to 2 hours without room cooling. Thus, due to the relatively short period of time required for low pressure core spray injection (approximately 10 min), loss of core spray room cooling is not considered significant for this analysis.

The EECW pumps receive electrical power from the following 4160 V shutdown boards:

<u>Pump Pair</u>	<u>4160 V Shutdown Board</u>
A3, C3	3EA, 3EB (Unit 3)
B3, D3	C, D (Units 1 and 2)

The EECW also serves as a backup supply to nonsafety-related components normally cooled by the RCW system to increase plant availability. The EECW support system FMEA is shown as Table B-77.

Instrumentation and Control. The EECW system is normally in standby readiness with the A3, B3, C3, and D3 RHRSW pumps aligned to EECW service and "off." The RHRSW pumps aligned to EECW will automatically start on:

1. Low RCW header pressure.
2. Any time a diesel generator or core spray pump is started:
 - a. The two RHRSW pumps (B3 and D3) aligned to EECW and powered from shutdown boards in Units 1 and 2 will start automatically in less than 30 sec after starting of a diesel generator or core spray pump in Unit 1 or 2.
 - b. The two RHRSW pumps (A3 and C3) aligned to EECW and powered from shutdown boards in Unit 3 will start automatically in less than 30 sec after starting of a diesel generator or core spray pump in Unit 3.

TABLE B-77. EECW SYSTEM FMEA OF COMPONENT/SUPPORTING-SYSTEM INTERACTIONS

Components	Supporting System	Interface	Failure Mode of Support System	Local Effects on Front-Line System	Remarks
RHRSW Pump A3	4160 V SD-BD-3EA	Terminal 5	No power to board	Pump unavailable	--
	Battery Board 1	Control circuit	Board dead	Breaker will not close to energize pump	Battery Board 2 is alternate supply of control power
	Manual control	HS-23-85A	--	--	--
RHRSW Pump A1	- - - - - This pump is available for EECW service if manually realigned; FMEA for Pump A1 is found in RHRSW system- - - - -				
RHRSW Pump B3	4160 V SD-BD-C	Terminal 8	No power to board	Pump unavailable	--
	Battery Board 3	Control circuit	Board dead	Breaker will not close to energize pump	Battery Board 1 is alternate supply of control power
	Manual control	HS-23-15A	--	--	--
RHRSW Pump B1	- - - - - This pump is available for EECW service if manually realigned; FMEA for Pump B1 is found in RHRSW system- - - - -				
RHRSW Pump C3	4160 V SD-BD-3EB	Terminal 10	No power to board	Pump unavailable	--
	480 V diesel auxiliary Board 3A (through battery Charger 3B)	Control circuit	Board dead	Breaker will not close to energize pump	Battery Board 3 is alternate supply of control power
	Manual control	HS-23-31A	--	--	--
RHRSW Pump C1	- - - - - This pump is available for EECW service if manually realigned; FMEA for Pump C1 is found in RHRSW system- - - - -				
RHRSW Pump D3	4160 V SD-BD-D	Terminal 6	No power to board	Pump unavailable	--
	Battery Board 2	Control circuit	Board dead	Breaker will not close to energize pump	Battery Board 3 is alternate supply of control power
	Manual control	HS-23-23A	--	--	--
RHRSW Pump D1	- - - - - This pump is available for EECW service if manually realigned; FMEA for Pump D1 is found in RHRSW system- - - - -				
FCV-67-49	480 V diesel auxiliary Board-A	Terminal 12C	No power to board	Valve inoperable	Header supply valve from alternate pump
	Manual control	HS-67-49A	--	--	--
FCV-67-48	480 V diesel auxiliary Board-B	Terminal 12C	No power to board	Valve inoperable	Header supply valve from alternate pump
	Manual control	HS-67-48	--	--	--

B-384

TABLE B-77. (continued)

<u>Components</u>	<u>Supporting System</u>	<u>Interface</u>	<u>Failure Mode of Support System</u>	<u>Local Effects on Front-Line System</u>	<u>Remarks</u>
FCV-67-51	Control air system	FSV-67-51	--	Normally open flow control valve	--
FCV-67-14	480 V diesel auxiliary Board-B	Terminal 12E	No power on board	Normally open desectionalizing valve	Inability to isolate Unit 1 from other units
FCV-67-13	480 V diesel auxiliary Board-A	Terminal 12E	No power on board	Normally open desectionalizing valve	Inability to isolate Unit 1 from other units
FCV-67-18	480 V RMOV-1B	Terminal 14A	No power on board	Normally open desectionalizing valve	Inability to isolate Unit 1 from other units

3. ECCS initiation signals of high drywell pressure (+2 psig) or low-low-low reactor vessel water level (-143.5 inches) in any unit (part of the core spray initiation logic).

Figure B-36 is a simplified diagram of the EECW auto-initiation circuitry for the B3 pump. The circuits are similar for each of the four pumps.

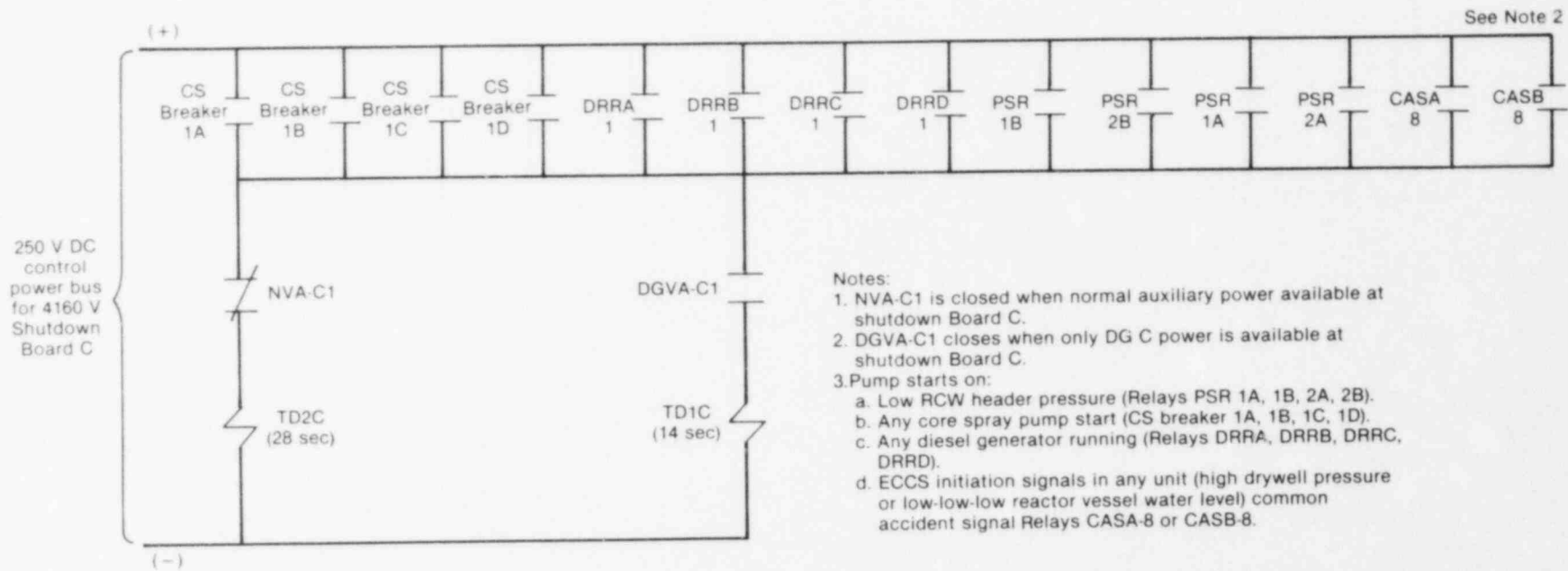
As discussed above and as shown by Figure B-36, any of the multiple contacts can initiate a pump start. Time delay relay contacts close in the pump control circuit in 28 sec if normal power is available or in 14 sec if only diesel generator power is available.

The self-cleaning strainers in the supply headers automatically start their cleaning cycle on pressure differential switch signals indicating that the pump aligned to that supply header has been started.

Testing. Surveillance of the EECW system is provided under the guidelines of SI 4.5.C. Essentially, a functional test of the EECW is performed each time the diesel generators are tested, which is at least monthly as required by SI 4.9.A.1.a. As noted in the previous section, "Instrumentation and Control," two EECW pumps start automatically after starting of a diesel generator in Unit 1 or 2, and, similarly, two EECW pumps start when a diesel generator is started in Unit 3. Thus, operability of the EECW start circuitry, pumps, backwash strainers, and check valves, and status of valve positioning is ensured monthly. The EECW system test requirements are summarized in Table B-78. This detection time interval is also reflected in Table B-79.

Maintenance. EECW system components are maintained following surveillance testing for those components that are found to be in a failed state. Plant maintenance personnel indicate that equipment is generally not taken out of service on a routine basis unless known or suspected to be inoperable. Thus, unavailability of the EECW system due to maintenance acts falls into two categories: (a) unavailability due to repair following detection of the failure, and (b) unavailability of system components due to scheduled preventative maintenance.

For maintenance acts of the first category, data was taken from WASH-1400, Table III 5-2, "Summary of Major Maintenance Act Duration" for pumps, valves, diesels, and instrumentation. The plant electrical and mechanical maintenance schedules were consulted to identify those preventative maintenance actions that render portions of the EECW unavailable until completion of the procedure. Upon reviewing the BFI maintenance schedules, only two maintenance acts were identified that were assumed to contribute to the overall EECW system unavailability: the EECW electric motor oil is changed annually, and once every 2 years the EECW header strainers are disassembled, cleaned, and lubricated. The annual oil change requires that the associated pump be taken out of service for approximately 4 hours. It is assumed that only one pump is taken out of service, the oil in the motor changed, and then the pump is returned to service before the next pump is taken out of service. During service of the EECW header strainer, each strainer and, therefore, the associated header path, are unavailable for 12 hours.



B-387

INEL 2 1586

Figure B-36. EECW auto-initiation logic for B3 pump.

TABLE B-78. EECW SYSTEM TEST REQUIREMENTS SUMMARY

Component Undergoing Test	Type of Test	Test Procedure Number	Components Aligned Away from Engineered Safeguards Position for Test	Expected Test Frequency	Expected Test Outage Time	Remarks
FCV-67-14 FCV-67-18 FCV-67-22 FCV-67-26 FCV-67-13 FCV-67-17 FCV-67-21 FCV-67-25	Stroke	SI 4.5.C.1	None	Once every 3 months	90 sec (max)	Tests capability of sectionalizing off headers, no system degradation will result from running this test
EECW system	Pump and header operability and flow test	SI 4.5.C.2	None	Once every 3 months	--	No system degradation will result from running this test
	Diesel generator auto-start	SI 4.9.A.1.a	None	Once every month	--	The EECW will automatically start and run each time the diesel generators are tested

B-388

TABLE B-79. EECW SYSTEM FAILURE DATA SUMMARY

Component/Activity (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (\bar{A})	Remarks
Circuit breaker (CB)	Does not close (N)	--	--	--	1E-3/D	1E-3	--
Motor-driven pump control circuit (CK)	No output (G)	360 hr	7 hr	367 hr	7.6 E-6/hr + 1E-4/D	2.9E-3	$\bar{A} = 1E-4 + 7.6E-6T$ T_R --WASH-1400, Table III 5-2 T_D = half test interval; based on pump operability test and stroke time test, once every month
Motor-operated valve control circuit (CK)	No output (G)	360 hr	7 hr	367 hr	7.7E-6/hr 4.1E-4	3.2 E-3	-- $A = 4.1E-4 + 7.7E-6T$ T_R --WASH-1400, Table III 5-2 T_D = half test interval; based on pump operability test and stroke time test, once every month
Motor-driven pump (PM)	Does not start (R)	--	--	--	1E-3/D	1E-3	--
Motor-driven pump (PM)	Does not run (S)	0 hr	37 hr	8 hr	3E-5/hr	2.4E-4	8 hr mission time based on time to hot shutdown
Pipe (PP)	Leakage/ rupture (F)	360 hr	24 hr	384 hr	1E-10/hr/ section	3.8E-8	$T_R = 24$ hr, assumed time to cold shutdown T_D --based on pump operability test, once every month
Check valve (VK)	Does not open (P)	--	--	--	1E-4/D	1E-4	--
Manual valve (VH)	Does not remain open (Q)	--	--	--	1E-4/D	1E-4	--
Motor-operated valve (VM)	Does not open (P)	--	--	--	1E-3/D	1E-3	--
Pump DC control power (ADCOO--V)	Does not energize (V)	0	7 hr	7 hr	1E-6/hr	7E-6	λ --developed by analysis T_R --WASH-1400, Table III 5-2
Strainer (FL)	Plugged (E)	360 hr	24 hr	384 hr	1E-6/hr	3.8E-4	Estimated failure and repair rates

B-389

TABLE B-79. (continued)

Component/Activity (Code)	Failure Mode (Code)	Time to Detect (T_D)	Time to Repair (T_R)	Fault Duration Time ^a ($T = T_D + T_R$)	Failure Probability	Unavailability (A)	Remarks
Heat exchanger (HX)	Plugged (E)	360 hr	24 hr	384 hr	1E-6/hr	3.8E-4	Estimated failure and repair rates
Relay (RE)	Does not energize (V)	--	--	--	--	1E-4	--
Contacts (CO)	Open (O)	360 hr	7 hr	367 hr	1E-7/hr	3.7E-5	--
Instrumentation (IN)	Erroneous output (I)	360 hr	7 hr	367 hr	1E-6/hr	3.7E-4	--
Pump maintenance (KPMO__J)	Unavailable due to test or maintenance (J)	--	--	--	--	5E-4	Input data to estimate \bar{A} from Table B-80
Strainer maintenance (KFLO__J)	--	--	--	--	--	7E-4	Input data to estimate \bar{A} from Table B-80

a. If $T_D = 0$, then $T = T_R$ if the mission time (8 hr) $> T_R$. If $T_D = 0$, then $T =$ mission time (8 hr) if mission time $\leq T_R$.

Table B-80 is a summary of the EECW system maintenance acts identified as a result of the review mentioned above. When the maintenance act is considered to contribute to EECW system unavailability, the act is coded as a basic event and included in the system fault tree. Where applicable, the basic event code associated with the corresponding maintenance act is included in parentheses under the "Maintenance Requirement" column of the table.

TABLE B-80. EECW SYSTEM MAINTENANCE ACTS SUMMARY

<u>Maintenance Requirement</u>	<u>Instruction</u>	<u>Frequency</u>	<u>Duration</u>	<u>Remarks</u>
Disassemble and maintain EECW header strainers (KFLO ___ J)	--	Once every 2 years	12 hr/strainer	Header path out of service
Change oil in RHRSW pump motor (KPMO ___ J)	--	Once every year	4 hr/pump	Assumed: pump out of service; only one pump down at a time

Browns Ferry maintenance and testing procedures require operability of components to be demonstrated when returning equipment to service after maintenance, thus minimizing the probability that components are not left in an inoperable state. For example, EECW SI 4.5.C states, "When returning an EECW pump to service after maintenance to the pump, the following data must be included on SI 4.5.C.2 (EECW System Functional Test): pump flow, pump discharge pressure, and vibration amplitude. Additionally, SI 4.5.C.4 (EECW System Annual Flow Rate Test) must also be performed to provide operability per technical specifications."

Technical Specification Limitations. The limiting conditions for operation of the EECW system are spelled out in Section 3.5.C of the BFl Technical Specifications. Since the RHRSW and EECW systems are both covered by Section 3.5.C, the previous discussion in the RHRSW system description applies to this portion of the EECW writeup.

3.3.3 Operation

The previous discussion on "Instrumentation and Control" listed the automatic start features of the EECW pumps. These pumps may also be manually started from the MCR of any of the three units.

EECW recovery actions essentially consist of providing additional EECW flow from standby RHRSW pumps via cross-connect piping. In the event that three of four EECW pump flow is not available, the operator can readily align the RHRSW C1 or C2 pump to the EECW north supply heater by opening

motor-operated flow control valve (FCV-67-49) from the main control room. The other RHRSW pumps are not immediately available for effective recovery for the following reasons:

1. The A pumps are cross-connected to the EECW piping through a normally closed manual valve. This valve is located at the remote intake pumping station and would require dispatching an individual to manipulate the valves to the desired configuration. It has been estimated by TVA that it would take approximately 30 min to 2 hour to perform this recovery action.
2. The B pumps are similarly unavailable for EECW recovery due to a normally closed manual valve in the cross-connect piping.
3. The D pumps can be aligned to the EECW south supply header by opening a motor-operated valve (FCV-67-48); however, technical specifications require that at least one of the D1 or D2 pumps be available as the SBCS system pump. In order to use the D1 pump for EECW supply, the discharge header cross-connect valve (563) would have to be closed. This valve is a normally open manual valve remotely located at the pumping station. By closing valve (563), the RHRSW Pump D1 could be used for EECW supply and Pump D2 could be used for RHRSW or standby coolant supply if needed.

3.3.4 Fault Tree

Figure B-37 is the EECW system fault tree. Since a reduced tree is depicted in Figure B-37, many of the logical OR gates have been combined into one tabulation OR (TAB OR) gate in order to save space and make the tree easier to comprehend. The TAB OR gates were only used where system fault logic would not be compromised by compressing the appropriate gates and their corresponding basic events into one logic gate. Where this could not be accomplished, no reduction was attempted and the fault logic is fully developed.

There are two house events in the EECW tree. Both appear in the initiation circuitry model. The events HOUSENVA and HOUSENVL account for whether the shutdown boards powering the EECW pumps are being supplied by normal power or the diesel generator. The two events are mutually exclusive. Whenever HOUSENVA is "on," HOUSENVL is "off" and vice versa. For all initiators other than loss of offsite power, HOUSENVA is "on" and HOUSENVL is "off." For loss of offsite power sequences the reverse is true.

Since the EECW only provides a support function, the EECW fault model was constructed based on those systems that require EECW following the accidents considered in the Browns Ferry IREP assessment. That is, transfers are appropriately provided in the fault tree where safety-related components require the EECW support system interface. These cooling water loads are: (a) RHR room coolers, (b) RHR pump seal coolers, and (c) Units 1, 2, and 3 diesel generator engine coolers.

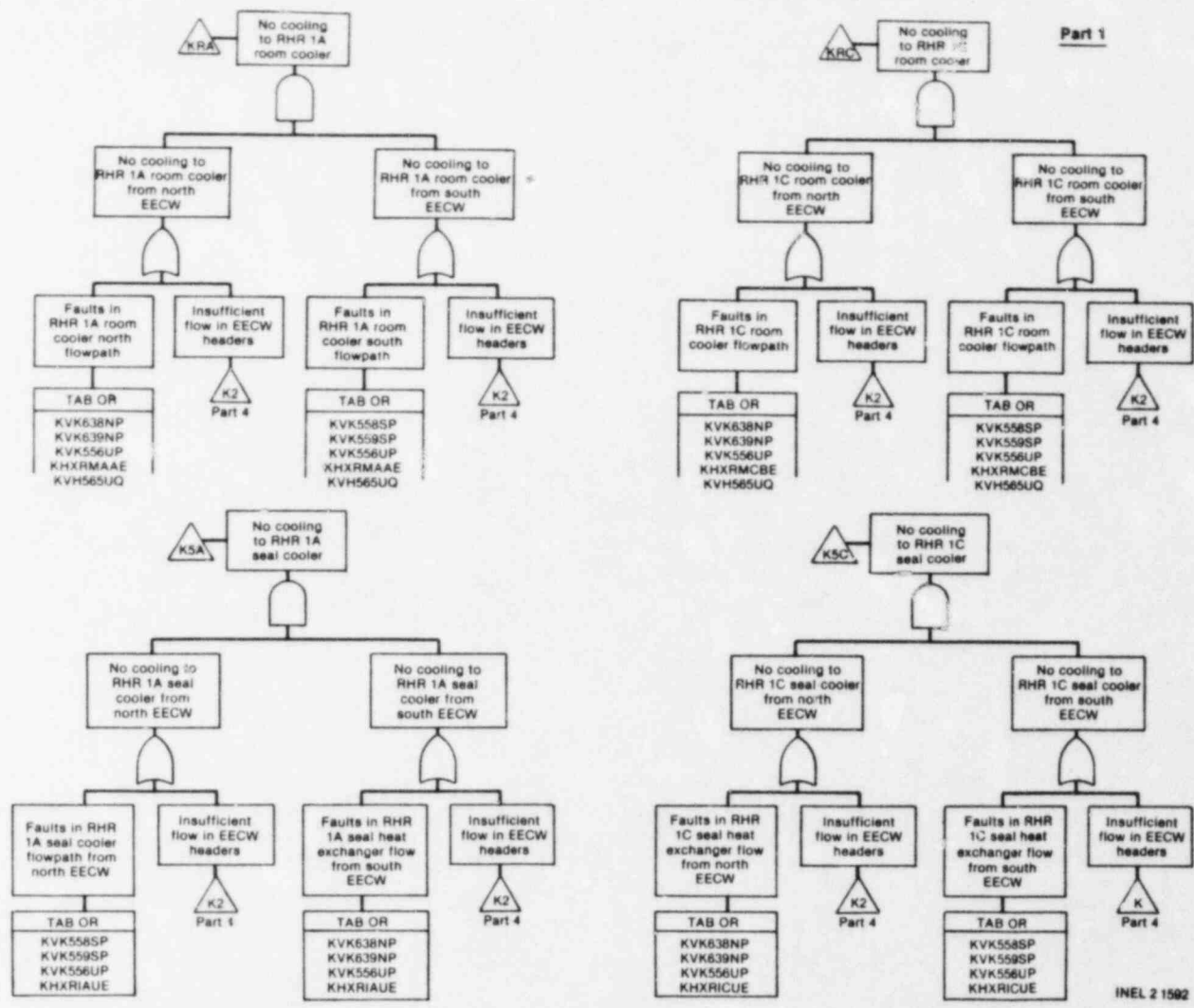


Figure B-37. EECW fault tree.

Part 2

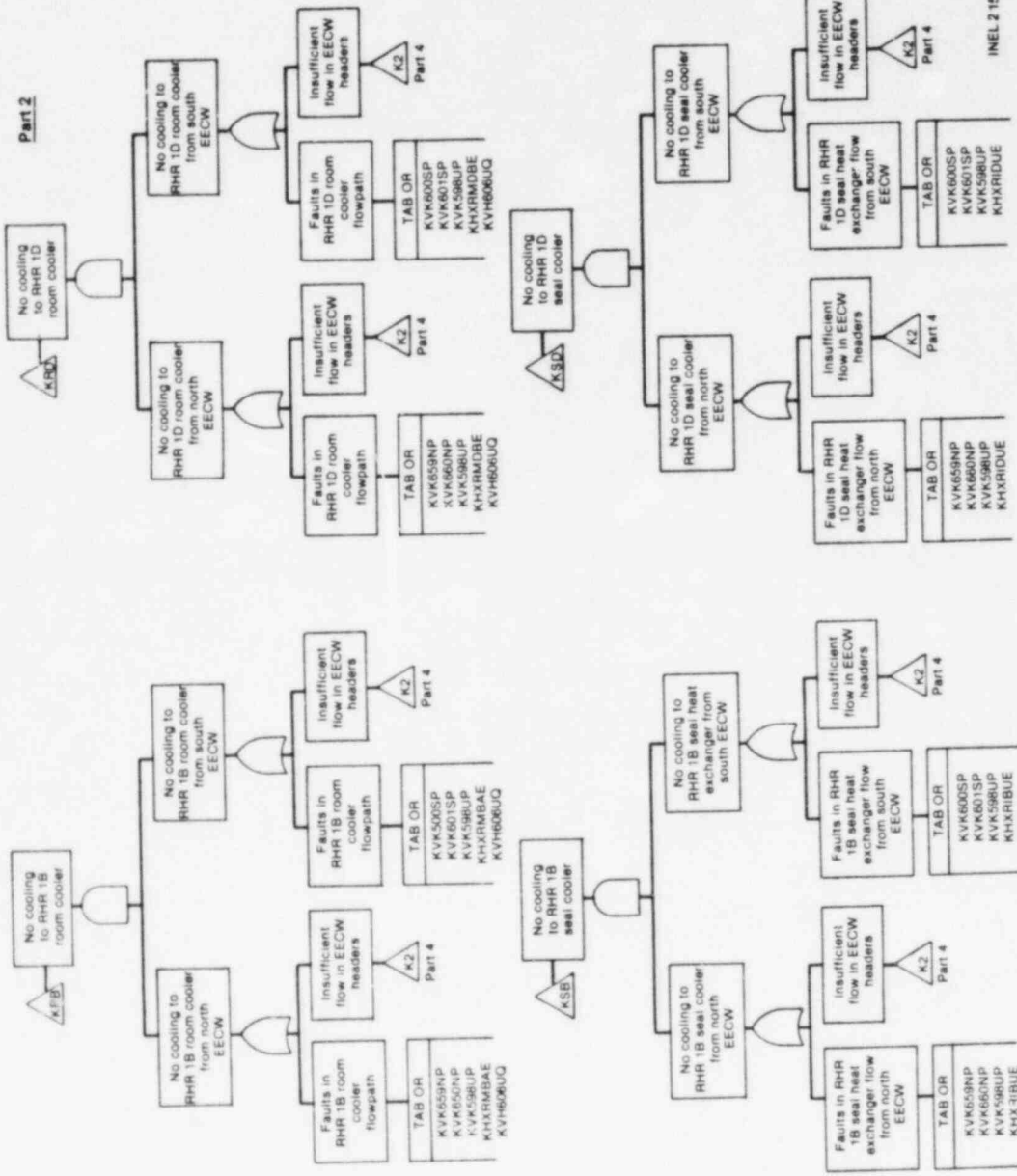


Figure B-37. (continued).

INEL 21583

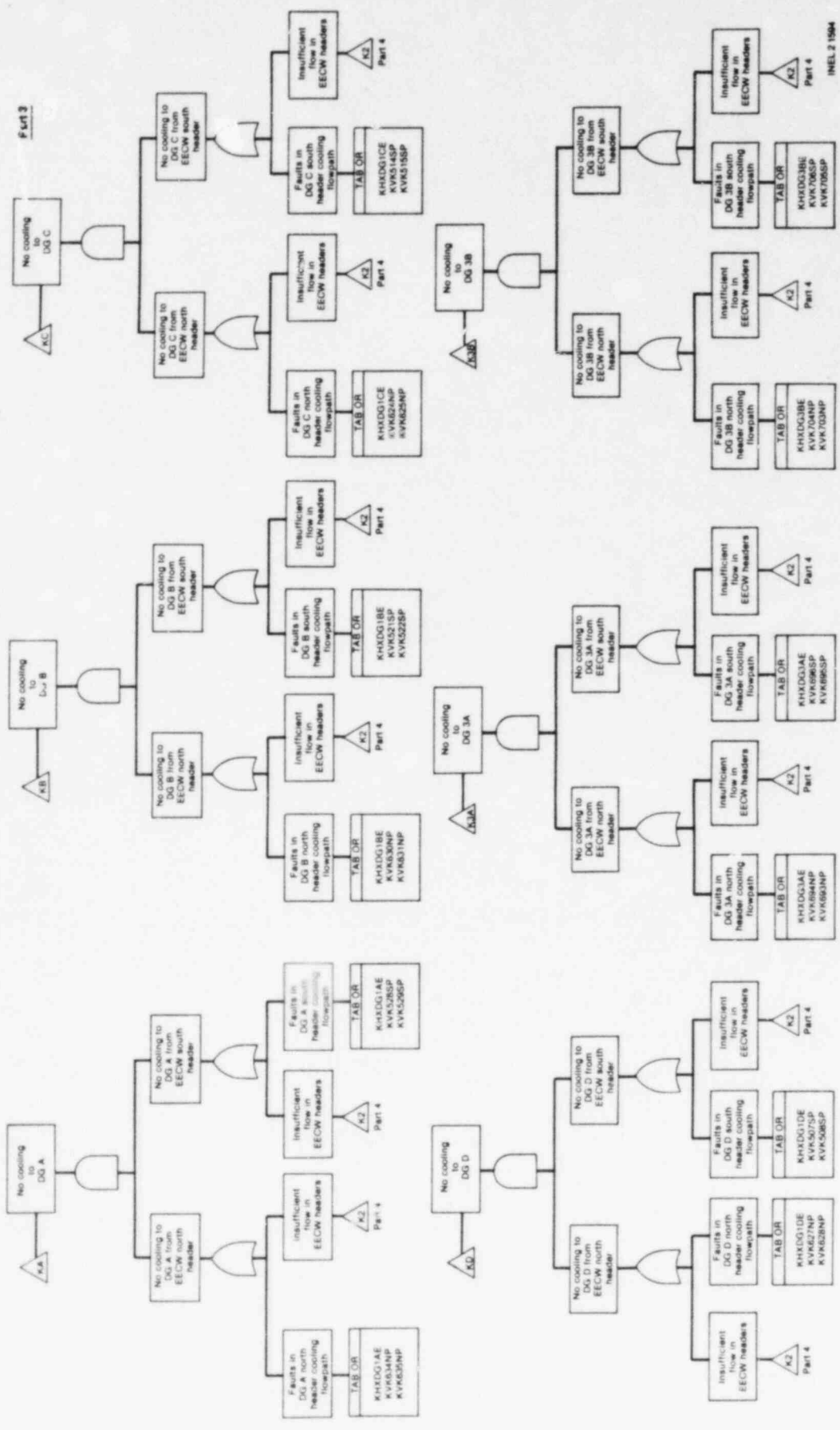
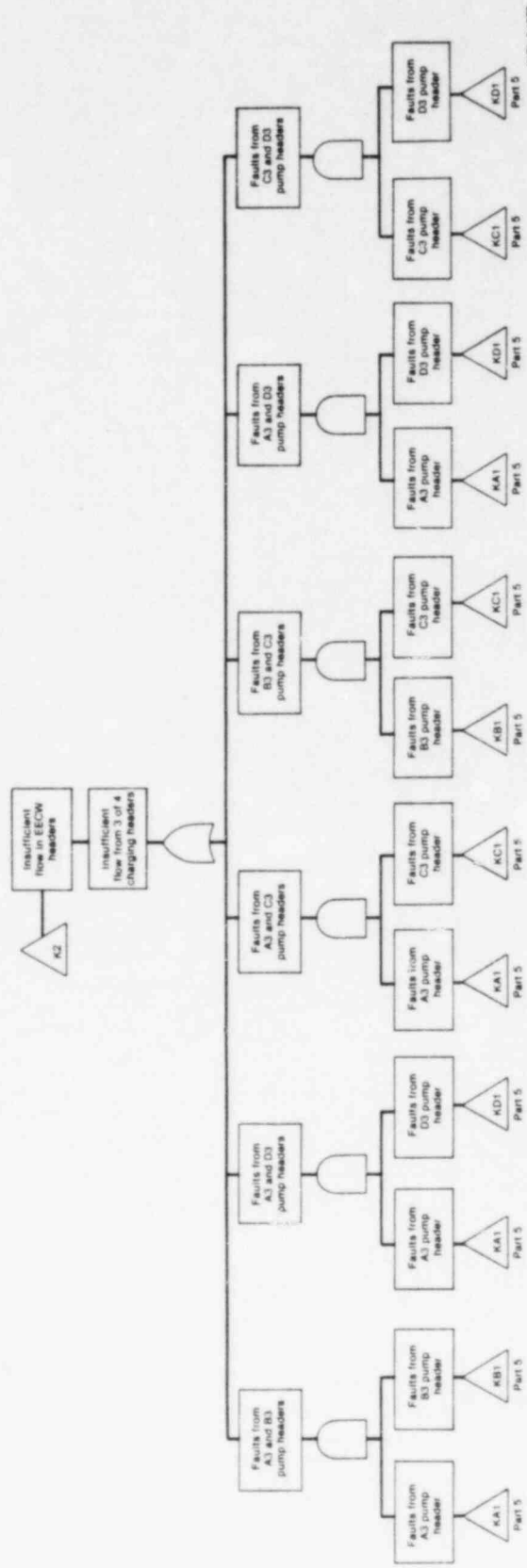
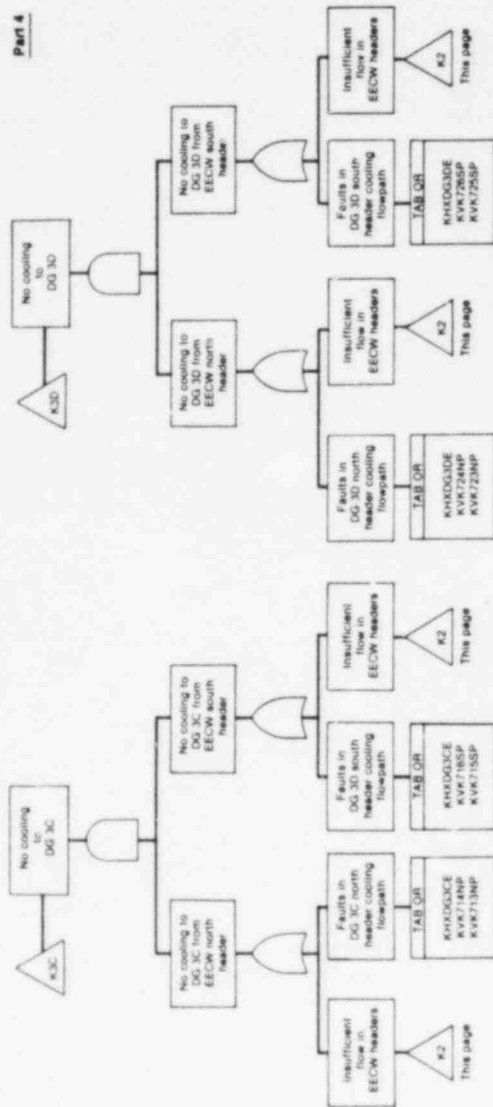


Figure B-37. (continued).

Part 4



INEL-2 1056

Figure B-37. (continued).

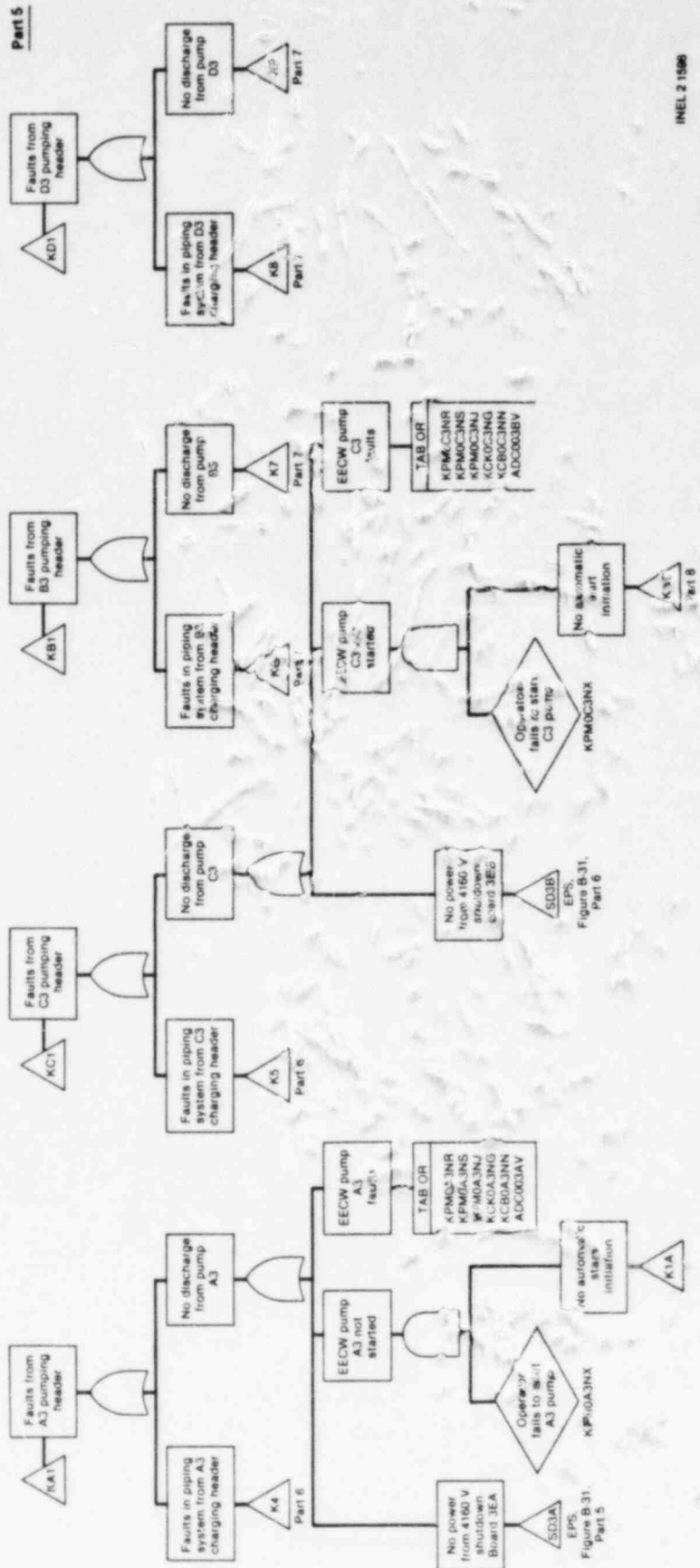


Figure B-37. (continued).

B-39C

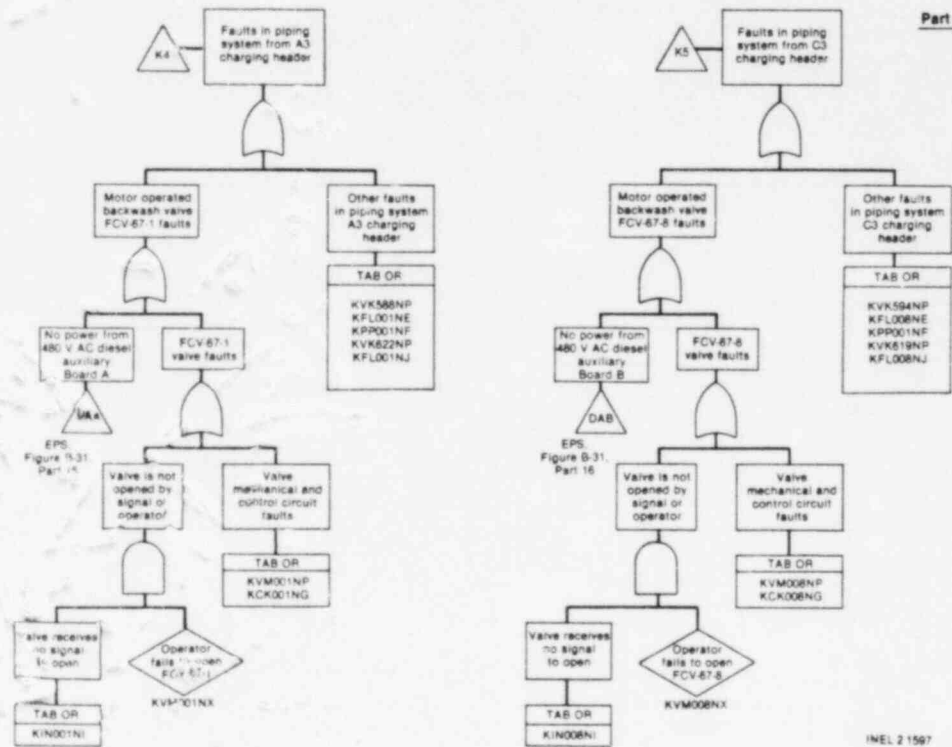
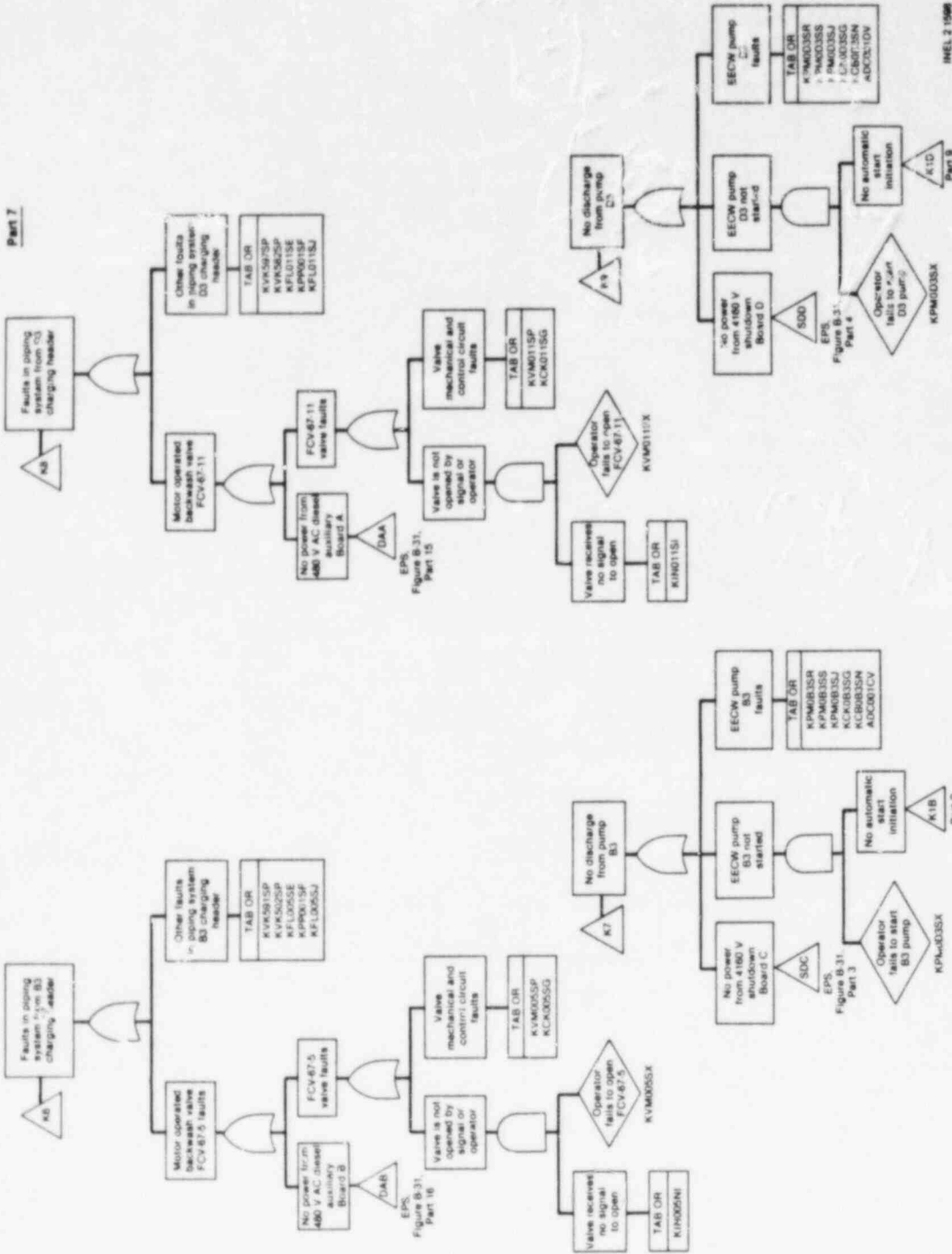
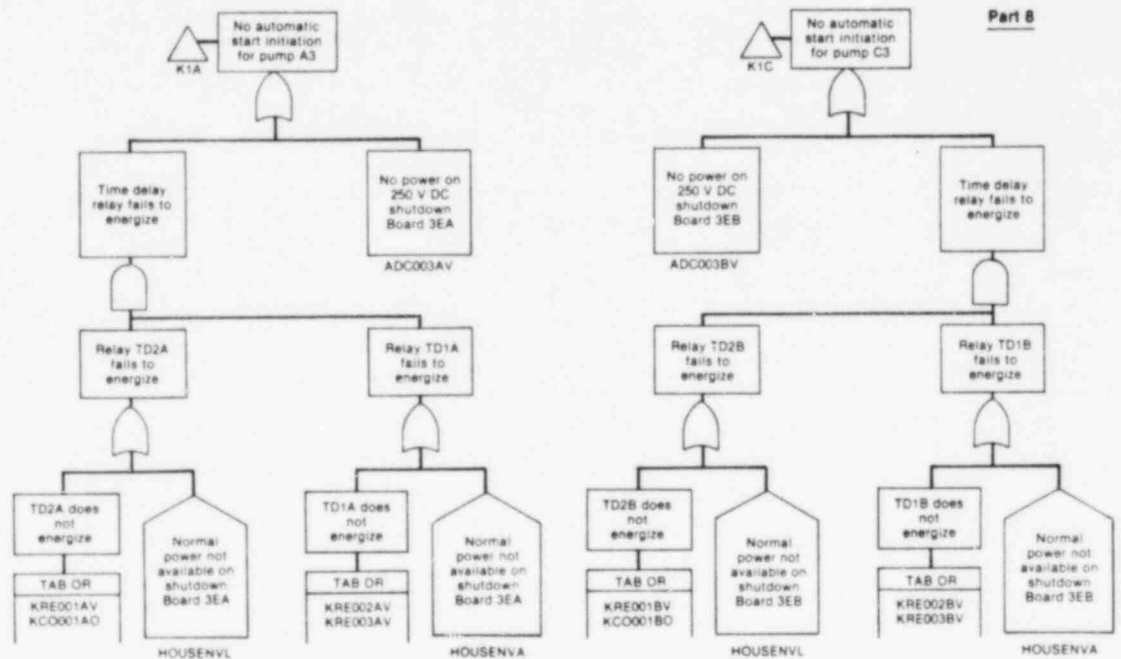


Figure B-37. (continued).



INEL 21596

Figure B-37. (continued).



B-401

Figure B-37. (continued).

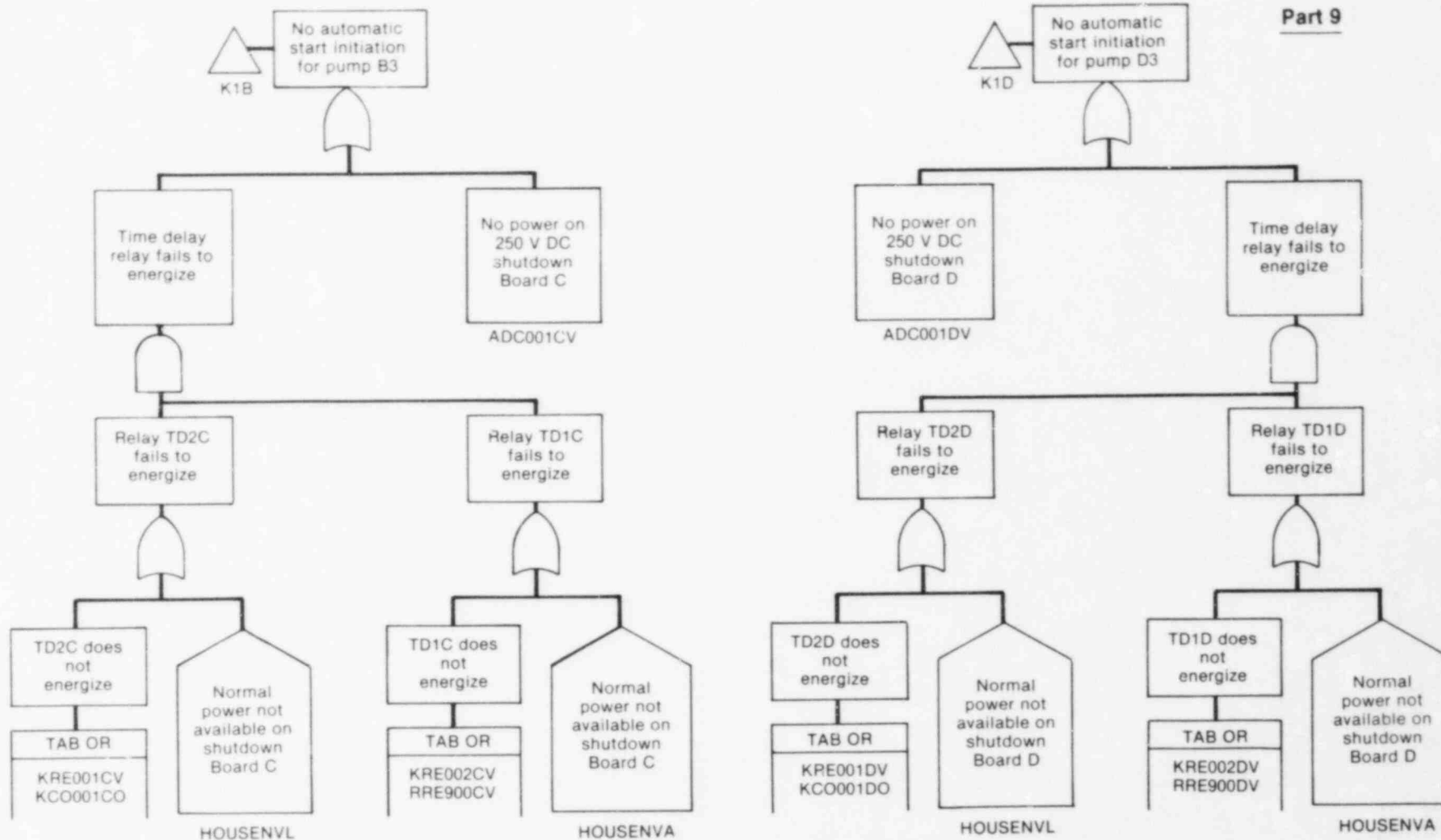


Figure B-37. (continued).

B-401

Loss of cooling flow in the north and south headers and the loss of the EECW flow paths from these headers to the various safety-related components listed above are developed on the fault tree. Fault tree models of the automatic initiation circuits are shown in Parts 8 and 9 of the EECW fault tree. As discussed previously, any of several multiple contacts can initiate a pump start. Time delay relay contacts close in the pump control circuit in 28 sec if normal power is available or in 14 sec if only diesel generator power is available. Only the faults associated with the time delay relays were included in the fault model of the EECW auto-initiation logic since it is very unlikely that one of the multiple start conditions would not be present when EECW is required.

Success/Failure Criteria. The top event descriptions in the EECW fault tree are "No cooling to . . ." These top event descriptions are interpreted to mean that failure of the component function occurs if adequate flow cannot be delivered through the component of interest. Adequate flow is defined as the flow delivered by at least one of the two independent piping headers (north and south headers) supplied by three of the four EECW pumps.

Major Assumptions. The EECW system fault tree was constructed based on the following major assumptions:

1. The EECW pumps are initially aligned as shown in Figure B-35.
2. Detailed information necessary for the analysis of intake station faults was not available for this report. Discussions with TVA personnel concluded that most intake station faults resulted in high intake temperatures for the RHRSW system. This closely resembles an external event (fire, flood, earthquake), and the IREP procedures dictated that external events should not be considered in our analysis. Therefore, as a result of both of these considerations, intake station faults were not developed in this analysis.
3. Supply header ruptures are assumed to encompass all pressurized piping from the EECW pump discharge check valves to the branch runouts supplying the various cooling loads. No other single passive faults could disable the EECW system. However, passive faults of normally open manual valves were considered due to their potential for loss of multiple RHR coolers.
4. Although operator recovery for manually starting the EECW pumps was shown on the EECW fault tree, no credit was taken for this recovery action. No auto-initiation faults were significant to the multiple start features of the EECW pumps.

Basic Events. The information associated with the various basic events listed in the fault tree is summarized in the EECW fault summary short form, Table B-81. In addition, the failure data associated with these basic events is summarized in Table B-79. Tables B-82 and B-83 list the dominant contributors to EECW unavailability.

TABLE B-81. EECW SYSTEM FAULT SUMMARY SHORT FORM

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
KVK638NP	Check Valve 638	Does not open	1E-4/D	--	3
KVK639NP	Check Valve 639	Does not open	1E-4/D	--	3
KVK556UP	Check Valve 556	Does not open	1E-4/D	--	3
KHXRMAAE	RHR 1A room cooler	Plugged	1E-6/hr	384	10
KVK558SP	Check Valve 558	Does not open	1E-4/D	--	3
KVK559SP	Check Valve 559	Does not open	1E-4/D	--	3
KHXRMCBE	RHR 1C room cooler	Plugged	1E-6/hr	384	10
KHXR1AUE	RHR 1A seal cooler	Plugged	1E-6/hr	384	10
KHXR1CUE	RHR 1C seal cooler	Plugged	1E-6/hr	384	10
KVK659NP	Check Valve 659	Does not open	1E-4/D	--	3
KVK660NP	Check Valve 660	Does not Open	1E-4/D	--	3

B-403

TABLE B-81. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
KVK598UP	Check Valve 598	Does not open	1E-4/D	--	3
KHXRMBAE	RHR 1B room cooler	Plugged	1E-6/hr	384	10
KVK600SP	Check Valve 600	Does not open	1E-4/D	--	3
KVK601SP	Check Valve 601	Does not open	1E-4/D	--	3
KHXRMDBE	RHR 1D room cooler	Plugged	1E-6/hr	384	10
KHXRI1BUE	RHR 1B seal cooler	↓	↓	↓	↓
KHXRI1DUE	RHR 1D seal cooler	↓	↓	↓	↓
KHXDG1AE	Diesel Generator A engine cooler	↓	↓	↓	↓
KVK634NP	Check Valve 634	Does not open	1E-4/D	--	3
KVK635NP	Check Valve 635	↓	↓	--	↓
KVK528SP	Check Valve 528	↓	↓	--	↓
KVK529SP	Check Valve 529	↓	↓	--	↓

TABLE B-81. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
KHXDG1BE	Diesel Generator B engine cooler	Plugged	1E-6/hr	384	10
KVK630NP	Check Valve 630	Does not open	1E-4/D	--	3
KVK631NP	Check Valve 631	↓	↓	--	↓
KVK521SP	Check Valve 521	↓	↓	--	↓
KVK522SP	Check Valve 522	↓	↓	--	↓
KHXDG1CE	Diesel Generator C engine cooler	Plugged	1E-6/hr	384	10
KVK624NP	Check Valve 624	Does not open	1E-4/D	--	3
KVK625NP	Check Valve 625	↓	↓	--	↓
KVK514SP	Check Valve 514	↓	↓	--	↓
KVK515SP	Check Valve 515	↓	↓	--	↓
KHXDG1DE	Diesel Generator D engine cooler	Plugged	1E-6/hr	384	10
KVK627NP	Check Valve 627	Does not open	1E-4/D	--	3

TABLE B-81. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
KVK628NP	Check Valve 628	Does not open	1E-4/D	--	3
KVK507SP	Check Valve 507	Does not open	1E-4/D	--	3
KVK508SP	Check Valve 508	Does not open	1E-4/D	--	3
KHXDG3AE	Diesel Generator 3A engine cooler	Plugged	1E-6/hr	384	10
KVK694NP	Check Valve 694	Does not open	1E-4/D	--	3
KVK693NP	Check Valve 693	↓	↓	--	↓
KVK696SP	Check Valve 696	↓	↓	--	↓
KVK695SP	Check Valve 695	↓	↓	--	↓
KHXDG3BE	Diesel Generator 3B engine cooler	Plugged	1E-6/hr	384	10
KVK704NP	Check valve	Does not open	1E-4/D	--	3
KVK703NP	Check valve	Does not open	1E-4/D	--	3

TABLE B-81. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
KVK706SP	Check valve	Does not open	1E-4/D	--	3
KVK705SP	Check valve	Does not open	1E-4/D	--	3
KHXDG3CE	Diesel Generator 3C engine cooler	Plugged	1E-6/hr	384	10
KVK714NP	Check Valve 714	Does not open	1E-4/D	--	3
KVK713NP	Check Valve 713	↓	↓	--	↓
KVK716SP	Check Valve 716	↓	↓	--	↓
KVK715SP	Check Valve 715	↓	↓	--	↓
KHXDG3DE	Diesel Generator 3D engine cooler	Plugged	1E-6/hr	384	10
KVK724NP	Check Valve 724	Does not open	1E-4/D	--	3
KVK723NP	Check Valve 723	↓	↓	--	↓
KVK726SP	Check Valve 726	↓	↓	--	↓
KVK725SP	Check Valve 725	↓	↓	--	↓

B-407

TABLE B-81. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
KPMOA3NR	EECW Pump A3	Does not start	1E-3/D	--	3
KPMOA3NS	EECW Pump A3	Does not run	3E-5/hr	8	10
KPMOA3NJ	EECW Pump A3	Unavailable due to maintenance	5E-4	--	0
KCBOA3NN	EECW Pump A3 circuit breaker	Does not close	1E-3/D	--	3
KCKOA3NG	Motor control circuit for EECW Pump A3	No output	2.9E-3	--	10
ADC003AV	250 V DC control power for closing Pump A3 circuit breaker	Does not energize	1E-6/hr	7	3
KPMOA3NX	Operator error	Does not energize	1E-3/D	--	10
KPMOC3NX	Operator error	Does not energize	1E-3/D	--	10
KPMOC3NR	EECW Pump C3	Does not start	1E-3/D	--	3
KPMOC3NS	EECW Pump C3	Does not run	3E-5/hr	8	10

TABLE B-81. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
KPMOC3NJ	EECW Pump C3	Unavailable due to maintenance	5E-4	--	0
KCK003NG	Motor control circuit for EECW Pump C3	No output	2.9E-3	--	10
KCBOC3NN	EECW Pump C3 circuit breaker	Does not close	1E-3/D	--	3
ADC003BV	250 V DC control power for closing Pump C3 circuit breaker	Does not energize	1E-6/hr	7	3
KVK588NP	Check Valve 588	Does not open	1E-4/D	--	3
KFLOO1NE	EECW north header strainer	Plugged	1E-6/hr	384	10
KPFO01NF	North header piping	Rupture	1E-10/hr/section	384	10
KVK622NP	Check Valve 622	Does not open	1E-4/D	--	3
KFLOO1NJ	North header Strainer 1	Unavailable due to maintenance	7E-4	--	0
KVMOO1NP	FCV-67-1	Does not open	1E-3/D	--	3

TABLE B-81. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
KCK001NG	Motor control circuit for FCV-67-1	No output	3.2E-3	--	10
KVMO01NX	Operator error	--	1E-3/D	--	10
KINO01NI	Pressure Switch PS-67-1	Erroneous output	1E-6/hr	367	10
KVK594NP	Check Valve 594	Does not open	1E-4/D	--	3
KFLO08NE	EECW north header strainer	Plugged	1E-6/hr	384	10
KVK619NP	Check Valve 619	Does not open	1E-4/D	--	3
KFLO08NJ	North Header Strainer 8	Unavailable due to maintenance	7E-4	--	0
KVMO08NP	FCV-67-8	Does not open	1E-3/D	--	3
KCK008NG	Motor control circuit for FCV-67-8	No output	3.2E-3	--	10
KVMO08NX	Operator error	--	1E-3/D	--	10
KINO08NI	Pressure Switch PS-67-8	Erroneous output	1E-6/hr	367	10

TABLE B-81. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
KVK591SP	Check Valve 591	Does not open	1E-4/D	--	3
KVK502SP	Check Valve 502	Does not open	1E-4/D	--	3
KFL005SE	EECW south header strainer	Plugged	1E-6/hr	384	10
KPP001SF	South header piping	Rupture	1E-10/hr/ section	384	10
KFL005SJ	South header Strainer 5	Unavailable due to maintenance	7E-4	--	0
KVM005SP	FCV-67-5	Does not open	1E-3/D	--	3
KCK005SG	Motor control circuit for FCV-67-5	No output	3.2E-3	--	10
KVM005SX	Operator error	--	1E-3/D	--	10
KIN005SI	Pressure Switch PS-67-5	Erroneous output	1E-6/hr	367	10
KVK597SP	Check Valve 597	Does not open	1E-4/D	--	3

TABLE B-81. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
KVK582SP	Check Valve 582	Does not open	1E-4/D	--	3
KFLO11SE	EECW south header strainer	Plugged	1E-6/hr	384	10
KFLO11SJ	South header Strainer 11	Unavailable due to maintenance	7E-4	--	0
KVM011SP	FCV-67-11	Does not open	1E-3/D	--	3
KCK011SG	Motor control circuit for FCV-67-11	No output	3.2E-3	--	10
KMV011SX	Operator error	--	1E-3/D	--	↓
KIN011S1	Pressure Switch PS-67-11	Erroneous output	1E-6/hr	367	
KPMOB35X	Operator error	--	1E-3/D	--	
KPMOB3SR	EECW Pump B3	Does not start	1E-3/D	--	3
KPMOB3SS	EECW Pump B3	Does not run	3E-5/hr	8	10

TABLE B-81. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
KPMOB3SJ	EECW Pump B3	Unavailable due to maintenance	5E-4	--	0
KCBOD3SN	EECW Pump B3 circuit breaker	Does not close	1E-3/D	--	3
KCKOB3SG	Motor control circuit for EECW Pump B3	No output	2.9E-3	--	10
ADC001CV	250 V DC control power for closing Pump B3 circuit breaker	Does not energize	1E-6/hr	7	3
KPMOD3SX	Operator error	--	1E-3/D	--	10
KPMOD3SR	EECW Pump D3	Does not start	1E-3/D	--	3
KPMOD3SS	EECW Pump D3	Does not run	3E-5/hr	8	10
KPMOD3SJ	EECW Pump D3	Unavailable due to maintenance	5E-4	--	0
KCBOD3SN	EECW Pump D3 circuit breaker	Does not close	1E-3/D	--	3

TABLE B-81. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
KCKOD3SG	Motor control circuit for EECW Pump D3	No output	2.9E-3	--	10
ADCO01DV	250 V DC control power for closing Pump D3 circuit breaker	Does not energize	1E-6/hr	7	3
KVH565UQ	Manual Valve 656	Does not remain open	1E-4/D	--	
KVH606UQ	Manual Valve 606	Does not remain open		--	
KRE001AV	Time delay Relay TD2A	Does not energize		--	
KRE002AV	Time delay Relay TD1A	Does not energize		--	
KRE003AV	Diesel generator available Relay DGVA-A1	Does not energize		--	
KC0001A0	Normal power available Contacts NVA-A1	Open	1E-7/hr	367	10

B-414

TABLE B-81. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
KRE001BV	Time delay Relay TD2B	Does not energize	1E-4/D	--	3
KRE002BV	Time delay Relay TD1B	Does not energize	1E-4/D	--	3
KRE003BV	Diesel generator available Relay DGVA-B1	Does not energize	1E-4/D	--	3
KC0001B0	Normal power available [*] Contacts NVA-B1	Open	1E-7/hr	367	10
KRE001CV	Time delay relay TD2C	Does not energize	1E-4/D	--	3
KC0001C0	Normal power available Contacts NVA-C1	Open	1E-7/hr	367	10
KRE002CV	Time delay relay TD1C	Does not energize	1E-4/D	--	3
RRE900CV	Diesel generator available Relay DGVA-C1				
KRE001DV	Time delay Relay TD2D				
KRE002DV	Time Delay Relay TD1D				

TABLE E-81. (continued)

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
RRE900DV	Diesel generator available Relay DGVA-D1	Does not energize	1E-4/D	--	3
KC0001D0	Normal power available Contacts NVA-D1	Open	1E-7/hr	367	10

TABLE B-82. EECW SYSTEM CUT SETS
(Gate K2)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
1.0E-5	1.7	KCK001NG, KCK008NG	Yes
1.0E-5	1.7	KCK001NG, KCK011SG	Yes
1.0E-5	1.7	KCK005SG, KCK011SG	Yes
1.0E-5	1.7	KCK001NG, KCK005SG	Yes
1.0E-5	1.7	KCK008NG, KCK011SG	Yes
1.0E-5	1.7	KCK008NG, KCK005SG	Yes
9.3E-6	1.6	KCK0A3NG, KCK011SG	Yes
9.3E-6	1.6	KCK0D3SG, KCK008NG	Yes
9.3E-6	1.6	KCK0C3NG, KCK001NG	Yes
9.3E-6	1.6	KCK0C3NG, KCK005SG	Yes
9.3E-6	1.6	KCK0B3SG, KCK011SG	Yes
9.3E-6	1.6	KCK0C3NG, KCK011SG	Yes
9.3E-6	1.6	KCK0B3SG, KCK001NG	Yes
9.3E-6	1.6	KCK0A3NG, KCK005SG	Yes
9.3E-6	1.6	KCK0A3NG, KCK008NG	Yes
9.3E-6	1.6	KCK0D3SG, KCK001NG	Yes
9.3E-6	1.6	KCK0D3SG, KCK005SG	Yes
9.3E-6	1.6	KCK0B3SG, KCK008NG	Yes
8.4E-6	1.4	KCK0D3SG, KCK0C3NG	Yes
8.4E-6	1.4	KCK0D3SG, KCK0B3SG	Yes
8.4E-6	1.4	KCK0B3SG, KCK0C3NG	Yes
Cumulative importance	33.6		

TABLE B-83. EECW SYSTEM CUT SETS
(LOSP)

<u>Unavailability</u>	<u>Importance (%)</u>	<u>Cut Sets</u>	<u>Potentially Recoverable</u>
9E-4	4.3	ADL003AR,ADL001CR	No
9E-4	4.3	ADL003AR,ADL003BR	No
9E-4	4.3	ADL003AR,ADL001DR	No
9E-4	4.3	ADL003BR,ADL001CR	No
9E-4	4.3	ADL001DR,ADL001BR	No
9E-4	4.3	ADL001CR,ADL001DR	No
9E-4	4.3	ADL001AR,ADL001BR	No
9E-4	4.3	ADL003BR,ADL001DR	No
9.6E-5	0.5	KCK008NG,ADL001CR	Yes
9.6E-5	0.5	KCK001NG,ADL003BR	Yes
9.6E-5	0.5	ADL003BR,KCK011SG	Yes
9.6E-5	0.5	ADL003RR,KCK005SG	Yes
9.6E-5	0.5	KCK008NG,ADL001DR	Yes
9.6E-5	0.5	KCK001NG,ADL001DR	Yes
9.6E-5	0.5	ADL003AR,KCK008NG	Yes
9.6E-5	0.5	ADL003AR,KCK011SG	Yes
9.6E-5	0.5	KCK001NG,ADL001CK	Yes
9.6E-5	0.5	ADL001CR,KCK011SG	Yes
9.6E-5	0.5	KCK005SG,ADL001DR	Yes
9.6E-5	0.5	ADL003AR,KCK005SG	Yes
Cumulative importance	40.4		

3.4 Keep-Full System

3.4.1 Purpose

The keep-full system at BFl is also known as the keep-fill system and the pressure suppression chamber water transfer system. For this report, it is referred to as the keep-full system and is classified as a support system.

The function of the keep-full system is to keep the core spray system Loops 1 and 2 and the RHR system Loops 1 and 2 filled with water. The critical section of piping in both systems (i.e., the piping that must remain full of water) is the section from the core spray/RHR pump discharge check valves to the normally closed core spray/RHR injection valves. Keeping this section of piping full of water will ensure that no piping damage will result from water hammer upon core spray or RHR system initiation.

3.4.2 System Configuration

The keep-full system consists of two pumps, a head tank, and various valves and piping. Figure B-38 is a simplified diagram of the system.

The head tank pumps take water from the torus via the core spray pump suction line and maintain head tank water level while pressurizing the system to greater than 48 psig. Pumps automatically cycle on high and low head tank levels as shown in Table B-84.

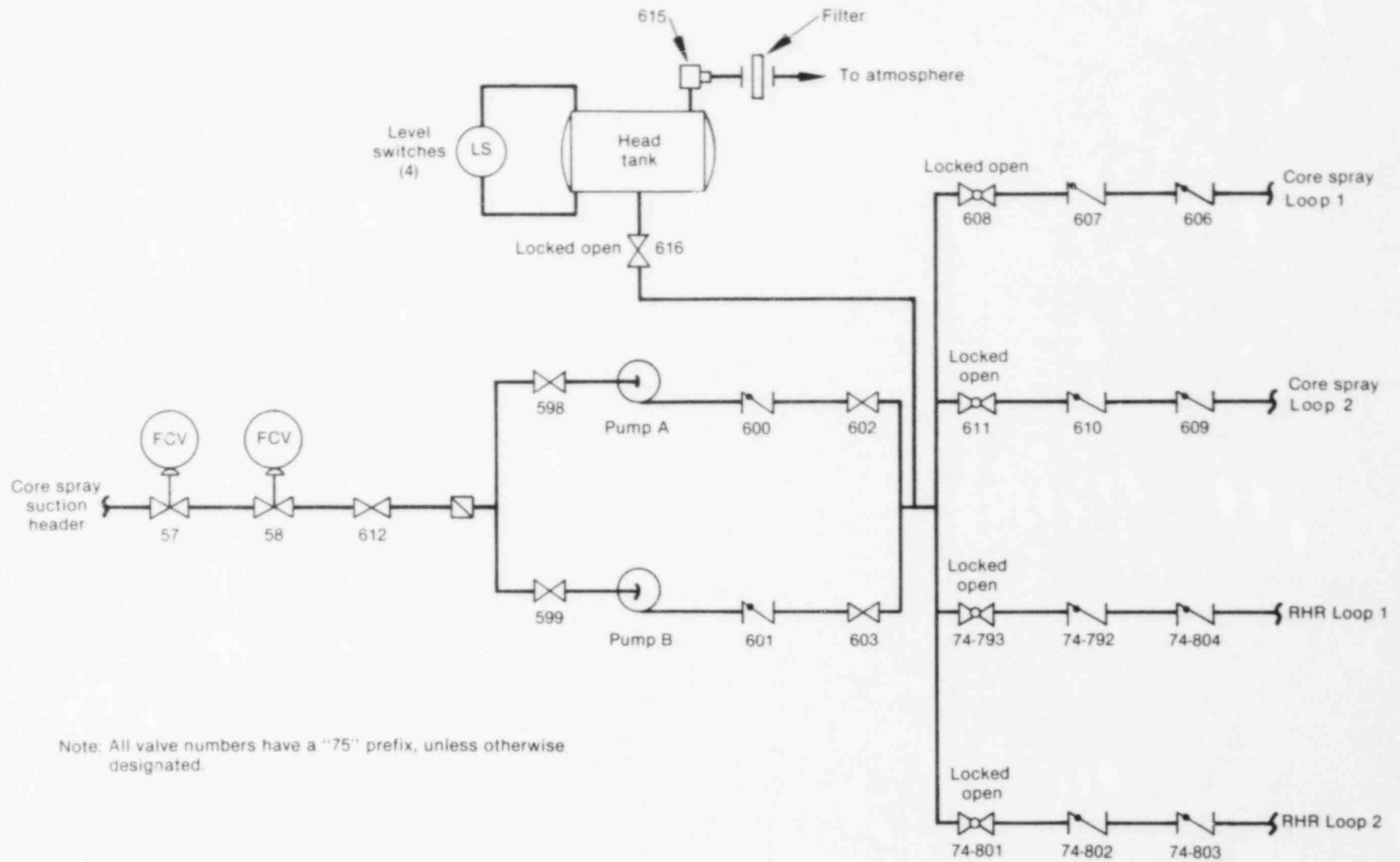
Each pump will trip if a high differential pressure exists across the common suction strainer or if either of the two air-operated suction valves close. The pumps have a rated capacity of 40 gpm. Pump A is powered from 480 V RMOV Board 1C, while Pump B is powered from the 480 V RMOV Board 1B.

The system head tank has a capacity of 3090 gallons. When the system pumps are not running, the water level in the head tank maintains a static head of greater than 48 psig on the system by virtue of head tank elevation above the system. This ensures that the associated core spray and RHR system piping is full and pressurized at all times that the keep-full system valves are to supply water to the associated core spray and RHR loops. Head tank level control is discussed in Table B-84.

There are two normally open, air-operated suction valves in the common pump suction header. The solenoid for the air operator on valve (FCV-75-57) is powered from the 120 V, 60 Hz, instrumentation and control Bus A, while the solenoid for FCV-75-58 is powered from Bus B. Both valves will fail shut on loss of power or loss of control air pressure. These valves are primary containment isolation system Group 2 isolation valves and will close on high drywell pressure (2 psig) or low reactor vessel water level (+10 inches). The valves also serve as suppression pool drain valves.

The system discharge paths to each core spray and RHR loop contain a locked-open, manually operated globe valve and two check valves. In addition, each loop has a backup fill system provided by valves and piping from the condensate system. This condensate flow path is normally isolated. However, should the keep-full system fail to maintain at least 48 psig in the associated loops, this alternate fill path will be used.

B-420



INEL 2 1610

Figure B-38. Keep-full system.

TABLE B-84. HEAD TANK LEVELS

<u>Tank Level Elevation</u>	<u>Associated Level Switch</u>	<u>Action</u>
647 ft, 0 in.	LS-75-78A	Both pumps trip: high level annunciated in control room
646 ft, 6 in.	LS-75-78B	Pump(s) stops
645 ft, 6 in.	LS-75-78C	One pump starts
645 ft, 0 in.	LS-75-78D	Both pumps start: low level annunciated in control room

3.4.3 Fault Tree

The core spray and RHR systems are initially aligned such that the system valves are in a normal configuration, the system is filled, and the system is ready for operation pending initiation signals or operator commands. Also, back-leakage through system check valves is insignificant. Given these assumptions, the keep-full system will be required to operate if gross leakage develops in the core spray/RHR loops as a result of component rupture or operator error, or if an operator intentionally drains a loop, in the latter case, the associated keep-full system supply line should be isolated. In the former case, the rupture or operator error causes loop failure regardless of the status of the keep-full system. In order to intentionally drain a loop, the operator must violate a number of procedures and ignore several indications and alarms in order to cause failure of the keep-full system. This operator action is incorporated in the test and maintenance contribution to the failure rates of the core spray and RHR systems.

Since faults in the keep-full system will not disable the RHR or core spray system unless a fault in the RHR or core spray systems has already disabled them, it is unnecessary to model keep-full system faults.

3.5 Condenser Circulating Water System

3.5.1 Purpose

The CCW system is designed to provide an efficient means of rejecting waste heat by providing flow to the condensers that condense the steam formed during the power generation cycle or following plant shutdown.

3.5.2 System Configuration

Overall Configuration. The CCW system is designed to provide a flow of 630,000 gpm to the condenser during open cycle operation and 30,000 gpm to the auxiliaries of each unit. The system consists of three pumps per unit, each with a capacity of 220,000 gpm at a design head of 32.5 feet.

The full power requirements of each generating unit are satisfied by that unit's respective group of three CCW pumps. A simplified diagram of the CCW system is shown as Figure B-39.

Each of the three pump discharge lines are equipped with a 96-inch diameter motor-operated butterfly valve. The three discharge lines are brought together into a single tunnel that varies throughout its length from an 18.5-foot diameter round culvert to a 14.5 x 14.5-foot square culvert. The condenser circulating water is carried to the condenser via this tunnel. The condenser discharge passes to the discharge tunnel and then on to either the warm water channel to the cooling towers or to the discharge diffusers.

The CCW system is capable of operating in any of three possible modes. These three modes of operation are referred to as the open mode, the closed mode, and the helper mode. In the open mode, water is drawn into the circulating water pumping station forebay, pumped through the main condenser, passed through Gate 1A, and discharged back into the reservoir through the diffusers.

In the closed operating mode, water is returned to the pumping station forebay from the cooling towers, pumped through the main condenser, diverted through the vacuum loop into the warm water channel going to the cooling towers, pumped out of the warm water channel, and through the cooling towers by the lift pumps.

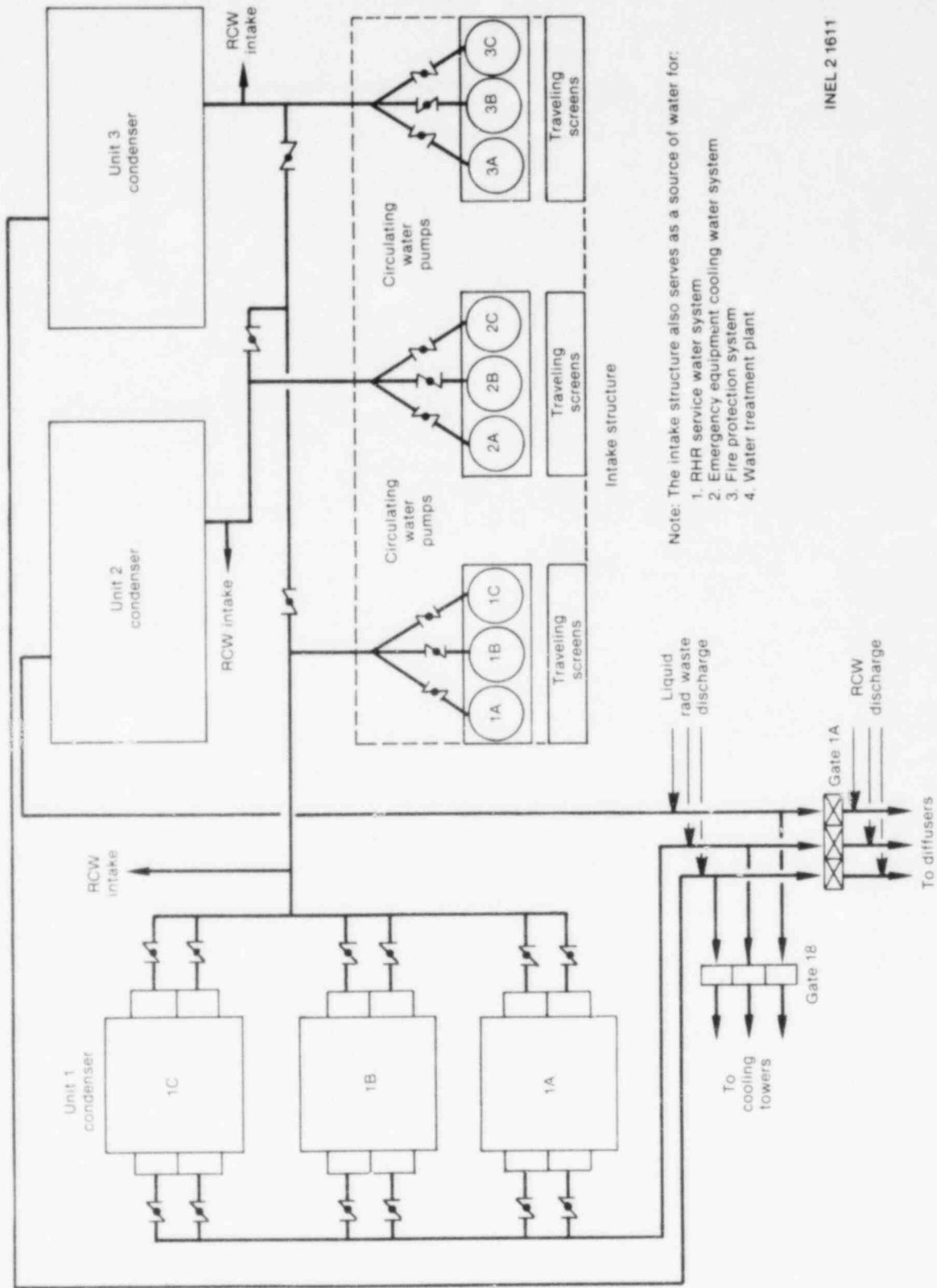
In the helper mode, water is drawn into the circulating water pumping station forebay, through the main condenser, diverted through the vacuum loop into the warm water channel going to the cooling towers, and pumped out of the warm water channel through the cooling towers by the lift pumps. The discharge from the cooling towers is discharged back to the reservoir via the discharge diffusers.

The Unit 1 condenser is actually composed of three condensing units, identified as Condensers 1A, 1B, and 1C. Each condenser unit is served by two inlet lines and two discharge lines. Each inlet line and each discharge line is equipped with a motorized flow control valve. The CCW system is normally operating during plant operation. All valves are normally open and all pumps are normally running.

System Interfaces. During the examination of the CCW system, interfaces between major CCW system components and auxiliary systems were identified. The three Unit 1 CCW pumps (1A, 1B, and 1C) are powered off of 4 kV unit Boards 1A, 1B, and 1C, respectively. The FSAR states that a procedure exists that allows for the provision of emergency AC power to the CCW pumps by hooking up two parallel diesel generators. However, it was assumed that under high stress conditions, this operator action is not likely to occur and, thus, no interface between the CCW system and the onsite emergency AC power system was included in this analysis.

The CCW pumps also interface with the raw water system that provides lube water to the CCW pumps.

Because the CCW system is normally operating during plant operation, detection of the unavailability of these interfacing support systems would occur very quickly.



Note: The intake structure also serves as a source of water for:

1. RHR service water system
2. Emergency equipment cooling water system
3. Fire protection system
4. Water treatment plant

INEL 2 1611

Figure B-39. CCW system.

Instrumentation and Control. The CCW system, as stated earlier, is a normally operating system that serves to condense steam formed during the power generation cycle. As such, this system does not require any sort of initiation signal and is not subject to initiation-type faults such as pumps failing to start or valves failing to open.

The only system control requirement for successful operation of the CCW system is that in the event that any two of the three Unit 1 CCW pumps become unavailable, the operator must throttle the six condenser discharge valves in order to maintain sufficient pump head.

Testing. The CCW system is operating during normal plant operation and, thus, is not subject to periodic system testing. The system is, in effect, being constantly tested. As such, the availability of the CCW system is not effected by a testing schedule.

Maintenance. There are no scheduled maintenance procedures associated with the CCW system. Maintenance is performed on CCW components only when they develop some apparent operational problem. Scheduled maintenance is, thus, not a contributor to the unavailability of the CCW system.

Technical Specification Limitations. The CCW system is not specifically subject to any technical specification limitations that effect system unavailability.

3.5.3 Operation

Operation of the CCW system is discussed in the previous subsection, "Overall Configuration."

3.5.4 Fault Tree

The CCW system operates during normal power operation. For this reason, the CCW is not required to change state in response to the LOCA or transient condition nor are components within the system required to change state or position. During normal power operation, three CCW pumps serve Unit 1. Following scram, only one CCW pump is required to condense shutdown steam.

Since the CCW system is in operation during normal power operation, a fault tree model of the CCW system was not constructed for the following reasons: (a) the operational requirements of CCW pump availability are less stringent following scram than they are during power operation, and (b) the CCW may be obtained from Units 2 or 3, if necessary.

An additional consideration that led to the decision not to model CCW faults is that a good base of data describing failures of boiling water reactor PCS in response to transients exist in documents such as Electric Power Research Institutes EPRI NP-801. CCW faults are described within the context of PCS failures, and, as such, no new or significant information would be generated as a result of performing a fault tree analysis of the Bf1 CCW system.

3.6 Raw Cooling Water System

3.6.1 Purpose

The RCW system furnishes cooling water to various nonsafety-related in-plant cooling loads during normal operations. The purpose of the RCW system is to remove heat from the RHR pump seals and room coolers under shutdown conditions other than LOSP conditions. The RCW system is not a safety-related system nor does it interface with any safety-related systems other than the interconnection with the RHR pump seals and room coolers. The purpose of this interconnection is to obviate the need for operation of the EECW system during normal shutdown. That is, the RCWS can remove the RHR pump heat loads during long-term decay heat removal when the RHR pumps are used in the shutdown cooling or torus cooling modes. Although the EECW automatically assumes these and other safety-related loads under LOCA conditions and for most of the transients considered in this study, the RCWS is still available should EECW fail.

3.6.2 System Configuration

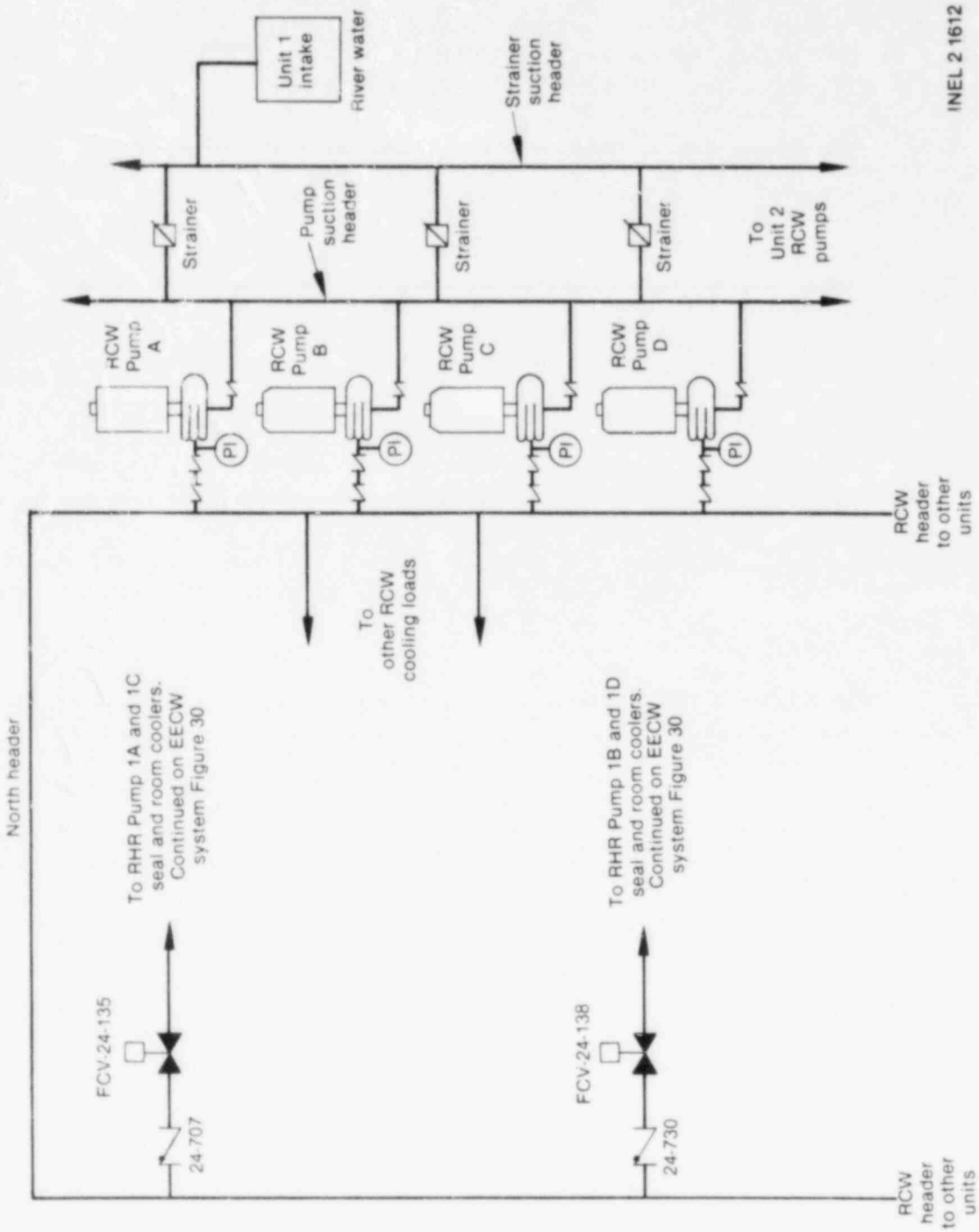
Browns Ferry Nuclear Station has 11 main raw cooling water (RCW) pumps of which two are spares. Units 1 and 2 are supplied by six RCW pumps with one common pump as a spare. The RCW pumps are supplied river water from the CCW intake conduits. Suction headers for Units 1 and 2 are interconnected. All of the RCW pumps discharge into a common (three unit) cooling header system.

Three pumps are required for each unit during normal operations. Upon normal unit shutdown, there is still a need by that unit for at least one RCW pump for miscellaneous cooling services. If Unit 1 is shutdown and Unit 2 is operating, no more than four pumps are required for the 2 units.

The RCW system pumps are powered from the 4160 V nonsafety-related unit buses. Under LOSP conditions the D spare pump can be manually connected to the Unit 1 and 2 4160 V shutdown Board A bus supplied by Diesel Generator A. The purpose of this connection is to supply water to selected turbine auxiliary equipment to prevent equipment damage and to assist getting back into power operation. However, one RCW pump is insufficient to supply both Units 1 and 2 cooling loads. Therefore, no credit is taken for this manual connection for the LOSP transient.

In the event that the pressure in the RCW header that supplies the RHR cooling loads decreases to a preset value, pressure switches sense the drop and start the EECW pumps.

To conserve RCW, an automatic air-operated valve is provided in each RCW supply line, controlled by the operation of the RHR pumps it serves. Figure B-40 is a simplified diagram of the RCW system showing only the Unit 1 pumps, major headers, and the interconnection with the EECW for the RHR pump seals and room coolers.



INEL 2 1612

Figure B-40. RCW system.

3.6.3 Fault Tree

The RCW system operates during normal power operation. Thus, the RCW system is not required to change state in response to a LOCA or transient condition nor are components within the system required to change state other than the valves in the lines supplying the RHR pump seal coolers and room coolers. Since the RCW system is in operation during normal power operation, a detailed fault model of the RCW system was not required for the following reasons: (a) the operational requirements of RCW system pump availability are less stringent following scram than they are during power operation (only one pump required), and (b) the RCW may be obtained from Units 2 or 3, if necessary. Part 25 of the RHR fault tree delineates the cooling faults for each of the RHR pumps. As shown by this portion of the model, inadequate pump seal cooling or room cooling can occur only if both RCW and EECW cooling to the associated heat exchangers are lost.

The fault tree model representing loss of RCW to the RHR pump seal coolers and heat exchangers is shown as Figure B-41. The house event for loss of offsite power (HOUSELOP) is provided to indicate that the RCW system is failed with a probability of 1.0 for LOSP when "on." When "off," the house event represents a failure rate of 2.7×10^{-5} /hr for LOSP at Browns Ferry subsequent to occurrence of any other initiating event. Also shown on the fault model are those RCW system components that must change state to supply the RHR cooling loads; in addition, since the RCW flow path through the RHR heat exchangers is the same as that for EECW, the common EECW flow path faults (designated K___) are listed. The RCWS fault tree was combined quantitatively with the EECW fault tree to account for these commonalities when considering loss of RHR pump seal and room cooling.

RCW fault event descriptions and associated failure data are provided in Table B-85. The EECW faults shown on the tree can be found in the EECW fault summary form, Table B-81.

3.7 Reactor Protection System

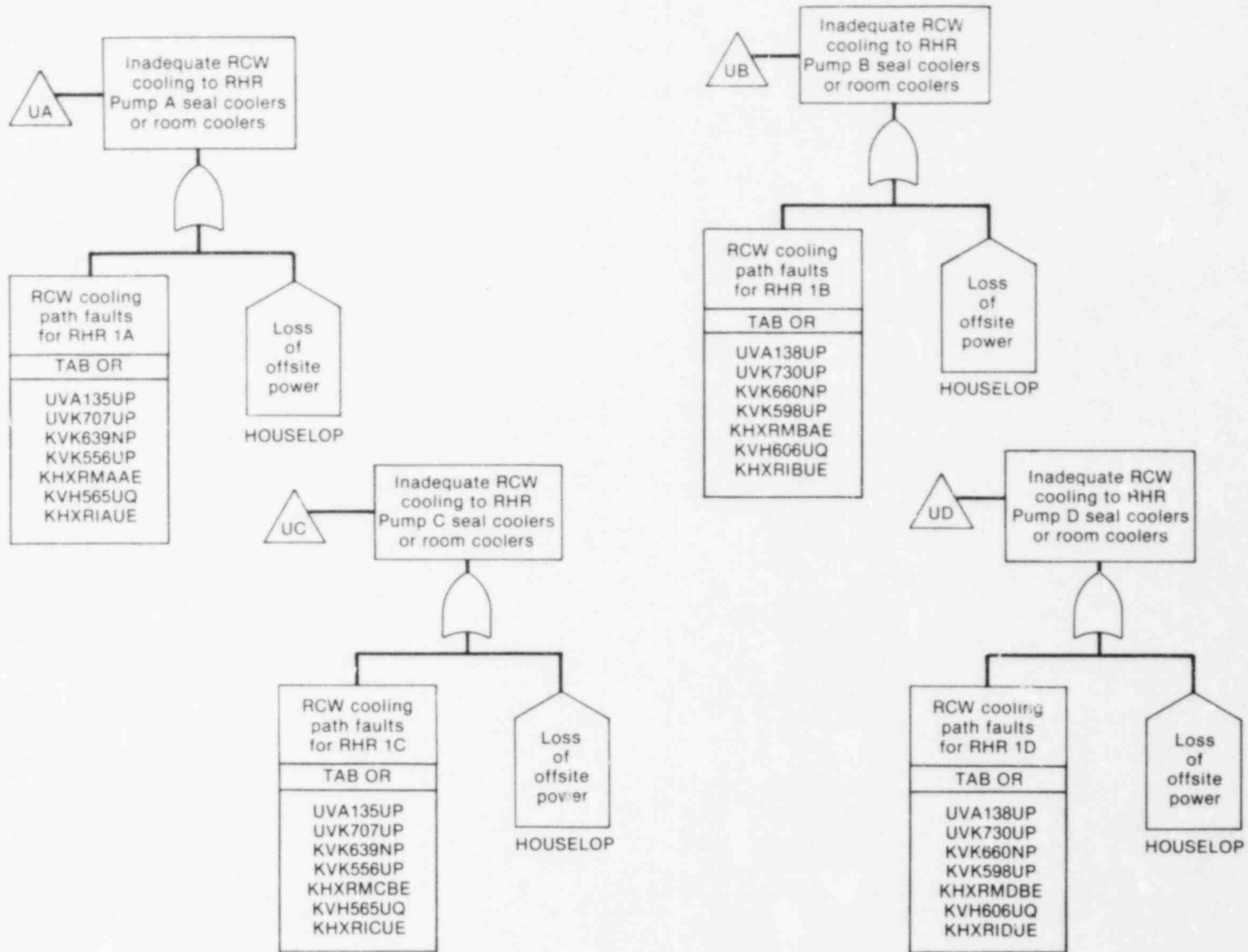
3.7.1 Purpose

The RPS monitors key plant parameters in order to protect against conditions that could damage the fuel or reactor pressure boundary integrity. The RPS automatically initiates a reactor scram in order to preserve cladding integrity, protect the reactor coolant pressure boundary, minimize the energy that must be absorbed following a LOCA, and prevent subsequent recriticality.

3.7.2 System Configuration

The RPS includes the sensors, relays, and switches that detect abnormal conditions and initiate a rapid insertion of the control rods to shut down the reactor. The system consists of two independent trip systems (A and B), each having two automatic scram channels (A1, A2, B1, and B2) and one manual scram channel (A3 and B3). Scram initiation requires a trip of at least one channel from each trip system. Power to each RPS trip system is from an independent RPS bus fed by an AC motor generator. The RPS channels are designed to initiate a scram upon loss of power to the system. Figure B-42 shows RPS Channel A. Channel B is similar.

B-425



INEL 2 1613

Figure B-41. RCW fault tree.

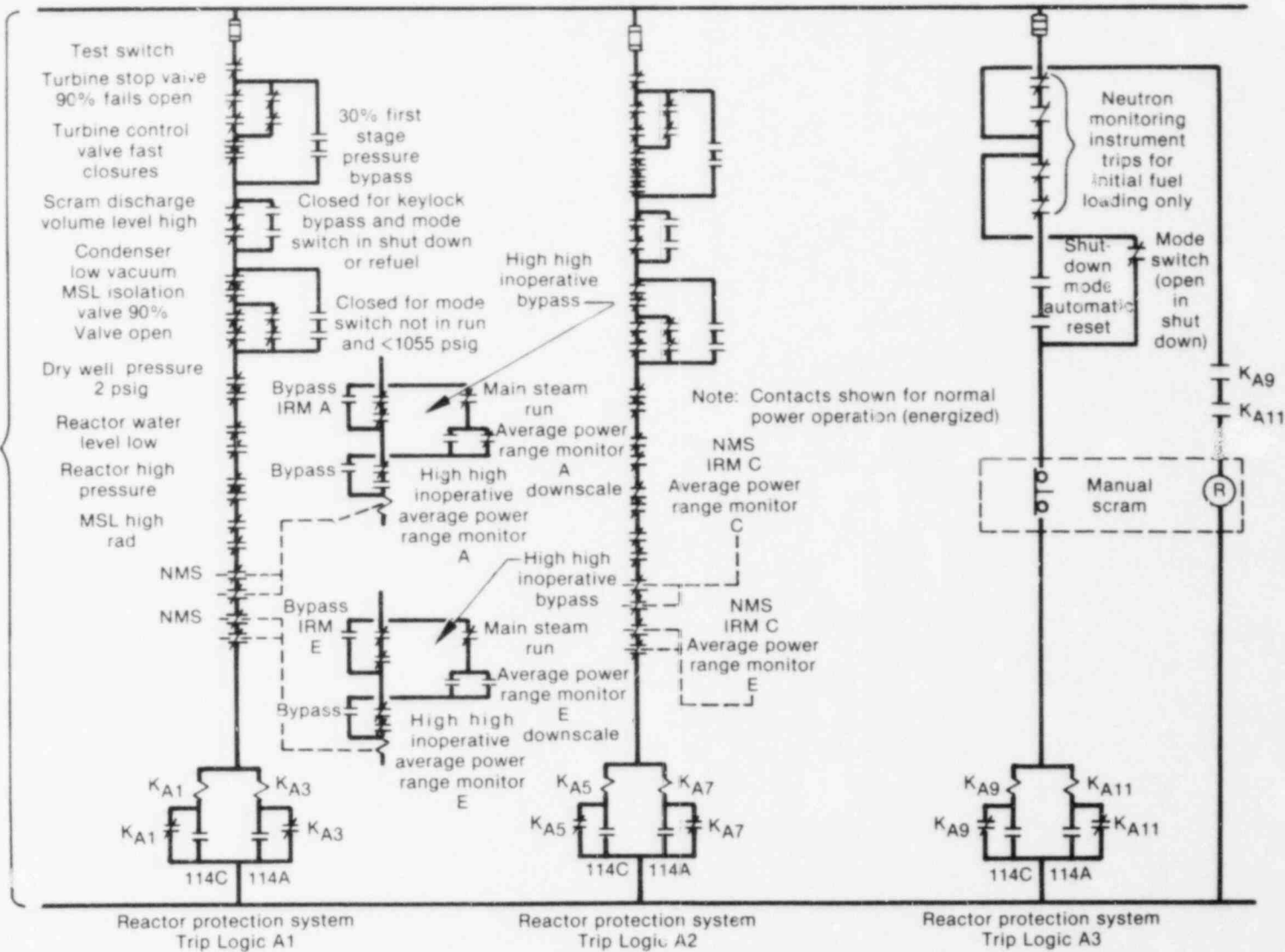
TABLE B-85. RCW SYSTEM FAULT SUMMARY SHORT FORM

Event Name	Event Component	Failure Mode	Primary Failure		
			Failure Rate	Fault Duration (hr)	Error Factor
UVA135UP	Air-operated Valve FCV-24-135	Does not open	3E-4/D	--	3
UVA138UP	Air-operated Valve FCV-24-138	↓	3E-4/D	--	↓
UCK135UP	Check Valve 24-707	↓	1E-4/D	--	↓
UCK138UP	Check Valve 24-730	↓	1E-4/D	--	↓

B-429

B-430

120 V AC RPS Bus A



INEL 2 1614

Figure B-42. RPS Channel A.

3.7.3 Fault Tree

The Browns Ferry RPS is very similar to the Peach Bottom system modeled in WASH-1400 and was, therefore, not analyzed for this report. NUREG-0460 provides the value for failure to achieve subcriticality (3×10^{-5} /demand). This value takes into account RPS failures.

For the majority of accident sequences, no mitigating systems other than the CRDH system required use of the RPS. For one case, transients where the PCS is available and the reactor subcriticality systems fail, the recirculation pump trip requires an input from the RPS. The value used for RPS failure in this case is the 1.9×10^{-6} for common mode failures from WASH-1400. This value was chosen since it represents failures that would disable both the reactor scram systems and recirculation pump trip system.

3.8 Equipment Area Cooling System

3.8.1 Purpose

The EAC system cools the air in a specific location or for a specific component.

3.8.2 System Configuration

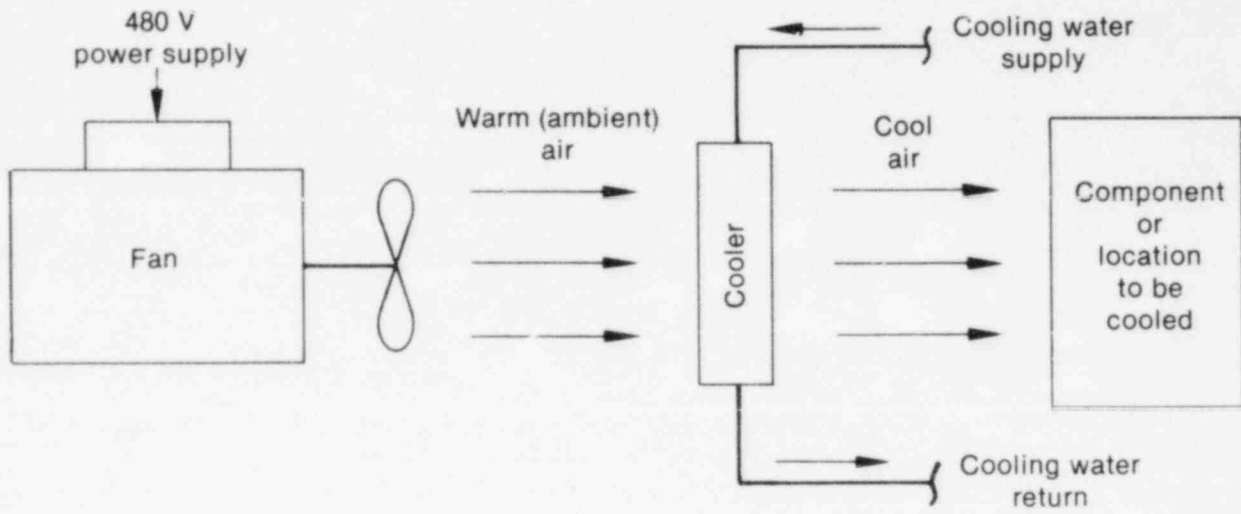
The EAC system is not a system, per se. Nevertheless, in this analysis, the EAC system is considered to be the individual area for, the associated cooler, the cooling water interface to the cooler, and the power supply and control circuit for the fan. Figure B-43 is a simplified diagram of the EAC system.

This analysis determined that the only equipment area cooling systems that were important for correctly modeling front-line system response were those associated with each of the RHR pumps. When these pumps are required to run in the RHR system shutdown cooling or torus cooling modes, the pumps may run for relatively long periods of time. Consequently, lack of area cooling for the pump surroundings will ultimately lead to pump failure. The remaining ECCS pumps run for relatively short periods. Therefore, they do not require EAC for successful operation.

There is a fan for each RHR pump. The A and C RHR pump fans are powered from 480 V RMOV Board 1A. The B and D RHR pump fans are powered from 480 V RMOV Board 1B. The cooling water supply to each of the associated coolers is from either the RCW system during normal plant conditions or the EECW system during abnormal plant conditions.

3.8.3 Fault Tree

There is no fault tree for the EAC system. The EAC system component faults are shown in the appropriate branches of the RHR system fault tree.



INEL 2 1345

Figure B-43. Simplified diagram of EAC system.

4. HUMAN ERROR MODELS AND PROBABILITIES

Initial guidelines for IREP human error analysis suggested that all human error probabilities be assigned a value of 0.1. The intention was to screen the human error interfaces using this value and thereby identify the important human error contributions to system unavailability. Additional emphasis would be placed on these important interfaces, and more sophisticated analytical methods would be used to refine the associated human error probability. Consequently, the system fault trees were originally constructed and evaluated using this screening value for all human error interfaces. As a result, the human errors completely dominated the system unavailabilities and, in most cases, masked any significant hardware contributions. This was unacceptable for several reasons. Engineering judgment identified many of these dominant human errors as unrealistic. In addition, certain hardware contributions were expected to be more important than indicated by the model results. These expectations were derived largely by insights gained during the system analysis that is necessary for model construction. Consequently, the screening method was reevaluated.

In the end, a case-by-case evaluation of each interface was conducted, and screening values of either 0.01 or 0.001 were assigned to each human error interface in the models. The decision as to which value to assign to the interface was largely influenced by general consideration of the human error factors that led to postulation of the human error event in the first place. This second screening method identified several potentially significant human error interfaces and these were analyzed in more detail by supplying the analytical methods suggested in NUREG/CR-1278⁷. The results of these analyses are discussed in this section. Table B-86 summarizes the human error probabilities derived from these analyses. Explanation and use of the associated error factors is discussed in detail in Section 5.3 of Appendix C. Figures B-44 through B-51 depict the human error models used in these analyses. (In the figures, the branch points, called "steps," are designated with the letters "A," "B," "C," etc.)

4.1 Miscalibration Errors

Two significant maintenance activities were identified and analyzed. Errors associated with these maintenance activities could degrade more than one system, which is one reason for their significance.

If reactor level switches (LIS-3-58A through 58D) are miscalibrated, the HPCI, RCIC, RHR (LPCI mode), and core spray systems could be directly affected. Figure B-44 depicts the human error model used to derive a human error probability (HEP) for this event. Table B-87 provides the event descriptions of the level switch model; Box A provides detailed explanations of the assumptions and rationale used to develop the level switch model. The derived value, 2.4×10^{-5} , applies only to one level switch.

We assumed there would be low dependence among the four switches for the common maintenance error. This assumption was based on several observations. The procedure used by the maintenance person (SI 4.2.B-1; see Attachment B), implies that the instruments will be calibrated sequentially. As a result, it was further assumed that the instruments would be calibrated

TABLE B-86. IREP HUMAN ERROR PROBABILITIES

Description	HEP	Error Factor	Human Error Model (Figure Number)
<u>Miscalibration Errors</u>			
1. Maintenance person causes failure of reactor level switches	2.4×10^{-5}	10	B-44
2. Maintenance person causes failure of drywell pressure switches	0.001	10	B-45
<u>Operational Errors</u>			
3. Operator fails to manually depressurize the reactor	0.003	10	B-46
4. Operator fails to transfer RCIC suction to the torus	0.0015	10	B-47
5. Operator fails to manually isolate RCIC pump suction from the CST	0.0045	10	B-48
6. Operator fails to initiate RHRSW cooling	5.5×10^{-4}	10	B-49
7. Operator fails to initiate SBCS	0.005	10	B-50
8. Operator fails to transfer electrical bus to alternate supply	0.001	10	--
9. Operator fails to initiate torus cooling	0.001	10	--
10. Operator fails to initiate shutdown cooling	0.001	10	--
11. Operator fails to manually depressurize the reactor (with recovery)	1.8×10^{-4}	10	B-51

B-436

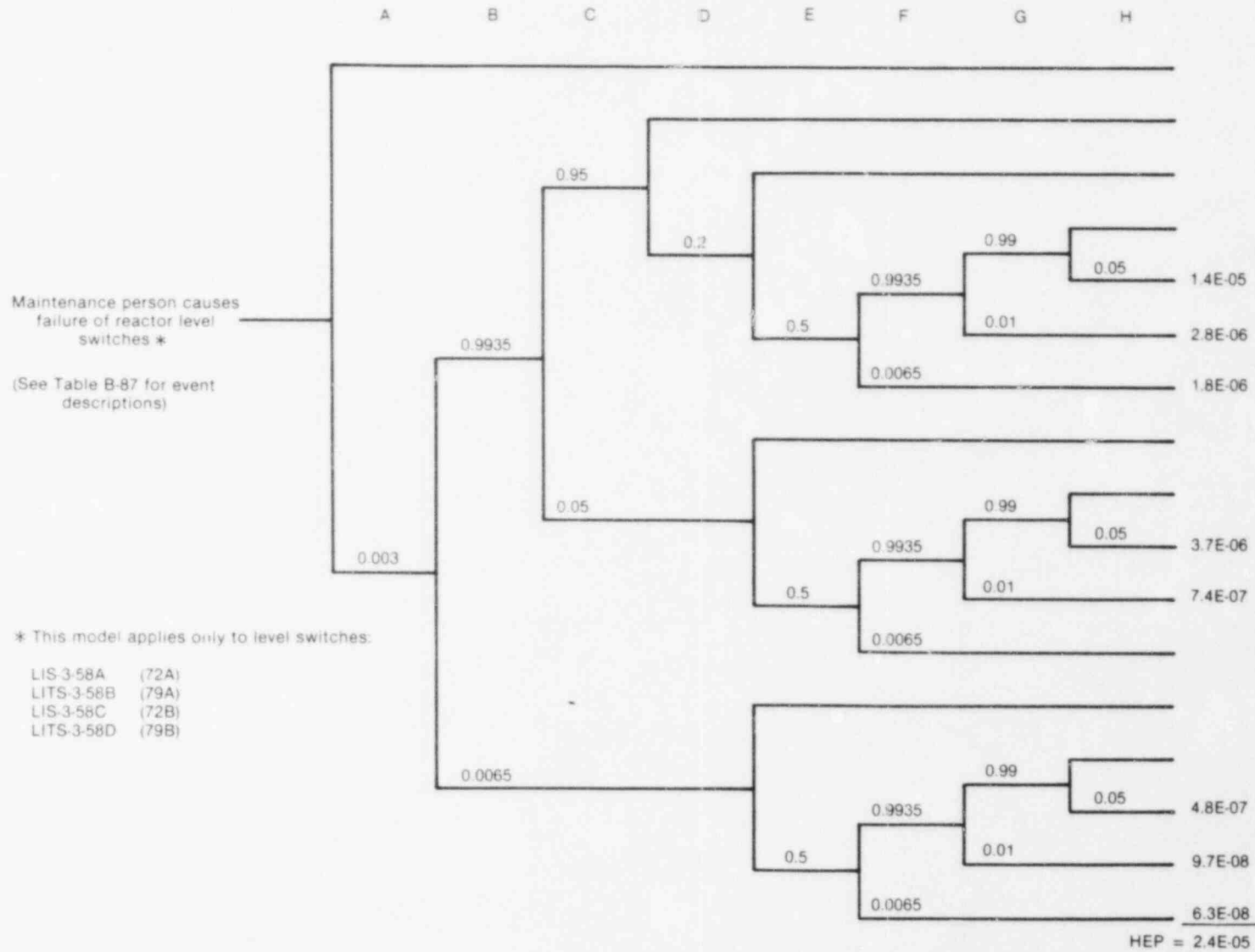
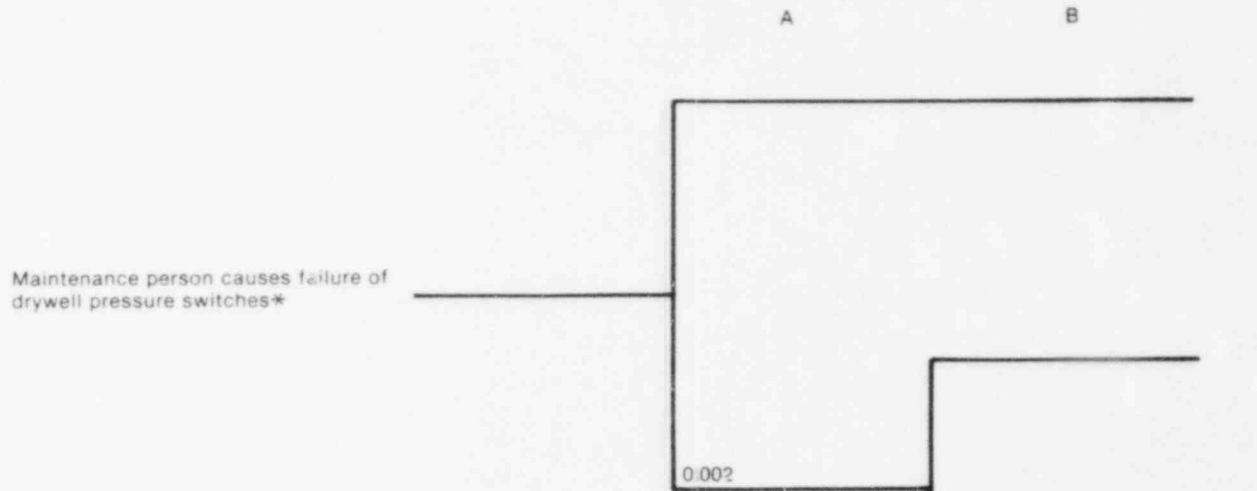


Figure B-44. HEM--maintenance person causes failure of reactor level switches (see Box A).

BOX A. ASSUMPTIONS AND RATIONALE FOR THE LEVEL SWITCH MODEL

1. See Attachment B for relevant procedures (SI 4.2.B-1).
2. Errors of administrative control are not included in the model. It was assumed that the maintenance person would always take the procedure with him to perform the maintenance activity. Whether or not he followed the procedure once he began maintenance activities would still result in the same six steps being critical to successful performance of Step A. An HEP could not be determined that takes into account the maintenance person's ability to return the lineup to normal given memorization to the proper procedure, redundancy of the act, and simplicity of the act. It was assumed that the HEP would not be significantly different from the error probability associated with following a short procedure with no checkoff provisions.
3. Errors of commission on the part of the maintenance person are possible. That is, the maintenance act could damage the instrument. However, these errors would have to be combined with the errors of omission (failure to detect the damaged or improperly aligned instrument) and the model results would essentially remain unchanged. Deliberate acts (sabotage) were not considered.
4. Step E was included in the model because of years of similar experience on the part of the analysts involved in construction of the model. This type of activity is common practice for maintenance personnel anytime components are being returned to service. The procedures do have a step that alludes to this activity (Step 4.47), but Step 4.47 was considered in the complete dependence assumption of Step A. What the analysts are attempting to consider in Step E is "good engineering practice" that comes with many years of experience and will be performed regardless of the existence of a procedure to direct the action be taken. The HEP of 0.5 associated with Step E is probably overly conservative. However, since no guidance could be readily determined from the NUREG, this HEP was considered appropriate.
5. Steps B, E, and F are considered to be recovery factors.
6. It was assumed that there is zero dependence between operators and maintenance persons. This is primarily because they are physically separated during their activities. The same assumption was used for dependence between the maintenance persons and the assistant shift engineer. Zero dependence was also assumed between the assistant shift engineer and the operator, because it was assumed that the assistant shift engineer's activities were normally external to the control room and he would only enter the control room to make specific checks that would in no way technically involve the operator.



A. Maintenance person fails to correctly return pressure switch to normal.

Significant factors: 1. Short list
2. With checkoff provisions

HEP source: ** Table 20-20, page 20-29, (with checkoff provisions, short list), items 1 and 4

HEP value: Short list - 0.001
improperly used checkoff provisions - 0.003
 $\bar{x} = 0.002$

B. Maintenance person fails to verify that the instrument is valved in properly.

Significant factors: 1. Low dependence with rest of procedure
2. Strictly a judgment HEP by the analyst

HEP source: ** 1. Page 15-2, second paragraph
2. Engineering judgment

HEP value: 0.5

* This model applies only to pressure switches:

- PS-64-58A (101B)
- PS-64-58B (101A)
- PS-64-58C (101D)
- PS-64-58D (101C)

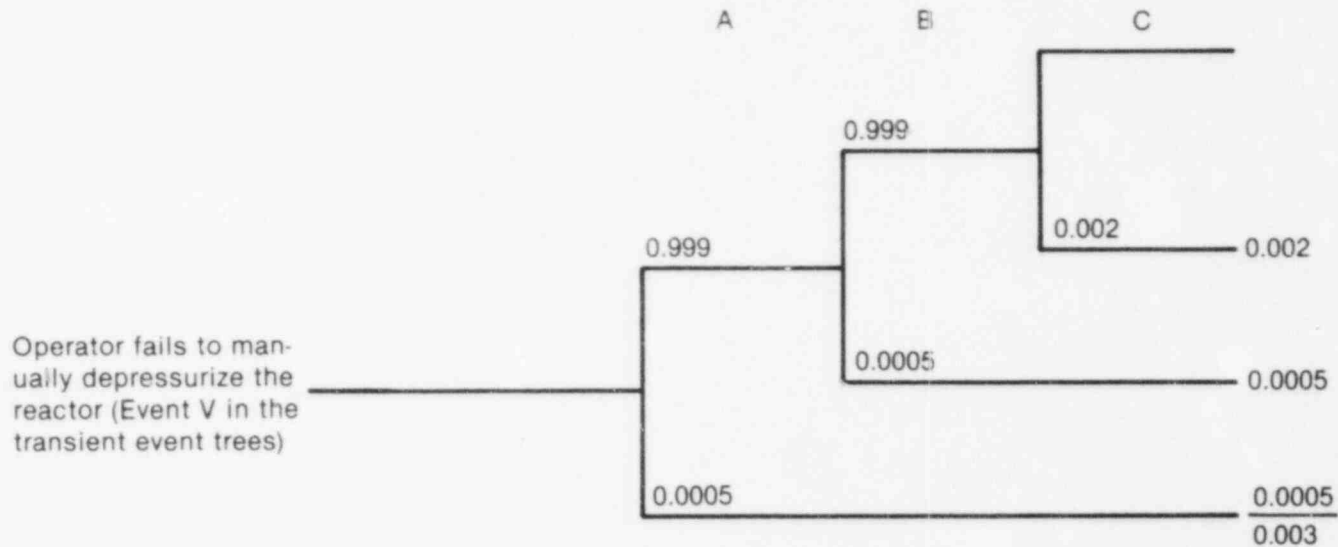
** HEP source of information is NUREG/CR-1278.

INEL 2 1616

Figure B-45. HEM--maintenance person causes failure of drywell pressure switches (see Box B).

BOX B. ASSUMPTIONS AND RATIONALE FOR THE DRYWELL PRESSURE SWITCH MODEL

1. See Attachment C for relevant procedures (SI 4.2.B-5 and IMI-202).
2. Errors of administrative control were not considered in this model for the same reasons as discussed in Remark 2 of Box A.
3. Errors of commission on the part of the maintenance person are possible. However, the model results would remain essentially the same if these errors were considered. See Remark 3 of Box A for further explanation.
4. Step B was put in the model to allow for "good engineering practice." Remark 4 of Box A discusses this HEP in detail.
5. There are few chances for recovery once this maintenance error has been committed. The assumption is that "normal" indication of drywell pressure in the control room is usually zero. Also, an additional assumption is that the limiting maintenance error would be one that resulted in a zero output from the drywell instruments. Therefore, the maintenance person would always be responsible for any recovery actions.



A. Shift supervisor fails to recognize need to depressurize.

- Significant factors:
1. Will fail to make a correct response with an HEP of 0.0001
 2. Plant is in transient condition
 3. Moderately high stress; dynamic task

HEP source: * Page 10-9; and Table 20-23, pg. 20-32
 HEP value: $0.0001 \text{ (pg. 10-9)} \times 5 \text{ (pg. 20-23)} = 0.0005$

B. Operator fails to follow correct procedure.

- Significant factors:
1. Oral instruction to depressurize
 2. Only one item to recall
 3. Also recognizes need to depressurize

HEP source: * Table 20-15, pg. 20-23, item 2
 HEP value: 0.0005 (lower bound)

C. Operator selects wrong controls.

- Significant factors:
1. Functionally grouped set of controls
 2. Moderately high stress
- HEP source: * Table 20-13, pg. 20-19, item 2; and Table 20-23, pg. 20-32, item 3
 HEP value: $0.001 \text{ (pg. 20-19)} \times 2 \text{ (pg. 20-32)} = 0.002$

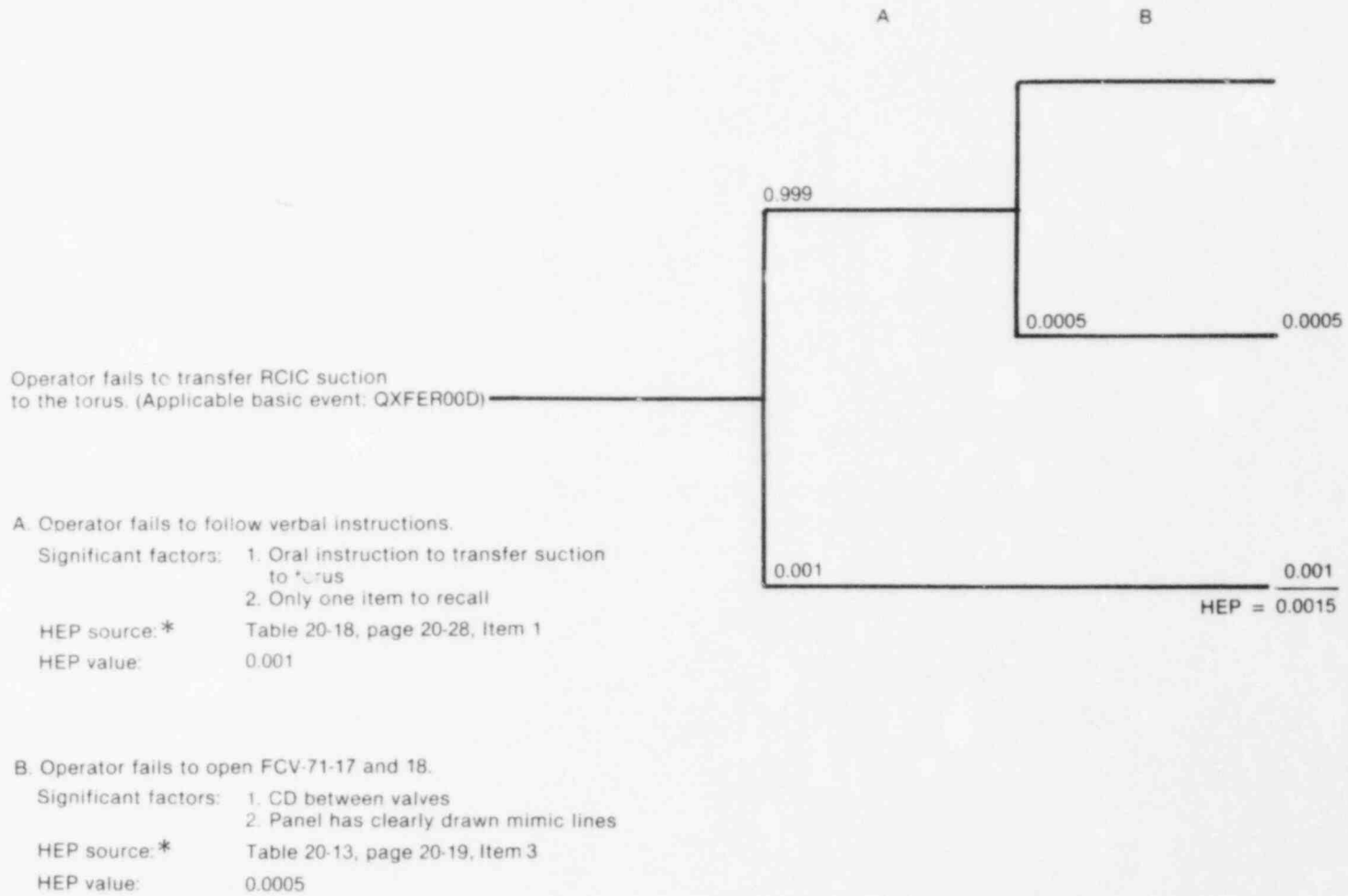
*HEP source of information is NUREG/CR-1278.

Figure B-46. HEM--operator fails to manually depressurize the reactor (see Box C).

BOX C. ASSUMPTIONS AND RATIONALE FOR THE MANUAL DEPRESSURIZATION MODEL

1. The intent of Step A is to account for the probability that the shift supervisor may not recognize the need to manually depressurize the plant. The operators will probably not depressurize without the shift supervisor's orders. Therefore, the decision by the shift supervisor to give the order to depressurize could be critical. For this event, the plant is considered to be in a transient condition. This assumption follows from the fact that manual depressurization (Event V) is shown in the transient event trees. In addition, it is assumed that the shift supervisor will be performing under moderately high stress due to the transient condition and also due to the nature of the critical decision he must make. A stress multiplier of five is used because it is assumed that there is dynamic interplay between the shift supervisor and system indications.
2. Step B accounts for the probability that the operator will fail to take steps to depressurize the reactor, given he has been ordered to do so by the shift supervisor. It is assumed that only one oral instruction to depressurize the plant will be given. Therefore, the operator will only have to recall one item. This HEP also is recommended for quantifying failure to initiate a task, which is also implied by this step. The lower bound for the HEP was picked for several reasons. The operator will probably be aware of the need to depressurize and only be awaiting orders. In addition, once given the orders, it is unlikely that he will fail to carry them out, due to the critical nature of the action. The operator will also be aware that the shift supervisor will probably be closely monitoring his actions, so he will be less likely to forget to carry out the task.
3. Even though the operator fully intends to carry out the order, there is still a likelihood that the wrong controls will be selected for the task. Step C accounts for this probability. The controls for manually depressurizing the reactor are assumed to be arranged in a functionally grouped set. Like the shift supervisor, the operator is also assumed to be under moderately high stress for similar reasons. However, in the case of the operator, there will be only one action to carry out and that is to open the relief valve(s). Since the only operator action required is to manually open the relief valve(s), it is assumed that this will be a memorized action and no step-by-step procedure will be required. It is also assumed, at least for purposes of depressurizing the reactor, that there will be no dynamic interaction between the operator and the system indications. This is due to the simple nature of the procedure. Consequently, a stress factor of 2 is used rather than a factor of 5.

B-442



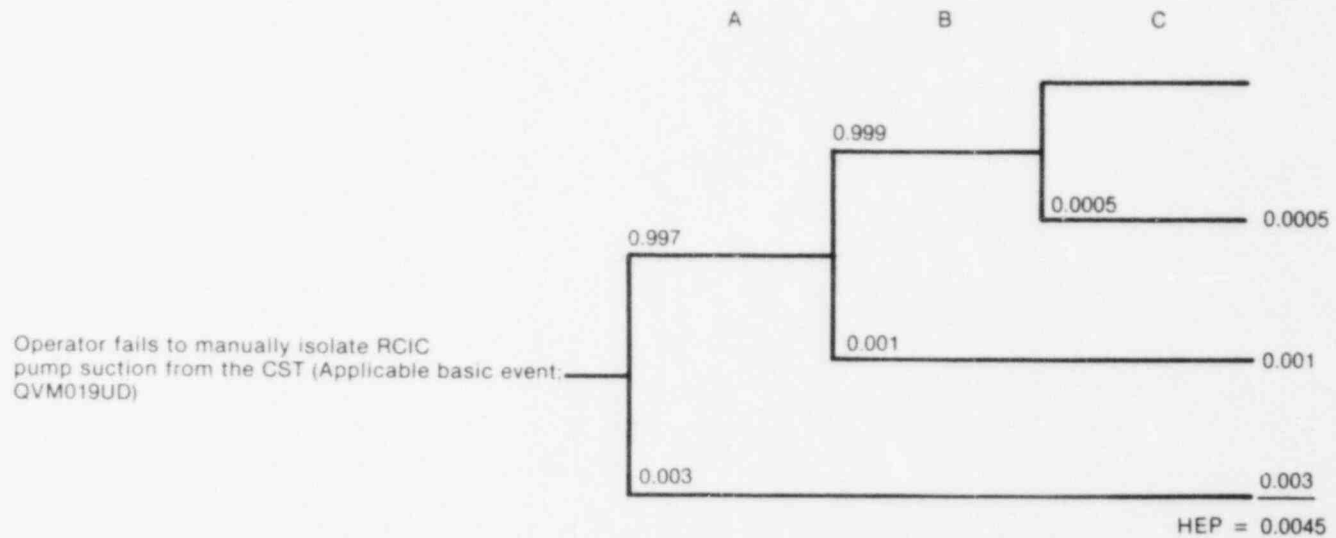
*HEP source of information is NUREG/CR-1278.

INEL 2 1618

Figure B-47. HEM--operator fails to transfer RCIC suction to the torus (see Box D).

BOX D. ASSUMPTIONS AND RATIONALE FOR THE RCIC SUCTION TRANSFER MODEL

1. Based on the results of engineering analyses performed by TVA (FSAR, Appendix Q), it is assumed that this operator action will not be required for at least 8 hours following the transient. Consequently, it is assumed that the operator will be performing under optimum stress conditions. It should be noted that the overall risk assessment assumes that the RCIC system will not require suction transfer during LOCA conditions; therefore, the LOCA stress factors do not apply for this human error model.
2. Step A reflects the probability that the operator fails to follow verbal instructions to initiate RCIC suction transfer. The assumption is that the shift supervisor will always make this decision and that the suction transfer will not take place without the authorization of the shift supervisor. There should also be adequate time for the shift supervisor to make this decision. It is further assumed that only a single order to transfer RCIC suction to the torus will be given to the operator. Consequently, the operator will only have one item to recall.
3. Once the operator decides to transfer RCIC suction, there are two valves he must open: FCV-71-17 and 18. Since this is a straight forward and simple action, it is assumed that no written procedure is necessary, and the operator can easily perform the action from memory. However, the operator could select the wrong valves to operate. This possibility is shown in Step B. Complete dependence is assumed between FCV-71-17 and 18 because their controls are both located on the same panel and adjacent to each other. In addition, mimic lines clearly indicate their function. Consequently, it is assumed they will be operated as a pair, as intended by design, and their operation will be completely dependent.



A. Operator checks wrong indicator lamp.

Significant factors: 1. Array of lamps

HEP source: * Table 20-7, page 20-12, Item 8

HEP value: 0.003

B. Operator misinterprets the indication on the indicator lamp.

Significant factors: None

HEP source: * Table 20-7, page 20-12, Item 9

HEP value: 0.001

C. Operator fails to shut FCV-71-19.

Significant factors: 1. Clearly drawn mimic lines

HEP source: * Table 20-13, page 20-19, Item 3

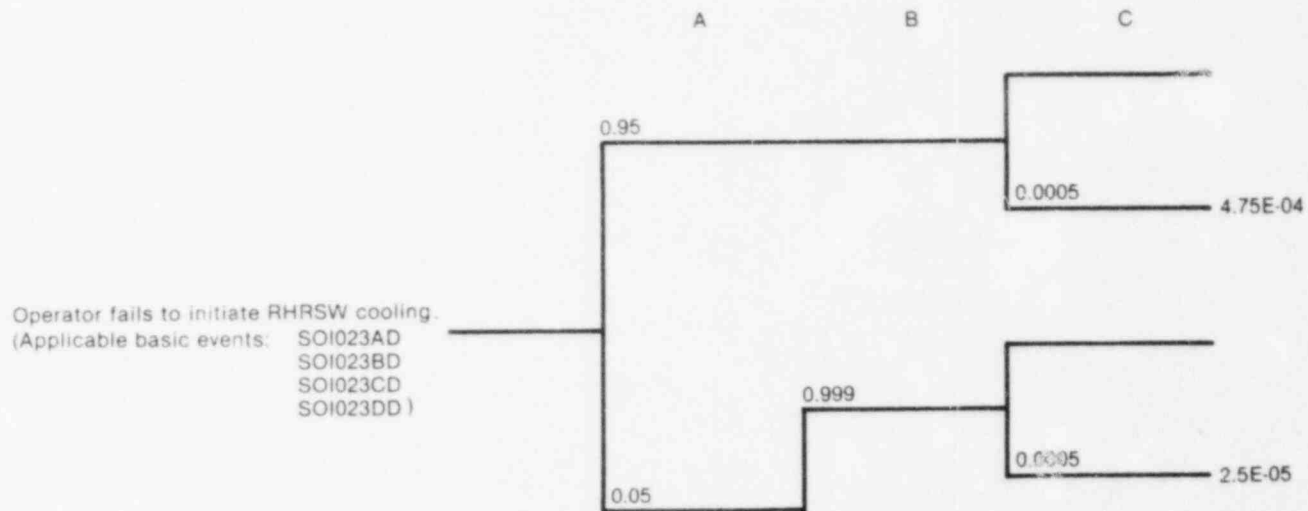
HEP value: 0.0005

*HEP source of information is NUREG/CR-1278.

Figure B-48. HEM--operator fails to manually isolate RCIC pump suction for the CST (see Box E).

BOX E. ASSUMPTIONS AND RATIONALE FOR THE RCIC SUCTION ISOLATION MODEL

1. Optimum stress is assumed in this model for the reasons discussed in Box D, Remark 1.
2. This action is required upon transfer of RCIC pump suction. Normally, FCV-71-19 will close automatically. However, if automatic closure fails, the operator can still override the failed automatic circuit and manually close the valve. This model is intended to quantify failure to perform the manual closure of the valve.
3. Since the operator's cue to perform this task is the manual transfer of RCIC suction, it is assumed that the operator will initiate this task when he is shifting suction and he notices that FCV-71-19 does not close when FCV-71-17 and 18 are opened. However, there is a possibility that the operator could check the wrong position indicator lamp out of the array of indicator lamps on the RCIC mimic board. This is reflected in Step A.
4. It is also possible that the operator could check the correct position indicator lamp but misinterpret the lamp as indicating the valve is closed when, in fact, the valve is open. Step B depicts this probability.
5. Finally, given that the operator recognizes the need to close the valve by correct interpretation of FCV-71-19 valve position indication, there is still a possibility that he will operate the wrong valve. Step C shows this probability.
6. Again, due to the simplicity of the required procedure, it is assumed that the correct procedure is memorized by the operator and no written procedure for this action is require.



A. Operator fails to initiate RHRSW cooling in accordance with EOI-36 at 30 minutes following the initiating event.

Significant factors: 1. Nonpassive control room task
 HEP source: * Table 14-3, page 14-12, Item 4
 HEP value: 0.05

B. Operator fails to respond to annunciator at 40 minutes following the initiating event.

Significant factors: 1. Annunciators functionally grouped
 2. Transient or LOCA in progress; therefore, interruptions and distractions
 HEP source: * Page 10-9, page 10-11
 HEP value: 0.0001 (page 10-9) X 10 (page 10-11) = 0.001

C. Operator selects wrong pump and valve controls.

Significant factors: 1. CD between corresponding pump and valve controls
 2. Clearly drawn mimic lines
 HEP source: * Table 20-13, page 20-19, Item 3
 HEP value: 0.0005

HEP = 5.5E-04

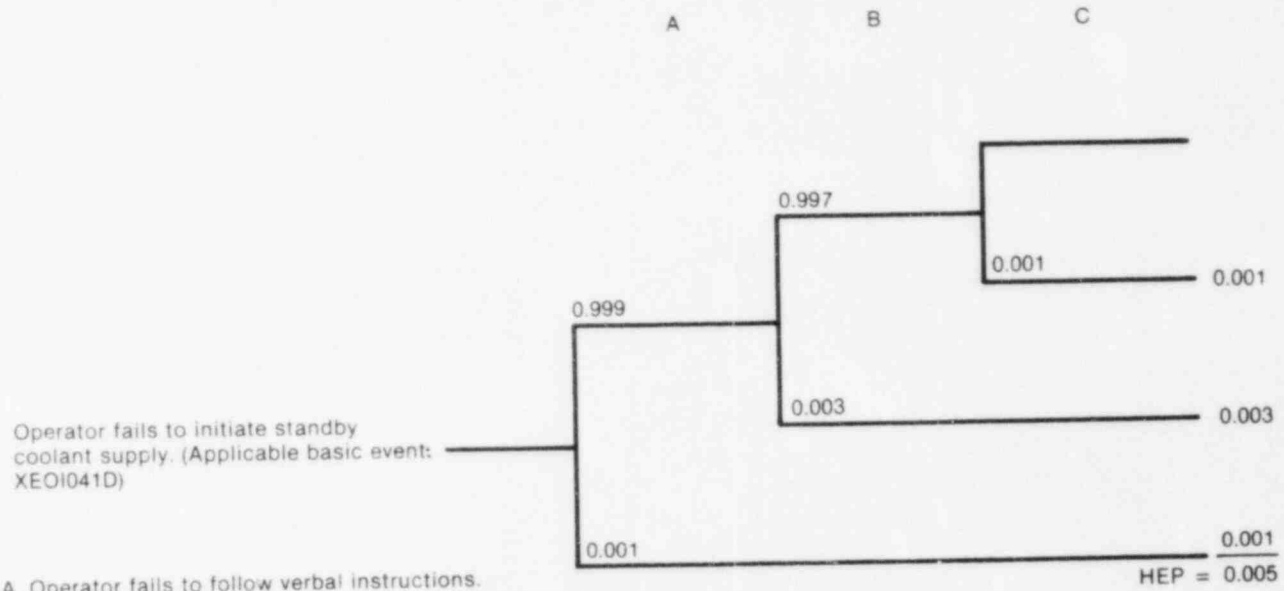
INEL 2 1620

* HEP source of information is NUREG/CR-1278.

Figure B-49. HEM--operator fails to initiate RHRSW cooling (see Box F).

BOX F. ASSUMPTIONS AND RATIONALE FOR THE RHRSW COOLING INITIATION MODEL

1. Step A depicts the probability that the operator will not initiate RHRSW cooling 30 min from the initiation of the transient or LOCA event. Major assumptions here are that the operator will be required to perform this task by EOI-36, but due to the nature of the initiating event, he is likely not to use EOI-36 and, therefore, not be aware of the requirement for RHRSW until he receives a suppression pool high temperature alarm approximately 40 min subsequent to the initiating event.
2. Even though the high temperature alarm sounds, the operator may still fail to respond. In this case, there are probably many other interruptions and distractions taking place, which could increase the likelihood of the operator ignoring the alarm. This is indicated by Step B.
3. If the operator follows the correct procedures or responds to the high temperature alarm, he may still operate the wrong RHRSW pump and valve controls. Both the pump and valve controls are located in proximity on the RHRSW mimic panel. Therefore, complete dependence is assumed between the pump and valve controls. That is, the assumption is if the operator fails to operate one RHRSW control he will fail to operate any of the RHRSW controls.



- A. Operator fails to follow verbal instructions.
 Significant factors: 1. Will be ordered by shift supervisor to initiate standby coolant supply
 2. Only one item to recall
 HEP source:* Table 20-18, page 20-28, Item 1
 HEP value: 0.001
- B. Operator fails to correctly follow written procedures (EOI 41).
 Significant factors: 1. Short list; no checkoff provisions
 2. Experienced person; step-by-step task
 HEP source:* Table 20-20, page 20-29, Item 4
 HEP value: 0.003
- C. Operator selects wrong controls.
 Significant factors: 1. Functionally grouped set of controls
 HEP source:* Table 20-13, page 20-19, Item 2
 HEP value: 0.001

INEL 2 1621

*HEP source of information is NUREG/CR-1278.

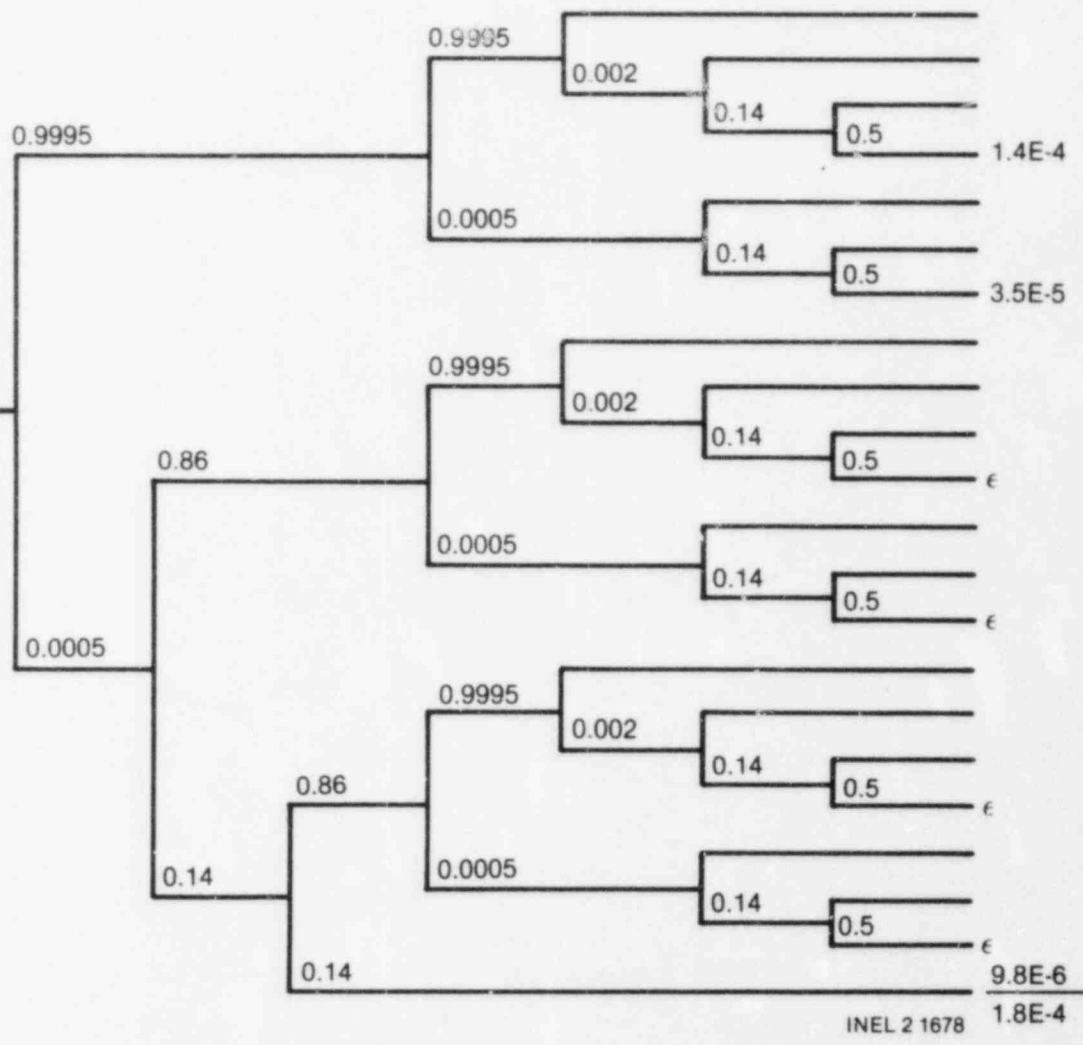
Figure B-50. HEM--operator fails to initiate SBCS (see Box G).

BOX G. ASSUMPTIONS AND RATIONALE FOR THE SBCS INITIATION MODEL

1. It is assumed that many hours or even days will have passed before it is necessary to carry out this operation. Therefore, there should be no recognition error as the need to initiate SBCS is concerned. There should be many people on hand to recognize that need and give the order to initiate SBCS, if necessary.
2. Stress, on the part of the operator, will probably be moderately high, due to the nature of the act he is about to perform (i.e., pump river water into the reactor vessel). However, it is assumed that as long as his actions can be monitored, stress errors will be minimized by direct and concentrated supervision.
3. Step A is the failure of the operator to follow orders to initiate SBCS. It is assumed that stress errors are counteracted by close supervision. Only a single order will be given to initiate SBCS in accordance with EOI-41.
4. Step B shows the likelihood of the operator omitting a step in the written procedure for this action (see Attachment D for the relevant procedure, EOI-41).
5. It is assumed that the controls for SBCS initiation are functionally grouped on the RHRSW control panel. The operator error of selecting the wrong controls once he has read the procedure is depicted by Step C. Again, stress errors are assumed to be minimized by close supervision. Due to the simplicity of the procedure and the proximity of the SBCS coolant supply system controls, complete dependence is also assumed for operation of these components.

A B C D E F G

Operator fails to manually depressurize the reactor (with recovery)
(Event V in the transient event trees)



B-450

Figure B-51. HEM--operator fails to manually depressurize the reactor (with recovery) (see Box H and Table 88).

BOX H. ASSUMPTIONS AND RATIONALE FOR THE MANUAL DEPRESSURIZATION MODEL
(WITH RECOVERY)

1. It is assumed that this human action will not take place until approximately 40 min subsequent to the initiating event. Therefore, it is further assumed that the shift supervisor and two operators will be present in the control room.
2. It is assumed that there is a moderate level of dependence between the shift supervisor and each of the two operators. A high level of dependence is assumed between the two operators.
3. Where applicable, when the operator or shift supervisor recognizes that an error has been made, it is assumed that full recovery will take place. That is, the error will not be repeated.

TABLE B-87. EVENT DESCRIPTIONS FOR THE LEVEL SWITCH MODEL

Event	Significant Factors	HEP Source ^a	HEP Value
A. Maintenance person fails to correctly return the level instrument to service	Six steps in procedure with complete dependence No checkoff provided	Table 20-20, Page 20-29, Item 4 (no checkoff provisions; short list)	0.003
B. Maintenance person fails to notify operator	Long list With checkoff provisions	Table 20-20, Page 20-29, Items 2 and 5 (with checkoff provisions; long list)	Long list--0.003 Improperly used checkoff provisions--0.01 $\bar{x} = 0.0065$
C. Operator fails to verify correct level	Not required by procedure Could be busy with other concerns	Table 20-22, Page 20-31, Item 1 (carry out a plant policy when there is no check on a person)	0.05 (upper bound)
D. Operator reads/interprets level incorrectly	Analog meter with no limit marks Just skims meters; no written material to tell him what to look for	Table 15-1, Page 15-3. Item 2 (usual monitoring without written materials)	0.2
E. Maintenance person fails to verify that the instrument is valved in properly	Low dependence with rest of procedure Strictly a judgment HEP by the analyst	Page 15-2, second paragraph Engineering judgement	0.5
F. Maintenance person fails to notify the assistant shift engineer when maintenance is complete	Long list With checkoff provisions	Same as B. above	0.0065
G. Assistant shift engineer fails to verify correct level	Not required by procedure Not busy with other concerns	Same as C. above	0.01
H. Assistant shift engineer reads/interprets level incorrectly	Short-term, one-of-a-kind check Supervisor checking performance of maintenance person	Table 20-9, Page 20-14, Item 3 (special short-term, one-of-a-kind checking)	0.05

a. HEP information source is NUREG/CR-1278.

in approximately the same time frame (i.e., all in one shift or on consecutive shifts). Thus, the final assumption was that these instruments must have some level of dependence for this maintenance error, and that level of dependence was judged to be "low." These switches are also arranged in a one-out-of-two-twice logic; thus, one of two pairs of switches must fail in order to fail the level circuit; specifically, Switches 58A and 58C must fail together or 58B and 58D must fail together.

Given the independent value, 2.4×10^{-5} , for failure of a level switch, and using the NUREG/CR-1278 (Page 7-30) formula for low dependence among the level switches, the probability that the maintenance person causes failure of the level circuit is:

$$P(58C|58A|LD) = \frac{1 + 19(2.4 \times 10^{-5})}{20} = 0.05$$

$$P(58D|58B|LD) = 0.05,$$

therefore

$$P(58A \text{ and } 58C|LD) = 0.05 (2.4 \times 10^{-5}) = 1.2 \times 10^{-6},$$

and

$$P(58B \text{ and } 58D|LD) = 1.2 \times 10^{-6}.$$

Since failure of either pair will fail the circuit, the joint probability of circuit failure given low dependence among the four level switches is:

$$P(\text{circuit failure}|LD) = 2(1.2 \times 10^{-6}) = 2.4 \times 10^{-6}.$$

This value (2.4×10^{-6}) is the HEP used in the associated fault trees to account for this miscalibration error. The associated basic event code is OPSLLVLX.

If drywell pressure switches (PS-64-58A through 58D) are miscalibrated a similar problem ensues. Figure B-45 depicts the human error model used to derive an HEP for this event; Box B provides detailed explanations of the assumptions and rationale used to develop the drywell pressure switch model. Again, the derived value (0.001) represents the HEP for just one switch. Unlike the level switch model, there are few chances for recovery once the error has been committed. This is because we assumed the pressure indication in the control room is normally zero for drywell pressure; therefore, the personnel in the control room would be unable to detect a valve misalignment or miscalibration error. We assumed these errors would always result in a zero-pressure indication in the control room. Thus, the maintenance person would always be solely responsible for any recovery actions.

We assumed moderate dependence among the four pressure switches for the common maintenance error. This assumption was based on several observations. The procedure used by the maintenance person (SI 4.2.B-5; see

Attachment C), implies that the sensors can be calibrated sequentially. However, unlike the level sensors discussed for Figure B-44, the drywell pressure sensors are all covered under this one procedure rather than by independent procedures. It was further assumed that the instruments would be calibrated in approximately the same time frame (i.e., all in one shift or on consecutive shifts). Thus, the final assumption was that these instruments exhibit a higher level of dependence than the level switches, and that level of dependence was judged to be "moderate." These switches are also arranged in one-out-of-two-twice logic. Thus, paired failure must occur in order for circuit failure to occur; specifically, Switches 58A and 58B must fail together, or 58C and 58D must fail together.

Given the independent value, 0.001, for failure of a pressure switch, and using the NUREG/CR-1278 formula for moderate dependence among the pressure switches, the probability that the maintenance person causes failure of the drywell pressure circuit is:

$$P(58B|58A|MD) = \frac{1 + 6(0.001)}{7} = 0.144,$$

and

$$P(58D|58C|MD) = 0.144,$$

therefore,

$$P(58A \text{ and } 58B|MD) = 0.001 \times 0.144 = 1.44 \times 10^{-4},$$

and

$$P(58C \text{ and } 58D|MD) = 1.44 \times 10^{-4}.$$

Since failure of either pair will fail the circuit, the joint probability of circuit failure given moderate dependence among the four drywell pressure switches is:

$$P(\text{circuit failure}|MD) = 2(1.44 \times 10^{-4}) = 2.9 \times 10^{-4}.$$

This value, 2.9×10^{-4} , is the HEP used in the associated fault trees to account for this miscalibration error. The associated basic event code for this error is OPSDWHPX.

4.2 Operational Errors

Eight significant operator responses were identified and analyzed for accident sequences where manual intervention of the operator was necessary for system success. These responses are modeled in Figures B-46 through B-51. Boxes C through H correspond, respectively, to these figures and explain the assumptions and rationale used to develop the models. Table B-88 lists the event descriptions associated with the manual depressurization model that considers recovery actions (see Figure B-51). There are no human error models and, consequently, no figures for the electrical bus transfer, torus cooling initiation, and shutdown cooling initiation

TABLE B-88. EVENT DESCRIPTIONS FOR THE MANUAL DEPRESSURIZATION MODEL
(With Recovery)

Event	Significant Factors	HEP Source ^a	HEP Value
A. Shift supervisor fails to recognize need to depressurize	Same event as Event A in Figure B-46	Same event as Event A in Figure B-46	Same event as Event A in Figure B-46
B. First operator fails to recognize need to depressurize	Moderate level of dependence	Page 17-24 and 25; Table 20-1, Page 20-6; Item 7	0.14
C. Second operator fails to recognize need to depressurize	Moderate level of dependence	Page 17-24 and 25; Table 20-1, Page 20-6; Item 7	0.14
D. Operator fails to follow correct procedure	Same event as Event B in Figure B-46	Same event as Event B in Figure B-46	Same event as Event B in Figure B-46
E. Operator selects wrong controls	Same event as Event C in Figure B-46	Same event as Event C in Figure B-46	Same event as Event C in Figure B-46
F. Shift supervisor fails to recognize error	Moderate level of dependence	Page 17-24 and 25; Equation 7-16, Page 7-30	0.14
G. Second operator fails to recognize error	High level of dependence	Page 17-24 and 25; Equation 7-17, Page 7-30	0.5

a. HEP information source is NUREG/CR-1278.

B-455

HEPs (Items 8, 9, and 10 in Table B-86). These HEPs were estimated using engineering judgement and the RHRSW initiation model (Figure B-49) as a basis for the estimated value. This is further discussed in Section 4.2 of Appendix A.

The logic associated with development of the remaining models, as well as the models discussed above, is explained in detail on each figure and in the associated tables and boxes. Further insight into some of the models can be gained by referring to Section 4 of Appendix A.

4.3 Recovery Model

The latter stages of this risk assessment determined that the human error of failing to manually depressurize the reactor was a potentially significant event. However, the analysts recognized that the human error model for this event did not consider any recovery actions (see Figure B-46 and Box C). Normally, a recovery factor was simply applied to the HEP to allow for recovery. However, in this case, the analysts judged that a specific human error model for failure to manually depressurize the reactor, which took recovery into account, would be appropriate. Figure B-51 is the resulting model. Table B-88 provides the explanation for the figure.

The consideration of recovery reduced the probability estimate for the manual depressurization Event V from 0.003 to 1.8×10^{-4} , i.e., by a factor of 0.06. Thus, 0.06 is used as the corresponding recovery factor in Appendix C, Section 4.2.7.

4.4 Relevant Procedures

Various Browns Ferry procedures were used to conduct the human error analyses. Relevant sections of these procedures are included verbatim in Attachments B through D.

5. GENERIC CONTROL CIRCUIT ANALYSES

5.1 Introduction

Detailed fault tree models were developed for BFl's front-line and support systems required for accident mitigation. Not surprisingly, these systems contain a large number of motor-operated valves and motor-driven pumps to accomplish their intended functions. Schedule constraints prohibited developing a detailed fault model for the motor control circuits for each and every pump and valve encountered in these systems. Instead, a representative control circuit for both motor-operated valves and motor-driven pumps was analyzed, which resulted in a generic control circuit failure rate that varied only by the consideration of how often the circuit was tested for operability.

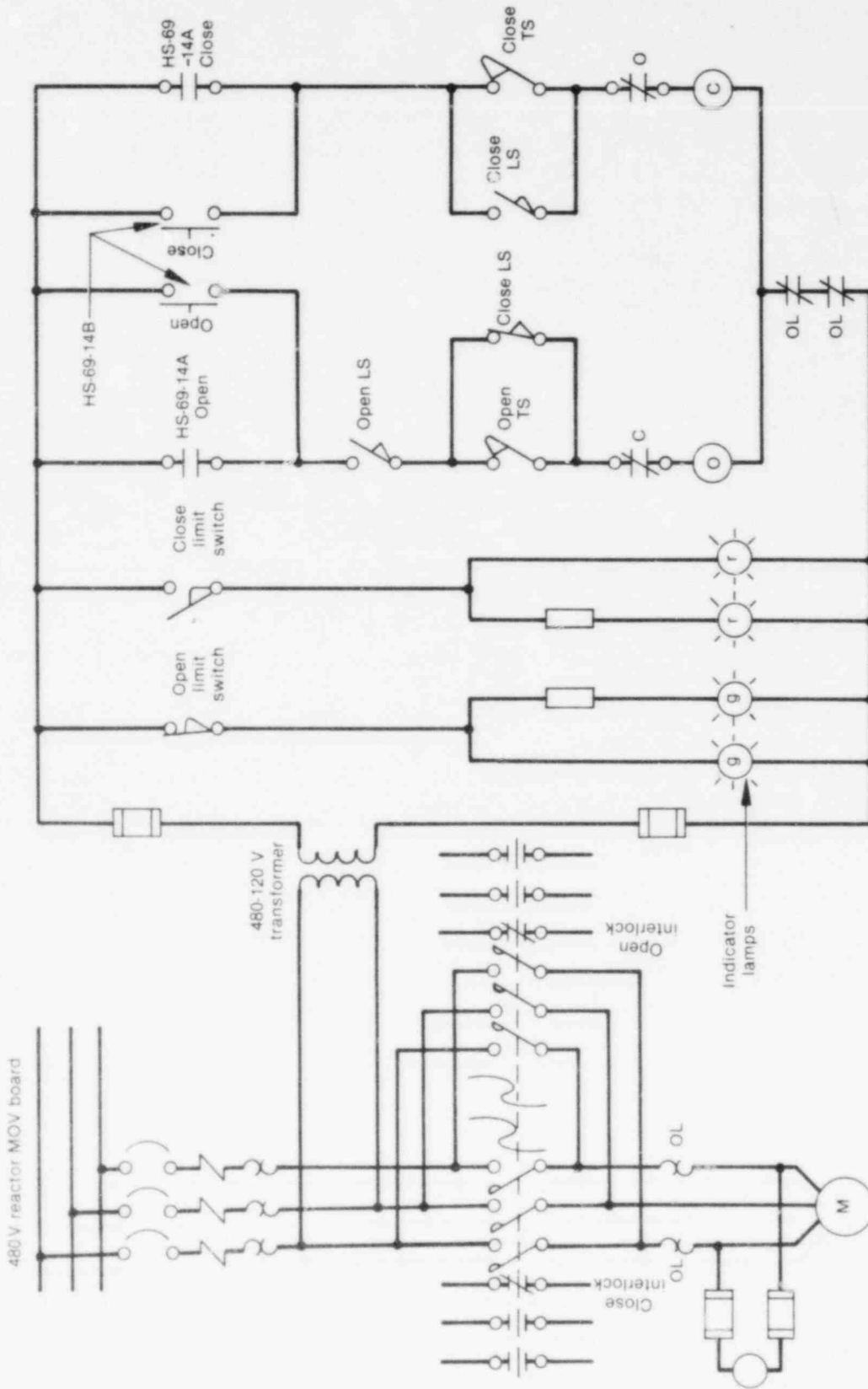
Thus, for each valve and pump considered in the fault tree models, contributions to the unavailability of that component, e.g., a motor-operated valve failing to open, were composed of local faults and no power supplied to the motor from its respective bus. Local faults included "valve fails to open" (VM ___ P), "value fails to close" (VM ___ N), and "no output" (CH ___ G) from the associated motor control circuit to reposition the valve even though a manual or automatic safeguards actuation signal had been received by the motor control circuit.

5.2 Generic Motor-Operated Valve Control Circuit

Figure B-52 is a representative motor control circuit for a valve that may be positioned open or closed. Basically, the open and close relays control contacts that reverse phases to the motor in order to drive the valve open or shut. Limit switches are used to interrupt power to the relays when the valve has reached the full-open or full-closed position. Power for the control circuit is obtained by a 480 to 120 V AC stepdown transformer off the main supply to the motor. Fuses provide control circuit protection in the event of short circuits. Thermal overload devices also protect the motor by interrupting the open and close relay circuit paths in the event of motor overheating due to excessive current flow.

Table B-89 lists these basic design features and the failure modes associated with these components that could prevent the control circuit from providing the correct output to the open and close motor-phase contacts. For this example, it is assumed that the valve is being commanded to open either by a manual switch or by contacts associated with some automatic safeguards actuation signal. The failure-to-close condition would be similar.

Also shown in Table B-89 are the associated failure rates for the failure modes considered. Some of these are expressed in failures per demand, while others are expressed as failures per hour. The unavailability for the control circuit can be expressed as the sum of the demand (D) contributions and hourly contributions:



FCV-69-14 Reactor water cleanup restricting orifice bypass MOV
 FCV-69-8 Reactor water cleanup filter and demin system bypass MOV

LS Limit Switch
 TS Torque Switch
 HS Hand Switch
 OL Overload

INEL 2 1622

Figure B-52. Motor-operated valve-control circuit.

TABLE B-89. MOTOR-OPERATED VALVE GENERIC CONTROL CIRCUIT

Component	Failure Mode	Number (N)	Failure Rate (λ)	$N\lambda$
Switch contacts (open or close)	Fail to close	1	1E-7/hr	1E-7/hr
Circuit wiring	Open	--	3E-6/hr	3E-6/hr
	Short to ground	--	3E-7/hr	3E-7/hr
Transformer	Open	1	1E-6/hr	1E-6/hr
	Short		1E-6/hr	1E-6/hr
Fuses	Open	2	1E-6/hr	2E-6/hr
Limit switch	Fails to operate	1	3E-4/D	3E-4/D
Overload contacts	Open	2	1E-7/hr	2E-7/hr
"Close" relay	Short to power	1	1E-8/hr	1E-8/hr
"Open" relay	Does not energize	1	1E-4/D	1E-4/D
"Close" relay contact	Open	1	1E-7/hr	1E-7/hr

Sum of demand rates = 4E-4/D.				
Sum of hourly rates = 7.7E-6/hr.				

$$\bar{A}_{ck} = \sum \bar{A}_D + \sum \bar{A}_h$$

$$= \sum \bar{A}_D + \sum (\lambda_h) \times t,$$

where t is the time to detect the failure (1/2 of the test interval) plus the time to repair. Since the operability of these control circuits is generally unknown until tested, lengthy intervals between tests results in relatively high contribution to the unavailability of the control circuits. For example, from Table B-89,

$$\bar{A}_{ck} = 4 \times 10^{-4}/D + (7.7 \times 10^{-6}/hr \times t).$$

Using the repair time for instrumentation (7 hours) from Table III 5-2 of WASH-1400 and assuming monthly surveillance, the unavailability of the control circuit would be:

$$\begin{aligned} \bar{A}_{ck} &= 4 \times 10^{-4} + 7.7 \times 10^{-6}/\text{hr} \times 367 \text{ hr} \\ &= 3.2 \times 10^{-3}. \end{aligned}$$

If the valve circuit is only tested every 3 months (quarterly) then the circuit unavailability becomes:

$$\bar{A}_{ck} = 8.8 \times 10^{-3}.$$

Each of the motor-operated valve control circuits included in the fault tree models had basically the same design features as the generic circuit model, with the exception of the 250 V DC motor-operated valves. The control circuit associated with 250 V DC motor-operated valve differs from the generic AC control circuit utilized in the quantification in the following two ways:

1. The DC control circuit has no power supply transformer.
2. There are two relays in parallel in the "closing" circuit and "opening" circuit of the DC control circuit, compared to only a single relay in the AC control circuit. (Note: A single relay failure in the DC control circuit will disable the valve.)

The same method is used to quantify the AC and DC control circuit. The DC control circuit unavailability is:

$$\bar{A}_{DC} = \sum \bar{A}_D + \sum (\lambda_{hr}) \times t.$$

The hourly contribution for the DC control circuit is:

$$\begin{aligned} (\lambda_h) \times t &= (\lambda_{fuses} + \lambda_{wire} + \lambda_{overload} + \lambda_{close\ contacts} + \lambda_{open\ contacts}) \times t \\ &= (2 \times 10^{-6} + 3.3 \times 10^{-6} + 2 \times 10^{-7} + 4 \times 10^{-7} + 3 \times 10^{-7}) \times t \\ &= 6.1 \times 10^{-6} \times t. \end{aligned}$$

Therefore,

$$\bar{A}_{DC} = 5 \times 10^{-4} + 6.1 \times 10^{-6} \times t.$$

If monthly testing is performed, then

$$\begin{aligned} \bar{A}_{DC} &= 5 \times 10^{-4} + 6.1 \times 10^{-6} \times 367 \\ &= 2.7 \times 10^{-3}. \end{aligned}$$

If quarterly testing is performed, then

$$\begin{aligned}\bar{A}_{DC} &= 5 \times 10^{-4} + 6.1 \times 10^{-6} \times 1087 \\ &= 7.1 \times 10^{-3}.\end{aligned}$$

These values compare well with the monthly and quarterly AC control circuit values of 3.2×10^{-3} and 8.8×10^{-3} , respectively. The usage of the AC control circuit unavailability for the DC control circuit unavailability results in a slightly conservative estimate of the system unavailability.

An error factor of 10 was assigned to the generic control circuit unavailabilities to account for any variations in design from the base circuit.

5.3 Generic Motor-Driven Pump Control Circuits

There are basically two control circuit designs for controlling the operation of the various motor-driven pumps at BFl. The applicable control circuit is dependent on the type of power consumption the motor develops. For small motors utilizing 480 V AC, or lower, operation is controlled by the circuit represented in Figure B-53. For larger motors utilizing higher than 480 V AC, such as 4160 V AC, the motor is controlled by operation of the motor's circuit breaker.

Basically, power is supplied to motor when the motor coil (M) contacts close in each of the motor phases. Power for the control circuit is obtained by a 480 to 120 V AC stepdown transformer off the main supply to the motor. Fuses provide control circuit protection in the event of short circuits. Thermal overload devices also protect the motor by interrupting the motor coil circuit path in the event the motor is overheating due to excessive current flow.

Table B-90 lists these basic design features and the failure modes associated with these components that could prevent the control circuit from providing the correct output to the motor phase contacts. For this example, it is assumed that the pump is being commanded to start either by a manual switch or by contacts associated with some automatic safeguards actuation signal.

In a manner similar to that described previously for the generic valve control circuit, the unavailability for the pump control circuit can be expressed as:

$$\begin{aligned}\bar{A}_{ck} &= \sum \bar{A}_D + \sum \bar{A}_{hr} \\ &= 1 \times 10^{-4}/D + (7.6 + 10^{-6}/hr \times t),\end{aligned}$$

where t is the time to detect (1/2 of the test interval) plus the time to repair.

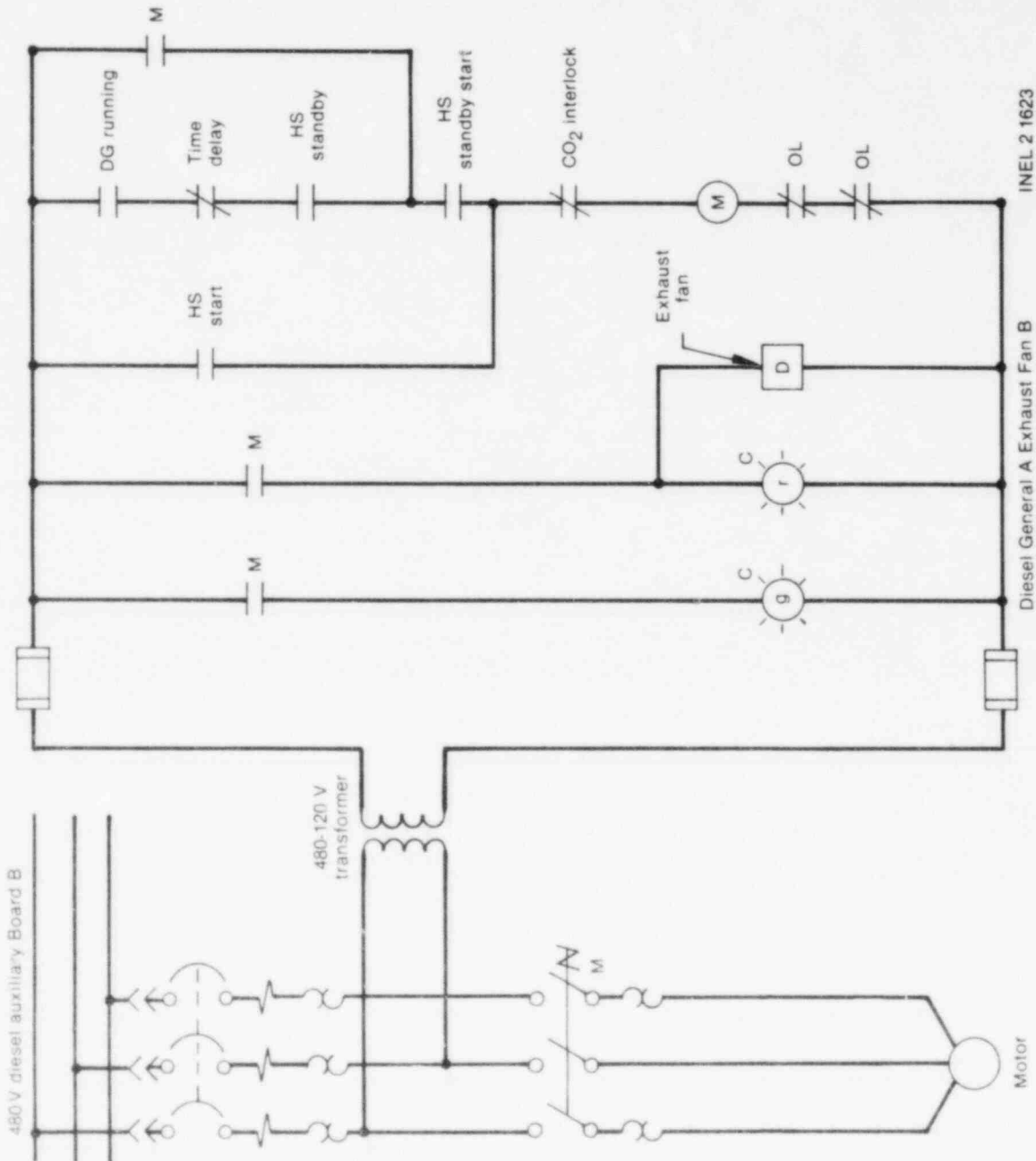


Figure B-53. Motor-driven pump-control circuit.

TABLE B-90. MOTOR-DRIVEN PUMP CONTROL CIRCUIT

Component	Failure Mode	Number (N)	Failure Rate (λ)	$N\lambda$
Switch contacts	Fail to close	1	1E-7/hr	1E-7/hr
Circuit wiring	Open	--	3E-6/hr	3E-6/hr
	Short to ground	--	3E-7/hr	3E-7/hr
Transformer	Open	1	1E-6/hr	1E-6/hr
	Short		1E-6/hr	1E-6/hr
Fuses	Open	2	1E-6/hr	2E-6/hr
Overload contacts	Open	2	1E-7/hr	2E-7/hr
M relay or circuit breaker closing relay	Does not energize	1	1E-4/D	1E-4/D
Sum of demand rates = 1E-4/D.				
Sum of hourly rates = 7.6E-6/hr.				

For monthly testing, the motor-driven pump control circuit unavailability is:

$$A_{ck} = 2.9 \times 10^{-3}$$

For quarterly testing this value becomes 8.4×10^{-3} .

The operation of the 4160 V AC motors is basically the same as the 480 V AC motor, with the following exceptions:

1. The 480 V AC motor's circuit breaker is permanently closed; starting and stopping is accomplished by contacts downstream of the circuit breaker. The 4160 V AC control circuit starts and stops the motor by closing and opening the motor's circuit breaker.
2. The control circuit for the 4160 V AC motor-driven pump contains additional components, such as limit/position switches and contacts operated by the circuit breaker, which contribute to the failure of the 4160 V AC control circuit.

Following the same rationale as applied in the 480 V AC control circuit analysis, we then have

$$\bar{A}_{4160 \text{ V AC}} = \bar{A}_D + \sum_h (\lambda_h) \times t.$$

The hourly contribution for the 4160 V AC control circuit consists of failure of fuses (2), switch contacts (2), circuit breaker contacts (4), and wire, therefore,

$$\begin{aligned} \sum (\lambda_h) \times t &= (2 \times 10^{-6} + 2 \times 10^{-7} + 4 \times 10^{-7} + 3.3 \times 10^{-6}) \times t \\ &= (5.9 \times 10^{-6}) \times t. \end{aligned}$$

The contribution of the demand-related failures is from the failure of the closing relay (1) and the limit switches (2). Therefore,

$$\begin{aligned} \bar{A}_D &= 1 \times 10^{-4} + 6 \times 10^{-4}, \\ &= 7 \times 10^{-4} \end{aligned}$$

The overall unavailability of the 4160 V AC control circuit is

$$\bar{A}_{4160 \text{ V AC}} = 7 \times 10^{-4} + (5.9 \times 10^{-6}) \times t.$$

If monthly testing is performed, then

$$\bar{A}_{4160 \text{ V AC}} = 2.9 \times 10^{-3}.$$

If quarterly testing is performed, then

$$\bar{A}_{4160 \text{ V AC}} = 7.1 \times 10^{-3}.$$

Failures associated with the 4160 V AC circuit breaker are included under the local faults as a separate event.

Comparing the 4160 V AC values with the 480 V AC values, shows the values agree very well. The conclusion is that the use of the 480 V AC generic value for the 4160 V AC has little effect on the final system unavailability.

ATTACHMENT A--EVENT NAMING CODE

To facilitate the computer handling of events, an eight-character code name was assigned to basic events. This coding scheme is described as follows:

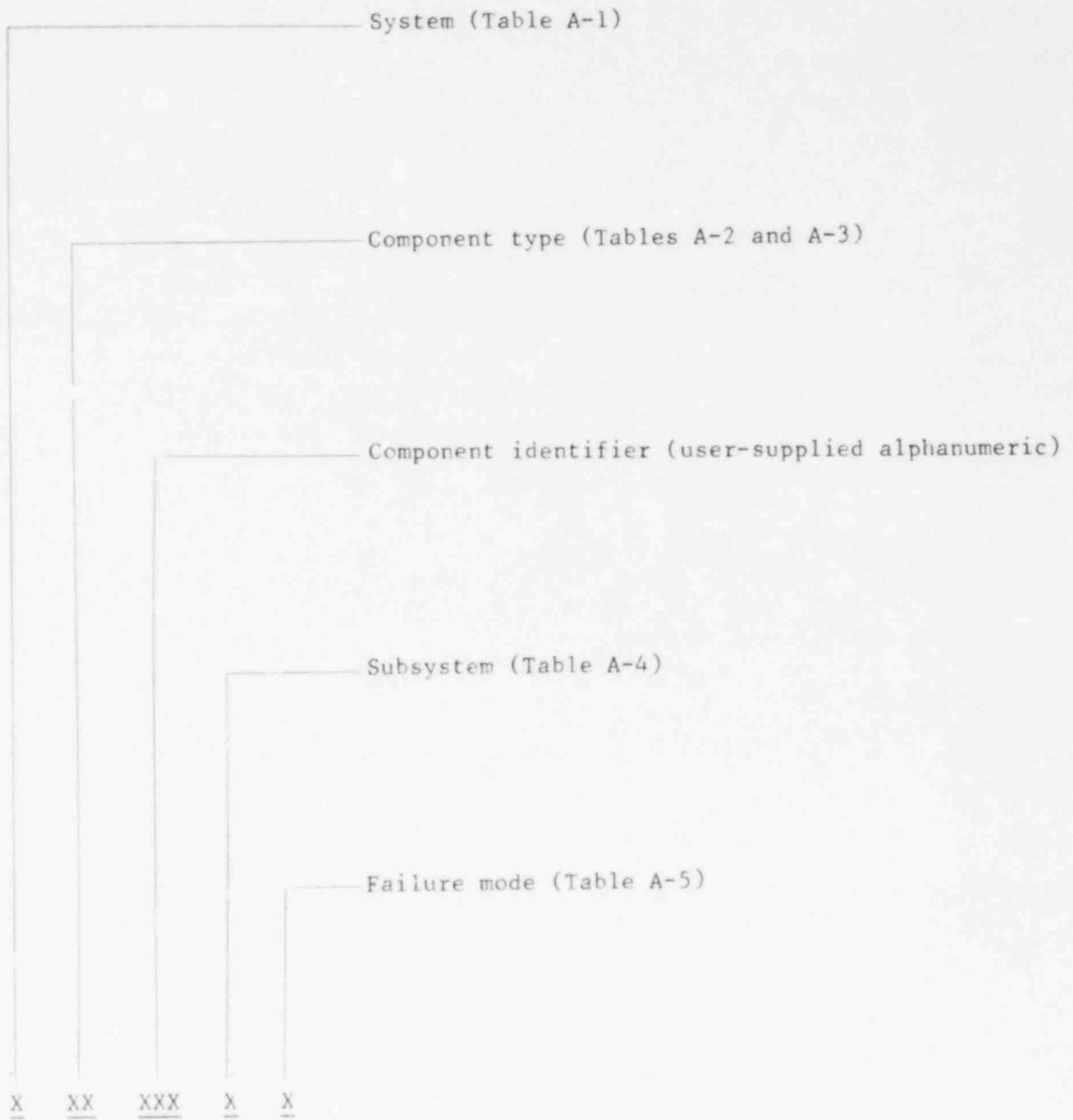


TABLE A-1. SYSTEM CODE

<u>Code</u>	<u>System Name</u>
A	AC power
B	Automatic depressurization system
C	Containment atmosphere dilution system
D	Condenser circulating water
E	Containment isolation system
F	Control air system
G	Control rod drive hydraulic
H	Condensate transfer and storage system
I	DC power
J	Equipment area cooling
K	Emergency equipment cooling water
L	Engineered safety features actuation system
M	High pressure coolant injection
N	Keep-full system
O	Low pressure core spray
P	Power conversion system
Q	Reactor core isolation cooling
R	Residual heat removal
S	Residual heat removal service water
T	Reactor protection system
U	Raw cooling water system
V	Reactor recirculation system
W	Reactor water cleanup
X	Standby coolant supply system
Y	Standby gas treatment
Z	Vapor suppression

TABLE A-2. MECHANICAL COMPONENT TYPE CODE

<u>Code</u>	<u>Mechanical Components</u>	<u>Code</u>	<u>Mechanical Components</u>
AC	Accumulator	PT	Pump (turbine-driven)
CD	Control rod drive unit	PV	Pressure vessel
CH	Chiller	RD	Rupture disk
CL	Clutch	SD	Steam drum
CM	Compressor	SL	Seals
CN	Condenser	SP	Sparger
DL	Diesel	TB	Turbine
FE	Flow element	TK	Tank
FL	Filter or strainer	VA	Valve (pneumatic)
FN	Fan	VC	Valve (control)
GB	Gas bottle	VE	Valve (solenoid-operated)
HX	Heat exchanger	VH	Valve (manual)
NZ	Nozzle	VK	Valve (check)
OO	Conditional event	VM	Valve (motor-operated)
OR	Orifice	VB	Vacuum breaker
PD	Pipe device	VO	Valve (hydraulic-operated)
PM	Pump (motor-driven)	VR	Valve (relief)
PP	Pipe	VS	Valve (stop check)

TABLE A-3. ELECTRICAL COMPONENT TYPE CODE

Code	Electrical Component	Code	Electrical Component
AM	Amplifier	LT	Light
AN	Annunciator	ME	Meter
AT	Switch (automatic transfer)	MO	Motor
BC	Battery charger	ND	Neutron detector
BS	Bus	OO	Conditional event
BY	Battery	OT	Transformer (potential or control)
CA	Cable	PI	Process indicator
CB	Circuit breaker	PS	Switch (process)
CC	Capacitor	RC	Recorder
CK	Control circuit	RE	Relay
CO	Contacts	RG	Voltage regulator
CT	Transformer (current)	RS	Resistor
DC	DC power supply	RT	Resistor (temperature device)
DE	Diode or rectifier	SC	Speed controllers
DP	Distribution panel	ST	Solid state device
FU	Fuse	SW	Switch (manual)
GE	Generator	SZ	Position sensor
GS	Ground switch	TE	Temperature element
HR	Heater	TI	Timer
HT	Heat tracing	TP	Process transmitter
IN	Instrumentation	TR	Transformer (power)
IV	Inverter (solid-state)	TZ	Position transmitter
KS	Switch (lock-out)	WR	Wire
LA	Lightning arrester	XT	Transformer (voltage)
LS	Limit switch		

TABLE A-4. SUBSYSTEM CODE

Alphanumeric: Use A or B for Train A or B.
 Use 1 or 2 for Loop 1 or 2.

For nonredundant trains or components, use U.

TABLE A-5. FAILURE MODE CODE

Code	Failure Mode
Passive:	
A	Short to power
B	Open circuit
C	Short to ground
D	Operator response error
E	Plugged
F	Leakage/rupture
G	No output
H	Wrong output
I	Erroneous output
J	Unavailable due to test or maintenance
Active:	
K	Does not reclose
L	Conditional event occurs
M	Calibration shift
N	Does not close
O	Does not remain closed
P	Does not open
Q	Does not remain open (plugged)
R	Does not start
S	Does not continue to run
T	Does not operate
U	Does not insert
V	Does not energize
W	Loss of function
X	Operational or maintenance fault
Y	Disengaged/does not engage
Z	Engaged

ATTACHMENT B--SI 4.2.B-1

4. Procedure - Functional Test and Calibration (continued)

- 4.33 If indicators were adjusted, record "as left" data on calibration data card.
- 4.34 Record "as left" data for switches 1 through 4 on data sheet.
- 4.35 Remove test pressure from yarway.
- 4.36 Verify:
 - a. All relays dropped out
 - b. All trip status lights extinguished
 - c. Annunciator REACTOR VESSEL WATER LOW CLEAR
 - d. Annunciator CORE COOLING SYSTEM/DIESEL INITIATE CLEAR.
- 4.37 Disconnect test gauge from water box.
- 4.38 Close high and low side calibration valves on water box.
- 4.39 Open equalizer valve on water box.
- 4.40 Disconnect water box from yarway both high and low side.
- 4.41 Remove VOM from test connection and secure junction box.
- 4.42 Open manifold equalizer valve on yarway.
- 4.43 Inspect yarway chambers for water level. Fill from water box if necessary
- 4.44 Replace vent plugs in yarway.
- 4.45 Slowly open low side manifold valve of yarway, check for and repair leaks.
- 4.46 Close manifold equalizing valve on yarway.
- 4.47 Slowly open high side manifold valve of yarway. The indicator should assume a position equal to the actual level.
- 4.48 Notify unit operator test is complete on that instrument and proceeding to next instrument (if applicable).

*Revision _____ (initialed)

DATA COVER SHEET SI 4.2.B-1

REACTOR LOW WATER LEVEL
LIS-3-58A and C, LITS-3-58B and D, LI-3-58A and B

Calibration and Functional Test

Unit _____

Performed By: _____ Date _____
Instrument Mechanic

Technical Specification criteria satisfied. _____ Yes _____ No

Surveillance Instruction criteria satisfied. _____ Yes _____ No

If either one above is no, the shift engineer will review the data to determine if a LCO is violated.

LCO violated. _____ Yes _____ No Shift Engineer _____ Date _____

Reason for test:

- _____ After maintenance
- _____ Plant condition (explain in remarks)
- _____ Required by schedule
- _____ Other (explain in remarks)
- _____ Another system inoperable

Results reviewed _____ Date _____
Instrument Mechanic Foreman

Results reviewed and instruction _____ Date _____
criteria satisfied. Cognizant Reviewer

Results reviewed for QA requirements _____ Date _____
QA supervisor

REMARKS _____

Data Sheet SI 4.2.B-1-A

LIS-3-58A

Unit _____

Date _____

Calibration and Functional Test

<u>Step</u>	<u>Initials/Data</u>
1. Remove yarway from service (steps 4.2 through 4.5 of procedure)	_____
2. Connect test equipment to yarway (steps 4.6 through 4.13 of procedure)	_____
3. Inform operator he will receive the following alarms: CORE COOLING SYSTEM/DIESEL INITIATE, AND REACTOR VESSEL LOW LEVEL panel 9-3 (step 4.14 of procedure)	_____
4. Check SW#4 operation Verify: a. Relay 10A-K79A picked up panel 9-32 b. Status light 10A-DS146A illuminated panel 9-32 (steps 4.15 through 4.17 of procedure)	_____ _____
5. Check SW#3 operation Verify: a. Relay 23A-K40 picked up panel 9-32 b. Status light 23A-DS70 (LIS-3-58A) illuminated panel 9-39) c. Annunciator REACTOR VESSEL LOW LEVEL (9-3) (steps 4.18 through 4.21)	_____ _____ _____
6. Check SW#2 operation Verify: a. Relay 2E-K28 picked up panel 9-30 b. Status light 2E-DS10A illuminated panel 9-30 (steps 4.22 through 4.24 of procedure)	_____
	Note 1 "As found" SW#3 _____ in. H ₂ O
*7. Check SW#1 operation Verify: a. Relays 14A-K7A and 10A-K7A picked up panel 9-32 b. Status light 14A-DS31A illuminated panel 9-32 c. Annunciator CORE COOLING SYSTEM/DIESEL INITIATE (9-3) (steps 4.25 through 4.28 of procedure)	_____ _____ _____
	Note 2 "As found" SW#1 _____ in. H ₂ O

*Revision _____ (Initialed)

Data Sheet SI 4.2.B-1-A (Continued)

Unit _____

Date _____

Step

Initials/Data

8. Check local indicator (step 4.29 of procedure) _____
9. Calibrate indicator and switches if out of specified values (steps 4.31 through 4.33 of procedure) _____
10. Record "as left" data of switches (step 4.34 of procedure)
- Note 3 "As left" SW#4 _____ in. H₂O
- Note 3 "As left" SW#3 _____ in. H₂O
- Note 4 "As left" SW#2 _____ in. H₂O
- Note 4 "As left" SW#1 _____ in. H₂O
11. Remove test pressure from yarway (step 4.35 of procedure) _____
- *12. a. Verify the following relays dropped out:
- 10A-K79A (panel 9-32), 23A-K40 (panel 9-32),
2E-K28 (panel 9-30), 14A-K7A (panel 9-32)
10-K7A (panel 9-32) _____
- b. Verify the following status lights extinguished:
- 10A-DS146A (panel 9-32)
23A-DS70 (panel 9-39), 2E-DS10A (panel 9-30),
14A-DS31A (panel 9-32) _____
- c. Verify annunciator REACTOR VESSEL WATER LOW clear _____
- d. Verify annunciator CORE COOLING SYSTEM/DIESEL INITIATE clear (step 4.36 of procedure) _____
13. Remove test equipment from yarway (steps 4.37 through 4.41 of procedure) _____
14. Return yarway to service (steps 4.42 through 4.47 of procedure) _____
15. Unit operator notified test is complete on LIS-3-58A, and proceeding to next instrument (step 48 of procedure) _____

REMARKS: _____

*Revision _____ (Initialed)

ATTACHMENT C--SI 4.2.B-5 and IMJ-202

4. Procedure (continued)

4.4 Return to Service

- a. Release the test pressure.
- b. Check that trip lights reset.
- c. Perform steps 13 and 14 of IMI-202 and return pressure switch to service.

5. Acceptance Criteria

- 5.1 Technical specification criteria are satisfied if pressure switches PS-64-58 (A through D) each energize the appropriate relays at ___ 2 psig.
- 5.2 Surveillance instruction criteria are satisfied only if all procedural steps are safely completed.
- 5.3 PS-64-58A and C and PS-64-58B and D form two channels in either trip system. Both channels are required to be operable for each trip system. If the channel is found to be inoperable, it must be repaired within 24 hours or declare the trip system inoperable.

6. Return to Normal

- 6.1 Assure trip lights reset.
- 6.2 Assure sensors are valved in correctly.
- 6.3 Notify assistant shift engineer upon completion.
- 6.4 Verify by signature and date on the data cover sheet that the channel was functionally tested and/or calibrated in accordance with this instruction.

DATA COVER SHEET SI 4.2.B-5

Instrumentation that Initiate or Control the CSCS
Drywell High Pressure
Calibration and Functional Test

Unit _____

Performed: (Check one) Functional Test _____ Calibration and Functional Test _____

Performed By: _____ Date _____
Instrument Mechanic

Technical Specification criteria satisfied. _____ Yes _____ No

Surveillance Instruction criteria satisfied. _____ Yes _____ No

If either one above is no, the shift engineer will review the data to determine if a LCO is violated.

LCO violated. _____ Yes _____ No Shift Engineer _____ Date _____

Reason for test:

_____ After maintenance

_____ Plant condition
(explain in remarks)

_____ Required by schedule

_____ Other (explain in remarks)

_____ Another system inoperable

Results reviewed _____ Date _____
Senior Instrument Mechanic Foreman

Results reviewed and instruction _____ Date _____
criteria satisfied. Cognizant Reviewer

Results reviewed for QA requirements _____ Date _____
QA Supervisor

REMARKS _____

Data Sheet SI 4.2.B-5

Section	Date _____	Initials data			
		<u>PS-64-58A</u>	<u>PS-64-58B</u>	<u>PS-64-58C</u>	<u>PS-64-58D</u>
4.1.a	Sensor valved out in accordance with IMI-202.	_____	_____	_____	_____
4.2.a	Sensor calibrated in accordance with this section and results are satisfactory. (As found and as left data)				
	SW #1	<u> / </u> AF AL	<u> / </u> AF AL	<u> / </u> AF AL	<u> / </u> AF AL
	SW #2	<u> / </u> AF AL	<u> / </u> AF AL	<u> / </u> AF AL	<u> / </u> AF AL
4.3.a	Panel trip light				
	9-31 10A-DS-122A	_____			
	10A-DS-120A		_____		
	10A-DS-123A			_____	
	10A-DS-121A				_____
	9-33 10A-DS-120B	_____			
	10A-DS-122B		_____		
	10A-DS-121B			_____	
	10A-DS-123B				_____
	9-39 PS-64-58A	_____			
	PS-64-58B		_____		
	PS-64-58C			_____	
	PS-64-58D				_____

Data Sheet SI 4.2.B-5 (Continued)

<u>Section</u>		Date _____			
		Initials data			
		<u>PS-64-58A</u>	<u>PS-64-58B</u>	<u>PS-64-58C</u>	<u>PS-64-58D</u>
4.3.b	Relay 10A-K5B energizes	_____	_____	_____	_____
	Relay 14A-K5B energizes	_____	_____	_____	_____
	Relay 10A-K5A energizes	_____	_____	_____	_____
	Relay 14A-K5A energizes	_____	_____	_____	_____
	Relay 10A-K6B energizes	_____	_____	_____	_____
	Relay 14A-K6B energizes	_____	_____	_____	_____
	Relay 10A-K6A energizes	_____	_____	_____	_____
	Relay 14A-K6A energizes	_____	_____	_____	_____
4.4.a	Pressure removed	_____	_____	_____	_____
4.4.b	Trip lights reset	_____	_____	_____	_____
4.4.c	IMI-2-2 steps 13 and 14 performed and pressure switch returned to service	_____	_____	_____	_____
6.1	Trip lights reset	_____	_____	_____	_____
6.2	Sensors valved in	_____	_____	_____	_____
6.3	Assistant shift engineer notified of work completion	_____	_____	_____	_____

- *9. Record "as left" setpoint data on the Calibration Data card (repeat 1 blank).
- *10. Repeat step 6 and record "as left" setpoint data on the Calibration Data card (repeat 2 blank).
- *11. If the switch contains more than one bistable, repeat steps 7 through 10 and record data in numbers 2, 3 and 4 (as applicable) of the Calibration Data card.
- *12. Record "as left" input test instrument number on the Calibration Data card.
- *13. Remove calibration standard from calibration TEE and replace cap as indicated on test flow indicator.
- *14. Return pressure switch to service. Observe caution.

CAUTION: Exercise care in valving the pressure switch in service and be reasonably assured that it is in service.

- *15. If the switch is to be loop checked, proceed with this step. If the switch is the loop, proceed to step 18.

NOTE: The pressure switch is calibrated, but no assurance that the loop accuracy is correct or of the loop integrity. Refer to the applicable standard calibration instructions for applying a simulated signal to the primary element (same as calibration for one point).

- *16. Apply the signal to the primary element representing the designated point.

Verify that the loop is with loop accuracy.

NOTE: If the loop is not within the required accuracy, immediately notify the Senior Instrument Mechanic Foreman to determine whether other loop components need calibrating.

- *17. Record the loop accuracy on the pressure switches Calibration Data card as follows:

Standard	X
A.L. Loop	X
A.L. Instr.	X

*Revision _____ (Initialed)

ATTACHMENT D--EOI-41

II. Methods of Low Pressure H₂O Makeup (Continued)

E. Utilization of core spray charging H₂O pumps through core spray piping.

1. Open or check open
 - a. HCV-75-1 Loop I torus suction
 - b. FCV-75-57 and 75-58 common suction for charging H₂O pumps
 - c. HCV-75-598 and HCV-75-599 pumps A & B suction
 - d. HCV-75-602 and HC-75-603 pumps A and B discharge
 - e. HCV-75-608 to Loop I and HCV-75-611 to Loop II
 - f. FCV-75-23, FCV-75-25, and HCV-75-27 (Loop I)
 - g. FCV-75-51, FCV-75-53, and HCV-75-55 (Loop II).
2. Close HCV-75-616, head tank isolation.
3. Start charging H₂O pump(s).
4. Maintain flow as required.

F. Standby Coolant Supply

NOTE: To be used only as a last resort method of maintaining reactor water level.

1. Use of RHR Service Water (4250 gpm)
 - a. Utilization of RHRSW pumps
 - 1) Check RHRSW pump B1, B2, or D1, D2 running
 - 2) Open FCV-23-57 and FCV-74-101, or FCV-74-100 on unit 3
 - 3) Open FCV-74-66 and FCV-74-67
 - 4) Close FCV-23-52 and 23-46.

REFERENCES

1. Reactor Safety Study--An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014), October 1975.
2. Anticipated Transients without Scram, Vol. 1, NUREG-0460, April 1978, p. 28.
3. Failure of 76 of 185 Control Rods to Fully Insert During a Scram at a BWR, IE Bulletin No. 80-17 (with Supplements 1-5), NRC Office of Inspection and Enforcement, July 3, 1980 (and July 18, July 22, August 22, and December 18, 1980; and February 13, 1981).
4. B. J. Verna, "Scram Discharge Volume Problems--Part 1" and "--Part 2," Nuclear News, Vol. 24, Nos. 2 and 5, February and April 1981.
5. J. Pittman, Scram Discharge Volume Fault Tree Model, private communication, NRC Reactor Risk Branch to EG&G Idaho Reliability and Statistics Branch (J. A. Murphy to J. Trainer), April 30, 1981.
6. Failures of the Continuous Water Level Monitor for the Scram Discharge Volume at Dresden Unit No. 2, IE Bulletin No. 80-43, NRC Office of Inspection and Enforcement, December 5, 1980.
7. A. D. Swain and H. E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, October 1980.

EG&G Idaho, Inc.
P.O. Box 1625
Idaho Falls, Idaho 83415



U.S. Department of Energy

Idaho Operations Office • Idaho National Engineering Laboratory

Interim Reliability Evaluation Program: Analysis of the Browns Ferry, Unit 1, Nuclear Plant

Appendix C—Sequence Quantification

EG&G Idaho, Inc.

Energy Incorporated, Seattle Office

S. E. Mays

R. C. Bertucio

J. P. Poloski

T. J. Leahy

W. H. Sullivan

J. E. Trainer

July 1982

Prepared for the
U.S. Nuclear Regulatory Commission
Under Sandia National Laboratories
Purchase Order No. 62-7776

 **EG&G** Idaho

8209270448

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, nor 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

**INTERIM RELIABILITY EVALUATION PROGRAM:
ANALYSIS OF THE BROWNS FERRY,
UNIT 1, NUCLEAR PLANT**

APPENDIX C—SEQUENCE QUANTIFICATION

EG&G Idaho, Inc.

S. E. Mays
J. P. Poloski
W. H. Sullivan
J. E. Trainer

Energy Incorporated, Seattle Office

R. C. Bertucio
T. J. Leahy

Published July 1982

EG&G Idaho, Inc.
Idaho Falls, Idaho 83415

Prepared for the
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
Under Sandia National Laboratories
Purchase Order No. 62-7776
FIN No. A1241

FOREWORD

This report describes a risk study of the Browns Ferry, Unit 1, nuclear plant. The study is one of four such studies sponsored by the NRC Office of Research, Division of Risk Assessment, as part of its Interim Reliability Evaluation Program (IREP), Phase II. Other studies include evaluations of Arkansas One, Unit 1, by Sandia National Laboratories; Calvert Cliffs, Unit 1, by Science Applications, Inc.; and Millstone, Unit 1, by Science Applications, Inc. EG&G Idaho, Inc. was assisted by Energy Inc., Seattle, in its evaluation of the Browns Ferry, Unit 1, plant. Battelle-Columbus Laboratories provided information regarding the fission product releases that result from risk-significant accident scenarios. Sandia National Laboratories has overall project management responsibility for the IREP studies. It also has responsibility for the development of uniform probabilistic risk assessment procedures for use on future studies by the nuclear industry.

This report is contained in four volumes: a main report and three appendixes. The main report provides a summary of the engineering insights acquired in doing the study and a discussion regarding the accident sequences that dominate the risks of Browns Ferry, Unit 1. It also describes the study methods and their limitations, the Browns Ferry plant and its systems, the identification of accidents, the contributors to those accidents, and the estimating of accident occurrence probabilities. Appendix A provides supporting material for the identification of accidents and the development of logic models, or event trees, that describe the Browns Ferry accidents. Appendix B provides a description of Browns Ferry, Unit 1, plant systems and the failure evaluation of those systems as they apply to accidents at Browns Ferry. Appendix C generally describes the methods used to estimate accident sequence frequency values.

Numerous acronyms are used in the study report. For each volume of the report, these acronyms are defined in a listing immediately following the table of contents.

CONTENTS

FOREWORD	C-ii
NOMENCLATURE	C-vii
1. APPROACH	C-1
1.1 System Unavailabilities	C-1
1.2 Treatment of Commonalities	C-3
1.3 Treatment of Complement or Success Sets	C-8
1.4 Treatment of Initiator Effects on Mitigating Systems	C-9
1.5 Treatment of Potential Logic Loops	C-9
2. EXAMPLE CALCULATION	C-12
2.1 Initiator Frequency	C-12
2.2 Example System Unavailabilities	C-12
2.3 Sequence Calculations	C-15
3. FAILURE DATA	C-21
3.1 Component Failure Data	C-21
3.2 Human Error Rates	C-21
3.3 Recovery Factors	C-31
4. CANDIDATE DOMINANT SEQUENCES	C-32
4.1 Introduction	C-32
4.2 Sequence Evaluation	C-32
4.3 Dominant Sequences	C-77
5. UNCERTAINTY ANALYSIS	C-80
5.1 Introduction	C-80
5.2 Methodology	C-80
5.3 Data Base	C-80
5.4 Results	C-81
5.5 Insights on Uncertainty Analysis	C-81

6.	SENSITIVITY ANALYSIS	C-83
6.1	Introduction	C-83
6.2	Scope of Analysis	C-83
6.3	Evaluation	C-84
	REFERENCES	C-87

FIGURES

C-1.	RHR/RHRSW/EECW system power dependencies	C-10
C-2.	LOCA systemic event tree for intermediate steam break (I_V), with system and sequence values filled in	C-13
C-3.	LOCA systemic event tree for large liquid break, suction- side of recirculation pumps (I_S)	C-33
C-4.	LOCA systemic event tree for large liquid break, discharge- side of recirculation pumps (I_D)	C-34
C-5.	LOCA systemic event tree for large steam break (I_V)	C-35
C-6.	LOCA systemic event tree for intermediate liquid break (I_L)	C-36
C-7.	LOCA systemic event tree for intermediate steam break (I_V)	C-37
C-8.	LOCA systemic event tree for small liquid or steam break (S)	C-38
C-9.	Transient systemic event tree where PCS is unavailable (T_U)	C-39
C-10.	LOSP-induced transient systemic event tree (PCS unavailable) (T_P)	C-40
C-11.	Transient systemic event tree where PCS is available (T_A)	C-41
C-12.	Transient-induced SORV LOCA systemic event tree (intermediate steam break) (TK)	C-42
C-13.	LOSP-induced SORV LOCA systemic event tree (intermediate steam break) (T_PK)	C-43
C-14.	Systemic event tree showing the $T_P R_B R_A$ sequence	C-52
C-15.	Dominant contributors to the unavailability of torus cooling and shutdown cooling given LOSP	C-53
C-16.	Systemic event tree showing the $T_P Q R_B R_A$ sequence	C-55

C-17. Dominant contributors to the unavailability of RCIC, torus cooling, and shutdown cooling given LOSP	C-56
C-18. Systemic event tree showing the $T_{URB}R_A$ sequence	C-58
C-19. Dominant contributors to the unavailability of RHR systems following a transient which disables the PCS (normal power available)	C-59
C-20. Systemic event tree showing the $T_{UQRB}R_A$ sequence	C-61
C-21. Dominant contributors to the unavailability of the RCIC and RHR systems following a transient which disables the PCS (normal power available)	C-62
C-22. Systemic event tree showing the $T_{PKRB}R_A$ sequence	C-63
C-23. Systemic event tree showing the $TKR_B R_A$ sequence	C-65
C-24. Systemic event tree showing the T_{UQDV} sequence	C-67
C-25. Dominant contributors to the unavailability of RCIC, HPCI, and manual depressurization following a transient which disables the PCS (normal power available)	C-68
C-26. Systemic event tree showing the $T_{pQDFB}G_D X$ sequence	C-70
C-27. Dominant contributors to the unavailability of RCIC, HPCI, LPCI, core spray, and SBCS given LOSP	C-71
C-28. Systemic event tree showing the $T_{pKDFB}G_D$ sequence	C-73
C-29. Dominant contributors to the unavailability of HPCI, LPCI, and core spray, given LOSP and SORV	C-74
C-30. Systemic event tree showing the T_{UB} sequence	C-76
C-31. Systemic event tree showing the T_{ABM} sequence	C-78
C-32. Dominant contributors to the unavailability of the CRD and RPT systems following a transient where the PCS is available	C-79

TABLES

C-1. Component unavailabilities	C-4
C-2. Intermediate steam break ECI criteria	C-14
C-3. Decay heat removal failure criteria	C-15
C-4. IREP data Table 3A and 3B	C-22

C-5. Component data not available in Table C-4	C-30
C-6. Nonrecovery factors	C-31
C-7. Sequence frequencies greater than 10^{-8} by initiator	C-44
C-8. Systemic sequence frequencies in decreasing order of magnitude	C-45
C-9. Candidate dominant sequences	C-46
C-10. Initiator designators	C-47
C-11. Front-line systems unavailabilities	C-47
C-12. System combinations of importance	C-49
C-13. Commonalities of importance	C-50
C-14. Dominant sequences	C-79
C-15. Dominant sequence uncertainties	C-81

NOMENCLATURE

\bar{A}	The complement of A (a success event if A is a failure event). (\bar{A} may also be used to mean "unavailability.")
A	Alarm
AC	Alternating current
ACC	Accumulator
ADS	Automatic depressurization system
AH	Alarm-high
AO	Air operator
APRM	Average power range monitor
AT	Anticipated transient
ATWS	Anticipated transient without scram
BF1	Browns Ferry, Unit 1, nuclear plant
BI	Break isolation
BWR	Boiling water reactor
CAD	Containment atmosphere dilution
CCW	Condenser circulating water
CD	Complete dependence
CE	Conductivity element
CIS	Containment isolation system
Clg	Cooling
COND	Main condenser
CR-3	Crystal River, Unit 3, nuclear plant IREP study
CRD	Control rod drive
CRDH	Control rod drive hydraulic
CRDHS	Control rod drive hydraulic system
CRW	Clean rad waste
CS	Core spray
CS&T	Condensate storage and transfer
CSCS	Core standby cooling system
CSS	Core spray system
CST	Condensate storage tank
CV	Control valve
D	Demand
DC	Direct current
DEP	Depressurization
DG	Diesel generator
DHR	Decay heat removal
Diff	Different
DPI	Differential pressure indicator
DPIS	Differential pressure indicating switch
DPS	Differential pressure switch
DPT	Differential pressure transmitter
EAC	Equipment area cooling
ECCS	Emergency core cooling system
EGI	Emergency coolant injection
EECW	Emergency equipment cooling water
EHC	Electro-hydraulic control

EMI	Electrical Maintenance Instruction
EOI	Equipment Operating Instructions
EPRI	Electric Power Research Institute
EPS	Electrical power system
ESFAS	Engineered safety features actuation system
F(*)	Frequency of initiator in parentheses
FCV	Flow control valve
FE	Flow element
FI	Flow indicator
FIC	Flow indicating controller
FLS	Front-line system
FMEA	Failure mode effects analysis
FR	Flow recorder
FS	Flow switch
FSAR	Final Safety Analysis Report
FT	Flow transmitter
FWC	Feedwater control
FWCS	Feedwater control system
G	Green
GOI	General Operating Instructions
H	High
H/L	High/low
HCU	Hydraulic control unit
HCV	Hand control valve
HEP	Human error probability
HPCI	High pressure coolant injection
HPCS	High pressure core spray
HPI	High pressure injection
HS	Handswitch
HSS	High speed stop
HVAC	Heating, ventilation, and airconditioning
HX	Heat exchanger
I&C	Instrumentation and control
I&E	Inspection and enforcement
IMI	Instrument Maintenance Instruction
INJ	Injection
IREP	Interim Reliability Evaluation Program
IRM	Intermediate range monitor
L	Low
LA	Level alarm
LD	Low dependence
LER	Licensee Event Report
LIC	Level indicating controller
LIS	Level indicating switch
LL	Low-low
LOCA	Loss of coolant accident
LOSP	Loss of offsite power
LPCI	Low pressure coolant injection
LPI	Low pressure injection

LS	Limit switch
LSS	Low speed stop
LT	Level transmitter
M	Motor (operated valve)
MCR	Main control room
MD	Moderate dependence
MGU	Master governor unit
MMG	Motor generator
MMI	Mechanical Maintenance Instruction
MO	Motor operated
MOV	Motor-operated valve
MSC	Manual speed control
MSI	Main steam isolation
MSIV	Main steam isolation valve
MSL	Main steam line
NA; N/A	Not applicable
NC	Normally closed
NMS	Neutron monitoring system
NO	Normally open
OI	Operating Instructions
OL	Overload
OP	Overpressure protection
OP(C)	Overpressure protection (relief valves closed)
OP(O)	Overpressure protection (relief valves open)
PA	Pressure alarm
PB	Pipe break
PCIS	Primary containment isolation system
PCS	Power conversion system
PCV	Pressure control valve
PG	IREP Procedure Guide
PI	Pressure indicator
PORV	Power-operated relief valve
PRA	Probabilistic risk assessment
PS	Pressure switch
PSCWT	Pressure suppression chamber water transfer
PT	Pressure transmitter
PWR	Pressurized water reactor
Q(*)	Unavailability of system in parentheses
QA	Quality assurance
R	Red
RBCCW	Reactor building component cooling water
RBEDT	Reactor building equipment drain tank
RCB	Reactor coolant boundary
RCIC	Reactor core isolation cooling
RCS	Reactor coolant system
RCW	Raw cooling water
RCWS	Raw cooling water system
Recirc	Recirculation

RFP Reactor feed pump
 RFPT Reactor feed pump turbine
 RFWPT Reactor feedwater pump turbine
 RHR Residual heat removal
 RHRSW Residual heat removal service water
 RMOV Reactor motor-operated valve
 RMS Remote manual switch
 RPS Reactor protection system
 RPT Recirculation pump trip
 RS Reactor subcriticality; reactor shutdown; reactor scram
 RV(C) Relief valve (closed)
 RV(O) Relief valve (open)
 RWCU Reactor water cleanup
 RX Reactor

S/D Shutdown
 S/RV Safety relief valve
 S/V Safety valve
 SBCS Standby coolant supply
 SBGT Standby gas treatment
 SCI Short-term containment integrity
 SD-BD Shutdown board
 SDV Scram discharge volume
 SIV Scram instrument volume
 SJAE Steam jet air ejector
 SLCS Standby liquid control system
 SORV Stuck-open relief valve
 SRM Source range monitor

TA Temperature alarm
 TCV Turbine control valve
 TD Time delay
 TDC Time delay contact
 TDPU Time delay pickup
 TE Temperature element
 TIP Traversing in-core probe
 TMI Three Mile Island
 TR Temperature recorder
 Trans Transient
 TS Technical Specifications; torque switch
 TVA Tennessee Valley Authority

UV Undervoltage

V Volts
 VB Vacuum breaker
 VO Valve open
 VS Vapor suppression
 VSS Vapor suppression system
 VWI Vessel water inventory

ε An insignificant quantity, generally less than 10^{-8}

INTERIM RELIABILITY EVALUATION PROGRAM:
ANALYSIS OF THE BROWNS FERRY, UNIT 1, NUCLEAR PLANT

APPENDIX C--SEQUENCE QUANTIFICATION

1. APPROACH

The purpose of Appendix C is to describe the method used to quantify the accident sequences defined in Appendix A that result in a core melt. The basic approach to calculate a sequence frequency is to multiply the probabilities associated with the various events depicted in the accident sequence. That is, the frequency of the sequence is equal to the frequency of the initiating event multiplied times the probability of system (or systems) failure. Sequence quantification was based on the systemic event trees for LOCAs and transients. For each system, the unavailability was calculated from the fault trees using the Reliability Analysis System (RAS) computer code.¹ System minimal cut sets of order five or more and having a probability value less than 10^{-8} were truncated.

Dependencies were incorporated in the risk analysis at various stages. During event tree formulation, functional dependencies between the various accident mitigating systems were depicted in the accident sequence construction. The fault trees for the front-line systems were constructed considering potential interface dependencies such as human error, test and maintenance, and support systems. Finally, in the event tree quantification, system fault trees were reduced by Boolean techniques using the COMCAN code² to pinpoint any further common dependencies between systems.

The potential for recovery was considered for those sequences where the dominant contributors to sequence frequency were recoverable.

1.1 System Unavailabilities

Each front-line and support system fault tree was evaluated using the RAS computer code. The RAS code resolves the fault tree into its minimal cut sets and evaluates the system unavailability based on the failure data associated with the basic events. RAS calculates a time dependent unavailability that was specified for this analysis as 8 hours. The analysis considered stable hot shutdown as successful core cooling. After discussion with TVA personnel,³ the time limit of 8 hours was chosen as a reasonable limit for reaching stable hot shutdown conditions.

The RAS code calculates component unavailabilities based on the failure rate data. Failure rates may be entered either as demand rates or hourly rates.

1.1.1 Demand Failure Probabilities

Standby safety systems are characterized by having many components that are required to change state when the system is demanded. The RAS computer code treats the demand failure probabilities for these components as a constant unavailability. That is, these values are unaffected by the length of time the system is required to operate (8-hour mission time as noted

above). However, it is possible that these components could have been tested, found to be failed, and undergoing repair at the time the accident or transient places the demand for the component. This unscheduled maintenance contribution to the unavailability of the component (and therefore, system) is negligible compared with demand failures when the component repair time is small compared to the testing interval. This is shown as follows:

$$Q = (\text{unavailability on demand}) + (\text{unavailability due to unscheduled maintenance})$$

$$= Q_D + \frac{Q_D T_R}{T} = Q_D (1 + T_R/T),$$

where

Q_D = demand unavailability

T = testing interval

T_R = repair time.

If $T_R \ll T$, then

$$Q = Q_D (1 + 0)$$

$$= Q_D.$$

A review of Browns Ferry component data shows that this is the case. Typically, T_R is less than 3 days and T is 1 month. Thus, the unscheduled maintenance contribution at Browns Ferry is negligible for demand failures.

1.1.2 Time-Dependent Failure Probabilities

Some of the failure modes considered for components of standby safety systems are characterized as "fails to continue to run/operate given the initial demand on the component was successful." The RAS computer code calculates a time-dependent unreliability (λT_m) for these component failure modes based on the mission time; that is, the component is required to work for the length of the mission (T_m). Since the operability of the component is known at essentially mission time zero (given that the demand was successful), it is not necessary to consider any unavailability contribution due to unscheduled maintenance.

However, for components with failure rates (λ) given per hour, where it is not known at mission time zero if the component is in a failed state, it is necessary to determine the component unavailability manually based on the testing interval and repair time and then to enter this point estimate as a constant unavailability to the RAS code.

The unavailability for these components depends primarily on the time to detect faults, which depends on their testing interval (T). Assuming that the accident or transient is equally likely to occur at any time during

the testing interval results in an average value for the component unavailability of $\lambda T/2$. The time to detect failures was based on the testing frequencies in the surveillance procedures associated with the components of the system being modeled. For example, if the surveillance procedures for a certain system required a system flow check be performed once per month, then this test frequency was used to determine the time to detect failures associated with the pump in that system.

In addition to this average unavailability over the testing interval, it is necessary to account for the component unavailability due to unscheduled maintenance. That is, for components with hourly failure rates where it is not known at mission time zero if it is in a failed state, a modification to the unavailability must be made to account for the fact that the component may be undergoing repair at mission time zero due to a fault that occurred within the span of mission time zero minus the component repair time.

Correction to the unavailability is made in the following manner. The probability of the component entering a failed state during any testing interval is estimated as λT , where T is the testing interval. The maintenance unavailability during any testing interval equals the probability of being in a down state times the fraction of the interval during which the component is in repair. This fraction is the repair time T_R divided by the testing interval T . Thus, the unavailability due to unscheduled maintenance is $(\lambda T)(T_R/T)$, which equals λT_R . The unavailability for these components is modified by adding this factor to the previously calculated fault detection based value. This combined value is entered into the RAS code as a constant unavailability.

$$\begin{aligned} Q &= (\text{average unavailability over testing interval}) \\ &\quad + (\text{unavailability due to unscheduled maintenance}) \\ &= \lambda T/2 + \lambda T_R \\ &= \lambda(T/2 + T_R). \end{aligned}$$

Repair times were taken from Table III 5-2 of WASH-1400⁴ for pumps, valves, diesels, and instrumentation. Electrical components (other than diesels) were assumed to have the same repair rate as that shown for instrumentation (7 hours). Table C-1 summarizes the treatment of component unavailabilities used for system quantification.

1.2 Treatment of Commonalities

Wherever possible, the RAS code was used to evaluate the unavailability of combinations of systems. However, due to the complexity of the individual system fault trees, computer core space, and processing time limitations, this method was not viable for some system combinations and the following approach was used.

1.2.1 Use of COMCAN

The unavailability of two systems in an AND logic configuration is equal to the product of the individual unavailabilities if the cut sets for

TABLE C-1. COMPONENT UNAVAILABILITIES

<u>Failure Mode</u>	<u>Unavailability without Unscheduled Maintenance</u>	<u>Unscheduled Maintenance</u>	<u>Final Unavailability</u>
Fails to start/operate when required	Q_D	$Q_D T_R / T$	Q_D^*
Fails to continue to run/operate, given start	λT_m	None	λT_m
Fails to run/operate, successful start not given	$\lambda T / 2$	λT_R	$\lambda (T / 2 + T_R)$

Q_D = demand unavailability
 T_R = repair time
 T = testing interval
 T_m = mission time

* $T_R \ll T$.

the two systems are independent. If dependent cut sets exist, then the unavailability of the combined systems equals the product of the independent cut sets plus the value of the dependent sets. Equations (C1) and (C2) apply.

$$Q(A \cap B) = Q(A)Q(B), \text{ if } A \text{ and } B \text{ are independent} \quad (C1)$$

$$Q(A \cap B) = Q(A_I)Q(B_I) + Q(D), \text{ if } A \text{ and } B \text{ are dependent,} \quad (C2)$$

since

$$Q(A) = Q(A_I) + Q(D)$$

$$Q(B) = Q(B_I) + Q(D),$$

where

$$Q(A_I) = \text{unavailability of cut sets in } A \text{ independent of } B$$

$$Q(B_I) = \text{unavailability of cut sets in } B \text{ independent of } A$$

$$Q(D) = \text{unavailability of dependent cut sets in both.}$$

To calculate the unavailability of the dependent cut sets for the two systems, the COMCAN code was used to identify the commonalities between the systems. The COMCAN code does not quantify the commonalities, but identifies those combinations of similar events which can cause both systems to fail.

The fault tree models for the systems evaluated on COMCAN were modified so that the first three characters in the eight-character code for each support system were the same (SUP). This allowed COMCAN to identify all combinations of support systems that could cause both systems to fail. COMCAN also identified, based on the first three characters in the eight-digit code, all combinations of similar basic events (i.e., those with the same three characters) that could cause both systems to fail. These cut sets were then evaluated manually or using RAS.

The unavailability of the potentially dependent cut sets identified by COMCAN were compared to the unavailability of the systems assuming independence. If the unavailability of these common sets was at least two orders of magnitude less than the unavailability of both systems assuming independence, then the unavailability assuming independence was used. If the unavailability of the common sets was less than two orders of magnitude smaller than the unavailability assuming independence, the sum of the two was used to represent the unavailability of the two system combination. Equations (C3) through (C5) apply.

$$Q(A \cap B) = Q(A_I)Q(B_I) + Q(D), \quad (C3)$$

If $Q(D) \ll Q(A)Q(B)$, then

$$Q(A \cap B) = Q(A_I)Q(B_I) \approx Q(A)Q(B). \quad (C4)$$

If $Q(D) \geq \frac{Q(A)Q(B)}{100}$, then

$$\begin{aligned} Q(A \cap B) &= Q(A_I)Q(B_I) + Q(D), \text{ or} \\ &\approx Q(A)Q(B) + Q(D). \end{aligned} \quad (C5)$$

Note that the product of $Q(A)Q(B)$ is always greater than or equal to $Q(A_I)Q(B_I)$. No attempt was made to determine $Q(A_I)$ or $Q(B_I)$. Instead, the minimal conservatism caused by using $Q(A)$ and $Q(B)$ in the equations for finding $Q(A \cap B)$ was not significant enough to justify the time and expense of calculating $Q(A_I)$ or $Q(B_I)$ (by removing $Q(D)$ from the fault trees for A and B and recalculating their unavailabilities using RAS).

1.2.2 Treatment of Commonalities Not Found Using COMCAN

A potential problem involved with using COMCAN in this manner to calculate the unavailability of two systems is that only those cut sets that are combinations of events with the same first three characters in their code identifier are identified. Although COMCAN has other uses, this analysis used the code only in one mode of operation as described before. Therefore, if a cut set X exists in System A and a cut set XY exists in System B where the first three characters of the basic event Y are different from those in X, COMCAN will not identify either cut set as a potential common candidate. Although X and XY are not the same cut set and are thus only partially dependent, the dependence that comes from X having an effect on both systems must be accounted. Equations (C6) through (C9) apply to this situation.

Let

$$Q(A) = Q(A_1) + \text{COM}(A \cap B) + Q(X), \text{ and} \quad (C6)$$

$$Q(B) = Q(B_1) + \text{COM}(A \cap B) + Q(XY), \quad (C7)$$

where

$Q(A_1)$ and $Q(B_1)$ are defined as before

$\text{COM}(A \cap B)$ = unavailability of commonalities found using COMCAN

$Q(X)$ = unavailability of a cut set in A

$Q(XY)$ = unavailability of a cut set in B;

then

$$Q(A \cap B) = Q(A_1)Q(B_1) + \text{COM}(A \cap B) + Q(XY), \quad (C8)$$

but using COMCAN as previously described only produces

$$Q(A \cap B) = Q(A)Q(B) + \text{COM}(A \cap B). \quad (C9)$$

The problem of identifying all the X,XY combinations possible between two systems at this point is impractical. Therefore, a numerical bounding analysis was used to determine whether or not such a combination, if it existed, would have a value large enough to cause a significant nonconservative error in the evaluation of $Q(A \cap B)$ previously discussed.

In order for the X,XY combination to be important, the unavailability $Q(XY)$ must be on the same order of magnitude as $Q(A \cap B)$ previously calculated. The RAS code lists cut set probabilities in descending order of magnitude such that the unavailability of the first cut set listed is always greater than or equal to that of the second cut set listed. Equations (C10) and (C11) apply.

From RAS,

$$Q(A) = Q(A_1) + Q(A_2) + \dots + Q(A_n), \quad (C10)$$

where

$$Q(A_1) \geq Q(A_2) \geq \dots \geq Q(A_n). \quad (C11)$$

Therefore, the highest valued cut set for Systems A and B is readily identified and hereafter identified as A_T or B_T . Thus, if the X,XY combination exists, $Q(X) \leq Q(A_T)$ and $Q(XY) \leq Q(B_T)$.

Assuming that the X,XY combination exists and that the unavailability $Q(XY)$ is greater than or equal to one tenth of the value of $Q(A \cap B)$ calculated previously, a lower bound on the value of Y can be determined. Equations (C12) through (C19) apply.

If

$$Q(XY) \geq \frac{Q(A \cap B)}{10}, \text{ and} \quad (C12)$$

$$Q(A_T) \geq Q(X), \quad (C13)$$

then

$$Q(A_T Y) \geq Q(XY). \quad (C14)$$

Therefore,

$$Q(A_T Y) \geq Q(XY) \geq \frac{Q(A \cap B)}{10}, \text{ or} \quad (C15)$$

$$Q(A_T Y) \geq \frac{Q(A \cap B)}{10}. \quad (C16)$$

But

$$Q(A_T Y) = Q(A_T)Q(Y) \quad (C17)$$

since they are independent.

Thus,

$$Q(A_T)Q(Y) \geq \frac{Q(A \cap B)}{10}, \text{ and} \quad (C18)$$

$$Q(Y) \geq \frac{Q(A \cap B)}{10 \cdot Q(A_T)}. \quad (C19)$$

Using this lower bound for $Q(Y)$, the basic event list for System B is searched to see if any basic events exist in B with unavailabilities greater than $Q(Y)$. If not, then there can not exist any X,XY combinations whose unavailability $Q(XY)$ is significant compared to $Q(A \cap B)$.

If there are basic events in B that have unavailabilities greater than $Q(Y)$, a list of these events is made. Then the cut set list of System B is examined. Each cut set containing a basic event from the list is examined to see if its comembers appear as cut sets of A. If not, then no X,XY combinations of significance exist. If the comembers are cut sets of A by themselves, then the value of that XY type cut set is added to the previously calculated value of $Q(A \cap B)$. The process is then repeated to determine if any X,XY combinations exist where X is in System B and XY is in A.

It should be noted that this method will detect dependencies not found using COMCAN that are within one order of magnitude of the value of $Q(A \cap B)$. Dependencies with values less than $Q(A \cap B)/10$ may not be located. The choice for $Q(A \cap B)/10$ as a bounding value is an arbitrary

one based on engineering judgement and familiarity with the systems. The bounding value could be chosen as $Q(A \cap B)/100$ or $Q(A \cap B)/1000$ if desired. The latter choices merely expand the scope of the manual search of the system cut set lists. The method described above is conservative, however, because: $Q(A_T)$ is an upper bound for the unavailability of potential cut sets X of A completely contained in cut sets of B ; and an examination of the Browns Ferry cut set lists, for cases where this issue applies, shows that $Q(A_T)$ is always several orders of magnitude greater than the highest-valued unavailability of a cut set in A containing any basic events that are also in B .

1.3 Treatment of Complement or Success Sets

It is necessary in sequence quantification to account for the effect of success of one system in an AND combination with failure of another. Since the RAS code does not deal with complement or success sets, they were treated in the following manner. If the systems are totally independent then Equation (C20) applies.

$$Q(\bar{A} \cap B) = Q(\bar{A})Q(B), \quad (C20)$$

where \bar{A} designates success for A .

If there are common cut sets between A and B , then Equations (C21) and (C22) apply.

$$Q(\bar{A} \cap B) = Q(\bar{A})Q(B_I) \quad (C21)$$

$$Q(\bar{A} \cap B) = Q(\bar{A}) [Q(B) - \text{COM}(A \cap B)], \quad (C22)$$

where

$\text{COM}(A \cap B)$ = value of common cut sets of A and B

$Q(B_I)$ = value of cut sets of B independent of A .

A screening tool used in the sequence quantification determines when potential commonalities of significance may exist. If $Q(B) \gg Q(A)$, then even if all of A is assumed to be common with B , $Q(B)$ is still essentially equal to $Q(B_I)$. If $Q(B) \leq Q(A)$, then a COMCAN search is used to identify the potential commonalities. If the unavailability of the commonalities $\text{COM}(A \cap B)$ is much less than $Q(B)$, then again $Q(B)$ is essentially equal to $Q(B_I)$. Otherwise, $Q(B_I)$ is calculated by subtracting $\text{COM}(A \cap B)$ from $Q(B)$. Also, since $Q(\bar{A})$ equals $1 - Q(A)$ and $Q(A)$ is usually small, $Q(\bar{A}) \approx 1$ in most cases. Therefore, Equation (C23) applies.

$$Q(\bar{A} \cap B) \approx Q(B) - \text{COM}(A \cap B). \quad (C23)$$

Therefore, success sets, or complements, are accounted for by either recognizing the nonsignificant potential impact or by evaluating the known commonalities for significance and including their effect where appropriate.

1.4 Treatment of Initiator Effects on Mitigating Systems

Some of the LOCA initiators have the potential to render LOCA mitigation systems partially or completely inoperable. To account for this possibility in the sequence calculations, the following procedure was used.

If a LOCA initiator could disable a mitigating system, the length of piping for the mitigating system susceptible to that LOCA was calculated using TVA supplied isometric drawings. Then, the total length of piping susceptible to that initiator was calculated. It was assumed that for a particular break size, the LOCA was equally likely to occur at any point on the piping susceptible to the LOCA. The unavailability of the mitigating systems was calculated considering the initiator affecting the system and then without considering the effect of the initiator. Therefore, the sequence frequency is the sum of two terms. The first term is the product of the probability of a break occurring in a location that affects the mitigating systems and the unavailabilities of those systems. The second term is the product of the probability of the break occurring in a location that does not affect the mitigating systems and the unavailability of those systems under that condition. The example calculation in Section 2 provides an example of this method.

For transient initiators, Section 2.3.2 of Appendix A describes the methodology for identifying potential transient initiators that would affect the unavailabilities of the mitigating systems. Only the loss of offsite power (LOSP) event was significant in this regard. A separate event tree exists for this particular initiator.

1.5 Treatment of Potential Logic Loops

A potential problem in the quantification of $T_{pR_B R_A}$, as well as the other sequences involving loss of offsite power ($T_{pQR_B R_A}$ and $T_{pKR_B R_A}$), is the presence of loop dependencies. That is, the EECW system requires electrical power in order to function. Given a loss of offsite power, this power must come from the diesel generators. However, the diesel generators need EECW or they will eventually fail.

This problem was resolved by recognizing three important considerations. First, the diesels can operate for some finite time without rated flow from the EECW system. Second, the diesels that supply EECW are not all the same as those supplying power to other mitigating systems. Figure C-1 shows the power dependencies between the RHR, RHRSW, and EECW systems. Third, EECW represents a common mode failure not only of the diesel generators but all AC powered mitigating systems.

Therefore, quantification of sequences involving loss of offsite power requires a special process. First, the unavailability of EECW is calculated assuming that diesel failures are not caused by loss of EECW. In other words, EECW does not cause its own failure. Then, the mitigating systems' unavailabilities are calculated assuming successful EECW operation. This

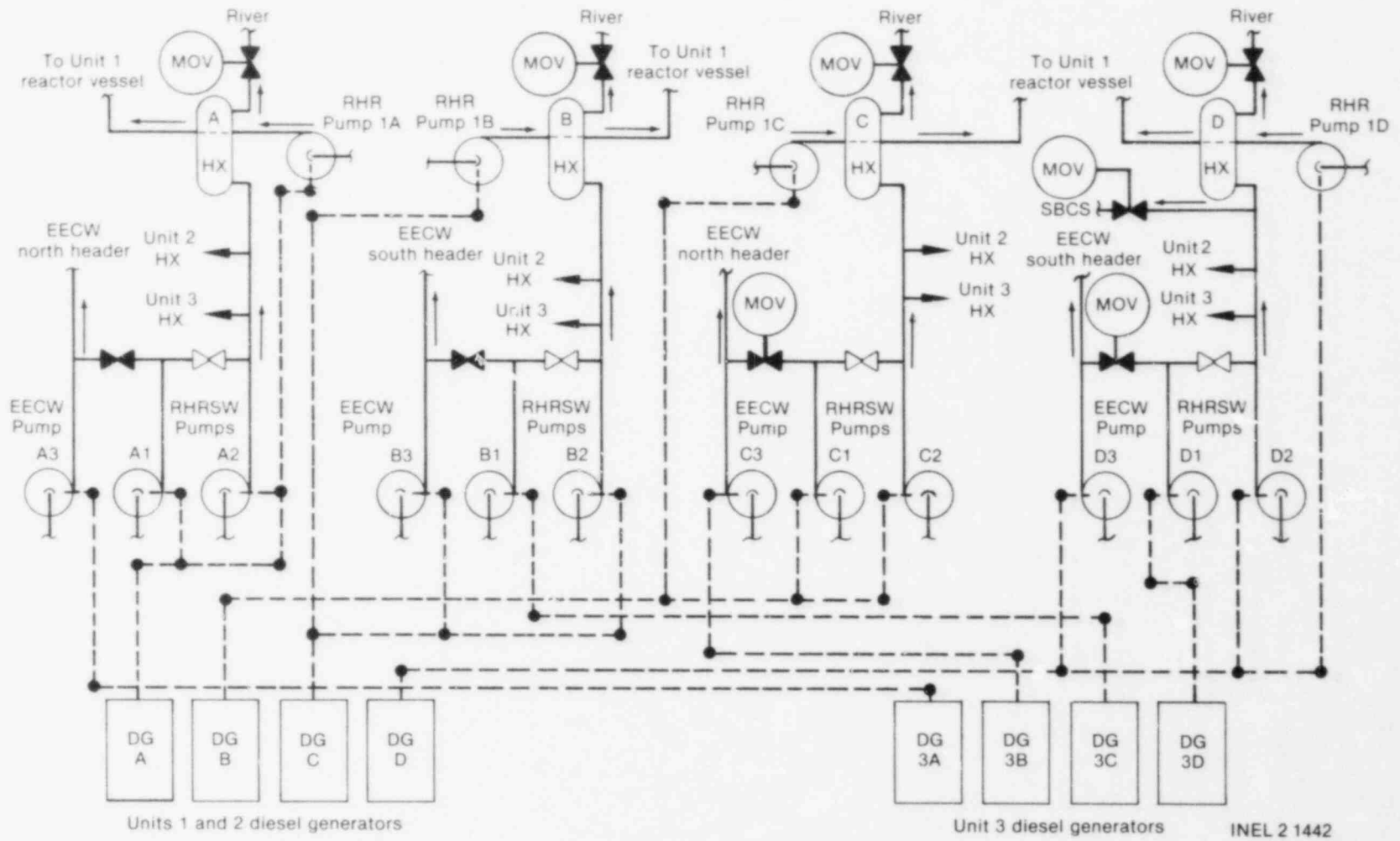


Figure C-1. RHR/RHRSW/EECW system power dependencies.

value added to the EECW unavailability represents the total system unavailability. That is, the system unavailability can be dichotomized into the unavailability due to EECW faults and the unavailability assuming EECW works. When considering the case where two or more AC systems must fail, the EECW unavailability is treated as a common mode failure of both AC systems. Thus, for a general sequence, the frequency is given by the following equations.

$$\begin{aligned}
 F(\text{seq}) &= F(\text{LOSP})[Q(\text{DC powered systems}) \cap Q(\text{AC powered systems})] \\
 &= F(\text{LOSP})Q(\text{DC systems})[Q(\text{AC systems given EECW works}) \cup Q(\text{EECW})] \\
 &= F(\text{LOSP})Q(\text{DC systems})Q(\text{AC systems given EECW works}) \\
 &\quad + F(\text{LOSP})Q(\text{DC systems})Q(\text{EECW}).
 \end{aligned}$$

In general, the unavailability of EECW was about an order of magnitude higher than the unavailability of the combinations of AC powered systems. Therefore, these sequences tended to be dominated, at least in part, by EECW faults.

2. EXAMPLE CALCULATION

The intermediate steam break was chosen for this example calculation since its sequence quantification requires the use of all the methods described previously. All of the intermediate steam break sequences are evaluated in this example. Figure C-2 is the systemic event tree for the intermediate steam break with the system and sequence values filled in.

2.1 Initiator Frequency

The intermediate steam break frequency was determined to be 2.1×10^{-4} per reactor-year. Since 70% of all piping susceptible to intermediate breaks is steam piping, the remaining 30% of the piping would cause an intermediate liquid break if it ruptured. The WASH-1400 frequency of 3×10^{-4} per reactor-year was used as the frequency of all intermediate breaks. Assuming that an intermediate break was equally likely to occur at any point in the piping susceptible to intermediate breaks, the frequency of intermediate steam breaks would be 70% of 3×10^{-4} , or 2.1×10^{-4} per reactor-year.

2.2 Example System Unavailabilities

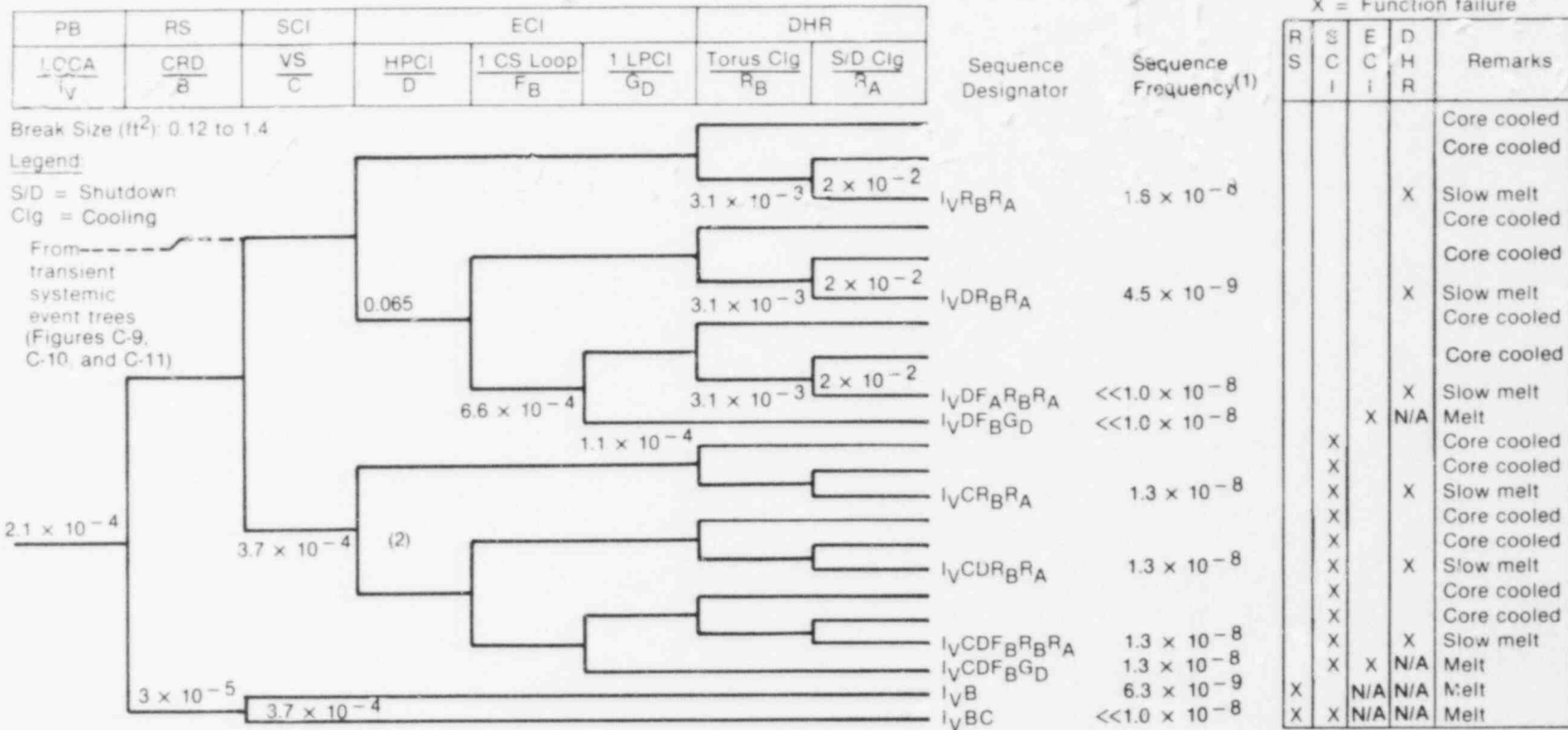
2.2.1 Reactor Subcriticality

The unavailability for the reactor subcriticality function was taken from NUREG-0460⁵ to be 3×10^{-5} per demand. A qualitative model was developed (in Appendix B, Section 2.9.4) for the control rod drive mechanism but was not quantified since insufficient data exists for estimating the occurrence rate for common mode failures identified in the model.

2.2.2 Vapor Suppression System

Short-term containment integrity (SCI) is maintained and containment overpressurization is prevented by directing the steam from the break through the downcomer piping to a position below the water level of the torus. This action condenses the steam formed and provides a "scrubbing" effect to trap radioactivity from the steam in the torus water rather than allowing it to remain airborne. Failure of the vapor suppression system will result in a containment rupture and a release of radioactivity. The amount of radioactivity released depends on the performance of the ECI and DHR systems.

Bypass leakage from the drywell to the airspace of the wetwell could pressurize the wetwell airspace to the same pressure as the drywell, preventing the pressure differential required to force the steam through the downcomer piping into the pool of water in the suppression chamber (torus). Therefore, the quenching and scrubbing features will not be accomplished and overpressurization will result. The RAS code was used to evaluate the vapor suppression system unavailability from the fault tree given in Appendix B, Section 2.8.4, and the value 3.7×10^{-4} was obtained. Dominant cut sets are listed in Table B-53 of Appendix B.



(1) Sequence values include contributions from system commonalities, but do not include operator recovery actions.
 (2) Conditional probability of torus failure gives VS failure ~ 0.162.

Figure C-2. LOCA systemic event tree for intermediate steam break (I_V), with system and sequence values filled in.

2.2.3 Emergency Cooling During Injection

There are three systems available to mitigate the intermediate liquid break. These are the HPCI, core spray, and LPCI systems. The designations for these systems for the systemic event trees are D, F_B, and G_D, respectively. Table C-2 lists each system, its failure criteria, the unavailability for each calculated by the RAS code, and Appendix B tables for lists of dominant cut sets. Operation of any of these three systems is sufficient to perform the ECI function.

TABLE C-2. INTERMEDIATE STEAM BREAK ECI CRITERIA

System Designation	Failure Criteria	Unavailability	Appendix B Dominant Cut Set Table Number
D	HPCI fails to inject rated flow to core	6.5×10^{-2}	B-33
F _B	Less than one of two core spray loops delivers rated flow to core	6.6×10^{-4}	B-47
G _D	Less than one of four LPCI pumps delivers rated flow to core	1.1×10^{-4}	B-17 B-18

2.2.4 Decay Heat Removal

There is only one system that performs the DHR function, the RHR system. However there are two modes of RHR used to mitigate the intermediate liquid break: torus cooling (R_B) and shutdown cooling (R_A). Either torus cooling or shutdown cooling must operate to remove decay heat from the reactor to prevent containment overpressurization and eventual core melt.

Table C-3 summarizes the failure criteria for each mode of RHR operation and presents Appendix B dominant contributor tables, and the unavailability from the RAS code for each. It is noteworthy that, although R_A only requires one of four pumps and heat exchangers where R_B requires two of four, the unavailability of R_A is significantly higher than that of R_B. This is because shutdown cooling (R_A) uses a single suction line with three MOVs, whereas torus cooling (R_B) uses a double suction line with no valves required to change position.

TABLE C-3. DECAY HEAT REMOVAL FAILURE CRITERIA

System Designation	Failure Criteria	Unavailability	Appendix B Dominant Cut Set Table Number
R _A	Less than one of four pump and heat exchanger combinations recirculating reactor coolant	2.0 x 10 ⁻²	B-19 B-20
R _B	Less than two of four pump and heat exchanger combinations recirculating torus water	3.1 x 10 ⁻³	B-21

2.3 Sequence Calculations

There are 10 core melt sequences on the intermediate steam break systemic event tree. Six sequences involve failure of the DHR function, two involve failure of the reactor subcriticality function, and two involve failure of the ECI function. The sequences are designated by the initiating event letter code, I_V, and the system(s) failure code associated with the particular sequence.

2.3.1 Sequence I_VR_BR_A

In this sequence the reactor subcriticality, vapor suppression, and HPCI systems perform satisfactorily, but the torus cooling and shutdown cooling modes of the RHR system fail. The unavailability of torus cooling and shutdown cooling for this sequence is 7.6 x 10⁻⁵ as shown below.

$$\begin{aligned}
 Q(R_B R_A) &= Q(\bar{B} \cap \bar{C} \cap \bar{D} \cap R_B \cap R_A) \\
 &= Q(R_B \cap R_A) - \text{COM}[R_B \cap R_A \cap (B \cup C \cup D)] \\
 &= Q(R_B \cap R_A) - \text{COM}(R_B \cap R_A \cap B) - \text{COM}(R_B \cap R_A \cap C) - \text{COM}(R_B \cap R_A \cap D) \\
 &= Q(R_B \cap R_A) - 0 - 0 - 0 \\
 &= Q(R_B) Q(R_A) + \text{COM}(R_B \cap R_A) \\
 &= (3.1 \times 10^{-3})(2.0 \times 10^{-2}) + 1.4 \times 10^{-5} \\
 &= 7.6 \times 10^{-5}.
 \end{aligned}$$

The term $COM[(R_B \cap R_A \cap (B \cup C \cup D))]$ accounts for success of the systems preceeding $R_B \cap R_A$ precluding some failure modes of $R_B \cap R_A$. In this case, they are negligible. The term $COM(R_B \cap R_A)$ accounts for commonalities between R_B and R_A . These commonalities were identified using the methods of Section 1.2 above. Three dominant cut set tables in Appendix B (Tables B-19 through B-21) apply to the RHR system (two tables for two loops of R_A and one table for R_B). However, cut sets that simultaneously fail all three systems cannot be readily identified from these tables. Rather, a case-by-case examination of potential commonalities flagged by COMCAN runs was required. The results showed that commonalities between R_B and R_A are primarily due to minimum-flow bypass valve faults.

Since the initiator has no effect on torus cooling or shutdown cooling, the sequence frequency is equal to the product of the initiator frequency and the systems unavailability:

$$\begin{aligned} P(I_V R_B R_A) &= F(I_V) Q(R_B R_A) \\ &= (2.1 \times 10^{-4})(7.6 \times 10^{-5}) \\ &= 1.6 \times 10^{-8}. \end{aligned}$$

2.3.2 Sequence $I_V D R_B R_A$

This sequence is similar to the previous one, but in this sequence the HPCI system fails. The core spray system operates to replace the lost reactor coolant. Subsequently, torus cooling and shutdown cooling fail. The unavailability for HPCI, torus cooling and shutdown cooling is 4.9×10^{-6} as shown below.

$$\begin{aligned} Q(D R_B R_A) &= Q(\bar{B} \cap \bar{C} \cap D \cap \bar{F}_B \cap R_B \cap R_A) \\ &= Q(D \cap R_B \cap R_A) - COM[D \cap R_B \cap R_A \cap (B \cup C \cup F_B)] \\ &= Q(D \cap R_B \cap R_A) - 0 \\ &= Q(D) Q(R_B \cap R_A) + COM(D \cap R_B \cap R_A) \\ &= (0.065)(7.6 \times 10^{-5}) + 0 \\ &= 4.9 \times 10^{-6}. \end{aligned}$$

The term $COM[(D \cap R_B \cap R_A \cap (B \cup C \cup F_B))]$ accounts for the success of the reactor subcriticality, vapor suppression, or core spray systems precluding some failure modes of $D \cap R_B \cap R_A$. In this case, they are negligible. The term $COM(D \cap R_B \cap R_A)$ accounts for commonalities between the HPCI system and $R_B \cap R_A$. These are also negligible.

Unlike the previous sequence, the initiator can affect the mitigating systems for this sequence since 23.2% of the piping susceptible to intermediate steam breaks is HPCI piping. The first term in the equation below, $0.232 F(I_V)Q(R_B R_A)$, represents the frequency when the break is on the HPCI line. Note that D does not appear in this term since it is assumed that the break disables HPCI. The term $0.768 F(I_V)Q(DR_B R_A)$ represents the sequence frequency for intermediate steam breaks that do not affect HPCI operability.

$$\begin{aligned}
 P(I_V DR_B R_A) &= 0.232 F(I_V) Q(R_B R_A) + 0.768 F(I_V) Q(DR_B R_A) \\
 &= (0.232)(2.1 \times 10^{-4})(7.6 \times 10^{-5}) + (0.768)(2.1 \times 10^{-4})(4.9 \times 10^{-6}) \\
 &= 3.7 \times 10^{-9} + 8.0 \times 10^{-10} \\
 &= 4.5 \times 10^{-9}.
 \end{aligned}$$

2.3.3 Sequence $I_V DF_B R_B R_A$

After successful operation of the reactor subcriticality and vapor suppression systems, both the HPCI and core spray systems fail. The LPCI mode of RHR functions properly but torus cooling and shutdown cooling fail. The unavailability for the mitigating systems for this sequence is negligible as shown below.

$$\begin{aligned}
 Q(DF_B R_B R_A) &= Q(\bar{B} \cap \bar{C} \cap D \cap F_B \cap \bar{G}_D \cap R_B \cap R_A) \\
 &= Q(D \cap F_B \cap R_B \cap R_A) - \text{COM}[D \cap F_B \cap R_B \cap R_A \cap (B \cup C \cup G_D)] \\
 &= Q(D \cap F_B \cap R_B \cap R_A) - \text{COM}(D \cap F_B \cap R_B \cap R_A \cap B) \\
 &\quad - \text{COM}(D \cap F_B \cap R_B \cap R_A \cap C) \\
 &\quad - \text{COM}(D \cap F_B \cap R_B \cap R_A \cap G_D) \\
 &= Q(D \cap F_B \cap R_B \cap R_A) - \text{COM}(D \cap F_B \cap R_B \cap R_A \cap G_D) - 0 - 0 \\
 &= Q(D) Q(F_B) Q(R_B \cap R_A) + \text{COM}(D \cap F_B \cap R_B \cap R_A) \\
 &\quad - \text{COM}(D \cap F_B \cap R_B \cap R_A \cap G_D) \\
 &= Q(D) Q(F_B) Q(R_B \cap R_A) + 0 - \text{COM}(D \cap F_B \cap R_B \cap R_A \cap G_D).
 \end{aligned}$$

The term $\text{COM}[D \cap F_B \cap R_B \cap R_A \cap (B \cup C \cup G_D)]$ accounts for success of the reactor subcriticality, vapor suppression, or LPCI mode of RHR precluding some failure modes of $D \cap F_B \cap R_B \cap R_A$. In this case the contribution from reactor subcriticality or vapor suppression is negligible.

However, the success of the LPCI mode precludes the dominant contributors to failure of $R_B \cap R_A$. Therefore, the value of $Q(DF_B R_B R_A)$ is much less than the 3.9×10^{-9} value obtained by ignoring the success of the LPCI mode.

Since the initiator frequency for this sequence is 2.1×10^{-4} and the unavailability $Q(DF_B R_B R_A)$ must be less than 3.9×10^{-9} , the sequence frequency will be much less than 1.0×10^{-8} . As discussed later, 1.0×10^{-8} was chosen as the initial screening value for determining candidate dominant sequences. Since it is obvious that this sequence frequency will be less than 1.0×10^{-8} , no further quantification is necessary.

2.3.4 Sequence I_VDF_BG_D

Following successful reactor subcriticality and vapor suppression system operation, none of the ECI systems operate to restore reactor vessel water level. The unavailability for the mitigating systems for this sequence is 7.2×10^{-9} , as shown below.

$$\begin{aligned}
 Q(DF_B G_D) &= Q(\bar{B} \cap \bar{C} \cap D \cap F_B \cap G_D) \\
 &= Q(D \cap F_B \cap G_D) - \text{COM}[D \cap F_B \cap G_D \cap (B \cup C)] \\
 &= Q(D \cap F_B \cap G_D) - 0 \\
 &= Q(D) Q(F_B \cap G_D) + \text{COM}(D \cap F_B \cap G_D) \\
 &= Q(D) Q(F_B \cap G_D) + 0 \\
 &= Q(D) [Q(F_B) Q(G_D) + \text{COM}(F_B \cap G_D)] \\
 &= (0.065)(7.3 \times 10^{-8} + 3.4 \times 10^{-8}) \\
 &= 7.2 \times 10^{-9}.
 \end{aligned}$$

The term $\text{COM}[D \cap F_B \cap G_D \cap (B \cup C)]$ accounts for success of either reactor subcriticality or vapor suppression precluding some failure modes of $D \cap F_B \cap G_D$. In this case they are negligible. The term $\text{COM}(D \cap F_B \cap G_D)$ accounts for commonalities between the HPCI system and the combination of $F_B \cap G_D$. The term $\text{COM}(F_B \cap G_D)$ accounts for commonalities between $F_B \cap G_D$ that are primarily due to combinations of electric power faults.

In this sequence also, the initiator can effect the mitigating systems since 23.2% of piping susceptible to intermediate steam breaks is HPCI piping and 3.8% is core spray piping. The term $0.232 Q(F_B G_D)$ accounts for that percentage of breaks that disables HPCI. Therefore, D does not appear in this term. The next term, $0.038 Q(DF_B' G_D)$, accounts for those breaks that disable one core spray loop. The term F_B' represents the unavailability of the remaining loop; its probability is less than that

of F_B since there are no longer two loops available in this case. The last term, $0.730 Q(DF_B G_D)$, accounts for breaks not occurring on any of the mitigating systems. As with the previous sequence, this sequence is designated as having a frequency less than 1×10^{-8} .

$$\begin{aligned}
 P(I_V DF_B G_D) &= F(I_V) [0.232 Q(F_B G_D) + 0.038 Q(DF_B G_D) + 0.730 Q(DF_B G_D)] \\
 &= (2.1 \times 10^{-4}) [(0.232)(1.1 \times 10^{-7}) + (0.038)(0.065)(5.7 \times 10^{-6}) \\
 &\quad + 0.730 (7.2 \times 10^{-9})] \\
 &= (2.1 \times 10^{-4}) (2.6 \times 10^{-8} + 1.4 \times 10^{-8} + 5.3 \times 10^{-9}) \\
 &= (2.1 \times 10^{-4}) (4.5 \times 10^{-8}) \\
 &< 1 \times 10^{-8}.
 \end{aligned}$$

2.3.5 Sequences $I_V CR_B RA$, $I_V CDR_B RA$, $I_V CDF_B R_B RA$, and $I_V CDF_B G_D$

These sequences are identical to the four sequences just discussed except that the vapor suppression system fails to operate properly and overpressurization of the containment occurs. Overpressurization causes the containment to rupture. This could impact the ability of the ECI and DHR functions if the rupture occurs below the water line of the torus. Assuming that the break is equally likely to occur anywhere on the primary containment boundary, the probability of the break occurring below the torus water line is equal to the ratio of surface area of the containment below the water line to the total surface area (about 0.162). Therefore, the unavailability of the ECI and DHR systems given vapor suppression system failure is $0.162 + 0.838$ (the unavailability for those systems from the vapor suppression system success sequences). In each case, the dominant contributor to ECI or DHR failure is where the rupture occurs below the torus water line. Thus, the unavailability of the mitigating systems for these sequences are equal and have a value of 6.0×10^{-5} as shown below. The designator X in this case represents the combination of any of the four previous ECI or DHR systems.

$$\begin{aligned}
 Q(CX) &= Q(\bar{B} \cap C \cap X) \\
 &= Q(C \cap X) - \text{COM}(B \cap C \cap X) \\
 &= Q(C \cap X) - 0 \\
 &= Q(C)(0.162 + 0.838 Q(X)) \\
 &= Q(C)(0.162) \\
 &= 6.0 \times 10^{-5}.
 \end{aligned}$$

Therefore, the sequence frequency for each of these sequences is equal. The value of the frequency is the product of the initiator frequency and the systems unavailability.

$$\begin{aligned}
 P(I_V CX) &= F(I_V)Q(CX) \\
 &= (2.1 \times 10^{-4})(6.0 \times 10^{-5}) \\
 &= 1.3 \times 10^{-8}.
 \end{aligned}$$

2.3.6 Sequences I_VB and I_VBC

In both of these sequences, an intermediate steam break is followed by a failure to scram. While both sequences result in a core melt, they are treated as distinct sequences since the operability of the vapor suppression system can effect the magnitude of the radionuclide release by "scrubbing" some of the fission products prior to containment failure. The unavailabilities and sequence frequencies are given below.

$$\begin{aligned}
 Q(B) &= Q(B \cap \bar{C}) \\
 &= Q(B) - \text{COM}(B \cap C) \\
 &= 3.0 \times 10^{-5} - 0 \\
 &= 3.0 \times 10^{-5}
 \end{aligned}$$

$$\begin{aligned}
 Q(BC) &= Q(B \cap C) \\
 &= Q(B) Q(C) + \text{COM}(B \cap C) \\
 &= (3.0 \times 10^{-5})(3.7 \times 10^{-4}) + 0 \\
 &= 1.1 \times 10^{-8}
 \end{aligned}$$

$$\begin{aligned}
 P(I_V B) &= F(I_V) Q(B) \\
 &= (2.1 \times 10^{-4})(3.0 \times 10^{-5}) \\
 &= 6.3 \times 10^{-9}
 \end{aligned}$$

$$\begin{aligned}
 P(I_V BC) &= F(I_V) Q(BC) \\
 &= (2.1 \times 10^{-4})(1.1 \times 10^{-8}) \\
 &< 1.0 \times 10^{-8}.
 \end{aligned}$$

3. FAILURE DATA

3.1 Component Failure Data

Each of the failure events identified in the various fault trees and described by the eight-character event-naming code was assigned failure data so that fault tree quantification based on these events could be accomplished.

In general, the recommended data base provided by NRC (Table C-4) was utilized to obtain this failure data. WASH-1400 was the major source of the tabular data. However, in some instances, the WASH-1400 data is supplemented by data found in the various LER Data Summary NUREGs. For the Browns Ferry study, the generic WASH-1400 data was applied where appropriate.

Occasionally, a failure rate that corresponded directly to a specific component failure mode could not be determined from the data in Table C-4. In these cases, other methods were used to determine an acceptable failure rate for the component in question. Table C-5 lists these failure modes and the corresponding failure rates that were used in the BFI study. Most of these additional failure modes considered could be related to a similar failure mode category in the WASH-1400 data, with three exceptions:

1. Rupture disk leakage/rupture failure rates were estimated by using plant-specific data supplied by TVA.
2. No data source was available for the probability of heat exchanger or strainer plugging; an estimate of 1.0×10^{-6} per hour was used for these modes.
3. Since many of the motor-operated valves (MOV) and pump control circuits were similar in design, generic probability values were derived for output failure of typical MOV and pump motor control circuits. These values varied depending on whether the circuit was tested or demanded on a monthly or quarterly basis. The auto-initiation logic placing the "demand" on the control circuit was explicitly modeled in every case. The analysis of the generic control circuits can be found in Section 5 of Appendix B.

The repair times for components was taken from Table III 5-2 of WASH-1400, Summary of Major Maintenance Act Duration, for pumps, valves, diesels, and instrumentation. Electrical components (other than diesels) were assumed to have the same repair rate as that shown for instrumentation (7 hours).

3.2 Human Error Rates

Human errors of omission were included where appropriate in the fault tree models for errors involving test and maintenance, and those involving errors in response to an accident situation. Surveillance and maintenance instructions were reviewed to identify potential human errors during testing or maintenance and are discussed in Appendix B on a system-by-system basis. Emergency operating instructions were reviewed with regard to potential

TABLE C-4. IREP DATA TABLE 3A AND 3B

Mechanical Components
(from WASH-1400, Table III 4-1)

Component and Failure Mode	Failure Rate Type	Assessed Range		Median	Error Factor
Pumps (includes driver)					
Motor and turbine driven (generic class)					
Failure to start on demand	D ^a	3E-4	3E-3	1E-3	3
Failure to run, given start (normal environments)	O	3E-6	3E-4	3E-5	10
Failure to run, given start (extreme, post accident environments inside containment)	O	1E-4	1E-2	1E-3	10
Failure to run, given start (postaccident, after environmental recovery)	O	3E-5	3E-3	3E-4	10
Turbine driven pumps					
Failure to start on demand (failure rates shown are in addition to WASH-1400 values)	D	1E-3	1E-2	3E-3	3
Failure to run, given start (failure rates shown are in addition to WASH-1400 values)	O	1E-5	1E-4	3E-5	3
Valves					
Motor operated					
Failure to operate (includes driver)	D ^b	3E-4	3E-3	1E-3	3
Failure to remain open (plug)	D ^c	3E-5	3E-4	1E-4	3
Failure to remain open (plug)	S	1E-7	1E-6	3E-7	3
Rupture	S	1E-9	1E-7	1E-8	10
Solenoid operated					
Failure to operate	D ^b	3E-4	3E-3	1E-3	3
Failure to remain open (plug)	D	3E-5	3E-4	1E-4	3
Rupture	S	1E-9	1E-7	1E-8	10

C-22

TABLE C-4. (continued)

Mechanical Components (from WASH-1400, Table III 4-1)					
Component and Failure Mode	Failure Rate Type	Assessed Range		Median	Error Factor
Valves (continued)					
Air-fluid operated					
Failure to operate	D ^b	1E-4	1E-3	3E-4	3
Failure to remain open (plug)	D	3E-5	3E-4	1E-4	3
Failure to remain open (plug)	S	1E-7	1E-6	3E-7	3
Rupture	S	1E-9	1E-7	1E-8	10
Check valves					
Failure to open	D	3E-5	3E-4	1E-4	3
Internal leak (severe)	D	1E-7	1E-6	3E-7	3
Rupture	S	1E-9	1E-7	1E-8	10
Vacuum valve					
Failure to operate	D	1E-5	1E-4	3E-5	3
Manual valve					
Failure to operate (failure rates shown are in addition to WASH-1400 values)	D	3E-5	3E-4	1E-4	3
Failure to remain open (plug)	D	3E-5	3E-4	1E-4	3
Rupture	S	1E-9	1E-7	1E-8	10
Primary safety valves (PWR)					
Fail to open (failure rates shown are a revision of WASH-1400 values)	D	1E-3	1E-2	3E-3	3

TABLE C-4. (continued)

Mechanical Components (from WASH-1400, Table III 4-1)					
Component and Failure Mode	Failure Rate Type	Assessed Range		Median	Error Factor
Valves (continued)					
Primary safety valves (PWR) (continued)					
Premature open (failure rates shown are a revision of WASH-1400 values)	S	1E-6	1E-5	3E-6	3
Failure to reclose (given valve opened) (failure rates shown are a revision of WASH-1400 values)	D ^d	3E-3	3E-2	1E-2	3
Primary safety valves (BWR)					
Fail to open (failure rates shown are a revision of WASH-1400 values)	D	3E-3	3E-2	1E-2	3
Premature open (failure rates shown are a revision of WASH-1400 values)	S	1E-6	1E-5	3E-6	3
Fail to reclose (given valve opened) (failure rates shown are a revision of WASH-1400 values)	D	1E-3	1E-2	3E-3	3
Test valves, flow meters, orifices					
Failure to remain open (plug)	D	1E-4	1E-3	3E-4	3
Rupture	S	1E-9	1E-7	1E-8	10
Pipes					
Pipes \leq 3-in. diameter (per section)					
Rupture/plug	S + D	3E-11	3E-8	1E-9	30
Pipe $>$ 3-in. diameter (per section)					
Rupture/plug	S + D	3E-12	3E-9	1E-10	30

TABLE C-4. (continued)

Mechanical Components (from WASH-1400, Table III 4-1)					
Component and Failure Mode	Failure Rate Type	Assessed Range		Median	Error Factor
Clutch, mechanical					
Failure to operate	D ^b	1E-4	1E-3	3E-4	3
Scram rods (single)					
Failure to insert	D	3E-5	3E-4	1E-4	3
Electrical Components (from WASH-1400, Table III 4-2)					
Clutch, electrical					
Failure to operate	D ^a	1E-4	1E-3	3E-4	3
Premature disengagement	O	1E-7	1E-5	1E-6	10
Motors, electric					
Failure to start	D ^a	1E-4	1E-3	3E-4	3
Failure to run, given start (normal environment)	O	3E-6	3E-5	1E-5	3
Failure to run, given start (extreme environment)	O	1E-4	1E-2	1E-3	10
Relays					
Failure to energize	D ^a	3E-5	3E-4	1E-4	3
Failure of NO contacts to close, given energized	O	1E-7	1E-6	3E-7	3
Failure of NC contacts by opening, given not energized	O	3E-8	3E-7	1E-7	3

TABLE C-4. (continued)

Electrical Components (from WASH-1400, Table III 4-2)					
Component and Failure Mode	Failure Rate Type	Assessed Range		Median	Error Factor
Short across NO/NC contact	O	1E-9	1E-7	1E-8	10
Coil open	O	1E-8	1E-6	1E-7	10
Coil short to power	O	1E-9	1E-7	1E-8	10
Circuit breakers					
Failure to transfer	D ^a	3E-4	3E-3	1E-3	3
Premature transfer	O	3E-7	3E-6	1E-6	3
Switches					
Limit					
Failure to operate	D	1E-4	1E-3	3E-4	3
Torque					
Failure to operate	D	3E-5	3E-4	1E-4	3
Pressure					
Failure to operate	D	3E-5	3E-4	1E-4	3
Manual					
Failure to transfer	D	3E-6	3E-5	1E-5	3

TABLE C-4. (continued)

Electrical Components (from WASH-1400, Table III 4-2)					
Component and Failure Mode	Failure Rate Type	Assessed Range		Median	Error Factor
Switch contacts					
Failure of NO contacts to close given switch operation	D	1E-8	1E-6	1E-7	10
Failure of NC contacts by opening, given no switch operation	D	3E-9	3E-7	3E-8	10
Short across NO/NC contact	D	1E-9	1E-7	1E-8	10
Battery power system (wet cell)					
Failure to provide proper output	S	1E-6	1E-5	3E-6	3
Transformers					
Open circuit primary or secondary	O	3E-7	3E-6	1E-6	3
Short primary to secondary	O	3E-7	3E-6	1E-6	3
Solid state devices, high power applications (diodes, transistors, etc.)					
Fails to function	O	3E-7	3E-5	3E-6	10
Fails shorted	O	1E-7	1E-5	1E-6	10
Solid state devices, low power applications					
Fails to function	O	1E-7	1E-5	1E-6	10
Fails shorted	O	1E-8	1E-6	1E-7	10

TABLE C-4. (continued)

Electrical Components (from WASH-1400, Table III 4-2)					
Component and Failure Mode	Failure Rate Type	Assessed Range		Median	Error Factor
Diesels (complete plant)					
Failure to start	D	1E-2	1E-1	3E-2	3
Failure to run, emergency conditions, given start	O	3E-4	3E-2	3E-3	10
Diesels (engine only)					
Failure to run, emergency conditions, given start	O	3E-5	3E-3	3E-4	10
Instrumentation--general (includes transmitter, amplifier, and output devices)					
Failure to operate	O	1E-7	1E-5	1E-6	10
Shift in calibration	O	3E-6	3E-4	3E-5	10
Fuses					
Failure to open	D	3E-6	3E-5	1E-5	3
Premature open	O	3E-7	3E-6	1E-6	3
Wires (typical circuits, several joints)					
Open circuit	O	1E-6	1E-5	3E-6	3
Short to ground	O	3E-8	3E-6	3E-7	10
Short to power	O	1E-9	1E-7	1E-8	10

TABLE C-4. (continued)

Terminal boards

Open connection	0	1E-8	1E-6	1E-7	10
Short to adjacent circuit	0	1E-9	1E-7	1E-8	10

a. Demand probabilities are based on the presence of proper input control signals. For turbine driven pumps, the effect of failures of valves, sensors, and other auxiliary hardware may result in significantly higher overall failure rates for turbine driven pump systems.

b. Demand probabilities are based on presence of proper input control signals.

c. Plug probabilities are given in demand probability, and per hour rates, since phenomena are generally time dependent; but plugged condition may only be detected upon a demand of the system.

d. These rates are based on LERs for Babcock & Wilcox pressurizer PORV failure to reseal, given the valve has opened.

Abbreviations:

D = Demand failure rate (failures per demand)

O = Operating failure rate (failures per hour of operation)

S = Standby failure rate (failures per hour of standby)

S + D = Standby or operating failure rate (failures per hour).

TABLE C-5. COMPONENT DATA NOT AVAILABLE IN TABLE C-4

Component	Failure Mode	Unavailability Calculation	Remarks
Stop check valve	Does not open	1×10^{-4}	Used check valve rate
Governor control valve	Does not operate	3×10^{-4}	Used data for air/fluid operated valves
Rupture disks	Leakage/rupture	2.1×10^{-2}	$\lambda = 5.7 \times 10^{-5}/\text{hr}$ (based on information from TVA)
Time-delay relays	Premature close	1×10^{-4}	Used relay failure-to-energize rate
Heat exchanger	Plugged	1×10^{-6}	Engineering judgement
Strainer	Plugged	1×10^{-6}	Engineering judgement
MOV control circuit	No output	3.2×10^{-3} (8.8×10^{-3})	Generic rate based on monthly testing (quarterly)
Pump control circuit	No output	2.9×10^{-3} (8.4×10^{-3})	Generic rate based on monthly testing (quarterly)

accident scenarios to determine the required human interactions with mitigating systems in response to the accidents. Section 4.2 of Appendix A describes in more detail these operator response errors.

Initial screening guidelines suggested that human error events in the models be assigned a probability value of 0.1. This proved to be too conservative and tended to mask significant hardware contributions to system unavailability. Thus, initial screening values were refined on a case-by-case basis using engineering judgement.

For those systems where the reduced human error rates still made a significant contribution to the probability of failure, an explicit human error model was developed based on the procedures found in the Sandia publication, NUREG/CR-1278.⁶ It was especially important to create these models for human error events that affected multiple systems. For example, miscalibration of reactor vessel level switches could result in failure of the core standby cooling systems to be auto-initiated when required. These human error models can be found in Section 4 of Appendix B.

3.3 Recovery Factors

For the candidate dominant accident sequences, the potential for recovery was considered in the final sequence frequency. To determine recoverability, the dominant contributors to the sequence frequency were examined to determine answers to several questions:

1. Are the failure modes of the dominant contributors ones that allow for recovery? For example, an initiation fault may be recoverable by having the operator manually starting a system/component, whereas a mechanical failure of a valve may not be recoverable.
2. How much time is available to take the recovery action?
3. What must be done to repair the fault, and where must the action be taken? The only faults considered recoverable when the time available was less than 2 hours were those where simple action by the operator, such as throwing a switch or pushing a button in the control room, would correct the fault. Local faults recoverable from outside the control room where the recovery time available was more than 2 hours were also considered.

Recoverable faults were requantified by multiplying the fault unavailability by the probability of nonrecovery factor. Table C-6 summarizes these factors.

TABLE C-6. NONRECOVERY FACTORS

<u>Time Available to Recover</u>	<u>Probability of Nonrecovery Factor</u>
Less than 5 min	1.00
5 to 10 min	0.25
10 to 20 min	0.10
20 to 30 min	0.05
30 to 60 min	0.03
More than 60 min	0.01
More than 2 hr (outside control room)	0.01

4. CANDIDATE DOMINANT SEQUENCES

4.1 Introduction

Figures C-3 through C-13 are the systemic event trees. As an initial screening tool, only sequences with frequencies greater than 1.0×10^{-8} were considered significant. From the systemic event trees listed above, Table C-7 lists by initiating event those sequence frequencies greater than 10^{-8} . Table C-8 lists these systemic event tree sequence frequencies in decreasing order of magnitude. Of these sequences, those with frequencies greater than 1.0×10^{-6} were chosen as the candidate dominant sequences. Table C-9 lists these sequences along with the sequence initiator, the systemic event tree sequence designator, the initial sequence frequency, and the final sequence frequency after recovery has been considered.

In the following section, the quantification for each candidate dominant sequence is discussed. Each candidate sequence is identified by a letter designator representing the initiator (see Table C-10) and a group of letters corresponding to the systems that fail for the sequence. The sequences are also described by a written description that includes the initiator and the system(s) that must fail to cause the sequence to occur. Each candidate sequence is discussed in terms of what happens, what its initial frequency is, what the dominant contributors are, and what, if any, recovery actions are possible. Where availability of data permits, the sequence frequencies were refined to take into account recovery actions.

For clarification, three tables are provided to assist the reader in understanding how the values for the sequence frequencies were determined. Table C-11 lists the various front-line systems and their corresponding designators and unavailabilities for various accident conditions. Appendix B gives the dominant cut sets for each system.

Table C-12 lists the unavailabilities for important combinations of systems. The table lists the independent, commonality, and net unavailabilities for these combinations. Appendix B contains the dominant cut sets for each system but does not show implicitly the source of commonalities between systems. Table C-13 lists the system combinations of Table C-12 that have significant commonalities and briefly describes the major contributions to each.

4.2 Sequence Evaluation

There are 11 candidate dominant accident sequences. Six of these sequences involve failure of the DHR function to remove decay heat, three involve failure to inject water, and two involve failure to scram. All of the candidate dominant sequences involve transient initiators.

4.2.1 Loss of Offsite Power with DHR Failure (TpR_BRA)

For this sequence, the LOSP transient results in a reactor scram and the reactor vessel is isolated from the steam system by the main steam isolation valves (MSIVs). The primary relief valves lift to relieve reactor vessel pressure and reclose when pressure falls below the valve setpoint.

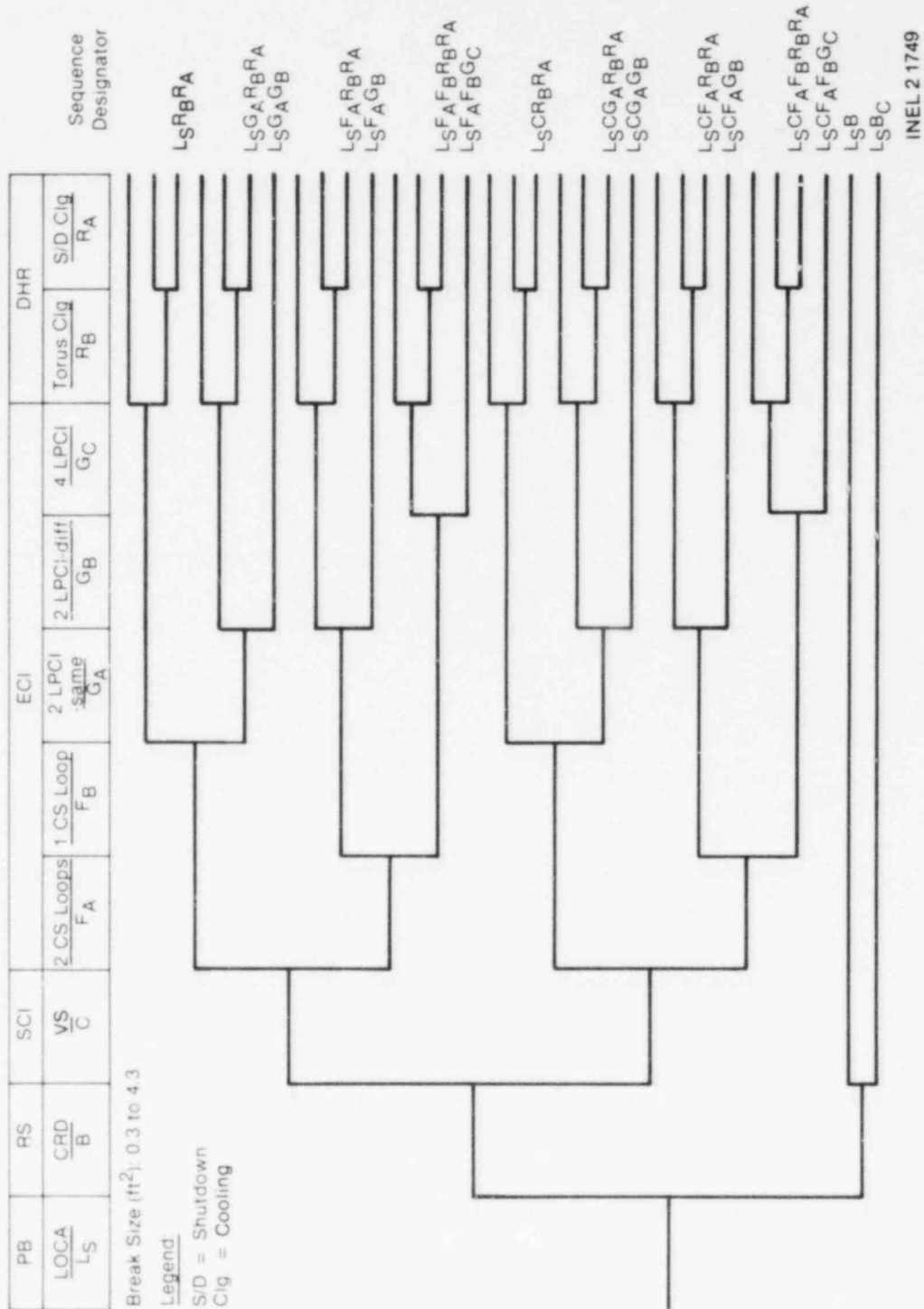
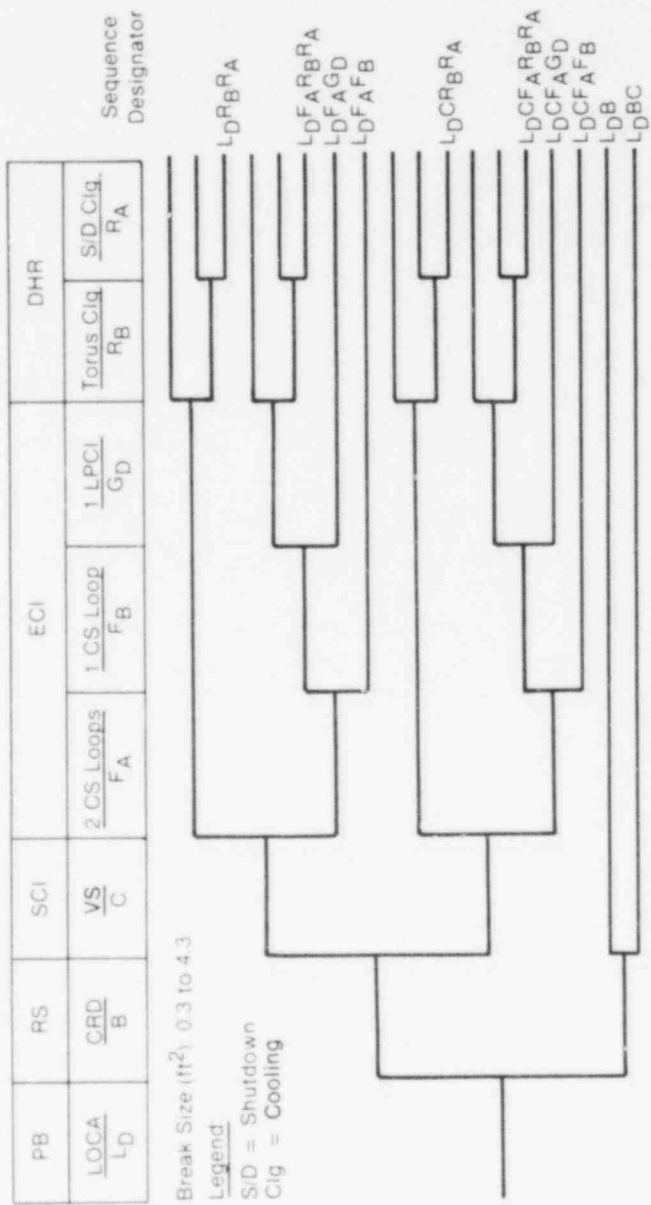


Figure C-3. LOCA systemic event tree for large liquid break, suction-side of recirculation pumps (LS).

INEL 2 1749



INEL 2 1750

Figure C-4. LOCA systemic event tree for large liquid break, discharge-side of recirculation pumps (LD).

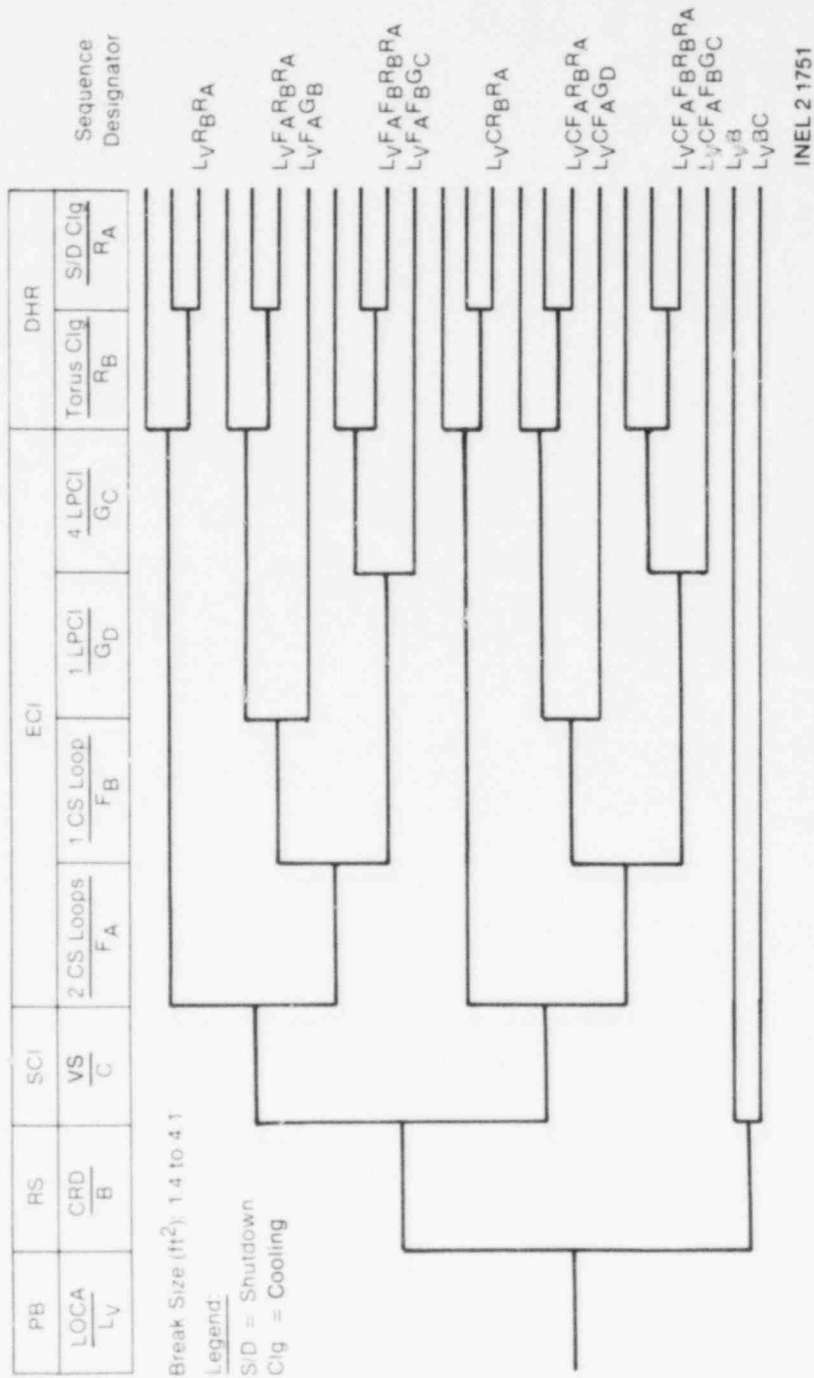


Figure C-5. LOCA systemic event tree for large steam break (Lv).

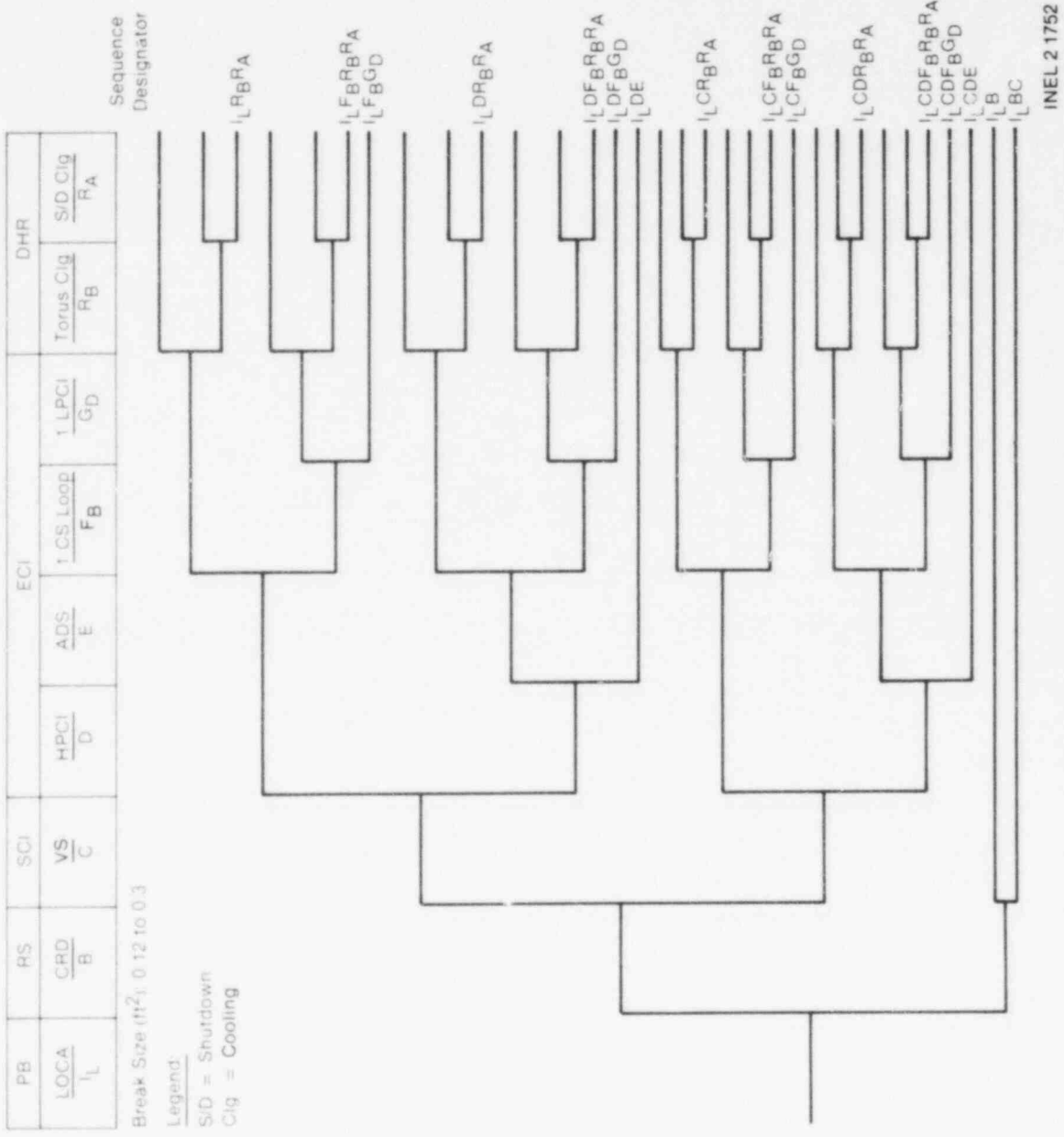
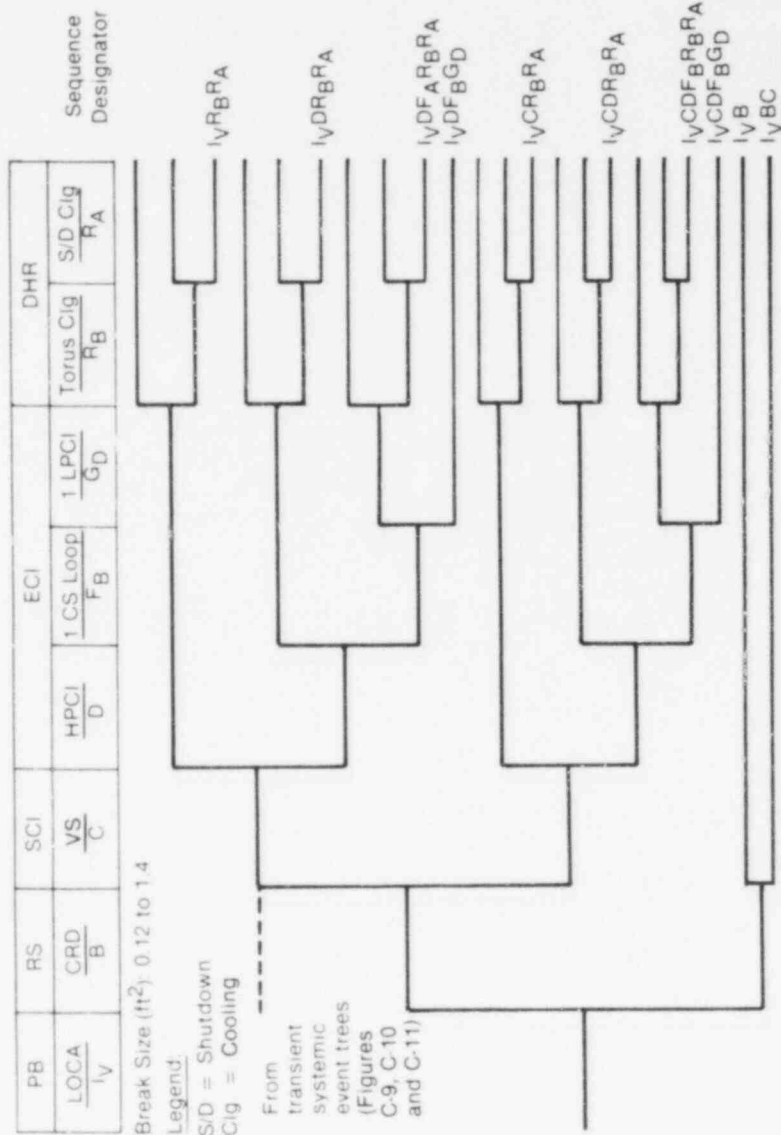
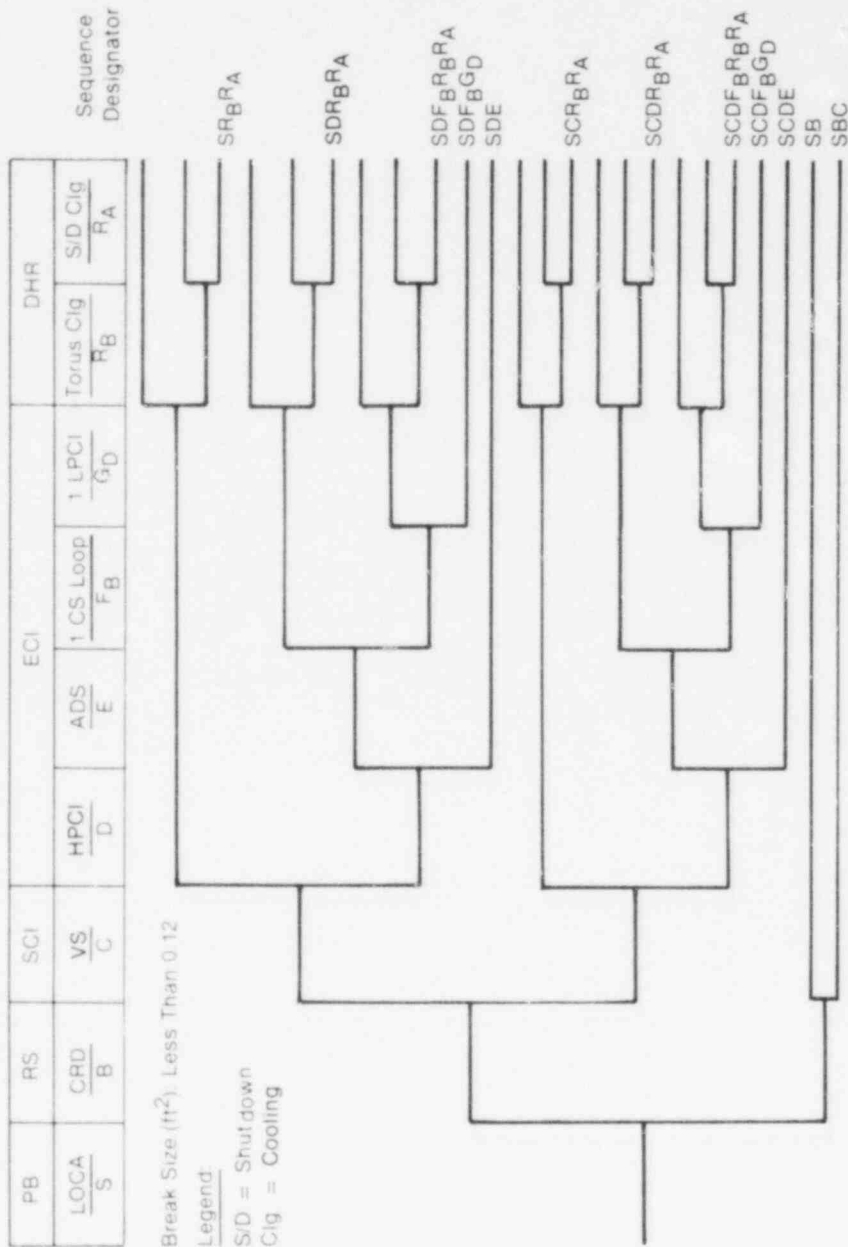


Figure C-6. LOCA systemic event tree for intermediate liquid break (I_L).



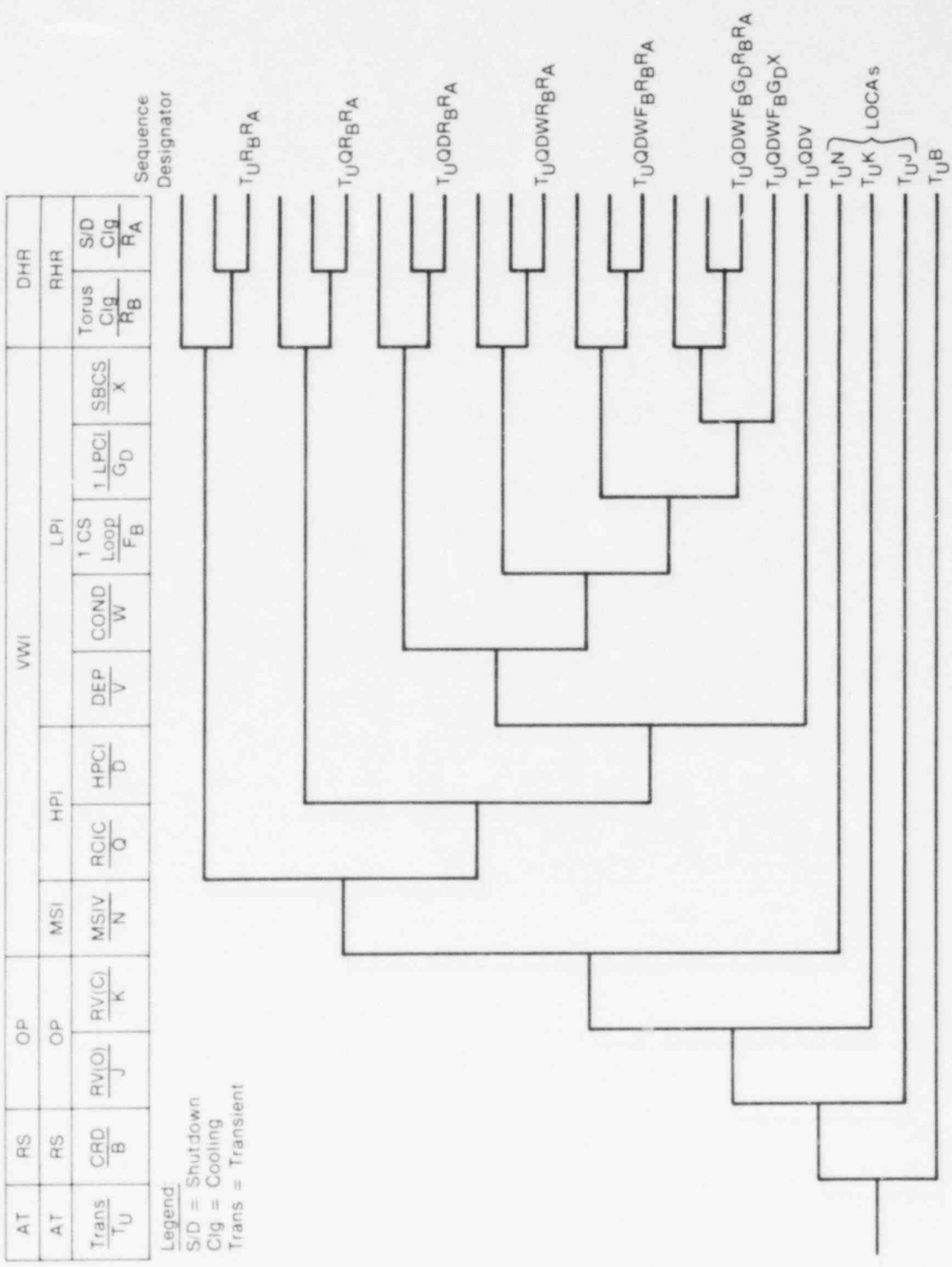
INEL 21753

Figure C-7. LOCA systemic event tree for intermediate steam break (I_V).



INEL 2 1754

Figure C-8. LOCA systemic event tree for small liquid or steam break (S).

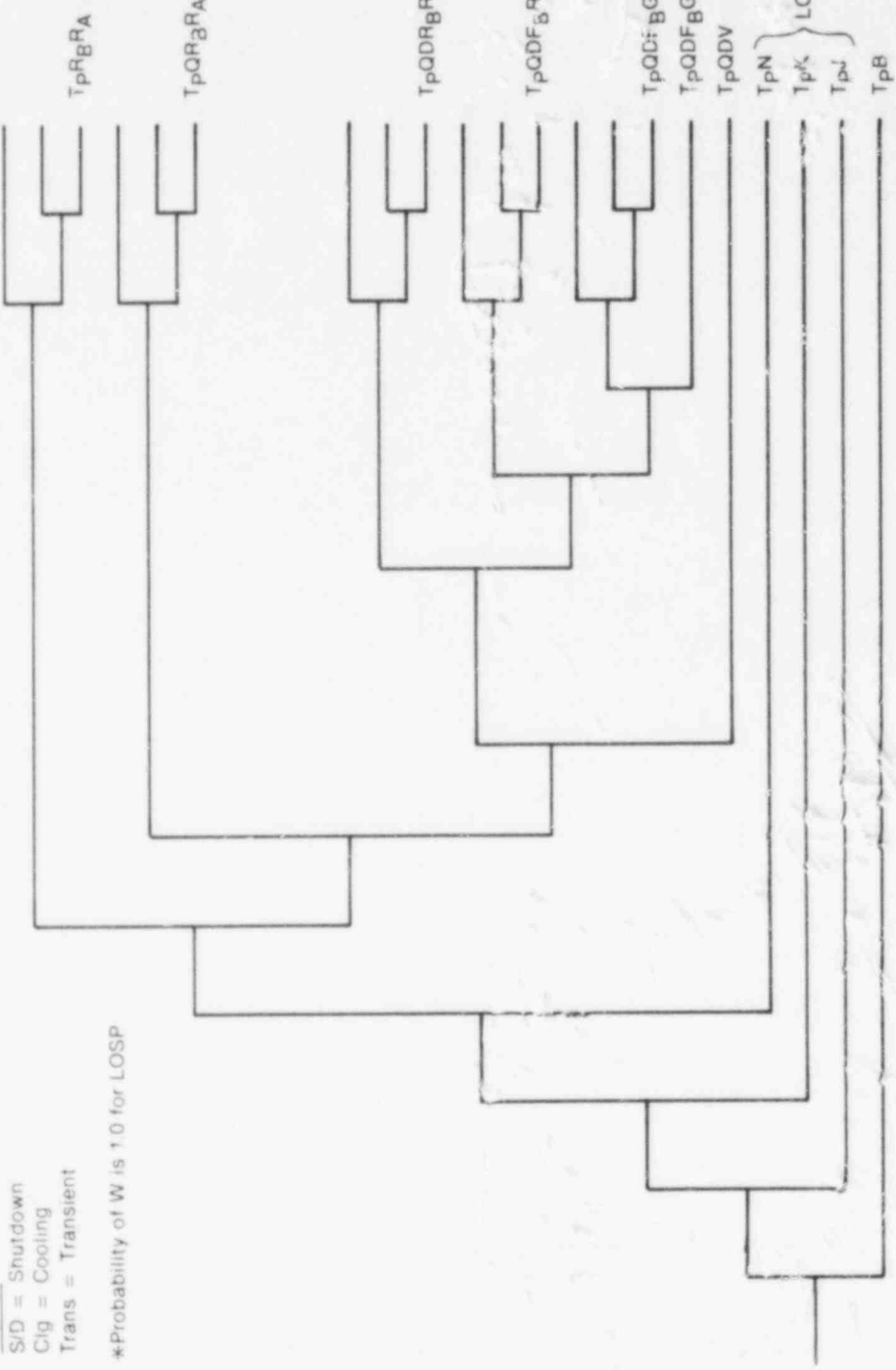


INEL 2 1755

Figure C-9. Transient systemic event tree where PCS is unavailable (T_U).

AT		RS		OP		VWI						DHR	
AT	RS	RS	OP	OP	MSI	HPI	LPI		SBCS		RHR	DHR	
Trans	CRD	RV(O)	RV(C)	MSIV	RCIC	HPCI	COND	1 CS	1 LPCI	Torus	S/D		
TP	B	J	K	N	Q	D	W*	Loop	GD	Cig	Cig	RA	
								FB	X	RB	RA		

Sequence Designator

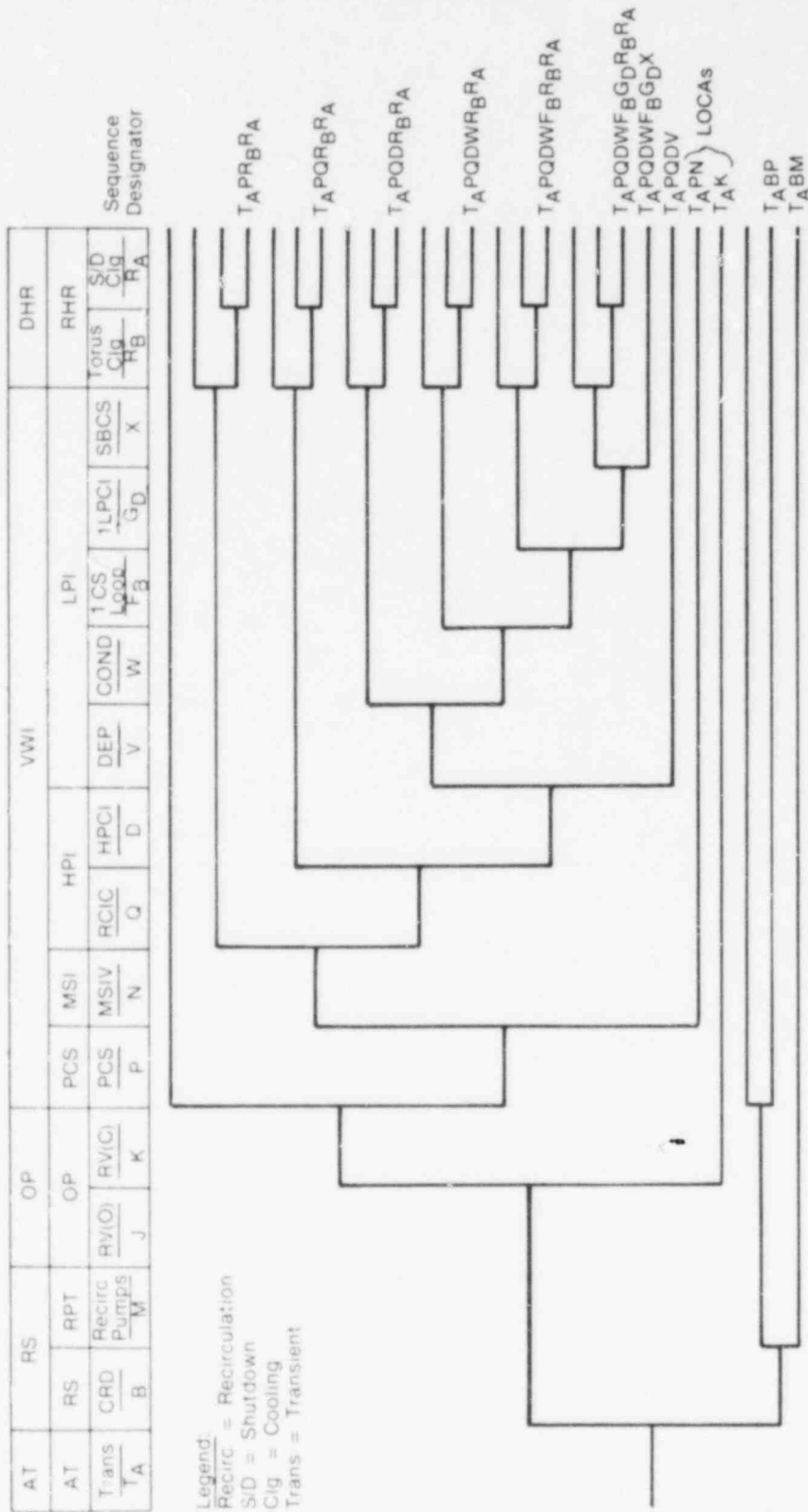


Legend:
 S/D = Shutdown
 Cig = Cooling
 Trans = Transient

*Probability of W is 1.0 for LOSP

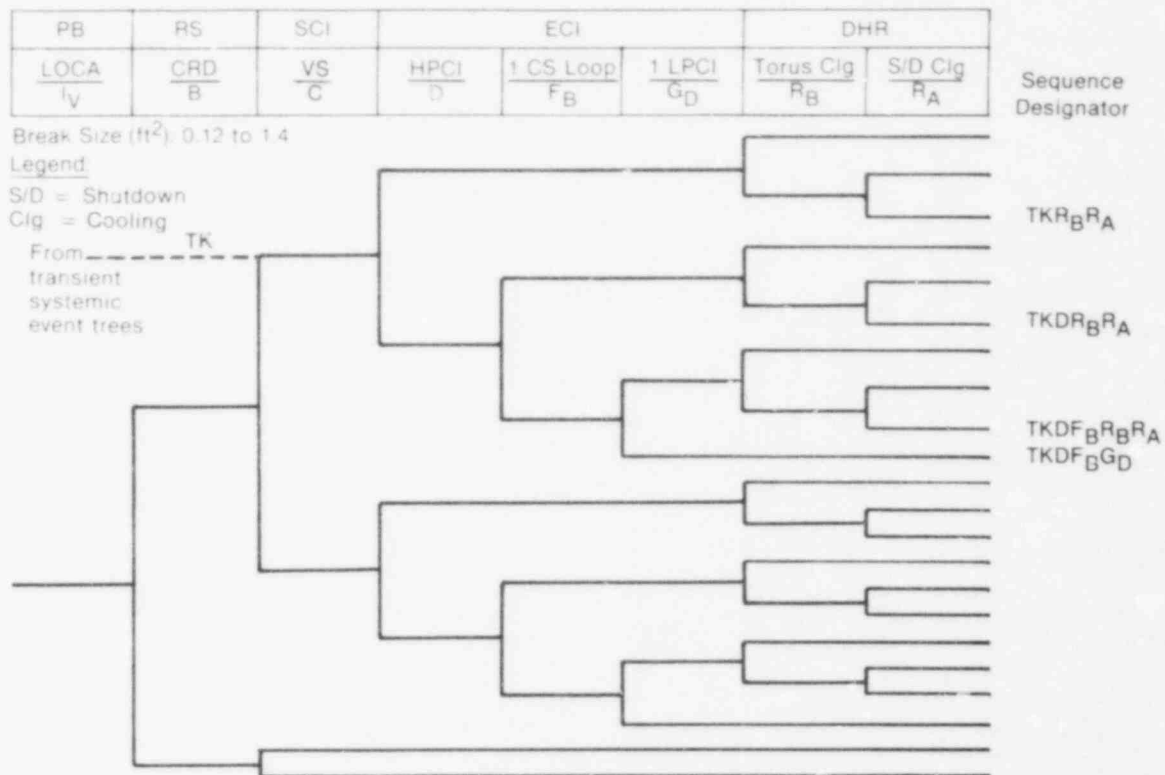
INEL 2 1647

Figure C-10. LOSP-induced transient systemic event time (PCS unavailable) (Tp).



INEL 2 1756

Figure C-11. Transient systemic event tree where PCS is available (TA).



INEL 2 1757

Figure C-12. Transient-induced SORV LOCA systemic event tree (intermediate steam break) (TK).

PB	RS	SCI	ECI		DHR		Sequence Designator
LOCA IV	CRD B	VS C	HPCI D	1 CS Loop FB	1 LPCI GD	Torus Clg RB	S/D Clg RA

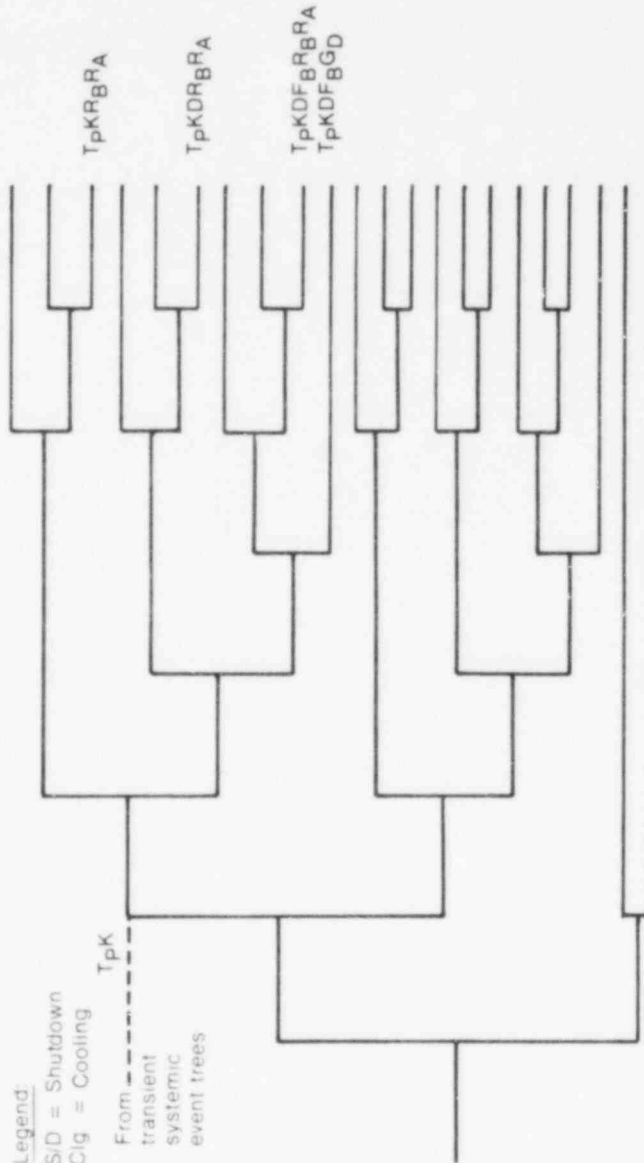
Break Size (ft²): 0.12 to 1.4

Legend:

S/D = Shutdown

Clg = Cooling

From --- TpK
transient
systemic
event trees



INEL 2 1758

Figure C-13. LOSP-induced SORV LOCA systemic event tree (intermediate steam break) (TpK).

TABLE C-7. SEQUENCE FREQUENCIES GREATER THAN 10^{-8} BY INITIATOR

<u>Sequence Designator</u>	<u>Sequence Frequency</u>	<u>Sequence Designator</u>	<u>Sequence Frequency</u>
LSR _B RA	1.7×10^{-8}	TUR _B RA	1.3×10^{-4}
LSF _A G _B	1.1×10^{-8}	TUQR _B RA	5.5×10^{-6}
LD _R BRA	6.3×10^{-8}	TUQDR _B RA	2.4×10^{-7}
LDFA _G D	2.0×10^{-8}	TUQDWF _B G _D X	4.1×10^{-8}
LDFA _F B	2.6×10^{-8}	TUQDV	9.2×10^{-6}
IL _R BRA	1.4×10^{-7}	TUB	5.1×10^{-5}
IV _R BRA	1.6×10^{-8}	TpR _B RA	1.5×10^{-3}
IVCR _B RA	1.3×10^{-8}	TpQR _B RA	6.2×10^{-5}
IVCDR _B RA	1.3×10^{-8}	TpQDR _B RA	1.7×10^{-8}
IVCDF _B R _B RA	1.3×10^{-8}	TpQDF _B G _D X	1.2×10^{-6}
IVCDF _B G _D	1.3×10^{-8}	TpQDV	1.7×10^{-7}
SR _B RA	5.3×10^{-7}	TpB	9.0×10^{-7}
SDR _B RA	1.2×10^{-7}	TAPR _B RA	8.9×10^{-7}
SCR _B RA	6.0×10^{-8}	TAPQR _B RA	3.7×10^{-8}
SCDR _B RA	6.0×10^{-8}	TAPQDWF _B G _D X	2.8×10^{-8}
SCDF _B R _B RA	6.0×10^{-8}	TAPQDV	6.3×10^{-8}
SCDF _B G _D	6.0×10^{-8}	TABP	3.5×10^{-7}
SCDE	6.0×10^{-8}	TABM	3.7×10^{-6}
SB	3.0×10^{-8}	TKR _B RA	1.2×10^{-5}
		TKDR _B RA	7.8×10^{-7}
		TKDF _B G _D	3.9×10^{-7}
		TpKR _B RA	8.3×10^{-5}
		TpKDR _B RA	3.3×10^{-8}
		TpKDF _B G _D	2.5×10^{-6}

TABLE C-8. SYSTEMIC SEQUENCE FREQUENCIES IN DECREASING ORDER OF MAGNITUDE

<u>Sequence Designator</u>	<u>Sequence Frequency</u>	<u>Sequence Designator</u>	<u>Sequence Frequency</u>
TpR _B R _A	1.5 x 10 ⁻³	L _D R _B R _A	6.3 x 10 ⁻⁸
T _U R _B R _A	1.3 x 10 ⁻⁴	SCR _B R _A	6.0 x 10 ⁻⁸
TpKR _B R _A	8.3 x 10 ⁻⁵	SCDR _B R _A	6.0 x 10 ⁻⁸
TpQR _B R _A	6.2 x 10 ⁻⁵	SCDF _B R _B R _A	6.0 x 10 ⁻⁸
T _U B	5.1 x 10 ⁻⁵	SCDF _B G _D	6.0 x 10 ⁻⁸
TKR _B R _A	1.2 x 10 ⁻⁵	SCDE	6.0 x 10 ⁻⁸
T _U QDV	9.2 x 10 ⁻⁶	T _U QDWF _B G _D X	4.1 x 10 ⁻⁸
T _U QR _B R _A	5.5 x 10 ⁻⁶	T _A PQR _B R _A	3.7 x 10 ⁻⁸
T _A BM	3.7 x 10 ⁻⁶	T _P KDR _B R _A	3.3 x 10 ⁻⁸
T _P KDF _B G _D	2.5 x 10 ⁻⁶	SB	3.0 x 10 ⁻⁸
T _P QDF _B G _D X	1.2 x 10 ⁻⁶	T _A PQDWF _B G _D X	2.8 x 10 ⁻⁸
T _P B	9.0 x 10 ⁻⁷	L _D F _A F _B	2.6 x 10 ⁻⁸
T _A PR _B R _A	8.9 x 10 ⁻⁷	L _D F _A G _D	2.0 x 10 ⁻⁸
TKDR _B R _A	7.8 x 10 ⁻⁷	T _P QDR _B R _A	1.7 x 10 ⁻⁸
SR _B R _A	5.3 x 10 ⁻⁷	L _S R _B R _A	1.7 x 10 ⁻⁸
TKDF _B G _D	3.9 x 10 ⁻⁷	I _V R _B R _A	1.6 x 10 ⁻⁸
T _A BP	3.5 x 10 ⁻⁷	I _V CR _B R _A	1.3 x 10 ⁻⁸
T _U QDR _B R _A	2.4 x 10 ⁻⁷	I _V CDR _B R _A	1.3 x 10 ⁻⁸
T _P QDV	1.7 x 10 ⁻⁷	I _V CDF _B R _B R _A	1.3 x 10 ⁻⁸
I _L R _B R _A	1.4 x 10 ⁻⁷	I _V CDF _B G _D	1.3 x 10 ⁻⁸
SDR _B R _A	1.2 x 10 ⁻⁷	L _S F _A G _B	1.1 x 10 ⁻⁸
T _A PQDV	6.3 x 10 ⁻⁸		

TABLE C-9. CANDIDATE DOMINANT SEQUENCES

Sequence Initiator	Sequence Designator	Sequence Frequency	
		Initial	Final
Transient-induced LOCAs	TKR _B RA	1.2×10^{-5}	9.3×10^{-6}
LOSP-induced LOCAs	TpKR _B RA	8.3×10^{-5}	1.6×10^{-6}
	TpKDF _B GD	2.5×10^{-6}	8.7×10^{-8}
PCS unavailable	TUR _B RA	1.3×10^{-4}	9.7×10^{-5}
	TUQR _B RA	5.5×10^{-6}	4.1×10^{-6}
	TUB	5.1×10^{-5}	5.1×10^{-5}
	TUQDV	9.2×10^{-6}	5.5×10^{-7}
PCS available	T _A BM	3.7×10^{-6}	3.7×10^{-6}
LOSP	TpR _B RA	1.5×10^{-3}	2.8×10^{-5}
	TpQR _B RA	6.2×10^{-5}	1.2×10^{-6}
	TpQDF _B GD _X	1.2×10^{-6}	3.6×10^{-8}

TABLE C-10. INITIATOR DESIGNATORS

Designator	Initiator	Frequency (per reactor-year)
L _S	Large suction break	9.9×10^{-6}
L _D	Large discharge break	3.9×10^{-5}
L _V	Large steam break	5.2×10^{-5}
I _L	Intermediate liquid break	9.0×10^{-5}
I _V	Intermediate steam break	2.1×10^{-4}
S	Small liquid or steam break	1.0×10^{-3}
T _U	Transients where PCS is unavailable	1.70
T _P	Loss of offsite power transient	3.0×10^{-2}
T _A	Transients where PCS is available	1.68
TK	Transient induced SORV	$1.63 \times 10^{-1*}$
T _P K	Loss of offsite power-induced SORV	$1.7 \times 10^{-3*}$

* Two additional initiators are defined in this table. In each case they represent transient-induced SORVs. The designator TK is used to represent the combined frequency for a SORV from both the PCS available and PCS unavailable transient event trees. The designator K represents a system that is described for both of these cases in Table C-11. T_PK represents the frequency for a SORV from the PCS unavailable transient event tree for only the special case where LOSP was the initiator. Each of these initiators transfer to the intermediate steam break LOCA systemic event tree at the ECI systems branch point. The LOSP transient-induced SORV was treated independently from the PCS unavailable category due to the important dependencies of the mitigating systems on emergency onsite AC power.

TABLE C-11. FRONT-LINE SYSTEMS UNAVAILABILITIES

Designator	System	Special Conditions	Unavailability
B	Control rod drive	--	3.0×10^{-5}
C	Vapor suppression	--	3.7×10^{-4}
D	HPCI	LOCA initiator Transient initiator	6.5×10^{-2} 4.4×10^{-2}
E	ADS	--	3.2×10^{-4}
FA	Core spray (two core spray loops)	Normal power	5.2×10^{-2}

TABLE C-11. (continued)

Designator	System	Special Conditions	Unavailability
F _B	Core spray (one core spray loop)	Normal power	6.6×10^{-4}
		LOSP	9.6×10^{-4}
		Steam break on core spray pipe	2.6×10^{-2}
G _A	RHR (LPCI mode) (two LPCI pumps in same loop)	--	6.6×10^{-4}
G _B	RHR (LPCI mode) (two LPCI pumps, one in each loop)	--	2.1×10^{-2}
G _C	RHR (LPCI mode) (four LPCI pumps)	--	5.0×10^{-2}
G _D	RHR (LPCI mode) (one LPCI pump)	Normal power	1.1×10^{-4}
		LOSP	2.7×10^{-4}
		Break on recirculation discharge	1.0×10^{-2}
J	Relief valves (opening)	--	7.2×10^{-9}
K	Relief valves (closing)	Transients without PCS	5.7×10^{-2}
		Transients with PCS	3.9×10^{-2}
M	Recirculation pumps	--	8.7×10^{-3}
N	Main steam isolation valve	--	4.4×10^{-7}
P	Power conversion system	--	7.0×10^{-3}
Q	RCIC	--	4.2×10^{-2}
R _A	RHR (shutdown cooling)	Normal power	2.0×10^{-2}
		LOSP	4.2×10^{-2}
		Break on recirculation discharge	3.1×10^{-2}
R _B	RHR (torus cooling)	Normal power	3.1×10^{-3}
		LOSP	7.2×10^{-3}
V	Manual depressurization	--	3.0×10^{-3}
W	Condensate pumps	--	7×10^{-3}
X	RHR (SBCS mode)	Normal power	4.2×10^{-2}
		LOSP	4.6×10^{-2}

TABLE C-12. SYSTEM COMBINATIONS OF IMPORTANCE

System Combination	Special Conditions	Unavailability		
		Independent	Common	Net
$R_A \cap R_B$	Normal power	6.2×10^{-5}	1.4×10^{-5}	7.6×10^{-5}
	LOSP	3.0×10^{-4}	4.9×10^{-2}	4.9×10^{-2}
	Break on recirculation discharge	1.6×10^{-3}	ϵ	1.6×10^{-3}
$G_A \cap G_B$	--	1.4×10^{-5}	4.2×10^{-4}	4.3×10^{-4}
$F_A \cap G_B$	--	1.1×10^{-3}	4.6×10^{-6}	1.1×10^{-3}
$F_B \cap G_C$	--	3.3×10^{-5}	2.5×10^{-6}	3.6×10^{-5}
$F_A \cap G_D$	Break on recirculation discharge	5.2×10^{-4}	2.4×10^{-6}	5.2×10^{-4}
	No break	5.7×10^{-6}	1.9×10^{-8}	5.7×10^{-6}
$D \cap E$	--	2.3×10^{-6}	ϵ	2.3×10^{-6}
$F_B \cap G_D$	Break on recirculation discharge	6.6×10^{-6}	2.3×10^{-6}	8.9×10^{-6}
	No break	7.3×10^{-8}	3.4×10^{-8}	1.1×10^{-7}
	LOSP	1.5×10^{-3}	2.1×10^{-2}	2.2×10^{-2}
$D \cap F_B \cap G_D$	No break	7.2×10^{-9}	2.4×10^{-6}	2.4×10^{-6}
	Break on recirculation discharge	5.8×10^{-7}	ϵ	5.8×10^{-7}
	Break on core spray pipe	1.9×10^{-7}	ϵ	1.9×10^{-7}
	LOSP	1.5×10^{-3}	ϵ	1.5×10^{-3}
$Q \cap D$	Transients	1.8×10^{-3}	2.4×10^{-6}	1.8×10^{-3}
$Q \cap D \cap F_B \cap G_D$	Transients	2.0×10^{-10}	2.4×10^{-6}	2.4×10^{-6}
$Q \cap D \cap V$	Transients	5.4×10^{-6}	ϵ	5.4×10^{-6}
$Q \cap D \cap F_B \cap G_D \cap W$	Transients	1.7×10^{-8}	ϵ	1.7×10^{-8}
$P \cap W$	Transients	4.9×10^{-6}	7.0×10^{-3}	7.0×10^{-3}
$P \cap Q \cap D \cap V$	Transients	3.8×10^{-8}	ϵ	3.8×10^{-8}
$P \cap Q \cap D \cap F_B \cap G_D$	Transients	1.7×10^{-8}	ϵ	1.7×10^{-8}

TABLE C-12. (continued)

System Combination	Special Conditions	Unavailability		
		Independent	Common	Net
$\cap W \cap X$				
$F_B \cap G_D \cap X$	LOSP	1.5×10^{-3}	2.1×10^{-2}	2.2×10^{-2}
$Q \cap D \cap F_B \cap G_D \cap X$	LOSP	3.8×10^{-5}	2.4×10^{-6}	4.0×10^{-5}
$B \cap M$	Transients	2.6×10^{-7}	1.9×10^{-6}	2.2×10^{-6}

TABLE C-13. COMMONALITIES OF IMPORTANCE

System Combination	Special Conditions	Commonalities Unavailable	Remarks
$R_A \cap R_B$	Normal power	1.4×10^{-5}	Minimum-flow bypass valves
	LOSP	4.9×10^{-2}	Diesel generator and EECW faults
$G_A \cap G_B$	--	4.2×10^{-4}	Minimum-flow bypass valves and loop discharge valves
$F_A \cap G_B$	--	4.6×10^{-6}	Electric power faults
$F_B \cap G_C$	--	2.5×10^{-6}	Electric power faults
$F_A \cap G_D$	Break on recirculation discharge	2.4×10^{-6}	Electric power faults
	No break	1.9×10^{-8}	Electric power faults
$F_B \cap G_D$	Break on recirculation discharge	2.3×10^{-6}	Electric power faults
	No break	3.4×10^{-8}	Electric power faults

TABLE C-13. (continued)

<u>System Combination</u>	<u>Special Conditions</u>	<u>Commonalities Unavailable</u>	<u>Remarks</u>
	LOSP	2.1×10^{-2}	Primarily EECW faults
$D \cap F_B \cap G_D$	Transients	2.4×10^{-6}	Maintenance error to level switches
$Q \cap D$	Transients		
$Q \cap D \cap F_B \cap G_D$	Transients		
$Q \cap D \cap F_B \cap G_D \cap X$	LOSP		
$P \cap W$	Transients	7×10^{-3}	Assumed that PCS failure causes condensate pump failure
$F_B \cap G_D \cap X$	LOSP	2.1×10^{-2}	Primarily EECW faults
$B \cap M$	Transients	1.9×10^{-6}	Reactor protection system common mode failures

The operator maintains normal reactor vessel water level using RCIC, a system that will automatically initiate on low reactor vessel level. Following successful coolant injection, the torus cooling (R_B) and shutdown cooling (R_A) systems fail. A sustained loss of these systems will result in the inability to provide makeup water to the reactor to replace the inventory lost due to boil off caused by decay heat. A core melt will eventually occur. The initial value for this sequence is 1.5×10^{-3} per reactor-year based on an initiating frequency of 3×10^{-2} per reactor-year and an unavailability of 4.9×10^{-2} for the combination of R_B and R_A . Figure C-14 is the systemic event tree for the LOSP transient.

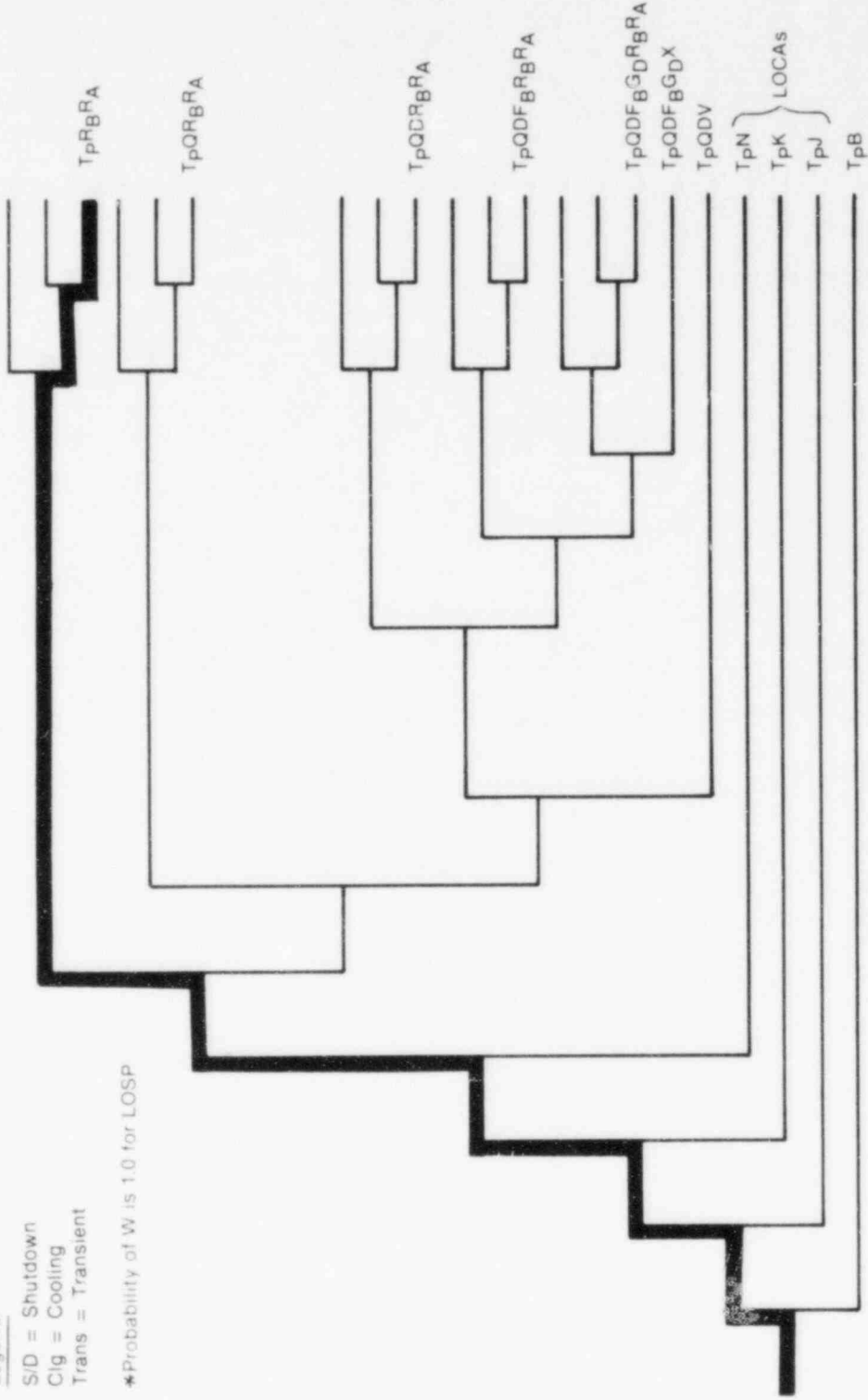
The RHR system in either shutdown cooling or torus cooling mode removes the reactor decay heat. The 4.9×10^{-2} unavailability for R_B and R_A is comprised of 2.9×10^{-2} due to failures of R_B and R_A independent of EECW faults and 2.0×10^{-2} due to EECW faults. The 2.9×10^{-2} unavailability is dominated by combinations of electric power system unavailabilities due primarily to diesel generator faults. The remaining 2.0×10^{-2} contribution to DHR failure comes from the unavailability of the EECW system to provide its required cooling given a LOSP. If the EECW fails, all diesel generators will eventually fail and the RHR system will be unavailable. The major contributor to the EECW unavailability is combinations of two or more diesel generators failing to start. These diesels are not necessarily the same as those that fail R_B and R_A directly. Section 1.5 details the procedure for handling this type of potential logic

AT		RS		OP		MSI				HPI				VWI				DHR											
AT		RS		OP		RV(O)		RV(C)		MSIV		RCIC		HPCI		DEP		COND		1 CS Loop		1 LPCI		SBCS		Torus		S/D	
Trans		CRD		RV(O)		RV(C)		MSIV		RCIC		HPCI		DEP		COND		1 CS Loop		1 LPCI		SBCS		Torus		S/D			
Tp		B		J		K		N		Q		D		V		W*		FB		GD		X		RB		Clg		RA	

Legend

- S/D = Shutdown
- Clg = Cooling
- Trans = Transient

*Probability of W is 1.0 for LOSP



INEL 2 1759

Figure C-14. Systemic event tree showing the TpRBRA sequence.

loop. Essentially, the R_B and R_A unavailability is split into two portions, with the unavailability assuming EECW works added to the unavailability of EECW. Each of the candidate dominant sequences involving loss of offsite power is treated similarly. Figure C-15 is a sequence evaluation diagram showing the dominant contributors to the unavailability of R_B and R_A .

Should this sequence occur, the RCIC system providing the VWI function can continue to do so for approximately 6 to 8 hours without RHR operation. This estimate is based on the time it takes to deplete the condensate storage tank and to heat the torus water to a temperature that prevents the RCIC system from pumping the water, assuming no containment backpressure.⁷ With containment backpressure considered, operation of RCIC can continue for approximately 24 hours before containment failure occurs, followed by an inability to pump the torus water back to the core.

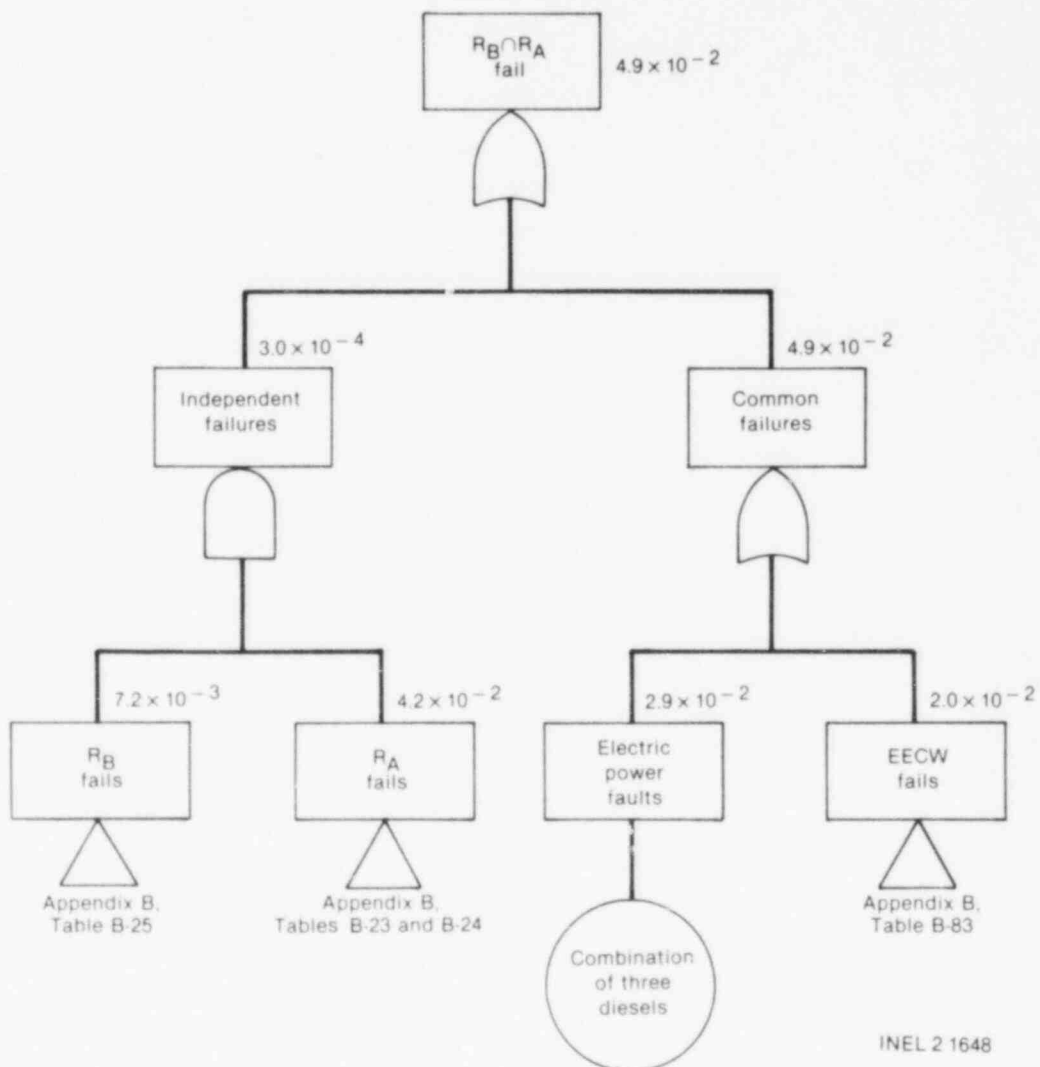


Figure C-15. Dominant contributors to the unavailability of torus cooling and shutdown cooling given LOSP.

There are several viable recovery considerations available to the operators during this time period. One is a restoration of offsite power. If offsite power is restored within the 6 to 8 hour period, the unavailability of the DHR function changes from 2.9×10^{-2} to 7.6×10^{-5} . Another recovery consideration is the restoration of EECW. The success criteria used in this analysis requires three of the four EECW pumps to operate to provide cooling to all of the EECW loads. Two of four pumps will provide up to 91% of rated flow and would provide the operator with some grace period to restore the lost pumps or valve in spare pumps from the RHRSW system. The operator could also isolate flow to nonessential loads supplied by EECW so that the flow of two pumps would provide sufficient cooling. The operator actions to restore EECW fall within the recovery guidelines as discussed previously in Section 3.3. That is, for the time period considered, there is only a 10^{-2} probability that the operator will not take corrective action during this time.

From the WASH-1400 data (Figure III 6-4), approximately 97% of all offsite power outages can be repaired in 6 to 8 hours. Using the WASH-1400 restoration figure plus the recovery factor for providing the EECW with sufficient pumping capability, the probability for R_B and R_A failure is given by:

$$\begin{aligned}
 Q(R_B R_A) &= (0.97)[\text{probability of } R_B R_A \text{ failure with LOSP recovered}] \\
 &\quad + (0.03)[\text{probability of } R_B R_A \text{ failure with LOSP not recovered}] \\
 &= (0.97)(7.6 \times 10^{-5}) + (0.03)[R_B R_A \text{ failure} + \text{EECW failure}] \\
 &= (0.97)(7.6 \times 10^{-5}) + (0.03)[(2.9 \times 10^{-2}) + (2.0 \times 10^{-2})(0.01)] \\
 &= 7.4 \times 10^{-5} + (0.03)(2.9 \times 10^{-2}) \\
 &= 9.4 \times 10^{-4}
 \end{aligned}$$

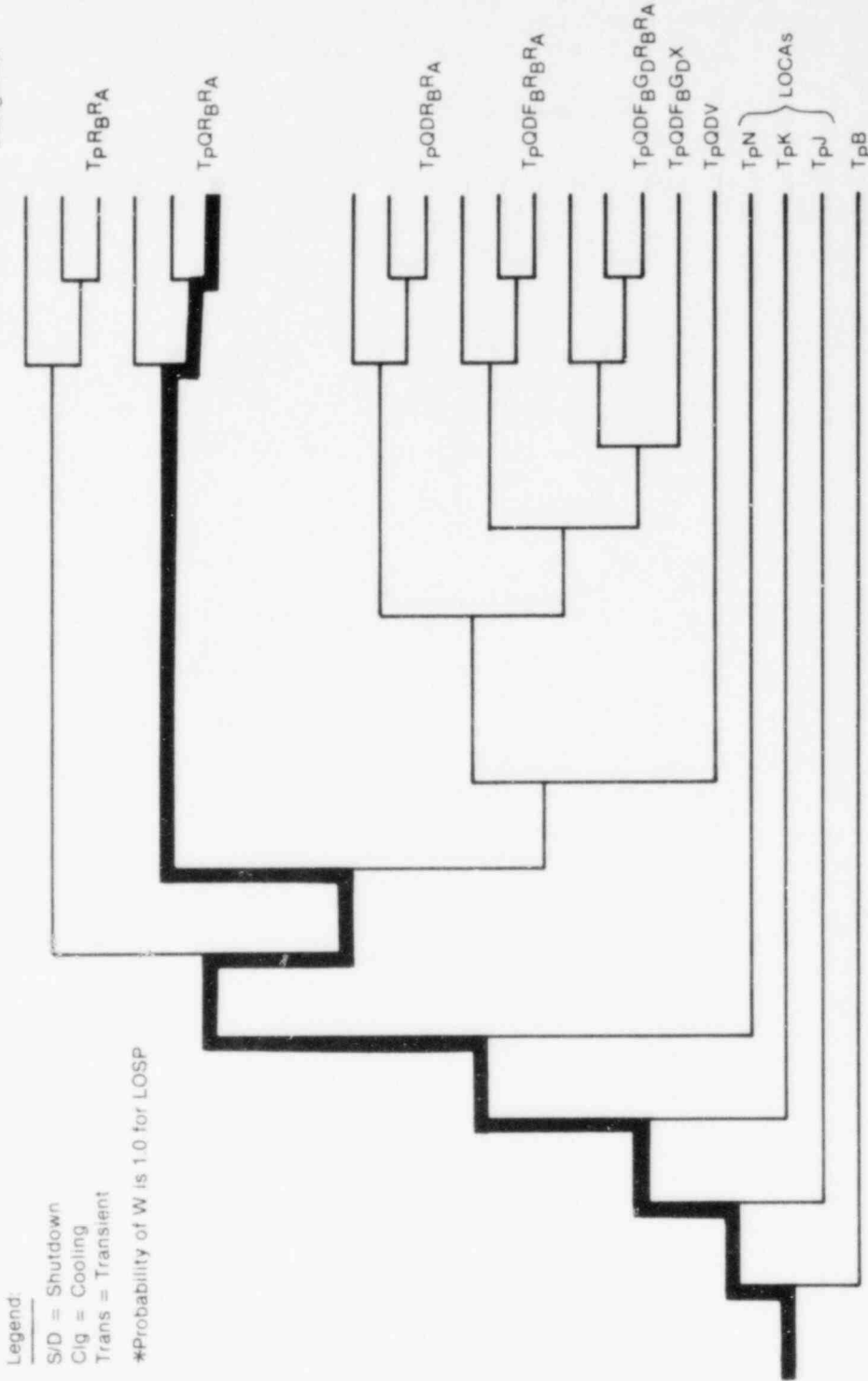
$$\begin{aligned}
 P(T_P R_B R_A) &= F(\text{LOSP}) Q(R_B \cap R_A) \\
 &= (3 \times 10^{-2})(9.4 \times 10^{-4}) \\
 &= 2.8 \times 10^{-5} \text{ per reactor-year.}
 \end{aligned}$$

4.2.2 Loss of Offsite Power with RCIC and DHR Failure ($T_P Q R_B R_A$)

This sequence is essentially identical to sequence $T_P R_B R_A$ except that the RCIC system fails but the HPCI system operates to maintain reactor water level. Subsequently, the torus cooling and shutdown cooling modes of RHR fail to remove decay heat. Sustained failure of these two modes will result in torus water heating to the point that the HPCI system can no longer pump water to the core. A core melt would then occur. This sequence is highlighted on the systematic event tree Figure C-16. Its initial value

AT		RS	OP	VWI						DHR				
AT		RS	OP	MSI		HPI		LPI		RHR				
Trans Tp		CRD B	RV(O) J	RV(C) K	MSIV N	RCIC Q	HPCI D	DEP V	COND W*	1 CS Loop FB	1 LPCI GD	SBCS X	Torus Clg RB	S/D Clg RA

Sequence Designator



INEL 2 1771

Figure C-16. Systemic event tree showing the TpQRBRA sequence.

is 6.2×10^{-5} , based on a 3×10^{-2} per year probability for the LOSP initiator and 2.1×10^{-3} for the unavailability of $Q \cap R_B \cap R_A$. Figure C-17 is a sequence evaluation diagram showing the dominant contributors to the unavailability of $Q \cap R_B \cap R_A$.

The dominant contributors to torus cooling and shutdown cooling failure for this sequence are the same as for sequence $T_P R_B R_A$. Therefore, the recovery factors for these two systems are the same. RCIC is essentially unaffected by the LOSP. Its dominant contributors are rupture disk and control circuit faults, which are not recoverable under the guidelines. Therefore, no credit is taken for recovery of the RCIC system. The unavailability of the mitigating systems becomes 3.9×10^{-5} . The final sequence value then is 1.2×10^{-6} , as shown below.

$$\begin{aligned}
 Q(QR_B R_A) &= Q(Q) Q(R_B R_A \text{ considering recovery}) \\
 &= Q(Q) Q(R_B R_A \text{ from sequence } T_P R_B R_A)
 \end{aligned}$$

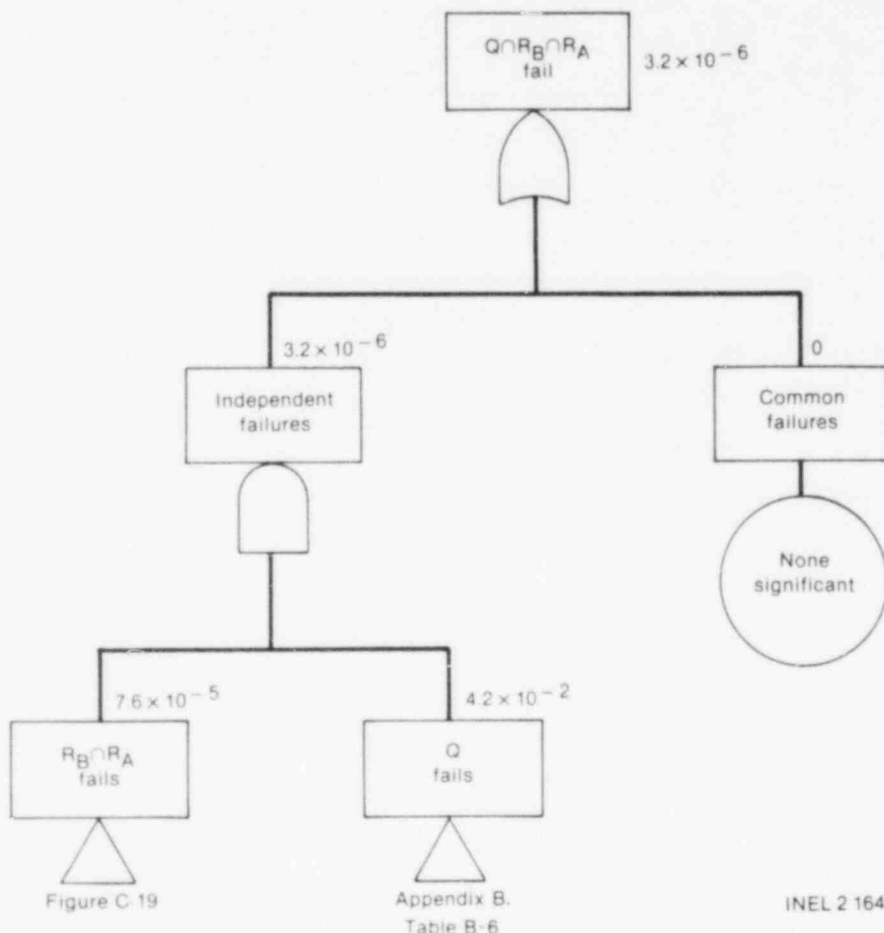


Figure C-17. Dominant contributors to the unavailability of RCIC, torus cooling, and shutdown cooling given LOSP.

$$= (0.042)(9.4 \times 10^{-4})$$

$$= 3.9 \times 10^{-5}$$

$$P(T_P QR_B R_A) = F(LOSP) Q(QR_B R_A)$$

$$= (3 \times 10^{-2})(3.9 \times 10^{-5})$$

$$= 1.2 \times 10^{-6} \text{ per reactor-year.}$$

Q in parenthesis (Q) represents the RCIC system code.)

4.2.3 Transients Where PCS is Unavailable and DHR Fails ($T_U R_B R_A$)

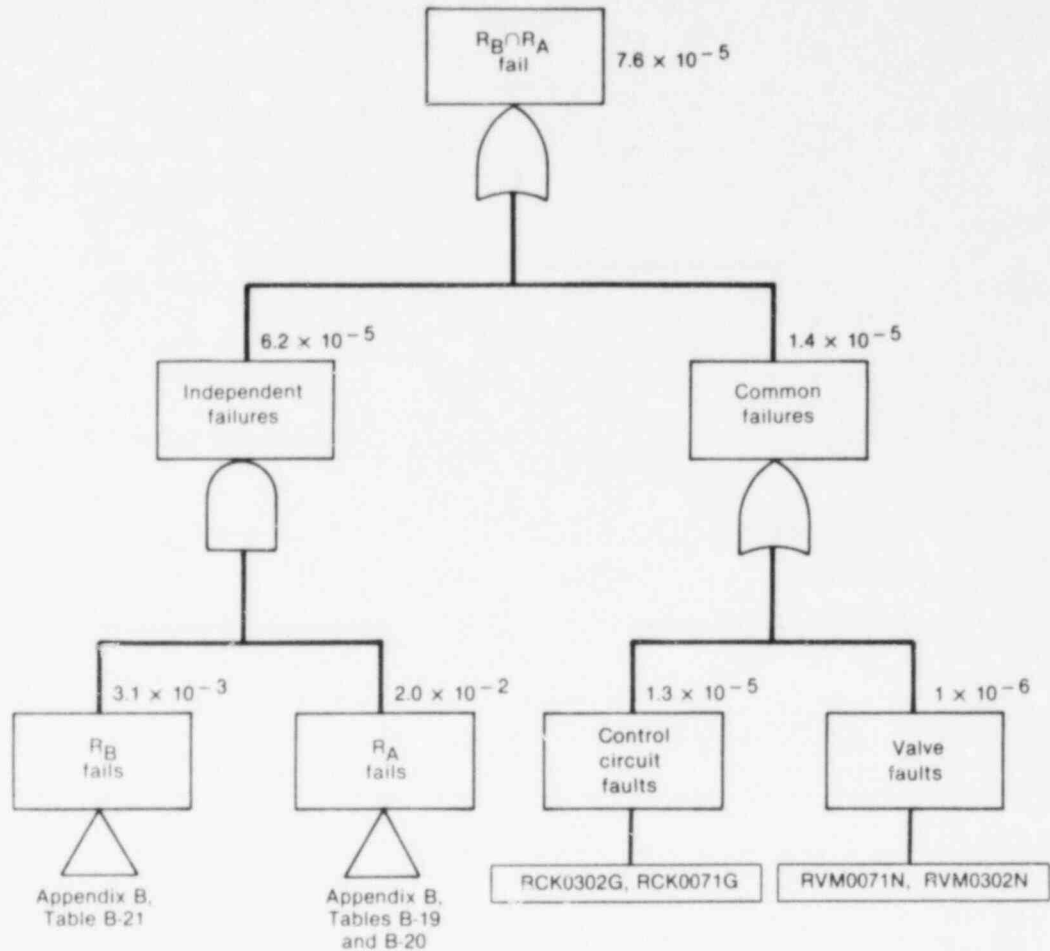
For this sequence, the RS, OP, MSI, and RCIC systems succeed and the long term decay heat removal of torus cooling and shutdown cooling fails. This sequence is similar to the previously-discussed sequence ($T_P R_B R_A$) except that offsite power remains available. The initial screening value for the frequency of this sequence is 1.3×10^{-4} per reactor-year, based on an initiating frequency of 1.70 per reactor-year and an unavailability of 7.6×10^{-5} for the combination of R_B and R_A . The sequence is outlined on the systemic event tree, Figure C-18.

In this sequence, the RHR system in shutdown cooling or torus cooling mode provides the decay heat removal. Both modes must be inoperable to fail the function. The unavailability for both systems is 7.6×10^{-5} . Control circuit faults for the suction and discharge motor-operated valves and the minimum-flow bypass valves dominates this unavailability. It was assumed during the fault tree analyses of the core spray and RHR systems that minimum flow bypass valves failing to close could divert sufficient flow in a given loop to cause failure of that coolant path. Section 6 provides a sensitivity analysis of this assumption. Figure C-19 is a sequence evaluation diagram showing the dominant contributors to the unavailability of $R_B \cap R_A$.

For these transients, even though the PCS was originally lost due to MSIV closure, the potential exists to recover the main condenser as a heat sink. This depends on the cause of the transient. For example, if the transient were initiated by a fault in the feed pumps that was not immediately repairable, then the PCS could not be used. If the transient was due to faulty automatic level control, the operator could manually control level with the feed pumps after reopening the MSIVs. However, there is inadequate data available on which to base a probability of PCS recovery.

Recovery of the RHR system due to the dominant faults (control circuit faults) would involve either manual operation of the affected valves or bypass/repair of the faulted control circuit. In either case, the control room operator would have to recognize the cause of the valve's failure to operate and dispatch personnel to operate/repair the valve. Given that the RCIC system has been successful, the operator would have at least 6 to

AT		RS		OP		VWI					DHR		
Trans		CRD		RV(O)		MSI		HPI		LPI		RHR	
TU		B		J		N		Q		D		V	
				K		O		D		W		X	
						S		V		G		R	
						I		D		D		A	
						V		C		C		C	
						N		O		S		S	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C		C	
						V		D		S		S	
						N		O		C		C	
						S		D		B		B	
						I		V		C			



INEL 2 1761

Figure C-19. Dominant contributors to the unavailability of RHR systems following a transient which disables the PCS (normal power available).

8 hours to accomplish this recovery as discussed previously in Section 4.2.2. The recovery guidelines provide for a probability of non-recovery for these faults of 0.01. The unavailability of R_B and R_A due to both independent and common control circuit faults is 1.9×10^{-5} . The remaining unavailability not subject to recovery is 5.7×10^{-5} . The final sequence value is 9.7×10^{-5} , as shown below.

$$Q(R_B R_A) = (0.01) (\text{recoverable faults}) + (\text{nonrecoverable faults})$$

$$= (0.01)(1.9 \times 10^{-5}) + 5.7 \times 10^{-5}$$

$$= 5.72 \times 10^{-5}$$

$$P(T_U R_B R_A) = F(T_U) Q(R_B R_A) = (1.7)(5.7 \times 10^{-5})$$

$$= 9.7 \times 10^{-5} \text{ per reactor-year.}$$

4.2.4 Transients Where PCS is Unavailable and RCIC and DHR Fail ($T_U QR_B R_A$)

This sequence is essentially identical to sequence $T_U R_B R_A$ except that the RCIC system fails but the HPCI system operates to maintain reactor level. Subsequent failure of torus cooling and shutdown cooling will eventually lead to a core melt. This sequence is shown on the systemic event tree Figure C-20. Its initiator frequency is 1.7 per reactor-year and 5.5×10^{-6} per reactor-year is the screening sequence value. Figure C-21 is a sequence evaluation diagram showing the dominant contributors to the initial value of 3.2×10^{-6} for the unavailability of $Q \cap R_B \cap R_A$.

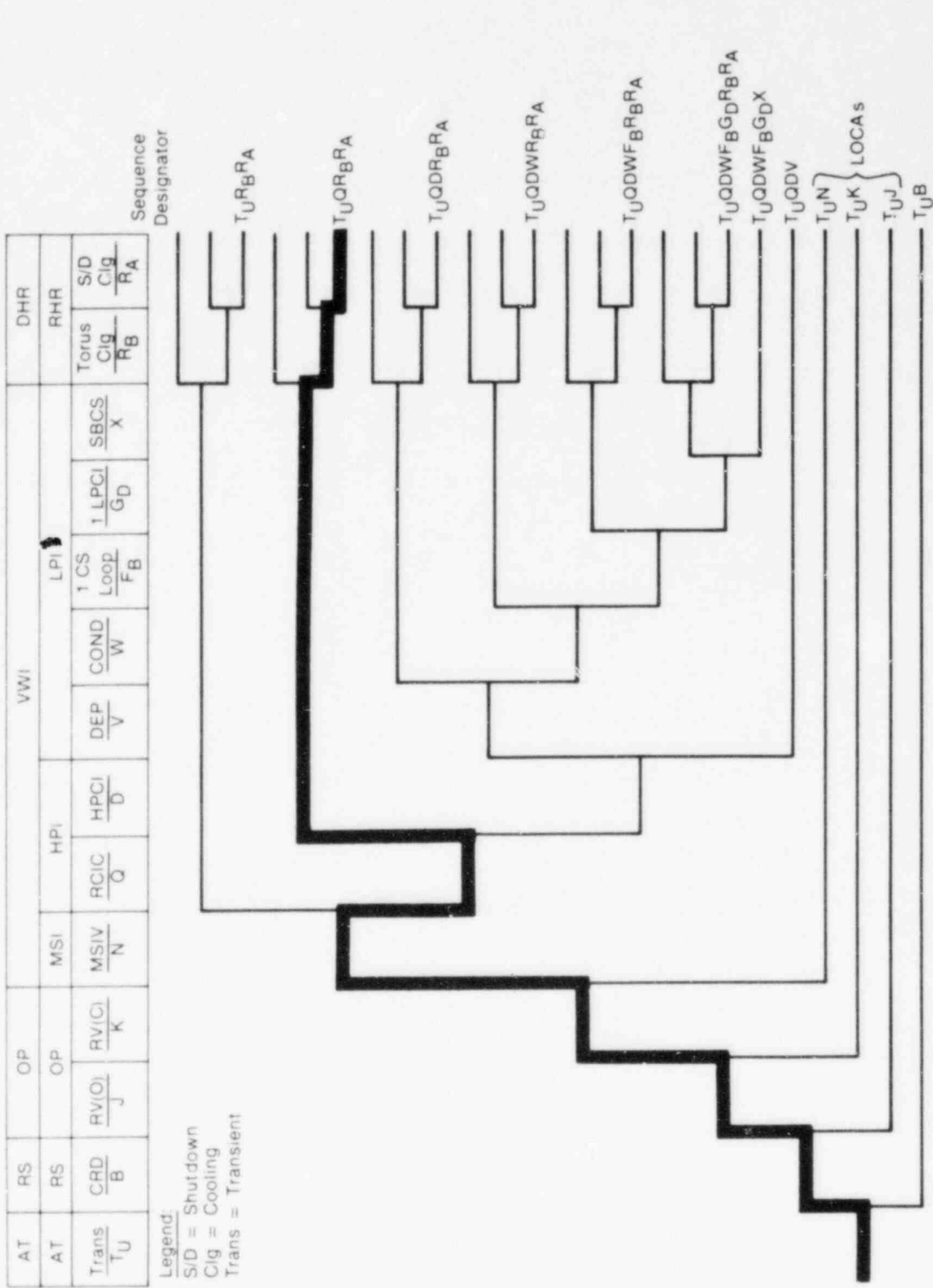
The dominant contributors for torus cooling and shutdown cooling failure are the same for this sequence as for sequence $T_U R_B R_A$. The recovery factors are also the same. The RCIC system dominant faults involve rupture disks and control circuits and are independent of the torus cooling and shutdown cooling faults. These faults are not recoverable under the guidelines, so no credit is taken for RCIC system recovery. Therefore, the unavailability of the mitigating systems considering recovery is 2.4×10^{-6} , as shown below.

$$\begin{aligned} Q(QR_B R_A) &= Q(Q) Q(R_B R_A \text{ considering recovery}) \\ &= Q(Q) Q(R_B R_A \text{ for sequence } T_U R_B R_A) \\ &= (0.042)(5.7 \times 10^{-5}) \\ &= 2.4 \times 10^{-6} \end{aligned}$$

$$\begin{aligned} P(T_U QR_B R_A) &= F(T_U) Q(QR_B R_A) \\ &= (1.7)(2.4 \times 10^{-6}) \\ &= 4.1 \times 10^{-6} \text{ per reactor-year.} \end{aligned}$$

4.2.5 LOSP-Induced Stuck Open Relief Valve (SORV) with DHR Failure ($T_p KR_B R_A$)

In this sequence, the LOSP causes a turbine trip without bypass, a reactor scram, main steam isolation, and opening of the relief valves. However, one or more of the relief valves fail to reclose after pressure has fallen below the relief valve setpoint. This is equivalent to an intermediate steam break with one exception. The steam from the relief valves does not go into the drywell. Rather, it goes to the torus water directly. After the HPCI system has succeeded in restoring reactor vessel level to normal, the torus cooling and shutdown cooling systems fail. The initial value for this sequence is 8.3×10^{-5} , based on an initiating frequency of 1.7×10^{-3} per year and 4.9×10^{-2} for the unavailability of $R_B \cap R_A$. The marked systemic event tree is Figure C-22.



INEL 2 1755

Figure C-20. Systemic event tree showing the TUQRBRA sequence.

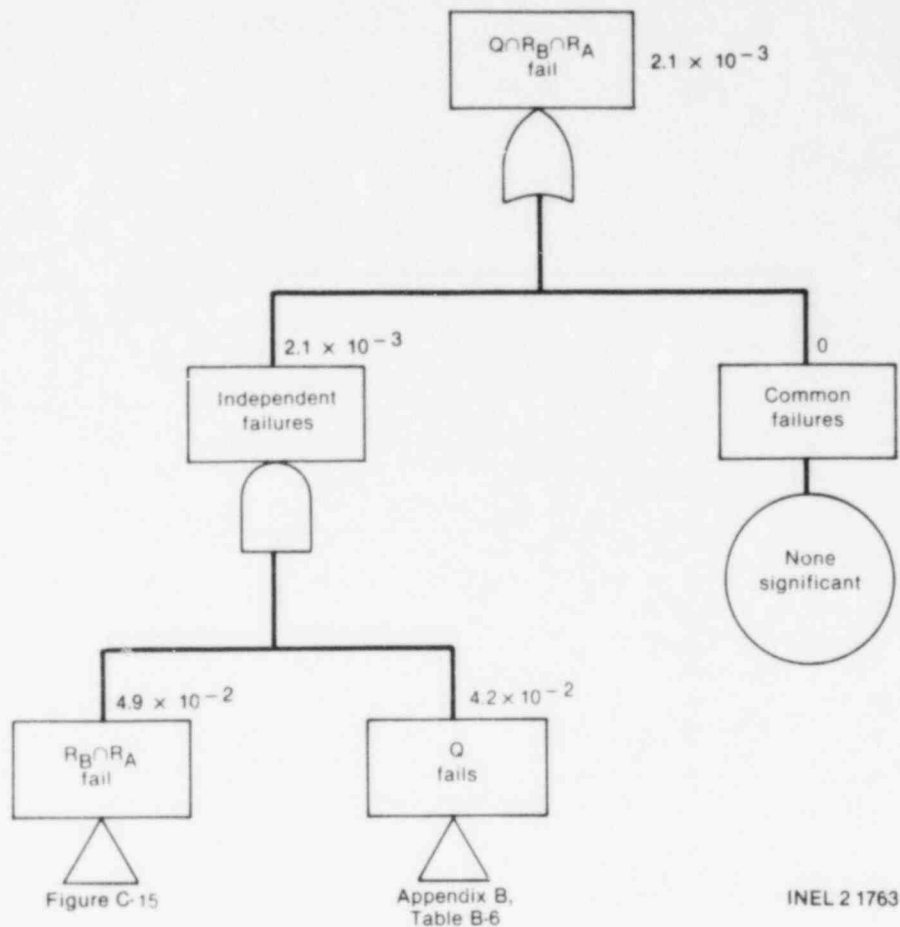
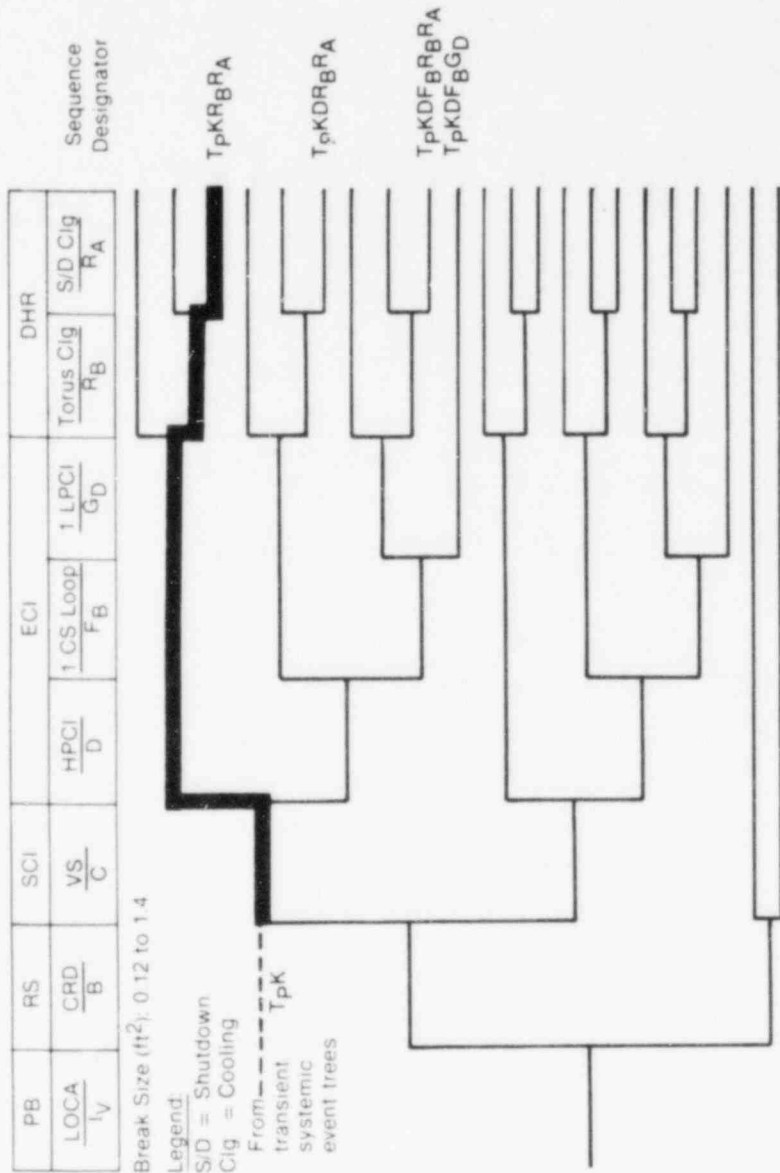


Figure C-21. Dominant contributors to the unavailability of the RCIC and RHR systems following a transient which disables the PCS (normal power available).

The RHR system in shutdown cooling or torus cooling mode provides the long term cooling. As was the case in the sequence $T_p R_B R_A$ of Section 4.2.1, the unavailability of the DHR function is 4.9×10^{-2} . The dominant contributor sequence evaluation diagram for that sequence applies to this sequence as well.

Preliminary phenomenological calculations being performed at INEL on BFI as part of the Severe Accident Sequence Analysis (SASA) program⁸ indicate that core temperatures will start to rise rapidly in as little as 30 min if the HPCI system does not function to replenish lost coolant inventory. Even with successful HPCI, torus water temperature will rise and eventually reach a temperature where the HPCI system will no longer have sufficient net positive suction head to maintain reactor level. The time available to recover is approximately the same as the LOSP with R_B and R failure. For this sequence, since HPCI is successful, it was assumed that at least 6 to 8 hours are available to restore offsite power. Using the WASH-1400 restoration figure and recovery factors based on 6 to 8 hours, the probability for R_B and R_A failure is the same as for sequence $T_p R_B R_A$ (9.4×10^{-4}). The final sequence value is then 1.6×10^{-6} .



INEL 2 1758

Figure C-22. Systemic event tree showing the TpKR_BRA sequence.

$$P(T_P K R_B R_A) = F(T_P K) Q(R_B R_A)$$

$$= (1.7 \times 10^{-3}) (9.4 \times 10^{-4})$$

$$P(T_P K R_B R_A) = 1.6 \times 10^{-6} \text{ per reactor-year.}$$

4.2.6 Transient-Induced SORV with DHR Failure (TKR_BR_A)

For this sequence, a transient causes a reactor scram and a number (depending on the initiator) of relief valves open. When pressure falls below the relief valve setpoint, one or more relief valves fail to close, and the reactor continues to blow down to the torus. When low water level is reached, the MSIVs shut and the HPCI system initiates. Following successful ECI by the HPCI system, the torus cooling and shutdown cooling systems fail. The initial value for this sequence is 1.2×10^{-5} per reactor-year, from a frequency of 1.63×10^{-1} per year for the initiator and an unavailability of 7.6×10^{-5} for the combination of $R_A \cap R_B$. The sequence is shown on the systemic event tree, Figure C-23.

This sequence is similar to the LOSP-induced SORV sequence of Section 4.2.5 except that the unavailability for the R_B and R_A combination is much lower because offsite power is available. However, the initiator frequency is approximately two orders of magnitude higher than for the LOSP-induced SORV sequences. The RHR system provides the long-term decay heat removal function in either the shutdown cooling or torus cooling mode. The unavailability for both modes is 7.6×10^{-5} . The major contributors to this unavailability are control circuit faults of the minimum-flow bypass valves and the suction and discharge path MOVs. The dominant contributor sequence evaluation diagram of Section 4.2.3 applies for this sequence also.

As with the sequence $T_U R_B R_A$ of Section 4.2.3, recoverability of the torus cooling and shutdown cooling systems is either by manual operation/repair of faulted RHR valve control circuits or by recovery of the PCS as a heat sink if possible. However, recovery of PCS is not easily quantifiable. Therefore, the final sequence probability for this sequence does not include a probability of recovery of PCS. The recoverability of R_B and R_A has been previously accounted for (5.7×10^{-5}). Therefore, the final sequence value is 9.3×10^{-6} , as shown below.

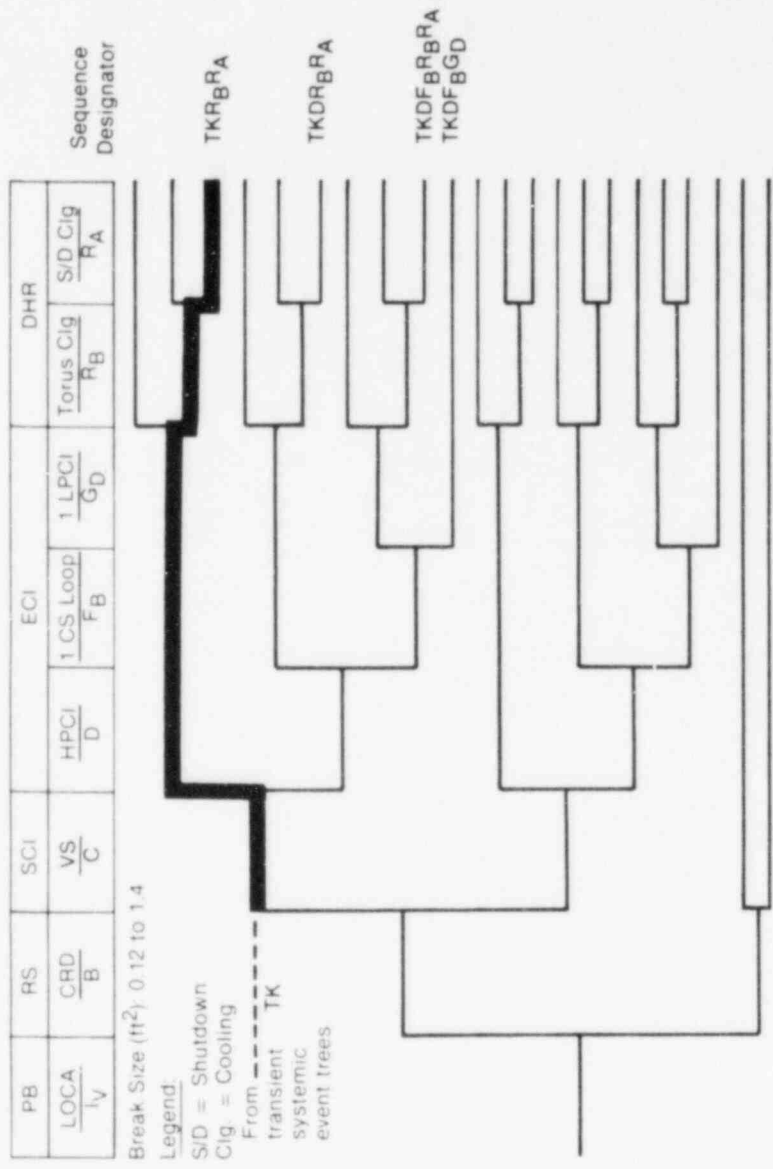
$$P(TK R_B R_A) = F(TK) Q(R_B \cap R_A)$$

$$= (0.163)(5.7 \times 10^{-5})$$

$$= 9.3 \times 10^{-6} \text{ per reactor-year.}$$

4.2.7 Transients without PCS with VWI Failure (T_UQDV)

A transient occurs that causes the reactor to scram and the MSIVs to close. After the relief valves open to relieve the increase in reactor pressure, all the valves reclose. This action repeats as reactor decay heat



INEL 2 1757

Figure C-23. Systemic event tree showing the TKRBRA sequence.

causes pressure to rise due to the lack of a heat sink. When low reactor level is reached, the HPCI and RCIC systems (D and Q, respectively) fail to operate to restore water level. As the water level continues to drop due to relief valve action, the operator fails to manually depressurize the reactor. If this condition persists, core melt occurs. The initial probability for this sequence is 2.8×10^{-5} per reactor-year, based on an initiating event frequency of 1.70 per year and 5.4×10^{-6} for the unavailability of $Q \cap D \cap V$. The systemic event tree showing this sequence is Figure C-24.

The unavailability of HPCI and RCIC combined is 1.8×10^{-3} and is dominated by rupture disk faults and control circuit faults of the MOVs in each system. The probability of failure to manually depressurize is dominated by failure of the operator to initiate depressurization, since only 4 of 13 valves are required to open for successful depressurization. Figure C-25 is a sequence evaluation diagram of the dominant contributors for this sequence. During the injection phase, there is little time available (30 to 40 min) for the operator to dispatch personnel to correct faults involving the HPCI and RCIC MOVs. If the operator fails to depressurize, then water level continues to decrease and the low pressure systems such as core spray, LPCI, and the condensate system cannot provide water to the reactor because reactor pressure is too high.

The probability of the operator failing to depressurize was originally taken to be 3×10^{-3} , based on the human error modeling guide of NUREG/CR-1278. This model, shown in Section 4.2 of Appendix B, does not include recovery because it was developed for initial screening purposes. However, recovery from an initial operator error in failing to depressurize is likely because of the heavy emphasis on depressurization given to operators during their training and the ease with which this action can be carried out. Since this recovery relates to operator error rather than actions directly mitigating the effect of hardware faults, the nonrecovery factors of Table C-6 are not applicable. Therefore, a more detailed operator action model was developed, considering not only the time frame for operator action but also the effect of additional operators in the control room. The new model, presented in Section 4.3 of Appendix B, shows that a consideration of recovery reduces the human error probability of failure to depressurize by a factor of 0.06. The final sequence frequency is then 5.5×10^{-7} per reactor-year, as shown below.

$$\begin{aligned} Q(QDV) &= (0.06) Q(Q \cap D \cap V) \\ &= (0.06)(5.4 \times 10^{-6}) \\ &= 3.2 \times 10^{-7} \end{aligned}$$

$$\begin{aligned} P(T_U QDV) &= F(T_U) Q(QDV) \\ &= (1.7)(3.2 \times 10^{-7}) \\ &= 5.5 \times 10^{-7} \text{ per reactor-year.} \end{aligned}$$

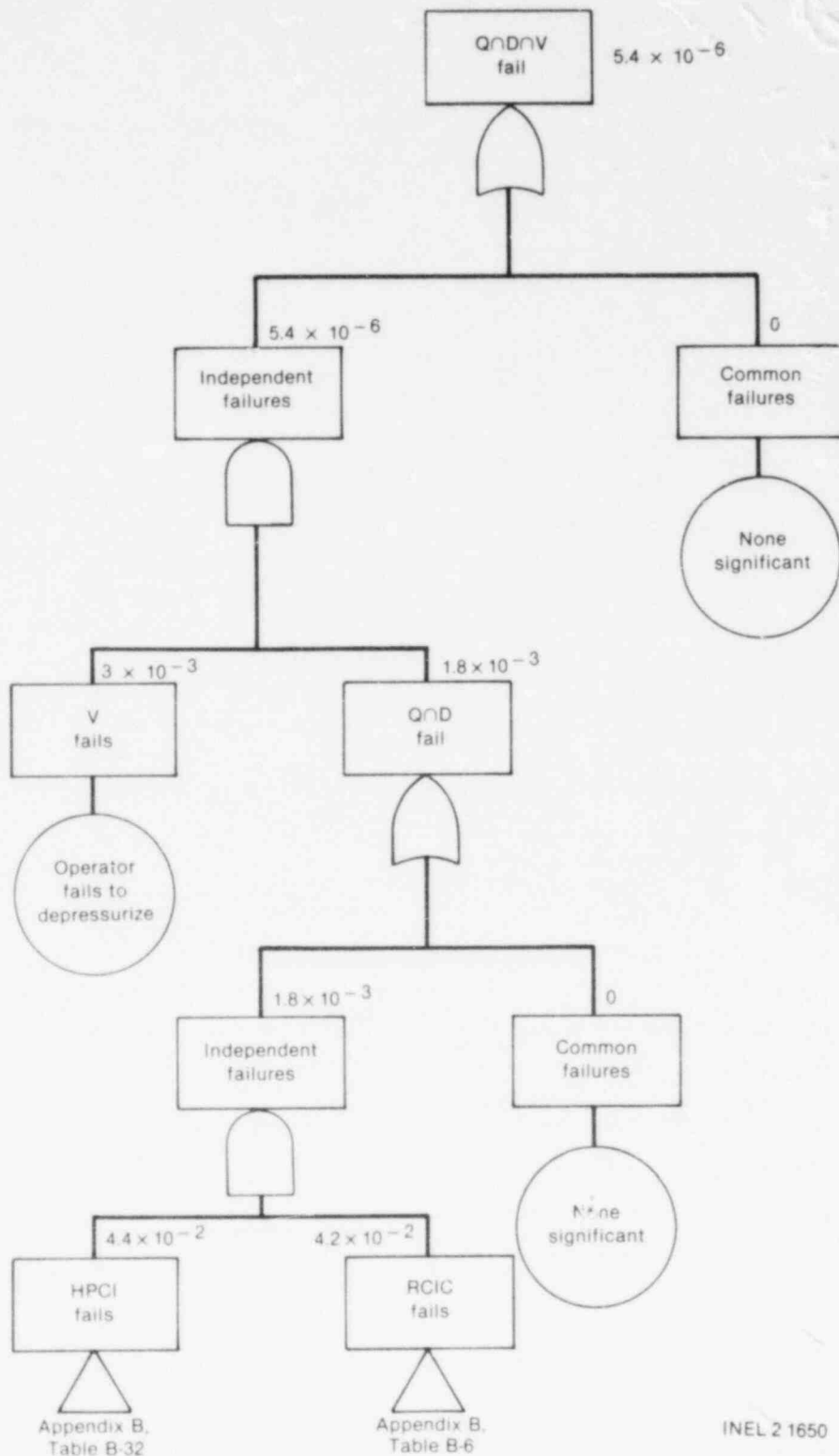


Figure C-25. Dominant contributors to the unavailability of RCIC, HPCI, and manual depressurization following a transient which disables the PCS (normal power available).

4.2.8 Loss of Offsite Power with VWI Failure ($T_p Q D F_B G_D X$)

After a LOSP, a turbine trip without bypass and a reactor scram occur. The relief valves open to relieve the pressure increase caused by the loss of the heat sink and reclose when pressure falls below the relief valve setpoint. This cycle continues until a low reactor water level is reached. At this point, the HPCI and RCIC systems (D and Q) fail to operate to maintain reactor water level. As the water level continues to drop due to relief valve action, the operator successfully depressurizes the reactor, but the core spray, LPCI, and SBCS systems (F_B , G_D , and X, respectively) fail to restore water level and core melt occurs. The initial value for this sequence is 1.2×10^{-6} per reactor-year, based on 1.70 per reactor-year for the frequency of LOSP and 4×10^{-5} for the unavailability of $D \cap F_B \cap G_D \cap X$. This sequence is highlighted on Figure C-26, the systemic event tree for the LOSP transient.

The unavailability of the injection systems for this sequence, i.e., the unavailability of HPCI and RCIC, is 1.3×10^{-3} and is essentially unaffected by the loss of offsite power. The unavailability of core spray, LPCI, and SBCS is affected by the LOSP and is 1.5×10^{-3} . This number is primarily due to diesel generator faults. Additionally, failure of the EECW system to provide its required cooling will cause the loss of all diesels and, thus, AC power for the RHR and core spray pumps. The EECW unavailability is 2.0×10^{-2} . The EECW value is dominated by combinations of failure of two diesels to start. These are not necessarily the same diesels that cause core spray and LPCI failure. Figure C-27 is a sequence evaluation diagram showing the dominant contributors to the mitigating systems unavailability.

Should this sequence occur, with the injection systems failed there are approximately 30 to 40 min before boiloff reduces reactor coolant inventory to a point where core temperature begins to rapidly rise. There are several viable recovery considerations available to the operators during this time period. One is a restoration of offsite power. From WASH-1400 (Figure III 6-4), approximately 70% of all offsite power outages can be repaired in 30 to 40 min. If LOSP is restored, this sequence is essentially the same as the transients without PCS with VWI failure, sequence $T_U Q D W F_B G_D X$.

Similarly, as with the LOSP with DHR failure sequence $T_p R_B R_A$ of Section 4.2.1, the EECW success criteria require three of four pumps to operate. If only two of four pumps operate, up to 91% of rated flow is available. Two additional RHRSW pumps are available for EECW service by opening (from the control room) one MOV for each pump.

Considering recovery, the unavailability of the injection systems becomes 1.2×10^{-6} . The final sequence frequency is then 3.6×10^{-8} , as shown below.

$$\begin{aligned} Q(QDF_B G_D X) &= (0.70)(\text{injection systems failure with LOSP recovered}) \\ &+ (0.30)(\text{injection systems failure without LOSP recovered}) \\ &= (0.70)(\text{unavailability of sequence } T_U Q D W F_B G_D X) \end{aligned}$$

AT		RS	OP	VWI				DHR	
AT	RS	OP	MSI	HPI		LPI		RHR	
Trans	CRD	RV(O)	MSIV	PCIC	DEP	COND	1 LPCI	Torus	S/D
TP	B	J	N	Q	V	W*	GD	Clg	Clg
		K		D			FB	RB	RA

Legend:

S/D = Shutdown

Clg = Cooling

Trans = Transient

* Probability of W is 1.0 for LOSP

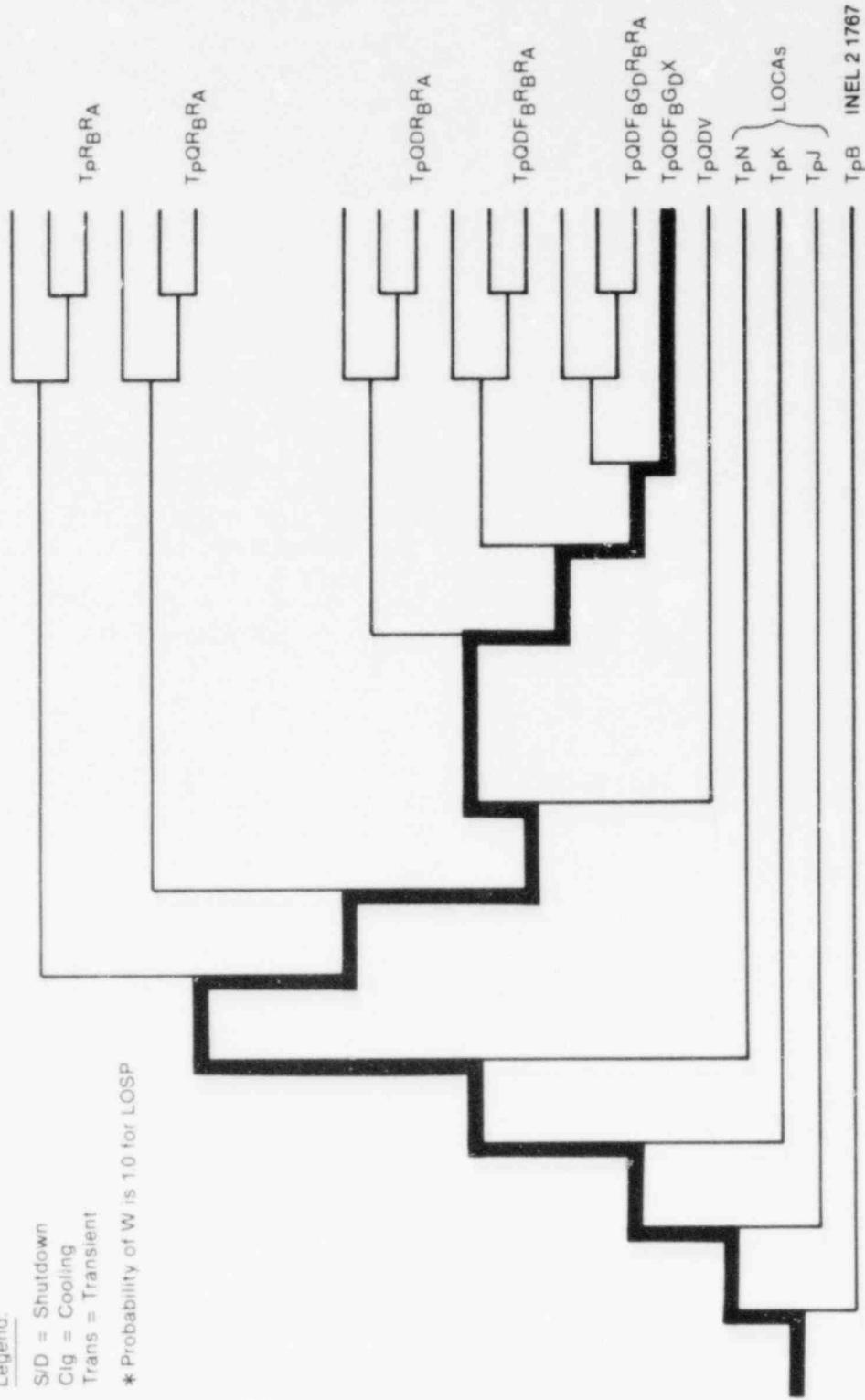


Figure C-26. Systemic event tree showing the TpQDFBGDX sequence.

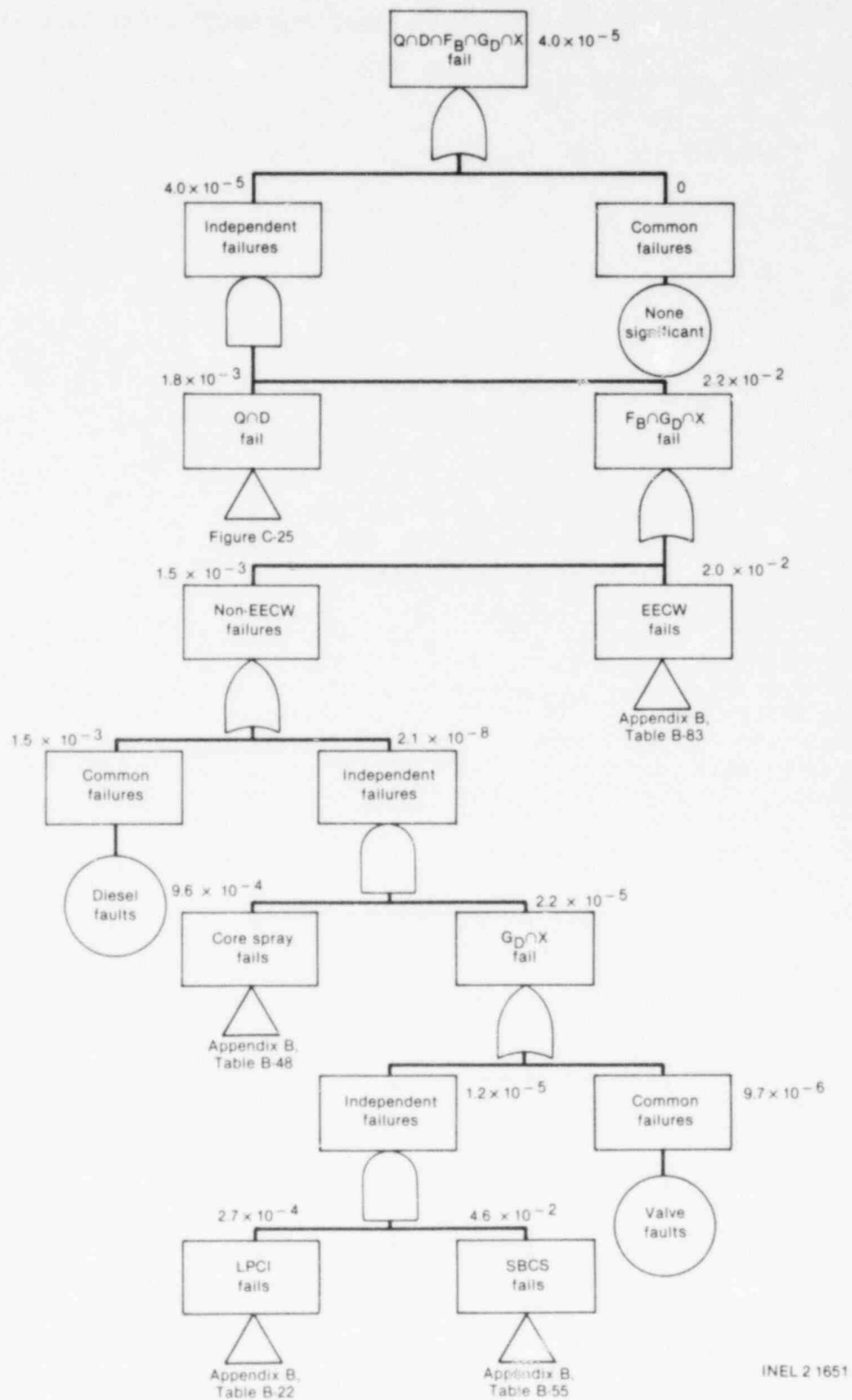


Figure C-27. Dominant contributors to the unavailability of RCIC, HPCI, LPCI, core spray, and SBCS given LOSP.

$$\begin{aligned}
& + (0.30)(\text{failure of HPCI and RCIC}) \\
& \cdot [(\text{failure of LPCI, core spray, and SBCS}) + (\text{failure of EECW}) \\
& \cdot (\text{operator nonrecovery})] \\
= & (0.70)(1.7 \times 10^{-8}) \\
& + (0.30)(1.8 \times 10^{-3})[1.5 \times 10^{-3} + (2.0 \times 10^{-2})(0.03)] \\
= & 1.2 \times 10^{-8} + 1.2 \times 10^{-6} \\
= & 1.2 \times 10^{-6}
\end{aligned}$$

$$\begin{aligned}
P(T_P QDF_B G_D X) &= F(T_P) Q(QDF_B G_D X) \\
&= (3 \times 10^{-2})(1.2 \times 10^{-6}) \\
&= 3.6 \times 10^{-8} \text{ per reactor-year.}
\end{aligned}$$

4.2.9 LOSP-Induced SORV with ECI Failure ($T_P KDF_B G_D$)

A LOSP causes a reactor scram and turbine trip without bypass. After the relief valves open to relieve the pressure increase caused by the loss of the heat sink, one or more of the relief valves fail to reseal when pressure drops below the relief valve setpoint. When water level drops to the low level point, the MSIVs shut but the HPCI system does not operate to refill the reactor. Subsequently, as level and pressure drop, neither the core spray nor LPCI systems operate to fill the reactor and a core melt occurs. The initial value for this sequence is 2.5×10^{-6} per reactor-year based on an initiating frequency of 1.7×10^{-3} per reactor-year and an unavailability of 1.5×10^{-3} for the combination of D, F_B , and G_D . The sequence is shown on the systemic event tree, Figure C-28.

The unavailability for the injection systems for this sequence is based on failure of the HPCI, core spray, and LPCI systems to operate. The HPCI unavailability is essentially not affected by the LOSP. The unavailability of core spray and LPCI, however, is dominated by combinations of diesel generator faults. Furthermore, the EECW unavailability (2.0×10^{-2}) also contributes to the probability of core spray and LPCI failure. Figure C-29 is a sequence evaluation diagram showing the dominant contributors to the mitigating systems unavailability.

As mentioned before in other LOSP sequences, the EECW success criteria was three of four pumps operating. Since two of four pumps can provide at least 91% of rated flow and since two other RHRSW pumps are readily available to provide flow to the EECW header, EECW is subject to recovery considerations.

Approximately 30 min is available for recovery while the relief valve remains stuck open. As discussed in previous sequence descriptions,

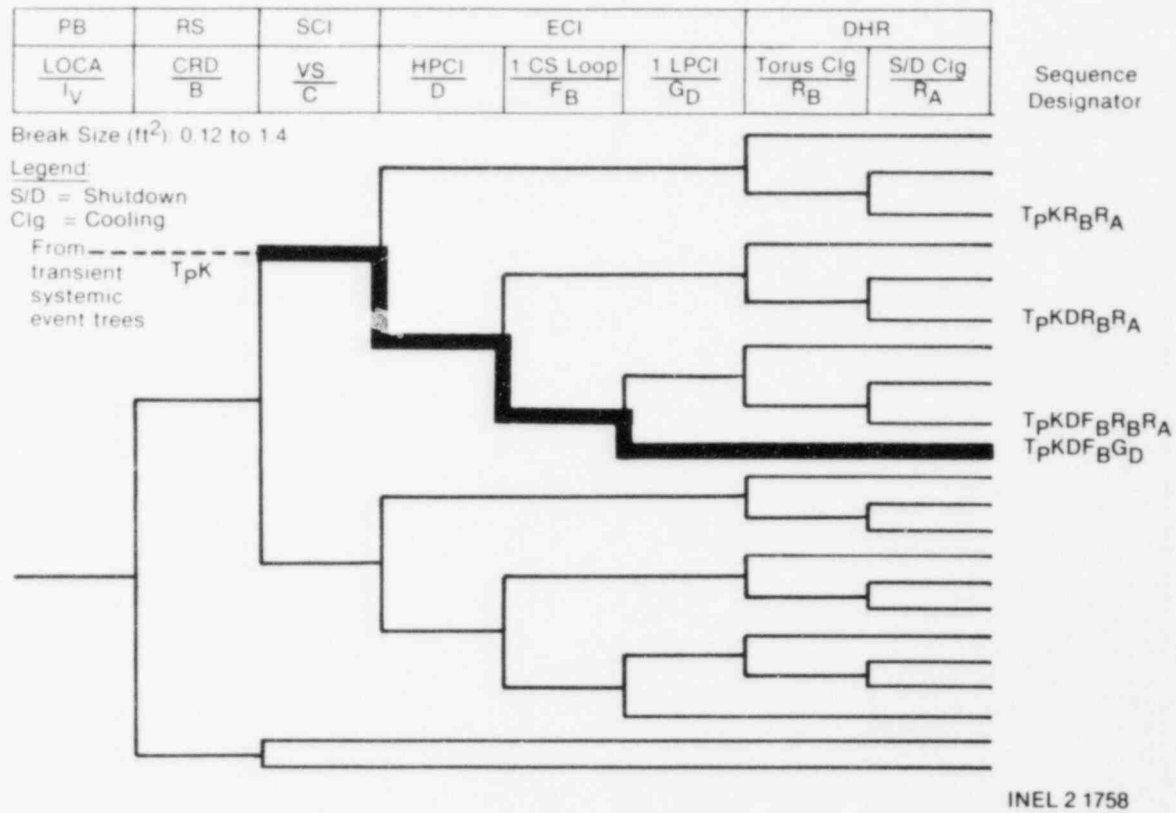


Figure C-28. Systemic event tree showing the TpKDF_BG_D sequence.

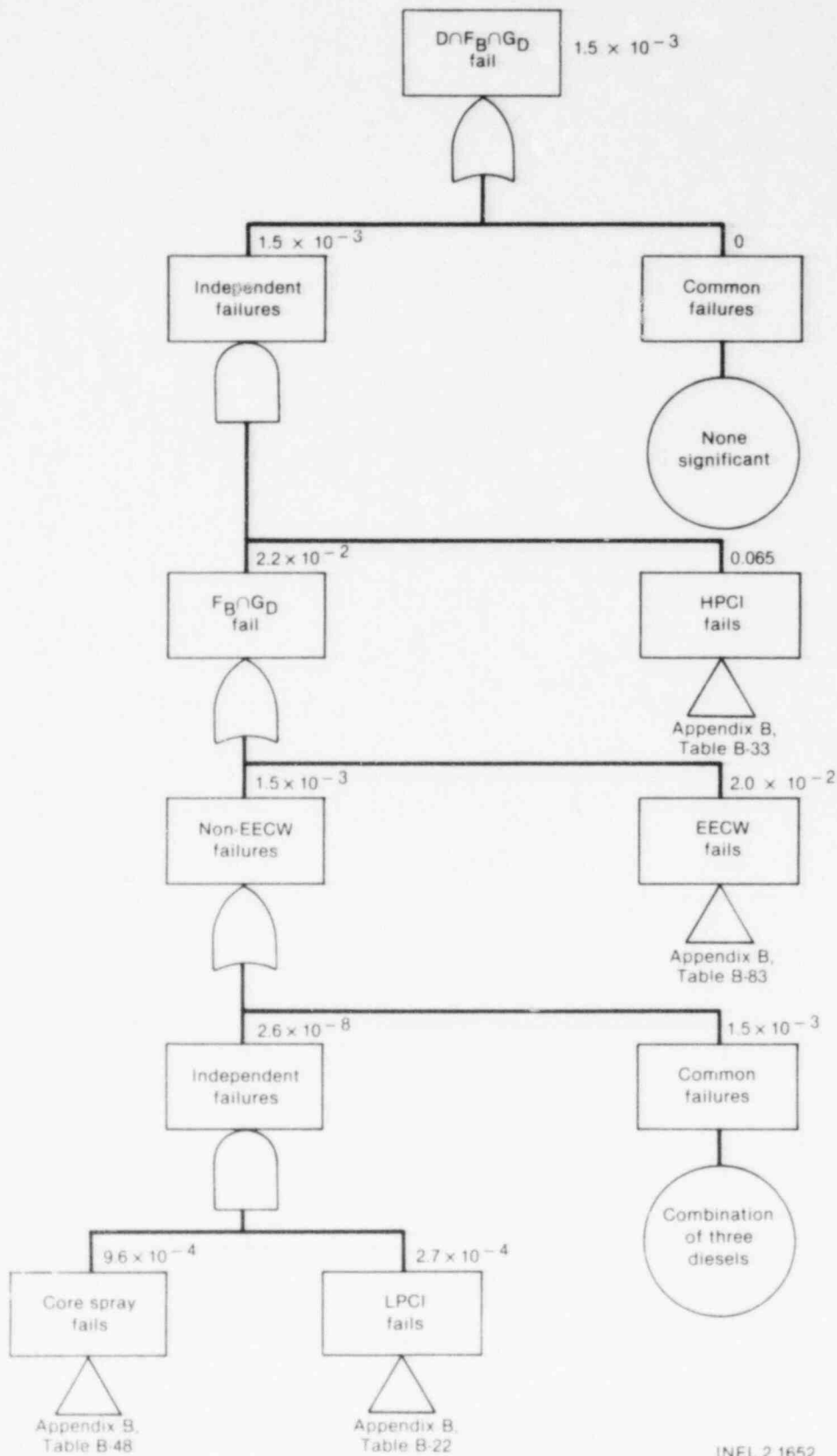


Figure C-29. Dominant contributors to the unavailability of HPCI, LPCI, and core spray, given LOSP and SORV.

approximately 70% of the offsite power outages can be repaired during this time. If offsite power is restored, this sequence becomes very similar to the transient-induced SORV sequence, TKDF_BG_D.

Considering the potential recovery of offsite power and the EECW system, the injection system unavailability becomes 5.1×10^{-5} . The final sequence frequency is then 8.7×10^{-8} , as shown below.

$$\begin{aligned}
 Q(F_{B D} G_D) &= (0.70) \text{ (unavailability with LOSP recovered)} \\
 &+ (0.30) \text{ (unavailability with LOSP not recovered)} \\
 &= (0.70) \text{ (injection systems for sequence TKDF}_{B D} G_D) \\
 &+ (0.30) \text{ (failure of HPCI)} [\text{(failure of core spray and LPCI to} \\
 &\quad \text{operate)} + \text{(failure of EECW (operator nonrecovery))}] \\
 &= (0.70)(2.4 \times 10^{-6}) + (0.30)(6.5 \times 10^{-2}) \\
 &\quad \cdot [(1.5 \times 10^{-3}) + (2.0 \times 10^{-2})(0.05)]
 \end{aligned}$$

$$\begin{aligned}
 Q(DF_{B D} G_D) &= 1.7 \times 10^{-6} + 4.9 \times 10^{-5} \\
 &= 5.1 \times 10^{-5}
 \end{aligned}$$

$$\begin{aligned}
 P(T_P KDF_{B D} G_D) &= F(T_P K) Q(DF_{B D} G_D) \\
 &= (1.7 \times 10^{-3})(5.1 \times 10^{-5}) \\
 &= 8.7 \times 10^{-8} \text{ per reactor-year.}
 \end{aligned}$$

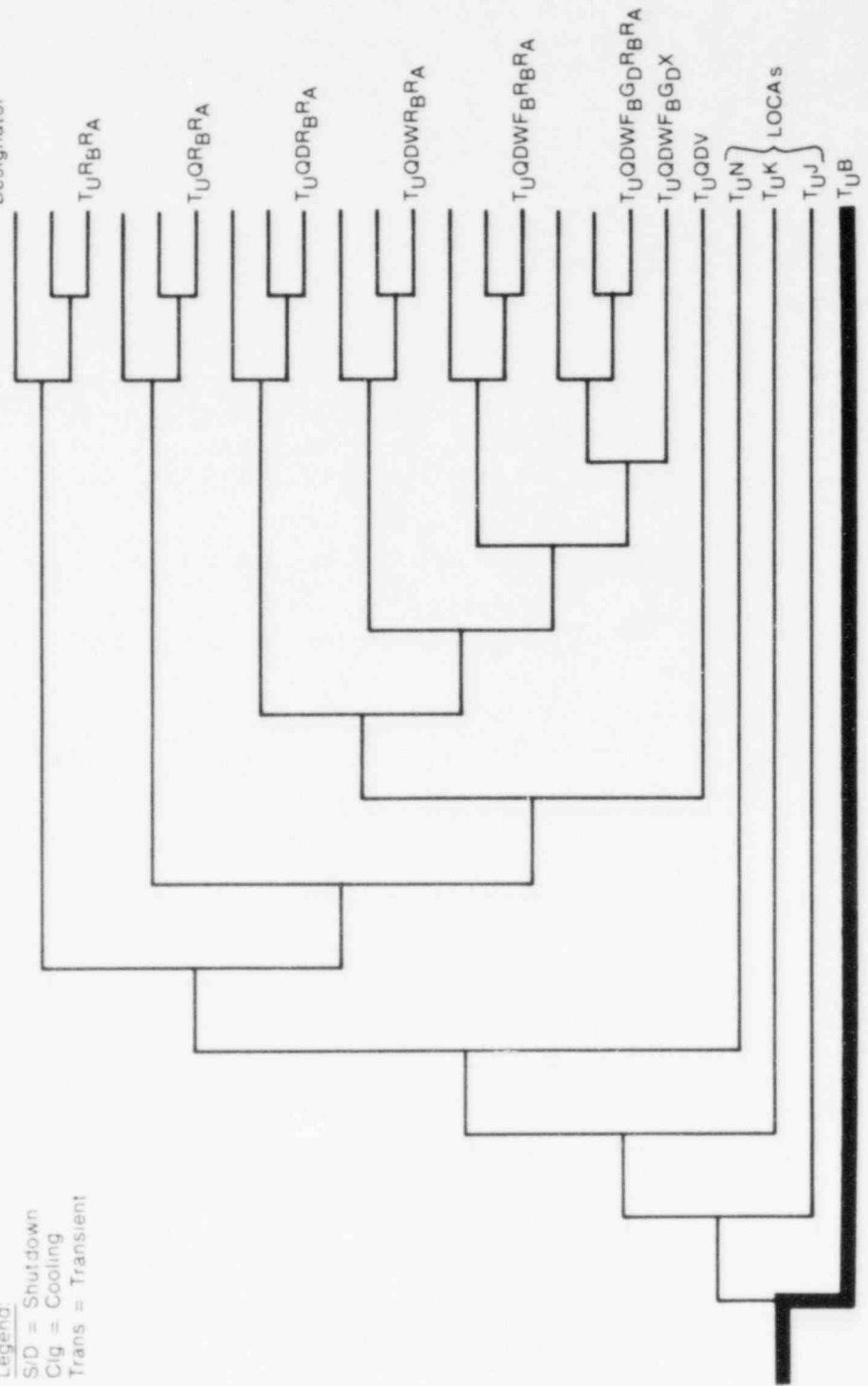
4.2.10 Transients Without PCS with Failure to Scram (T_UB)

In this sequence, a transient occurs that makes the main condenser unavailable as a heat sink. Failure of the reactor to scram allows reactor power to remain high. As a result, the pressure increases until the relief valves open. The HPCI and RCIC systems are not capable of providing makeup to the reactor as fast as steam is being lost to the torus via the relief valves. Therefore, the core uncovers and melts. The initial value for this sequence is 5.1×10^{-5} , based on an initiating frequency of 1.70 per reactor-year and an unavailability of 3×10^{-5} for failure to scram. The sequence is shown on the systemic event tree, Figure C-30.

Since core uncover in this scenario will occur within the first 10 min (depending on power level), the recovery guidelines do not allow for considering operator action to correct the condition. Therefore, the final sequence value is the same as the initial value of 5.1×10^{-5} .

AT		RS		OP		VWI				DHR	
AT		RS		OP		HPI		LPI		RHR	
Trans		CRD		RV(O)		MSIV		1 CS		S/D	
U		B		J		N		Loop		Clg	
				K		O		FB		RA	
				V		D		GD		RB	
				W		Q		X			
				X							

Legend:
 S/D = Shutdown
 Clg = Cooling
 Trans = Transient



INEL 2 1755

Figure C-30. Systemic event tree showing the TU_B sequence.

The unavailability for the reactor scram function is 3.0×10^{-5} . This number was taken from the ATWS document NUREG-0460. This analysis did not evaluate the probability of failure to scram using the fault tree methodology. As noted in WASH-1400 and NUREG-0460, the exact number of rods that must fail to insert and the relative position of those rods is not easily calculated and was considered beyond the scope of this analysis. Thus, the NUREG-0460 probability value for failure to reach subcriticality was used in lieu of a specific evaluation of the reactor subcriticality function.

4.2.11 Transients with PCS with Failure to Scram and Recirculation Pump Trip Failure (T_{ABM})

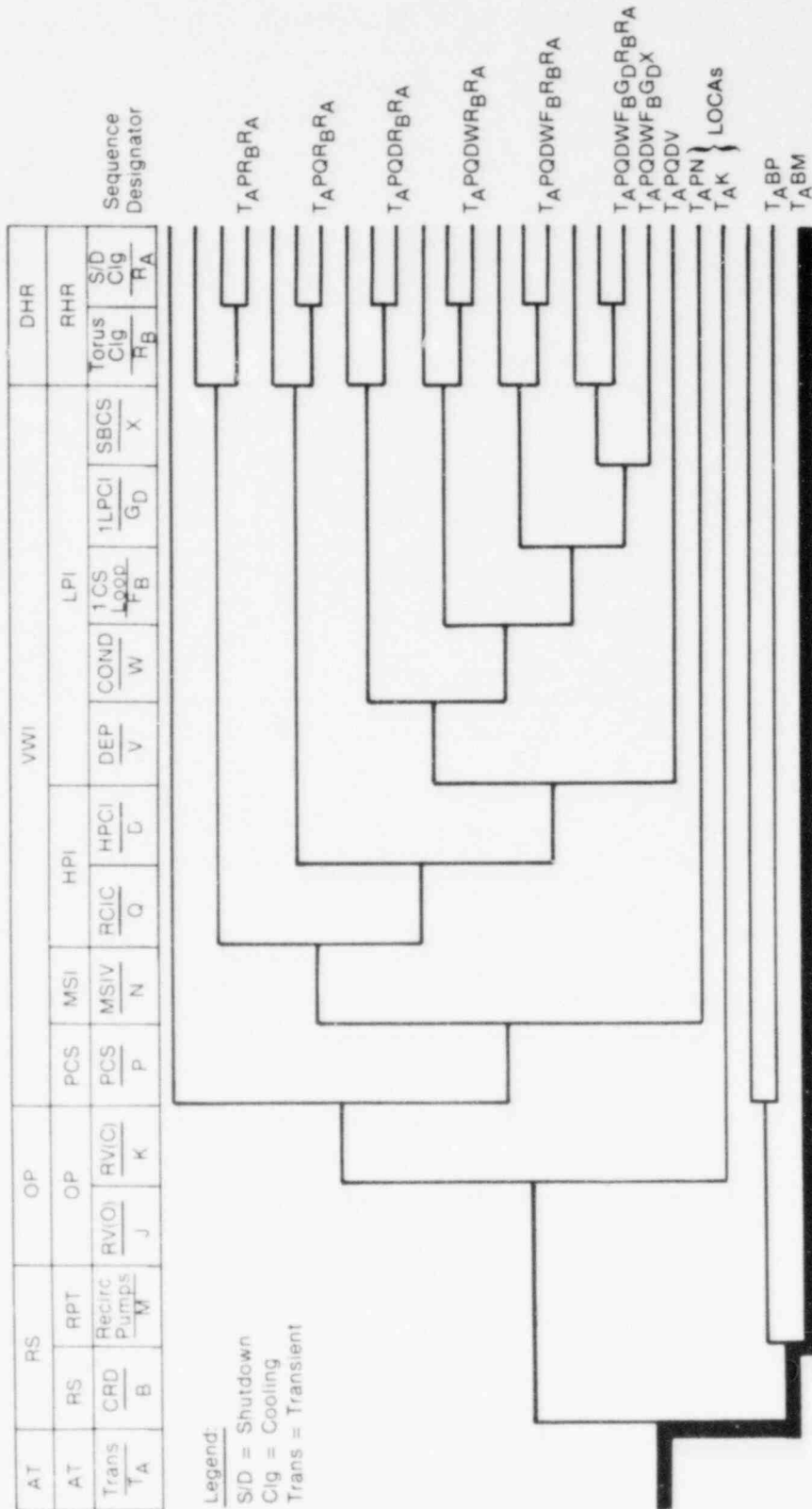
In this sequence, a transient occurs that does not cause the MSIVs to close. The PCS is available both as a heat sink and a source of makeup water to the reactor. If the RPT is successful, the resulting reactor power level is within the capacity of the bypass valves to remove heat from the reactor. Failure of the RPT allows reactor power level to remain above the capacity of the bypass valves. Therefore, reactor pressure increases until the relief valves open. The feed pumps are able to maintain level but the steam going through the relief valves to the torus does not return to the condenser to be reinjected to the core. Thus, condensate storage tank level decreases until the condensate and feed systems trip. At this point, reactor water level decreases until the MSIVs close making the PCS unavailable. Level continues to drop until core uncover occurs and a core melt ensues. The initial value for this sequence is 3.7×10^{-6} , based on an initiating frequency of 1.68 per reactor-year and 2.2×10^{-6} for the unavailability of the combination of B and M. The sequence is shown on the systemic event tree, Figure C-31. Figure C-32 is a sequence evaluation diagram showing the dominant contributors to the mitigating systems unavailability.

The dominant contributor to failure of both the reactor scram system and the RPT is failure of the reactor protection system to initiate either one. This value was taken to be 1.9×10^{-6} from the WASH-1400 report, since no analysis of the reactor protection system was done for the present report.

The potential recovery actions for this sequence involve manually scrambling the reactor or operator trip of the recirculation pumps. The time available to do either of these is a function of the reactor power level. Since the reactor power/bypass valve mismatch could be as high as 70% of full power, the time available for operator action would be minimal. Therefore, no credit is taken for operator action to prevent a core melt for this sequence. The final sequence value is then 3.7×10^{-6} .

4.3 Dominant Sequences

Those sequences from Table C-9 that have final sequence frequencies greater than 1.0×10^{-6} per reactor-year are the dominant sequences. There are eight dominant accident sequences. Six of these are transient sequences, while the other two are transient-induced LOCAs. Table C-14 lists these sequences in decreasing order of frequency.



INEL 2 1770

Figure C-31. Systemic event tree showing the TABM sequence.

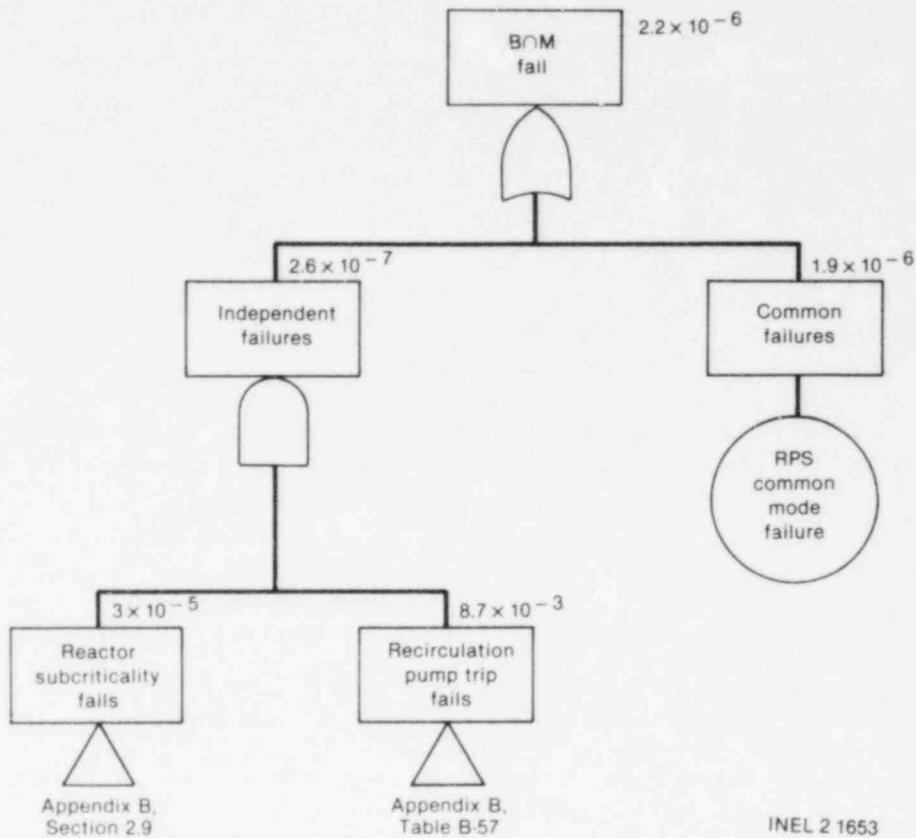


Figure C-32. Dominant contributors to the unavailability of the CRD and RPT systems following a transient where the PCS is available.

TABLE C-14. DOMINANT SEQUENCES

<u>Sequence Initiator</u>	<u>Sequence Designator</u>	<u>Frequency</u>
Transient without PCS	T _U R _B R _A	9.7 × 10 ⁻⁵
Transient with PCS	T _U B	5.1 × 10 ⁻⁵
Loss of offsite power	T _P R _B R _A	2.8 × 10 ⁻⁵
Transient-induced LOCAs	T _K R _B R _A	9.3 × 10 ⁻⁶
Transient without PCS	T _U Q _R B _R A	4.1 × 10 ⁻⁶
Transient with PCS	T _A BM	3.7 × 10 ⁻⁶
LOSP-induced LOCAs	T _P K _R B _R A	1.6 × 10 ⁻⁶
Loss of offsite power	T _P Q _R B _R A	1.2 × 10 ⁻⁶

5. UNCERTAINTY ANALYSIS

5.1 Introduction

The point estimate of the frequency of each dominant sequence appears in Table C-14. In addition to knowing the point estimate of the frequency for these sequences, it is also useful to understand the uncertainty associated with each point estimate. The uncertainty analysis of this report only propagates errors associated with the given basic event failure rates and initiating event frequencies. Other uncertainties associated with quality assurance, success criteria, etc., are not included. The results of this analysis, therefore, only evaluate the uncertainty associated with the failure rate data base. The main purpose of the uncertainty analysis is to provide those using this report with additional perspective on the results. When evaluating potential design or operational changes, it may well be useful to examine changes to the uncertainty bounds as well as to the point-value estimates.

5.2 Methodology

The uncertainty bounds for each sequence were determined by assigning an uncertainty bound and a distribution to each basic event and sequence initiator. The MOCARS computer code⁹ uses this information along with the cut sets for the systems to perform a Monte Carlo simulation that describes the resulting distribution for the systems. In much the same way as point estimates were obtained, the COMCAN code was used to identify cut sets common to two or more systems. These cut sets were also evaluated using the MOCARS code and appropriately combined to generate the distribution for the sequence.

The upper bound value was chosen to be the value of the sequence distribution at the 95% quantile. In other words, 95% of the distribution values generated by MOCARS were less than or equal to the upper bound value. Rather than expressing this upper bound as a fixed value, it is associated with the point estimate by an error factor that equals the upper bound divided by the point estimate.

5.3 Data Base

Table C-4 gives the error factors used for the basic event point estimates for most of the basic events. For human error probabilities and the generic control circuit models, an error factor of 10 was used. Most hardware failure data had error factors of three. Using an error factor of 10 for these two cases is, therefore, more conservative and puts the uncertainty for these events on the same level as short circuits, valve ruptures, and similar passive failures where the data base is sparse.

The lognormal distribution was chosen as the distribution for each basic event and for the initiating events. The lognormal distribution is commonly used in analyses where the uncertainty associated with the data is expressed in orders of magnitude differences from the point estimate.

The dominant sequence initiators are all transients or transient-induced LOCAs. The point estimates for these initiators came from EPRI

NP-801 as noted in Appendix A, Section 2.2. While EPRI NP-801 did assign 95% upper bound values on transient initiator frequencies, these bounds were assigned on a generic basis (i.e., BWRs, PWRs). Since the point estimates used for sequence frequency calculations were Browns Ferry-specific and EPRI NP-801 did not assign uncertainty bounds on a plant-specific basis, an error factor of three with a lognormal distribution was assigned for each initiator. Compared with the EPRI NP-801 generic data, an error factor of three is more conservative as is the assumption of a lognormal distribution.

5.4 Results

Table C-15 summarizes the results of the uncertainty analysis. Each dominant sequence is listed in descending order of the final frequency. Both the initial sequence frequency and error factor and the final sequence frequency (considering recovery) and error factor appear in the table. In addition, the sum of the dominant sequence frequencies and its associated error factor is shown. The error factor for the sum represents the result of a MOCARS evaluation of the sum of the dominant sequence distributions.

5.5 Insights on Uncertainty Analysis

In Section 4, the effect of control circuit faults on sequence frequencies involving failure of torus cooling and shutdown cooling is discussed. Table C-15 shows another aspect of the control circuit fault contribution. This contribution is to the uncertainty. Because of the assumption of an error factor of 10 for control circuit faults and their dominance in the point estimate of some sequences, control circuit faults

TABLE C-15. DOMINANT SEQUENCE UNCERTAINTIES

<u>Sequence Designator</u>	<u>Initial Frequency</u>	<u>Error Factor</u>	<u>Final Frequency</u>	<u>Error Factor</u>
T _{URB} RA	1.3 x 10 ⁻⁴	20.5	9.7 x 10 ⁻⁵	8.7
T _{UB}	5.1 x 10 ⁻⁵	5.0	5.1 x 10 ⁻⁵	5.0
T _{PRB} RA	1.5 x 10 ⁻³	5.6	2.8 x 10 ⁻⁵	2.8
T _{KRB} RA	1.2 x 10 ⁻⁵	21.5	9.3 x 10 ⁻⁶	9.0
T _{UQRB} RA	5.5 x 10 ⁻⁶	36.3	4.1 x 10 ⁻⁶	15.3
T _{ABM}	3.7 x 10 ⁻⁶	4.6	3.7 x 10 ⁻⁶	4.6
T _{PKRB} RA	8.3 x 10 ⁻⁵	6.7	1.6 x 10 ⁻⁶	2.8
T _{PQRB} RA	6.2 x 10 ⁻⁵	10.7	1.2 x 10 ⁻⁶	4.7
Total	1.9 x 10 ⁻³	5.8	2.0 x 10 ⁻⁴	5.6

are large contributors to the error factor associated with the initial frequency of these sequences. After adjusting for recovery, but keeping an error factor of 10, the error factor for the final frequency is reduced considerably. These control circuit faults were considered to be recoverable whenever there is enough time (a) to repair or bypass the control circuits, (b) to manually operate a valve, or (c) to valve in another pump, as is the case with torus cooling and shutdown cooling (long-term decay heat removal). Therefore, their contribution to the final sequence frequency was less than their contribution to the initial sequence frequency. Similarly, the final frequency error factor is less sensitive to control circuit faults than its corresponding initial frequency error factor.

Another example of this particular sensitivity is that the uncertainty for sequence $T_{URB}R_A$ initially is quite a bit higher than for sequence $T_{PRB}R_A$. In the case of sequence $T_{PRB}R_A$, the dominant faults were combinations of diesel generator faults (error factor of three) instead of control circuit faults (error factor of 10) as in sequence $T_{URB}R_A$.

Thus, it is apparent that the high error factors in some dominant sequence initial values are associated with the conservatism in the choice of the error factor of 10 for control circuit faults. Furthermore, when recovery is considered, the uncertainty diminishes by approximately a factor of two even when the conservative error factor of 10 is carried through.

To further demonstrate the conservative nature of the error factor used for control circuit faults, a MOCARS evaluation of the generic model using the data of Table C-4 was performed. This analysis provided an error factor of 2.1, which is considerably less than the assumed value of 10.

Another interesting insight comes from the sequence totals before and after recovery is considered. Even when control circuits are considered in their conservative case, the total core melt frequency error factor is only 5.8. After considering recovery, the error factor drops to 5.6. Thus, despite the fact that some sequences have relatively high error factors, their effect on the cumulative core melt frequency error factor is relatively modest. Furthermore, consideration of recovery actions reduces the cumulative frequency by approximately one order of magnitude while maintaining approximately the same error factor. This tends to indicate that the error factor for the cumulative core melt frequency is not significantly affected by recovery factors or by the wide error spread of a few sequences.

6. SENSITIVITY ANALYSIS

6.1 Introduction

After selection of the dominant sequences and evaluation of the uncertainties associated with each, it is important to examine the assumptions and uncertainties that went into the original values. A sensitivity analysis can aid in understanding the contributors to dominant sequence frequencies. The method of performing such an analysis is to identify potential uncertainties and recalculate the sequence frequencies to show how much variations in selected input parameters change the final value.

6.2 Scope of Analysis

Review of the dominant sequences revealed several areas where a sensitivity analysis would be desirable. These areas are summarized below.

1. The RHR trees assumed that failure of the minimum-flow bypass valves to close would disable the RHR loops. Since about 90% of the flow per loop would not be diverted by such a failure, what would be the effect on sequence frequency if such failures did not disable the RHR loops?
2. For the LOSP initiated sequences, failure of EECW was an important contributor to the sequence frequencies. The analysis assumed that three of four pumps were needed to supply adequate cooling. Since two of four pumps provides up to 91% of the necessary cooling, what change to the sequence frequency would occur if the EECW model were changed to require only two of four pumps for successful cooling?
3. The transient-induced LOCA initiator frequencies were derived from the transient systemic event trees using the WASH-1400 failure data for relief valves. What would be the change in these sequences if the generic stuck open relief valve frequency from EPRI NP-801 was used instead?
4. Unavailabilities for valve and pump control circuits were based on analysis of typical systems. A more detailed analysis of the corresponding systems would be possible. In particular, what would be the effect of modeling differences between AC- and DC-powered valve control circuits, and of modeling the effect of 4160 V rather than 480 V AC motor control circuits?

Other areas considered for sensitivity analysis include the usage of cross-connects between the three units at Browns Ferry in recovery actions for the dominant sequences. Cross-connects are described in Appendix B Section 1.2, but no credit was taken in the analysis for their use. While they do represent a potential resource for cooling the core, their components are tested less frequently than ECCS and operators must follow complicated, seldom-used procedures to bring them online. Their impact on recovery possibilities is thus judged to be minimal, and sensitivity studies to consider their effect were not performed.

The remaining sections describe the sensitivity analysis results for the four topics listed above.

6.3 Evaluation

In order to answer the questions previously noted, the fault trees or the initiator values were changed. The resulting sequence frequencies are presented for comparison.

6.3.1 Exclusion of Minimum-Flow Bypass Valves

Removal of minimum-flow bypass valve faults from the RHR fault trees reduces torus cooling unavailability from 3.1×10^{-3} to 1.7×10^{-3} . Shutdown cooling unavailability decreases from 2.0×10^{-2} to 1.0×10^{-2} . The commonalities between torus cooling and shutdown cooling are reduced to 2.4×10^{-6} when the bypass valves are removed, since the original values contained both support system and minimum-flow bypass valve faults. Therefore, the unavailability of torus cooling and shutdown cooling becomes 2.0×10^{-5} . This value is approximately 3.8 times less than the value obtained with the minimum-flow bypass valves considered in the RHR model.

Considering potential recovery further reduces the unavailability of torus cooling and shutdown cooling without the bypass valves. Of the 1.0×10^{-2} unavailability for shutdown cooling, approximately 2.3×10^{-3} represents nonrecoverable faults. The remaining 7.7×10^{-3} is potentially recoverable. Applying the recovery guidelines discussed previously in Section 3.3 produces a final unavailability for shutdown cooling of 2.4×10^{-3} . Of the torus cooling unavailability of 1.7×10^{-3} , approximately 1.1×10^{-3} is nonrecoverable. The remaining 6.0×10^{-4} is potentially recoverable. The resulting torus cooling unavailability is then 1.1×10^{-3} . The commonalities of torus cooling and shutdown cooling are also recoverable. Therefore, the resulting unavailability is 2.6×10^{-6} . This value is approximately 22 times lower than the unavailability after recovery with the bypass valves included.

Because the minimum-flow bypass valves are common to both the torus cooling and shutdown cooling fault trees, exclusion of these two valves reduces the prerecovery unavailability of the systems. Since many of the minimum-flow bypass valve faults were not recoverable, postrecovery unavailabilities are not affected as much when the valves remain in the tree (7.6×10^{-5} to 5.7×10^{-5}) as when they are removed (2.0×10^{-5} to 2.6×10^{-6}). This indicates that the torus cooling and shutdown cooling unavailabilities are sensitive to minimum-flow bypass valve faults, especially when recovery is considered.

Therefore, for those dominant accident sequences involving transients other than LOSP where shutdown and torus cooling fail ($R_B R_A$), the final sequence frequencies would be reduced approximately by a factor of 22 if faults associated with the minimum-flow bypass valves were not considered. For LOSP-initiated sequences, failure of $R_B R_A$ is dominated by faults other than those associated with the bypass valves, and no change in sequence frequency would be realized.

6.3.2 Modification of EECW Success Criteria

As noted in the discussions of candidate dominant sequences, for LOSP initiators, the EECW system represents a common mode failure for all the AC systems. The success criteria for EECW in these sequences was three of four pumps operating. Since two of four pumps can provide up to 91% of the design flow requirements, it would be desirable to understand how those sequence frequencies would be affected if two of four pumps were sufficient.

Evaluation of the EECW system with a success criteria of two of four pumps under a LOSP condition reduces the unavailability from 2.0×10^{-2} to 2.3×10^{-3} . For the three LOSP initiated dominant sequences, this change would reduce the unavailability of torus cooling and shutdown cooling from 4.9×10^{-2} to 3.1×10^{-2} , thereby reducing the initial sequence frequency for these sequences by a factor of 1.6. Since the EECW contribution after recovery is considered negligible for these sequences (even with the original 2.0×10^{-2} value for three of four pumps), the final sequence frequency for these sequences would not be affected by the change in EECW success criteria to two of four pumps.

6.3.3 Transient-Induced SORV Initiator

The frequency of transient-induced stuck open relief valves in this analysis is based on the EPRI NP-801 frequencies for transients and the failure data for failure of the relief valves to reclose after a demand (see the treatment of System K in Appendix B, Section 2.6). It is desirable to investigate how using the EPRI NP-801 value for SORV frequency would change these sequence frequencies.

From the EPRI NP-801 data, the frequency of a SORV for Bf1 is 0.95 per reactor-year compared to an average of 0.2 per reactor-year for General Electric (GE) plants. The transient event tree analysis for Bf1 yielded a frequency of SORV initiators of 0.16 per reactor-year. Using the Bf1-specific number would increase the sequence frequency of transient induced SORVs by a factor of 5.9. Using the GE average only increases the frequency of a factor by 1.25.

This information tends to indicate that the event tree frequency determination for SORVs matches well with the industry average data but not with the Bf1-specific data. It should be noted that the three-stage relief valves originally installed at Bf1 are being replaced by two-stage versions. Therefore, the previous plant-specific data for SORVs may now be unrepresentative of the current design. Also, the EPRI NP-801 data for Bf1 was based on the first 37 months of operation. Accounting for subsequent operation may change the plant-specific frequency. In fact, EPRI document NP-2230¹⁰ contains updated information and revisions to the original EPRI NP-801 data. This document reflects a much larger data base than EPRI NP-801, but the GE average value changes only from 0.20 to 0.21. The Bf1-specific value is reduced to 0.05, and the average of Bf-1, -2, and -3 is 0.31. In light of the GE average and updated Bf1 specific data, the Bf1 event tree determined frequency (0.16) seems to be reasonable.

The impact of this frequency on the overall BFI core melt frequency estimate is insignificant, since SORV-initiated sequences contribute only 5% to the dominant sequence total and the final frequency estimate has a large error factor.

6.3.4 Use of Generic Control Circuit Unavailabilities

The generic control circuit analysis for valves in Appendix B, Section 5, is based on AC power supplies. The resulting unavailability estimates were also used for DC valve control circuits in the PRA. The effect of this assumption on dominant sequence frequencies was investigated by identifying the main differences between AC and DC valve control circuits and computing generic unavailability estimates for DC circuits. The details of this analysis are reported in Appendix B, Section 5.2. The result is that DC valve control circuit unavailability is 15% less than the corresponding AC unavailability with monthly testing and 19% less with quarterly testing.

Similarly, a generic 4160 V AC motor control circuit was analyzed to assess the difference in unavailability associated with the higher voltage system as opposed to the 480 V AC generic motor control circuit originally used for all motor control circuits in the PRA. This analysis, documented in Appendix B, Section 5.3, shows no change in unavailability for the circuits with monthly testing. The unavailability with quarterly testing was 8.4×10^{-3} for the generic motor control circuit originally analyzed and 7.1×10^{-3} for a 4160 V AC circuit, which represents a drop in unavailability of 15%.

These results show that, for both the generic control circuits analyzed, the differences in power assumptions do not have a significant impact on system unavailabilities.

REFERENCES

1. N. H. Marshall, et al., User's Guide for the Reliability Analysis System (RAS), TREE-1168, EG&G Idaho, September 1977.
2. N. H. Marshall, et al., COMCAN II: A Computer Program for Common Cause Failure Analysis, TREE-1289, EG&G Idaho, September 1978.
3. T. Tyler, M. Linn, H. Jones, and T. Barkalow, private communication (discussions with Browns Ferry IREP team), TVA Nuclear Engineering Branch, Knoxville, TN, March 9 and 10, 1981.
4. Reactor Safety Study--An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014), October 1975.
5. Anticipated Transients without Scram, Vol. 1, NUREG-0460, April 1978, p. 28.
6. A. D. Swain and H. E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, October 1980.
7. Browns Ferry Nuclear Plant Final Safety Analysis Report, NRC Docket 50-259, Tennessee Valley Authority, September 1970, Appendix Q, Question 4.8.
8. B. F. Saffell, Three Station Blackout Sequences at the BF Unit 1 Plant Conducted as Part of the Severe Accident Sequence Analysis (SASA), EG&G letter report to R. E. Tiller, November 1981.
9. S. D. Matthews and J. P. Poloski, MOCARS: A Monte Carlo Code for Determining Distribution and Simulation Limits and Ranking System Components by Importance, TREE-1138, Rev. 1, EG&G Idaho, August 1978.
10. A. S. McClymont and E. W. Poehlman, ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients, EPRI NP-2230, Electric Power Research Institute, January 1982.

1

EG&G Idaho, Inc.
P.O. Box 1625
Idaho Falls, Idaho 83415