NUREG-0666
RG

A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants

Manuscript Completed: March 1981
Date Published: April 1981

P. W. Baranowsky (U. S. Nuclear Regulatory Commission)
A. M. Kolaczkowski (Sandia National Laboratories)
M. A. Fedele (Evaluation Associates, Inc.)

Division of Systems and Reliability Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

ABSTRACT

A probabilistic safety assessment was performed as part of the Nuclear Regulatory Commission's generic safety task A-30, "Adequacy of Safety Related DC Power Supplies." Event and fault tree analysis techniques were used to determine the relative contribution of DC power related accident sequences to the total core damage probability due to shutdown cooling failures. It was found that a potentially large DC power contribution could be substantially reduced by augmenting the minimum design and operational requirements. Recommendations included (1) requiring DC power divisional independence, (2) improved test, maintenance, and surveillance, and (3) requiring core cooling capability be maintained following the loss of one DC power bus and a single failure in another system.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Acknowledgments

The authors wish to acknowledge the contributions of Dr. G. E. Edison (U.S. Nuclear Regulatory Commission) who provided program direction, Mr. F. Rosa (U.S. Nuclear Regulatory Commission) for his review of this report, and Mr. D. W. Stack (Sandia National Laboratories) who performed the computer runs required for the analyses in this program.

1. SUMMARY

A probabilistic safety assessment was performed as part of the Nuclear Regulatory Commission generic safety task designated A-30, "Adequacy of Safety Related DC Power Supplies." This issue stemmed from a concern regarding the dependence of shutdown cooling systems required for decay heat removal on DC power systems which nominally meet the single failure criterion, and the potential for a sudden gross failure of these power supplies resulting in an inability to adequately cool the reactor core. The initial assessment of the safety significance of this issue was reported in NUREG-0305, "Technical Report on DC Power Supplies at Nuclear Power Plants" dated July, 1977. In that report, it was concluded that the failure of DC power supplies represented a small contribution to the probability of a core melt accident; however, performance of a quantitative reliability assessment of the DC power systems was recommended to add confidence to that judgment, and to identify and provide a basis for any changes in licensing criteria that may be deemed necessary. This report represents the completion of the recommended study.

The technical approach used in this study was to perform a bounding type of reliability assessment for DC power supply design requirements at nuclear power plants. This was accomplished by: (1) selecting for evaluation the minimum two division DC power system configuration, one which could be viewed as just meeting minimum requirements such as the single failure criterion; (2) postulating heavy dependence for shutdown cooling on this minimally configured DC power system; and (3) making conservative

interpretations of operating experience (licensee event reports) in the determination of component, system, and human error failure rates which were used in the reliability assessment. It can be stated that, in general, operating plants have DC power system design features and associated test and maintenance procedural requirements that exceed those of the minimum system used in this assessment. Therefore, the reliability of DC power supplies will be correspondingly better at these facilities.

A probabilistic analysis was performed using event and fault tree techniques to determine the relative contribution of DC power related accident sequences to the total core damage probability resulting from shutdown cooling failures. Both a PWR and BWR plant design were analyzed in which the operability of shutdown cooling systems was assumed to be heavily dependent on the minimum DC system. Uncertainties were estimated and propagated through the calculations for all data and probabilities. It was found that the DC power related accident sequences could represent a significant contribution to the total core damage probability for the accident sequences studied. It was also found that this contribution to core damage probability could be substantially reduced by implementation of the design and procedural requirements recommended below.

Based on this work, the following recommendations are made for augmenting the minimum requirements for DC power systems: (1) prohibiting certain design and operational features of the DC power systems, such as use of a bus tie breaker, which could compromise division independence; (2) augmenting the test and maintenance activities presently required for battery operability to also

include preventive maintenance on bus connections, procedures to demonstrate DC power availability from the battery to the bus, and administrative controls to reduce the likelihood of battery damage during testing, maintenance, and charging activities; (3) requiring staggered test and maintenance activities to minimize the potential for human error-related common cause failure associated with these operations; and (4) requiring design and operational features be adequate to maintain reactor core cooling in the hot standby condition following the loss of any one DC power bus and a single independent failure in any other system required for shutdown cooling.

The sensitivity of the results to variations in nuclear power plant design and operational features was analyzed to determine the effect on core damage probability. It was shown that other design features can have a significant effect on shutdown cooling reliability in addition to DC power reliability considerations.

In view of the conservatisms inherent to the approach used in this study, the work reported here generally confirms the earlier assessment reported in NUREG-0305. However, this report provides recommendations, and supporting technical bases, for augmenting the minimum design criteria and procedural requirements which will provide greater assurance of DC power supply reliability.

2. INTRODUCTION

The DC power systems in a nuclear power plant provide control and motive power to valves, instrumentation, emergency diesel generators, and many other components and systems during all phases of plant operation including abnormal shutdowns and accident situations. A reliability assessment of DC power systems required for the operation of shutdown cooling systems has been identified as a generic safety task by the U.S. Nuclear Regulatory Commission (NRC).[1,2] This report provides the results of a reliability based safety evaluation relevant to current DC power system design criteria[3] with particular attention to shutdown cooling requirements. The purpose of this study has been to provide a technical basis to assess the adequacy of DC power supply design requirements for currently operating light water reactors and, if found necessary, to provide recommendations to improve the reliability of these systems.

Background

The adequacy of safety related DC power supplies was questioned by a nuclear consultant in a letter[4] to the Advisory Committee on Reactor Safeguards in April 1977. A specific area of concern was the adequacy of the minimum design requirements for DC power systems, particularly with regard to multiple and common cause failures. This concern related to the application of the single failure criterion for assuring a reliable DC power supply which may be required for the functionability of shutdown cooling systems. In addition, questions were raised regarding the frequency of reported single DC power system division failures including those resulting from human error, and the potential for multiple coincident DC power system failures.

The NRC staff reviewed the adequacy of safety related DC power supplies at operating nuclear power plants.[5] The staff reviewed typical designs, operating experience, and decay heat removal capability with DC power system failure. A preliminary assessment of accident scenario probabilities was made using the results of the Reactor Safety Study (RSS)[6] which indicated that the failure of DC power supplies leading to a loss of shutdown cooling was a small contribution to the core melt probability. However, it was concluded that a more detailed study was required to add confidence to the results and conclusions of the preliminary evaluation.

Accordingly, the adequacy of safety related DC system power supplies was identified as a generic safety task (designated A-30) and a task action plan was developed. This report provides the results of further detailed study in this area, and represents the completion of generic reliability assessments for this task.

Technical Approach

The approach followed in this study involved the use of event and fault tree techniques to perform a reliability based assessment of safety related DC power supplies. The objective was to evaluate DC power supply reliability in the context of its functional importance to reactor safety. In this approach, the most likely accident scenarios involving DC power failures which could result in a loss of shutdown cooling and possible core damage were identified and compared with similar accident sequences involving other safety system failures.

Since there are many variations in the design and usage of DC power supplies at operating nuclear power plants, the approach was tailored to provide an evaluation of the minimum design requirements for DC power supplies. A DC power supply configuration which could be viewed as just meeting the minimum requirements was selected for evaluation. This system consisted of two DC power divisions with one battery and charger per bus. Plant design specific details related to power distribution, layout, and test, maintenance, and operating procedures were kept to a minimum to maintain the generic nature of the analysis. However, these factors were implicitly included through the evaluation of operating experiences related to system and component failures of various DC power systems in operating reactors. Since virtually all operating nuclear power plants contain some operational and design features in excess of the minimum, this approach served to envelope the concern regarding the reliability of DC power supply designs.

DC power system battery capacity requirements and protection from external phenomena such as fires, floods, and earthquakes, were not included in this study.

A failure modes and effects analysis (FMEA) was performed for the minimum DC power system and a review of licensee event reports (LERs) for electrical power system failures was made to identify potential common cause and important independent failure modes. These failure modes were included in a minimum DC power system fault tree model which was used to estimate system unreliability. Failure probabilities were determined for each fault tree event using actual operating experience where possible.

General human factors were used in this evaluation to be consistent with the generic approach, recognizing that they tend to be quite plant and procedure specific.

A probabilistic safety analysis was performed for the shutdown cooling requirements of a pressurized water reactor (PWR) and a boiling water reactor (BWR) assuming heavy dependence on the minimally configured DC power system. DC power availability was assumed necessary to operate systems required to safely cool the reactor core. For convenience, the shutdown cooling system configurations used in the RSS were also used this study. However, heavy dependence on DC power was specifically incorporated in this present study to limit the sensitivity of the results to plant design variations and to bound the importance of DC power supply reliability in the context of reactor safety. In this way, the adequacy of the DC power supply design requirements could be assessed without performing a large number of plant specific evaluations. Event trees were constructed for the PWR and BWR to identify the principal functional interactions and accident sequences important to the shutdown cooling functions of each plant type. A spectrum of accident sequences, which do not include DC power failures but require shutdown cooling systems operation, were included to provide a measure of the relative safety importance of DC power supply reliability.

During this study, consideration was given to the findings and recommendations of the RSS Risk Assessment Review Group report[7] and the subsequent NRC policy statement[8] regarding the use of probabilistic risk assessment techniques for licensing

decisions. Although these considerations have been implicitly incorporated in this study, a section on design sensitivity and analysis uncertainties is provided to give the results added perspective.

3. SYSTEMS DESCRIPTIONS

The systems required for the shutdown cooling functions of the PWR and BWR were selected for convenience from plants used in the RSS. However, the DC power dependencies in these systems were revised by assuming that the systems would fail to operate or perform their intended function if power from the DC buses was unavailable. In addition, the same electrical power system, including a minimally configured DC power system, was used for both plant types for comparative purposes.

The extent to which shutdown cooling systems and related plant functions are dependent on DC power supplies was reviewed for six nuclear power plant designs. A compilation of the typical DC power system dependencies observed is provided in Appendix A. As a result of this review, the shutdown cooling system and electric power system interrelationships shown in Table 1 for the PWR and in Table 2 for the BWR were selected for this study. These DC power dependence assignments are consistent with the intent of the study to perform a limiting design assessment enveloping the minimum DC power supply design requirements. In essence, the DC power supply requirements for shutdown cooling functions are assumed to follow the single failure criterion. The following sections provide descriptions of these systems.

Electrical Power System

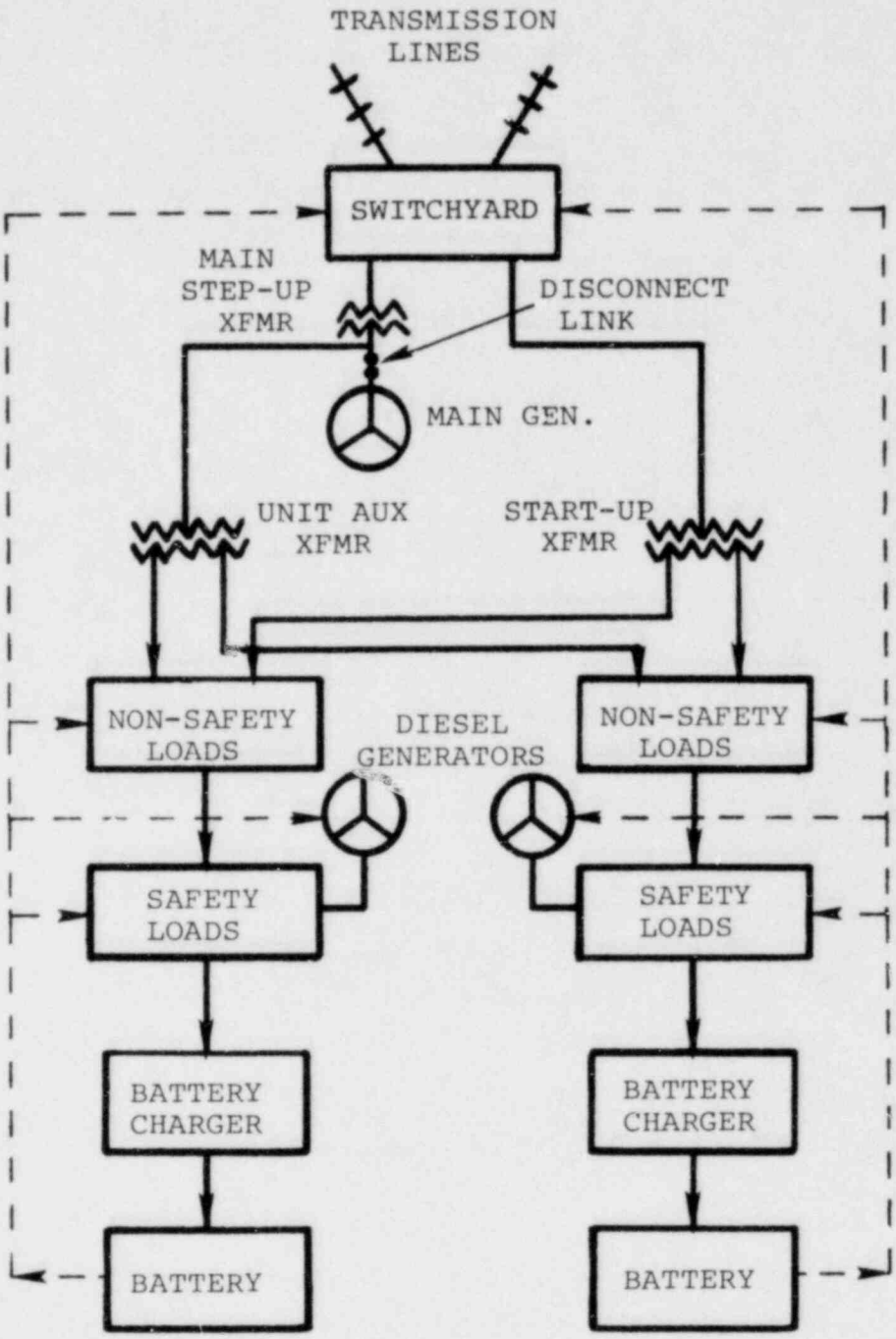
An electrical power system incorporating two safety divisions (the minimum required) was selected for this study. The simplified block diagram, shown in Figure 1, illustrates the

TABLE 1. PWR Electric Power Dependencies

	AC Power			DC Power	
		Emergency			
	Off-site	Div. 1	Div. 2	Div. 1	Div. 2
MFWS					
Condensate Pumps	X				
Emergency Breaker Controls				X	X
AFWS					
Motor Driven Pump Train 1					
Pump Drive & Valve Motive Power	X	X			
Pump Actuation & Control				X	
Motor Driven Pump Train 2					
Pump Drive & Valve Motive Power	X		X		
Pump Actuation & Control					X
Steam Turbine Driven Pump Train					
Pump Actuation & Control				X	
AC Steam Admission Valve	X	X			
DC Steam Admission Valve				X	
RCS Safety/Relief Valves					
Pilot Operated Relief Valve "A"	X	X			
Pilot Operated Relief Valve "B"	X		X		
Block Valve "A"	X	X			
Block Valve "B"	X		X		
HPIS					
Train A (1 Pump)					
Pump Drive & Valve Motive Power	X	X			
Pump Actuation & Control				X	
Train B (2 Pumps)					
Pump Drive & Valve Motive Power	X		X		
Pump Actuation & Control					X
Emergency AC Power System					
Diesel Generator 1					
Actuation & Control				X	
Diesel Generator 2					
Actuation & Control					X
DC Power System					
Battery Charger 1	X	X			
Battery Charger 2	X		X		

TABLE 2. BWR Electric Power Dependencies

	AC Power			DC Power	
		Emergency			
	Off-site	Div. 1	Div. 2	Div. 1	Div. 2
MFWS					
Condensate Pu :	X				
Emergency Breaker Controls				X	X
RCIC					
Pump Actuation & Control				X	
DC Steam Admission Valve				X	
Other System Valves				X	
HPCI					
Pump Actuation & Control					X
DC Steam Admission Valve					X
Other System Valves					X
ADS					
Relief Valve Actuation & Control				X	X
LPCS/LPCI/LPCRS/ESWS/HPSWS					
Train A					
Pump Drive & Valve Motive Power	X	X			
Pump Actuation & Control				X	
Train B					
Pump Drive & Valve Motive Power	X		X		
Pump Actuation & Control					X
Emergency AC Power System					
Diesel Generator 1					
Actuation & Control				X	
Diesel Generator 2					
Actuation & Control					X
DC Power System					
Battery Charger 1	X	X			
Battery Charger 2	X		X		



NOTE: EITHER DIVISION CAN ALONE PROVIDE ALL SAFETY FUNCTIONS

FIGURE 1. TYPICAL TWO DIVISION AC/DC ELECTRICAL DISTRIBUTION SYSTEM

relationship between AC and DC power supplies for this typical nuclear power plant system which meets the single failure criterion. In this design the emergency AC power supplies provided by two diesel generators (the minimum requirement) rely on DC power for excitation and control functions. Thus, DC power is required in order to power the emergency AC power buses if power supplied from the main startup or auxiliary transformers is lost. The bulk AC power supply was considered to be an offsite power source with a reliability dependent on grid availability. The emergency AC power supplies, which are automatically actuated on loss of bulk AC power, were assumed to be as reliable as the start, load, and run reliability of the diesels.

Minimum DC Power System

The DC power system selected for this analysis includes two independent 125 VDC buses with each bus being fed by one battery charger and/or one battery, depending on plant conditions. Each bus supplies the required DC loads via 125 VDC distribution panels and vital 120 VAC loads through inverters. A manually operated bus tie circuit breaker is provided for parallel operation of the chargers and batteries or operation with either battery or charger out of service for maintenance. A simplified schematic of the DC power system is shown in Figure 2.

Each charger supplies power for operation of equipment supplied from its bus section and maintains a floating charge on its associated battery. The two chargers provide an output of 130 VDC with an input of 440 volts, 3Ø, 60 Hz. Each charger is equipped with a DC voltmeter, ammeter, ground detector relay, and an AC

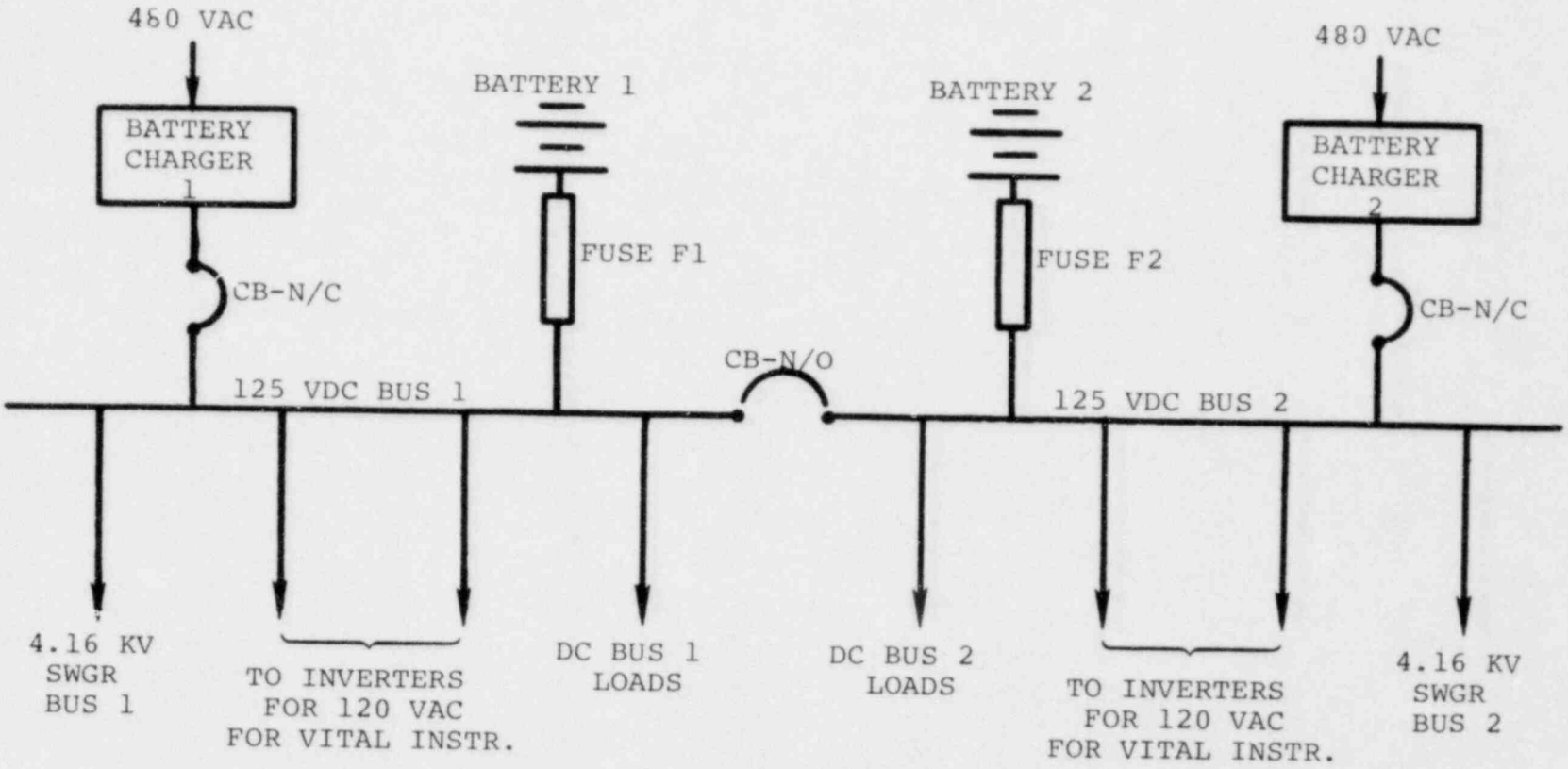


FIGURE 2. SIMPLIFIED SCHEMATIC, MINIMUM DC POWER SYSTEM

supply failure relay with additional indications and alarms in the control room. Each DC bus section is provided with an under-voltage relay which provides an alarm in the control room in the event that a low DC voltage condition occurs.

During normal plant operation, the two DC bus sections are operated independently with the bus tie breaker open. The battery chargers supply all the essential 125 VDC and vital 120 VAC loads. The bus loads include such items as turbine-generator emergency auxiliaries, switchgear, motor operated disconnect switches, annunciators, 125 VDC solenoid valves, vital bus inverters and emergency lighting. In the event that the AC power input to the chargers is lost, the batteries are sized to supply the required DC power for at least two hours under all operating and accident conditions.

Unavailability of a charger or battery, due to maintenance or malfunction, is accommodated by closure of the manually operated bus tie breaker which permits the operable charger to supply the required DC power to both buses while maintaining a floating charge on both batteries.

Surveillance and maintenance of the DC power system is covered by technical specifications. Technical specification surveillance includes weekly battery pilot cell checks, quarterly inspections of all battery cells, battery load tests once per eighteen months (typically during refueling), and periodic battery discharge tests. During the quarterly battery inspections, it was assumed that charger maintenance or adjustments in charger output parameters may need to be performed thus requiring the bus

tie breaker to be closed for approximately two hours per quarter. In addition, it was assumed that the battery would be disconnected from its DC bus to perform test or maintenance procedures one time per year and for no longer than two hours. During these battery tests or maintenance, the DC power system configuration would also include closing of the bus tie breaker to maintain adequate DC power to both buses.

PWR Shutdown Heat Removal

Shutdown cooling for decay heat removal in a PWR can be provided by the power conversion system with main feedwater available, or by the auxiliary feedwater system (AFWS) and elements of the power conversion system which would include steam relief via the secondary system safety/relief valves or if available, the main condenser. Reactor coolant system (RCS) pressure control and water makeup for pressurizer level (inventory) and pressure requirements would be provided by the RCS safety/relief valves and the high pressure injection system (HPIS) during the transients which require shutdown cooling initiation. Descriptions of the PWR shutdown cooling systems used in this study are provided in Appendix B.

Maintaining a hot shutdown condition was assumed to be an adequate and safe mode of decay heat removal for the PWR in this study. A compelling need to achieve a cold shutdown state was not identified, and it was assumed that at some appropriate time following the establishment of hot shutdown, the reactor would be further cooled and depressurized. This operation could be

accomplished slowly after equipment repair or after power systems restoration has been performed following the initiating transient which required a plant shutdown. Moreover, DC power system failures which would negate the ability to achieve a safe hot shutdown condition would also preclude attaining the cold shutdown condition.

BWR Shutdown Heat Removal

Shutdown cooling in the BWR is normally initiated through use of the power conversion system (PCS) with the turbine bypass valves aligned to direct steam to the main condenser. Makeup to the reactor vessel is provided by the feedwater system. In the event that the power converson system becomes isolated or otherwise unavailable, shutdown cooling can be accomplished by the high pressure coolant injection (HPCI) or the reactor core isolation cooling (RCIC) systems. This form of shutdown cooling can be maintained for extended periods if the low pressure coolant recirculation system (LPCRS), a name for the decay heat removal mode of the residual heat removal system (RHRS), is operable and properly aligned. The LPCRS mode of operation also requires use of the emergency service water system (ESWS) for essential component cooling and the high pressure service water system (HPSWS) for removing the decay heat to the ultimate heat sink. The automatic depressurization system (ADS) is used to reduce the reactor pressure to the operating range of the low pressure core spray (LPCS) and low pressure coolant injection (LPCI) systems if they are required; particularly if both the HPCI and RCIC have failed to adequately reduce

the reactor pressure and maintain coolant inventory. Descriptions of the BWR shutdown cooling systems used in this study are provided in Appendix B.

4. EVENT TREES

The initial systems analysis task was the development of the PWR and BWR event trees. This was done in order to identify the various relationships in the accident sequences which would have to be incorporated in the shutdown cooling fault tree models for each plant type. The event trees were constructed to explicitly show the electric power success and failure paths with particular emphasis on the DC power system and subsequent operability of shutdown cooling systems. Accident sequences which do not include DC power failures but incorporate the need for shutdown cooling systems were also included to provide a comparison of the relative safety importance of accident sequences involving DC power failures.

The event trees begin with an initiating event and continue in steps through the various system and functional operations with a success or failure determination made at each event. The event trees are constructed such that, in most cases, subsequent functions are dependent on the success or failure of preceding functions. The end points of the sequences are either a safe shutdown cooling condition or a severe core damage accident. The content and level of detail in the event trees was selected to clearly identify the DC power related accident sequences as well as accident sequences involving only the shutdown cooling systems. In this way, a measure of the contribution of DC power related accident sequences could be made relative to the overall probability of core damage accidents.

Initiating Events

Accident sequence initiators considered in this study were limited to those anticipated occurrences which would result in the loss of the normal power conversion system and thus put a demand on the shutdown cooling systems. These initiators include: (1) hardware and operational failures of the PCS, particularly those which result in a loss of main feedwater (MFW); (2) interruptions in the preferred electrical power supply to the station, as typified by a loss of offsite power; and (3) small LOCAs including those induced by reactor coolant system overpressure transients. Transients induced by (4) a loss of one or more DC power system buses were also included since two or more uninterruptable power supplies would also be lost and a reactor trip would follow. Should this occur, there is a potential for loss of the PCS, and in particular, a MFW trip, which was assumed to follow a DC power bus failure.

Accident sequence initiators of lessor likelihood and those which require reactor coolant inventory makeup and heat removal capability in excess of the normal shutdown cooling systems were not included. The probability of accident scenarios involving low probability initiating events and subsequent DC power failures would not be large enough to represent a major contributor to the overall core damage probability. Table 3 provides a summary of the frequencies for the initiating events considered in this study.

The recovery of the PCS, MFW or offsite power is treated in subsequent events of the tree when loss of one or more of these systems is included in the accident sequence of interest.

TABLE 3. Quantitative Summary of Initiating Events Excluding DC Power Supply Failures

Initiating Event	Approximate Frequency Per Reactor Year	
Reactor Trip	10	
Loss of MFW/PCS	3	
Loss of Offsite Power	0.2	
Overpressure Transients	0.2*	
Small LOCA	$>10^{-3}$	
Large LOCA	$<10^{-4}$	Initiating Events Not Considered In This Study.
Severe Reactivity Transients	10^{-4}-10^{-5}	

*Value is for the PWR. For the BWR, all transients were assumed to result in overpressure of the primary system and thus the need to operate at least one safety/relief valve.

PWR Event Tree

The PWR event tree shown in Figure 3 was developed to include system success states associated with a hot shutdown cooling condition. The PWR event tree headings, the definition of each heading, and the system success criteria for each heading are provided in Table 4.

Accident sequences which involve the initiating events identified in Table 3 require removal of decay heat through one of the secondary heat removal systems and may require reactor coolant inventory (pressure and level) control through the use of pressure relief and high pressure makeup systems. These systems have various dependencies on the AC and DC power supplies which are described in Section 3. Most notable is the heavy dependence of decay heat removal systems and emergency AC power on DC power supplies. Thus, the loss of both DC divisions results in a core damage sequence outcome. Another important dependence is the main feedwater system's requirement for offsite power, without which it cannot perform. The AFWS can perform its function without AC power; however, in this case DC power from division 1 is required for system activation and control for successful operation.

Accident sequences which include a loss of RCS integrity up to approximately the size of a stuck open pilot operated relief valve (PORV) would require reactor coolant makeup by the HPIS and decay heat removal by the AFWS. The high pressure makeup and RCS integrity functions were assumed to be dependent on the availability of secondary heat removal. If AFWS operation was not successfully initiated, the RCS pressure would reach

FIGURE 3 PWR EVENT TREE FOR DC POWER STUDY

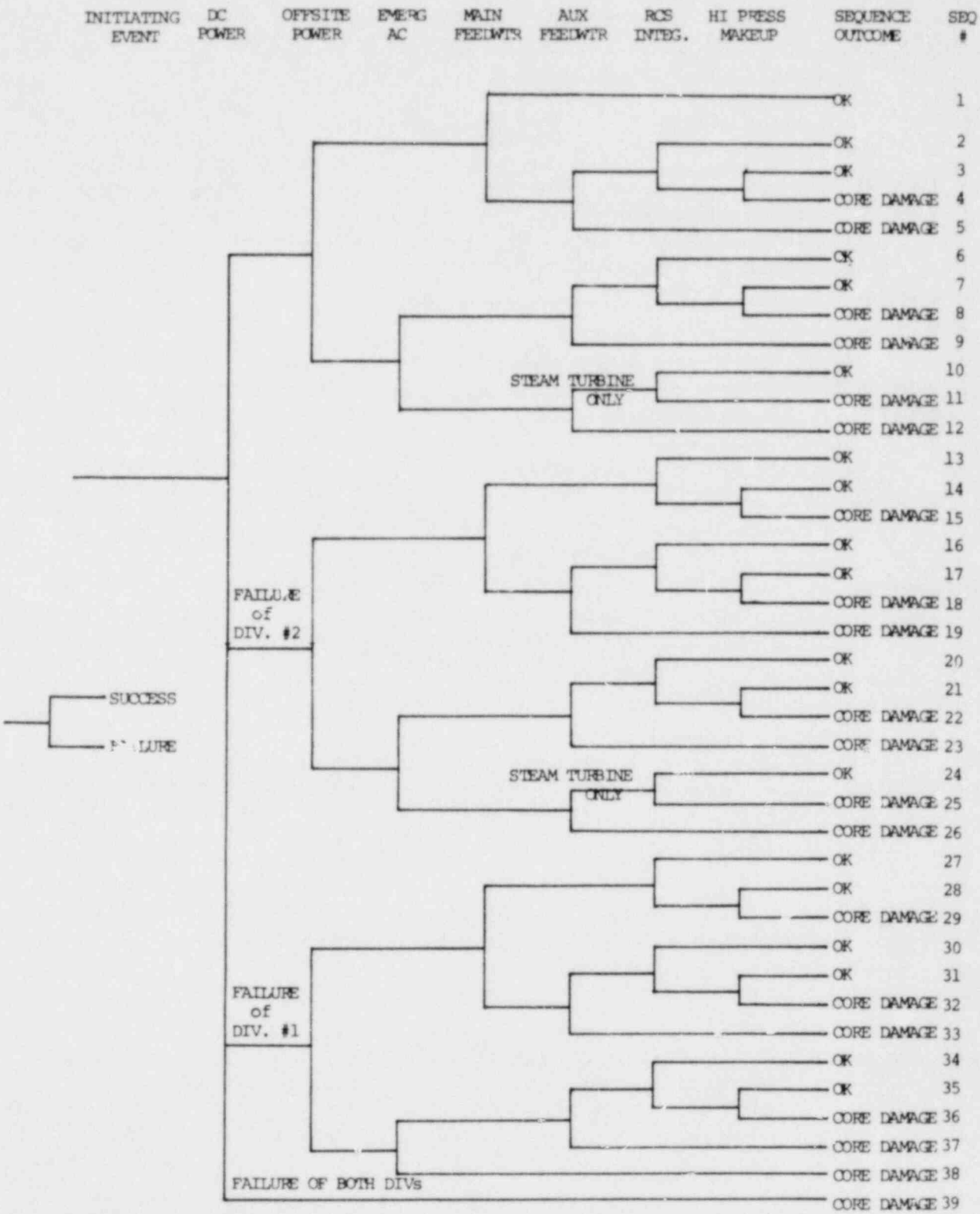


TABLE 4. Description of PWR Event Tree Headings

Heading	Heading Description	Success Criteria
DC Power	Minimum DC power system includes two redundant power supplies (buses) as described in section 3. Provides instrumentation and control (I&C) power to vital systems.	One or both buses continue to supply required DC power to I&C loads required for shutdown cooling system operation. Failure of one or both buses requires unavailability for greater than approximately 1 hour.
Offsite (Preferred) Power	AC power supplied to the station transformers for distribution to normal operating and emergency plant systems.	AC power available from station transformers following an initiating transient. Failure of the offsite (preferred) power supply requires unavailability for greater than approximately 1 hour.
Emergency AC Power	AC power supplied to the emergency buses from the diesel generators when offsite power is unavailable.	Emergency AC power supplied to shutdown cooling systems by at least one emergency diesel generator division upon loss of the offsite power system.
Main Feedwater	The normal main feedwater system and associated controls used to remove reactor heat during power operation.	Main feedwater system continues to supply water to one or more steam generators following reactor trip. Failure requires unavailability of main feedwater supply for approximately 1 hour after reactor trip.
Auxiliary Feedwater System	Secondary heat removal system used to remove reactor decay heat through steam generators when the reactor is shut down and the main feedwater system is not in use. The AFWS is described in Appendix B.	Any one of three pump trains supply adequate heat removal capability through the steam generators for decay heat removal. Failure constitutes unavailability for approximately 1 hour.

TABLE 4. (continued)

Heading	Heading Description	Success Criteria
RCS Integrity	Represents integrity of the RCS pressure boundary.	Maintenance of the RCS pressure boundary precluding a loss of reactor coolant in excess of technical specification limits. Maximum leak size for RCS integrity failure limited to equivalent of one stuck open PORV.
High Pressure Makeup	High pressure coolant injection part of emergency core cooling systems as described in Appendix B.	Any one of three pump trains supplies necessary makeup water to RCS for pressure and inventory requirements for leak sizes up to equivalent of one stuck open PORV.

the safety relief set point which is assumed to exceed the maximum head for successful high pressure coolant injection.

Also, it has been assumed that the loss of AC power or the failure of a single DC division would not result directly in the loss of RCS integrity. That is, the single failure criterion is assumed to have been properly applied for RCS isolation on loss of a DC power division. Since the failure of all DC power is assumed to result in an accident involving core damage (by many potential pathways), the RCS isolation requirements are not further investigated for this event.

BWR Event Tree

The BWR event tree shown in Figure 4 was developed to include system success states for both the hot and cold shutdown cooling conditions. The cold shutdown sequences which involve low pressure cooling systems were included because the BWR can successfully depressurize from high pressure without the need for high pressure makeup and cooling. In addition, the BWR must remove decay heat from the suppression pool using low pressure cooling systems when the PCS is unavailable. Failure to do so within 2 to 27 hours, depending on the accident sequence, could result in suppression pool failure and a loss of makeup cooling water for the reactor core. These considerations are included in the BWR event tree accident sequences. A description of each BWR event tree heading and the system success criteria for each heading are provided in Table 5.

FIGURE 4 BWR EVENT TREE FOR DC POWER STUDY

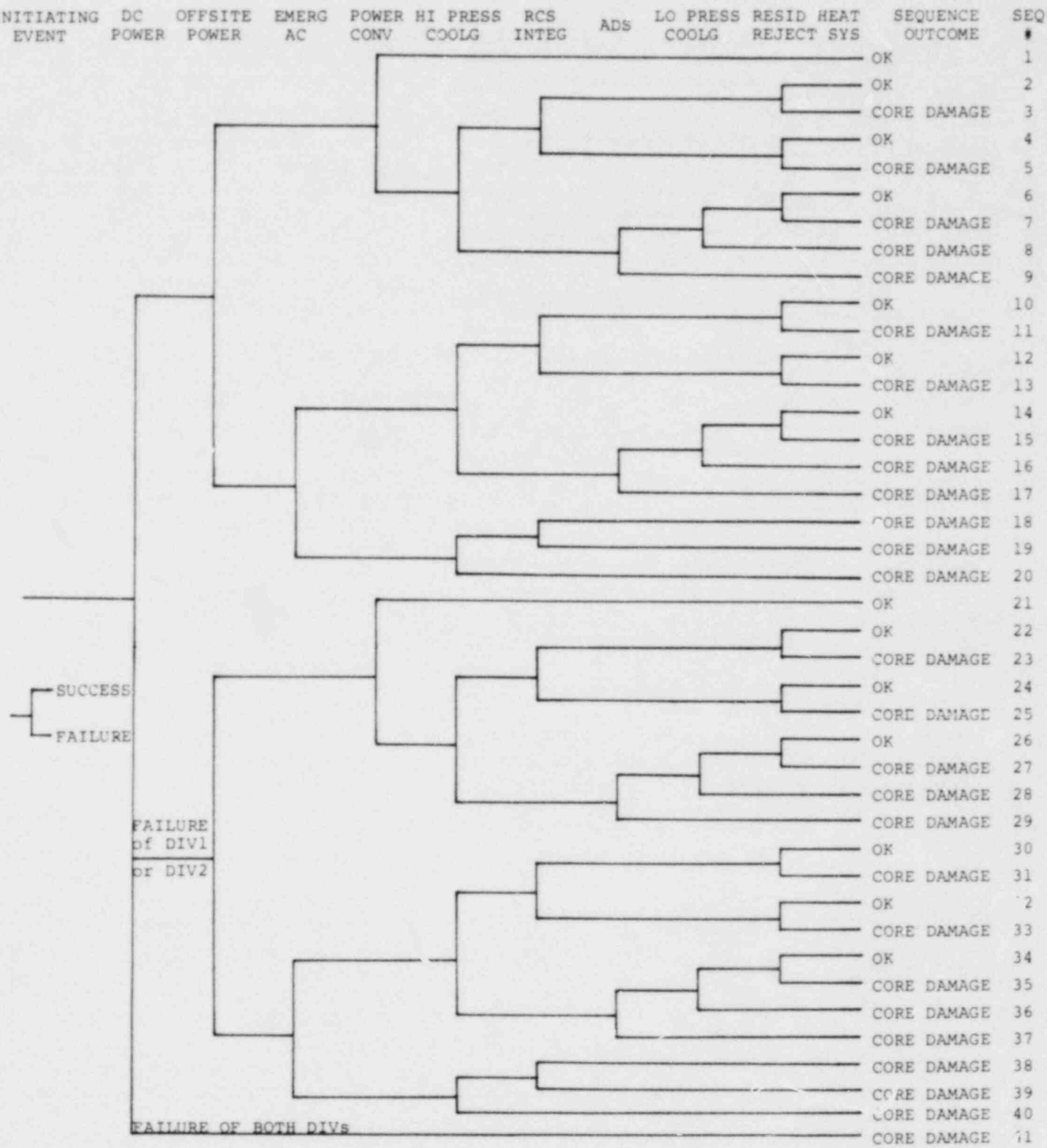


TABLE 5. Description of BWR Event Tree Headings

Heading	Heading Description	Success Criteria
DC Power	Minimum DC power system includes two redundant power supplies (buses) as described in section 3. Provides instrumentation and control (I&C) power to vital systems.	One or both buses continue to supply required DC power to I&C loads required for shutdown cooling system operation. Failure of one or both buses requires unavailability for greater than approximately 1 hour.
Offsite (Preferred) Power	AC power supplied to the station transformers for distribution to normal operating and emergency plant systems.	AC power available from station transformers following an initiating transient. Failure of the offsite (preferred) power supply requires unavailability for greater than approximately 1 hour.
Emergency AC Power	AC power supplied to the emergency buses from the diesel generators when offsite power is unavailable.	Emergency AC power supplied to shutdown cooling systems by at least one emergency diesel generator division upon loss of the offsite power system.
Power Conversion System	The system used to remove reactor heat and generate steam for power production including main feedwater, condensate and main steam systems.	PCS continues to supply main feedwater for reactor vessel inventory requirements and remove decay heat through the main condenser following a reactor trip. Inability of main condenser to remove reactor decay heat for 1-27 hours required for system failure.
High Pressure Cooling	The high pressure coolant injection by HPCI or RCIC systems as described in Appendix B. Maintains reactor vessel water level for decay heat removal when vessel is above ~300 psi.	Either HPCI or RCIC system operates and provides water inventory makeup to the reactor vessel following reactor trip and loss of PCS. Failure requires unavailability for approximately 1 hour.

TABLE 5. (continued)

Heading	Heading Description	Success Criteria
RCS Integrity	Represents integrity of the RCS pressure boundary.	Maintenance of the RCS pressure boundary precluding a loss of reactor coolant at a rate in excess of the technical specification limits. Maximum leak size limited to the equivalent of one stuck open SRV.
ADS	The automatic depressurization system described in Appendix B. Used to depressurize RCS when high pressure cooling is unavailable or low pressure cooling is otherwise required.	If required to rapidly reduce RCS pressure for the initiation of low pressure coolant injection, 4 of 5 ADS valves must open.
Low Pressure Cooling	The LPCI mode of the RHRS and the LPCS as described in Appendix B. Maintains reactor vessel water level for successful shutdown cooling decay heat removal when vessel is depressurized below ~300 psi.	To supply adequate reactor vessel inventory requirements for shutdown cooling 3 of 4 LPCS pumps, or 2 of 4 LPCI pumps, or 2 of 4 LPCS pumps and 1 of 4 LPCI pumps are required. Failure constitutes unavailability of at least one of these system combinations for approximately 1 hour.
Residual Heat Rejection System	The LPCRS mode of the RHRS and the HPSWS and ESWS as described in Appendix B. Removes reactor decay heat to the ultimate heat sink.	Decay heat will be successfully removed from the RCS and/or suppression pool to the ultimate heat sink if at least 1 of 4 trains in each of these three systems operates. Failure requires unavailability of this heat rejection mode for 2-27 hours, depending on the scenario.

Since the BWR provides main steam directly from the primary coolant system to the PCS, for most transients the primary coolant system will be isolated from the PCS and decay heat will be deposited in the suppression pool. This decay heat removal process can be accomplished by high pressure coolant injection and safety relief to the suppression pool or by depressurization, low pressure injection and discharge to the suppression pool. Removal of decay heat from the suppression pool (residual heat rejection) requires the operation of the RHRS and portions of the ESWS and the HPSWS.

There are two important cases to be considered for the loss of suppression pool integrity. The first relates to the potential for severe condensation loads associated with a "ramshead" safety relief valve discharge into the suppression pool at elevated temperatures. This may occur if a safety relief valve (SRV) becomes stuck open or when intermittent opening and closing of the SRV is used to regulate reactor vessel pressure. The discharge of steam into the suppression pool will raise the water temperature and, if heat removal from the pool is not initiated within approximately 2 hours, the regime of severe condensation loads may be reached and a loss of pool integrity may be expected.[9]

If the regime of severe condensation loads can be successfully circumvented, the second challenge to suppression pool integrity will result from overpressure. The failure to initiate suppression pool cooling will result in the eventual rise in the suppression chamber pressure to the point where loss of integrity may occur. In the RSS this condition was estimated to require

approximately 27 hours of decay heat discharge to the pool without residual heat rejection to the ultimate heat sink.

5. MINIMUM DC POWER SYSTEM ANALYSES

The DC power system analyses included a failure modes and effects analysis (FMEA), a review of licensee event reports (LERs) associated with DC power system failures, the construction of a DC power system fault tree, and identification of dominant failure modes and estimates of their probabilities of occurrence. The FMEA and LER review were used in the development of the minimum DC power system fault tree to identify the potentially important independent and common cause system failure modes. Nuclear plant operating experience (LERs) was used wherever possible to develop component failure rates used to quantify the DC power fault tree and determine the dominant system failure causes.

Failure Modes and Effects Analysis

The first part of the minimum DC power system analysis involved a FMEA of the system design. The FMEA included identification of potential DC system component failure modes and their causes, methods of detection, and effects of component failures on the DC system performance. Compensating features inherent in the DC power system design for mitigating a component failure were also identified. The detailed FMEA is provided in Appendix C.

The principal components included in the FMEA were the batteries and chargers. The battery output failures identified included internal failures due to defective cells, low electrolyte, or incorrect charging; and external failures such as inadvertant opening of a battery fuse or breaker, poor cable connections, and loss of ventilation with resultant battery degradation. The battery

chargers are subject to varied internal component failures and malfunctions. A detailed breakdown was not provided in the FMEA. Externally, the chargers need 480 VAC power to operate, the interruption of which will cause a loss of charger output. Other external failure modes for the chargers were similar to those of the batteries.

In addition to these component related failure modes, each bus was analyzed to identify potential single point failures. These included system shorts and operational (human) errors. The bus tie breaker was also considered since this is an obvious source of common cause failure of the DC power system. A bus short to return was the only hardware caused tie breaker related failure mode found to disable both DC power bus outputs.

LER Review

In conjunction with the FMEA, a review was performed of over 1000 LERs related to electric power with emphasis on DC power supplies. This review was done to supplement the FMEA in a quantitative manner and to determine potential system failure modes which may not have been identified in the FMEA. The detailed results of the LER review are also provided in Appendix C.

The LER review covered approximately 332 years of reactor operating experience. The LERs were screened to eliminate nonfailure reports while repetative and common cause types of failure were highlighted.

There were 12 incidents of possible DC bus failures identified in the review of which 5 were immediately correctable. These incidents were primarily due to operational and test and maintenance errors. For instance, operators have failed to remove a parasitic load from the DC power supplies causing loss of a DC bus. In other instances, improper switching or maintenance practices have resulted in the interruption of DC power output from a bus.

Although there were no recorded instances of the coincident loss of multiple DC power buses, several possible precursors to common cause failure were observed. These were classified as two types. The first is operational in nature and was related to the single bus failures which were previously identified. Typically, one additional human error or complication could have resulted in the failure of two buses. For instance, if the bus tie breaker had been closed during an event in which a parasitic load was inadvertently left on one of the DC power buses, both divisions could have been subject to failure.

The second group of common cause failure precursors involved operation of the DC system with batteries in a degraded condition or with cable faults such that the batteries could not provide sufficient power to the buses if the chargers lost power or otherwise failed. Improper charging was found to be an important contributor to battery degradation and premature failure. Unavailability of battery output due to cable and wiring faults, as typified by corrosion or loose connections, was also found to be an important contributor to potential DC bus loss. Additional problems associated with stratification of the electrolyte and possibly unbalanced cell

operation due to imbalances in plate polarization voltages (associated, for example, with different production lots of battery cells), could also be causes of battery degradation and potential DC bus loss. In addition, the LER experience has shown that some conditions of battery degradation or unavailability are not detected and corrected until substantial operating time has accumulated in this condition.

Minimum DC Power System Fault Tree Analysis

Considering the failure modes identified in the FMEA and LER review, a fault tree of the minimum DC power system was constructed and the dominant failure modes were quantified. The fault tree was drawn to show the coincident failure to provide DC power from both buses due to independent and common cause failure mechanisms. The system configuration and failure modes during normal operation and for periods of test and maintenance were included in the fault tree. A simplified DC power system fault tree showing the ways in which system failures could result is provided in Appendix D.

The failure probabilities of the basic and undeveloped events of the DC power system fault tree were estimated from nuclear power plant operating experience where possible. The principal data base was developed from the LER review. A limited number of DC power system component failure rates were obtained from the RSS. Human error related failure rates were obtained from the LERs and a recently published handbook on human reliability.[10] Additional detail on the development of DC power system failure rates is provided in Appendix E.

The basic and undeveloped event probability estimates were used to obtain point estimates for the dominant single and multi-bus failure rates. The statistical median and uncertainty estimates associated with these point estimates are provided in Section 6 and discussed in Appendix E. The dominant single and multi-bus failures generally fell into two categories: (1) failure to provide DC power on demand as characterized by the loss of charger output coincident with the unavailability of DC power from the batteries; and (2) operational, test, or maintenance errors resulting in the loss of DC power during normal plant operation.

The principal cause of failure for the first category involved operation of the DC power system with one or more batteries unable to provide sufficient power to the bus if battery charger output is lost. Battery unavailability in this circumstance was found to be dominated by inadequate maintenance practices and failure to detect battery unavailability due to bus connection faults. The point estimate for the unavailability of batteries was evaluated as:

$P_{\text{single battery}}$ $\sim 1 \times 10^{-3}$/Demand

$P_{\text{two batteries}}$ $\sim 4 \times 10^{-4}$/Demand

It was determined that charger output loss is most likely to follow the momentary loss of the 480 VAC power supply to the chargers when the offsite (preferred) power supply is lost. The frequency of loss of the offsite power supply has been estimated at 0.22 occurrences per year. When combined with the unavailability of sufficient battery output, the estimated single and multiple

(common cause) bus failure probabilities per reactor year were the following:

$P_{\text{single DC bus}}$	$\sim 2 \times 10^{-4}$
$P_{\text{two DC buses}}$	$\sim 9 \times 10^{-5}$

The second category of DC power supply failure included operational, test, and maintenance errors propagating to system failure. In most cases this failure category involved procedural mistakes during periods when the tie breaker would be closed and divisional independence compromised. In this configuration, incidents which would cause the failure of one bus would contribute to the failure of the second bus. The estimates of the probability per reactor year of single and multiple division failure due to this second category of events are the following:

$P_{\text{single DC bus}}$	$\sim 6 \times 10^{-3}$
$P_{\text{two DC buses}}$	$\sim 6 \times 10^{-5}$

Minimum DC Power System Improvement Analysis

A limited assessment of potential reliability improvements to the minimum DC power system was performed. Since the failure of the DC power system was dominated by two types of common cause failures, reliability improvement features were evaluated in terms of capability for reducing the probability of these failure modes so that power necessary for shutdown cooling functions would be available. Several areas were identified where improvements to the minimum system (analyzed in this study) might be beneficial.

The features analyzed are, for the most part, representative of variations in DC power system design and operation for the current generation of nuclear power plants. A description of these items is provided below.

1. Addition of another DC power train

This modification would upgrade the minimum DC power system design by the addition of a separate, independent, and diverse DC power train or division. This division could be used for specific functions such as: (a) switch yard operations; (b) emergency diesel generator actuation, control, and alignment; or (c) shutdown cooling actuation and control. Diversity could be provided by such parameters as voltage and capacity requirements, component supplier or design concept, procedures for maintenance and testing, or other operational characteristics. It was assumed that the common cause failure coupling between the original two train system and this additional DC train would be negligible for this concept.

2. Use AC uninterruptable power (converted DC power) for actuation and control functions

Various instrumentation and reactor protection features use AC power which has been converted from DC power in the form of an uninterruptable AC power supply. This concept would involve the use of an uninterruptable power supply for actuation and control of the shutdown cooling systems which is separate from the 120 VAC vital instrument buses. It would require AC power availability for shutdown cooling functions from the preferred power supply during normal operation and from the AC power supply from DC inverters when the

preferred power source is interrupted. For those components which must have a direct current power source to function, the AC power could be rectified to supply a DC power source. Inverter and power supply switching reliability limit the usefulness of this concept.

3. Eliminating use of the bus tie breaker

Use of the DC bus tie breaker could be eliminated or restricted to conditions of cold shutdown or refueling. Elimination of the tie breaker would represent another step toward complete division independence. Malfunctions affecting one DC division could not be propagated to affect the second DC division through DC system interactions. Maintenance and testing requirements during plant power conditions could be affected. However, there are hardware and procedural remedies available and currently in practice. These would include scheduling certain battery and battery charger test and maintenance activities during periods of reactor shutdown. A third battery charger which could be connected to either bus may also be required.

4. Addition of a standby battery charger independent of station power

This addition to the minimum DC power system could be implemented by providing a battery charger powered by an internal combustion engine. Sizing, procedures, and bus connection requirements would be sufficient to provide DC power to one bus with a failed (or otherwise unavailable) battery and charger. Operator actions would most likely be required to align this unit for use.

5. Enhanced battery failure surveillance

An improvement in the surveillance reliability from that observed in this study should be possible. Through improved training, procedures, and possibly additional or improved tests, the onset of battery deterioration could be identified at a sufficiently early stage that preventive maintenance would reduce the frequency of battery failures. Daily or weekly surveillance could be upgraded to detect the majority of deteriorated battery conditions currently found through quarterly or refueling period tests.

6. Improved maintenance procedures

Study of the human reliability factors contributing to the operational reliability of the DC power system indicates that there is a potential for improvement. Such improvements could be achieved through training and consideration of human reliability factors in the development and implementation of maintenance procedures and administrative controls. For instance, specific written procedures with a checklist could replace or supplement verbal instructions. Staggering of test and maintenance activities with alternating crews is another possibility.

Other improvements to the minimum DC power system are certainly possible. However, it was not the intent of this study to perform a comprehensive assessment of all possible DC power system supply reliability improvements.

An analysis was performed to evaluate the potential reduction in the minimum DC power system failure probability for the improvements discussed above. In this analysis, the unreliabilities of

the DC power system improvements were estimated from the values obtained in this study for similar subsystems, components, and procedures. These estimates were used to determine the effectiveness of each improvement in reducing the probability of the dominant DC power system failure modes. In the minimum DC power system analysis there were two types of failures identified which dominated the system unreliability. These are: 1) Common cause failure of batteries to provide sufficient power to buses given a loss of power to the chargers, and 2) operational, test or maintenance errors causing loss of both DC divisions with the bus tie breaker closed. The likelihood of either type of failure was found to be approximately equal. Therefore, the improvement analysis was performed for these two types of failures assuming each contributed 50% to the minimum DC power system unreliability.

The results of the minimum DC power system reliability improvements analysis are provided in Table 6. The estimated unreliabilities of the DC power system improvements are shown along with the calculated reduction in DC power system failure probability. The effectiveness of each improvement in reducing the probability of the two dominant failure modes is also shown, since some improvements are more effective in reducing the likelihood of one or the other type of failure. In Table 6, the minimum DC power system failure probabilities have been normalized to unity for the convenience of showing a relative improvement in unreliability. The results show that a reduction in the minimum DC power system unreliability of at least one order of magnitude should be achievable.

Table 6. Approximate Comparison of Reliability Improvements to the Minimum DC Power System

DC Power System Features for Potential Improvement	Assumed Unreliability on Demand	Relative Reduction in Minimum System Unreliability		
		Type 1 Failures	Type 2 Failures	Both Failure Modes
0. Minimum System	--	1.0	1.0	1.0
1. Add another DC power train				
a. switch yard	10^{-2}-10^{-3}	>0.5	1.0	>0.75
b. emergency diesel gen.	10^{-2}-10^{-3}	0.01	1.0	0.5
c. shutdown cooling	10^{-2}-10^{-3}	0.01	0.01	0.01
2. Use of AC uninterruptable power for actuation/control	$\sim 10^{-2}$	1.0	0.01	0.5
3. Eliminate bus tie breaker	$\sim 10^{-3}$	1.0	0.001	0.5
4. Add standby battery charger	10^{-1}-10^{-2}	0.03	1.0	0.5
5. Improved surveillance	10^{-1}-10^{-2}	0.03	1.0	0.5
6. Improved maintenance and testing	$\sim 10^{-1}$	0.1	0.1	0.1
Combinations of Features				
1a and 2				0.25
1a and 3				0.25
1b and 2				0.01
1b and 3				<0.01
2 and 4				0.02
2 and 5				0.02
3 and 4				0.02
3, 5, and [illegible]				0.02

6. ACCIDENT SEQUENCE ASSESSMENT

The accident sequence assessment involved the quantification and characterization of the accident sequences of the PWR and BWR event trees. The more likely accident scenarios involving DC power failures were identified and compared with similar accident sequences involving other safety system failures. This task involved the development of fault tree models incorporating a logic structure which would include all of the accident sequences of the event trees.

Shutdown Cooling Fault Trees

A shutdown cooling fault tree model was constructed for each plant type incorporating the accident sequences and associated systems of the event trees. The undesired "top event" was defined as "loss of shutdown cooling leads to core damage." The models were developed such that the relative contribution of DC power system failures to shutdown cooling unreliability could be seen explicitly. The PWR and BWR shutdown cooling fault trees are provided in Appendix D.

The top logic for the PWR and BWR fault trees is identical. The RSS and more recent studies[11] have indicated that a loss of cooling for greater than 1 hour could result in severe core damage and possible melting of the core. Thus, the top logic was developed to show loss of the normal PCS followed by loss of shutdown cooling capability. Also included in the top logic was consideration of the accident initiator to reflect the conditional failure probabilities of the various shutdown cooling modes.

System sub-trees were developed for compatibility with the appropriate initiating events and with the interdependencies previously provided in Tables 1 and 2. The basic modeling for each shutdown cooling system sub-tree was derived from the RSS. However, the RSS fault trees were condensed except for those areas involving electric power dependence in which case faults leading to system failure were explicitly included.

AC power system sub-trees were also developed using simplified models based on insights obtained from the RSS and included explicit DC power dependencies where applicable. The offsite or preferred power supply was treated as a grid reliability estimate and recovery probability. The emergency AC power supplies were modeled as two divisions with a reliability equivalent to that of the emergency diesel generators. Common cause failure of the emergency AC power supplies was included in addition to DC power related and independent component failure modes.

The data used to quantify the probabilities of the basic and undeveloped events of the PWR and BWR shutdown cooling fault trees were obtained for the most part from the RSS. These failure rate estimates are provided in Appendix E.

Accident Sequence Probabilities

The development of the accident sequence probabilities for the PWR and BWR involved the quantification of the ways that loss of shutdown cooling and resulting core damage could occur. The results of this quantification were used to obtain the accident sequence probabilities of the event trees. This evaluation was performed to determine the contribution of the minimum DC power

system unreliability to the failure of shutdown cooling and potential core damage.

Using the basic and undeveloped event input data provided in Appendix E, the PWR and BWR fault trees coupled with the DC power fault tree were "solved" using two computer codes. First the Boolean algebra expressions for the two shutdown cooling trees were obtained using the "SETS" computer code[12] leading to mathematical expressions for the minimal cut sets for the accident sequences that lead to the top event of each tree. Each minimal cut set describes a sequence of events necessary for the top event (core damage) to occur. These expressions and the event probabilities were used as input to the "SEP" computer code[13] to obtain the minimal cut set probabilities using the rare event approximation. Each sequence of the event trees was then quantified by combining the probabilities of similar minimal cut sets which together define a sequence of events depicted on the event trees. During this combination, event median probabilities and their uncertainties were propagated through each cut set using Monte Carlo simulation. At this stage of the quantification process, adjustments for conditional probabilities (i.e., the probability of one event given another has occurred) are made depending on each event tree sequence.

The results of the accident sequence quantification are provided in Table 7 for the PWR and in Table 8 for the BWR. The dominant accident sequences which make up approximately 98% of the total probability are shown. The median estimates of the dominant accident sequence probabilities per reactor year are

Table 7

PWR Accident Sequence Probabilities

Seq. No.	Initiator - Subsequent Events	Probability/RY
39	DC Power Failure (operational common mode)	1.1×10^{-4} (30)
	LOP - DC Power Failure (battery common mode)	9.3×10^{-5} (30)
4*	MFWS - RCS Integ. - Hi Press Makeup	6.9×10^{-5} (12)
8	LOP - RCS Integ. - Hi Press Makeup	1.5×10^{-5} (20)
12	LOP - Emerg. AC - AFWS	1.5×10^{-5} (12)
33	DC1 - MFWS - AFWS	1.3×10^{-5} (20)
5	MFWS - AFWS	1.0×10^{-5} (20)
9	LOP - AFWS	6.4×10^{-6} (10)
38	LOP - DC1 - Emerg. AC	6.1×10^{-6} (9)
11	LOP - Emerg. AC - RCS Integ.	5.3×10^{-6} (32)
37	LOP - DC1 - AFWS	2.8×10^{-6} (8)
18	DC2 - MFWS - RCS Integ. - Hi Press Makeup	1.4×10^{-6} (37)
32	DC1 - MFWS - RCS Integ. - Hi Press Makeup	2.0×10^{-7} (32)
19	DC2 - MFWS - AFWS	1.5×10^{-7} (20)

All other sequences ~ $<10^{-7}$ Total ~ 3.6×10^{-4}

*Includes sequences initiated by small LOCA

Table 8

BWR Accident Sequence Probabilities

Seq. No.	Initiator - Subsequent Events	Probability/RY
41	DC Power Failure (operational common mode)	1.1×10^{-4} (30)
	LOP - DC Power Failure (battery common mode)	9.3×10^{-5} (30)
5	PCS - RCS Integ. - RHRS	8.6×10^{-5} (12)
19	LOP - Emerg. AC - RCS Integ.	5.3×10^{-5} (32)
18	LOP - Emerg. AC	6.8×10^{-6} (12)
3	PCS - RHRS	4.0×10^{-6} (12)
9	PCS - Hi Press. Cool'g - ADS (Lo Press. Cool'g)	3.0×10^{-6} (5)
13	LOP - RCS Integ. - RHRS	3.0×10^{-6} (12)
11	LOP - RHRS	2.2×10^{-6} (6)
40	LOP - DCI - Emerg. AC - Hi Press. Cool'g	8.1×10^{-7} (7)
39	LOP - DCI - Emerg. AC - RCS Integ.	8.1×10^{-7} (24)
20	LOP - Emerg. AC - Hi Press. Cool'g	8.0×10^{-7} (8)
17	LOP - Hi Press. Cool'g - ADS (Lo Press. Cool'g)	8.0×10^{-7} (5)
25	DCI - PCS - RCS Integ. - RHRS	4.0×10^{-7} (12)

All other sequences $\sim < 10^{-7}$ Total $\sim 3.7 \times 10^{-4}$

Note: Probabilities for sequences with DCI are the sum for sequences with DC1 or DC2 failed.

given. The corresponding uncertainty factor for each estimate is also shown in parenthesis for each accident sequence. These uncertainty factors were obtained through the Monte Carlo simulation used to quantify the accident sequence probabilities. The uncertainty factors represent the 95th and 5th percentiles of the Monte Carlo simulation. The upper bound on each sequence probability in the tables is obtained by multiplying the median estimate by its corresponding uncertainty factor. The lower bound is obtained by dividing each median estimate by the uncertainty factor.

The total probability per reactor year of accident sequences leading to a loss of shutdown cooling and possible core damage is slightly less than 4×10^{-4} for each plant design studied.

Description of Dominant Accident Sequences

A description of the accident sequences which were found to dominate the shutdown cooling failure and core damage probability are provided below.

PWR-39 and BWR-41 Loss of all DC power.

There are two principal DC power failure categories for this sequence. The first is due to operational error when the DC power system buses are tied together (bus tie breaker closed). Multiple human errors and cascading failure of the DC power supplies typify this case. The second type of DC power failure is initiated by a loss of the offsite (preferred) AC power supply. This is followed by coincident failure of both batteries which results in the loss of all DC power. There are several possible scenarios which could follow a DC power system failure of either category and result in

a core damage accident. The accident would be characterized by a reactor trip, loss of the normal power conversion system (which may occur first if offsite power is lost), and the inability to initiate shutdown cooling automatically or by remote manual means. The loss of all DC power would result in a loss of vital instrumentation in the control room ("flying blind") which would complicate any opportunity for corrective actions by the operator. Undesirable fluid or electrical system alignments would not be automatically corrected. In approximately one hour, sufficient reactor coolant will have boiled off due to decay heat rejection to uncover the reactor core.

PWR-4, 8, 11, 18, 32 Small LOCA and loss of HPI.

These accident sequences are characterized by a small LOCA and failure to provide high pressure coolant makeup. The small LOCA can be transient induced by a loss of load or loss of offsite power, or it may be the initiating event with subsequent loss or isolation of the normal power conversion system. The auxiliary feedwater system will be successfully started and removing decay heat. However, failure of the HPIS to make up reactor coolant inventory will result in uncovering of the core and eventual core melting. HPIS failure can result from combinations of hardware failure, test and maintenance outages, AC and DC power failures, and operator error.

PWR-5, 9, 12, 19, 33, 37, 38 Loss of normal and auxiliary secondary heat removal.

These accident sequences involve the failure to remove decay heat through either the normal (main feedwater) or emergency (auxiliary feedwater) secondary heat removal systems. Loss of the normal secondary heat removal systems can result from operational errors and hardware failures, a loss of offsite power, or by the loss of a DC power bus. The restoration of main feedwater for secondary heat removal is dependent on the initiating event.

Failure of the AFWS following loss of the MFWS will deprive the reactor coolant system of heat removal capability through the steam generators. After the steam generators have boiled dry, the primary coolant system will heat up until the pressure rises to the relief valve set point. Pressure relief will control the saturation temperature of the primary coolant while decay heat continues to boil primary coolant. Within 1/2 hour after steam generator dryout, the core will be uncovered and core melting will follow.

BWR-5, 13, 19, 25, 39 Transient induced LOCA and failure to reject decay heat to the ultimate heat sink.

This set of accident sequences is initiated by loss of the power conversion system from operational errors or hardware failures, a loss of offsite power, or by the loss of a DC power bus. The RCS isolation and pressure surge which follow such an event causes one or more safety relief valves to open. One valve fails

to reseat and an uncontrolled discharge to the suppression pool begins. In these scenarios the suppression pool cooling mode of RHRS is unavailable. The discharge of steam through the stuck open SRV will heat the suppression pool to the unstable condensation temperature in approximately two hours. SRV condensation loads are assumed to breach suppression pool integrity. The subsequent loss of suppression pool water inventory will deprive the operating reactor coolant injection systems of makeup water and in approximately one hour the boil off of RCS inventory due to decay heat generation will uncover the core.

BWR-3, 11, 18 Reactor shutdown and failure to reject decay heat to the ultimate heat sink.

In this set of accident sequences, the reactor is tripped by loss of the power conversion system. The PCS loss would be due to major operational errors, hardware failures, or extended offsite power outages. The reactor is successfully depressurized and decay heat is removed from the reactor vessel to the suppression pool. The systems required to remove the decay heat from the suppression pool are unavailable due to hardware or emergency AC power failures. The inability to remove reactor decay heat from the suppression pool results in the gradual buildup of temperature and pressure in the suppression chamber. In approximately 27 hours, the suppression pool fails due to overpressure and the RCS makeup water inventory is lost. Failure to provide RCS makeup will then result in uncovering the reactor core through decay heat boil off of the primary coolant.

BWR-20, 40 Loss of AC power and failure of steam driven high pressure makeup.

These accident sequences involve the loss of offsite power resulting in the interruption of the main feedwater supply to the reactor vessel. The subsequent failure of standby emergency AC power supplies results in the total loss of AC power. High pressure makeup systems, which are independent of AC power for actuation, control, and pump motive power, are also unavailable or fail (independently) in this sequence. This results in the boil off of reactor coolant inventory without any makeup capability. In approximately one hour, the core will be uncovered and core melting may follow. Emergency AC power and high pressure makeup systems unavailability would be due to combinations of hardware failure, test and maintenance outages, and DC power bus failures.

BWR-9, 17 Reactor shutdown and loss of reactor core cooling.

This set of accident sequences is initiated by the loss of the power conversion system from operational errors, hardware failures, or a loss of offsite power. In these sequences the RCIC and HPCI systems are unavailable or fail independently and ADS actuation is unsuccessful due to operator error or hardware failures. Without ADS the low pressure cooling systems cannot be initiated. In approximately one hour, reactor coolant boil off will result in uncovering the core.

7. ANALYSIS OF RESULTS

The most likely accident scenarios involving failure of the minimum DC power system which could result in a loss of shutdown cooling and possible core damage have been identified and compared with similar accident sequences involving other safety system failures. These results establish an envelope on the reliability of DC power supplies and provide some perspective on the importance of DC power reliability to reactor safety. However, the results should be considered in light of their sensitivity to differences in design and operational features of nuclear power plants and the uncertainties inherent in the study. These aspects are discussed below.

Sensitivity of Results

Since the intent of this study was to perform a generic evaluation, it is desirable to provide insights about the sensitivity of the results to certain potentially important design or operational features in which differences exist between the study plants and many operating nuclear power plants. Several sensitivity items in addition to DC power supply reliability were selected for evaluation. This selection was made after considering the system design and operational characteristics of the study plants with the potential to increase or decrease the estimated core damage probability. An attempt was not made to identify all such factors, but rather to evaluate a spectrum of potentially significant features which could affect the total core damage probability and relative significance of DC power supply reliability.

The sensitivity analysis was performed in much the same manner as the DC power system improvements analysis. An unreliability was estimated for each sensitivity item and accident sequences containing these items were requantified to determine the potential increase or decrease in the total core damage probability. Tables 9 and 10 provide listings of the sensitivity items considered, the associated sensitivity value used in the analysis, the dominant accident sequences affected, and the net change in the total core damage probability estimate. The value of the sensitivity parameters used in the analysis reflects known reliability variations or an approximate bound on the reliability change. Only accident sequences which were estimated to contribute on the order of one percent or more to the total core damage probability are shown.

In the case of the DC power system, the unreliability estimates used in the sensitivity analysis were selected from the improvements analyses discussed in Section 5. Two cases were analyzed to demonstrate the effect of improvements in the DC power supply reliability. The first involved the addition of a third DC power division or combinations of dedicated DC power supplies and the use of uninterruptable AC power sources. These features provided approximately two orders of magnitude reduction in the unreliability of DC power supplies used for shutdown cooling. These features substantially reduce the DC power failure contribution to the probability of a severe core damage accident. The second case included elimination of the bus tie breaker to improve divisional independence and enhanced surveillance, test, and

Table 9. Results of PWR Sensitivity Evaluation

Sensitivity Factor	Approximate Unreliability This Study	Approximate Unreliability Sensitivity Value	Affected Accident Sequences	Change in Core Damage Probability
DC Power System Reliability -With improvements 3,5, & 6 (see Table 6)	2×10^{-4}	10^{-6} 4×10^{-6}	39 39	-55% -54%
Interaction with One DC Power Division Loss --Loss of RCS Integrity/ Isolation --MFW Loss/Recovery	2×10^{-3} 10^{-1}	1.0 1.0	18,32 19,33	+220% +34%
AFWS Reliability -AC Power Available -AC Power Unavailable	3×10^{-5} 10^{-2}	10^{-3} 10^{-3},10^{-1}	5,9,19,33,37 12	+174% -4%,+38%
Emergency AC Power Reliability	5×10^{-3}	5×10^{-4},10^{-2}	11,12,38	-7%,+7%
RCS Integrity/Isolation on Loss of AC Power	10^{-2}	1.0	11	+146%
MFW Recovery with Loss of AFWS	10^{-1}	1.0	5	+25%
"Feed and Bleed" Capability	1.0	10^{-2}	5,9,33,37	-9%
Time to Core Damage (LOP Recovery Factor)	0.4	0.2,0.6	9,11,12,37,38	-5%,+5%

Table 10. Results of BWR Sensitivity Evaluation

Sensitivity Factor	Approximate Unreliabiliy This Study	Sensitivity Value	Affected Accident Sequences	Change in Core Damage Probability
DC Power System Reliability with improvements 3, 5, & 6 (see Table 6)	2×10^{-4}	10^{-6} 4×10^{-6}	41 41	-54% -53%
Interaction with One DC Power Division Loss				
-Loss of RCS Integ./Isolation	10^{-1}	1.0	25,39	+3%
-PCS Loss/Recovery	10^{-1}	1.0	28,29	~ +1%
Shutdown Cooling Systems				
-RHRS with AC Power	2×10^{-4}	2×10^{-5},10^{-3}	3,5,11,13	-23%,+102%
-Hi Press. Cooling without AC Power	2×10^{-3}	10^{-1}	20,40	+22%
Emerg. AC Powe Reliability	5×10^{-3}	5×10^{-4},10^{-2}	18,19,20,39,40	-14%,+17%
RCS Integrity/Isolation on Loss of AC Power	10^{-1}	1.0	19,39	+131%
PCS Recovery with Loss of RHRS	7×10^{-3}	0.1	3	+14%
SRV Discharge Device	1.0	ϵ	5,13,19,25,39	-38%
Time to Core Damage (LOP Recovery Factor)	0.4	0.2,0.6	13,17,19, 20,39,40	-8%,+8%

maintenance features. For this case, the contribution of DC power unreliability to the core damage probability was also substantially reduced.

Analyses were also performed to determine the sensitivity of the results to assumptions regarding interactive or dependent failures in shutdown cooling systems following the loss of a single DC power supply or bus. For this case, it was assumed that the loss of one DC power bus would initiate a plant transient and also cause a substantial loss of shutdown cooling capability such that a second independent failure could result in a core damage accident. Interactions with a DC power bus loss or dependent failures could involve decay heat removal and support systems operability, RCS integrity or isolation capability, RCS makeup systems availability, and operational factors including procedural interactions, instrumentation, and control functions.

Two cases involving a DC power bus failure and interaction with shutdown cooling capability were analyzed. These included PCS or MFWS unavailability and the loss of RCS integrity following a single DC power supply loss. Since the PCS and MFWS are non-safety systems, a single failure, such as the loss of a DC power supply, could render these systems unavailable. This could be due to unbalanced dependence on one of the DC power divisions for certain balance of plant ("non-safety") functions. These functions could include circuit breaker alignments for offsite and onsite AC power sources, secondary system control logics, and various support systems. RCS integrity loss could also result from a single DC power supply loss, although proper application of the single failure criterion

should limit this possibility. For this case, DC bus faults might cause RCS isolation valves to fail open or render open valves unable to close. The inadvertent isolation or deactivation of certain RCS support systems could also result in the loss of RCS integrity. A loss of pump seal water injection and subsequent seal failure is one example.

The upper bound sensitivity for these interactions was analyzed and the PWR design was found to be highly sensitive to these interactions. The insensitivity of the BWR design to these interactions stems from the fact that several core cooling modes are available in the BWR design while only one is available in the PWR design. Although not analyzed, it is certainly possible that a lesser core cooling capability for different BWR designs could also have a high sensitivity for a single DC power supply loss.

A recent study[14] showed that a large variation existed in the reliability of AFWS designs in currently operating PWRs with and without AC power available. The approximate unreliability range identified was used in the two PWR sensitivity cases for that system. For comparative purposes, approximately the same reliability range was evaluated for the RHR systems of the BWR which require AC power. The results show the potentially significant influence that shutdown heat removal design variations could have on the probability of a severe core damage accident beyond considerations of DC power unreliability. The assessment of shutdown cooling in the BWR with one of the high pressure cooling systems unavailable on loss of AC power is also provided for comparison with the PWR shutdown cooling design. In this circumstance

the BWR would have only one AC independent cooling system compared to the one AFWS subsystem in the PWR which can also operate independent of AC power.

Both the PWR and the BWR results show a large sensitivity to the inability to isolate the RCS on loss of AC or combinations of AC and DC power. In the sequences affected, the RCS makeup systems are unavailable due to power loss or failed for other reasons. The RCS integrity loss is assumed to be large enough to result in uncovering the core within approximately one hour.

The unavailability of emergency AC power has also been analyzed as part of the sensitivity evaluation. The emergency AC power supply configuration and diesel generator unavailability estimates used in this study are about average for operating nuclear power plants. Sensitivity factors were selected to reasonably cover the potential variation in the emergency AC power unavailability. For this case a more substantial sensitivity would be obtained if shutdown cooling capability and reliability without AC power available were less than that of the systems used in this study.

The sensitivity to MFW recovery for the PWR and PCS recovery for the BWR was analyzed for accident sequences initiated by the loss of these systems. The short term restoration of these systems was assumed to be dominated by the operator's ability to recognize the need to attempt a MFW or PCS restart and diagnose any correctable impediments to that restart. Longer term outages of these systems would be dominated by the more severe hardware failure problems. The nonrecovery of MFW or PCS is shown to be more important for the PWR, again due to the availability of several BWR shutdown cooling modes.

The nonrecovery of MFW in PWR designs could be offset, at least in part, by the capability to make up and relieve reactor coolant at operating pressure with sufficient flow to remove decay heat. This "feed and bleed" capability could decrease the core damage probability for those accident sequences ending with failure of the AFWS, if emergency AC power is available.

The "ramshead" discharge device was assumed to be included in the BWR design analyzed in this study. As discussed in Section 4, the discharge of steam through a "ramshead" discharge device may result in severe condensation loads on the suppression pool under certain conditions of water temperature and discharge flow rate. In the sensitivity analysis it was assumed that the "quencher" discharge device is used which would not promote failure threshold suppression pool loading for the conditions associated with the dominant BWR accident sequences. Suppression pool integrity challenges related to long term PCS and suppression pool cooling failures would still be possible.

Another item which can affect the core damage probability estimate is the time available to restore shutdown cooling prior to uncovering the core. The variation in time is on the order of 1/2 to 1-1/2 hours, and is dependent on the nuclear steam supply system design to a major extent. Balance of plant design will also have some influence on the minimum recovery time available.

Uncertainty in Results

The identification of the dominant PWR and BWR accident sequences considered in this study has been primarily based on a relative comparison of the median core damage probability estimates.

However, uncertainty factors were included in the analysis to provide additional perspective in assessing the significance of the results. Figures 5 and 6 show the comparison of the dominant accident sequence probabilities as uncertainty estimates. The assignment of DC power system failure rate uncertainties is discussed in Appendix E. Accident sequences which do not involve DC power failures reflect the uncertainty estimates developed for the shutdown cooling systems in the RSS.

The uncertainty "bounds" for the accident sequences involving the loss of all DC power cover approximately three orders of magnitude. This amount of uncertainty reflects the generic nature of this study in which a minimum of design and operational specifics were used to describe the DC power system. These uncertainty bounds should not be strictly interpreted as 90% confidence intervals, although there is high confidence that the expected accident sequence probability lies within the identified range. The "best estimate" of the accident sequence probability is identified by the median probability. However, in some cases, this median estimate may tend to be conservatively high.

The uncertainty bounds should not be interpreted to include design and operational features significantly different from the study plants. Some of these have been analyzed in the preceeding discussion. On the other hand, some generality is included through the use of industry average failure data and consideration of accident or system failure precursors identified in the LER operating experiences. This is particularly true for the estimate of the coincident common cause failure of the DC power supplies.

FIGURE 5. PWR ACCIDENT SEQUENCE UNCERTAINTY RANGES

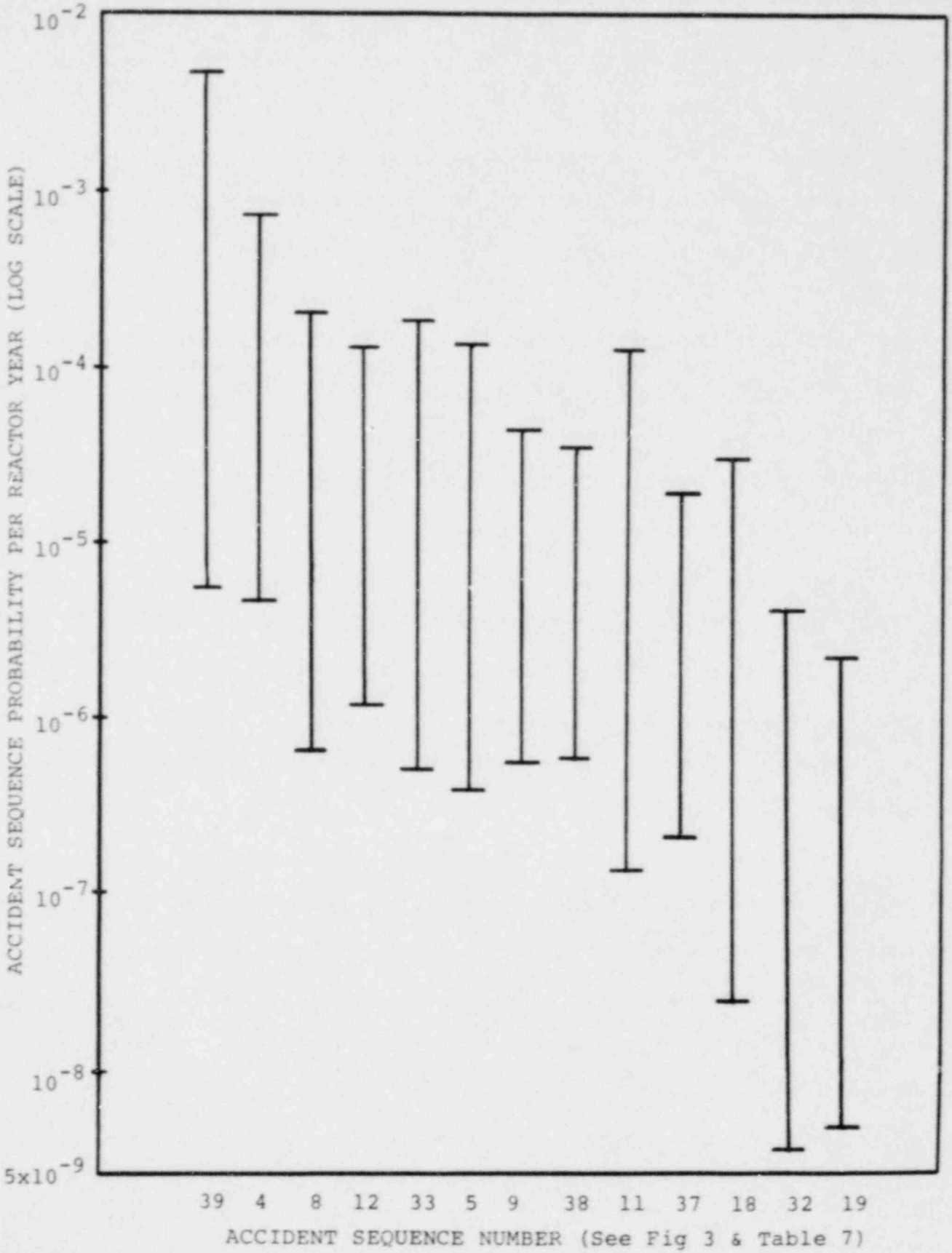
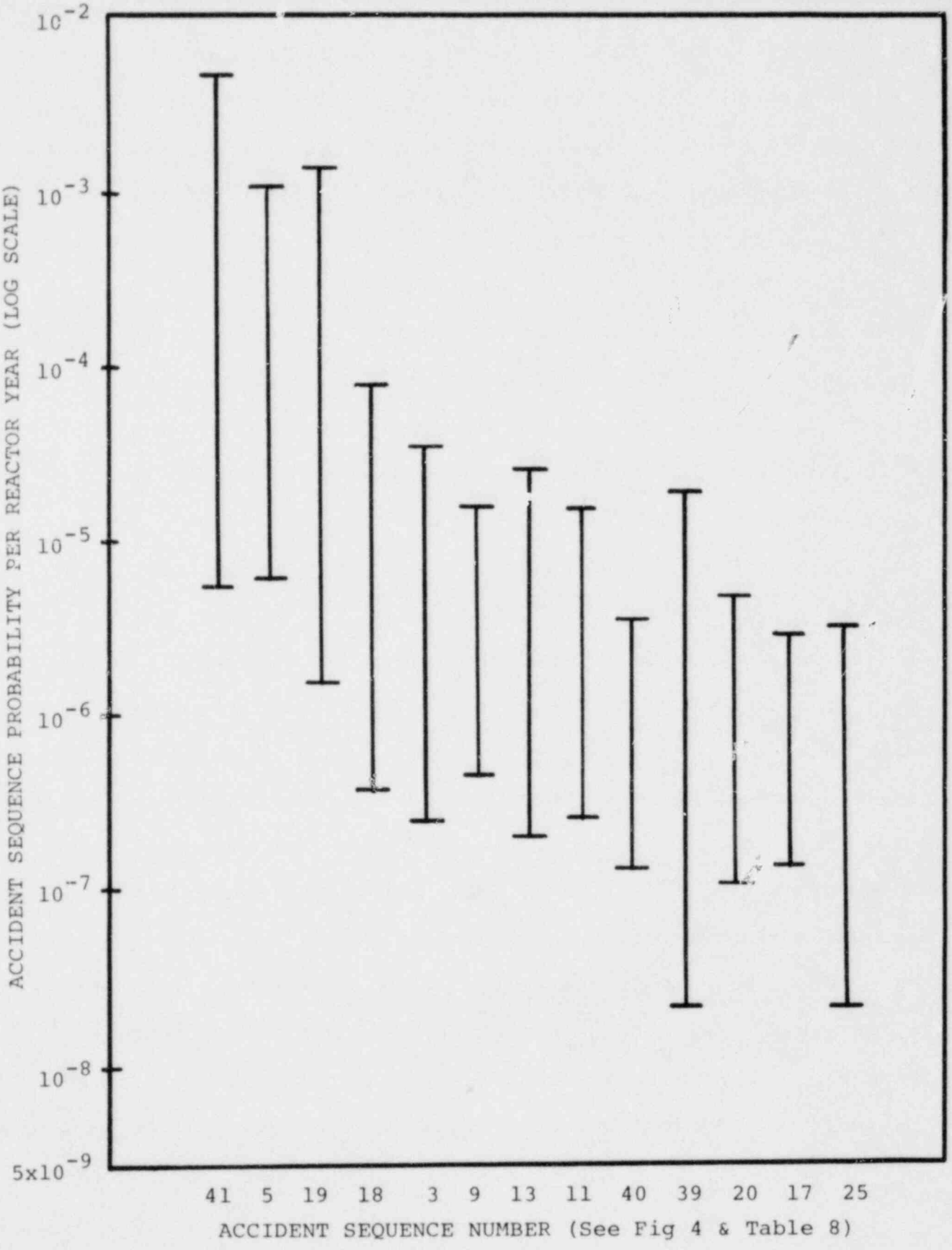


FIGURE 6. BWR ACCIDENT SEQUENCE UNCERTAINTY RANGES



There was a minimal amount of relevant data available from which certain key DC power supply failure rates could be estimated. This was particularly true for the common cause failure estimates. In general, probabilistic estimates developed from a small data base have relatively large statistical uncertainties. Considering the small population of failures in the data base, a simple sensitivity analysis was performed on the DC power supply failure rate uncertainty estimates. All DC power failure rate uncertainty bounds were increased by a factor of three and the accident sequences were requantified. The relative contribution of the minimum DC power system was not changed significantly and the uncertainty in the DC power accident sequences was increased by less than a factor of three. Therefore, the relative results of this work are not extremely sensitive to the uncertainty ranges developed for the DC power system analyses.

Information obtained from LERs represents a potentially significant source of uncertainty, particularly when used to estimate median failure probabilities. The quality of data extracted from LERs is deficient in many cases with regard to completeness, accuracy, and detail. The lack of completeness, due to the failure to report events, would tend to result in the under prediction of some failure rates while the inaccuracies and minimal detail could increase or reduce estimates through data misinterpretation. This is particularly true for the battery and common cause median failure probability estimates. The LER review conducted to identify battery failure experience was somewhat hampered by the lack of specificity of those reports and the stringent requirements of Technical Specifications

which includes the reporting of "failures" to meet the minimum operational requirements. For instance, the actual battery capability upon being "declared inoperable" or having identified "bad cells" or "bad connections" cannot easily be determined from the information provided in the LER. The battery may or may not be able to provide the minimum power necessary to allow the operation of shutdown cooling systems or actuate emergency AC power supplies. On the other hand these conditions do represent precursors or warnings to the potential unavailability of batteries when needed and therefore cannot be ignored. A similar uncertainty is inherent in the DC power failure rate estimates of an operational or procedural nature.

The absence of design specificity used in this study is another source of uncertainty, especially for the estimate of procedural errors resulting in DC power unavailability. For the most part, generalized human factors were used which cover a broad range of design configurations or layouts assuming limited procedural or administrative controls. Since all operating experiences identified in this study were assumed to be applicable to the minimum DC power system analyzed, this lack of specificity is considered to represent a potential conservatism in both the median and uncertainty upper bound probability estimates.

8. OBSERVATIONS AND RECOMMENDATIONS

A probabilistic safety analysis has been performed to assess the adequacy of DC power supply design requirements for nuclear power plants. The contribution of DC power unreliability to the loss of shutdown cooling capability and the probability of core damage was determined. The approach used included analyses which conservatively enveloped the differences in design and usage of DC power supplies at nuclear power plants. This was done by analyzing a DC power design which just meets the minimum requirements and by conservatively interpreting operating experience data used in the reliability analysis. In addition, the operability of shutdown cooling systems was assumed to be heavily dependent on the availability of the minimum DC power system. The sensitivity of the results to design variations was also determined and uncertainties were estimated for all major component failure rates and dominant accident sequences.

The results of this work showed that failure of the minimum DC power system could represent a significant contribution to the unreliability of shutdown cooling. It was also shown that this contribution could be substantially reduced through the use of various design and operational improvements to the minimum DC power system. Since operating nuclear power plants include some DC power supply features which exceed the minimum analyzed, DC power reliability will be correspondingly improved at these facilities. The sensitivity analyses showed that the probability of a core damage accident can be significantly affected by the reliance placed on any one DC power supply for shutdown cooling

functions. It was also shown through the sensitivity analyses that differences in design and operational features other than DC power can have a potentially large influence on the unreliability of shutdown cooling and the probability of a core damage accident.

The observations and recommendations derived from this study with regard to the design and operational characteristics important to DC power supply reliability are discussed below.

Observations

The failure of the minimum DC power system was dominated by two types of common cause failure. These included: (1) operational, test, and maintenance errors which result in the deenergizing or cascading failure of the DC power supplies; and (2) bus failure following a loss of offsite power (preferred AC power supply) to the chargers when batteries are in a deteriorated condition or otherwise unable to meet load requirements. In the first case, it was human procedural error and the compromise of system independence (tie breaker closed) which contributed most to the system failure rate estimate. The second case involved the limitation of surveillance techniques and unsatisfactory maintenance practices regarding proper battery condition and availability of power to the buses.

The design and operational characteristics which stand out in importance regarding DC power supply reliability include system maintenance and administrative controls, surveillance and monitoring effectiveness, and divisional independence. These items which can be interdependent are discussed below.

Improper maintenance was attributed as the cause of the highest probability DC power failures identified in this study. These failures may be due to poor administrative controls, flaws in procedures, inattentiveness during maintenance operations, or other reasons which are dependent on plant specific operations. When coupled with regular use of the bus tie breaker, these factors were found to be an important part of the potential for DC power system failure.

The effectiveness of DC power supply surveillance and monitoring was found to be important in this study, particularly with regard to the common mode failure of battery supplied power to the buses. Based on the LER review, evidence exists that undetected battery degradation and bus connection faults can occur between the quarterly maintenance and inspection periods and that this condition may not be detected until the quarterly surveillance is performed. Evidence also exists that the quarterly inspections may not uncover all degraded battery conditions. If weekly monitoring was highly effective in identifying the onset of conditions resulting in battery power supply unavailability, which apparently require the more thorough quarterly or refueling period tests for highly reliable detection, the unavailability could be reduced by an order of magnitude from that estimated in this study.

It has been shown that the maintenance and surveillance limitations to DC power reliability, and their effect on shutdown cooling, can be circumvented, at least in part, by DC power supply design or functional diversity. Independence from the main station DC power supply may be obtained by providing a separate and somewhat

diverse DC power supply for vital functions. Or, a portion of these vital functions may be supplied by an uninterruptable AC power supply. The loss of shutdown cooling probability due to DC power failure could be reduced by as much as two orders of magnitude using these design features.

Sensitivity analyses have shown the potential increase or decrease in the estimated core damage probability for several design features which are different from the plant designs analyzed in this study. It was shown that transients initiated by the loss of one DC power bus and involving causal failure in other systems required for successful shutdown cooling may be important contributors to the probability of a core damage accident for certain plant designs. This is particularly evident if following a single DC power bus loss an additional independent failure in the shutdown cooling systems would result in the loss of adequate core cooling capability. Potentially important DC power dependent failures could involve decay heat removal and support systems, RCS integrity and isolation, RCS makeup systems, and operational factors including procedures, instrumentation, and control functions.

It was also shown in the sensitivity analyses that certain design and operational features other than DC power can greatly affect shutdown cooling reliability.

Recommendations

The licensing requirements for the minimum DC power system can and should be improved. Several recommendations have been developed considering the functions of the minimum DC power system, the dependence of shutdown cooling on DC power supplies, and the accident

scenarios of the PWR and BWR event trees. These recommendations are outlined below.

1. Assure that design and operational features of the DC power supplies used for shutdown cooling do not compromise division independence. This includes eliminating use of a bus tie breaker, if provided, and revising test and maintenance activities with the potential for human error causing more than one DC division to be unavailable. Specific administrative controls and procedures should be provided where the human factor is involved.

2. Assure that test and maintenance activities required for battery operability also include preventive maintenance on bus connections, procedures to demonstrate DC power availability from the battery to the bus, and administrative controls to reduce the likelihood of battery damage during testing, maintenance, and charging.

3. Stagger test and maintenance activities and crews to the extent practicable. This should include weekly pilot cell observations, preventive maintenance on batteries and bus connections, battery discharge and load tests, battery charger maintenance, and off line battery charging.

4. Assure that plant design and operational features are such that following the loss of one DC power supply or bus: (a) redundant capability is maintained for providing shutdown cooling in the hot standby condition; (b) RCS integrity and isolation capability are maintained; and (c) operating procedures, instrumentation, and control functions are adequate

to initiate and maintain shutdown cooling in the hot standby condition. In essence, reactor core cooling capability should be maintained following the loss of any one DC power supply or bus and a single independent failure in any other system required for shutdown cooling.

References

1. U. S. Nuclear Regulatory Commission, "Technical Report on DC Power Supplies in Nuclear Power Plants," NRC Report NUREG-0305, NTIS, 1977.*

2. U. S. Nuclear Regulatory Commission Report to Congress, "NRC Program for the Resolution of Generic Issues Related to Nuclear Power Plants," NRC Report NUREG-0410, January 1978.*

3. U. S. Nuclear Regulatory Commission, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," NUREG-75/087, Section 8.3.2, September 1975.*

4. Letter from E. P. Epler to J. C. Ebersole and D. Okrent, Advisory Committee on Reactor Safeguards, "DC Power Supply Reliability," April 12, 1977.

5. U. S. Nuclear Regulatory Commission memorandum from W. R. Butler to R. L. Tedesco and D. G. Eisenhut, "Survey of DC Power Supplies at Operating Plants," August 18, 1977.

6. U. S. Nuclear Regulatory Commission, "Reactor Safety Study," NRC Report WASH-1400, NTIS, October 1975.**

7. H. W. Lewis, et al, "Risk Assessment Review Group Report to the U. S. Nuclear Regulatory Commission," NUREG/CR-0400, September 1978.*

8. U. S. Nuclear Regulatory Commission Press Release, "Nuclear Regulatory Commission Issues Policy Statement on Reactor Safety Study and Review by Lewis Panel," January 19, 1979.

9. U. S. Nuclear Regulatory Commission memorandum from D. G. Eisenhut to R. M. Bernero, "BWR Suppression Pool Temperature Response," April 11, 1980.

10. A. D. Swain and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, Albuquerque, NM, September 1980 (draft).**

11. U. S. Nuclear Regulatory Commission memorandum from Z. Rosztoczy to R. Bernero, "Revised Estimates of Core Uncovery Times for Loss of AC and DC Power," March 12, 1980.

12. R. B. Worrell and D. W. Stack, "A SETS Users Manual for the Fault Tree Analyst," SAND77-2051, Sandia Laboratories, Albuquerque, NM, November 1978.

13. SEP Computer Code, Sandia Laboratories, Albuquerque, NM (in the process of being published).

14. M. A. Taylor, et al, "An Assessment of Auxiliary Feedwater Systems," American Nuclear Society Transactions of 1979 Winter Meeting, Vol. 33, pp. 569-570, November 1979.

*Available for purchase from the National Technical Information Service, Springfield, VA 22161.

**Available free upon written request to the Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Appendix A

DC Power Dependencies in Representative Nuclear Power Plants

This appendix contains a summary of DC power dependencies in representative nuclear power plants. Table A-1 summarizes DC dependencies for four PWRs and Table A-2 summarizes DC dependencies for two BWRs. The shutdown cooling system and electric power system interrelationships shown in Tables 1 and 2 of this report were selected on the basis of the material in this appendix.

TABLE A1. PWR DC POWER SYSTEM DEPENDENCIES - Sheet 1 of 2

DESCRIPTION	PLANT			
	SURRY	CALVERT CLIFFS	SEQUOYAH	OCONEE
DC SYSTEM CONFIGURATION	Two 125 VDC Trains • one Battery/Train-1A & 1B • Two chargers/Train (redundant) • One Bus/Train • Bus Tie Breaker	Two 125 VDC Trains • One Battery/Train-11 & 12 • Two chargers/Train(redundant) • One Bus/Train	Emergency DC System Four 125 VDC Trains (Shared by Units one and two) • One Battery/Train-I, II, III & IV • One charger/Battery - spare charger/Two Battery • One Bus/Train Emergency AC System DCPS One 125 VDC Train/Diesel Generator (Two DG/unit)- Trains A, B • One Battery/Train • One charger/Battery	Emergency DC System Two 125 VDC Trains • One charger/Train- 1CA & 1CB • One charger/Battery - one spare charger • One Bus/Train • Bus Tie Breaker Switching Station DC System Two 125 VDC Trains • One Battery/Train-SY-1 & SY-2 • One charger/Battery - one spare charger • One Bus/Train • Bus Tie Breaker Emergency AC System DCPS (Keowee) Two 125 VDC Trains • One Battery/Train- 1 & 2 • One charger/Train - one spare charger • One Bus/Train • Bus Tie Sreaker
D. C. DEPENDENCIES				
EMERGENCY A.C. SYSTEM	Diesel Generator Startup, Control & Transfer to ESF (4160V) Buses • Train A-DG1 & 4160V C.B. • Train B-DG3 (swing) & 4160V C.B.	Diesel Generator Startup, Control & Transfer to ESF(4160V) Buses • Train 11-DG-11 & 4160V C.B. • Train 12-DG-12 & 4160V C.B.	Diesel Generator startup and control • Emergency AC DCPS Train A- D.G. 1 A-A • Emergency AC DCPS Train B - D.G. 1B-B Diesel Generator Transfer to ESF Buses (6.9KV) • 125 VDC Train I - D.G.1A-A • 125 VDC Train II - D.G.1B-B	Keowee startup, control & Transfer to ESF (4160V) Buses • Train 1CA - Keowee 1 • Train 1CB - Keowee 2 Keowee Station switching • 125 VDC Train 1-13.8KV (Keowee 1) underground feeder • 125 VDC Train 2-230KV (Keowee 2) overhead line
AUXILIARY FEEDWATER SYSTEM (AFWS)	125 VDC Train A-Electric pump P3-A controls 125 VDC Train B-Electric pump P3-B controls 125 VDC Trains A & B-Turbine pump P-2 controls 125 VDC Trains A & B-Power relief valves	125 VDC Train 11 • Turbine Pump 11 controls • Dump valve #1 • Turbine Bypass Valves (2) 125 VDC Train 12 • Turbine pump 12 controls • Dump Valve #2 • Turbine Bypass Valves (2)	125 VDC Train I • Aux Feed pump outlet pressure control valve; PCV-3-122 • Electric pump steam Generator Level Control Valves; LVC-3-156 & -164 • Turbine driven pump steam generator Level Control Valves LCV-3-171 & -172 • Electric pump 1A-A Controls • Turbine Driven pump 1A-S controls 125 VDC Train II • Aux Feed pump outlet pressure control Valve; PCV-3-132 • Electric pump steam generator Level Control Valves; LCV-3-148 & 171	125 VDC Train 1CA • Turbine Bypass Valve • Turbine Driven pump controls • Feedwater Injection Valve; FDW-36 • Aux Feed Injection Valve; FDW-38 125 VDC Train 1CB • Turbine Bypass Valve • Turbine Driven Pump Controls • Feedwater Injection Valve; FDW-45 • Aux Feed Injection Valve; FDW-47

TABLE A1. PWR DC POWER SYSTEM DEPENDENCIES - Sheet 2 of 2

DESCRIPTION	PLANT			
	SURRY	CALVERT CLIFFS	SEQUOYAH	OCONEE
AUXILIARY FEEDWATER SYSTEM (AFWS) (continued)			• Turbine Driven Pump Steam Generator Level Control Valves LCV-3-173 & -174 • Electric Pump 1B-B controls • Turbine Driven pump 1A-S controls	
PRESSURIZER	125 VDC Trains A & B - Power Spray Valves (2/unit)	125 VDC Train 11 - Power Relief Valve; 1-ERV 402 125 VDC Train 12 - Power Relief Valve: 1-ERV 404	125 VDC Train I - Pressurizer Heater; 1D (Control Group) 125 VDC Train II - Pressurizer Heater; 1A-A (Backup Group)	125 VDC Trains 1CA & 1CB - Electromagnetic Relief Valve
CHEMICAL & VOLUME CONTROL SYSTEM (CVCS)	125 VDC Trains A & B • Charging pump (3) controls • Boric Acid Transfer pump (4) controls • Volume Control Tank Divert. valve	125 VDC Trains 11 & 12 • Charging pump (3) controls • Boric Acid Transfer pump (2) controls • Solenoid control valves for divert. Valve and other air operated valves	125 VDC Trains I & II • Charging pump (3) controls • Boric Acid transfer pump (3) controls (pumps shared by units 1 & 2) • Solenoid control valves for divert. valve and other air operated valves	125 VDC Trains 1CA & 1CB • Charging pump (3) controls • Charging pump suction and discharge MOV Controls • HPCI Divert Valve • BWST Supply MOV Controls

TABLE A2. BWR DC POWER SYSTEM DEPENDENCIES - Sheet 1 of 2

DESCRIPTION	PLANT	
	PEACH BOTTOM	GRAND GULF
DC SYSTEM CONFIGURATION	Four 125 VDC Trains • One Battery/Train • One charger/Battery • Four 125 VDC Buses-ZA, ZB, ZC & ZD Two 250 VDC Trains • Two 125V Batteries Connected to give 250 VDC • Two 250 VDC Buses	Three 125 VDC Trains • One Battery/Train • Two chargers/Battery (Redundant) • Three 125 VDC Buses - 11DA, 11DB, 11DC -11DC Bus Dedicated to HPCS
DC DEPENDENCIES EMERGENCY A.C. SYSTEM	Diesel Generator Startup, Control & Transfer to ESF (4160V) Buses • 125 VDC Train ZA-D.G.0A12 & 4160V CB • 125 VDC Train ZB-D.G.0B12 & 4160V CB • 125 VDC Train ZC-D.G.0C12 & 4160V CB • 125 VDC Train ZD-D.G.0D12 & 4160V CB 250 VDC Trains 20D11 & 20D12 • HPCI Pumps & Shutdown cooling valves • RCICS Pumps & shutdown Cooling valves	Diesel Generator Startup, Control & Transfer to ESF (4160V) Buses • 125 VDC Train 11DA-D.G.11 & 4160V CB • 125 VDC Train 11DB-D.G.12 & 4160V CB • 125 VDC Train 11DC-D.G.13(HPCS) & 4160V CB
LOW PRESSURE COOLANT INJECTION SYSTEM (LPCIS)	125 VDC Trains ZA, ZB, ZC & ZD • Control Power for pump A,B,C&D • Control power for injection MOV's 154A, B and 25A, B • LPIS Logic channels A & B 250 VDC Train 2 - Head spray MOV 33	125 VDC Trains 11DA & 11DB • Control power for RHR supp. pump A-11DA • Control power for RHR supp. pumps B, C-11DB • Control power for pump suction and injection valves • LPCIS Initiation Logic
HIGH PRESSURE CORE SPRAY	125 VDC Trains ZB & ZD • HPCS Initiation Logic • Control Power For: - Turbine Isolation MOV's - Condensate pump suction MOV - Suppression Pool pump suction MOV's (2) - Pump discharge MOV's (2) to F.W. Line A - Pump discharge test line MOV's (3) - Min Flow Line MOV 250 VDC Train 20D11-operating power for above MOV's	125 VDC Train 11DC • Control Power for HPCS pump and pump suction and injection valves • HPCS Initiation Logic
REACTOR CORE ISOLATION COOLING SYSTEM (RCICS)	125 VDC Trains ZA & ZC • RCICS Initiation Logic • Control Power For: - Turbine Isolation MOV (outboard) - Steam supply MOV - Condensate Pump Suction MOV - Suppression pool pump suction MOV's (2) - pump discharge MOV's (2) to FW Line B - pump discharge test line MOV's (3) - Min flow line MOV 250 VDC Train 20D12 - Operating power for above MOV's.	125 VDC Train 11 DA • Control & Operating power for: - Turbine Isolation MOV - CSI Suction MOV - Suppression pool suction MOV - RCICS Injection MOV - Turbine Exhaust Isolation MOV - Inboard Isolation MOV - Outboard Isolation MOV - RCICS Initiation Logic
AUTOMATIC DEPRESSURIZATION SYSTEM (ADS)	125 VDC Trains ZA & ZB (Redundant) • ADS Initiation Logic • Control & Operating power for ADS valves	125 VDC Trains 11DA & 11DB (Redundant) • ADS initiation Logic • Control and Operating power for ADS valves

TABLE A2. BWR DC POWER SYSTEM DEPENDENCIES - Sheet 2 of 2

DESCRIPTION	PLANT	
	PEACH BOTTOM	GRAND GULF
LOW PRESSURE CORE SPRAY (LPCS)	———	125 VDC Train 11DA • Control Power For: - Suppression Pool Suction MOV - LPCS pump - Pump discharge MOV - LPCS Initiation Logic
STANDBY SERVICE WATER SYSTEM (SSW)	———	125 VDC Train 11DA, 11DB & 11DC • Loops A, B and C Control Power For: - SSW Loop Initiation Logic - SSW Loop pumps & MOV's

Appendix B

Shutdown Cooling Systems Descriptions

This appendix contains abbreviated system descriptions of the alternate shutdown cooling systems modeled in this study. Systems for both the PWR and the BWR are discussed in this appendix. Simplified schematics, brief descriptions, functional purpose, power requirements, and other system dependencies (where appropriate) compose the system descriptions which follow.

These system designs, which were incorporated into the event trees and fault trees in this study, are derived primarily from the PWR and BWR designs in the RSS. However, some modifications were made to the electrical power requirements of some sub-systems to accommodate the simple two bus AC/DC power system used in this study. These changes were also made to maximize the dependencies of shutdown cooling systems on DC power.

Auxiliary Feedwater System (AFWS)

The AFWS design used in this analysis consists of two electrical motor-driven pump trains and one steam turbine-driven pump train with the associated piping, valves, and controls. The system delivers water from a storage supply to the secondary side of the steam generators Heat is transferred from the reactor coolant system to the power conversion system via the steam generators and ultimately discharged to the atmosphere or, if available to the main condenser. Adequate heat removal can be achieved by delivery of feedwater from either of the electric motor-driven pumps or the steam turbine-driven pump. A simplified schematic of the AFWS is shown in Figure B-1.

During normal plant operation, the pumps are in standby and the flow control valves between the discharge of the pumps and the steam generators are closed. The electric motor-driven pumps and the steam turbine pump start automatically and deliver the required flow within one minute following a loss of offsite power, loss of main feedwater, receipt of a safety injection signal, or steam generator low-low water level. All pumps may also be started remote-manually or locally. The flow control valves open on a low-low water level signal. Provisions are included for manual control of the valves.

It has been assumed that each pump requires DC power (from separate buses) for activation and control. Each electric motor-driven pump receives power from a separate AC channel. Control

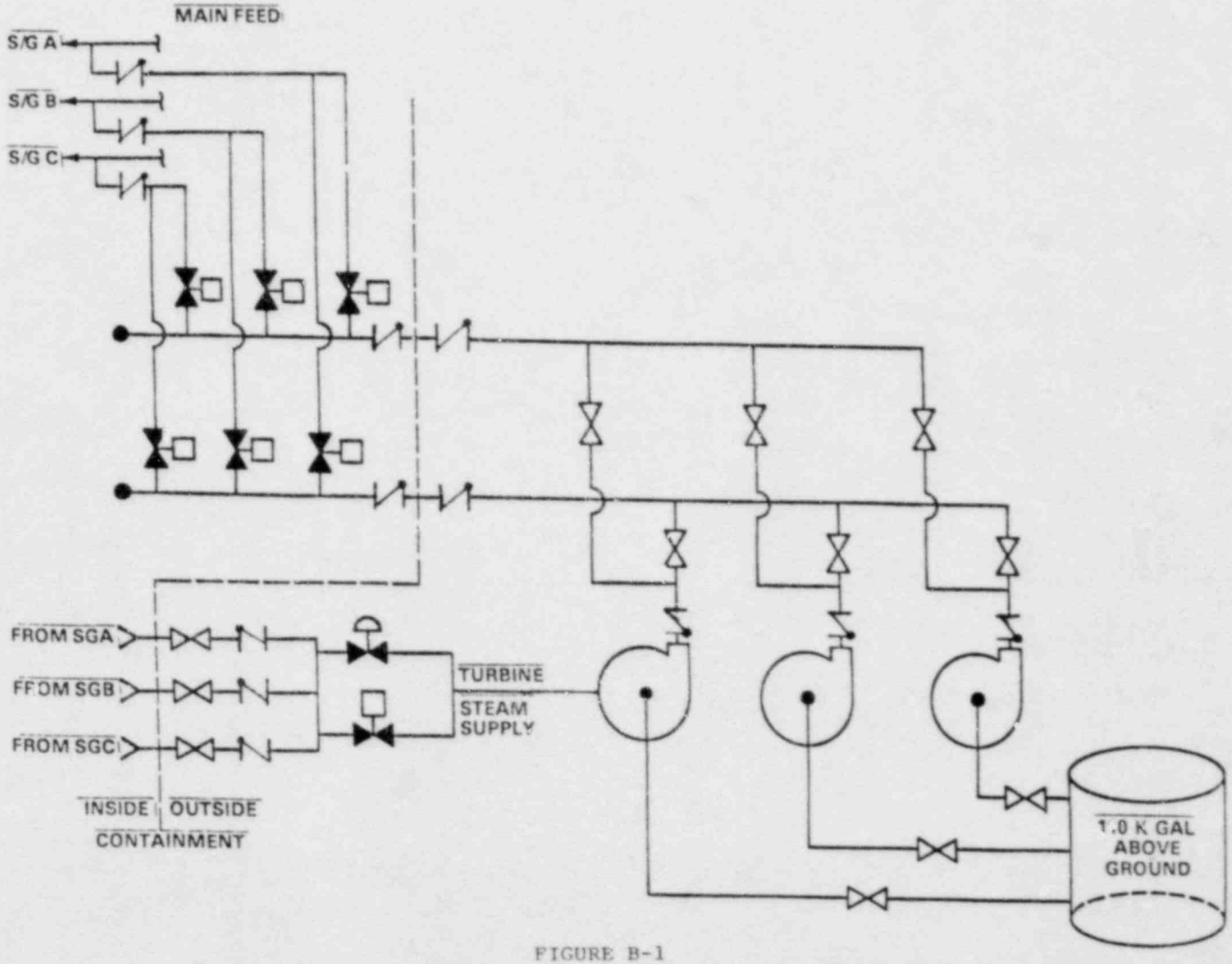


FIGURE B-1
SIMPLIFIED SCHEMATIC, AUXILIARY FEEDWATER SYSTEM

power for the steam turbine-driven pump is assumed to be supplied from bus 1 of the DC power system.

High Pressure Injection System (HPIS)

The HPIS design used in this analysis consists of three electric motor-driven high pressure charging pumps, associated piping, valves and controls, as shown in the simplified flow diagram of the HPIS in Figure B-2. These pumps normally draw water from the refueling water storage tank and inject this borated water into the reactor cold legs at normal primary system pressure. For most small loss of coolant accidents and transient conditions requiring high pressure makeup water, the flow from one charging pump is sufficient for successful operation.

During normal plant operation, one operating charging pump is used to control reactor coolant system inventory. Upon receiving a safety injection signal, both standby charging pumps are automatically started and the charging system is automatically realigned, as explained above, for high pressure injection. Normal high pressure water to the reactor coolant system pump seals is also maintained during the HPIS operation. Provisions also exist for manual operation as well as the use of alternate suction and discharge paths for the coolant recirculation mode.

For this study, it is assumed that train A, with one pump, is powered by DC and AC division 1 for actuation and motor power respectively. Train B has two pumps powered by AC division 2 with the necessary actuation and control signals powered by DC bus 2.

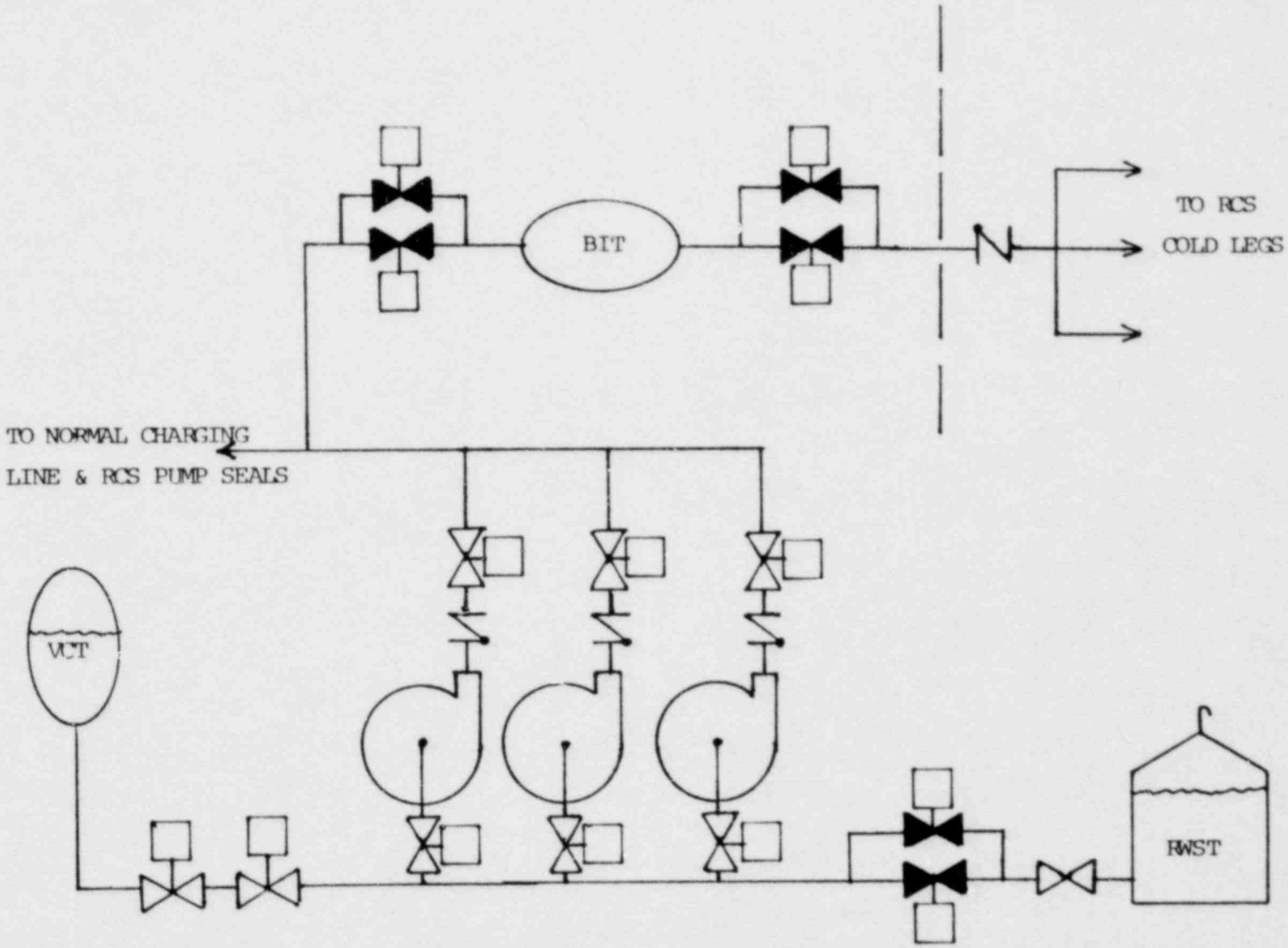


FIGURE B-2
SIMPLIFIED SCHEMATIC, HPIS

RCS Safety/Relief Valves

Besides the normal pressurizer heater and spray valve controls, RCS pressure is ultimately controlled by operation of the safety/relief valves located on the pressurizer. The system is comprised of three safety valves and two PORVs, as shown by the simplified schematic in Figure B-3.

In the cases where an initiating event raises the RCS pressure beyond the surge capability of the pressurizer, the PORVs or the safety valves would be used to limit the RCS pressure to acceptable limits. Normally, the PORVs would be automatically energized and opened upon a high pressure signal from the pressure control system. Manual operation of these valves is also provided. Should these fail to operate, the spring-loaded safety valves will automatically open as higher pressures are reached. Once the initial pressure surge has been controlled, the safety valves automatically reseat. In the case of the PORVs, these must be deenergized in order to reclose the valves. In the case of a stuck open valve, the PORVs can be blocked off by energizing and thus closing the PORV block valves.

For purposes of this study, it was assumed that the operation of any two safety/relief valves is sufficient to limit overpressure of the RCS. The PORVs and their associated block valves are assumed to be normally powered by offsite AC power with the additional capability of being supplied by emergency AC power if required.

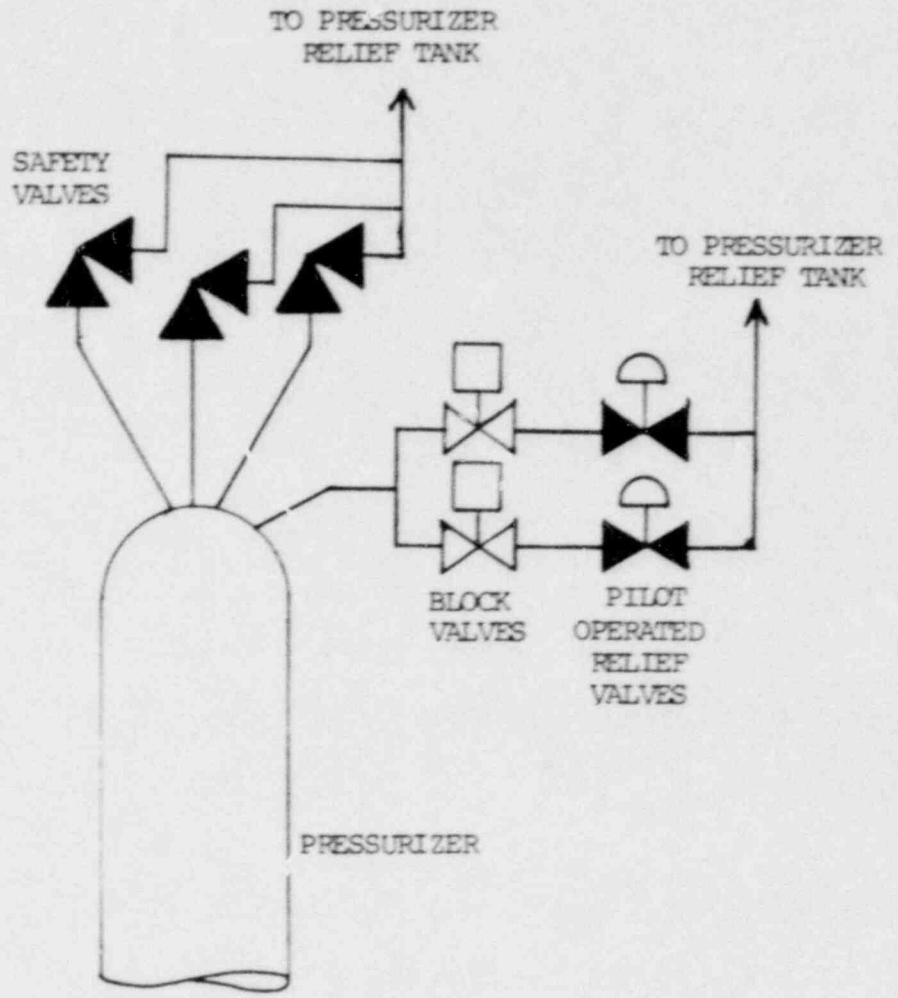


FIGURE B-3
SIMPLIFIED SCHEMATIC, RCS SAFETY/RELIEF VALVES

Reactor Core Isolation Cooling System (RCIC)

The RCIC system consists of a steam turbine driving a constant-flow pump with associated system piping, controls, and instrumentation as shown in Figure B-4. It is designed to deliver 600 gpm to the core at reactor vessel pressures from 1100 to 150 psig. The turbine is driven by steam which is generated by reactor residual heat and is supplied from main steam header "C" upstream of the main steam isolation valve in the drywell. The turbine is controlled by a demand signal from a flow controller located in the pump discharge line. Water discharged from the single stage pump is delivered to the core via feedwater line "B". Two sources of water are available to the RCIC system. Initially, water is used from the condensate storage tank with an option to manually transfer to the suppression pool.

System initiation is accomplished automatically upon receipt of a signal indicating low reactor water level. RCIC will continue to operate until vessel pressure drops to 150 psig, receipt of a high reactor water level signal, or a system malfunction occurs.

RCIC is not an engineered safeguard system. As part of the reactor coolant system, its primary function is to provide a backup source of water to the core during the initial phase of shutdown cooling. The RCIC requires only DC power for operation and control which is supplied from DC bus 1.

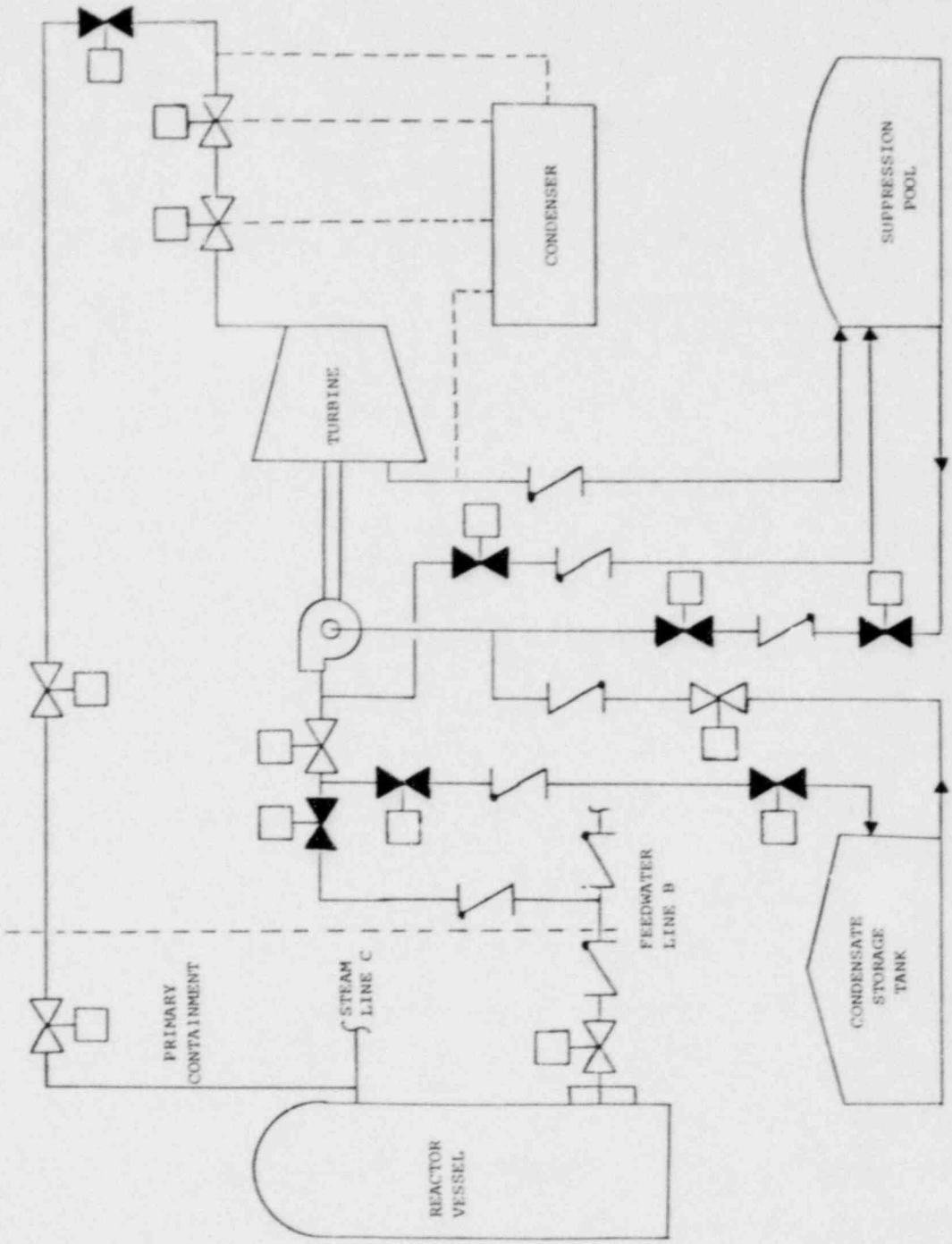


FIGURE B-4
SIMPLIFIED SCHEMATIC, RCIC

High Pressure Coolant Injection System (HPCI)

The HPCI system consists of a steam turbine driving a constant-flow pump with associated system piping, controls and instrumentation as shown in Figure B-5. It is designed to deliver 5000 gpm to the core at reactor vessel pressures from 1100 to 150 psig. The turbine is driven by steam which is generated by reactor residual heat and is extracted from main steam header "B" upstream of the main steam isolation valve. Turbine control is effected by a speed limiting governor and a control governor which is positioned in response to a flow controller located in the pump discharge line. Water discharged from the two series connected pumps is delivered to the core via feedwater line "A". Two sources of water are available to the HPCI system. Initially, water is taken from the condensate storage tank, and when the level in this tank is drawn down, automatic transfer to the suppression pool occurs. System initiation is accomplished automatically on receipt of a signal indicating low reactor water level or high drywell pressure. HPCI will continue to operate until vessel pressure drops below 150 psig, or until receipt of a signal indicating high reactor water level (indicating successful HPCI operation), or until a system malfunction occurs. The HPCI system requires only DC power for operation and control, which is supplied from DC bus 2.

Low Pressure Coolant Injection (LPCI)/Low Pressure Coolant Recirculation (LPCR) Systems

The LPCI system is one of the three operating modes of the Residual Heat Removal System (RHR). In general, it is a low

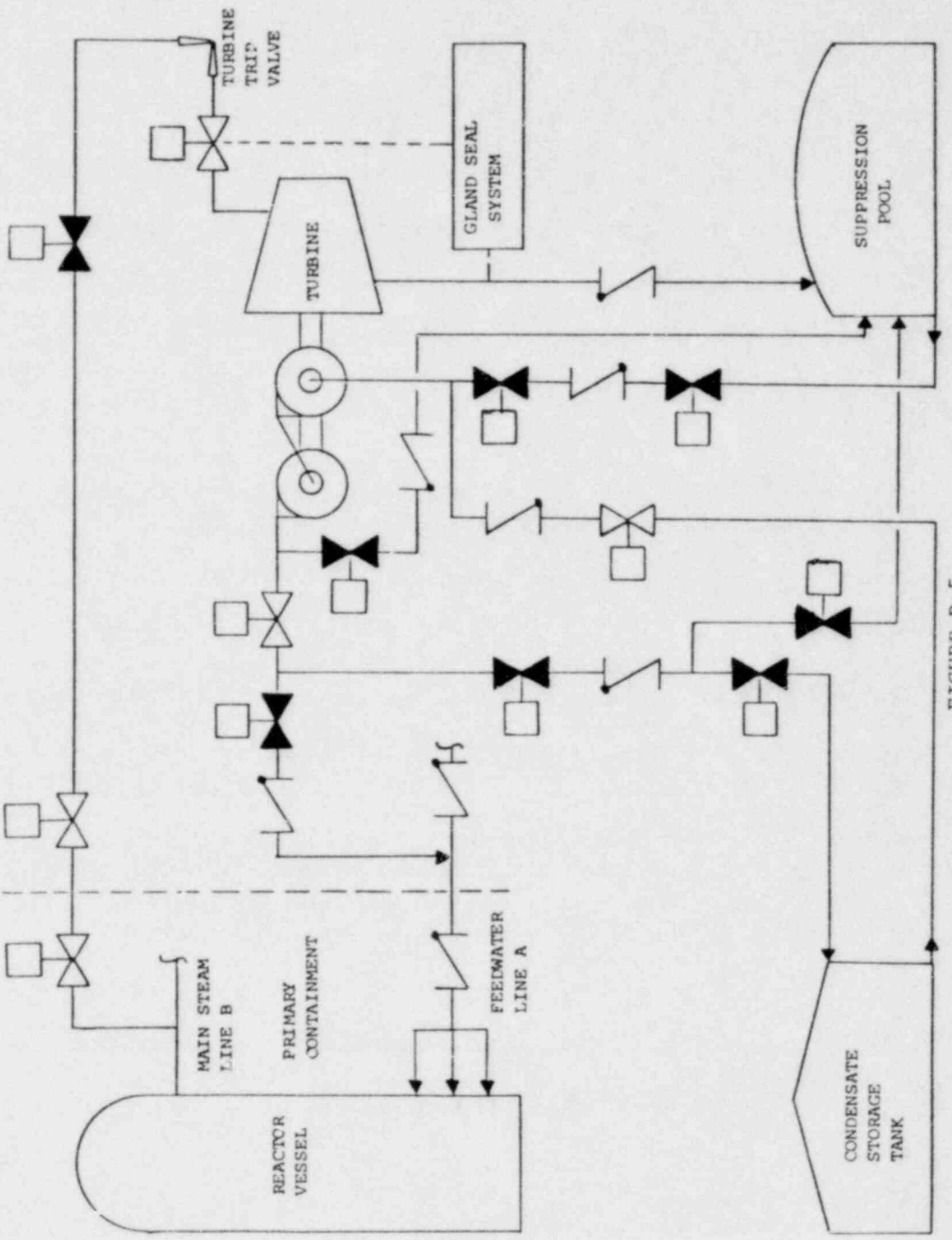


FIGURE B-5
SIMPLIFIED SCHEMATIC, HPCI

head, high flow system which can deliver rated flow to the pressure vessel when the differential pressure between the pressure vessel and the primary containment is 20 psi or less. The system can achieve a maximum output pressure of about 295 psig at minimum flow.

The major equipment of the LPCI system consists of four AC motor-driven centrifugal pumps, four heat exchangers and interconnecting piping and valves arranged as shown in Figure B-6. The major equipment is grouped in two divisions, or loops. Each loop consists of two pumps in parallel, two heat exchangers, associated piping and valves and a connection to a main recirculation loop through two motor-operated valves, a check valve and a "locked open" manually operated valve.

In operation, the four pumps take suction from the suppression pool and discharge to the reactor core through the jet pumps of the recirculation loop selected for LPCI injection by the LPCI control logic. The flow path includes the shell side of the heat exchangers (and the cross-connection for flow from the two pumps of the other loop). Flow through the tube side of the heat exchangers from the high pressure service water system is not required during use of the LPCI system as core heat is being transferred to the primary containment and suppression pool water through the ADS valves, in the case of a transient. Fluid lost from any of the lines within the primary containment returns to the suppression chamber through the pressure suppression vent lines.

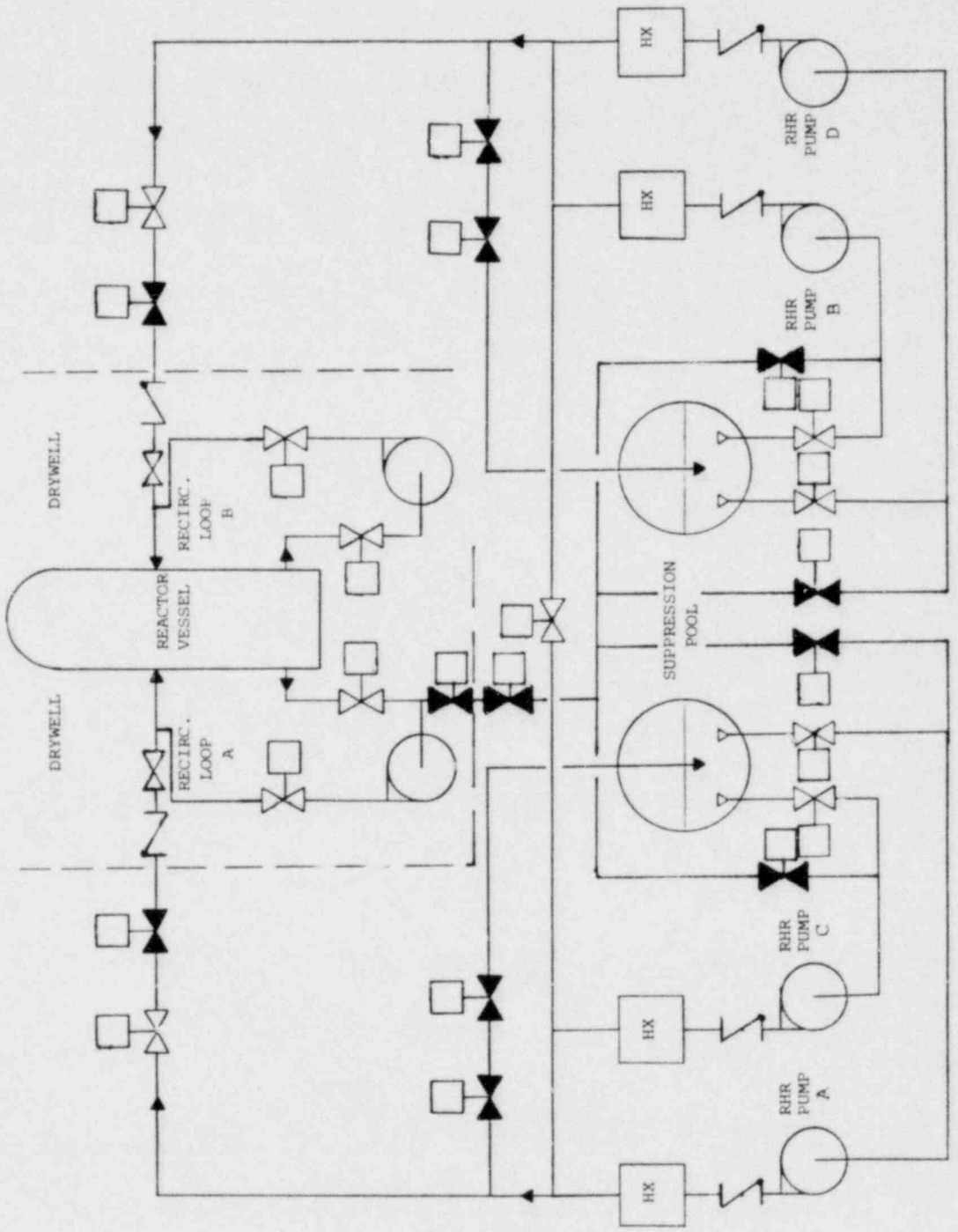


FIGURE B-6
SIMPLIFIED SCHEMATIC, LPCI/LPCRS

The two loops are cross-connected by a single line which contains a motor-operated valve. The cross-connect is intended to make it possible for the pumps of one loop to supply the other loop.

The AC and DC power requirements of the LPCI are equally divided between the two AC and DC divisions.

The LPCR system is the decay heat removal operating mode of the RHRS and consists of four pumps with associated piping, valves and heat exchangers as also shown in Figure B-6. The LPCR system is the LPCI system realigned for recirculating water from either the suppression pool or the reactor through heat exchangers and back to the suppression pool or the reactor core. The heat is extracted from the water by the high pressure service water system via the heat exchangers. Initiation of the LPCR mode of operation is performed manually by the plant operator.

Low Pressure Core Spray System (LPCS)

The major equipment of the LPCS consists of four AC motor-driven centrifugal pumps, two spray spargers in the reactor vessel above the core and interconnecting piping and valves. The equipment is arranged in two independent subsystems as shown in Figure B-7. Each subsystem contains two pumps in parallel and a connection to one sparger through two motor-operated valves, a check valve and a "locked open" manually operated valve.

Provisions for AC power and DC control power for the LPCS pumps and associated automatic motor-operated valves are similar to those described for the LPCI system.

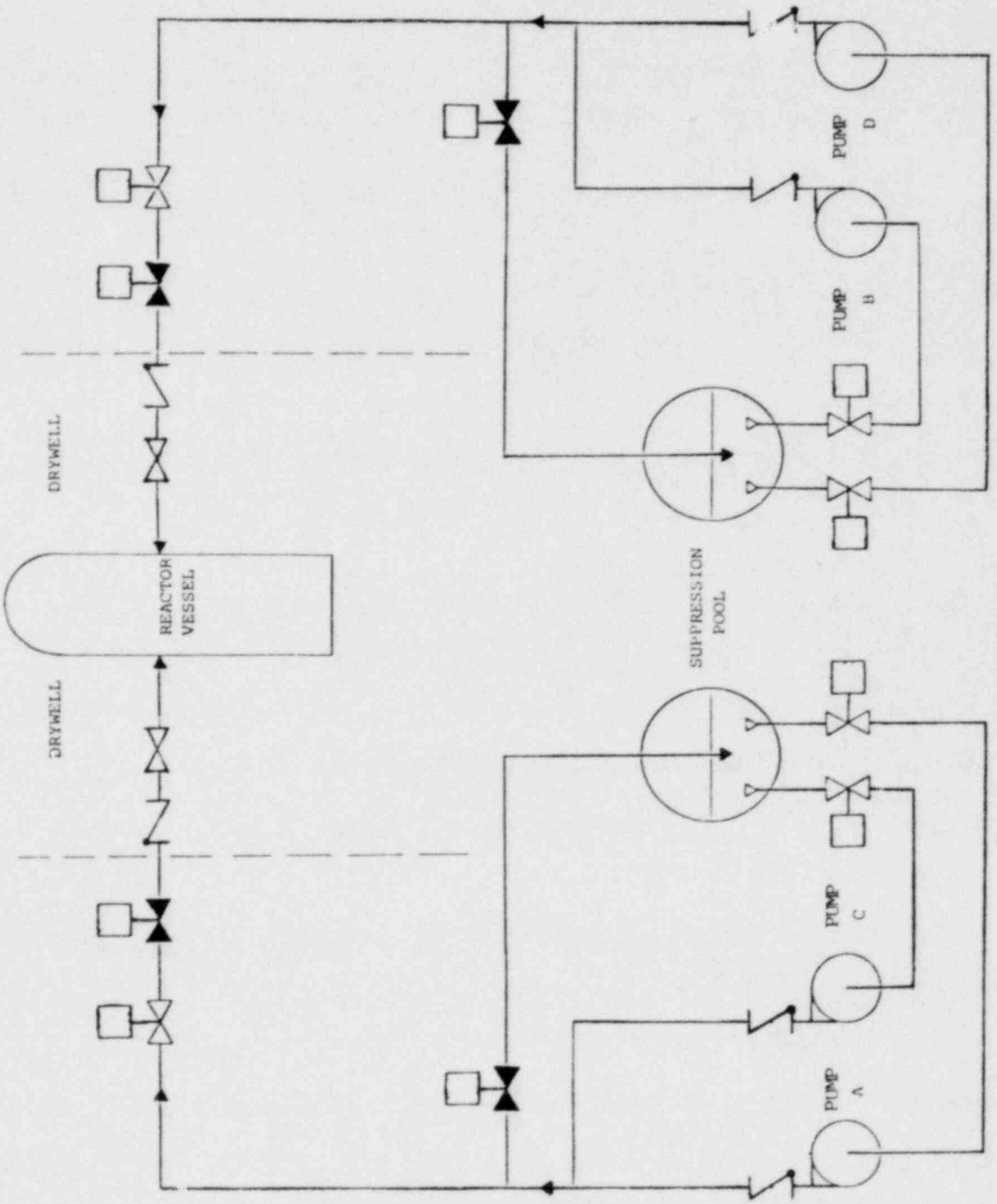


FIGURE B-7
SIMPLIFIED SCHEMATIC, LPCS

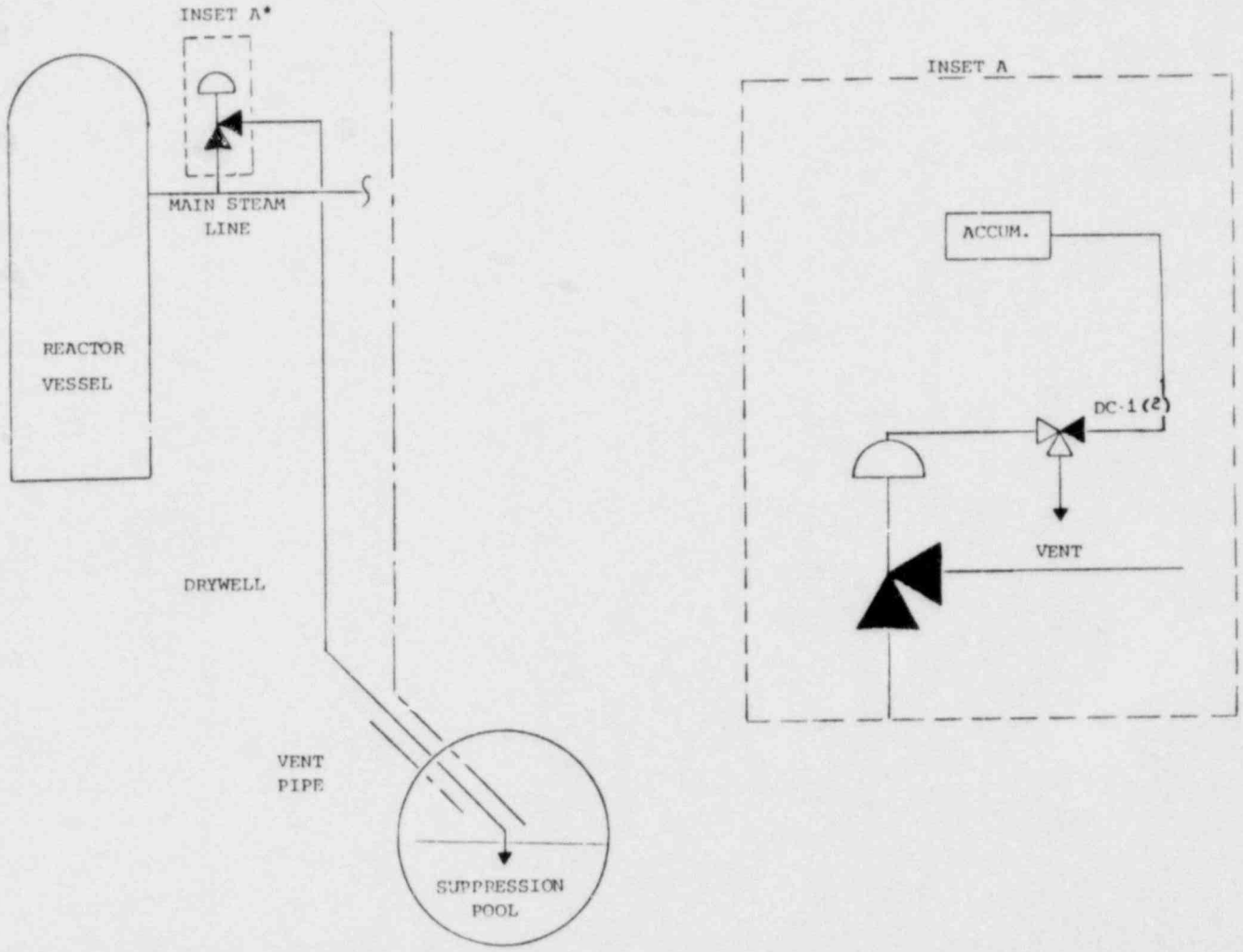
In operation, the two pumps of each subsystem take suction from the suppression pool and discharge to the reactor core through the spargers located above the core.

Automatic Depressurization System (ADS)

The ADS, shown in Figure B-8, consists of five normally closed relief valves which open automatically to reduce reactor vessel pressure to a level sufficient to permit coolant injection via the LPCI and LPCS systems. The system is activated on high drywell pressure and two coincident reactor vessel low water level signals. Depressurization is accomplished via the ADS logic which, upon sensing that the LPCI and LPCS discharge pressures are adequate, commands the five ADS relief valves to open, thus dumping the steam into the suppression pool. Each ADS valve has an air accumulator which supplies control to open the valve. Operation of the system requires only DC power which can be supplied by either DC bus. Sufficient depressurization will be achieved if four of the five relief valves open.

High Pressure Service Water System (HPSWS)/Emergency Service Water System (ESWS)

The HPSWS is comprised of the pumps, valves, heat eachangers, cooling towers and piping arranged as shown in the simplified schematic in Figure B-9. Any one HPSWS pump has the capacity to furnish sufficient flow of water to the four LPCRS heat exchangers during long term cooling. When the HPSWS is required for heat removal during LPCRS operation, each pump is started manually from a separate control room switch.



* TYPICAL OF FIVE VALVES

FIGURE B-8
SIMPLIFIED SCHEMATIC, ADS

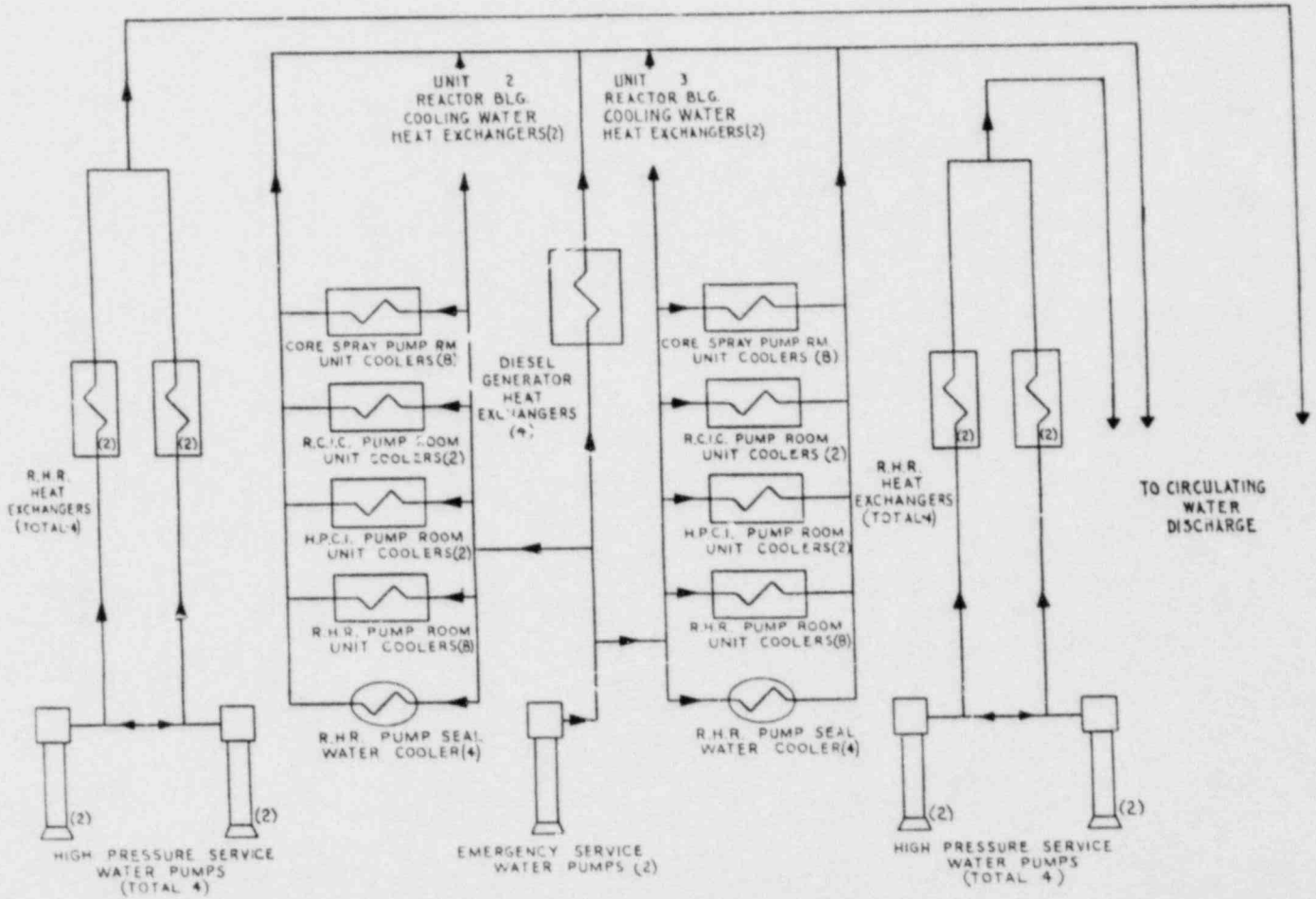


FIGURE B-9

SIMPLIFIED SCHEMATIC, HPSWS/ESWS

The AC and DC power requirements of the HPSWS are equally divided between the two AC and DC divisions.

The emergency service water system is also shown in Figure B-9. The function of the ESWS is to:

a) Provide a backup supply of cooling water to the LPCRS and LPCS pump compartment unit coolers and the LPCS pump lube oil coolers, and

b) provide cooling water to the diesel generators.

The ESWS and the "normal service water system" supply cooling water through check valves and a common manifold to the pump compartment unit coolers. Either water supply will suffice for pump compartment cooling. The ESWS is a standby system which supplies the needed cooling water upon loss of normal service water (e.g., if offsite power is lost). Water for both systems is normally taken from a reservoir adjacent to the plant and discharged back into the reservoir. If for some reason water is not available from the normal source, water can be taken by the ESWS from an on-site emergency cooling tower reservoir. In this case, water is circulated through the heat rejection loads, then through the cooling towers via the booster pumps, and back to the emergency reservoir.

The AC and DC power requirements of the ESWS are similar to that of the HPSWS.

Appendix C

DC Power System FMEA/LER Review

This appendix contains details of the FMEA and LER review which were performed as aids in developing and quantifying the DC power system fault tree. Table C-1 summarizes the FMEA. Tables C-2 thru C-4 list LERs used in the DC power system analysis. Table C-5 is provided to identify the LER categories and reporting periods covered in this study.

The FMEA includes identification of potential DC system component failure modes, their causes, methods of detection, and effects of the failures on the minimum DC power system performance. Other observations are also included such as compensating features for mitigating certain component failures and the identification of possible common cause failures.

The LERs were used in this study to also identify potential DC power system component failures and to quantify the various failure modes identified in both the FMEA and LER review. Below are brief discussions as to how the LERs were interpreted for this study. Use of the LERs to quantify DC system failure modes is discussed in Appendix E.

Of the 12 LERs listed in Table C-2, 6 were interpreted as operational/test and maintenance (T&M) errors causing bus degradation that was not immediately corrected or would not be easily correctable using a minimum DC system (e.g., no spare chargers). DC power (bus) failure was interpreted as those cases where the bus was either unavailable or bus voltage dropped significantly such that components requiring power from that bus could not function. These are item Nos. 1, 3, 8, 9, 10, and 12. The

remainder (except item 7, discussed below) appeared as easily correctable and thus were not considered as bus failures nor included in the quantification of single bus failures by operational/T&M errors provided in Appendix E.

Of the above six LERs, four items (numbers 3, 8, 10, and 12) were interpreted as possibly failing both buses of a minimum system if the two buses were tied together at the time of the event. In addition, item 1 is a failure mode indicative of operator error disabling more than one battery or bus. The use of these LERs in the quantification of common mode failures is discussed in Appendix E.

One of the 12 LERs, item 7, was interpreted as a design or manufacturing error which could cause loss of a DC bus.

In Table C-3, item 1 was interpreted as a common cause failure which rendered two batteries unavailable at the same time although power was supplied to the buses by the chargers. This item was used in the quantification of common mode failures as discussed in Appendix E. The others were used to identify other possible common cause failures and represent precursors to coincident unavailability of two batteries.

Table C-4 lists the DC power system component failure data obtained in the LER review. The criteria used for interpreting these component failures is outlined below:

Battery Charger -

- Output current/voltage high or low
- Erratic output
- Trip of a charger
- Loss of continuity due to open/short connections, cable assemblies, or corroded terminals.

Battery -

- Low or no voltage/current output as identified by instrumentation or inability to energize user equipment.
- Many buckled or damaged plates
- Battery declared inoperable (with evidence that inoperability extends beyond just not meeting technical specification limits)
- Loss of continuity due to open/short connections, cable assemblies, or corroded terminals
- Must be station battery

Using the above criteria, 24 charger failures and 8 battery failures were identified and used to estimate the failure rates of these components. Discussion of the determination of key DC system and component failure rates, including the battery failure rate, is provided in Appendix E.

TABLE C 1

FAILURE MODES AND EFFECTS ANALYSIS

NAME D.C. POWER SYSTEM

DWG. NO./REV.

ITEM #	ITEM DESCRIPTION	FAILURE MODE/CAUSE	METHOD OF DETECTION	LOCAL EFFECT	SYSTEM EFFECT	COMMENTS/RECOMMENDATIONS COMPENSATING PROVISIONS
1.	Battery Charger (BC1-1, BC1-2) The two battery chargers each have an output rating of 200 amperes at 130 VDC with an input of 440 VAC, 3φ, 60 Hz. Each charger is equiped with a d.c. voltmeter, ammeter, ground detector relay and an a.c. supply failure relay. Contacts of these relays operate annunciators on the main control board. Each charger supplies power for operation of equipment on its associated bus section and maintains a floating charge on its associated battery.	a) Low output voltage • voltage regulator malfunction • operator sets output level too low • low a.c. input to charger	• Charger output voltage and current monitored and alarmed	• Low d.c. bus voltage • insufficient charge maintained on associated battery	• Reactor trip due to loss of one of two d.c. buses - loss of capability to supply d.c. loads associated with failed bus	1) Remaining bus available to supply critical loads. 2) Note that low a.c. input may be common cause failure. If cause of low a.c. is malfunction or degradation at source common to both charger input buses then other d.c. bus will be similarly effected.
		b) Low output current • charge control malfunction • operator sets charging level too low • current limiter malfunction	• Charger output voltage and current monitored and alarmed	• Insufficient charge maintained on associated battery	• Loss of capability to supply d.c. loads via battery if associated charger trips	3) Note that operator error in setting charger output levels may be common cause failure. Probability that operator will err in setting second charger is high given error in setting first charger.
		c) High output voltage • voltage regulator malfunction • surge voltage suppressor malfunction • high a.c. input to charger • operator sets output level too high	• Charger output voltage and current monitored and alarmed	• High d.c. bus voltage - possible damage or trip out of associated battery due to high voltage	• Loss of d.c. bus if both charger and battery trip - reactor trip • Degraded d.c. bus if charger trips. Battery output will drop due to drain - reactor trip	4) An insufficiently charged battery will inhibit the supply of peak loads even though charger is still operable. In the event of loss of the charger, the effect of the degraded battery will be the loss of the d.c. bus since it will not be able to supply the required loads.
		d) High output current • charge control malfunction • current limiter malfunction • operator sets charging level too high	• Charger output voltage and current monitored and alarmed • Charger trips out due to high current output	• Possible battery damage due to excessive charging. - battery trips out if overcharged	• Loss of capability to supply required d.c. loads via battery. • Loss of d.c. bus if both battery and charger trip off - reactor trip	
		e) Over charges battery • charge control timer malfunction • operator error in setting charge levels	• None unless battery trips off due to overcharging	• Loss of battery due to damage caused by overcharging	• Loss of capability to supply required d.c. loads via battery	

TABLE C-2

NAME DC POWER SYSTEM

DWG. NO./REV.

FAILURE MODES AND EFFECTS ANALYSIS

ITEM #	ITEM DESCRIPTION	FAILURE MODE/CAUSE	METHOD OF DETECTION	LOCAL EFFECT	SYSTEM EFFECT	COMMENTS/RECOMMENDATIONS COMPENSATING PROVISIONS
1.	Battery Charger (BC1-1, BC1-2)	f) High a.c. ripple on d.c. output • rectifier malfunction	• None	• Battery and charger output fuses will open if ripple is sufficiently high (~25%). Otherwise, battery will act as filter	• Loss of d.c. bus if both charger and battery trip off - reactor trip • High ripple (~25%) will severely damage user equipment. • No effect for low level ripple	
		g) No output • Input or output fuse opens • Input or output circuit breaker trips • Surge voltage suppressor fails • Charge control malfunction • Voltage regulator malfunction • Short to d.c. return • Loss of a.c. feed • Operator sets trip settings too low for required loads • Cable/wiring faults to bus	• Charger output voltage and current monitored and alarmed	• Loss of charger	• Minor - battery will supply required d.c. loads	

TABLE C 1

FAILURE MODES AND EFFECTS ANALYSIS

NAME D.C. POWER SUPPLY

DWG. NO./REV

ITEM #	ITEM DESCRIPTION	FAILURE MODE/CAUSE	METHOD OF DETECTION	LOCAL EFFECT	SYSTEM EFFECT	COMMENTS/RECOMMENDATIONS COMPENSATING PROVISIONS
2.	Battery (#1, #2) Each battery, consisting of 60 cells, supplies power for operation of turbine-generator emergency auxiliaries, switchgear, motor operated disconnect switches, annunciators, 125 VDC solenoid valves, vital bus inverters, and emergency lighting. Battery #1 has a 3 hour rating of 120 amperes and a capacity of 960 amp-hour from a fully charged condition to 105 volts. Battery #2 has a corresponding 8 hour rating of 105 amperes and a capacity of 840 amp-hour.	a) Low Output • poor intercell connections due to loose fittings, corrosion, etc. • Defective cells • High resistance short across battery output terminals or to d.c. return • Insufficient electrolyte in cells • High ambient in battery room	• None except during battery testing	• Battery degraded	• Possible loss of capability to supply peak loads even though charger is operable • Loss of d.c. bus in the event charger trips off - reactor trip	5) High battery room ambient may be a common cause failure if high ambient is caused by ventilation system failure. If ventilation system is common to both battery rooms then other battery will be similarly affected. Also, build-up of hydrogen will occur and may result in loss of both batteries if hydrogen ignition occurs.
		b) No output • Output fuse opens • Open intercell connections • Defective cells - internal shorts • Insufficient or no electrolyte • Short to d.c. return • Operator inadvertently disconnects battery from bus • Cable/wiring faults to bus	• None except during battery testing	• Battery is unavailable	• Loss of capability to supply d.c. loads in the event charger trips off - reactor trip • Loss of capability to supply peak loads even though charger is operable	6) With battery unavailable, the inability to supply peak d.c. loads may serve as indication of an unavailable battery. 7) Insufficient electrolyte may be a common cause failure. Maintenance requirements include check of electrolyte level and loss of or a severely degraded battery due to insufficient electrolyte in battery cells may indicate maintenance error common to both battery systems. Also, other malfunctions leading severe loss of electrolyte may be common to both battery systems.

TABLE C-1

NAME 1E POWER SYSTEM

DWG. NO. REV.

FAILURE MODES AND EFFECTS ANALYSIS

ITEM #	ITEM DESCRIPTION	FAILURE MODE/CAUSE	METHOD OF DETECTION	LOCAL EFFECT	SYSTEM EFFECT	COMMENTS/RECOMMENDATIONS COMPENSATING PROVISIONS
3.	125 VDC Bus (#1, #2) Each bus section is rated at 125 VDC, 800 amperes. The loads supplied by the battery and battery chargers are supplied via the bus. Each bus is equipped with an undervoltage relay to provide an alarm should a low voltage condition occur.	a) No d.c. voltage on bus • Short to d.c. return • Operator inadvertently de-energizes bus • Overload by user equipment drops bus voltage	• Bus voltage monitored and alarmed	• Loss of 125 VDC bus	• Reactor trip due to loss of one of two d.c. buses • Loss of capability to supply d.c. loads associated with failed bus	8) Remaining bus available to supply critical loads.
		b) Low bus voltage • High resistance short to d.c. return • Overload by user equipment drops bus voltage	• Bus voltage monitored and alarmed	• Degraded 125 VDC bus	• Possible reactor trip due to degraded bus • Degradation in capability to supply required d.c. loads	
4.	Bus Tie Breaker Two-pole manually operated circuit breaker for interconnecting buses #1 and #2 to permit T&M on the battery chargers.	a) Fails to close on demand	• No immediate indication of failure to close	• Interconnection of both d.c. buses inhibited	• Failure to detect breaker failure combined with deenergization of charger for maintenance results in supplying d.c. loads on associated bus via battery - possible loss or degradation of d.c. bus and subsequent reactor trip • Minor effect if breaker failure is detected prior to de-energization of charger	9) Remaining bus available to supply critical loads.
		b) Fails to open on demand	• No immediate indication of failure to open	• Isolation of both d.c. buses inhibited	• Minor	
		c) Fails open after closure	• Output voltage on bus with charger de-energized will drop due to drain on battery and will be indicated in control room via voltage monitor and alarm	• Degraded 125 VDC bus	• Possible reactor trip due to degraded bus • Degradation in capability to supply required d.c. loads	

TABLE C-1

FAILURE MODES AND EFFECTS ANALYSIS

DATE DC POWER SYSTEM

DWG. NO./REV.

ITEM #	ITEM DESCRIPTION	FAILURE MODE/CAUSE	METHOD OF DETECTION	LOCAL EFFECT	SYSTEM EFFECT	COMMENTS/RECOMMENDATIONS COMPENSATING PROVISIONS
4.	Bus Tie Breaker (Continued)	d) Shorts to d.c. return while closed	• Loss of both d.c. buses will be detected via voltage monitor and alarm	• Loss of d.c. buses #1 and #2	• Reactor trip due to loss of d.c. buses • Loss of capability to supply all required d.c. loads.	10) The bus tie breaker constitutes a potential common cause failure due to the possibility of shorting to the d.c. return when closed and thereby causing the loss of both d.c. buses.
		e) One side shorts to d.c. return while open	• Loss of d.c. bus which is shorted out will be detected via voltage monitor and alarm	• Loss of d.c. bus #1 or #2	• Reactor trip due to loss of d.c. bus • Degradation capability to supply required d.c. loads	

Table C-2. Single Bus Failure Related Incidents

1.) Dresden-2 3/21/78: During normal operation, the isolation condenser was inadvertently rendered inoperable for 42 minutes while the HPCI system was also out of service for repair. A switching error after the unit 3 battery discharge test (250 V) caused a loss of feed to unit 2 reactor building 250 VDC MCC No. 2 bus. This rendered isolation condenser valve MOV 1301-3 (normally closed) inoperable. Both battery systems returned to normal. Procedures revised.

2.) Ft. St. Vrain-1 11/23/76: Improper switching due to a 1A battery charger failure overloaded 1D charger and dipped 1A instrument bus voltage. This caused a reactor scram and dump of both loops of the steam generators. Battery charger was overloaded which lowered voltage to trip levels. Personnel involved have been admonished. Electrical design deficiency also identified. Modification to circuit being made.

Table C-2 (Continued)

3.) H. B. Robinson-2 3/10/72: While at 85% of full power, a 50 hp DC emergency oil pump was left on battery A bus following a routine test. The station battery became depleted finally causing a reactor trip. Closing of tie breakers to the startup transformer and emergency bus E-1 did not occur due to this low DC voltage. Subsequent damage occurred to turbine generator bearings and recirculation pump seals. Design changes were made and operator procedures and training were reviewed.

4.) H. B. Robinson-2 7/10/76: While critical and at 0% power, battery B leads were removed for maintenance rendering the battery inoperative. Battery charger A tripped and leads were replaced on battery B. Personnel violated technical specification requiring reactor to be non-critical to render battery inoperative.

5.) Oyster Creek-1 12/14/73: Momentary interruption of 125 V DC power supply to various safeguards systems. Operator erred in jumper placement

while inspecting for electrical ground. Restored all systems to normal and revising procedures.

6.) Oyster Creek-1 12/12/75: During a routine 6 month load test on station batteries, a 125 V DC distribution center was deenergized. After reenergization, load reduction commenced but was later halted. Personnel error in following procedures caused the deenergization. The center was immediately reenergized. Procedure revised on battery load test.

7.) Palisades-1 6/9/74: A loss of DC control power to the 1D bus occurred. Breaker was found tripped and initial efforts to reset were unsuccessful. No undervoltage alarm was received. A marginal reset latch on the breaker required special motion to assure latching. Breaker replaced and wiring completed on alarm circuit.

Table C-2 (Continued)

8.) Palisades-1 10/20/76: During shutdown, DC bus 2 voltage dropped to about 60 volts which dropped voltages on two AC preferred buses. Redundant charger was energized and the bus returned to normal. Improper coordination of battery charger current limiter and the charger output breaker setting due to starting of an oil pump earlier which caused breaker trip.

9.) Prairie Island-2 4/14/76: During capacity test of No. 12 battery (battery unavailable) No. 12 battery charger failed which disabled train B for about 5 minutes. Several items of one train of safeguards were thus inoperable. A spare charger was immediately put in service. Voltage control card loose in its socket. All control cards cleaned and adjusted. Chargers added to annual electrical preventive maintenance program.

Table C-2 (Continued)

10.) Quad Cities-2 8/31/74: Reactor tripped due to trouble with controlling reactor water level. HPCI system would not operate so RCIC was manually operated to restore level. Investigations found that HPCI valves would not operate because 250 V DC battery was discharged to 70 volts because charger breaker had been tripped. Alarm had previously sounded but considered faulty when operator incorrectly determined that battery charger breaker was closed. Charger breaker was later reset and systems returned to normal. Occurrence attributed to operator error.

11.) Quad Cities-2 10/29/75: While the unit was in cold shutdown, the 125 V control power to RHR B and Core Spray B automatic logic was lost. Breaker was inadvertently left off following maintenance. Breaker was turned on and power was restored.

Table C-2 (Continued)

12.) Zion-2 9/19/76: While attempting to take battery 211 off of equalizing charge during start-up, a switching error caused bus 211 to be deenergized, resulting in reactor trip. Diesel generator 2A, in parallel to the grid, was overloaded and its field windings were burned open. Procedure changes made to avoid future switching errors.

Table C-3 Possible Battery Common Cause Failures

1.) Turkey Point-4 10/13/74: Two batteries found in poor condition with damaged cells (at least one battery failed a load test). Attributed to overcharging. Not detected until test and subsequent check of batteries.

2.) Big Rock Point 3/30/77: Cable connections to multiple batteries found loose and corrected upon receiving battery discharge alarm.

3.) Dresden-3 5/9/75: Two batteries failed discharge test due to bad cells (24 V DC system).

4.) J. M. Farley-1 4/18/78: Two battery banks declared inoperable during routine surveillance; bad cells.

Table C-4 DC System Component Failures

Battery Charger Failures:

1. Low output due to failure in charger control circuit - Beaver Valley-1, 3/20/78.

2. No current output due to current limiter malfunction - Big Rock Point, 11/7/74.

3. Low output due to failed silicon rectifiers - Big Rock Point, 6/30/76.

4. No current output due to failed DC output fuse resulting from high charging current and high temp. (cabinet door open) - Brunswick-1, 10/21/77.

5. No output due to failed voltage suppressors - Calvert Cliffs-1, 9/20/73

6. No output due to loose connections at current module and input breaker - Cooper-1, 6/27/78.

7. No output from 2 battery chargers due to open of fuse in charging circuit common to both chargers - Dresden-1, 7/29/77.

8. Erratic charger output caused "deep cycling" of battery - Dresden-3, 10/18/76.

9. Low output due to failed voltage regulator - E. I. Hatch-1, 4/30/74.

10. No output which caused subsequent overloading on other buses - Ft. St. Vrain, 11/23/76.

11. Cable insulation cut causing charger output breaker to trip - Ft. St. Vrain, 2/1/76.

12. High output due to failed charge control timer - Haddam Neck, 4/24/76.

13. No output due to blown fuse in fan motor (high temp.) - Indian Point-3, 5/10/76.

Table C-4 (Continued)

14. No output due to fan failure resulting in circuit breaker trip - Indian Point-3, 6/8/76.

15. No output due to dirty contacts on control circuit card - Oconee-1, 6/28/77.

16. Charger output breaker tripped due to improper current limiter and output breaker settings - Palisades-1, 10/20/76.

17. No output due to loose voltage control card - Prairie Island-2, 4/14/76.

18. No output due to failed charge control circuit - Quad Cities-2, 3/17/77.

19. No output due to thermal overload - St. Lucie-1, 12/16/77.

20. Loss of battery charger due to failed input transformer which caught fire - Turkey Point-3, 12/16/72.

21. As above in #20 - Turkey Point-3, 5/17/75.

22. Low output due to failed voltage regulator - Vermont Yankee-1, 10/13/76.

23. Charger failure due to defective bearing and procedural oversight - Yankee Rowe, 10/17/77.

24. No output due to failed voltage regulator - Zion-1, 8/25/75.

Insufficient Output From Battery:

1. Battery declared inoperable due to degraded condition resulting from erratic charging - Dresden-3, 10/18/76.

2. Two batteries in poor condition due to over-charging - Turkey Point-4, 10/13/74.

3. Low battery voltage due to charger failure - Vermont Yankee, 10/13/76

Table C-4 (Continued)

4. Loose connectors caused possible loss of multiple batteries (at least 1 battery lost) - Big Rock Point, 3/30/77.

5. Battery found with cracked cell; battery temporarily inoperable - Fitzpatrick-1, 10/20/77.

6. High resistance heating caused battery fire - H. B. Robinson-2, 7/16/78.

7. Defective terminal or inter-cell connection caused battery damage - Oconee-3, 7/27/78.

8. Battery system out of service due to many weak cells - Quad Cities-1, 9/24/77.

Other non-station battery failures indicative of battery failure modes (not used in quantification of battery failure rate since these are not station batteries).

1. 24 V battery nearly failed to start diesel starting motor due to corrosion on terminals - Big Rock Point, 11/14/74.

2. 24 V battery failed to start diesel due to cable failure - Big Rock Point, 8/12/76.

3. Diesel failed to start due to loose battery cables and solenoid connections - Big Rock Point, 8/29/77.

4. Battery connector broken off cell post - Browns Ferry-2, 7/9/76.

5. Two 24 V DC batteries failed test due to bad cells - Dresden-3, 5/9/75.

6. Battery failed to start fire pump diesel due to bad cell - Oyster Creek-1, 3/21/72.

7. Battery failed to start containment spray system diesel as a result of low charging level - Zion-1, 8/25/75.

Table C-5. LER DATA (Reviewed during study)

CAT. NO.	LER CATEGORY	REPORTING PERIOD	NO. of LERs
1	ELECTRIC POWER SYSTEMS AND BATTERIES	1969 TO 31 OCTOBER 1978	1021
2	EVENTS INVOLVING DC POWER	1969 TO 19 OCTOBER 1978	104
3	BATTERY EVENTS	1 JANUARY 1972 TO 18 OCTOBER 1978	87
4	DC ONSITE POWER SYSTEM EVENTS	9 NOVEMBER 1977 TO 27 JULY 1978	28
5	CABLE EVENTS	1974 TO 10 AUGUST 1978	150
6	RELAYS AND CIRCUIT CLOSERS	1969 TO 23 JULY 1979	1150
7	AIR CONDITIONING, HEATING, COOLING AND VENTILATION SYSTEMS AND CONTROLS	1969 TO 4 JUNE 1979	92

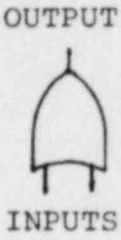
Appendix D

Fault Trees

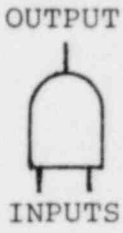
This appendix contains abbreviated forms of the fault trees for the minimum DC power system, PWR shutdown cooling systems, and BWR shutdown cooling systems. The fault trees depict the basic logic and system relationships of the PWR and BWR event trees.

In these abbreviated forms of the fault trees, transfers, particularly those from the DC fault tree to the shutdown cooling trees, have been simplified and do not necessarily rule out events that are not allowed to occur simultaneously. For example, the trees shown allow the combination of DC bus 1 down for test and maintenance while DC bus 2 is also out for test and maintenance. Unallowable concurrent events were properly treated by performing the analyses with fully expanded forms of the abbreviated fault trees. These expanded forms of the fault trees were drawn so that unallowable combinations of events could not lead to the top event. As a result, combinations such as DC bus 1 and 2 down for test and maintenance could not occur in the actual fault trees used in the analyses. Abbreviated forms for the trees are provided in this appendix for the purposes of brevity and to display the basic logic used in the fault tree models.

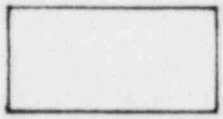
FIGURE D-1. KEY TO FAULT TREE SYMBOLS



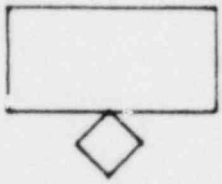
OR GATE: OUTPUT OCCURS IF ONE OR MORE INPUTS OCCUR.



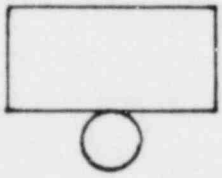
AND GATE: OUTPUT OCCURS IF ALL INPUTS OCCUR.



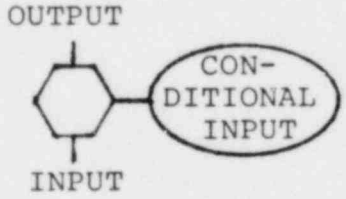
RECTANGLE: EVENT DESCRIPTION



UNDEVELOPED EVENT: EVENT IS NOT FURTHER DEVELOPED EITHER BECAUSE THE EVENT IS OF INSUFFICIENT CONSEQUENCE OR BECAUSE INFORMATION IS UNAVAILABLE.



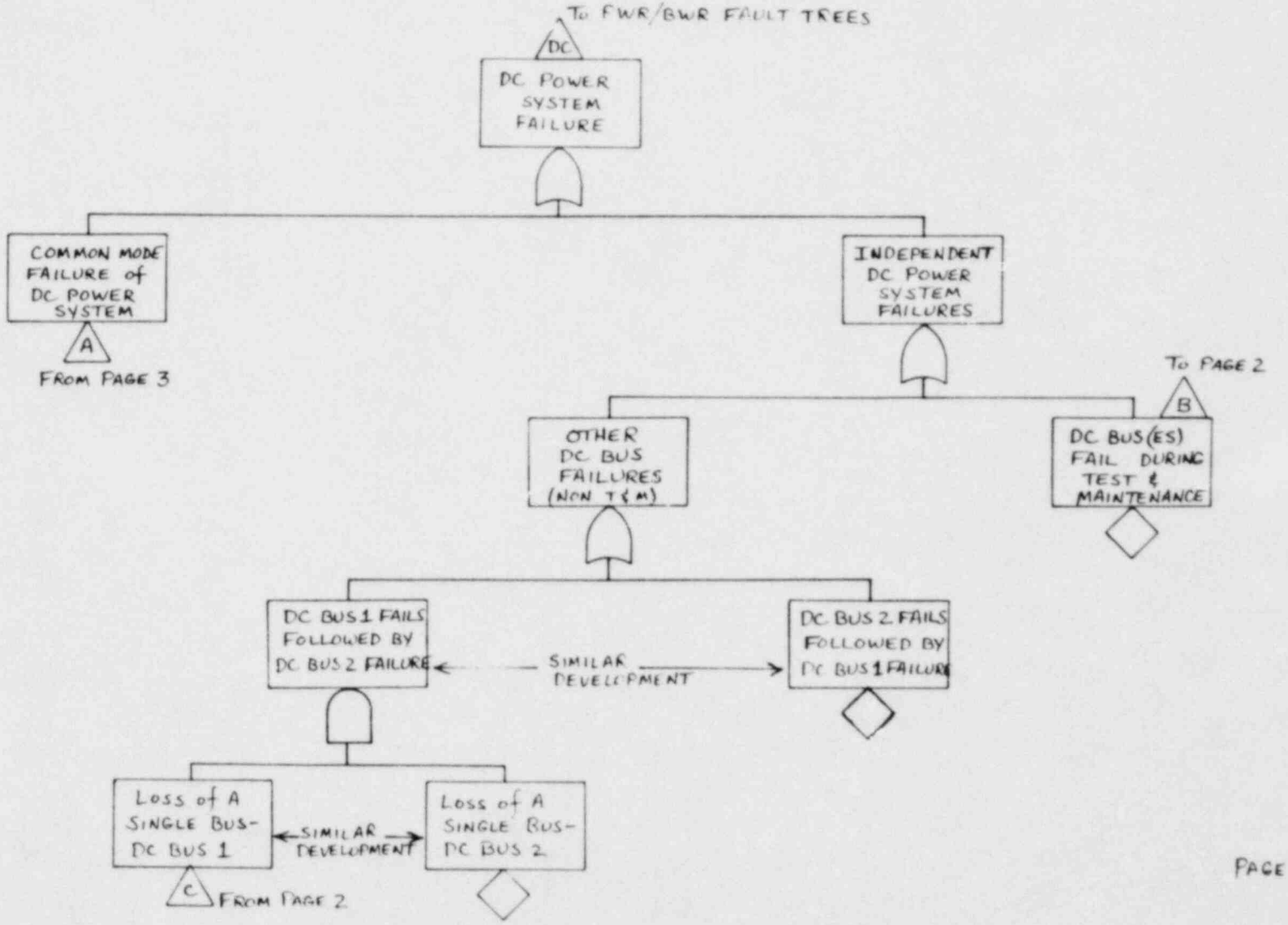
BASIC EVENT: EVENT DOES NOT REQUIRE FURTHER DEVELOPMENT

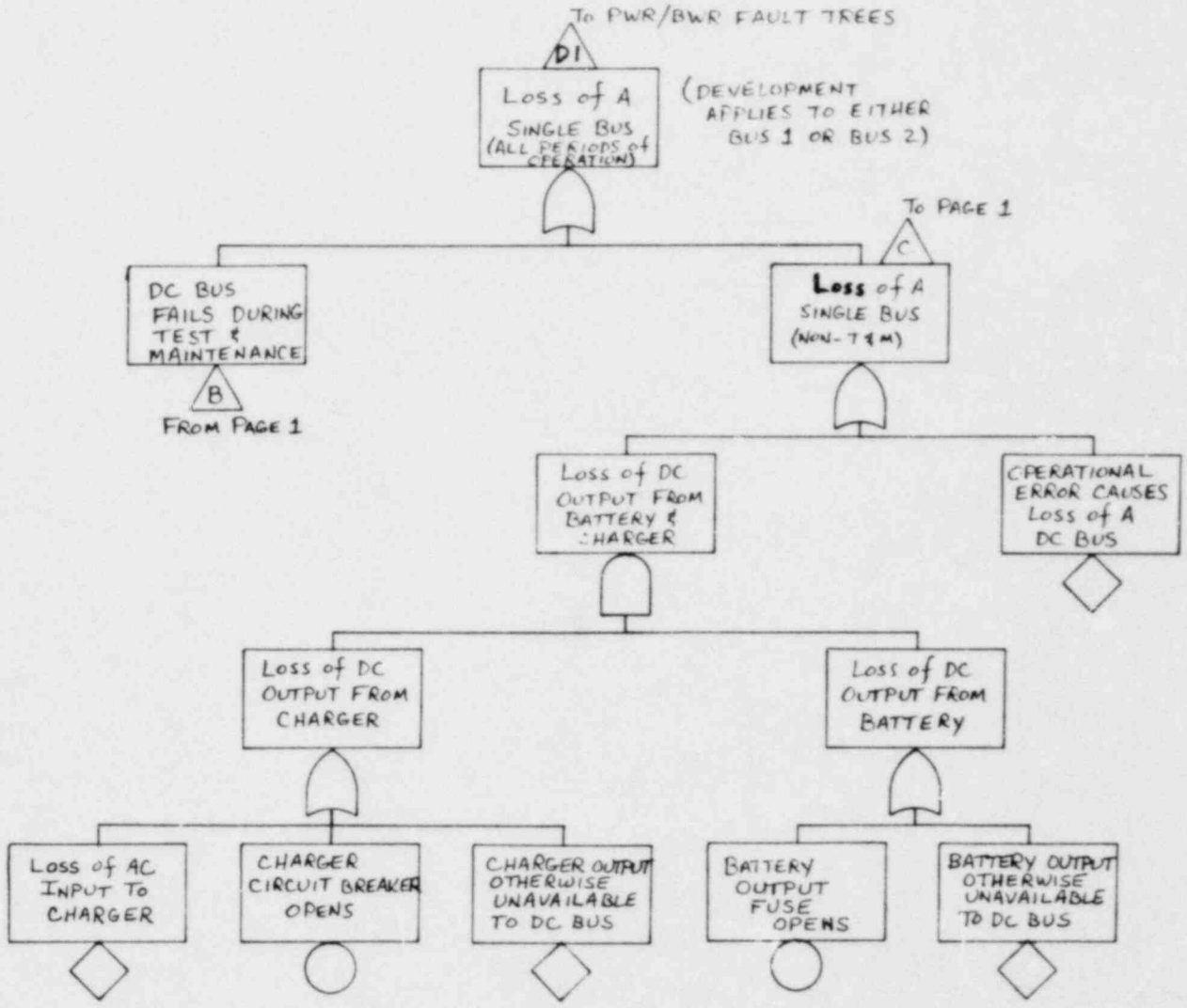


INHIBIT GATE: OUTPUT IS CAUSED BY THE INPUT PROVIDED THE CONDITIONAL INPUT IS SATISFIED.

TRIANGLE: TRANSFER SYMBOL WHICH LINKS LOGIC DEPICTED ON THE FAULT TREE TO OR FROM A DIFFERENT PORTION OF THE FAULT TREE (LIKE IDENTIFICATION WITHIN TRIANGLES LINK TOGETHER).

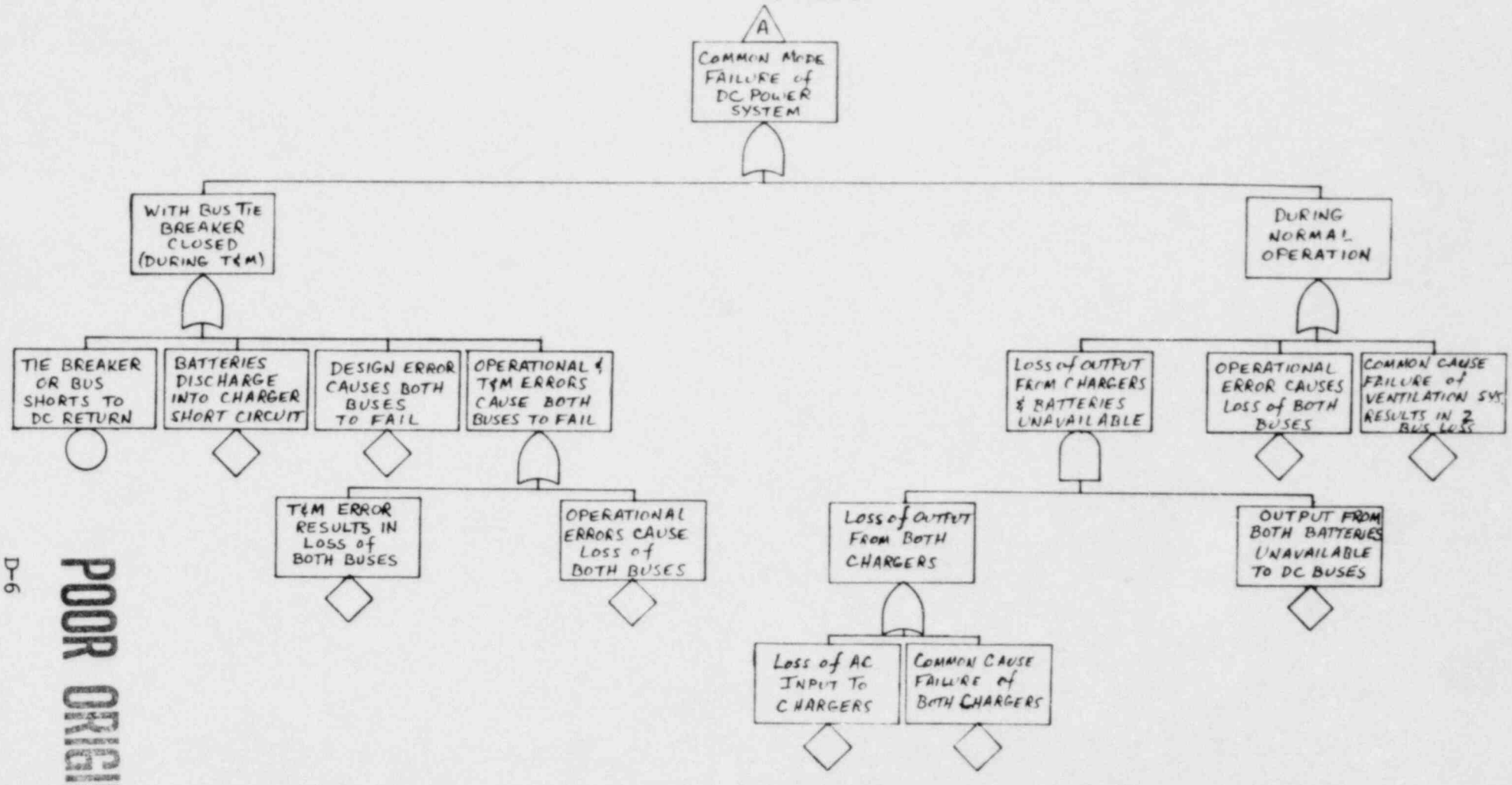
DC POWER SYSTEM FAULT TREE



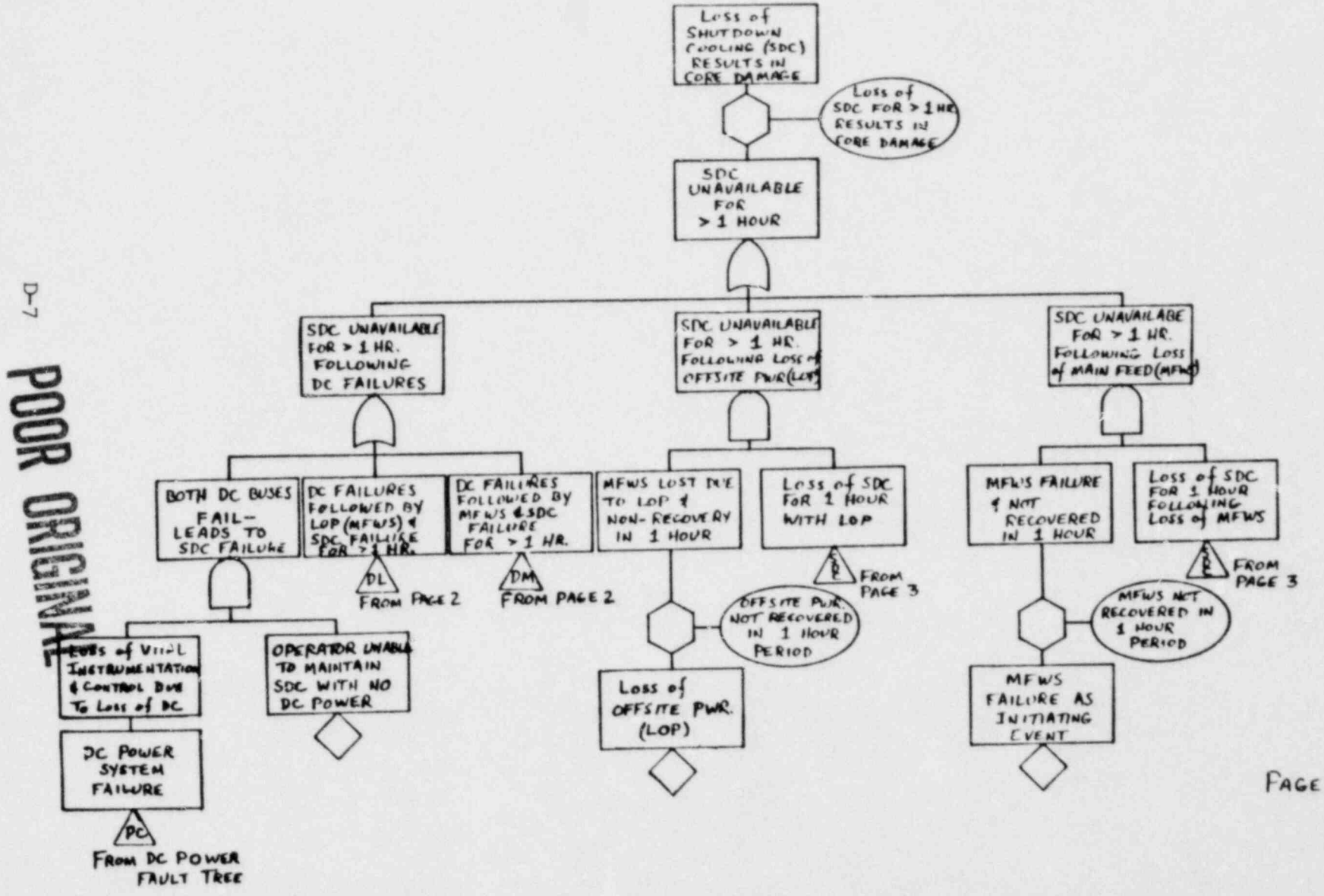


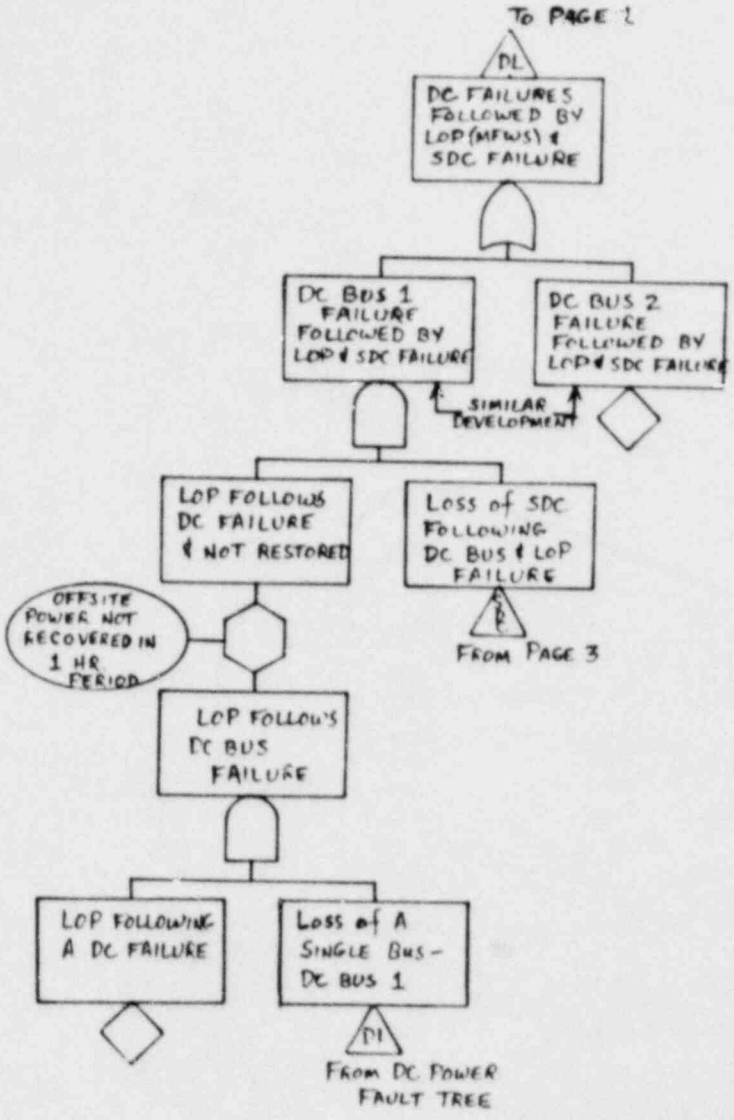
PAGE 2

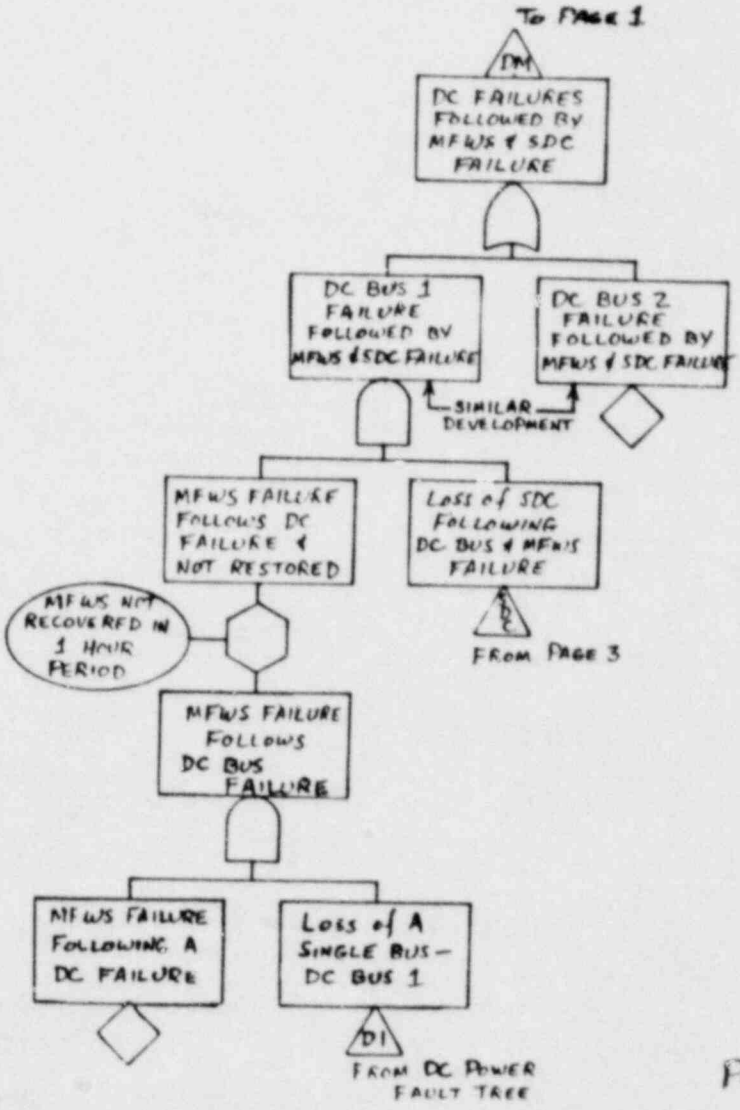
To Page 1

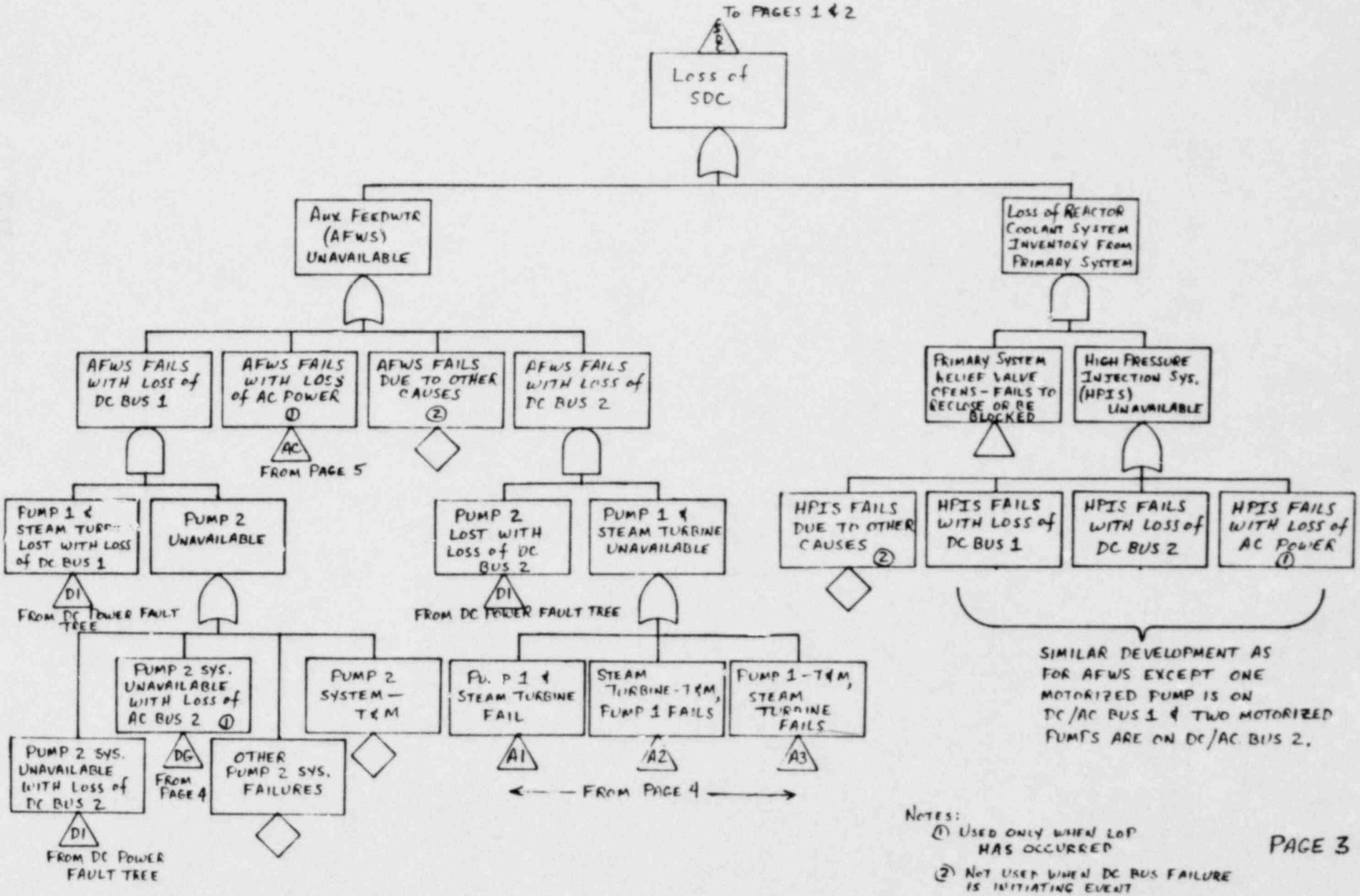


PWR SHUTDOWN COOLING FAULT TREE



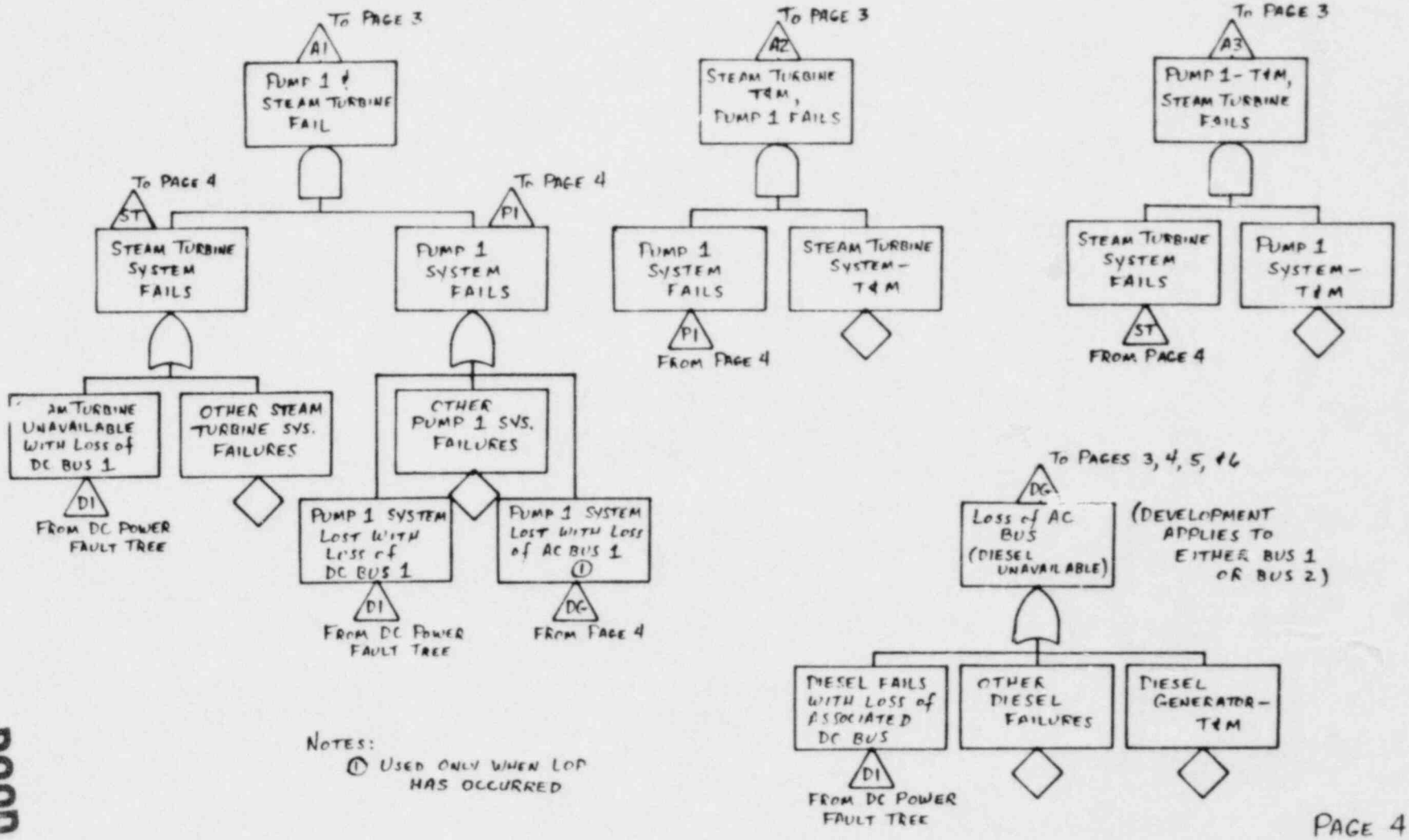






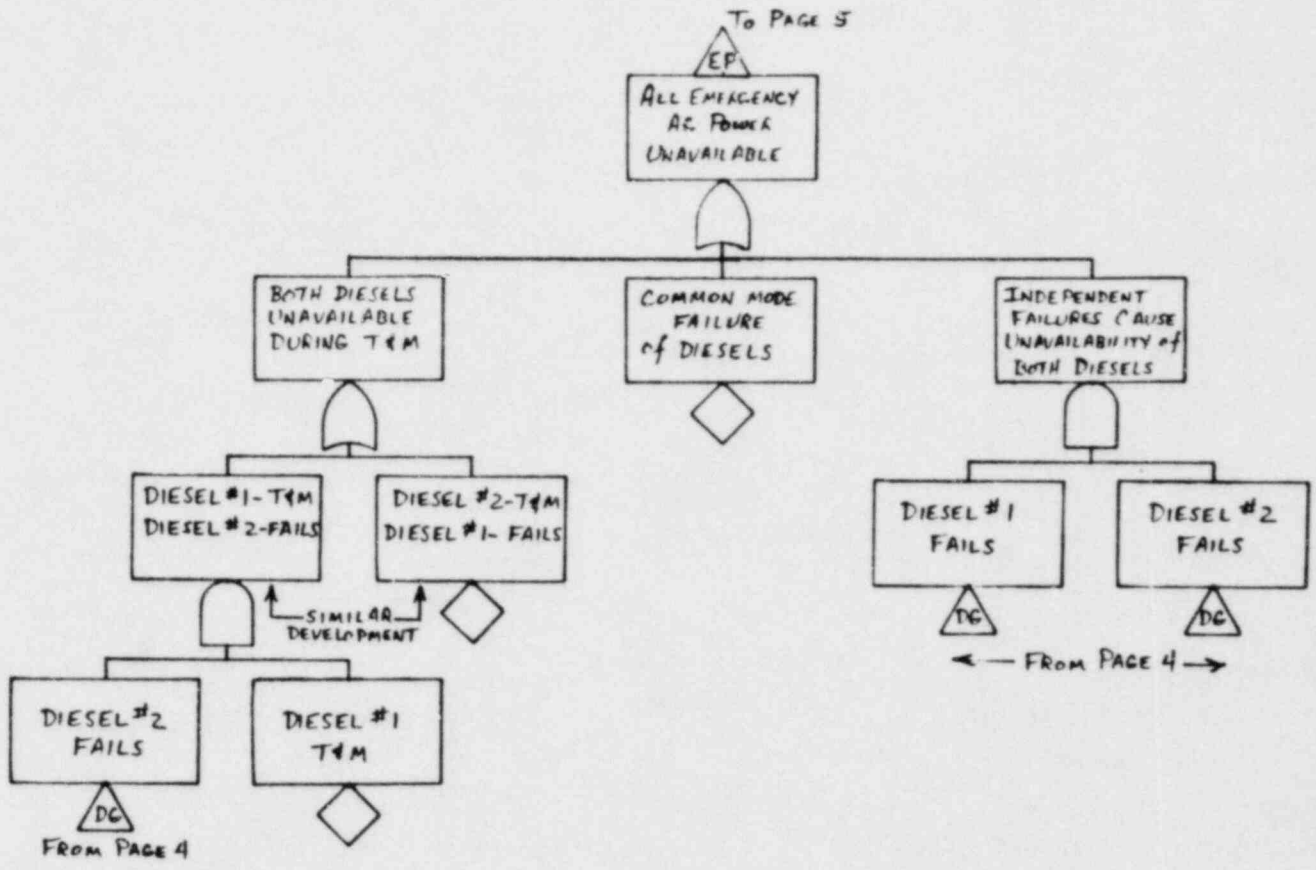
Notes:
① Used only when LOP has occurred
② Not used when DC BUS FAILURE is initiating event

PAGE 3

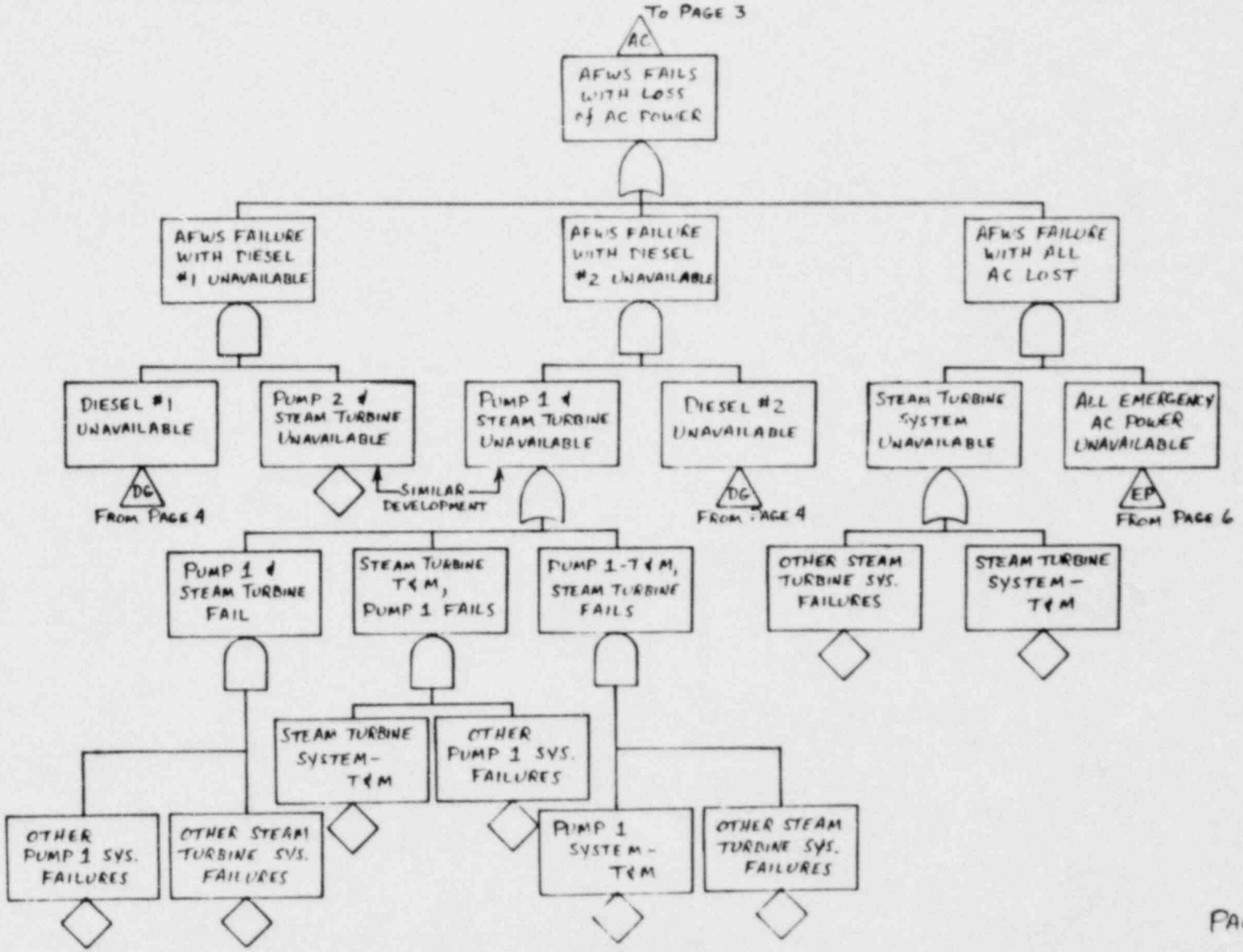


NOTES:

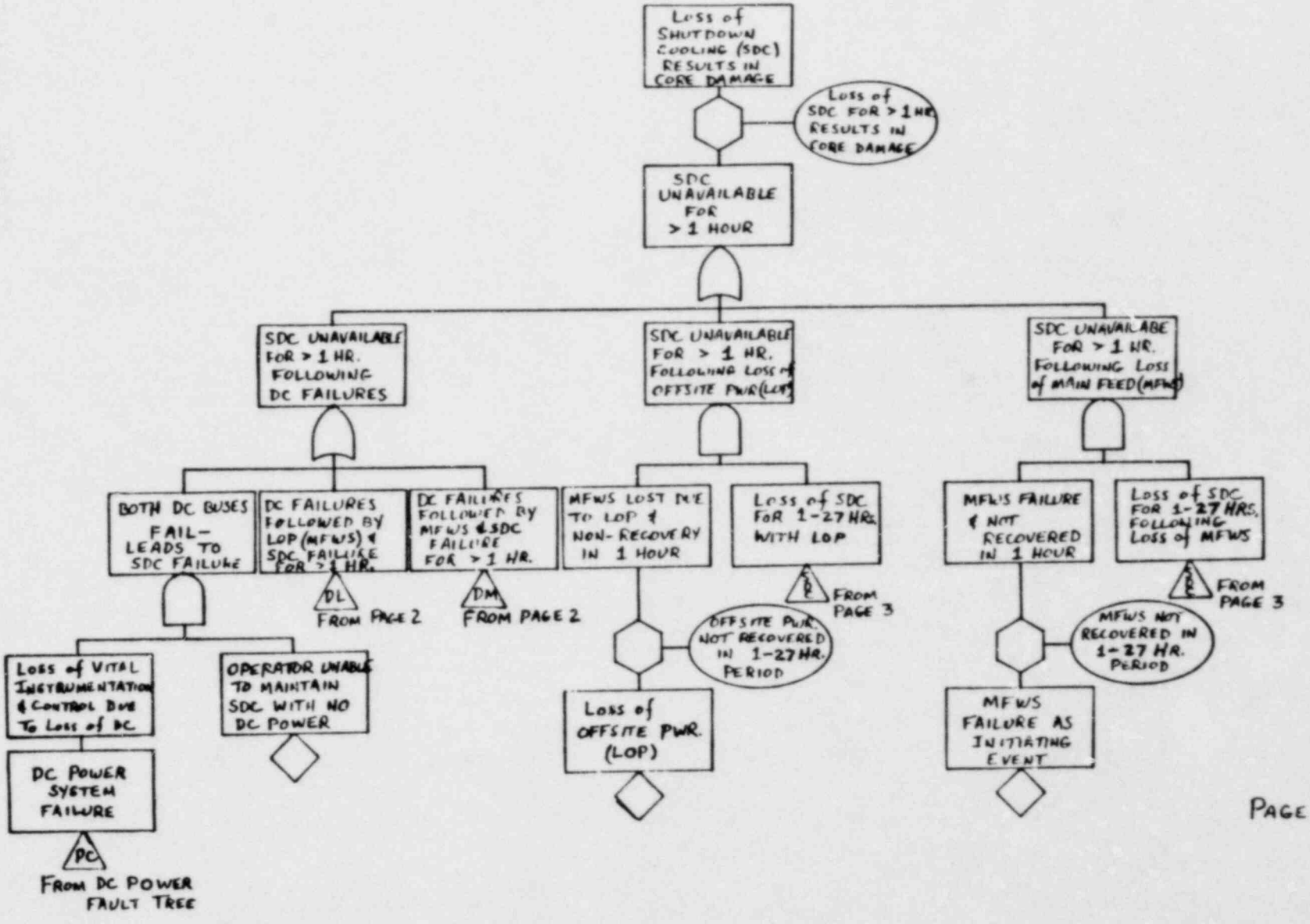
① USED ONLY WHEN LOP HAS OCCURRED

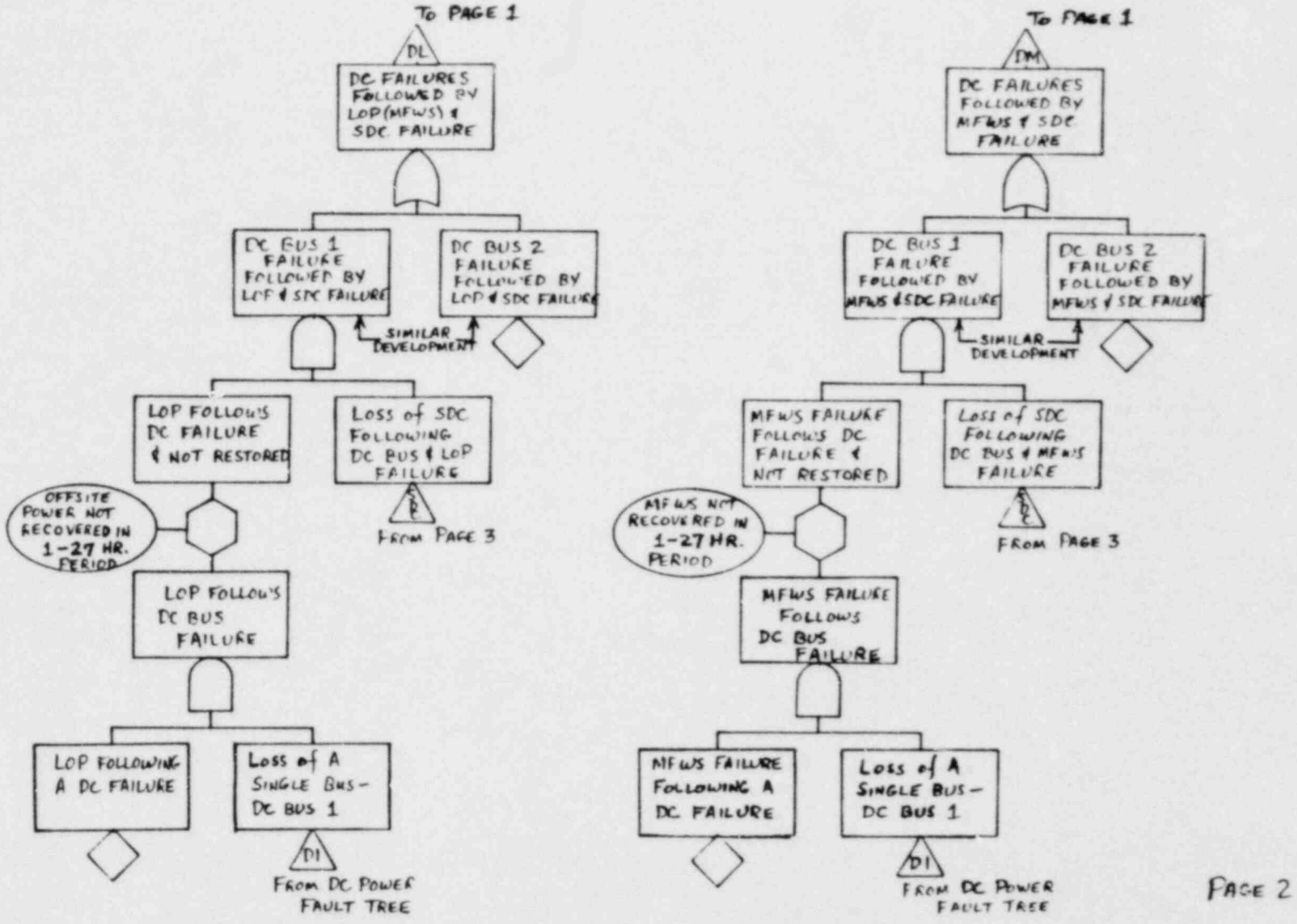


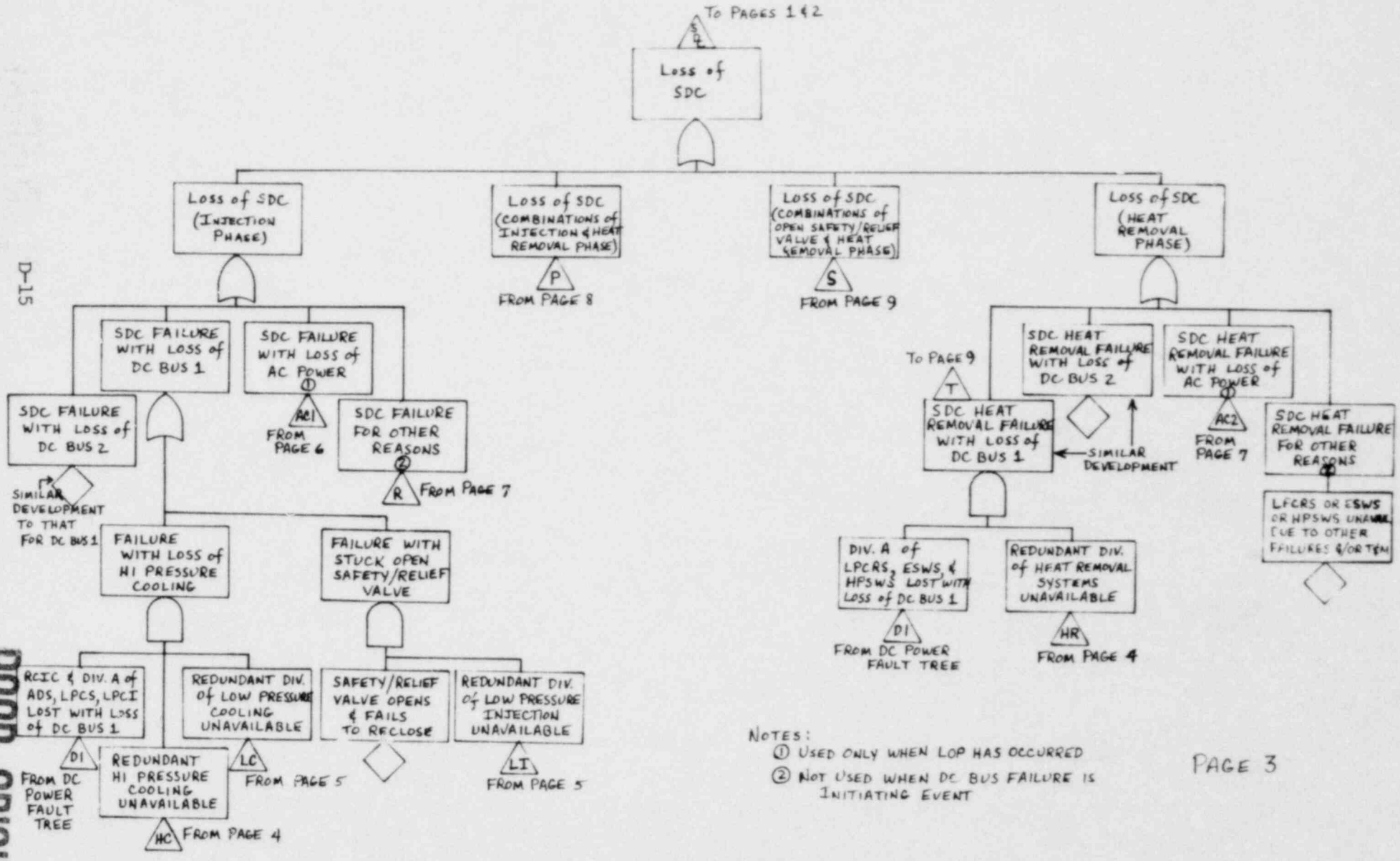
Note:
All "DG" transfers on this page exclude contribution from "Diesel Generator-T&M".



BWR SHUTDOWN COOLING FAULT TREE

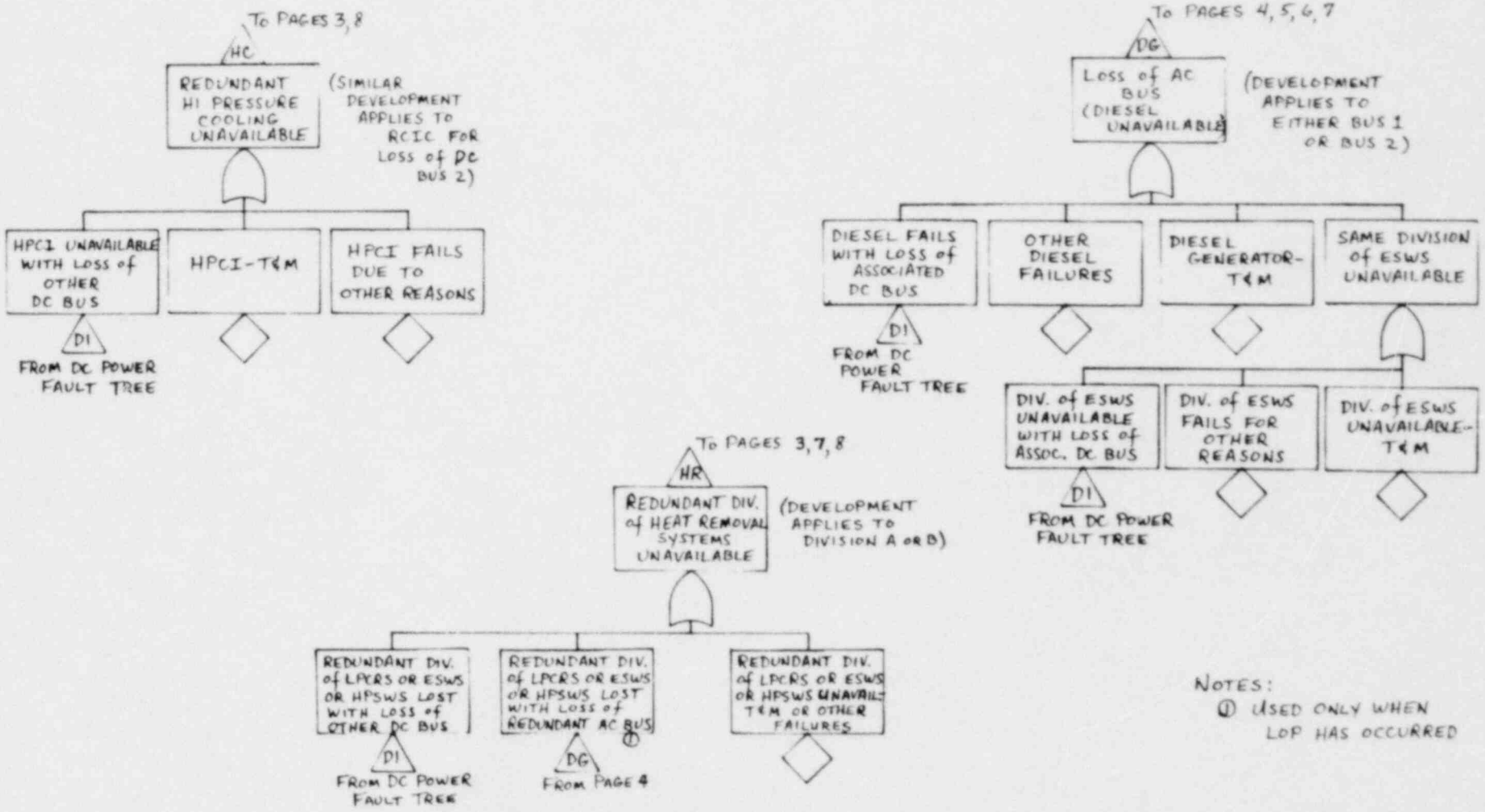




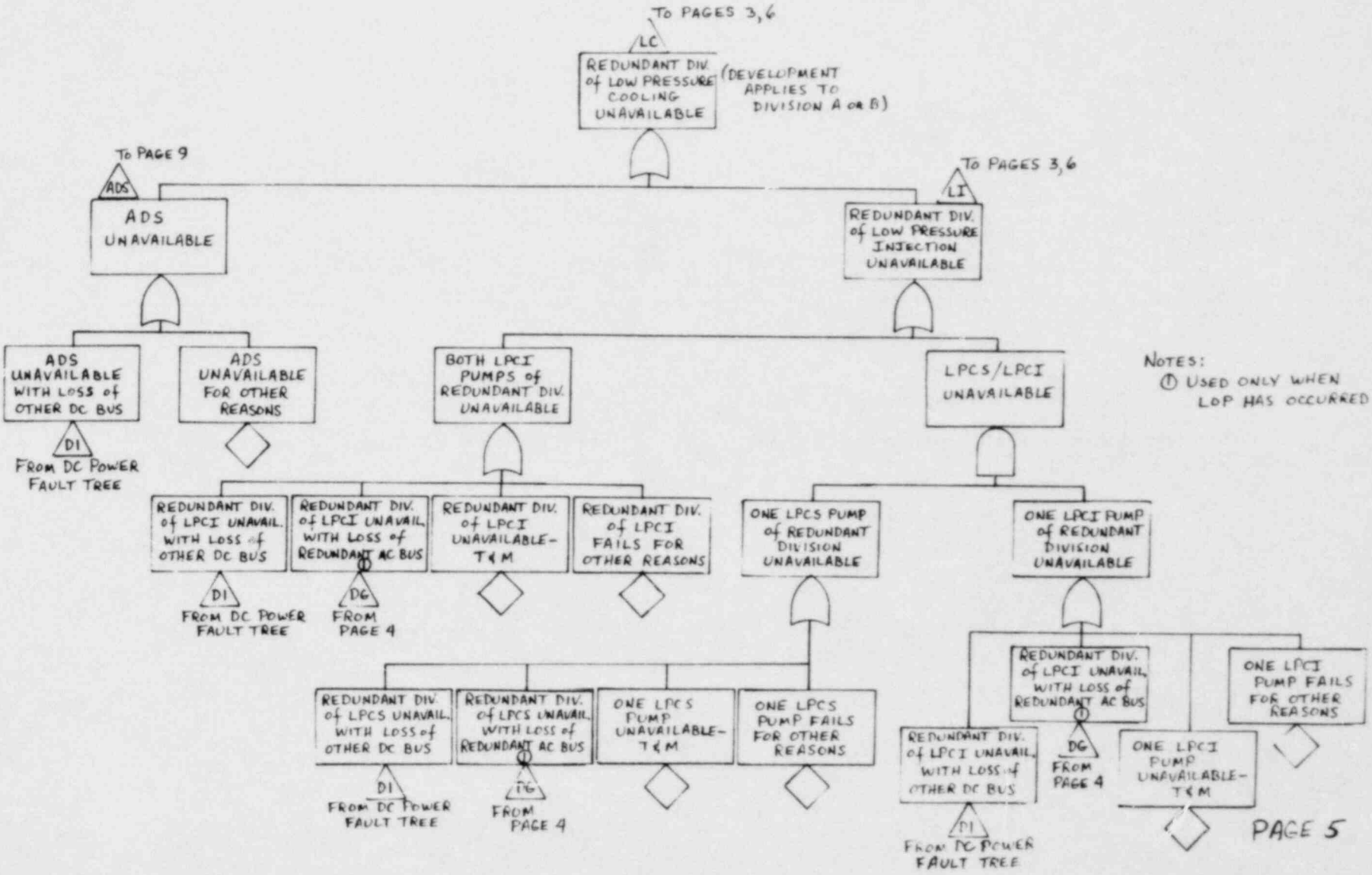


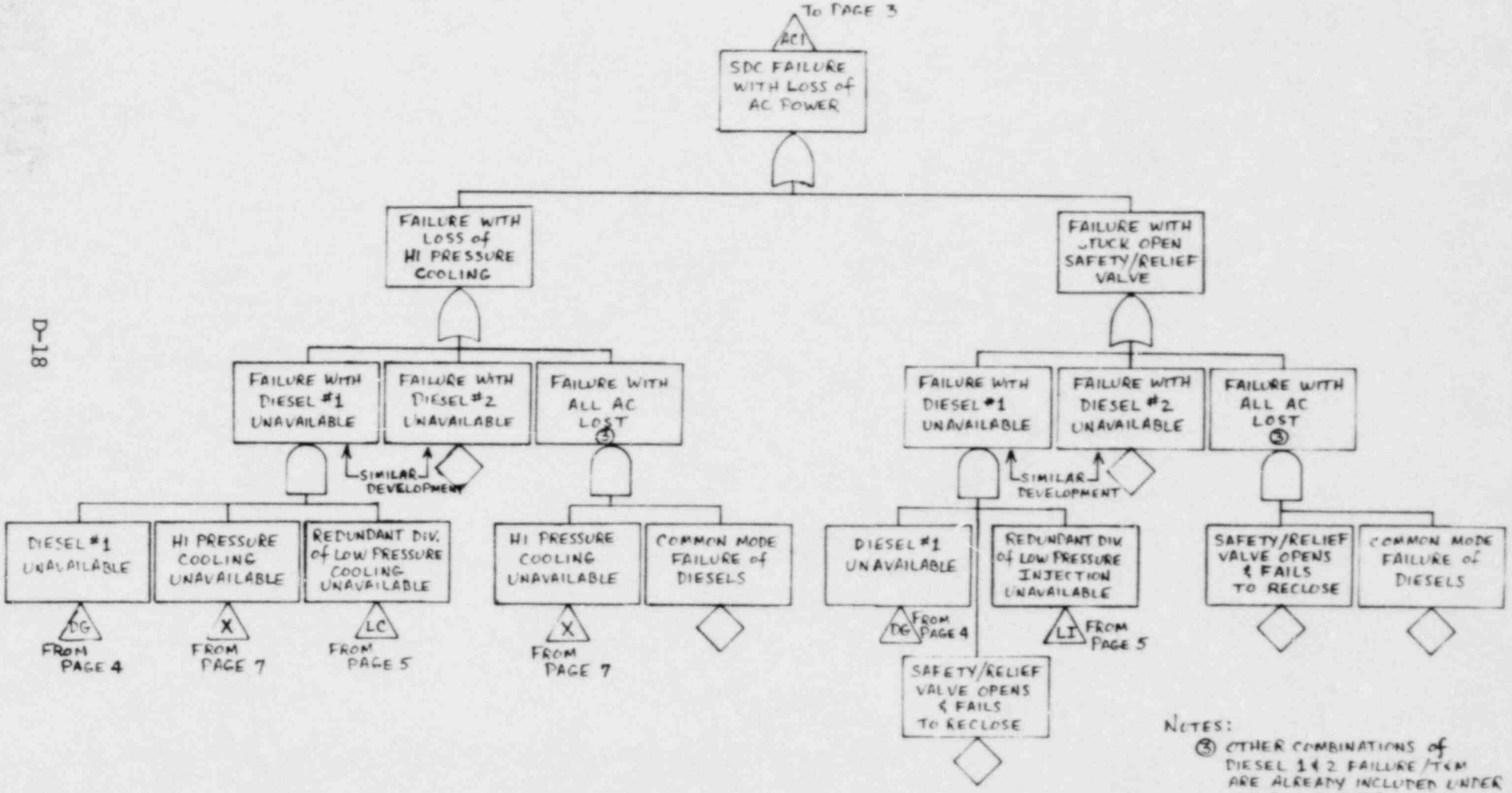
Notes:

1. Used only when LOP has occurred
2. Not used when DC Bus failure is initiating event



PAGE 4

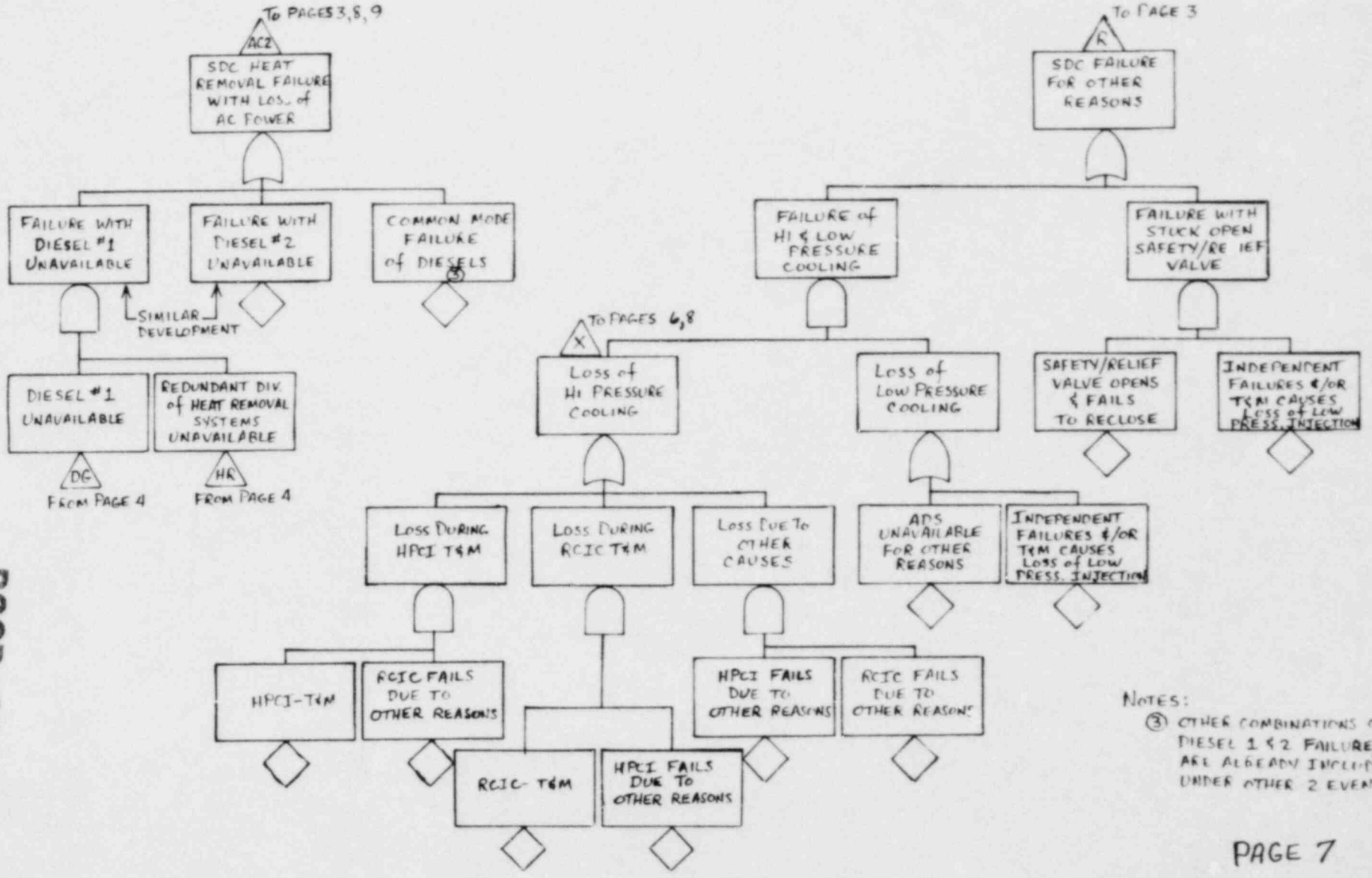




D-18

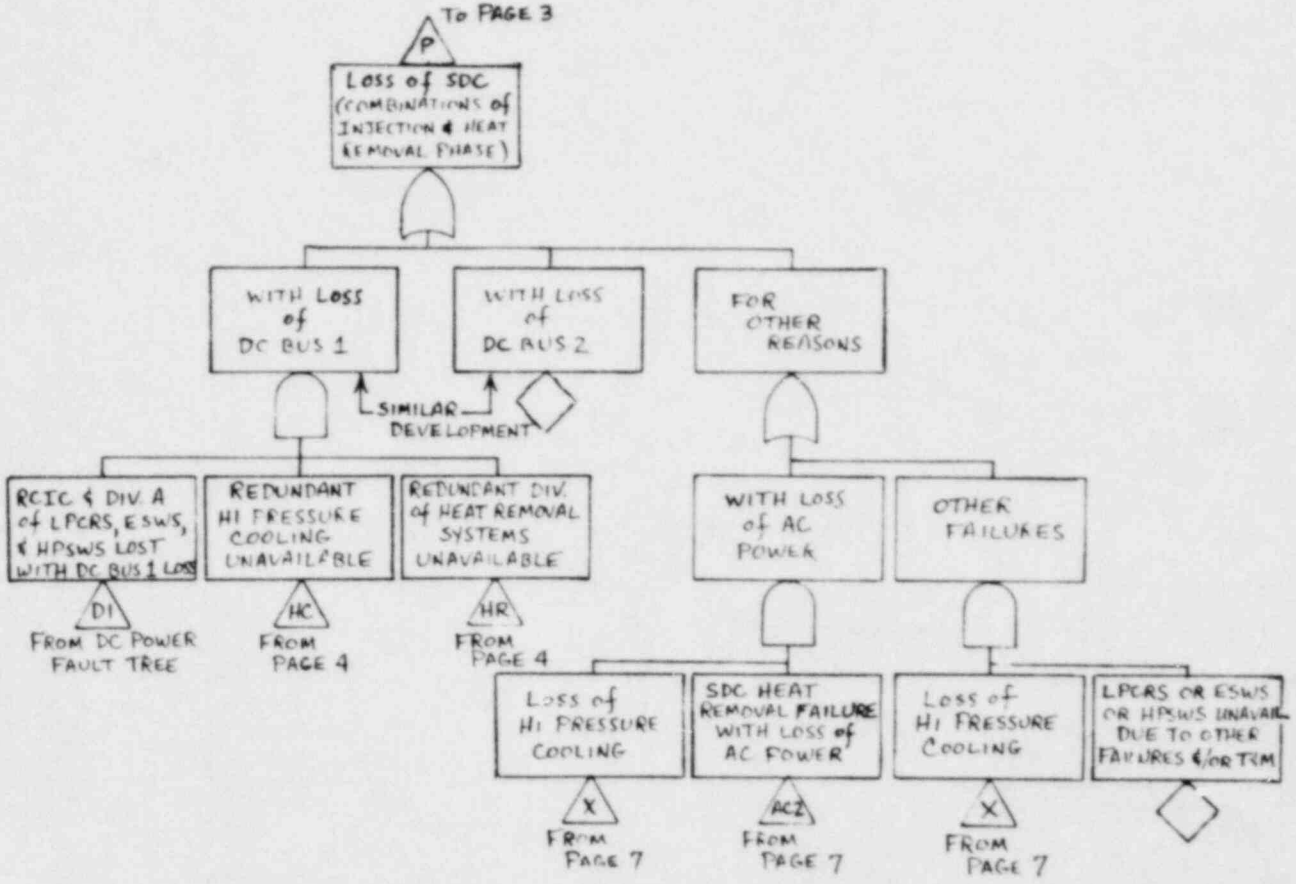
NOTES:

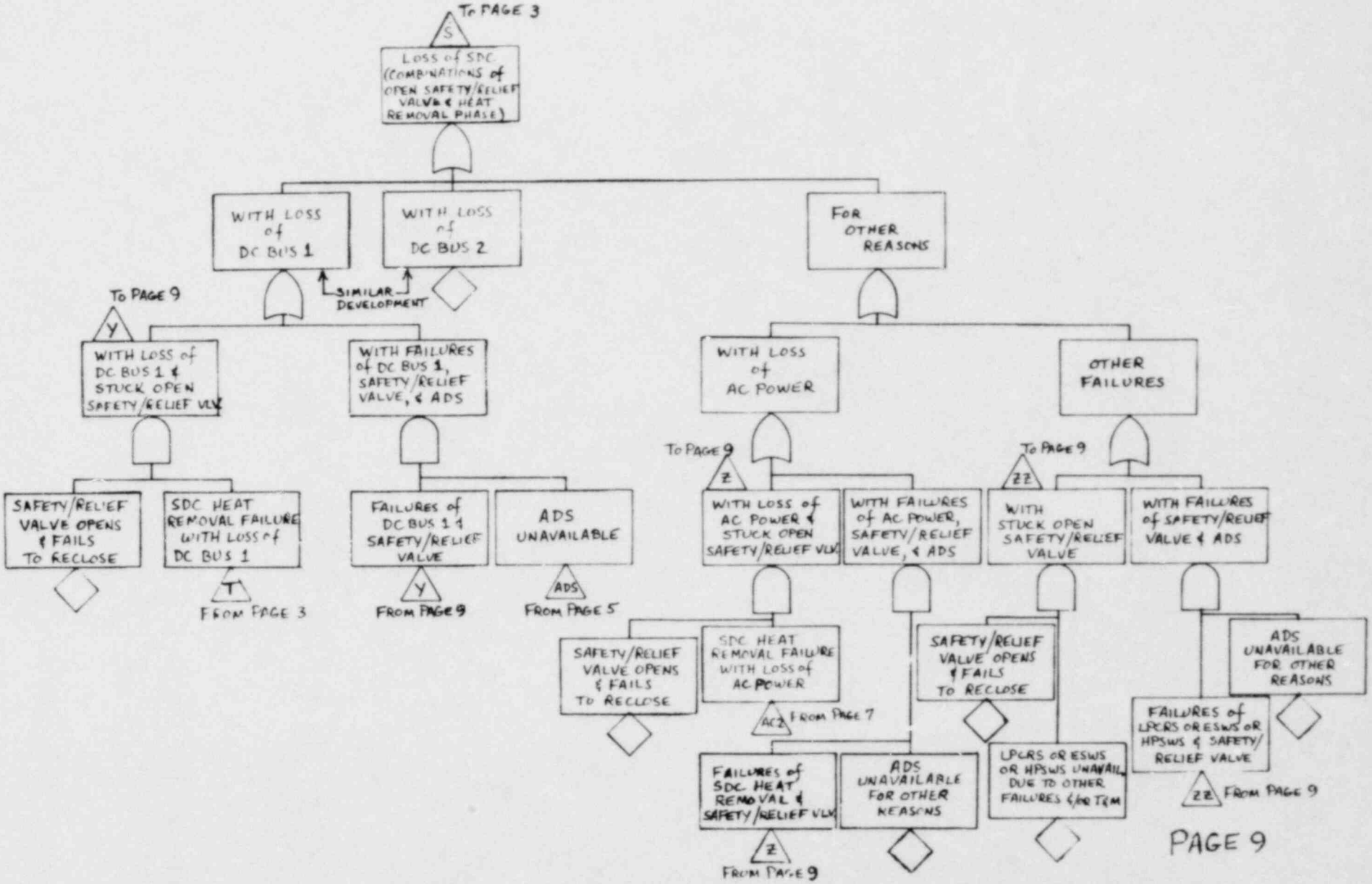
③ OTHER COMBINATIONS of DIESEL 1 & 2 FAILURE/T&M ARE ALREADY INCLUDED UNDER OTHER 2 EVENTS.



NOTES:

③ OTHER COMBINATIONS of DIESEL 1 & 2 FAILURE/T&M ARE ALREADY INCLUDED UNDER OTHER 2 EVENTS.





PAGE 9

Appendix E

DATA ANALYSIS AND PRIMARY EVENT QUANTIFICATION

This appendix contains details of the techniques used to estimate component failure probabilities and certain key undeveloped primary events of the DC power and shutdown cooling fault trees.

Component Failure Probability

Component failure probabilities were estimated using well known reliability techniques.(E1) For the most part, non-DC power system component failure rates and unavailabilities were obtained from the Reactor Safety Study. The major DC power system component failure probabilities were computed based on LER data described in Appendix C. Using data obtained from operating experience, the component failure rate was calculated as:

$$\lambda = n/T$$

where λ = failure rate for each type of component

n = number of observed component failures

T = total operating time during which component failures were observed.

The total operating time was set equal to the total number of reactor years multiplied by the total number of each component type per reactor. The LER review covered 332 reactor years of experience. It was assumed that on the average there were three DC power trains per plant, each train consisting of components comparable to one division of the minimum DC power system. Thus,

there was assumed to be 996 years of battery and battery charger experience covered in the LERs.

The failure rate estimate was usually calculated from a small failure data population. To account for statistical fluctuations in the observed failure rate, the median (50 percent confidence) failure rate estimate was calculated using the chi-square distribution such that:

$$\lambda = \frac{\chi^2_{50,2n+2}}{2T}$$

where λ = the median failure rate estimate

$\chi^2_{50,2n+2}$ = 50th percentile of the chi-square distribtuion for 2n+2 degrees of freedom

n = the number of component failures observed

T = operating time interval in which the failures were observed.

The probability that a component will fail in a given time interval, t, was calculated as:

$$P = 1-e^{-\lambda t} \sim \lambda t$$

where it has been assumed that (λt) is small. When t was equal to the component test interval, τ, and the component was assumed to be fully repaired after each test, the component unreliability was estimated as:

$$\overline{R} = \lambda\tau$$

and the average unavailability during this interval was estimated to be:

$$\bar{A} = \lambda\tau/2$$

For components which are taken out of service during periodic testing for a time τ_T, the unavailability due to testing was calculated as:

$$\bar{A}_T = \frac{\tau_T}{\tau + \tau_T}$$

A log normal probability distribution was used for the failure rate estimates for compatibility with existing data bases and computer codes used for fault tree quantification. For most components the uncertainty bounds used were taken from the RSS. Those uncertainty bounds represent the 90% confidence interval for that study. In this study, the uncertainty bounds associated with component failure rate estimates based on a few failure data points were expanded to account for the statistical uncertainty in the data. This was done by increasing the RSS uncertainty bounds proportionally to the statistical uncertainty determined from the 95 and 5 percent confidence limits of the chi-square distribution. For instance, if the uncertainty bound obtained from the RSS was a factor of 10 and the statistical uncertainty based on limited LER data was a factor of 3, the overall uncertainty was estimated as a factor of 30. Analytically, these uncertainty bounds were treated as 90% confidence intervals.

The treatment of human error and subsequent failure and uncertainty is discussed for the special cases of importance later in this appendix.

DC Power System Faults

There are several key undeveloped events in the DC power fault tree. These include battery failures due to independent and common causes and operations related failures which may affect the unavailability of one or both DC power supplies. Development of these event probabilities followed from the evaluation of the LER data. In the evaluation it was assumed that tests and inspections performed on the minimum DC power system included a weekly pilot cell check, a quarterly inspection of all battery cells and battery charger maintenance, and an eighteen month battery load test and general preventive maintenance. The buses were assumed to be connected by the bus tie breaker during the quarterly maintenance for two hours and a battery was assumed to be disconnected with the buses tied together once per year, also for two hours.

The undeveloped events involving human error and operational failures were quantified using incidents selected from the LER review as precursors. The precursor probabilities were estimated and combined with probability estimates of other system failures or operator errors which would be necessary to render the DC power supplies unavailable. Since the intent of this work was to provide a generic assessment, design and operational specifics were kept to a minimum. To some extent this has resulted in a conservative estimate of operationally related DC power failure probabilities.

The principal component and operational failure probabilities are discussed below:

1. Battery Unavailability

The LER review showed evidence that batteries may be subject to internal degradation or battery to bus connection faults, thus rendering them unavailable on demand. There were eight cases identified in which one battery division was affected and one case assessed as involving two batteries. The failure rate computed for a single battery (power to bus) was:

$$\lambda = 8 \text{ failures/996 battery years}$$
$$\sim 8 \times 10^{-3}/\text{year}$$

Since the failure population was small, the median failure rate estimate based on the chi-square distribution was used. The resulting failure rate estimate for DC power unavailable from a single battery was 8.7×10^{-3} per year. This failure rate estimate is in relatively good agreement with that reported in the RSS and IEEE 500.

Since, on the average, the quarterly maintenance was assumed to correct this situation, the unavailability was calculated to be:

$$\bar{A} = 8.7 \times 10^{-3} \times 0.25/2$$
$$\sim 1.1 \times 10^{-3}$$

An uncertainty factor of 3 was obtained from the RSS and used for the single battery failure rate. The uncertainty associated with detection of battery unavailability during the quarterly inspection was also included. This was done to reflect operating experience which showed that degraded battery conditions or battery to bus connection faults may not be detected until the more extensive yearly or refueling period maintenance is performed. An uncertainty factor of six was applied to the quarterly inspection time interval to encompass the upper bound of 18 months (6 quarters) between load tests. When applied as a lower bound, this factor slightly overlaps the weekly pilot cell inspection interval.

There was one occurrence in 996 battery years of operation which was indicative of two batteries unavailable simultaneously. The failure rate estimated for this case was:

$$\lambda = 1 \text{ occurrence}/996 \text{ battery years} \\ (x)\ 2 \text{ batteries/min system}$$

$$\sim 2 \times 10^{-3}/\text{year}$$

The median failure rate obtained using the chi-square distribution was approximately 3.4×10^{-3}/year. The unavailability was then estimated as 4.4×10^{-4} using the same approach as in the single battery case.

The same uncertainty considerations used in the single battery case were applied to the two battery estimates. However, since the failure data population was so small, the failure rate uncertainty was expanded in proportion to the statistical uncertainty on the median. A factor of 10 uncertainty was estimated for the two battery case as opposed to a factor of 3 in the single battery case.

2. Operational Errors Causing DC Power Failure

There were six occurrences identified in the LER review in which a DC power supply was made unavailable and not immediately corrected. The chi-square median probability estimate based on these occurrences is 6.7×10^{-3} in a year. The uncertainty associated with this failure probability was estimated as a factor of ten. This estimate was based on typical uncertainty factors provided in the Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (reference 10, main report).

An unavailability was not calculated for this event, since the loss of a DC power division will result in a reactor trip and, as such, is an accident initiator.

There were four cases identified in the LER review in which an operational error could have resulted in the

failure or deenergization of both DC power supplies, if the buses had been tied together. The estimated failure rate using the chi-square median was 4.7×10^{-3} per year. However, in a year of operation, the buses were assumed to be tied together for a total of 8 hours or 9.1×10^{-4} years. Thus, for this case the unreliability in a year was calculated to be:

$$\overline{R} = 4.7 \times 10^{-3}/\text{year} \times 9.1 \times 10^{-4} \text{ year}$$
$$\sim 4.2 \times 10^{-6}$$

As in the single division case, the uncertainty was estimated as a factor of 10 and the outage time was assumed to extend beyond the accident sequence recovery time.

A case in which human error during test and maintenance (T&M) operations caused the outage of two DC power supplies was identified in the LERs. The particular plant at which this incident occurred had several DC power supplies available and capability beyond that associated with the minimum DC power system. However, this incident has raised the possibility that maintenance personnel could disconnect one battery for T&M and then prior to reconnecting this battery the second could be disconnected through procedural error. The likelihood of this event lies somewhere between 10^{-5} and 10^{-3} depending on procedures, training, physical layout, and visual indicators available to the maintenance technician.

This range was estimated on the basis of values for acts of omission (e.g., failure to reconnect battery) from the human reliability handbook (reference 10). However, it must be stated that the applicability of the human error probabilities derived in that reference are somewhat in question for this case, and therefore a large uncertainty was accorded to the estimate used in this study. In consideration of this fact a median human error probability estimate of 10^{-4} with an uncertainty factor of 30 was used for this scenario.

In this scenario it was assumed that without the stabilizing effect of at least one battery on the buses, the battery chargers would trip. This may or may not happen, depending on charger design and changes in plant demand for DC power during this event. If the chargers trip, all DC power will be lost.

LER experience indicates that in approximately 50 percent of the incidents involving single DC bus failures due to operational errors, the maintenance personnel restored power very soon thereafter. The probability of performing an incorrect action in a moderate to high stress condition was estimated at between 0.1 and 0.9 in reference 10. Considering these factors, a recovery probability of 0.5 was assumed where recovery must be almost immediate.

Combining the initial human error probability with the recovery probability, a rough estimate was made for the sequence probability of 5×10^{-5} with an uncertainty factor on the order of 30.

Other Undeveloped Events

The following group of undeveloped events were quantified in this study to update RSS estimates where newer data was readily available and to modify certain estimates obtained in the RSS for better compatibility with this work.

1. Loss of Offsite Power and Recovery

There were two cases considered which involved the loss of offsite preferred power. The first involved loss of offsite power as an initiating event. Data was obtained from most operating nuclear plants regarding the number of offsite power losses at each plant.(E2) The industry-wide average frequency for total offsite power failures obtained was 0.22 events per year. An uncertainty bound of approximately 5 encompasses the best and worst offsite loss frequencies reported.

The second case regarding a loss of offsite power involved the probability of this event following

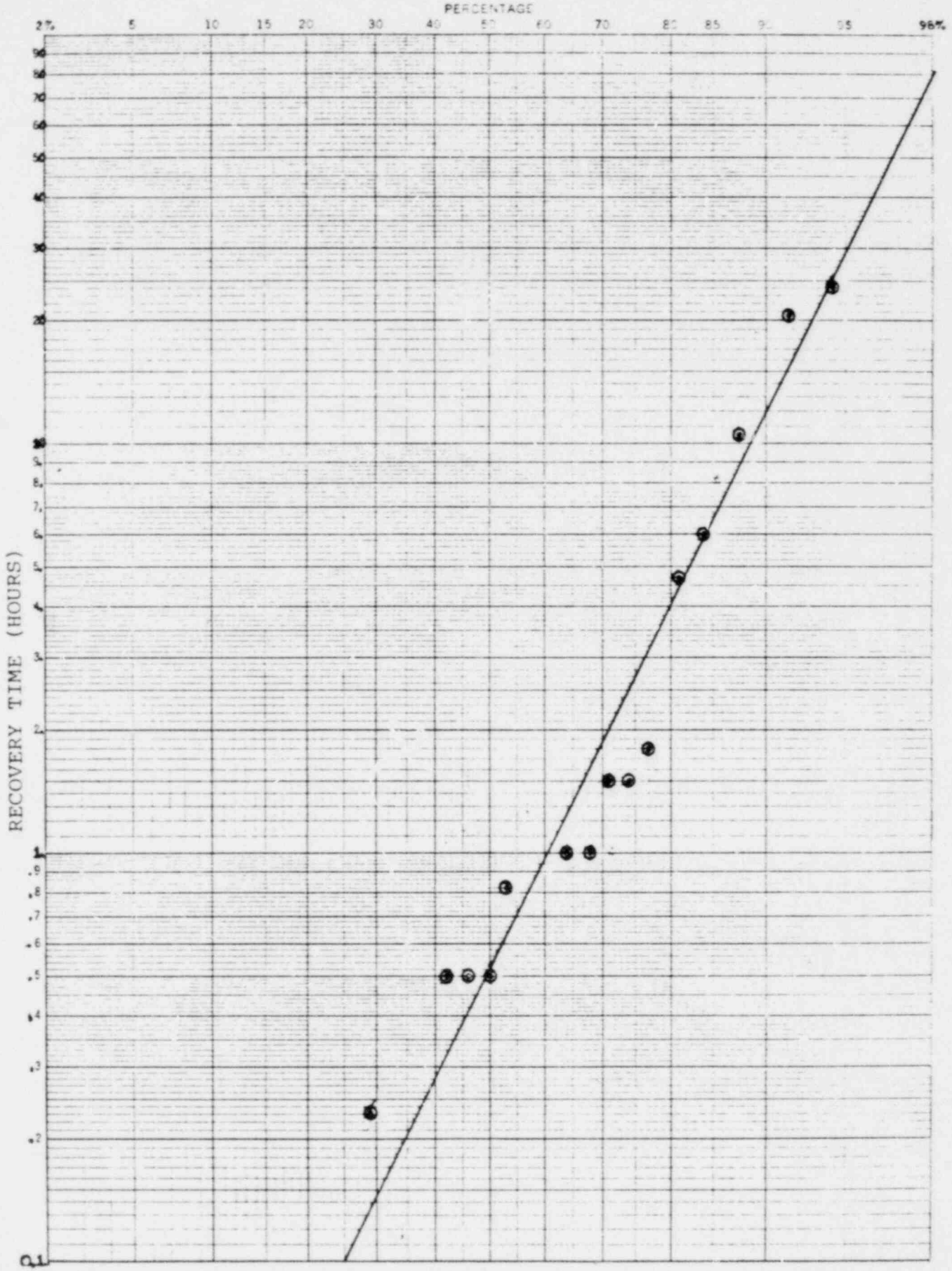
reactor trip. This was particularly important since a loss of one DC power division would result in a reactor trip. There were eight instances identified in the LERs in which a loss of offsite power followed a reactor trip. The frequency of reactor trip was estimated at approximately nine per year from EPRI NP-801.[E3] The chi-square median estimate obtained for loss of offsite power following reactor trip including cases initiated by DC power failure was 3.3×10^{-3}/reactor trip.

The likelihood that offsite power would be recovered in a given time was estimated in the Reactor Safety Study. This estimate was based on the data of one Northwestern United States power company. In this study the recovery probability was estimated using U.S. nuclear power plant data available in the LERs. Figure E-1 is a plot of that data showing the probability of recovering at least one offsite power source versus recovery time after the loss of offsite power. The mean recovery time obtained was 0.53 hours.

2. PCS/MFW Failure and Recovery

As an initiating event, the PCS/MFWS failure rates used in this study were taken from the RSS. PCS/MFWS unavailability will also follow the loss of

FIGURE E-1. RECOVERY OF OFFSITE POWER



offsite power with unity probability since many components and subsystems are dependent on that power source. The loss of a DC power supply (one bus) was assumed to affect the control and availability of electrical power for at least a part of the PCS/MFWS, and thus result in an initial system loss. However, the PCS/MFWS dependence on DC power was assumed to be evenly divided between the two DC power divisions. As such, up to 50% of the MFWS water delivery capability was assumed to be available through operator action following a single DC bus failure.

The recovery of main feedwater following its loss as an initiating event was estimated considering the RSS data, the potential interaction with DC power supply failures, and operator actions which would be directed at initiating alternate cooling systems. In this study the only accidents of interest which include a main feedwater failure as an accident initiator also include the failure or unavailability of shutdown heat removal systems. The Reactor Safety Study reported an estimated range of 10^{-3} to 10^{-1} for the probability that the main feedwater system would not be restored within approximately one hour after its loss. In another study[E4] the possibility that operators would exert most or all of their attention in an attempt to actuate the emergency shutdown cooling systems was evaluated

and a mean restoration probability of 10^{-1} was estimated. The upper bound on this probability is 1.0; that is, MFW flow to the steam generators in a PWR or the reactor vessel in a BWR would not be restored within one hour with unity probability. Considering these evaluations, the MFW/PCS recovery probability was estimated to lie between 10^{-2} and 1.0 with a median probability of 10^{-1}. The sensitivity of the results to this estimate is provided in section 6 of the main report. For the BWR there were accident sequences in which the PCS/MFWS recovery in 2 and 27 hours could avert suppression pool failure and would allow operators to establish a safe shutdown cooling condition. For this case, the greater likelihood of operators attempting the recovery of the normal heat removal systems in two hours rather than one hour was considered. The RSS nonrecovery probability of 10^{-2} with an uncertainty factor of 10 was used for accident sequences in which PCS/MFWS recovery in two hours was required. For the 27 hour case, the RSS nonrecovery probability of 7×10^{-3} was used.

3. Transient Induced LOCA Probability

Both the PWR and the BWR have primary system pressure relief valves which have a history of valve closure failures during transients. The probability that a pilot operated relief valve (PORV) would open and remain stuck open was developed considering U.S. nuclear power

plant experience which was reported[E5] following the Three Mile Island accident. The failure probability of a PORV to reclose once it has opened has been estimated as 2×10^{-2}/demand. A limited number of PORV openings per year are expected with the reactor trip and pressure relief setpoint changes made as part of the "TMI fixes." The PORV demand rate was estimated from reference E5 as 0.2 per reactor year for all transients except loss of offsite power. It was assumed that a loss of offsite power will result in a PORV opening. As a result of the TMI accident, operators are well informed about the need to isolate an uncontrolled PORV discharge. It was conservatively estimated that an operator would have a 50 percent or greater probability of taking appropriate actions to isolate a stuck open PORV. The probability of a transient induced LOCA in a PWR was then estimated as 2×10^{-3} per reactor year.

For the BWR it was assumed that all transients of concern in this study would result in at least one safety/relief valve (SRV) opening with a probability of 10^{-1} that one valve would remain in a stuck open position. This estimate is based on the value reported in the RSS. A more recent review of SRV malfunctions at BWRs[E6] shows reasonable agreement with this estimate.

TABLE E-1. Primary Event Probabilities Used in Quantification of DC Power System Fault Tree

Event Description	Exposure Time (hrs)	Frequency or Median Probability	Uncertainty Factor
DC Bus(es) fail during T&M (independent failures)	8	$< 10^{-7}$	-
Loss of a single bus (non-T&M)			
Operational Error Causes Loss of a DC bus	8752	6.7×10^{-3}	10
	1	ϵ	-
Loss of AC input to charger	-	0.22/yr.	5
Charger circuit breaker opens	8752	8.8×10^{-3}	3
	1	1.0×10^{-6}	3
Charger output otherwise unavailable to DC bus	8752	2.5×10^{-2}	3
	1	2.8×10^{-6}	3
Battery output fuse opens	8752	8.8×10^{-3}	3
	1	1.0×10^{-6}	3
Battery output otherwise unavailable to DC bus	2190	1.1×10^{-3}	3
Common mode; tie breaker closed			
Tie breaker or bus shorts to DC return	8	ϵ	-
Batteries discharge into charger short	8	ϵ	-
Design error causes both buses to fail	8	ϵ	-
T&M error results in loss of both buses	8	5×10^{-5}	30
Operational errors cause loss of both buses	8	4.2×10^{-6}	10
Common mode; during normal operation			
Operational error causes loss of both buses	8752	ϵ	-
Common cause failure of ventilation system	3752	ϵ	-
Loss of AC input to chargers	-	0.22/yr.	5
Common cause failure of both chargers	8752	ϵ	-
Output from both batteries unavailable to DC buses	-	4.4×10^{-4}	10

TABLE E-2. Primary Event Probabilities Used in Quantification of PWR Shutdown Cooling Fault Tree

Event Description	Frequency or Median Probability	Uncertainty Factor
Loss of SDC for > 1 hr. results in core damage	1.0 (see text discussion)	-
Operator unable to maintain SDC with no DC	1.0 (see text discussion)	-
Initiating Events		
Loss of offsite power (LOP)	0.22/yr.	5
Offsite power not recovered in 1 hour	0.39	2
MFWS failure as initiating event	3/yr.	2
MFWS not recovered in 1 hour	1.0×10^{-1} (see note 1)	10
LOP following a DC failure	3.3×10^{-3}	10
MFWS failure following a DC failure	1.0 (see text discussion)	-
Emergency AC		
Other diesel failures	3.0×10^{-2}	3
Diesel generator - T&M	6.4×10^{-3}	3
Common mode failure of diesels	3.3×10^{-3}	10
Primary system relief valve opens and fails to reclose or be blocked	1.0×10^{-2} (w/LOP) 2.0×10^{-3} (w/o LOP)	10 10
Auxiliary Feedwater System		
AFWS fails due to other causes	3.3×10^{-5}	10
Other pump 1 (or 2) system failures	1.6×10^{-2}	3
Pump 1 (or 2) system - T&M	2.1×10^{-3}	3
Other steam turbine system failures	$1.0 \times 10-2$	3
Steam turbine system - T&M	7.9×10^{-3} (see note 2) 2.1×10^{-3}	3

TABLE E-2. (Continued)

Event Description	Frequency or Median Probability	Uncertainty Factor
High Pressure Injection System		
HPIS fails due to other causes	9.0×10^{-3}	3
Pump 1 system failure or T&M	1.0×10^{-1}	3
Pump 2 and 3 systems fail or T&M	1.2×10^{-2}	3

TABLE E-3. Primary Event Probabilities Used in Quantification of BWR Shutdown Cooling Fault Tree

Event Description	Frequency or Median Probability	Uncertainty Factor
Loss of SDC for > 1 hr. results in core damage	1.0 (see text discussion)	-
Operator unable to maintain SDC with no DC	1.0 (see text discussion)	-
Initiating Events		
Loss of offsite power (LOP)	0.22/yr.	5
Offsite power not recovered in 1 or 2 hours	0.39	2
Offsite power not recovered in 27 hours	0.05	2
PCS failure as initiating event	3/yr.	2
PCS not recovered in 1 hour	1.0×10^{-1} (see note 3)	10
PCS not recovered in 2 hours	1.0×10^{-2}	10
PCS not recovered in 27 hours	7.0×10^{-3}	10
LOP following a DC failure	3.3×10^{-3}	10
PCS failure following a DC failure	1.0 (see text discussion)	-
Emergency AC (see note 4)		
Other diesel failures	3.0×10^{-2}	3
Diesel generator - T&M	6.4×10^{-3}	3
Common mode failure of diesels	3.3×10^{-3}	10

TABLE E-3. (Continued)

Event Description	Frequency or Median Probability	Uncertainty Factor
Safety/relief valve opens and fails to reclose	1.0×10^{-1}	10
High pressure coolant injection system		
HPCI - T&M	7.5×10^{-2}	1.5
HPCI fails due to other reasons	1.3×10^{-2}	1.5
Reactor core isolation cooling system		
RCIC - T&M	6.9×10^{-2}	1.5
RCIC fails due to other reasons	1.1×10^{-2}	1.5
Automatic depressurization system		
ADS unavailable for other reasons	5.0×10^{-3}	1.5
Low pressure coolant injection system		
Redundant division of LPCI unavailable - T&M	5.8×10^{-3}	3
Redundant division of LPCI fails for other reasons	1.0×10^{-3}	3
One LPCI pump unavailable - T&M	1.1×10^{-2}	3
One LPCI pump fails for other reasons	2.0×10^{-3}	3
Low pressure core spray system		
One LPCS pump unavailable - T&M	2.9×10^{-2}	3
One LPCS pump fails for other reasons	3.0×10^{-3}	3
Independent failure and/or T&M causes loss of Low Pressure Injection (LPCI and LPCS)	ϵ	-

TABLE E-3. (Concluded)

Event Description	Frequency or Median Probability	Uncertainty Factor
Emergency Service Water System		
Division of ESWS unavailable - T&M - for 1, 2 or 27 hours	ϵ	-
Division of ESWS fails for other reasons for 1 or 2 hours	1.1×10^{-4}	3
Division of ESWS fails for other reasons for 27 hours	1.1×10^{-4}	3
Combinations of LPCRS, ESWS, and HPSWS		
LPCRS or ESWS or HPSWS unavailable due to other failure and/or T&M - for 1 or 2 hours	2.4×10^{-4}	3
for 27 hours	1.6×10^{-4}	3
Redundant division of LPCRS or ESWS or HPSWS unavailable - (given other division is unavailable due to partial AC or DC loss)		
T&M or other failures - for 1 or 2 hours	2.5×10^{-4}	3
for 27 hours	2.0×10^{-4}	3

Notes for Tables E-1, E-2, and E-3

Note 1: In cases of RCS INTEGRITY failure by a failed open PORV or small LOCA, followed by failure of HIGH PRESSURE MAKEUP, it is assumed that recovery of MFWS is of little value in mitigating the event since blowdown continues to occur through the open PORV or small break. For this case, a nonrecovery factor of 1.0 was used for 'MFWS not recovered in 1 hour' instead of the value shown.

Note 2: Two values are given for the auxiliary feedwater system steam turbine T&M contribution. If AC bus 1 has failed, use the larger value since T&M contribution of the DC steam admission valve is also a factor. Otherwise use the smaller value.

Note 3: In cases of RCS INTEGRITY failure by a failed open safety/relief valve or small LOCA, followed by failure of RESIDUAL HEAT REJECTION, it is assumed that recovery of MFWS is of little value in mitigating the event for similar reasons as given in Note 1 above. For this case, a nonrecovery factor of 1.0 was used for 'MFWS not recovered in 1 hour' instead of the value shown.

Note 4: An additional nonrecovery factor of 0.1 was used for the emergency AC components for the 27 hour sequences.

References for Appendix E

E1 "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems," IEEE Standard 352-1975.

E2 U.S. Nuclear Regulatory Commission, Memorandum from G. Lainas to P. Baranowsky transmitting informal report, "Loss of Offsite Power Survey Status Report," April 25, 1980.

E3 F. L. Leverenz, Jr., et al, "ATWS: A Reappraisal, Part III, Frequency of Anticipated Transients," EPRI Report NP-801, July 1978.

E4 G. J. Kolb, et al, "Reactor Safety Study Methodology Applications Program: Oconee #3 PWR Power Plant," NUREG/CR-1659/2 of 4, SAND80-1897/2 of 4, Sandia National Laboratories, Albuquerque, NM, Battelle Columbus Laboratories, Columbus, Ohio, January 1981.

E5 U.S. Nuclear Regulatory Commission Special Inquiry Group Report, "Three Mile Island," Vol. 2, January 1980.

E6 "Technical Report on Operating Experience with BWR Pressure Relief Systems," NUREG-0462, Staff Report, July 1978.

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

ADS	Automatic Depressurization System
AFWS	Auxiliary Feedwater System
BWR	Boiling Water Reactor
ESWS	Emergency Service Water System
FMEA	Failure Modes and Effects Analysis
HPCI	High Pressure Coolant Injection
HPIS	High Pressure Injection System
HPSWS	High Pressure Service Water System
LER	Licensee Event Report
LOCA	Loss of Coolant Accident
LOP	Loss of Offsite Power
LPCI	Low Pressure Coolant Injection
LPCRS	Low Pressure Coolant Recirculation System
LPCS	Low Pressure Core Spray
MFW, MFWS	Main Feedwater (System)
NRC	Nuclear Regulatory Commission
PCS	Power Conversion System
PORV	Pilot Operated Relief Valve
PWR	Pressurized Water Reactor
RCS	Reactor Coolant System
RHR, RHRS	Residual Heat Removal (System)
RSS	Reactor Safety Study
SDC	Shutdown Cooling
SRV	Safety Relief Valve
T&M	Test and Maintenance

NRC FORM 335 (7-77) U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*
NUREG-0666

4. TITLE AND SUBTITLE *(Add Volume No., if appropriate)*
A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants

2. *(Leave blank)*

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S) P. W. Baranowsky
Alan M. Kolaczkowski
Mario A. Fedele

5. DATE REPORT COMPLETED
MONTH: March YEAR: 1981

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Division of Systems and Reliability Research
Washington, DC 20555

DATE REPORT ISSUED
MONTH: April YEAR: 1981

6. *(Leave blank)*

8. *(Leave blank)*

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Same as 9, above.

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.

13. TYPE OF REPORT
Technical

PERIOD COVERED *(Inclusive dates)*

15. SUPPLEMENTARY NOTES

14. *(Leave blank)*

16. ABSTRACT *(200 words or less)*

A probabilistic safety assessment was performed as part of the Nuclear Regulatory Commission generic safety task A-30, "Adequacy of Safety Related DC Power Supplies." Event and fault tree analysis techniques were used to determine the relative contribution of DC power related accident sequences to the total core damage probability due to shutdown cooling failures. It was found that a potentially large DC power contribution could be substantially reduced by augmenting the minimum design and operational requirements. Recommendations included (1) requiring DC power divisional independence, (2) improved test, maintenance, and surveillance, and (3) requiring core cooling capability be maintained following the loss of one DC power bus and a single failure in another system.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

DC Power
Reliability
Probabilistic Safety Analysis

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS *(This report)*
Unclassified

21. NO. OF PAGES

20. SECURITY CLASS *(This page)*
Unclassified

22. PRICE
$