MITNE-184

AN ACCIDENT PROBABILITY ANALYSIS AND DESIGN EVALUATION OF THE GAS-COOLED FAST BREEDER REACTOR DEMONSTRATION PLANT

P.De Laquil III,
D.D.Lanning
N.C. Rasmussen

January 1976

Massachusetts Institute of Technology
Department of Nuclear Engineering
Cambridge, Massachusetts

Copy 2

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

DEPARTMENT OF NUCLEAR ENGINEERING

Cambridge, Massachusetts

AN ACCIDENT PROBABILITY ANALYSIS AND DESIGN EVALUATION OF THE GAS-COOLED FAST BREEDER REACTOR DEMONSTRATION PLANT

by

P. De Laquil III, D.D. Lanning, and N.C. Rasmussen

January 1976

MITNE-184

AN ACCIDENT PROBABILITY ANALYSIS AND DESIGN EVALUATION OF THE GAS-COOLED FAST BREEDER REACTOR DEMONSTRATION PLANT

by

Pascal De Laquil III

Submitted to the Department of Nuclear Engineering on January 16, 1976 in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Abstract

The accident analysis methodology of the Reactor Safety Study (RSS) for light water reactors is extended for application to the design evaluation of a gas-cooled fast breeder reactor (GCFR). Specifically, the conceptual design of the 300 MW(e) demonstration plant is studied, and a detailed description of the design is provided.

The probability of core-melt accidents resulting from the loss of adequate decay heat removal following a reactor shutdown is investigated in detail. Also, the reactor shutdown initiating events are grouped into categories which cover the spectrum of these events. For each initiating event category, a median point estimate of the core-melt probability is developed using failure data from the RSS. Sensitivity analyses are performed in which the effect on the core-melt probability is determined for variations in the input parameters.

By the methods developed in this report, the overall probability of a core meltdown is estimated to be 7×10^{-6} per year. Common mode failures are included in this value. The common mode failure uncertainty is considered to be the major contributor to the uncertainty in the overall probability. Considering the uncertainty in the common mode failure probabilities yields a range for the core-melt probability of 3×10^{-5} to 3×10^{-6} per year.

In conclusion, the design of the GCFR demonstration plant shutdown cooling systems is shown to be quite well

balanced. Also, the results of the sensitivity analyses are applied to determine the effect of potential shutdown cooling system design changes.

Thesis Supervisor: Norman C. Rasmussen
Title: Professor of Nuclear Engineering

Thesis Supervisor: David D. Lanning
Title: Professor of Nuclear Engineering

Acknowledgements

The author wishes to acknowledge the special guidance and encouragement offered by both of his advisors, Professors Norman C. Rasmussen and David D. Lanning.

Financial support provided under a research contract by the General Atomic Company is gratefully acknowledged, and a special thanks is due James A. Larrimore for his guidance and encouragement and Archie Kelley, whose insightful comments have been especially appreciated.

Computer calculations were performed at the M.I.T. Information Processing Center, and Rachel Morton provided very helpful programming assistance.

The author would also like to acknowledge the Reactor Safety Study Group for the invaluable information which their study provided, and the many typists who ably handled the typing of this manuscript, especially Clare Egan.

TABLE OF CONTENTS

APPENDIX A - GCFR SUBSYSTEM DESCRIPTIONS AND RELIABILITY QUANTIFICATIONS

LIST OF FIGURES

FIGURE NUMBER PAGE

FIGURE NUMBER PAGE

FIGURE NUMBER PAGE

FIGURE NUMBER PAGE

FIGURE NUMBER PAGE

LIST OF TABLES

Chapter 1

Scope and Intent of Research

1.1 Introduction

The design of a nuclear power plant requires the consideration of a number of factors. The more important of these include safety, economics, reliability, and environmental impacts. In terms of an overall assessment, only the economics involved with designing, building, and operating the plant have generally been quantified. In the past few years, efforts have been started toward including environmental impacts quantitatively in the overall cost-benefit analysis of the plant. However, while safety has always been a major concern influencing nuclear power plant design, attempts are just beginning toward quantifying this aspect of the overall design process.

The nuclear power industry in the United States was the first major industry in which the safety of the public was a legislated concern prior to the establishment of the industry. The design review and safety analysis of the regulatory staff of the Nuclear Regulatory Commission (formerly the Atomic Energy Commission) before the construction and operation of an electricity generating nuclear power plant are unprecedented,

and these efforts are in part responsible for the presently excellent safety record of the industry. The philosophy of the regulatory staff in its review process has generally been that of the skeptic -- constantly asking, "What if ...?" and "Show that ..." -- in order to test, and verify when possible, the basic design assumptions of the plant. This approach has led to a high quality of safety, but only recently has a detailed quantitative assessment of nuclear power plant safety been performed for U.S. reactors. This study, known as the Reactor Safety Study (RSS) [1], demonstrated in the United States the usefulness of analytical techniques in assessing power plant safety. This has subsequently spurred interest toward applying these techniques to the design process itself where changes and improvements in the plant can be made more easily and cheaply.

The reliability techniques used in the RSS have been used by both NASA and the British, and the experience of the British particularly shows that accurate and useful results can be obtained given a good data base. [2,3] In this study, failure data from the RSS has been used. This data is based on the present nuclear power plant operating experience in the United States, and it should apply to the similar equipment and components of future nuclear power plants built in the United States. However, the emphasis of a design study is to provide useful design inputs by directing attention to those areas of the design with the greatest potential

impact on the public safety. It can then provide a useful basis for further design efforts and development work.

It should be mentioned that the techniques used in this research project are, in general, also applicable to a study of the plant reliability. Considering the cost of plant outages, such an undertaking would be quite worthwhile.

1.2 Outline of Thesis Research

This research project is an attempt to utilize the techniques of the RSS toward performing a first-cut safety assessment of the conceptual design of a nuclear power plant before it is actually constructed. The nuclear power plant design that was analyzed is the 300 MWe demonstration plant design of the gas-cooled fast-breeder reactor (GCFR). This reactor is being designed and developed by the General Atomic Company (GA) [4]. Figure 1.1 is a cross-sectioned view of the nuclear steam supply portion of the plant showing the principal components of the primary coolant system.

The main thrust of the analysis has been directed towards the investigation of the probability of accident sequences which might lead to a meltdown of the reactor core. Core melt accidents were specifically chosen because the largest inventory of radioactive nuclides is located in the core of the reactor. If these nuclides were to be released by the melting of the nuclear core, they would represent the largest potential hazard to the health and safety of the public. However,

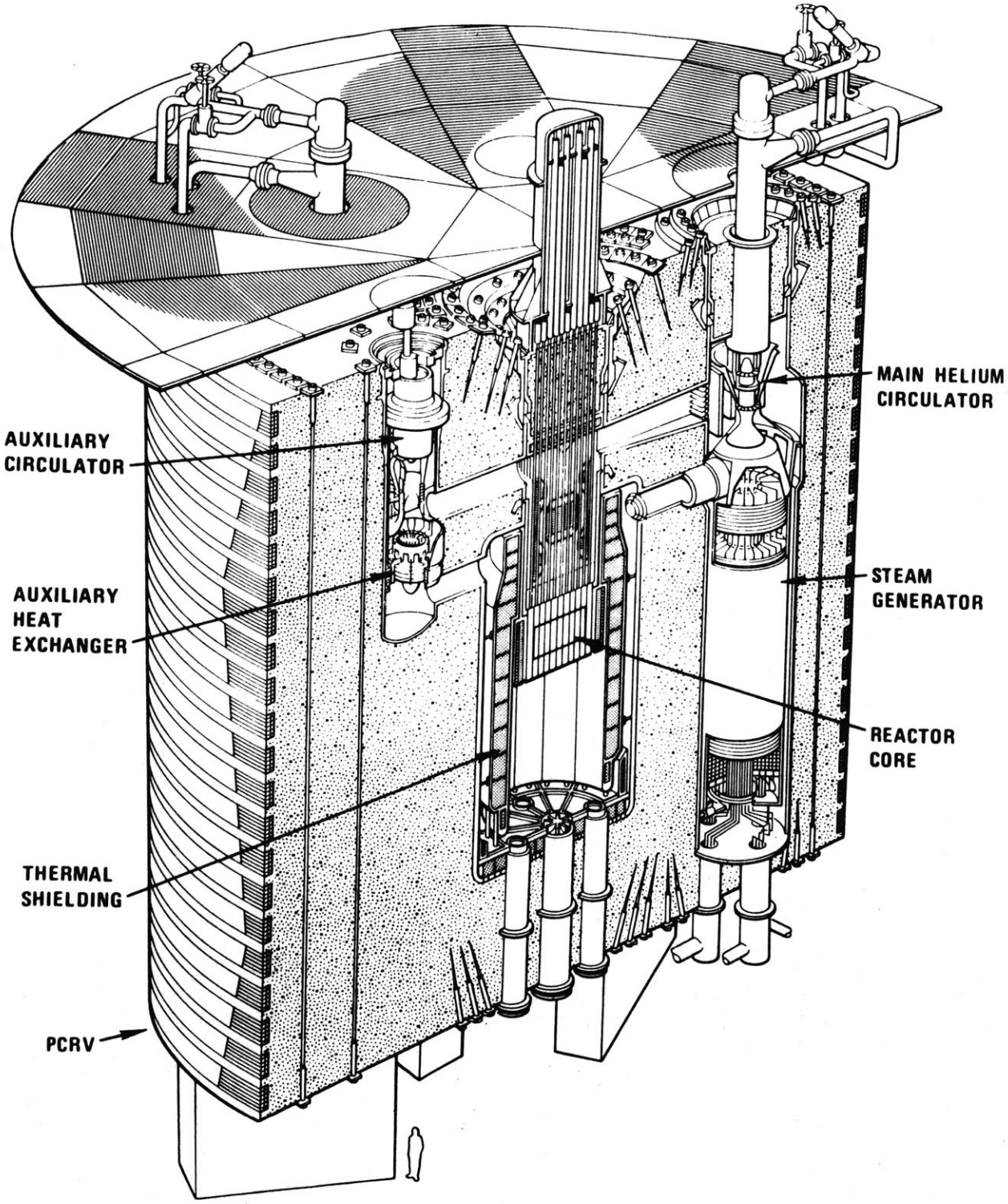


FIGURE 1.1 Cutaway View showing the Principal Components of the Nuclear Steam Supply System within the PCRV.

the evaluation of the consequences of a core meltdown to the public was not a part of this study.

The accident analysis methodology developed in the RSS was utilized to construct a model of the plant response under various transient and accident conditions, including those sequences of events which could lead to a core meltdown. This included:

1) the identification of the types of accidents which might cause the core to melt and the most probable types of event sequences which lead to core meltdown;
2) the modeling of the plant response following the initiating event in a probabilistic manner in order to allow the quantitative analysis of the accident sequences; and
3) the determination of the reliability values used in the probabilistic analysis of the accident sequences.

In general, GCFR core meltdown accidents can be classified as resulting either from severe power to heat removal imbalances following a reactor shutdown, or from severe power to heat removal imbalances during reactor operation. The first class of accidents results from losses of forced helium circulation or heat removal capability following a reactor shutdown. The second class of core-melt accidents may result from losses of adequate forced helium circulation without a reactor shutdown, or from a reactor overpower transient.

Thus the total probability of a core meltdown for a given initiating event may be considered to be the sum of two contributors:

$$P_i = (P_S + P_F)\, P_{IE}, \quad \text{where}$$

P_i is the total probability of a core meltdown for a given initiating event;

P_S is the conditional probability of a meltdown following reactor shutdown, given the initiating event;

P_F is the conditional probability of a meltdown due to the failure of the reactor shutdown systems, given the initiating event; and

P_{IE} is the probability or frequency of occurrence of the event requiring a reactor shutdown.

Because of the high reliability that is expected for the GCFR reactor shutdown systems, the events following the reactor shutdown were modeled in the most detail. The modeling of the shutdown cooling and decay heat removal operations was performed for two specific sets of circumstances. One model was constructed for those reactor shutdowns in which the reactor primary coolant system remains pressurized. The second model pertains to the reactor shutdown cooling operations following a reactor coolant system depressurization. Each of these models represents the possible shutdown event sequences which might occur due to the combinations of success or failure of the shutdown heat removal sub-systems. The

reactor shutdown initiating events were investigated and categorized according to their affect on the performance of either shutdown cooling system. For each of the shutdown heat removal subsystems, three contributors to the subsystem failure probability were considered. These were random equipment failures, intra-system common mode failures, and test and maintenance unavailabilities. A median probability of a loss of decay heat removal was determined for each of the initiating event categories, and the sensitivity of this valve to large changes in each of the subsystem failure contributors was determined.

In the remaining sections of this chapter, the research objectives of this study are outlined and the accident analysis methodology of the reactor safety study is outlined. Chapter 2 provides a description of the GCFR 300 MW(e) demonstration plant design with emphasis placed on the reactor shutdown cooling systems. Chapter 3 is a detailed description of the modeling of the plant responses following the initiation of a reactor shutdown signal. Chapter 4 is a discussion of the reactor shutdown initiating events, a description of the method in which the accident sequence probability calculations were performed, and a summary of the failure data and other probability inputs used in the analysis. In Chapter 5, the results of the sensitivity analyses performed for each of the reactor shutdown initiating event categories are pre-

sented. This includes the determination of a median point estimate of the core-melt probability for each reactor shutdown initiating event category along with the variation in this value due to changes in each of the subsystem failure contributors. The major results of the study are presented in this chapter. In chapter 6, the overall median probability of a core meltdown is determined and the various contributors to this final value are discussed. Chapter 7 summarizes the major results of the study and presents comments on both the GCFR shutdown cooling systems design and the methodology used in the study.

1.3 Research Objectives

The purpose of this study is to provide a first-cut assessment of the safety of a gas-cooled fast breeder reactor, as embodied in the 300 MW(e) demonstration plant design described in Ref. 4, in regard to the potential for core meltdown accidents. The quantitative analysis of the core-melt accident sequences allowed the determination of both the accident sequence probabilities and the sensitivity of these results to the reliability values of the subsystems and components involved in the reactor shutdown operations. It is hoped that this information will prove to be useful in the following ways:

1) The determination of the sensitivity of the subsystems and component reliability values will indicate those items which are most important in regard to changes in the probability of a core-melt accident. The future design and development efforts for these key subsystems can then be focused toward assuring an appropriately high reliability value. The intensification of effort into these key areas allows the overall plant safety to be increased more effectively than if the design effort were spread over all the systems which potentially affect the plant safety.

2) The analysis of the core-melt accident sequences also includes the determination of those specific accident paths which are the dominant contributors to the probability of a core meltdown. The identification of these accident paths may indicate possible design changes which could mitigate or even eliminate these dominant paths.

3) The detailed modeling of the accident sequences will provide useful information regarding calculations of both the core meltdown process and the accident consequences. These are needed to determine the risk to the health and safety of the public which would result from a core meltdown.

4) Lastly, the analysis should provide some quantifiable inputs into the overall plant optimization process which reflect the tradeoffs between the plant safety and the other aspects of the plant design.

1.4 Reactor Safety Study Accident Analysis Methodology

One of the stated objectives of the Reactor Safety Study (RSS) was to:

> Perform a quantitative assessment of the risk to the public from reactor accidents. This requires analyses directed toward determining both the probabilities and the consequences of such accidents.

However, in the following GCFR study, only the accident probabilities are to be investigated. The accident analysis methodology of the RSS is described briefly below, and examples are given to clarify the explanation of the methodology. These examples, which pertain to Light Water Reactors (LWR), were used because it was felt that the reader would be more generally familiar with LWRs.

The accident analysis methodology developed in the RSS allows for both a detailed determination of the events leading to a specified accident, and for an objective evaluation of the probabilities of the various events involved.

To describe the events leading to an accident, an event tree is used. This is a logical representation that describes a series of accident chains. These accident chains are sequences of events which start with the various initiating events and include the responses of the protection systems and engineered safeguard features that are designed into the plant. The event tree is developed from an understanding of the plant design and operation. It is used not only to consider the operability of the safety systems under the actual accident conditions, but also to help identify the detailed inter-relation of these various systems and any effects which this might have.

A simplified event tree is shown in Figure 1.2. It describes the accident sequences involved in a loss of coolant accident (LOCA) for a light water reactor. The diagram starts with a pipe break, as the initiating event, and includes the responses of the basis safeguard systems activated in this type of accident. The probabilities P_1 through P_5 depend upon the specific conditions associated with this initiating event, and they must be either calculated or estimated if the accident sequence probabilities are to be evaluated [5]. It is important to note that the analyst who constructed this tree used his knowledge of the plant operation and response to accident situations to

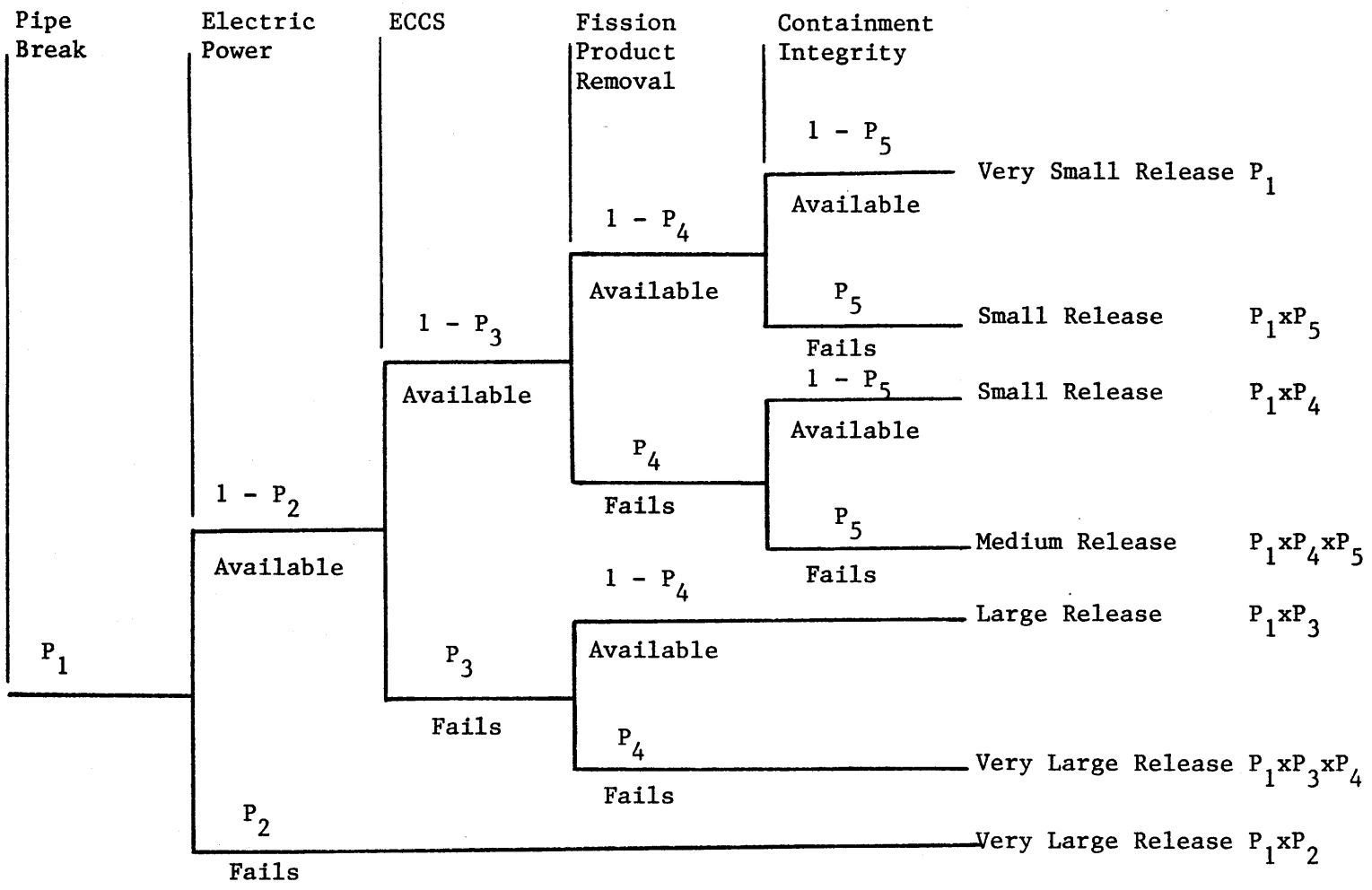
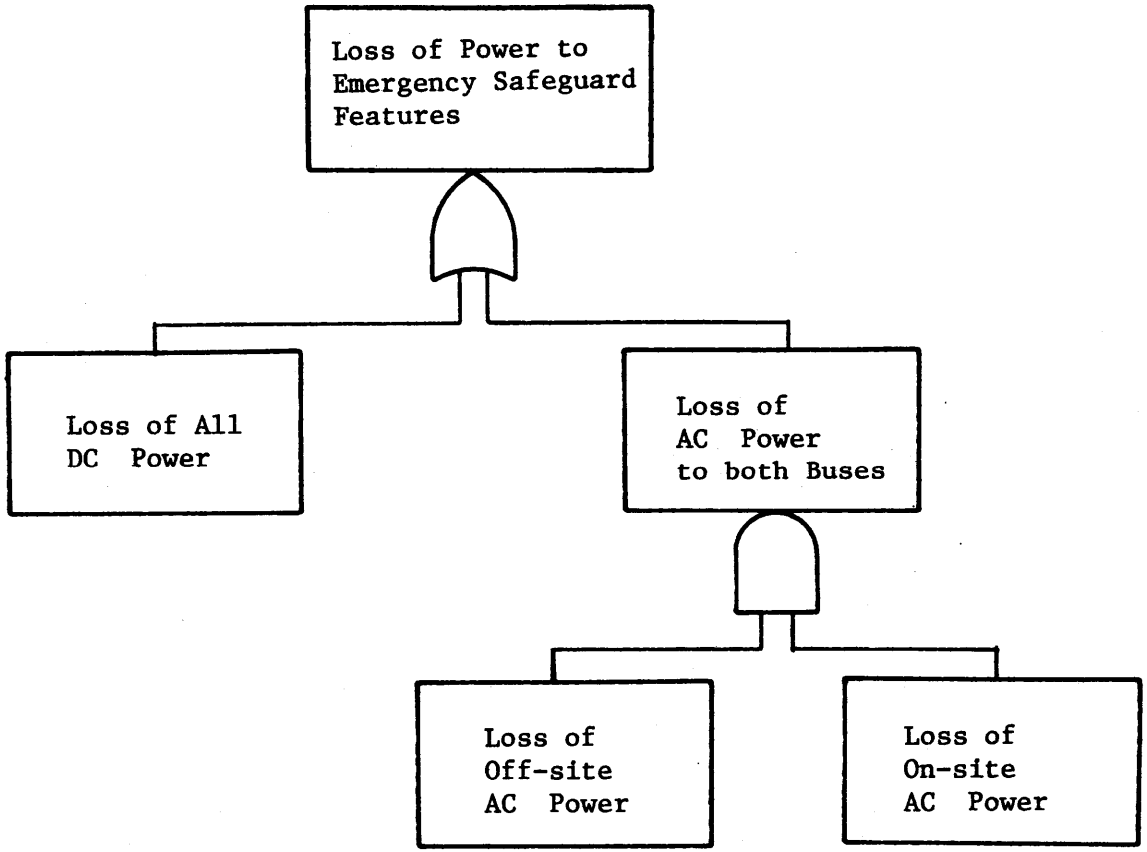


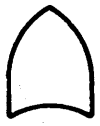
FIGURE 1.2 A Simplified Event Tree for a Loss of Coolant Accident in a Light Water Reactor (taken from reference 5)

arrange the tree in a manner which allowed major system interdependencies to be taken into account. For example, all of the safeguard systems, as shown here, depend upon electricity being available for power. Thus no success paths for these systems need be included given no electric power available. Also, the diagram shows that the containment integrity cannot be maintained if the ECCS fails, irrespective of what the fission product removal system does. Thus the event tree explicitly includes the major system inter-relationships.

The accident sequence probabilities can then be determined from the event tree if the probabilities of the individual events can be evaluated. However, these events represent the operation of complex engineering systems, and, in the case of nuclear power plants being built today, there is little directly applicable empirical data on which to base system failure rates. Therefore, in order to obtain these probabilities objectively, a fault tree is used. The fault tree employs a logic almost the reverse of the event tree in that it starts with the undesired event and proceeds through the intermediate events until the basic attributable causes are reached. Fault tree analysis is used to determine the probability with which a specific engineering system will operate, under specific conditions, from the existing or proposed failure rates of the system components [6].

A simplified fault tree, shown in Figure 1.3, indicates that the loss of power to the engineered safeguard features is dependent on the loss of either DC power to the control systems, or AC power to both the plant buses. Since either condition is sufficient to cause the loss of power, an "or" gate is used to couple the two events. The failure probability is then the sum of the probabilities of the two individual events. The loss of all AC power is dependent on the loss of both on-site and off-site AC power. Since both of these events are necessary to cause a loss of all AC power, they are coupled by an "and" gate. This signifies that the overall probability is the product of two individual probabilities. The actual probability values used in the bottom blocks of the fault tree depend upon the specific conditions determined by the initiating accident in the event tree in which the failure probability is to be used.




"OR" Gate

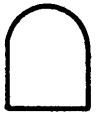

"AND" Gate

FIGURE 1.3 A Simplified Fault Tree for the Loss of Electrical Power (taken from reference 5)

Chapter 2

The Gas-Cooled Fast-Breeder Reactor (GCFR)

2.1 Introduction

The design and development of the gas-cooled fast-breeder reactor (GCFR) has been undertaken by the General Atomic Company (formerly the Gulf General Atomic Company) with support by ERDA and a large group of electric utility companies. Work on the design has continued since 1962. Conceptual designs for the major systems and components of the Nuclear Steam Supply System (NSSS) have been made, and these and the initial safety and design analyses have been compiled in a document called the Preliminary Safety Information Document (PSID) [1]. This document served as the basis for a review between March, 1971, and November, 1974, by both the regulatory staff of the AEC and by the Advisory Committee on Reactor Safeguards (ACRS). The questions and answers from this review process are contained in references 2 and 3, and a summary of the review was published in August, 1974, by the regulatory staff entitled "Preapplication Safety Evaluation of the Gas-Cooled Fast-Breeder Reactor" [4]. The material presented in this chapter is largely from these four documents.

A detailed balance-of-plant design study has been completed by the Bechtel Corporation [5] and was made available for this thesis research project. Since this study is not in the public domain, any material taken from it will be presented in full.

Basically, this chapter will describe the GCFR concept particularly as embodied in the design of a 300 MW(e) demonstration plant with emphasis on those aspects of the design which were of primary interest in performing this study. In reading this description, it should be kept in mind that the development of the GCFR concept has benefited greatly from technology developed for both the high temperature gas-cooled reactor (HTGR), and the liquid-metal fast breeder reactor (LMFBR). Specifically, the GCFR will utilize prestressed concrete reactor vessel (PCRV) technology, steam generator technology and helium circulator technology developed for the HTGR. In the areas of core physics and fuel element technology much of the work from the LMFBR development program is readily extended to the GCFR.

2.2 Design Description

2.1-1 Introduction

The GCFR, as its name states, utilizes a gaseous coolant. The coolant, which is pressurized helium, is the agent for removing heat from the core and for transferring it to the working power cycle. The term "fast" refers to the predominant energy of the neutrons in the core, which is much

greater for a "fast" reactor than for "thermal" reactors which, for example, use water as a coolant or contain large amounts of carbon in the core. The term "breeder" signifies that the reactor will actually generate more fissile fuel material than it consumes. Figure 2.1 is a cut-away view of the demonstration plant. The design capacity of the plant is 300 MW(e) and 830 MW(th).

2.2-2 The Nuclear Steam Supply System

Table 2-I is a summary of the principal design data for the GCFR, and Figure 2.2 is a schematic illustration of the nuclear steam supply system (NSSS). It shows the pre-stressed concrete reactor vessel (PCRV) and the major reactor components contained within it. A very important feature of the PCRV is that it encloses the entire primary coolant system. The helium coolant operates at a working pressure of 1305 psi and an average core outlet temperature of 1022^{o}F. The primary system consists mainly of two core cooling systems, which are the main loop cooling system and the core auxiliary cooling system (CACS). Each of these systems consists of three independent cooling loops. The nuclear core and surrounding breeder blanket is located in the central PCRV cavity. The three main cooling loops and the three CACS loops are located in separate cavities in the PCRV sidewall surrounding the central cavity and connected to it by cross ducts.

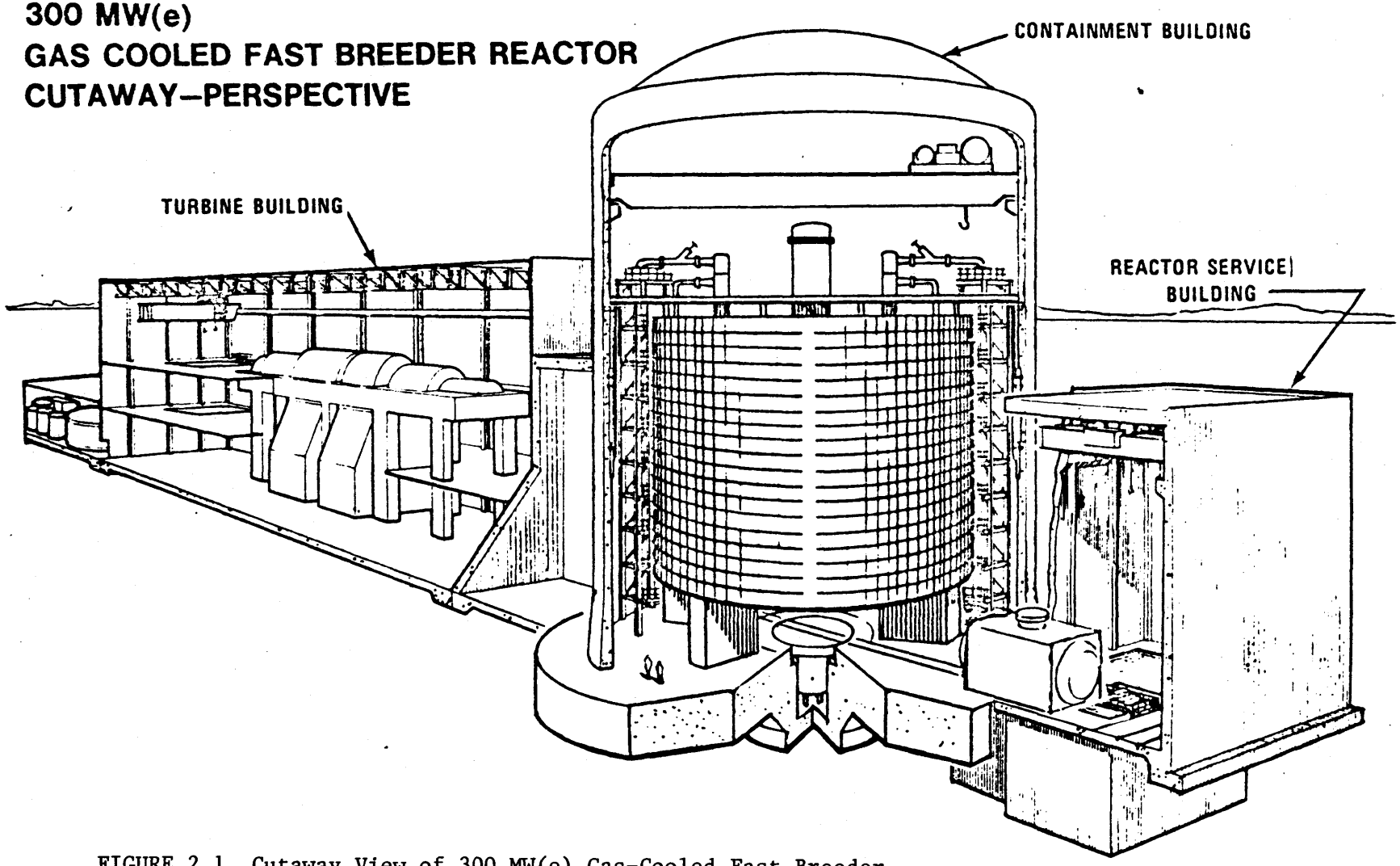


FIGURE 2.1 Cutaway View of 300 MW(e) Gas-Cooled Fast Breeder Reactor Demonstration Plant

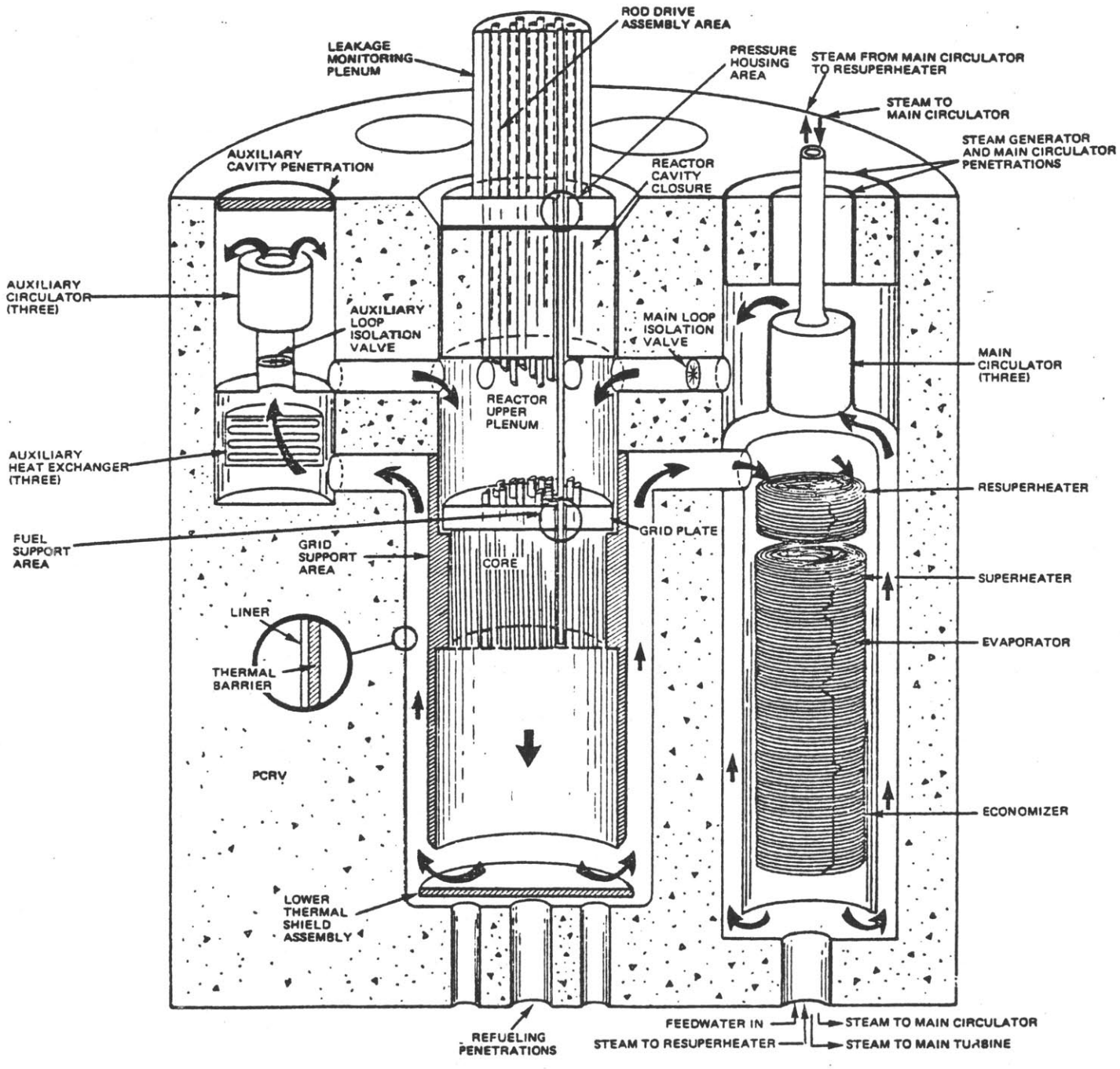


FIGURE 2.2 Principal Features of the Reactor and Primary Coolant System shown Schematically (Reference 4)

Table 2-I

Summary of Principal Design Data for the
300 MW(e) GCFR Demonstration Plant (Reference 1)

PLANT CHARACTERISTICS	
Reactor thermal power, MW(t)	830
Gross electrical power, MW(e)	304
Net electrical power, MW(e)	300
Plant efficiency, %	36.0
Net heat rate, Btu/kWh	9,474
Reactor outlet temperature, °F	1,022
Reactor inlet temperature, °F	613
Steam conditions	
Superheat outlet temperature, °F	876
Superheat outlet pressure, psia	2,900
Resuperheat outlet temperature, °F	927
Resuperheat outlet pressure, psia	1,260
Condenser pressure, in. Hg	3.0
Feedwater temperature, °F	412
Fuel lifetime, full-power days	750
Refueling cycle, yr	1
Fuel material	PuO_2-UO_2
Reactor coolant	Helium
Reactor vessel and primary coolant boundary	PCRV
PCRV dimensions	
Vessel outside diameter, ft	84
Vessel height, ft	80.5
Reactor cavity ID, ft	20.5
Reactor cavity height, ft	41.8
Reactor cavity penetration diameter, ft	12.5
Steam-generator cavity penetration diameter, ft	12.7
Steam-generator cavity diameter, ft	11.5

Table 2-I (continued)

REACTOR	
Reactor geometry	
Core height, in.	39.2
Core length-to-diameter ratio	0.5
Axial blanket length (each end), in.	17.7
Radial blanket elements, 3 rows	ThO_2
Reactor assemblies	
Fuel elements	91
Control elements	27
Blanket elements	147
Control and shutdown rods	
Control	21
Shutdown	6
Reactor heat transfer	
Helium temperatures	
Reactor inlet, ^{o}F (^{o}C)	613 (322)
Mixed mean outlet, ^{o}F (^{o}C)	1022 (550)
Flow control	Replaceable fixed orifices
Maximum linear rating, at full power, kW/ft	12.5
Maximum (hot-spot) cladding temperature (mid-wall), ^{o}F (^{o}C)	1,292 (700)
Radial maximum-to-average power ratio	1.25
Axial maximum-to-average power ratio	1.21
Average core heat flux, Btu/(hr)(ft^2)	340,000
Maximum heat flux, Btu/(hr)(ft^2)	510,000
Reactor inlet coolant pressure, psia	1,305
Reactor pressure drop, psi	42
Total helium coolant flow rate, lb/sec	1,548
Average power density, kW(t)/liter of core	240

Table 2-I (continued)

REACTOR (continued)	
Nuclear characteristics	
Core fissile enrichment, average, at-%	17.0
Fissile masses at midcycle	
Core (Pu^{239} + Pu^{241}), kg	1,210
Axial blanket (Pu^{239} + Pu^{241}), kg	81
Radial blanket (3-row ThO_2 (U^{233})), kg	320
Fissile loading at beginning of cycle, kg	1,244
Initial loading (Pu + U + Th)	
Core, kg	7,900
Axial blanket (UO_2), kg	7,400
Radial blanket (3 rows ThO_2), kg	28,930
Average breeding ratio	1.40
Maximum fuel burnup, MWd/Te heavy metal	100,000
Doppler constant, Tdk/kdT (T in ^oK)	-0.0040
Total helium reactivity worth, $	0.55
Power coefficient, ¢/MW(t)	-0.11
Average fast neutron flux (E > 0.1 MeV), n/cm^2-sec	2.2×10^{15}
Reactor rating, MW(t)/kg fissile	0.60
Reactivity control requirements	
Cold-to-hot operating, $	-3.47
Reactivity swing over equilibrium cycle, $	-9.00
Compensation for He, $	-0.55
Shutdown margin, $	-3.70
Total control requirements, $	-16.72
Absorber material	B_4C
Reactivity control requirements	
Cladding material	316 SS
Average rod worth	
Control, $	0.85
Shutdown, $	1.60

Table 2-I (continued)

REACTOR (continued)	
Fuel and blanket elements	
Shape of cross section	Hexagonal
Distance across flats, external, in	6.642
Lattice spacing, in	6.892
Duct wall thickness, in	0.100
Element overall length, ft	11.5
Fuel-rod cladding material	316 SS
Rod spacer type	Grid
Fuel element	
Number of rods, standard element	270
Number of rods, control element	232
Rod outside diameter, in	0.282
Rod inside diameter, in	0.244
Fuel length, in	39.2
Fuel material	Mixed PuO_2-UO_2
Fuel smear density, % theoretical	86
Axial blanket length (each), in	17.7
Axial blanket material	Depleted UO_2
Axial blanket material smear density, % theoretical	90
Fuel-rod surface roughening	
Fraction of active core length roughened, %	75
Heat-transfer multiplier	2
Friction-factor multiplier	3
Blanket element	
Number of rods	126
Rod outside diameter, in	0.504
Rod inside diameter, in	0.474
Blanket material	ThO_2
Blanket material smear density, % theoretical	90

Table 2-I (continued)

REACTOR COOLANT SYSTEM	
Number of loops	3 main 3 auxiliary
Helium inventory at design condition in PCRV, lb	10,240
MAIN LOOP COMPONENTS	
Main helium circulator (each of 3)	
Type	Single-stage axial
Drive	Steam turbine
Flow, lb/hr	1.86×10^6
Pressure rise, psi	54
Brake horsepower (per circulator)	21,000
Steam generators (each of 3)	
Economizer, evaporator, superheater sections	
Type	Helical
Heat duty, Btu/hr	8.46×10^8
Surface area, ft^2	31,700
Helium flow per steam generator, lb/hr	1.86×10^6
Water inlet temperature, ^oF	412
Steam outlet temperature, ^oF	876
Number of tubes per steam generator	218
Tube outside diameter, superheater, in	1.0
Tube outside diameter, evaporator-economizer, in	0.75
Resuperheater section	
Type	Helical
Heat duty, Btu/hr	1.47×10^8
Surface area, ft^2	3,930
Helium flow, lb/hr	1.86×10^6
Steam flow, lb/hr	0.88×10^6
Helium temperature in, ^oF	1,022
Helium temperature out, ^oF	958
Steam temperature in, ^oF	682
Steam temperature out, ^oF	928
Number of tubes	297
Tube outside diameter, in	1.0

Table 2-I (continued)

AUXILIARY LOOP COMPONENTS	
Auxiliary heat exchanger (design maximum conditions for each of 3)	
Type	Helical
Heat duty, Btu/hr	50.4×10^6
Surface area, ft^2	1,140
Helium flow, lb/hr	40,000
Helium temperature in, ^oF	1,414
Helium temperature out, ^oF	400
Water inlet temperature, ^oF	180
Water outlet temperature, ^oF	500
Water flow, lb/hr	154,000
Number of tubes	60
Tube outside diameter, in.	0.75
Auxiliary helium circulator (design maximum conditions for each of 3)	
Type	Single-stage Centrifugal
Drive	Electric motor
Flow, at depressurized condition, lb/hr	40,000
Pressure rise, psi	1.36
Brake horsepower (per circulator)	460
TURBINE GENERATOR	
Type	TC4F-25
Speed, rpm	3,600
Throttle flow, lb/hr	2.62×10^6
Throttle pressure, psia	1,179
Throttle temperature, ^oF	922
Condenser pressure, in. Hg (abs)	3.0
Number of feedwater heaters	6
Final feedwater heater temperature, ^oF	412
Gross electrical output, MW	304

Table 2-I (continued)

SECONDARY CONTAINMENT	
Type	Reinforced concrete
Inside diameter, ft	116
Inside height, ft	174
Atmosphere	Air
Equilibrium pressure, atm (abs)	1.8

The flow of the helium coolant is downward through the core and then upward through the annular passage between the reactor thermal shield and the PCRV liner to the cross ducts. The cross ducts direct helium to the steam generators of the main loops or to the heat exchangers of the auxiliary loops as appropriate. In the main cooling loops, the helium flows down through the helically coiled steam generator and up the annular passage between the steam generator shroud and the PCRV liner to the helium circulator inlet. The helium, after it is discharged from the circulator, then passes through the main loop isolation valve, and into the reactor inlet plenum. In the auxiliary loops, the helium flow is up through the heat exchanger, through the auxiliary loop isolation valve, and then to the auxiliary circulator before it returns to the reactor inlet plenum. The CACS is only used when the reactor is shut down. During normal reactor operation the auxiliary circulators are not running, and the auxiliary loop isolation valves remain shut preventing any backflow of helium.

2.2-3 The Main Loop Cooling System

The major components of the main loops are the main loop isolation valves, the main helium circulators, and the steam generators. Figure 2.3 is a drawing of both a main helium circulator and its loop isolation valve. The main loop isolation valves are louver-type self-actuating valves. The valve consists of seven louvers which have an air foil cross-section in the direction of normal loop flow. The

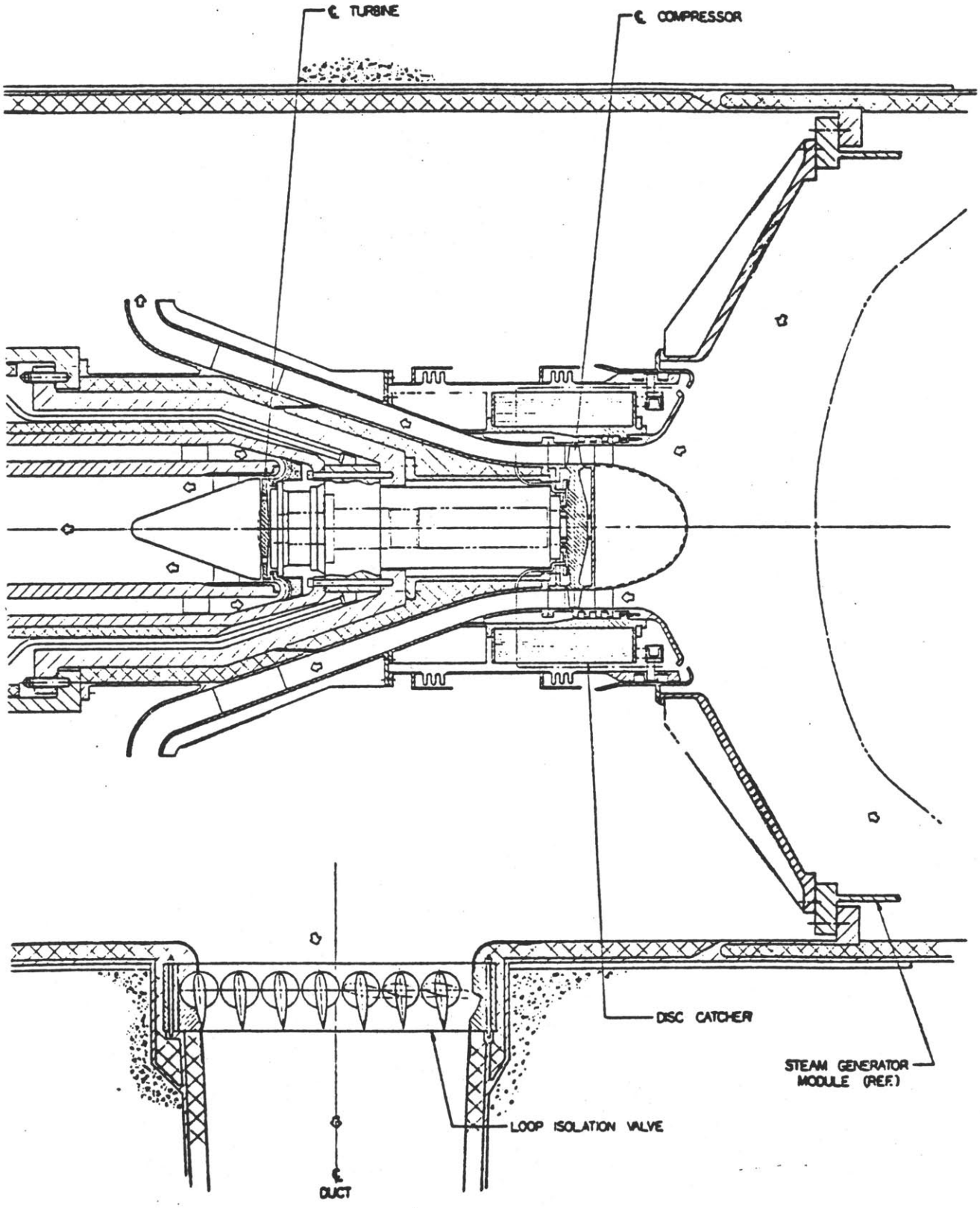


FIGURE 2.3 General Arrangement of Main Helium Circulator and its Loop Isolation Valve

valve is opened by the positive pressure head created by the operation of the helium circulator in its loop. Should its circulator stop, the valve will close due to the forces on the air foil created by the reversed pressure differential and thus prevent back-flow through the loop. The main helium circulators are single-stage, axial-flow helium compressors. The circulator drive is a direct coupled steam turbine. The circulator-turbine unit utilizes water-lubricated bearings, and a buffer-helium seal prevents the leakage of steam or water into the PCRV. The steam generator is a forced circulation, single pass helically-coiled unit. The lower portion of the steam generator module consists of an economizer, an evaporator, and a superheater. The superheated steam exiting this portion of the steam generator is used to drive the helium circulator. The steam exhausted from the circulator turbine then is returned to the upper portion of the steam generator module where it is resuperheated before it is used to drive the main turbine-generator set of the power plant. Figure 2.4 is a schematic illustration of the plant steam and helium flow paths. Because the entire steam flow from the steam generators passes through the helium circulator-turbines, the helium circulation can be maintained proportional to the steam generation. This provides a direct relationship between the helium cooling requirements and the supply of steam produced.

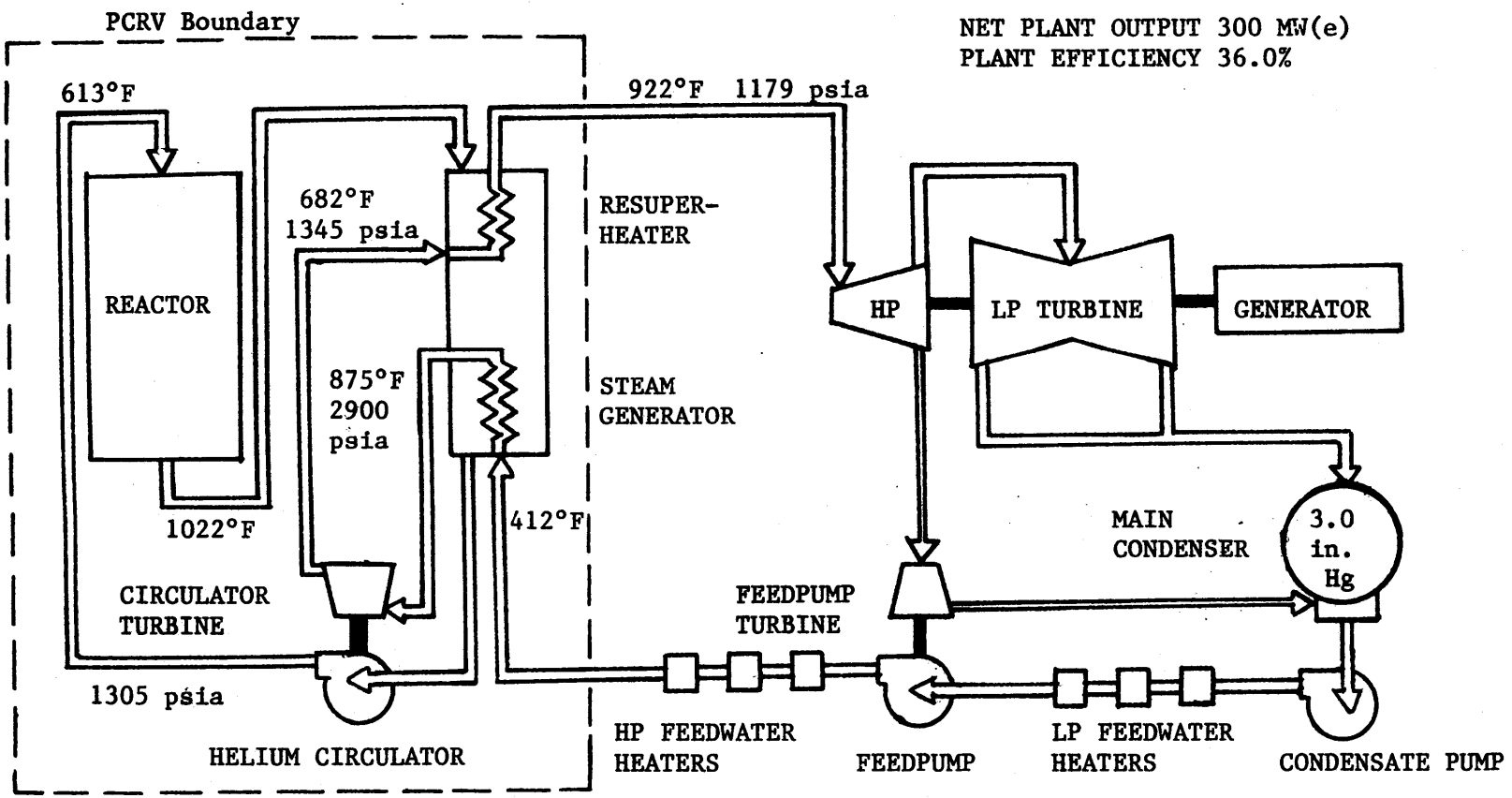


FIGURE 2.4 GCFR Demonstration Plant Flow Diagram.

2.2-4 The Core Auxiliary Cooling System (CACS)

The CACS is designed for long-term shutdown cooling and as a backup to the main loops for emergency core cooling. The equipment of the CACS is functionally diverse and independent from that of the main loops. The diversity of the main loop cooling system and the CACS includes the circulators, the isolation valves, and the methods of heat rejection. These areas are summarized in Table 2-II.

The auxiliary loop isolation valve is a butterfly-type check valve which is closed by the normal pressure differential created by the main loop operation. The valve is opened by the pressure rise created by the auxiliary circulator operating after the main circulators have stopped. The auxiliary heat exchanger is a pressurized water heat exchanger and the auxiliary circulator is a radial-flow, single-stage compressor which is powered by a variable speed electric motor drive. Each CACS loop is equipped with a forced-air heat exchanger for ultimate heat rejection to the atmosphere. A schematic illustration of the CACS operation is shown in Figure 2.5.

2.2-5 The GCFR Core Design

The reactor consists of 265 hexagonal elements on a triangular pitch. Of these, 147 are radial blanket elements, 91 are standard fuel elements, and 27 are control elements. The core and blanket dimensions are given in

Table 2-II

GCFR Cooling System Diversity

	Main Cooling System	Auxiliary Cooling System
Helium Circulators		
Type	Axial Flow	Centrifugal
Drive	Steam Turbine	Electric Motor
Bearings	Water Lubricated	Oil Lubricated
Power Source	Nuclear Steam for 30 Min. or Oil Fired Boilers After 20 Min.	Essential Electric Power; Separate Diesel for Each Loop
Loop Isolation Valves		
Type	Multiple Louver	Flapper
Position in Power Operation	Open	Closed
Actuation	Reverse Flow	Aux. Circulator Pressure Rise
Heat Dump		
Heat Exchangers	Main Steam Generators	Auxiliary Heat Exchangers
Coolant	Steam/Water	Pressurized Water
Feed Source	Main Condenser Hot Well or Condensate Storage	Closed Loop
Heat Sink	Main Condenser or Steam Exhaust to Atmosphere	Atmosphere Via Air Cooled Heat Exchangers

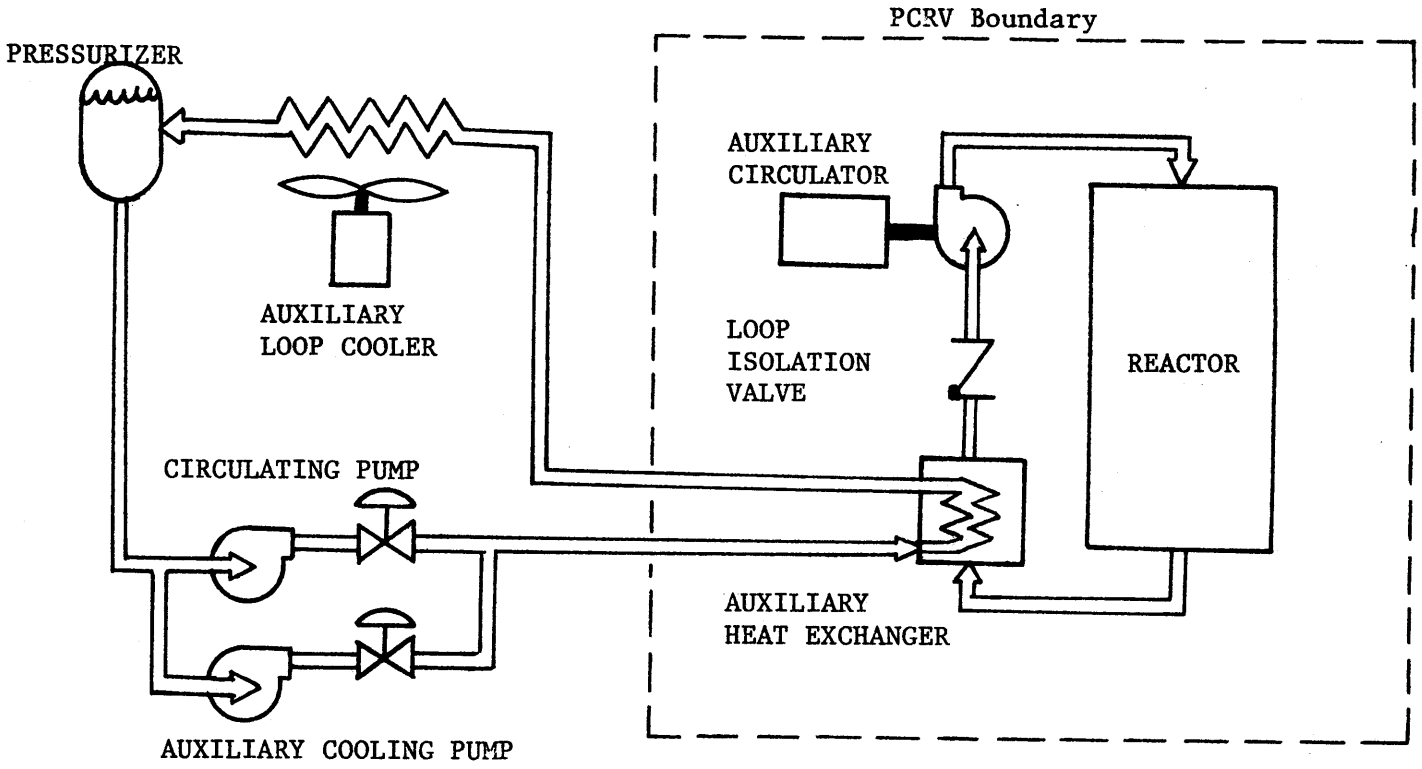


FIGURE 2.5 Core Auxiliary Cooling System Flow Diagram.

Table 2-I. Each element is 6.642 inches across the outside flats and 11.3 feet in overall length. A core plan and cross-sections of each fuel element type are shown in Figure 2.6.

In the GCFR, the core is supported from above by a two-foot-thick grid plate which is mounted in the upper portion of the central PCRV cavity. The elements are rigidly latched to the grid plate, but they are unrestrained over their remaining length. The fuel element latching mechanisms extend down from the PCRV central cavity closure, and they are also designed to provide backup support for the core from the PCRV head. Figure 2.7 is an illustration of the GCFR core, and Figure 2.8 shows a cross-section of the grid plate support structure.

Each standard fuel element contains 270 fuel rods with an outside diameter of 0.282 inches. The cladding surface of the rods is roughened over the lower 75 percent of the active core region to improve the convective heat transfer. The rods are positioned by means of grid plates at either end and eight intermediate spacer grids. The central position of each element contains, instead of a fuel rod, a rod containing three thermocouples for monitoring the outlet gas temperature from the element. A typical fuel element configuration is shown in Figure 2.9.

A significant design feature of GCFR fuel is the system for venting the fuel rods, known as the pressure equalization

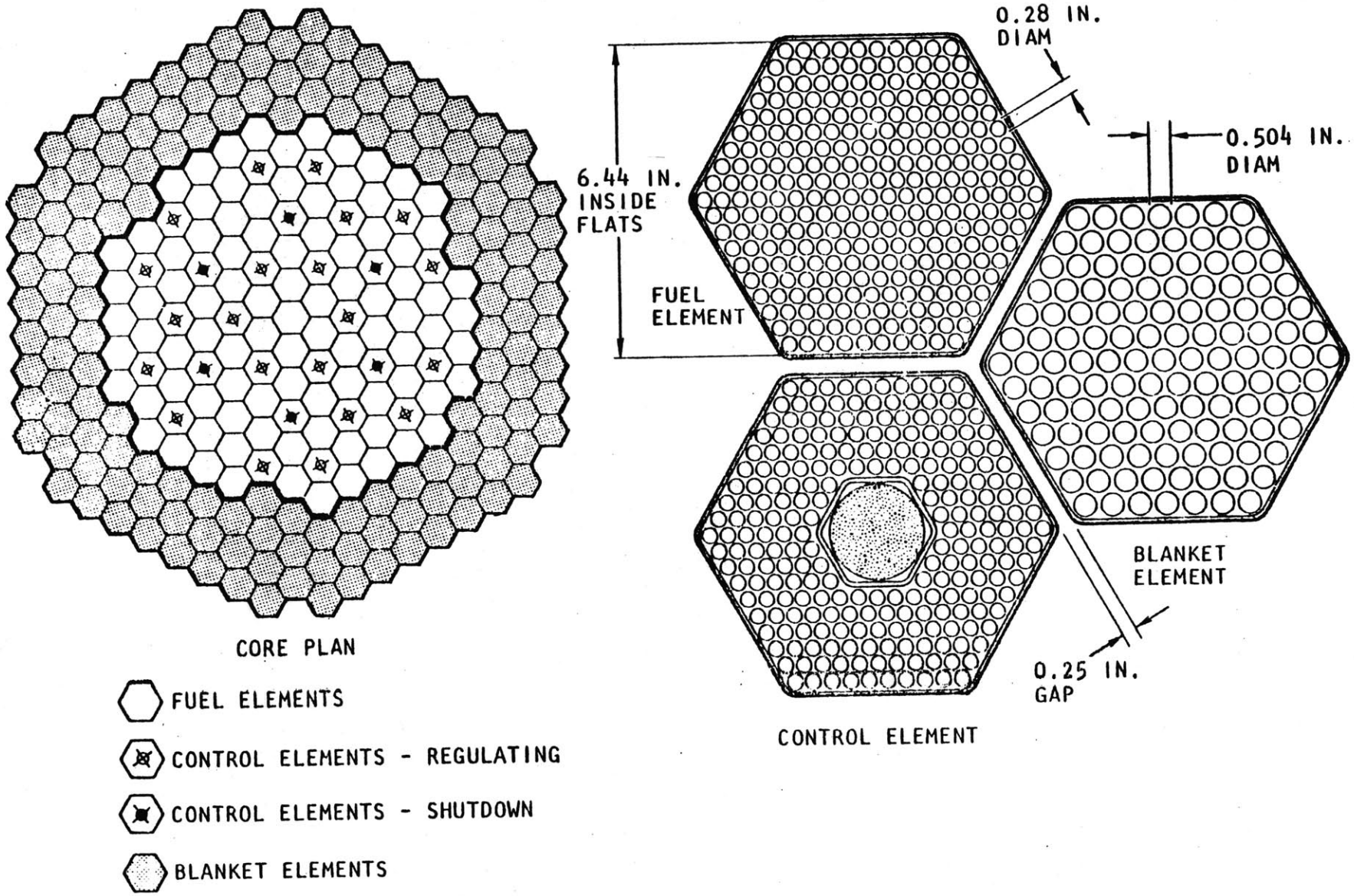


FIGURE 2.6 Core and Fuel-element Plan.

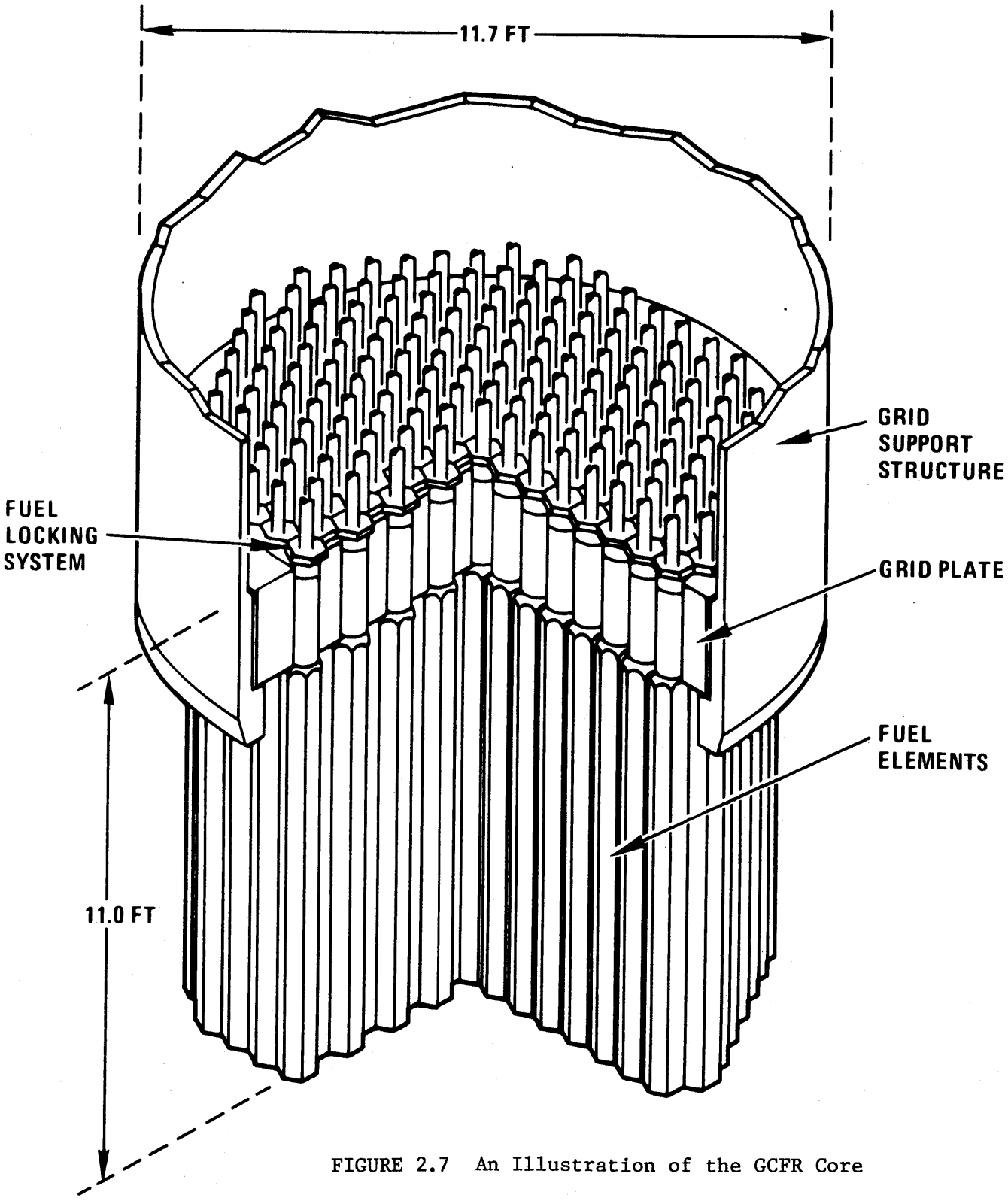


FIGURE 2.7 An Illustration of the GCFR Core

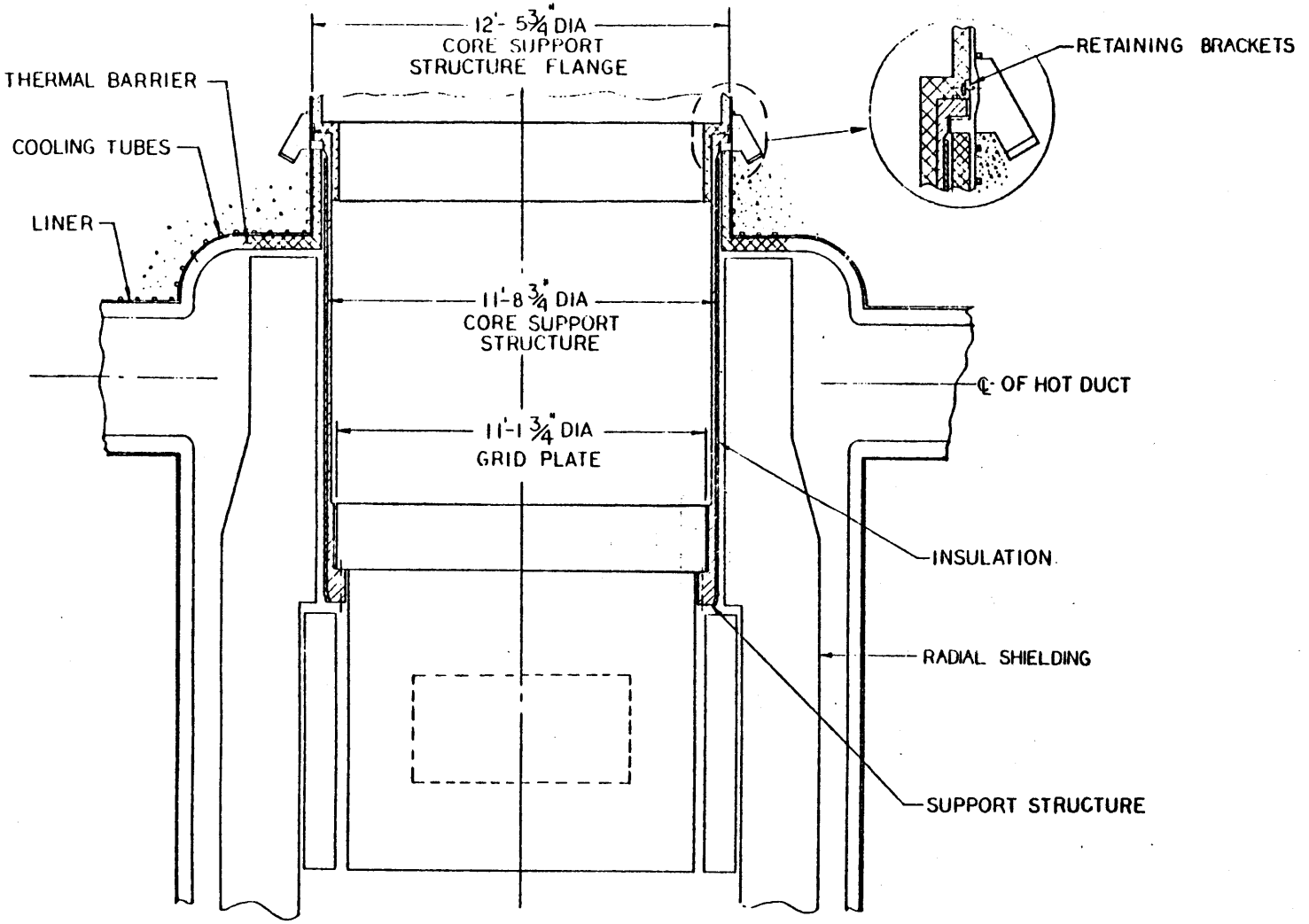


FIGURE 2.8 A Cross-section of the Core Grid Plate Support Structure

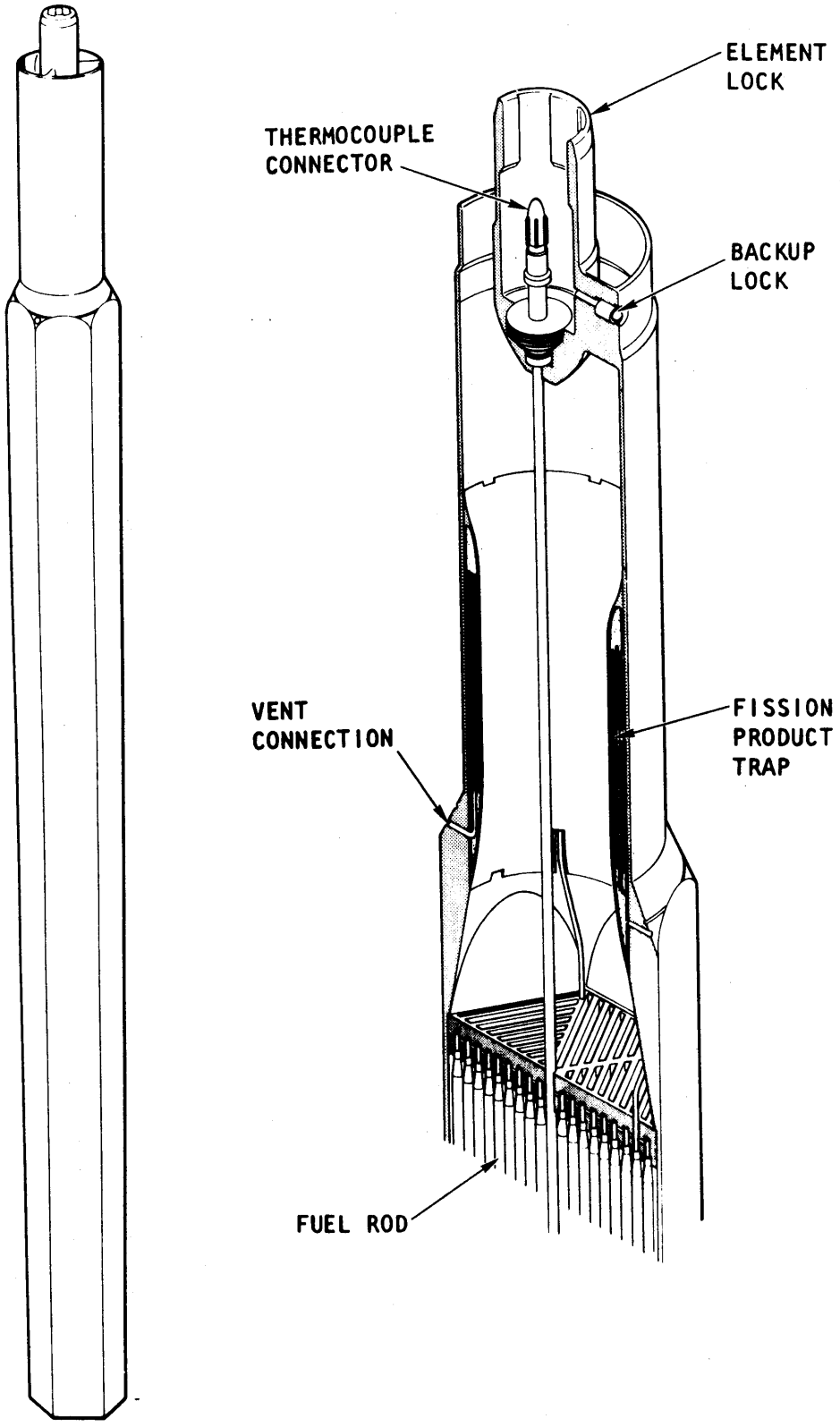


FIGURE 2.9 Fuel Element Configuration.

system (PES). This system is designed to limit the static pressure differential across the fuel cladding to very low values during steady state and transient operation. It does this by providing a means for venting fission product gases directly from the fuel rods to a helium purification system. Both the core and the blanket elements are connected to the PES.

The nuclear design for the core and axial blankets is based on the uranium-plutonium cycle. The fuel element cladding material is type 316 stainless steel with a wall thickness of 0.019 inches, and the fuel consists of sintered pellets of mixed oxides of uranium and plutonium with a smear density of 80 percent. However, the design of the radial blanket utilizes the uranium-thorium cycle. The average calculated breeding ratio is 1.40 with a maximum fuel burnup of 100,000 MWd/Te(U+PU).

2.2-6 Reactivity Control and Shutdown Systems

Control of the GCFR is accomplished with the control rod system. This is a set of twenty-one B_4C control rods that will provide for the normal control, burnup, and shutdown requirements of the reactor. The core plan in Figure 2.6 shows the location of these rods. These rods are located in control elements, and the concentration of absorber material in the rods varies so that each rod has a reactivity worth of 85¢. The control rod absorber section

is connected to the extension rod by a ball joint to allow rod insertion even in the event of some fuel element bowing. A schematic of a control element is provided in Figure 2.10. The control rods are connected to their drive mechanisms by electro-magnetic couplings, and the rods are inserted, during a reactor scram, by gravity drop after deenergizing the couplings. The fall is snubbed by a flywheel energy absorber, and a backup impact energy absorber is also provided.

Backup shutdown protection is provided by the shutdown rod system. This is a set of six rods each of which has a reactivity worth of 1.60$. These rods are also located in control elements. They are positioned outside the core region in the upper axial blanket under normal operation, and their insertion is initiated by all scram signals. The design of the shutdown rods is similar to that of the control rods with the exception that wear rings are not provided on the shutdown rods, and this increases their diametral clearance. However, the shutdown rods are mechanically coupled to their drive mechanisms, which are constant speed, direct-current motors. Each drive motor has its own individual battery power source, and during a scram the rods are power driven into the core. Figure 2.11 illustrates the drive mechanisms for the two shutdown rod systems, and a summary of the diverse features of the two systems is supplied in Table 2-III.

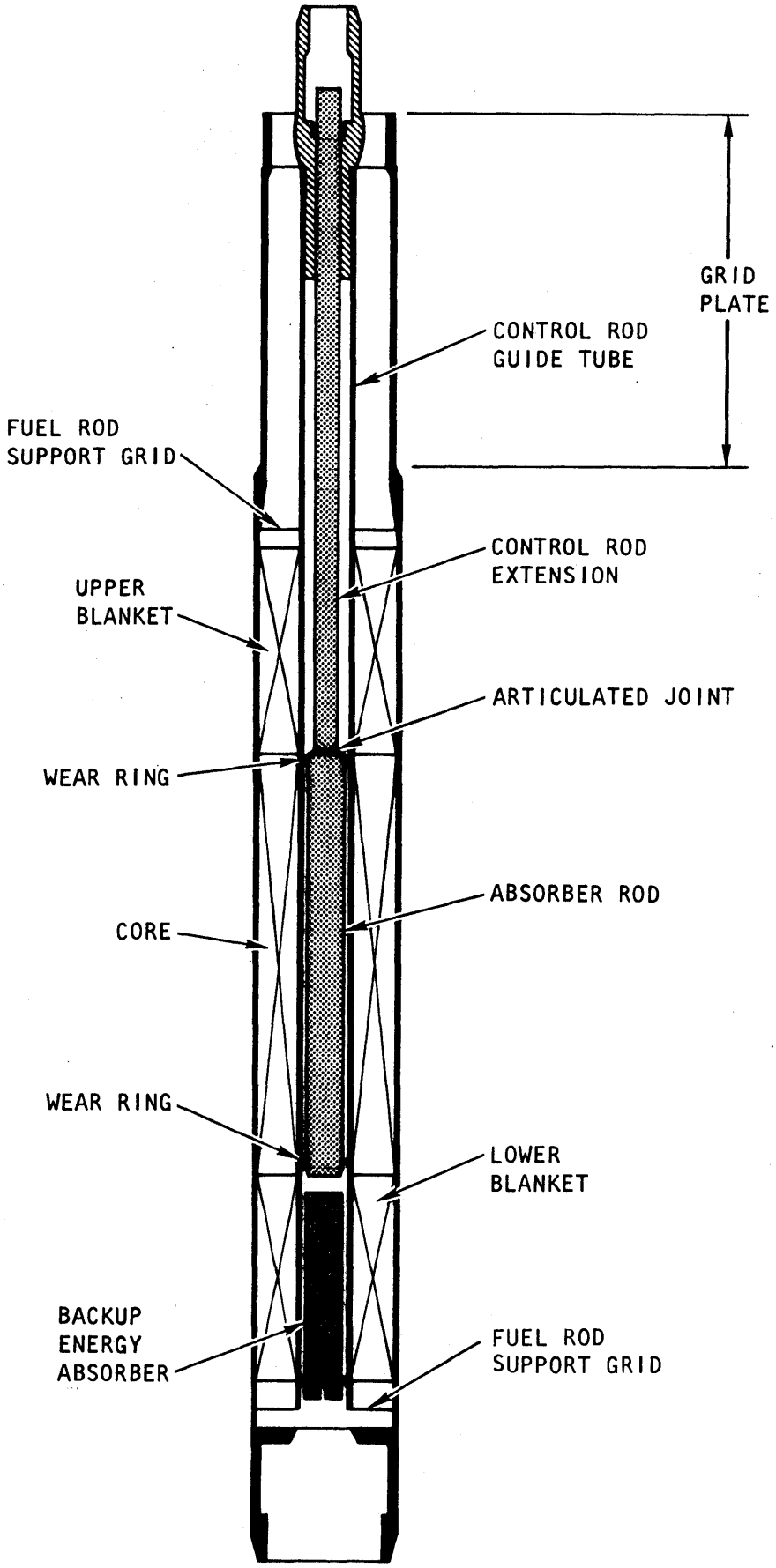


FIGURE 2.10 Schematic of a Control Element

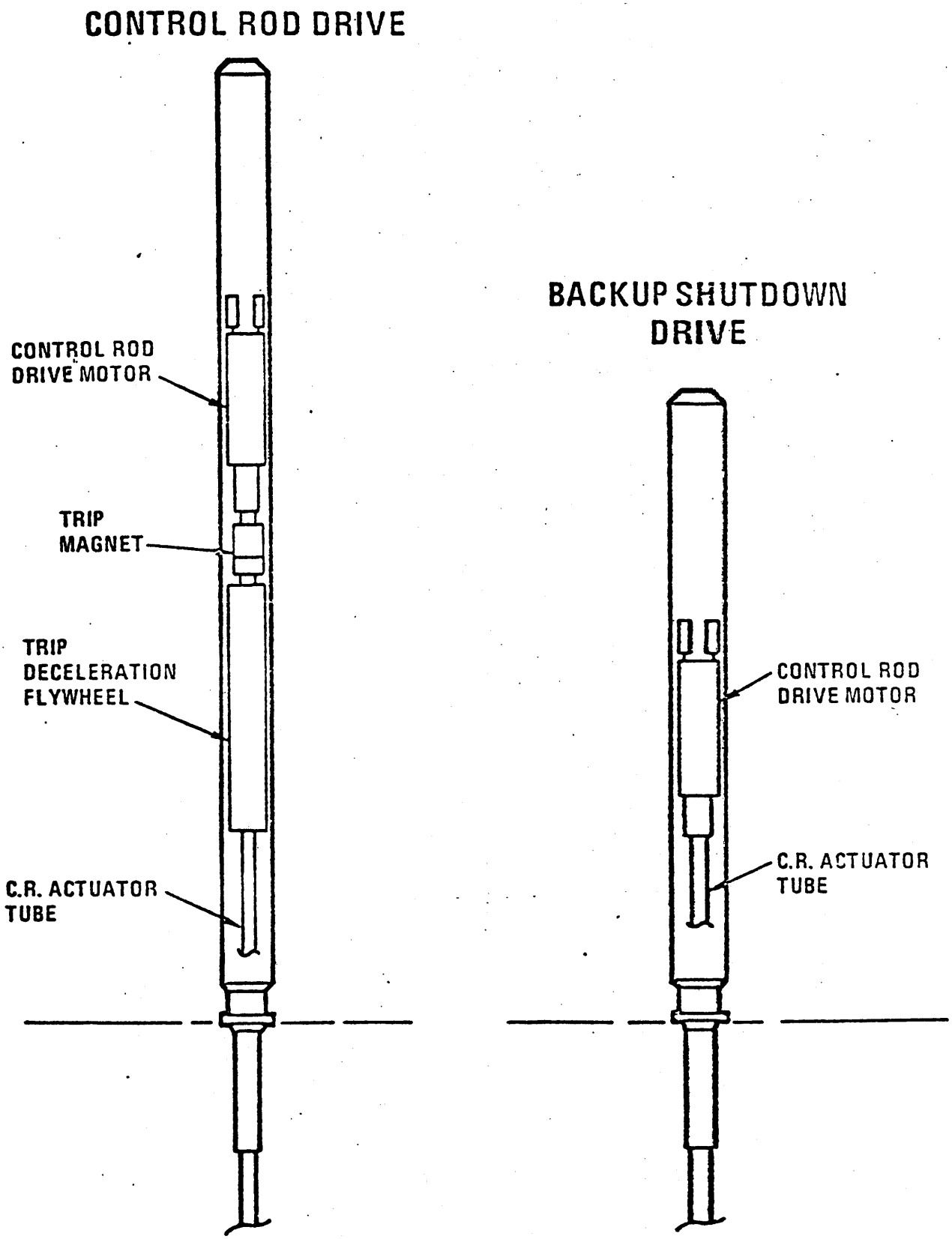


FIGURE 2.11 A Schematic of the Control and Shutdown Rod Drive Mechanisms

Table 2-III

A Summary of the GCFR Shutdown Systems Diverse Features

	Control Rod System	Backup Shutdown Rod System
Control Element		
Worth $	0.85	1.60
Diametral Clearance (in.)	0.05	0.20
Wear Rings	Yes	No
Drive		
Power Supply	Plant Control Rod Drive Power Supply	Individual Battery for Each Drive
Motor	Slow Speed, Stepping Motor	Constant Speed DC Motor
Trip Insertion	Magnet Release, Initial Spring Assistance, Gravity Fall	Power Driven Insertion, Initiated by All Trip Signals
Trip Snubber	Cam Operated Flywheel	None Required
Performance		
Regulating Mode	Yes	No
Trip-Insertion Times (sec.):		
Core Midplane	0.3	5
Full Insertion	0.5	9

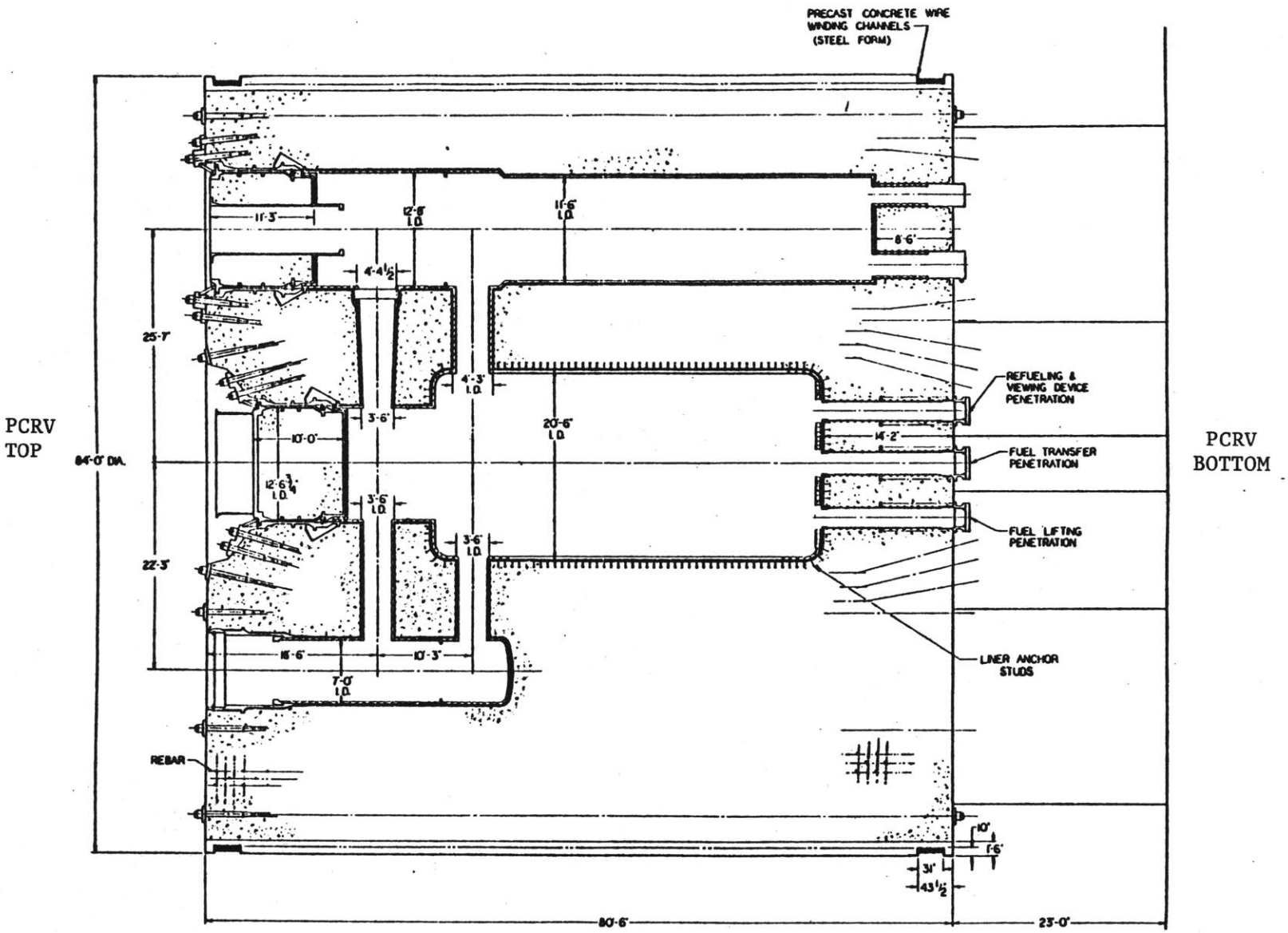


FIGURE 2.12 A Verticle Cross-section of the PCRV

2.2-7 The Prestressed Concrete Reactor Vessel (PCRV)

The PCRV is a multicavity pressure vessel which serves as the primary containment for the reactor core, the primary coolant system, and portions of the secondary coolant system. It is a thick-walled cylindrical concrete structure which contains a cylindrical central cavity for the reactor core and core support structures. The central cavity is surrounded by six cylindrical cavities. Three of these contain the main helium circulators and steam generators, and the other three contain the auxiliary circulators and auxiliary heat exchangers. Radial coolant ducts connect the top of the central cavity to all of the peripheral cavities. The upper end of the central cavity and the steam generator cavities are sealed by concrete closures. Figure 2.12 is a drawing of a vertical cross-section through the PCRV.

All of the PCRV cavities, ducts and penetrations are lined with steel liners that act as impermeable gastight membranes to contain the helium coolant. These, in turn, are lined with thermal insulation to protect the vessel from the high helium temperatures. The liner is also equipped with cooling coils on the concrete side which act to maintain acceptable concrete temperatures. Each PCRV penetration is equipped with a leaktight closure that is sealed to the liner by a gasketed joint or by welding. All of the penetrations are provided with flow restrictor means of limiting the leakage flow area in the event of a closure seal

failure, and at least two independent means of transferring the pressure load from the primary closure to the PCRV structure are provided.

The PCRV is constructed with high strength concrete that is reinforced with bonded reinforcing steel. The concrete vessel is prestressed vertically by a multiplicity of linear steel tendons, and the radial prestress is provided by bands of circumferential wire wrapping. The prestressing creates compressive stresses in the concrete which remain even at the maximum design internal cavity pressure. A high degree of structural integrity and strength are attained by the highly redundant amount of prestressing and reinforcing steels. The vertical tendons are located in metal conduits, and the circumferential wire strands are placed in steel channels around the outer surface of the PCRV. Not only are many redundant tendons and wire strands used, but the wire tension in typical locations can be monitored during operation and over the design life of the plant to assure that appropriate compressive stresses are available.

2.2-8 Plant Control and Protection Systems

The control and protection functions in the GCFR are provided by three separate systems. These are:

1) the Plant Control System (PCS), which regulates the plant in all normal modes of operation;

2) the Operational Protection System (OPS), which initiates actions intended to limit damage to the plant in fault situations which do not entail immediate risk to the health and safety of the public; and
3) the Plant Protection System (PPS), which initiates appropriate actions to mitigate the consequences of system or component failures where the health and safety of the public may be involved.

The Plant Control System

This system provides three separate functions. These are: 1) the normal on-load plant control; 2) shutdown heat removal control actions; and 3) control of the long-term decay heat removal operations.

The normal on-load portion of the control system is designed to provide automatic plant regulation in accordance with load demand between 25 and 105 percent of the rated load. Over this range, the steam pressure and temperature at the main turbine throttle should remain approximately constant. Also, as a result of directing the full steam generator output to drive the circulator turbines, the helium flow and steam flow both vary in proportion to the load. Therefore, the helium temperature rise through the core should remain constant. The helium

temperature level, however, will vary slightly due to heat transfer considerations.

The shutdown heat removal function of the plant control system is accomplished by individual shutdown control systems for each main loop. Each of these consists of a shutdown controller, which regulates the throttling of the circulator-turbine small control valve, and a resuperheater bypass controller, which regulates the resuperheater bypass control valve. The shutdown controller functions to maintain acceptable helium temperatures by controlling the steam flow for the circulator turbine. The resuperheater bypass controller functions to maintain the circulator-turbine exhaust pressure proportional to the reactor coolant inlet pressure. This function maintains the proportionality of the steam flow to the helium flow.

The decay heat removal control functions are also provided by separate control systems. These operate whenever the main circulator-turbines are being supplied by steam from the auxiliary boilers. They provide control of the circulator speed for long-term decay heat removal requirements.

The Operational Protection System

The OPS serves to prevent or limit damage to the plant in fault situations which do not present an immediate risk

to the public health and safety. It thereby serves to increase the plant availability.

The OPS provides four major actions:

1) automatic loop shutdown;

2) steam generator dump;

3) programmed load reduction; and

4) rod-withdrawal prohibit.

The signals initiating these actions are summarized in Table 2-IV, and these OPS actions are described in more detail below.

Automatic Loop Shutdown

In the event of a failure in a single main cooling loop, the loop can be shutdown and isolated by 1) closing the feedwater inlet and resuperheater outlet isolation valves, and 2) closing the circulator-turbine large control valve for the loop. These actions stop the helium circulator and allow the loop isolation valve to close. The signal that causes automatic loop shutdown also initiates a programmed load reduction to 60 percent power.

Steam Generator Dump

The indication of a high coolant-moisture level in a particular loop will trigger an automatic loop shutdown followed immediately by the opening of the valve connecting the steam generator to the

Table 2-IV

A List of Operational Protection System Parameters and Protective Actions

Sensed Plant Parameter	Indications	Automatic Loop Shutdown	Steam Generator Dump[a]	Programmed Load Reduction	Rod-withdrawal Prohibit
Loop reactor-coolant moisture	High	Yes	Yes	To 60% level	No
Loop resuperheater steam pressure	Low	Yes	No	To 60% level	No
Loop acoustic monitor	High	Yes	No	To 60% level	No
Loop feedwater pressure	Low	Yes	No	To 60% level	No
Loop superheat steam temperature	Low	Yes	No	To 60% level	No
Loop safety valves	Open	Yes	No	To 60% level	No
Loop circulator bearing-water pressure	Low	Yes	No	To 60% level	No
Loop circulator speed	High	Yes	No	To 60% level	No
Reactor-coolant pressure	High	No	No	To 25% level	No
Reactor-coolant pressure	Low	No	No	To 25% level	No
Anomalous reactivity	High/Low	No	No	To 25% level	No
Main turbine stop valves	Close	No	No	To 25% level	No
Main boiler feedpump flow rate	Low	No	No	To 60% level	No
Main steamline pressure	Low	No	No	To 25% level	No
Main turbine control valves closure rate	High	No	No	To 25% level	No
Rate of neutron-flux change	High	No	No	No	Yes
Neutron-flux level	High	No	No	No	Yes

[a]Following loop shutdown, the contents of the steam generator are dumped.

steam generator dump system. The entire contents of the steam generator can be dumped thus limiting the leakage of steam into the reactor coolant.

Programmed Load Reduction

A programmed load reduction is accomplished by the rapid automatic insertion of one or more control rods. Also, the plant load index is adjusted to the lower load value so that the plant control system can reestablish steady state conditions at this new power level. Operator intervention is required at this point to determine whether the plant can continue operating at the reduced power, or if an orderly shutdown is required.

Rod Withdrawal Prohibit

This action terminates the withdrawal of any control rods and thus prevents further positive reactivity insertion.

The OPS is independent of the plant protection system. However, the two systems do receive some inputs from common sensors, and in some cases actuate the same valves.

The Plant Protection System (PPS)

The PPS includes all electrical and mechanical devices and circuitry involved in generating signals associated with protective functions. These include those that 1) initiate

reactor shutdown, and 2) in the event of a serious reactor accident, actuate the engineered safeguard systems.

The initiation of a reactor shutdown signal actuates both the control rod system and the shutdown rod system along with the other plant actions necessary in the shutdown heat removal process. (These are described in detail in section 2.3-2.)

Table 2-V is a list of the trip parameters for the PPS. Item 15, two-main-loop trouble, is an interlock with the operational protection system which initiates a reactor shutdown in the event that the OPS receives signals from two main loops.

The engineered safeguard features include 1) the CACS and those portions of the main loop cooling system necessary to provide adequate core cooling during the start-up of the CACS; 2) the containment isolation system; and 3) the containment-atmosphere cleanup system.

2.3 Reactor Coolant System Operation

2.3-1 Main Loop Operation

The main loop cooling system primary side consists of the steam turbine-driven helium circulators, the steam generator and the main loop isolation valves. The secondary side of this system is the steam/water power cycle which drives the main turbine-generator set. The major components

Table 2-V

Plant Protection System Trip Parameters

1.	Manual	---
2.	Neutron flux	High
3.	Power-to-flow ratio	High
4.	Reactivity	High/low
5.	Reactor-coolant moisture	High
6.	Delayed-neutron activity	High
7.	Reactor-coolant pressure	High/low
8.	Reactor-coolant outlet temperature	High
9.	Containment pressure	High
10.	Circulator speed (rate of increase)	High
11.	Main feedwater pressure	Low
12.	Main feedwater flow	Low
13.	Condenser pressure	High
14.	Essential bus voltage	Low
15.	Two-main-loop trouble	---

of this system are described in Figure 2.4, however, a more detailed schematic flow diagram for the secondary coolant system is presented in Figure 2.13.

The steam/water flow path for the normal operation of the system is defined by the heavy lines. The entire amount of steam leaving the steam generator passes to the control valves for the main loop helium circulator drive turbine. At a point just prior to these valves, some steam is diverted to drive the bearing-water pump-turbine for the main circulator water bearings. The remainder passes through the circulator-turbine control valves to drive the helium circulator. The location of the steam take-off to the bearing-water pump-turbine ensures it of a continuous supply of steam.

The arrangement of the circulator-turbine control valves is very important. There are two valves arranged in parallel; these are the circulator-turbine large control valve (CT large CV) and the circulator-turbine small control valve (CT small CV). The CT large CV is designed for full steam flow and it is used for the control of the circulator-turbine during normal operation. The CT small CV is sized to pass only 12 percent of the normal full load steam flow. It is fully open during the normal operation of the reactor.

After being exhausted from the circulator-turbine, the steam is then returned to the steam generator module where

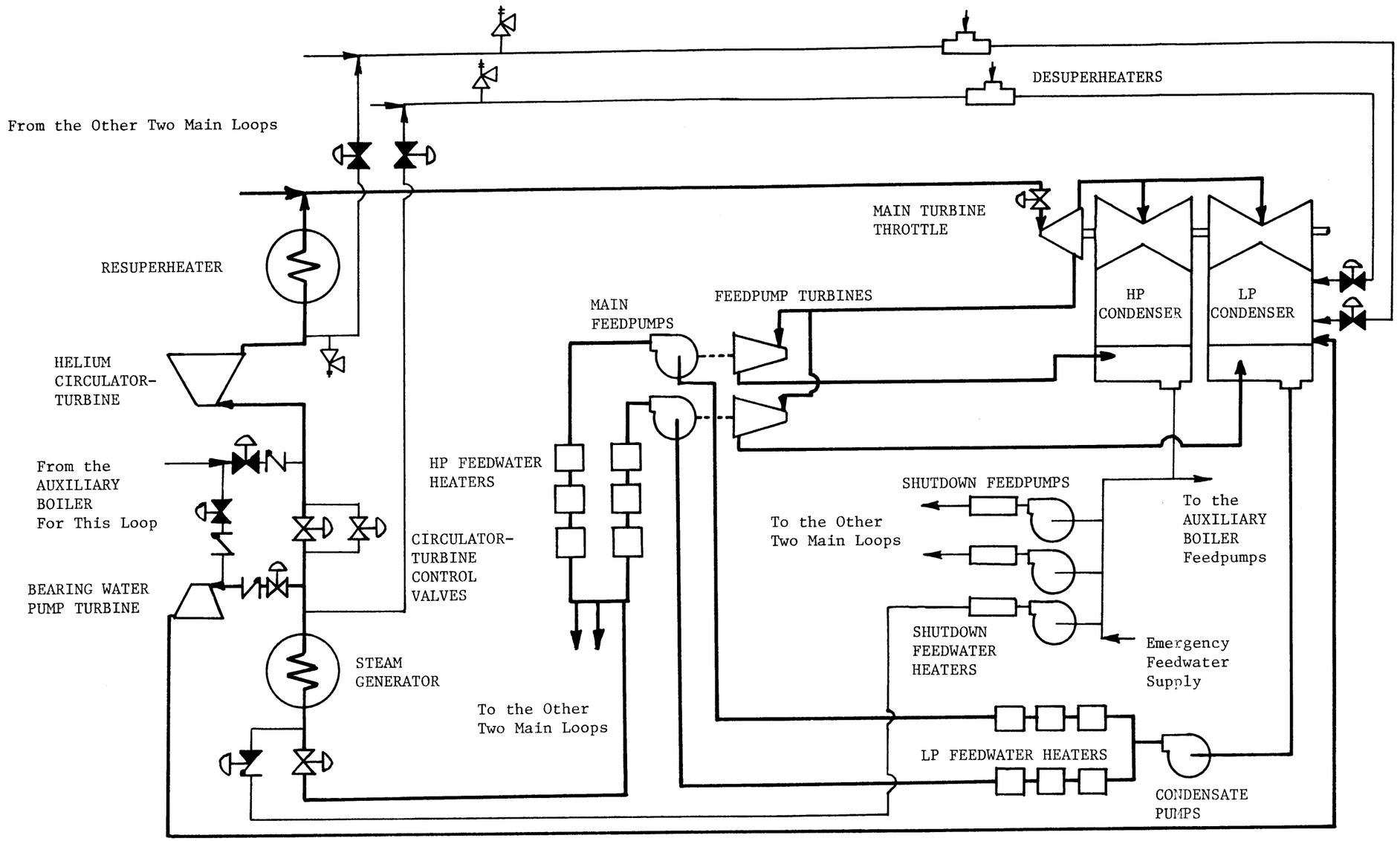


FIGURE 2.13 A Schematic Flow Diagram of the Secondary Coolant Normal Operating Mode.

it is resuperheated. This resuperheated steam combines with the steam from the other two main loops, after it leaves the containment building, to drive the main turbine-generator set. The main turbine exhaust-steam is condensed in the main condenser, and the condensate collected in the hotwell is pumped through a condensate demineralizer and three stages of feedwater heating by the condensate pumps. The main boiler feed pumps, which are turbine-driven by extraction steam from the main turbine, direct the feedwater through three more stages of heaters before it enters the steam generators. After the condensate demineralizer, the feedwater flows through two separate, parallel trains, each of which contains three low pressure feed water heaters, a feedwater pump, and three high pressure feedwater heaters.

2.3-2 Shutdown Cooling Operation

The main cooling loops are designed to provide continuous core cooling during a reactor shutdown. This is accomplished by continuing operation of the main helium circulators using the steam generated by the decay heat to drive the helium circulator-turbine.

The plant protection system is designed such that the same signal which scrams the reactor (called the reactor shutdown initiation signal) also trips the main turbine throttle valve closed. The closing of the main turbine throttle initiates a signal causing the resuperheater

bypass valve to open. This valve regulates the circulator-turbine exhaust pressure and directs this steam flow to the main condenser. However, failure of this valve either to open or to regulate properly may not be crucial; both safety and relief valves in the system will provide adequate turbine exhaust should the regulating valve fail. Figure 2.14 is a flow diagram for the shutdown cooling operations.

Notice that the closing of the turbine throttle eliminates the steam supply for the main feed pump turbines. The shutdown initiation signal, coupled with an additional signal from the plant protection system which verifies the fact that the reactor has actually shut down, causes the rapid closure of the CT large CV. This action is necessary to prevent the rapid depletion of the inventory of steam/water in the steam generator. The steam flow to drive the circulator-turbine is maintained by the CT small CV, and the shutdown control system regulates this valve to maintain the helium temperature within acceptable limits.

The operation of the plant at this point is limited by the depletion of the steam generators, which occurs in about thirty minutes if all three loops are operating. However, the shutdown initiation signal also starts the shutdown boiler feed pumps. These are electrically driven pumps which are designed to deliver two percent of the normal feedwater flow. There are three individual pumps; one for each of the

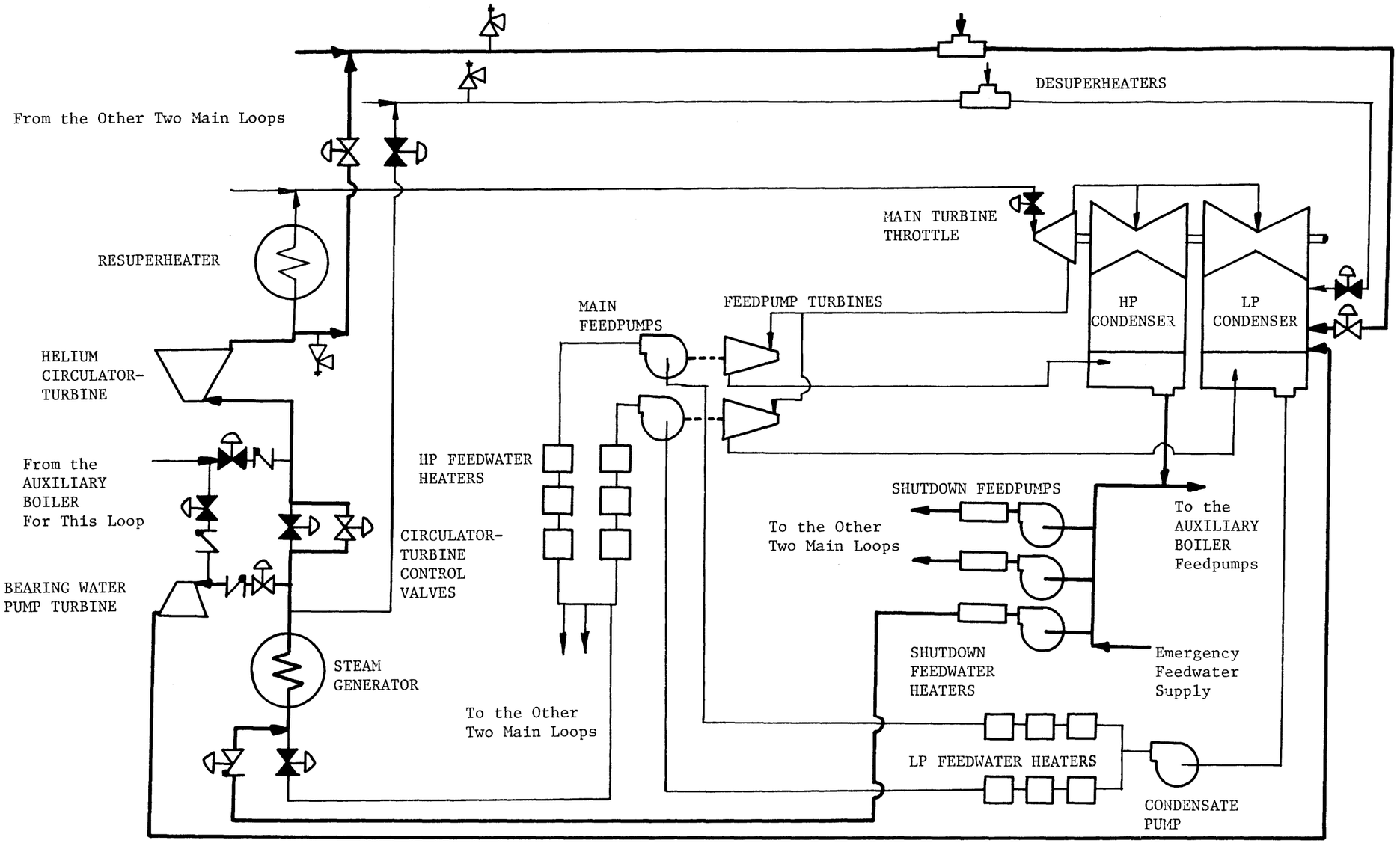


FIGURE 2.14 A Schematic Flow Diagram of the Secondary Coolant Shutdown Cooling Operating Mode.

main loops. These pumps draw from a common suction header which is connected directly to the condenser hotwell. The start-up of these pumps is not critical to the initial operation of the main loops. However, the feedwater they supply to the steam generators will prevent depletion of the steam/water inventory.

The operation of the main loops, in this operating state, is limited only by the quality of the steam produced in the steam generators. After 40 to 50 minutes, the quantity of steam produced is no longer sufficient to drive the circulator-turbines, and a secondary source of steam is needed to continue core cooling with the main loops. Note that the bearing water pump is supplied with steam as long as there is steam to drive the circulator-turbine.

2.3-3 Decay Heat Removal Operation

To provide for continued shutdown cooling operation of the main loops, oil-fired boilers are provided to supply the necessary steam to drive the main helium circulator turbines. These boilers are maintained in a hot standby condition, while the reactor is operating, by steam heating coils, and there are three independent boiler units. Each unit is aligned with a single main loop, and by opening the correct combination of valves, the unit will supply steam to drive both the circulator-turbine and the bearing-water pump-turbine. These boilers will be designed to achieve

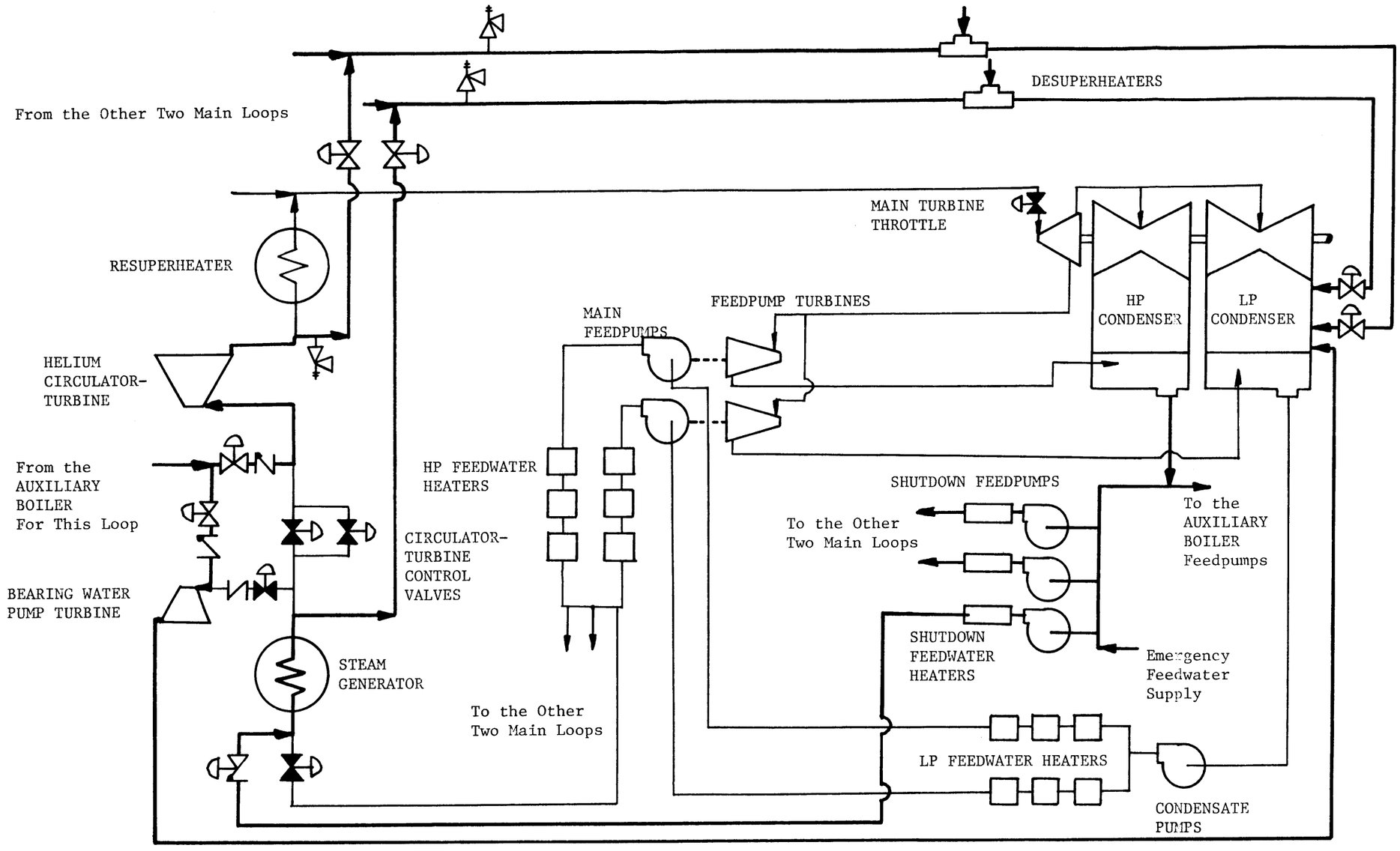


FIGURE 2.15 A Schematic Flow Diagram of the Secondary Coolant Decay-heat-removal Operating Mode.

their full-rated steaming condition twenty minutes after receipt of the shutdown signal. Figure 2.15 is the flow diagram for the decay heat removal operation.

The operation of these boilers will allow continued helium circulation with the main loops. However, to continue heat removal with the main loops, water must be continuously circulated through the steam generator. This is accomplished by the continued operation of the shutdown feed pumps and by the alternate discharge path provided to direct the steam/water exhaust from the steam generator to the main condenser. If the main condenser is unavailable or if the alternate discharge path regulating valve should fail to open, relief valves are provided to assure adequate flow. The operation of the main loops can now continue indefinitely, assuming the correct functioning of all equipment. However, if the main condenser is unavailable, then the main loop operation is dependent upon back-up supplies of feedwater.

2.3-4 Main Loop Shutdown Performance

Figure 2.16 indicates the main loop cooling system response to a reactor trip in which the reactor shutdown systems function normally. Shown in the figure are the core outlet temperature, maximum clad hot-spot temperature, helium flow rate, and the steam generator outlet pressure and percent of inventory for the first thirty minutes following the shutdown.

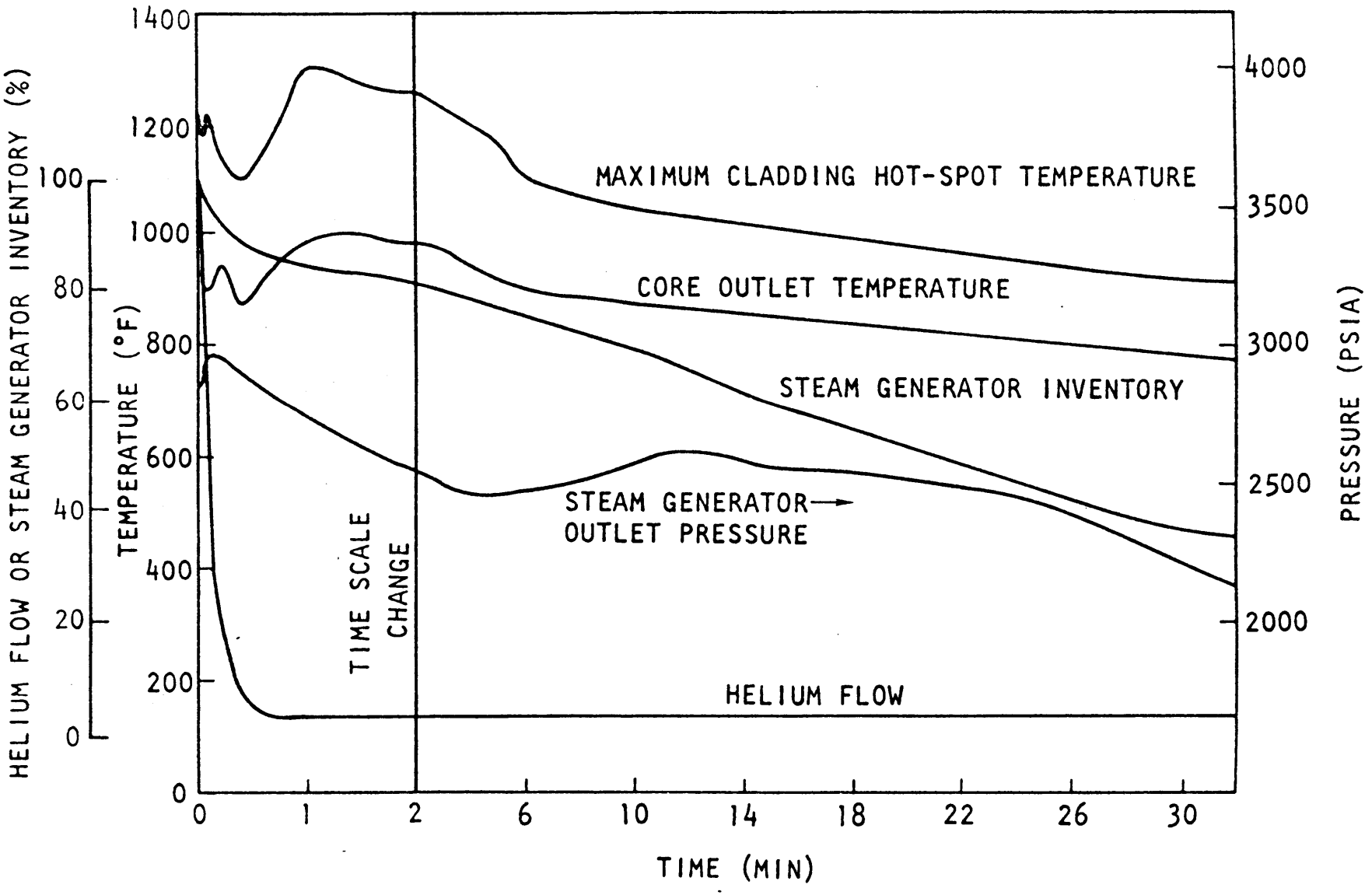


FIGURE 2.16 Main Loop Cooling System Response Following a Reactor Trip

With the insertion of the control rods and shutdown rods, the reactor power decreases rapidly to the decay heat level. The helium flow rate decreases more slowly due to the closure rate of the CT large CV ($\sim$ 3 seconds), and the helium circulator-turbine inertia. This causes a temporary overcooling of the core. After this, a mild temperature transient is observed. This results from the CT small CV controller action. Should the CT small CV throttle rapidly in the initial period following the shutdown, a lower helium flow rate and higher core temperatures will result. However, the steam generator inventory will be conserved, and main loop operation can be extended. If the CT small CV throttles slowly, lower core temperatures result, but steam generator inventory depletion occurs sooner. The design of the shutdown controllers has not yet been finalized, and so the results shown in Figure 2.16 are only preliminary.

2.3-5 CACS Operation

If at any time during the shutdown cooling operations the main loops fail to provide adequate helium circulation, the CACS is available to immediately take over core cooling. The major components of the primary and secondary sides of this system are described in Figure 2.13, and a detailed schematic flow diagram is provided in Figure 2.17. During normal reactor operation, the auxiliary helium circulator is stopped and the auxiliary loop isolation valve closed. The

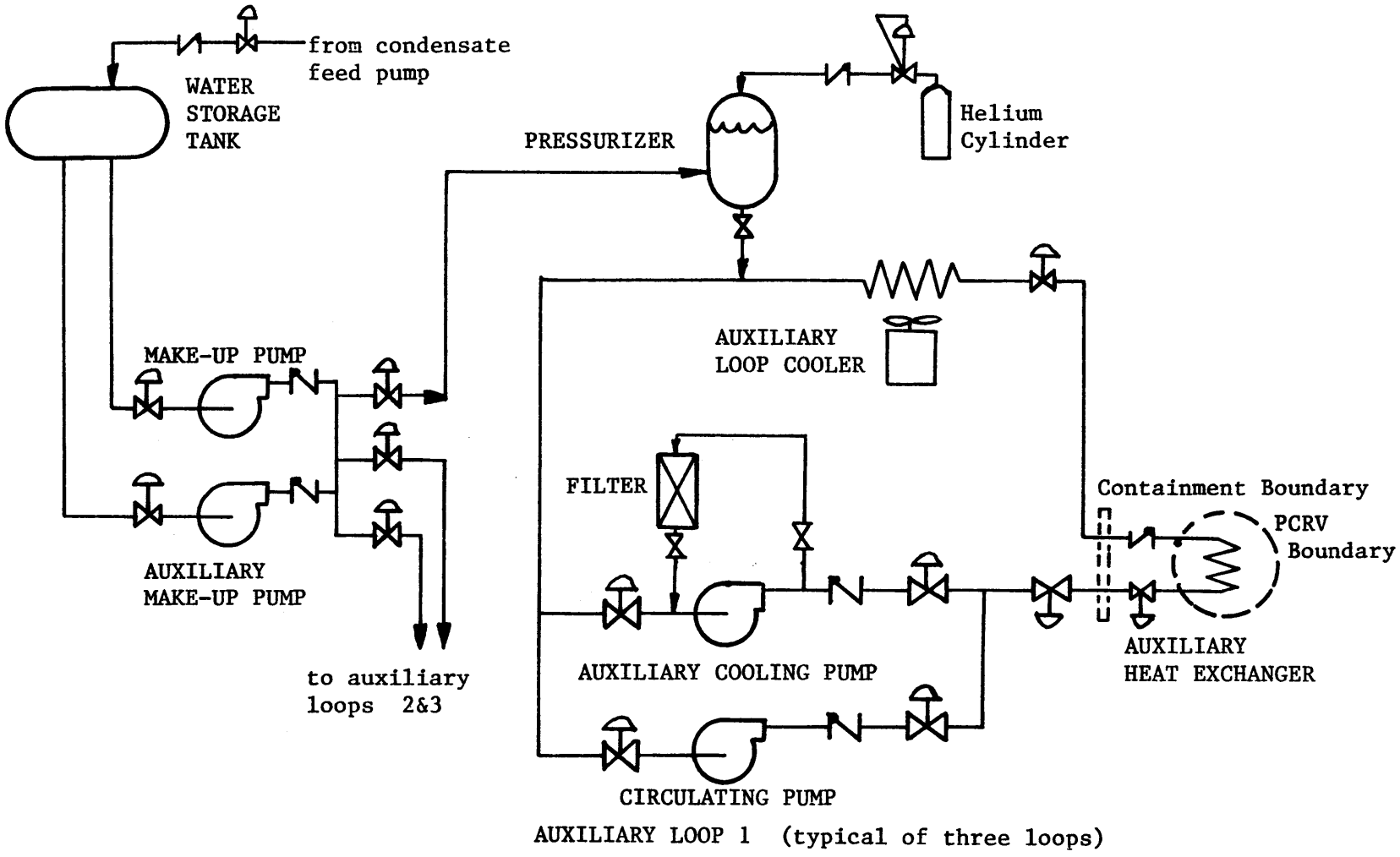


FIGURE 2.17 A Schematic Flow Diagram of the Core Auxiliary Cooling Water System.

The auxiliary circulating pump provides a small flow of pressurized water through the heat exchanger to maintain acceptable tube temperatures and to prevent thermal shock when the system is started in order to provide emergency cooling. This small heat loss from the reactor is rejected to the atmosphere by natural draft in the auxiliary loop cooler.

Upon receipt of the shutdown initiation signal, the CACS is brought to a ready condition. The auxiliary helium circulator is started and run at idle speed and is available to begin circulating helium at any time thereafter that the main loops fail.

2.3-6 Cooling System Arrangement

The intent of the design of the three main cooling loops is to make the loops as independent as possible so as to minimize the possibility of common mode failure eliminating all the loops. Thus, each main loop has its own separate support system for the helium circulator, its own shutdown boiler feed pump, and its own auxiliary boiler. In addition, all of the essential equipment for each of the loops, except for the auxiliary boiler, are supplied from a separate electrical bus. In the present design, the auxiliary boilers are supplied from the plant's non-essential electrical bus. These and some other cooling system characteristics are summarized in Table 2-VI.

Table 2-VI

A Summary of the Shutdown Cooling Operating Characteristics

	Main Cooling System	Auxiliary Cooling System
Readiness for Shutdown	Operation Continues	Can Start Heat Removal At Approx. 10 Sec.
Number of Loops Required	2 of 3 for DBDA 1 of 3 for Other Events	2 of 3 Equals Decay Heat At 2 Min; 1 of 3 After 15 Min
Electric Power Required	Not Essential for 15 Min	Yes
Seismic Capability	Category I for 30 Min (Limited by Feed Water Supply System)	Category I
Support Systems	Separate Shutdown FW Pump and Auxiliary Boiler for Each Loop	Separate Pressurized Water Loop and Air Cooler for Each Loop
	Separate Circulator Service Modules for Each Loop	Separate Circulator Service Modules for Each Loop
	Each Loop Fed by Different Essential Bus	Each Loop Fed by Different Essential Bus

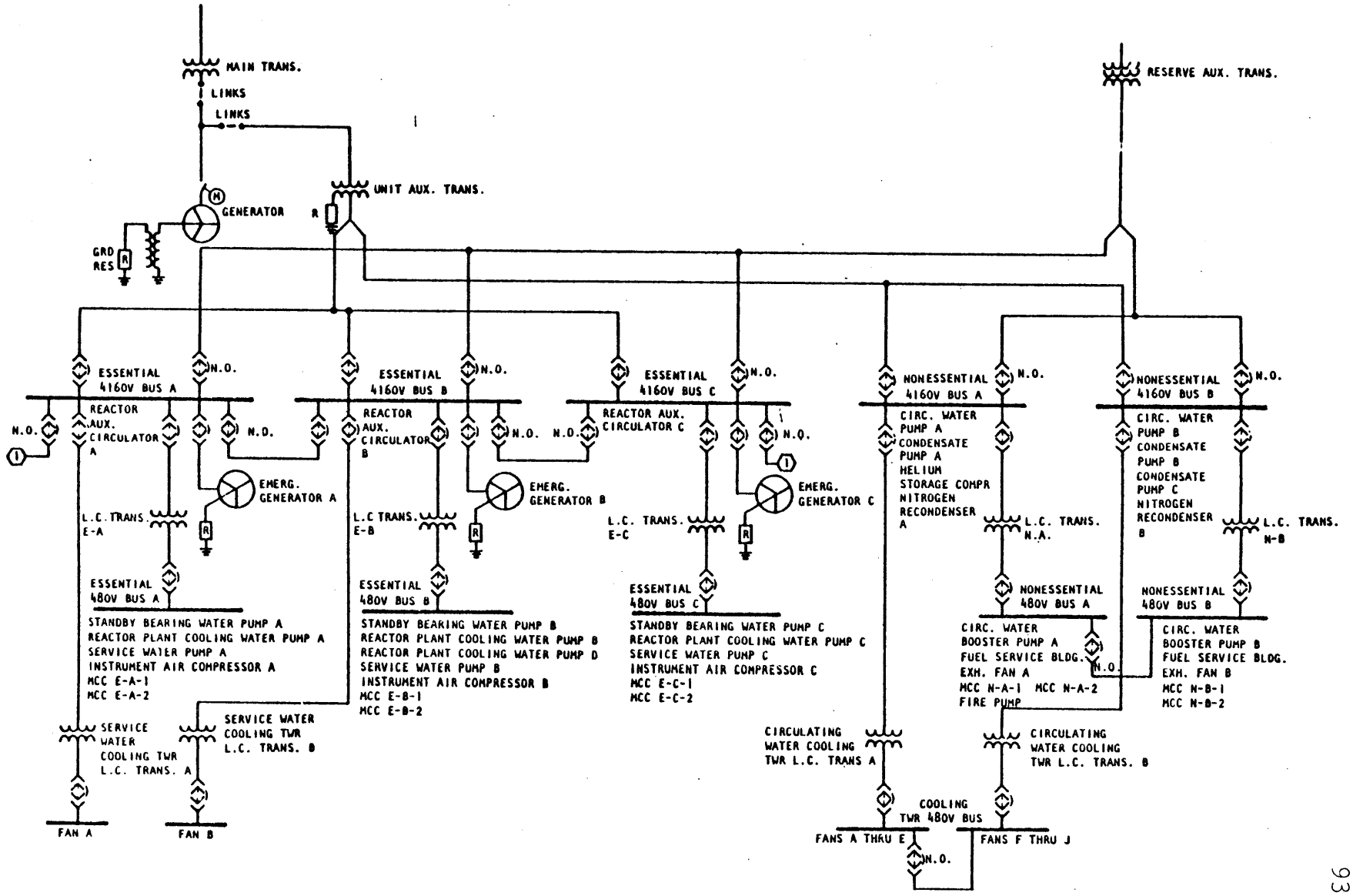


FIGURE 2.18 Plant electrical system single line diagram

TABLE 2-VII

DISTRIBUTION OF REDUNDANT LOADS AMONG ESSENTIAL BUSES

Load	Units Fed from			Connected hp per Unit[a]	Bus Voltage
	Bus A	Bus B	Bus C		
Core main cooling system					
Circulator standby bearing water pumps	A	B	C	180	480
Essential instrumentation and control	A	B	C	(b)	120 uninter.
Core auxiliary cooling system					
Helium circulators	A	B	C	500	4160
Main circulating water pumps	A	B	C	15	480
Auxiliary circulating water pumps	A	B	C	1	480
Makeup water pumps	A	B	C	(b)	480
Heat dump fans	A	B	C	30	480
Instrumentation and control	A	B	C	(b)	120 uninter.
Service-water system					
Pumps	A	B	C	150	480
Cooling tower fans	A	B		200	4160
Reactor plant cooling water system					
Pumps	A	B,D	C	125	480
Instrument and service air system					
Compressors	A	B	C	125	480
Ventilation systems					
Containment supply fans	A		B	7.5	480
Containment cooling fans	A	B	C	40	480
Containment exhaust fans	A		B	40	480
Containment cleanup fans	A	B	C	15	480
Control room emergency system	A	B	C,D	10	480
Emergency lighting and communication systems	(Redundant loads will be distributed among buses A, B and C)				

[a] Tentative estimates subject to change as the design proceeds beyond the conceptual stage.

[b] No estimate available at this early stage.

The essential electrical loads are supplied from the three essential buses as described above. Each of the essential buses is fed from both the main turbine generator unit of the plant through the unit transformer, and an offsite power source. Also, each bus is equipped with its own separate diesel generator to supply the essential loads when the two primary sources of power are lost. Figure 2.18 is a schematic single line diagram of the plant AC electrical system. It indicates both the essential electrical buses and the non-essential buses, and a listing of the major component loads carried by each of the electrical buses is provided in Table 2-VII.

2.4 Shutdown Cooling System Capabilities

2.4-1 Main Loop Shutdown Cooling System Capabilities

There are two general heat removal periods following a reactor shutdown. First is the shutdown-heat-removal phase in which the cooling system must reduce the plant heat load to the decay heat level, and second is the decay-heat-removal phase. The initial phase lasts the first twenty to thirty minutes, and during this period, the design intent is to keep the main loops operating (maintaining acceptable core temperatures) long enough to get the auxiliary boilers to their rated steaming condition. If all three of the main loops function as designed, then

the time margin available for firing up the auxiliary boilers is quite large (40 to 50 minutes).

The correct operation of each main loop depends upon the functioning of each of its separate subsystems. Furthermore, the overall core cooling capability of the main loop cooling system is dependent on both the number of main loops operating and the state of operation of those loops. This last point can be illustrated by considering the operation of the three pieces of equipment most important to correct main loop operation. These are the CT large CV, the CT small CV, and the shutdown feed pump. If the CT large CV for a particular loop fails to close, the steam generator inventory for that loop will be quickly depleted within one or two minutes, and the loop will no longer provide any shutdown heat removal. The core cooling process will continue with two main loops, which is well within the design margin. However, these two loops individually will have to circulate more helium than they normally would have had all three loops been operating.

The failure of a CT small CV to throttle down will also cause the steam generator inventory for the loop to deplete, but this will occur over a longer time period than results from failure of the CT large CV. The failure of a shutdown feed pump to deliver feedwater will also limit the availability of the main loop by allowing the steam generator inventory to deplete. However, more importantly,

the shutdown feed pump is essential to the operation of the auxiliary boiler in the decay heat removal phase. Thus, failure of the pump eliminates the possibility of providing decay heat removal with the main loop irrespective of whether the auxiliary boiler is available or not.

One more item in the operation of the main loops needs mention. That is the main loop isolation valves. Whenever steam generator depletion occurs, and a main circulator stops, the operation of the other circulators should cause the self-actuating isolation valve on the failed loop to close. If the valve fails to close, some helium flow bypassing the core through the shutdown loop will result. The actual amount of bypass flow is small, and the effect on core temperatures is not significant. This is because the bypass flow reduces the total flow resistance causing the helium circulators to speed up and compensate for the small bypass flow loss. However, this also causes them to use more steam; thus hastening the depletion of their steam generator inventories. Table 2-VIII lists the steam generator inventory depletion times as a function of the operating state of the main loop cooling system. The operating states are defined by the number of main loops operating (i.e., the number of loops without failed CT large CVs or CT small CVs), the number of operating loops supplied with feedwater, and the number of failed main loops allowing core-flow bypass. The values listed in the

table are the author's best estimates based on the present steam generator inventories and main helium circulator-turbine steam requirements following reactor shutdown.

In the event a PCRV depressurization occurs, the reactor shutdown cooling operations will be somewhat different. The correct operation of all three of the main loops will allow about thirty minutes to fire-up the auxiliary boilers before steam generator inventory depletion occurs. However, if one of the circulator-turbine control valves fails to function properly, its circulator will speed up to the overspeed trip point. Thus the circulator for that loop is eliminated almost immediately, and the cooling operations must proceed with two main loops. The failure of a shutdown feed pump or a main loop isolation valve will have a similar effect to that described for the pressurized reactor shutdowns. The steam generator inventory depletion times for shutdowns where the reactor is depressurized are listed in Table 2-IX. The design basis for the main loop shutdown cooling system following a depressurization accident is at least two main loops operating as opposed to only one for pressurized shutdowns. The operation of only a single main loop following a depressurization accident is limited to only a few minutes by the overspeed trip point of the circulator. The values listed in the table are the author's best estimates except where otherwise noted.

Table 2-VIII

A List of Steam Generator Depletion Times for Various Main Loop Operating States with the Reactor Pressurized

Number of Main Loops Available	Condition of Unavailable Main Loops	Number of Loops with Feedwater	Main Loop System Operating Time (minutes)		
			No Loop Bypass	1 Loop Bypass	2 Loop Bypass
3	--	3	>30	-	-
		2	>30	-	-
		1	>30	-	-
		0	~30	-	-
2	1 main loop shutdown, or with failed CT large CV	2	>30	25	-
		1	25	20	-
		0	17	15	-
	1 main loop failed CT small CV	2	>30	27	-
		1	27	22	-
		0	19	17	-
1	2 main loops failed CT large CVs	1	12	8	6
		0	8	6	5
	1 main loop failed CT large CV, 1 main loop failed CT small CV	1	14	10	8
		0	10	8	7
	2 main loops failed CT small CVs	1	17	13	11
		0	13	11	10
0	3 main loop failed CT large CVs	-	2	-	-
	3 main loops failed CT small CVs	-	10	-	-

Table 2-IX

A List of Main Loop Operating Times
for Reactor Shutdowns
Following a Depressurization Accident

Number of Main Loops Available	Number of Available Loops with Feedwater	Main Loop Operating Times (minutes)	
		Containment Equalization Pressure 1.8 Atm.	Containment Equalization Pressure 1.0 Atm.
3	3	>30	30
	2	>30	25
	1	>30	20
	0	30	15
2	2	25	4*
	1	20	
	0	15	
1	-	4*	2*
0	-	2	2

* limited by speed increase to the overspeed trip setpoint of the main circulators (Reference 6)

There is an additional complexity to be considered in the depressurized shutdown cooling operations. This is the effect of the containment equalization pressure. During a PCRV depressurization accident, the helium at 1300 psi will expand into the containment building volume and reach an equilibrium pressure in both the PCRV and the containment building. The present design is for an equalization pressure of 1.8 atmospheres. If the equalization pressure were lower the helium circulators would speed up due to the decreased helium density. The mass flow of helium through the core would also decrease due to this effect, although this would be counteracted somewhat by the increase in circulator speed.

Table 2-IX also lists the steam generator inventory depletion times (or main loop operation times) for shutdown cooling operations with an equalization pressure of one atmosphere. In all cases except where all three main loops operate, the main loop cooling system operation is limited by the overspeeding of the helium circulators.

In both the pressurized reactor shutdown cooling operations and the depressurized reactor shutdown cooling operations, decay heat removal will continue with the main loop cooling system only if the system has lasted at least twenty minutes, and also if those functioning auxiliary boilers correspond to the functioning main loops.

2.4-2 Core Auxiliary Cooling System Capabilities

If at any time after a reactor shutdown the main loop cooling system fails, the CACS is available to rapidly take over the shutdown or decay heat removal operations. Each CACS loop is sized to remove two percent of the full power heat load (for steady state operation), and the nuclear decay-heat level decreases such that at two minutes after the shutdown it is roughly four percent of the full power level. Two CACS loops are then fully capable of removing this decay heat and maintaining acceptable core temperatures. At fifteen minutes after the shutdown, the decay heat level is down to two percent of full power and only one CACS loop is then fully capable of core cooling.

The auxiliary circulators are driven by squirrel cage induction motors powered by a variable frequency power supply to allow variable speed operation over a large range. This is needed to account for the different design conditions of pressurized and depressurized operation. The design basis for the auxiliary circulator is actually determined by the operating requirements shortly after a design basis depressurization accident. This occurs about four minutes after initiation of the accident when the containment equalization pressure of 26.7 psia is reached.

Because of the depressurized design requirements, the helium circulation capability of the auxiliary circulators is quite large when the reactor is pressurized, and failures

of the main loop isolation values to close do not significantly affect the CACS performance [6]. However, during a depressurization accident, failure of the main loop isolation valves has a definite degrading effect on the CACS heat removal capabilities. Table 2-X lists the number of CACS loops capable of providing adequate decay heat removal, for various time intervals after imitiation of the shutdown, and as a function of the number of main loop isolation valves failing to open. These valves are based on the work in Reference 6.

The containment equalization pressure also has a significant effect on the CACS operation for depressurized reactor shutdowns. Table 2-X also lists the CACS capabilities for shutdowns in which the containment pressure equalizes at one atmosphere. These latter valves are the author's best estimates of CACS performance based on extrapolation and information from Reference 7.

Table 2-X

Core Auxiliary Cooling System Shutdown Cooling Capabilities

PRESSURIZED REACTOR SHUTDOWNS		
Time Interval following Shutdown during which Main Loop Failure Occurs	Number of Main Loop Isolation Valves Allowing Bypass-flow	CACS Loops Capable of Full Decay Heat Removal
before 15 minutes	0, 1, 2, 3	3, 2
after 15 minutes	0, 1, 2, 3	3, 2, 1

DEPRESSURIZED REACTOR SHUTDOWNS			
Time Interval following Shutdown during which Main Loop Failure Occurs	Number of Main Loop Isolation Valves Allowing Bypass-flow	CACS Loops Capable of Full Decay Heat Removal	
		CEP =* 1.8 Atm	CEP =* 1.0 Atm
before 5 minutes	0	3, 2	3
	1	3, 2	-
	2	3	-
	3	-	-
5 to 15 minutes	0	3, 2	3
	1	3, 2	3
	2	3, 2	-
	3	3	-
15 to 20 minutes	0	3, 2, 1	3
	1	3, 2	3
	2	3, 2	-
	3	3	-
after 20 minutes	0	3, 2, 1	3, 2
	1	3, 2	3
	2	3, 2	3
	3	3, 2	-

* CEP = Containment Equalization Pressure

Chapter 3
Methodology

3.1 Introduction

The major thrust of this research project has been directed at the analysis of the potential GCFR core-melt accident sequences following reactor shutdowns. The potential core-melt accident sequences following failure of the reactor to shutdown were not analyzed.

The accident analysis methodology of the RSS was utilized in the process of modelling the accident sequences following reactor shutdowns.[1] Because the GCFR is designed such that the main loop cooling system continues its heat removal functions from normal operation, through a reactor shutdown, to the shutdown and decay heat removal operations, the modelling of the shutdown event sequences was somewhat simplified. The shutdown cooling system response to the initiation of a reactor shutdown signal is identical in almost all cases whether it is a normal shutdown or a shutdown resulting from an anticipated plant transient. Thus, a single large modelling diagram of the reactor shutdown cooling operations was constructed for the majority of the types of reactor shutdown initiating events. In effect, one diagram

was used to model the shutdown cooling and decay heat removal operations when the reactor remains pressurized. Enough variation was included in the modelling to account for the slight differences in the plant response to different types of initiating events.

For initiating events which lead to a PCRV depressurization, a separate modelling diagram of the shutdown cooling operations was needed. This diagram accounted for the different design operating capabilities of the plant shutdown cooling systems following a PCRV depressurization accident.

This chapter presents the methodology used to model the events following the initiation of a reactor shutdown signal. Section 3.2 lays the foundation for the construction of the event sequence diagram (ESD), which is the model of the GCFR shutdown operations. The specific diagrams for the pressurized reactor shutdowns and for depressurization accidents are described in sections 3.3 and 3.4 respectively. Section 3.5 discusses how the individual event sequences were handled.

3.2 Event Sequence Modelling

3.2-1 Event Tree Modelling

To develop an initial understanding of the plant responses which were modelled, consider the simplified event tree shown in Figure 3.1. This event tree depicts the basic overall plant functions following the initiation of a reactor shutdown signal. The diagram indicates the initiating event

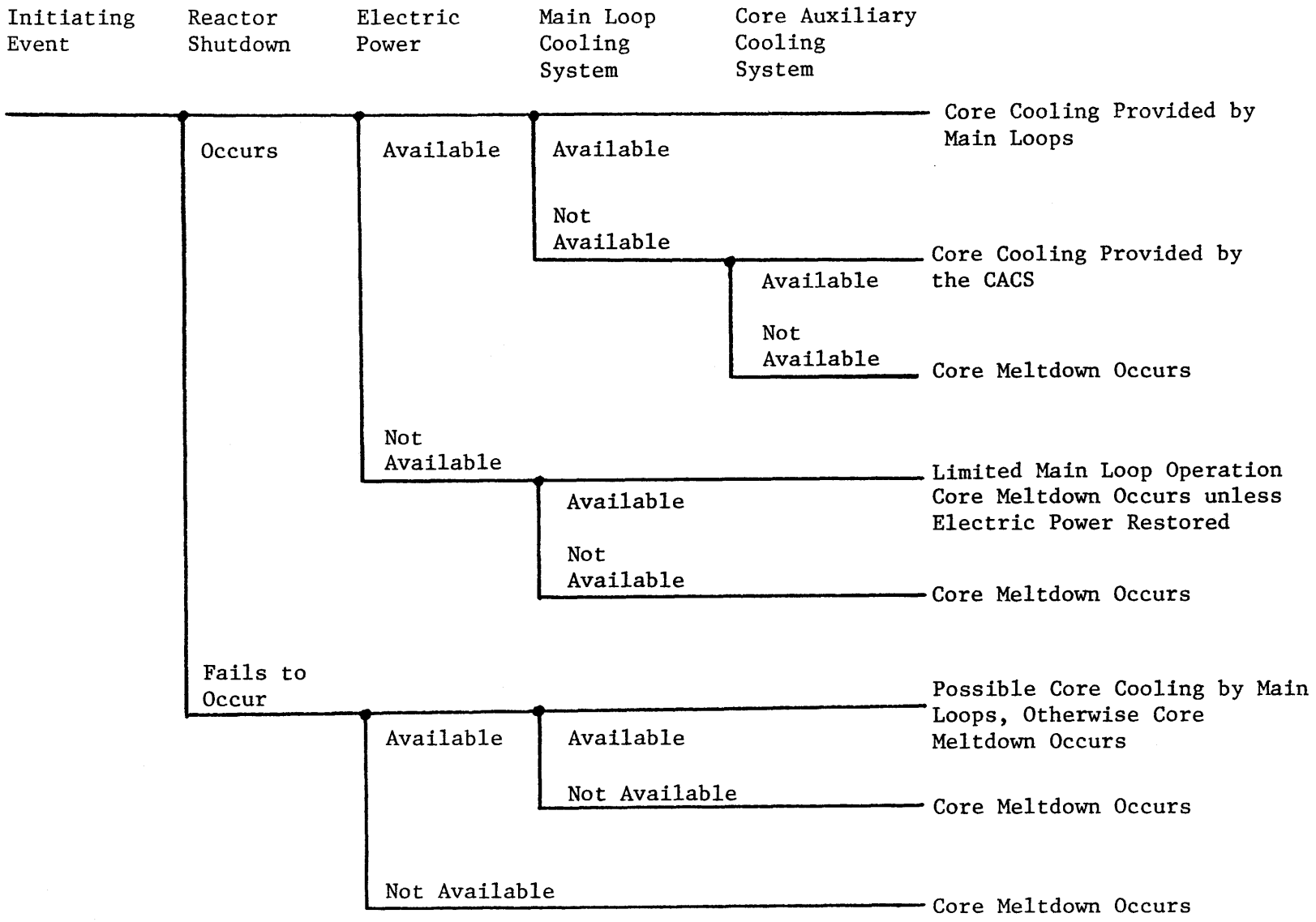


FIGURE 3.1 An Event Tree of the GCFR Shutdown Heat Removal Systems

followed by the two possibilities: reactor shutdown either occurs, or fails. It then considers the availability of electric power, which is necessary for CACS operation, and for extended operation of the main loops. The availability of either the main cooling loops or the CACS then dictate whether or not core meltdown will occur.

While this diagram helps in the understanding of the basic modelling approach, its usefulness in analyzing the plant operations is limited. This is basically because it does not allow a detailed description of the main loop cooling system capabilities, and because it does not allow consideration of the different successful CACS operating states.

The main loop cooling system operations need to be described in more detail so that the actual main loop cooling capabilities, for different operating states, can be reflected in the model. Figure 3.2 is an event tree diagram which describes how the shutdown cooling operations were modelled for a single main cooling loop. The diagram also shows the effect of the various shutdown cooling system components on the availability of a main loop. Given that a reactor shutdown occurs, failure of the resuperheater bypass discharge path was assumed to degrade the main circulator performance and result in the elimination of the loop. Failure of the CT large CV to close will cause the steam generator inventory to be exhausted in a few minutes, and this eliminates the loop. Failure of the CT small CV to throttle will also cause the

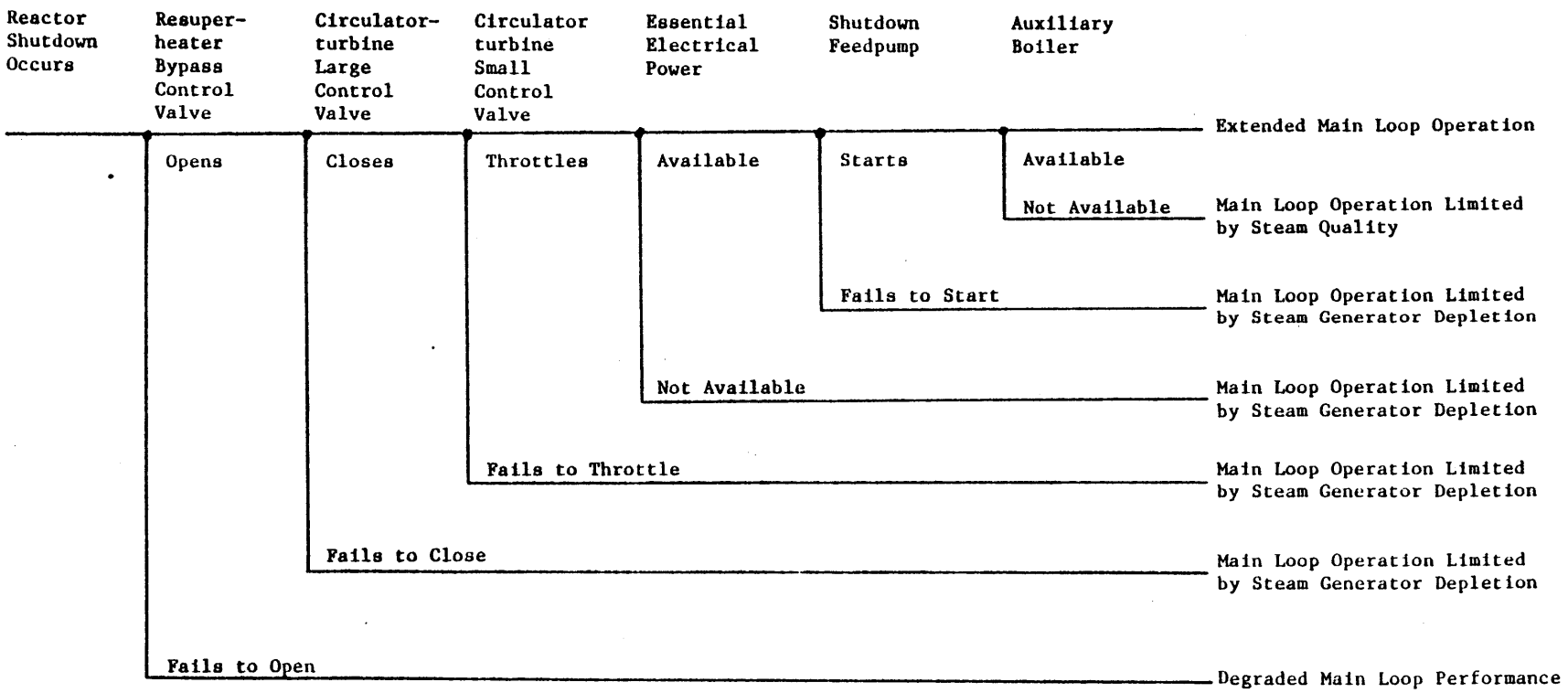


FIGURE 3.2 An Event Tree Diagram of the Shutdown Cooling Operations of a Single Main Cooling Loop

steam generator inventory to be exhausted sooner than desired, but it would allow operation of the loop for a considerably longer period of time compared to the case where the large valve is open. The availability of AC electric power is not considered until this point because the previous valve operations do not require it directly. The operation of the shutdown feedpumps actually has a small effect on the steam generator inventory depletion time, but more importantly its operation, along with that of the auxiliary boiler, is necessary for extended main loop decay heat removal operation.

Figure 3.2 describes the shutdown cooling operations of one main loop only. The GCFR, however, has three main loops in its main cooling system, and there is a very important dependence between the main loops with regard to the overall core cooling capability of the system. These capabilities were described in Chapter 2 for the various main loop cooling system operating states.

3.2-2 Event Sequence Diagram

In order to describe explicitly the main loop cooling system operating states, the simple event tree of Figure 3.2 was expanded considerably. This expanded event tree is called an event sequence diagram (ESD). It describes the same events contained in the event tree but in much finer detail. Also, it conserves as much as possible of the correct sequential occurrence of these events.

There are some very specific reasons why the ESD was

developed. The GCFR consists of identical and basically independent main loops. However, as discussed, there is a very strong dependence between the main loop operating states and the overall core heat removal. This dependence is reflected in both the ability to cool the core, and in the duration for which the main loops provide heat removal capability during the shutdown heat removal phase.

The event tree describes the overall system success or failure, but does not detail the different degrees of success or failure which exist in the GCFR. The reason for this is basically that the event tree methodology, as developed in the reactor safety study (RSS), was aimed at describing system availabilities toward the goal of determining accident sequence probabilities to be used in an overall risk evaluation. In describing a particular system, a decision as to what to call available and what to call unavailable had to be made. This approach in some systems ignored partial success modes, but the impact on the analysis was not thought to be critical for the types of systems being analyzed. Also, it was always in a conservative direction.

However, in the GCFR, these various success modes are quite important and need to be included. Also, the goal of this research project is not to do a risk evaluation, but to do a detailed analysis of the accident sequences in order to provide insights into the design and to determine the sensitivity toward the plant safety of the reliability values of the

various system and components in the design. Thus, detailed modelling of these systems and components is necessary.

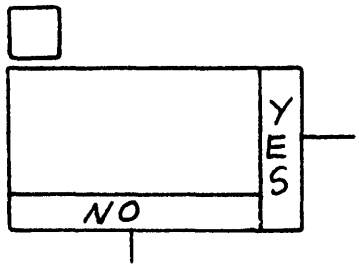
In this regard, some advantages of the ESD are:

1) it allows the detailed modelling of the independent items of all three of the main cooling loops;
2) it allows for the correct combination of those items which affect the main loop availability, and thus determine the number of main loops operable, and also what length of time they remain operable;
3) it provides a detailed description of the actual accident sequences; and
4) the information from the accident sequences will provide detailed input for the calculation of the possible accident sequence consequences.

3.2-3 ESD Symbology

The symbols which are used to construct the event sequence diagram are described below.

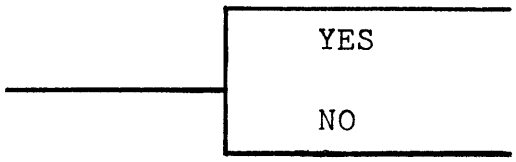
System Action Block



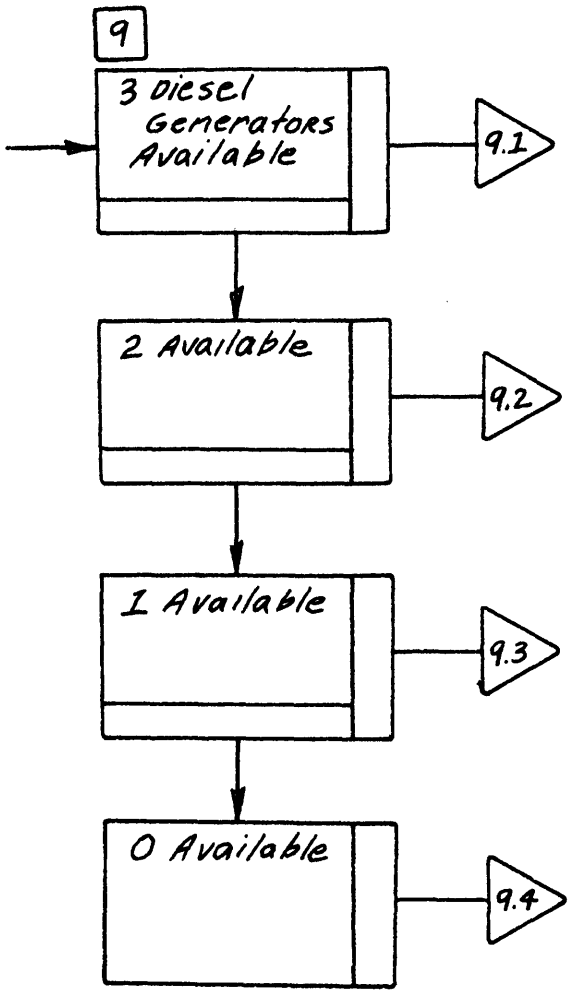
This rectangular symbol, called, a system action block,

represents the functioning of a specific system. The correct functioning of the system (as stated in the block) is always represented by a line leaving the right side of the block (marked YES), and the failure of the system to perform this function is always represented by a line leaving the bottom of the block (marked NO). While the block shown here is marked "YES" and "NO", those in the actual diagram are not.

The system action block is simply a decision point and it is depicted on an event tree as such.



Each sub-system or component function described by a system action block is coded with an index number which appears in a small square above the left hand corner of the block. Whenever one of the subsystems which consists of three identical, redundant components is modelled, its operation is described as is shown below for the operation of the emergency diesel generations.

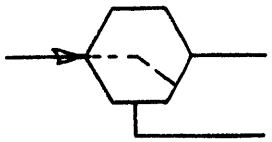


The subsystem index number is "9", and the triangles represent transfer symbols to direct the flow of the event sequences. The number inside the triangle represents the index name for a specific operating state of the system being described. 9.1 represents the operating state of the system with all three diesel generations available. 9.2 may occur if 9.1 does not, and it represents only two of the diesel generators being available. Similarly, 9.3 is only one diesel

generator available, and 9.4 is none available.

In some instances in the ESD modelling, it was necessary to know the specific main loop (or loops) to which the operating equipment corresponded. In these cases, the various combinations of operating equipment were given specific index names. See the shutdown feedwater system (subsystem 6) on Figure 3.3 for an example. The various combinations of available equipment on the main loops are assumed to occur randomly. Thus each combination is as equally likely to occur as the next.

Hexagon



The hexagonal symbols represent branching points in the flow of the event sequences. This symbol is also similar to a decision point on an event tree, however, there may be as many as four or five paths leaving a single branch point. Also, whereas the system action blocks describe the availability of specific subsystems, the branch points create alternate event paths as determined by the different availability states of the subsystem being considered. Usually, the availability of the particular subsystem will have been described elsewhere by system action blocks. The branching ratio is decided by the index numbers which are located within the different portions of the hexagon.

Each event sequence at the end of the diagram is given an index name in a special triangular symbol drawn below:

A summary of these symbols is given in Table 3-I.

3.3 EDS Description - Pressurized Reactor Shutdowns

The ESD is actually a detailed extension of the event tree, and there are specific parallels between the two types of diagrams. In describing the ESD, specific mention will be made of the event tree in Figure 3.2 in order to point out these parallels and to aid in the understanding of the ESD.

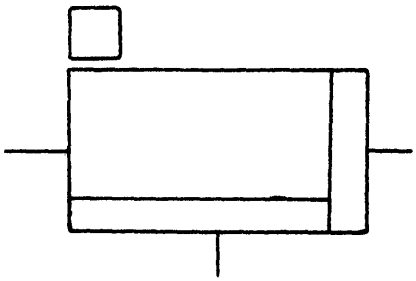
3.3-2 ESD Structure

The ESD models the reactor shutdown cooling operations in two segments. The first segment includes those plant operations which are initiated simultaneously with the reactor shutdown initiation signal and essentially occur within the first two minutes following the shutdown. This segment is called Phase One of the ESD and is included completely on Figure 3.3 At the end of Phase One, the event sequences modelled there correspond to the various operating states in which the main loop cooling system may begin shutdown heat removal.

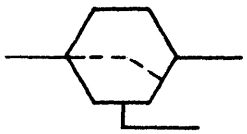
In Phase Two of the ESD, the shutdown heat removal process is modelled for each of these operating states. The

Table 3-I

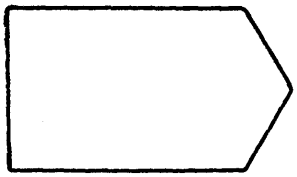
A DESCRIPTION OF SYMBOLS USED IN THE EVENT SEQUENCE DIAGRAM



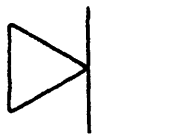
SYSTEM ACTION BLOCK represents system and component actions. The output from a block is always YES to the right, and NO to the bottom. Each system is coded with a number which appears in a small square above the block in the diagram.



The HEXAGON is a branching point in the operation sequence. The branching is directed by the numbers inside the hexagon.



HOUSES (large and small) are used to provide descriptive information concerning the operating condition of a system, or a particular shutdown path.



TRIANGLES are used as transfer signals. The numbers inside the triangle serve to direct both the coordination of output and input triangles, and the branching of the operation sequences through the hexagons. The output from the system action blocks is numbered according to the system number. The output from branching points (hexagons) is coded with a letter to correspond to different reactor shutdown operation conditions.

SPECIFIC EVENT SEQUENCE PATH INDICATORS

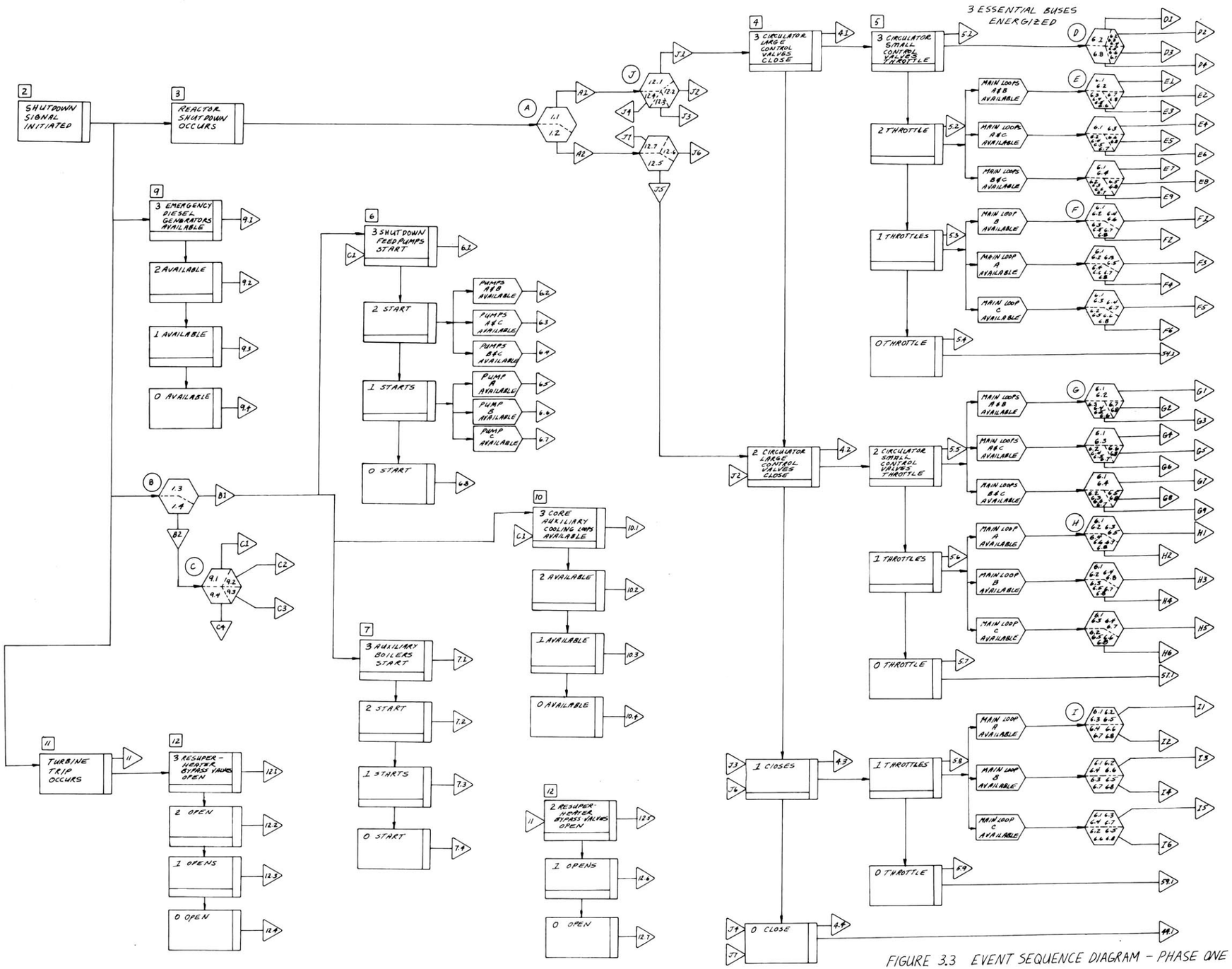


FIGURE 3.3 EVENT SEQUENCE DIAGRAM - PHASE ONE

Table 3-II

A List of ESD Subsystem Indexes

Item 1	The Initiating Event
Item 2	The Reactor Shutdown Initiation Signal
Subsystem 3	The Reactor Shutdown Systems
Subsystem 4	The Circulator-Turbine Large Control Valves
Subsystem 5	The Circulator-Turbine Small Control Valves
Subsystem 6	The Shutdown Feedwater System
Subsystem 7	The Auxiliary Steam Supply
Subsystem 8	Main Loop Transfer to Decay Heat Removal Operation
Subsystem 9	The Emergency Electrical Supply
Subsystem 10	The Core Auxiliary Cooling System
Item 11	Turbine Trip
Subsystem 12	The Resuperheater Bypass Control Valves
ITEM NUMBERS 13 and 14 WERE NOT USED	
Item 15	The Combination of Available Auxiliary Boilers and Available Main Loops
Item 16	The Probability of Restarting Initially Failed Shutdown Feedpumps or Diesel Generators During the Shutdown Cooling Process
Item 17	Main Loop Isolation Valve Operation: Closed to Open, and Main Circulator Availability After Imbalance Conditions

Table 3-II
(continued)

Item 18	Main Loop Isolation Valve Operation and Open to Closed During an Imbalance Condition
Item 19	Main Loop Support Systems
Item A	The Number of Main Loops Initially Available
Item B	The Availability of Offsite Power
Item 20	The Restoration of Offsite Power
Item 21	The Containment Equalization Pressure Range following a PCRV Depressurization Accident
Item 22	CACS operating states following a PCRV Depressurization Accident

main loop cooling system availability is described in detail along with the processes leading to eventual decay heat removal with either the main cooling loop system or the CACS.

To aid in the understanding of the ESD, a list of the subsystem and other indexes is provided in Table 3-II.

3.3-3 ESD - Phase One

Phase One of the ESD is included as Figure 3.3. The modelling begins with the initiation of a reactor shutdown signal and next considers whether or not the reactor scram actually occurs. The shutdown initiation signal also initiates a number of other system operations which are described explicitly in the ESD. These operations occur simultaneously with the shutdown of the nuclear reaction. They are:

1) Main turbine generator throttle trip, and the subsequent initiation of the resuperheater by-pass system;
2) The start-up of the emergency diesel generators;
3) The start-up of the shutdown feedwater pumps;
4) The start-up of the auxiliary boilers; and
5) The initiation of the CACS into its stand-by mode of operation.

Notice that the path leading to the latter three systems contains a branch point. The operation of these subsystems requires the availability of AC electrical power. With off-site power available (output B1 of the branch point) all of

the components of each subsystem are capable of functioning. Off-site power is necessary because the reactor shutdown signal also initiates a turbine-trip. If off-site power is not available, (output G2 of the branch point) then only those subsystems powered from the essential buses will be available. Furthermore, because each of the essential buses is supplied by one of the emergency diesel generators, only those buses on which the diesel has started will be energized. Thus the number of shutdown feedpumps and CACS loops capable of functioning is limited by the number of diesel generators starting. This is modelled on the ESD with branch point C, and the additional output operating states for subsystems 6 (the shutdown feedpumps) and 10 (the CACS) are shown in Figure 3.4b. Note that subsystem 7 (the auxiliary boilers) is not supplied from the essential buses. Also, the operation of the resuperheater by-bass system (subsystem 12) is modelled following the main turbine-trip becaue the initiation signal for this subsystem results from the turbine throttle closure and not the reactor shutdown initiation. Note that in the event tree of Figure 3.2, the operation of these subsystems is not described explicitly. Instead it is included implicitly in the diagram when the availability of these subsystems is considered.

Following the occurrence of a reactor shutdown, the event sequence path leads to branch point A. The purpose of this branch point is to include on the same diagram the modelling of those reactor shutdowns which begin with the main

loop cooling system either fully available, or with only two of the three main loops available. Therefore, the analysis of those initiating events which eliminate one main cooling loop (see Chapter 4 for a discussion of initiating events) can also be performed with this diagram.

Following branch point A are branch points J. These determine the number of main loops which are operable depending upon the availability of the resuperheater by-pass system for each loop. The operation of the CT large CV is next considered on the event sequence paths, and here one can see the parallels of the ESD to the event tree of Figure 3.2. The failure of the resuperheater by-pass system for one loop eliminates that loop leaving only two main loops available. Thus the CT large CV operation is considered for only those two available main loops. Branch point J1 leads to the system action block (3 CT large CVs close) while J2 leads to the block (2 CT large CVs close). In a similar fashion, the failure of a CT large CV to close for a specific main loop causes the steam generator inventory for that loop to be quickly depleted. This makes the correct functioning of the CT small CV for that loop unimportant, and it is not included in the modelling.

The next items considered in the ESD are the availability states of the essential electrical supply and the shutdown feedpumps. For those main loops in which a previous loop failure has occurred (either resuperheater by-pass sytem, CT large CV, or CT small CV), the operation of

the shutdown feedpump is not considered. Particular care was taken to correctly couple the available shutdown feedpumps to the available main loops. Yet, before the shutdown feedpump availability states can be combined with the available main loops, the availability of the electrical supply must be determined. The operation of subsystem 3, 12, 4 and 5 does not depend on the availability of electric power, and the main loop availability states up to the consideration of the CT small CVs may occur for any availability state of the electrical supply.

Phase one of the ESD ends by describing the specific shutdown heat removal operating states of the main loop cooling system. These are determined by the combinations of the available main loops and the available shutdown feedpumps for each availability state of the essential electrical supply. Figure 3.3 describes the main loop shutdown heat removal operating states with all three of the essential buses energized, and the operating states corresponding to the other availability states of the essential buses are described in Figure 3.4c.

Main loop operating states D1 through D4 correspond to the four operating states of the three shutdown feedpumps combined with three fully available main loops (output state 5.1) when all three essential buses are energized. Operating states D5 through D7 result whenever all three main loops are available but only two of the essential buses are energized.

The main loop operating states resulting from the combination of output state 5.2 (two main loops available, one main loop with a failed CT small CV) and the shutdown feedpump operating states are labeled E; those from output state 5.3 (one main loop available, two main loops with failed CT small CVs) one labeled F; those from output states 5.5, 5.6 and 5.8 are labeled G, H, and I respectively. Table 3-III lists the various main loop operating states and describes them briefly. The output states 5.4, 5.7, 5.9 and 4.4 are not combined with the shutdown feedpump operating states because these correspond to different failed states of all three main loops. However, there are four separate main loop operating states for each of these outputs which correspond to the different availability states of the essential electrical buses. These main loop operating states are labeled 54, 57, 59 and 44 respectively.

3.3-4 ESD - Phase Two

The shutdown heat removal operating states of the main loop cooling system, which are the output states from phase one of the ESD, constitute the input states for phase two of the ESD. In phase two, the shutdown heat removal operation for each main loop operating states is described. The diagram of the shutdown event sequences for phase two is shown in Figures 3.4 a,b,c,d,e and f.

The detailed information concerning the main loop cooling

Table 3-III

ESD - Phase One Output States

Main Loop Operating States Index and Description	Number of Main Loops With Essential AC Power	Number of Main Loops With Shutdown Feedwater Available	Final Event Sequence Index
D: 3 Main loops available. Output state 5.1			
D1	3	3	K
D2	3	2	L
D3	3	1	M
D4	3	0	N
D5	2	2	L
D6	2	1	M
D7	2	0	N
D8	1	1	M
D9	1	0	N
D10	0	0	N
E: 2 Main loops available; 1 main loop failed CT small CV. Output state 5.2			
E1, E4, E7	3	2	O
E3, E6, E9	3	1	P
E2, E5, E8	3	0	Q
E10, E19, E27	2	2	O
E11, E20, E28 E12, E21, E29	2	1	P
E13, E22, E30 E14, E23, E31	1	0	Q
E15, E24, E32	1	1	P
E16, E25, E33 E17, E26, E34	1	0	Q
E18	0	0	Q

Table 3-III continued

Main Loop Operating States Index and Description	Number of Main Loops With Essential AC Power	Number of Main Loops With Shutdown Feedwater Available	Final Event Sequence Index
F: 1 Main loop available. 2 Main loops failed CT small CVs. Output state 5.3			
F1, F3, F5	3	1	R
F2, F4, F6	3	0	S
F7, F15, F22	2	1	R
F8, F16, F23 F9, F17, F24 F10, F18, F25	2	0	S
F11, F19, F26	1	1	R
F12, F20, F27 F13, F21, F28	1	0	S
F14	0	0	S
G: 2 Main loops available. 1 Main loop failed CT large CV, or shutdown. Output state 5.5			
G1, G4, G7	3	2	W
G3, G6, G9	3	1	X
G2, G5, G8	3	0	Y
G10, G19, G27	2	2	W
G11, G20, G28 G12, G21, G29	2	1	X
G13, G22, G30 G14, G23, G31	2	0	Y
G15, G24, G32	1	1	X
G16, G25, G33 G17, G26, G34	1	0	Y
G18	0	0	Y

Table 3-III continued

Main Loop Operating States Index and Description	Number of Main Loops With Essential AC Power	Number of Main Loops With Shutdown Feedwater Available	Final Event Sequence Index
H: 1 Main loop available; 1 main loop failed CT small CV; 1 main loop failed CT large CV, or shutdown. Output state 5.6			
H1, H3, H5	3	1	Z
H2, H4, H6	3	0	AA
H7, H15, H22	2	1	Z
H8, H16, H23 H9, H17, H24 H10, H18, H25	2	0	AA
H11, H19, H26	1	1	Z
H12, H20, H27 H13, H21, H28	1	0	AA
H14	0	0	AA
I: 1 Main loop available; 1 main loop failed CT large CV; 1 main loop failed CT large CV, or shutdown. Output state 5.8			
I1, I3, I5	3	1	CC
I2, I4, I6	3	0	DD
I7, I15, I22	2	1	CC
I8, I16, I23 I9, I17, I24 I10, I18, I25	2	0	DD
I11, I19, I26	1	1	CC
I12, I20, I27 I13, I21, I28	1	0	DD
I14	0	0	CC

Table 3-III continued

Main Loop Operating States Index and Description	Number of Main Loops With Essential AC Power; Shutdown Feedwater Not Considered	Final Event Sequence Index
44: All 3 CT large CVs failed to close. Output state 4.4		
44.1	3	
44.2	2	
44.3	1	V
44.4	0	
54: All 3 CT small CVs failed to throttle. Output state 5.4		
54.1	3	
54.2	2	
54.3	1	T
54.4	0	
57: 2 Main loops failed CT small CVs; 1 main loop failed CT large CV, or shutdown. Output state 5.7		
57.1	3	
57.2	2	
57.3	1	BB
57.4	0	
59: 1 Main loop failed CT large CV; 1 main loop failed CT small CV; 1 main loop failed CT large CV, or shutdown. Output state 5.9		
59.1	3	
59.2	2	
59.3	1	U
59.4	0	

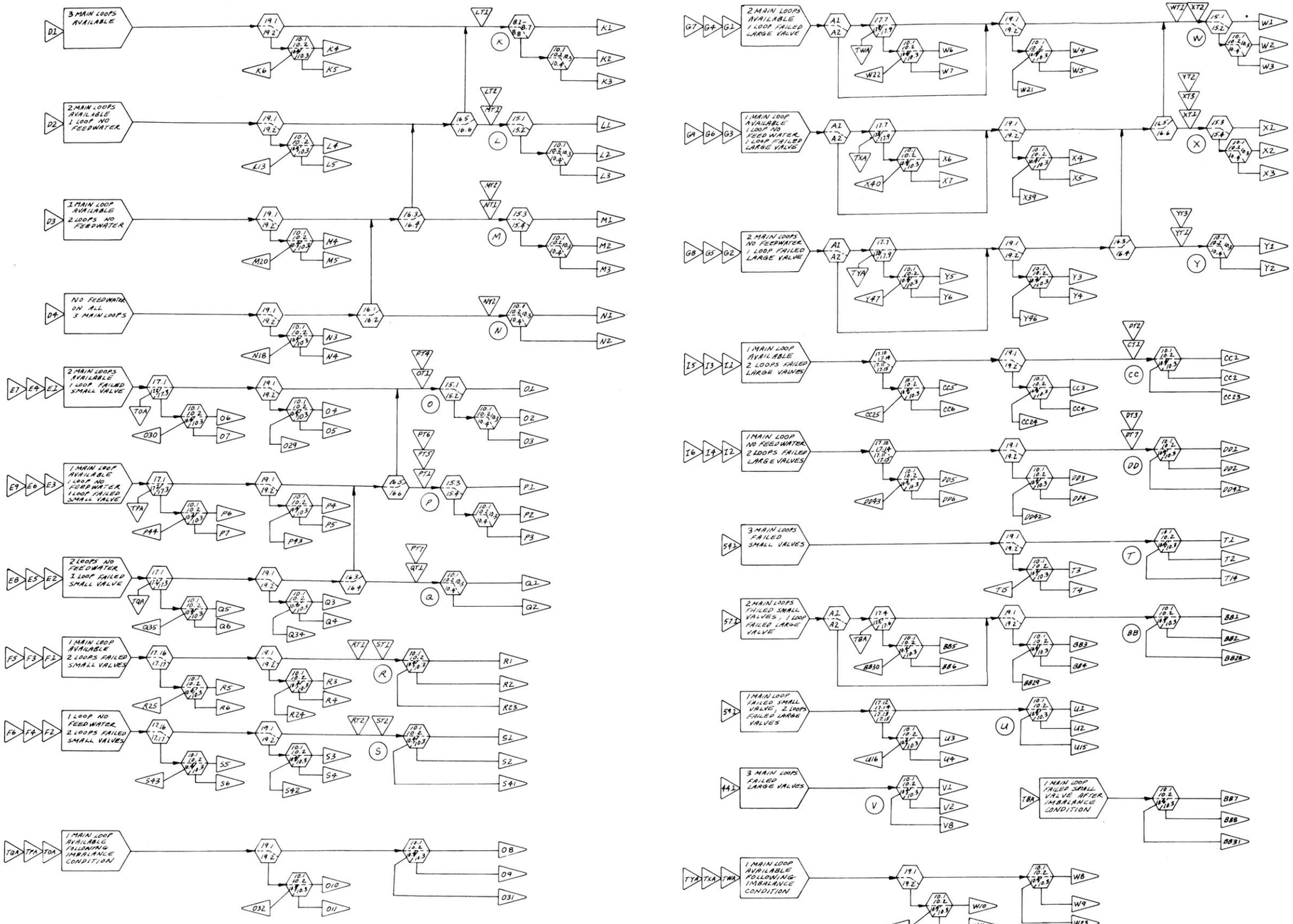


FIGURE 3.4a EVENT SEQUENCE DIAGRAM - PHASE TWO ; PRESSURIZED REACTOR SHUTDOWNS

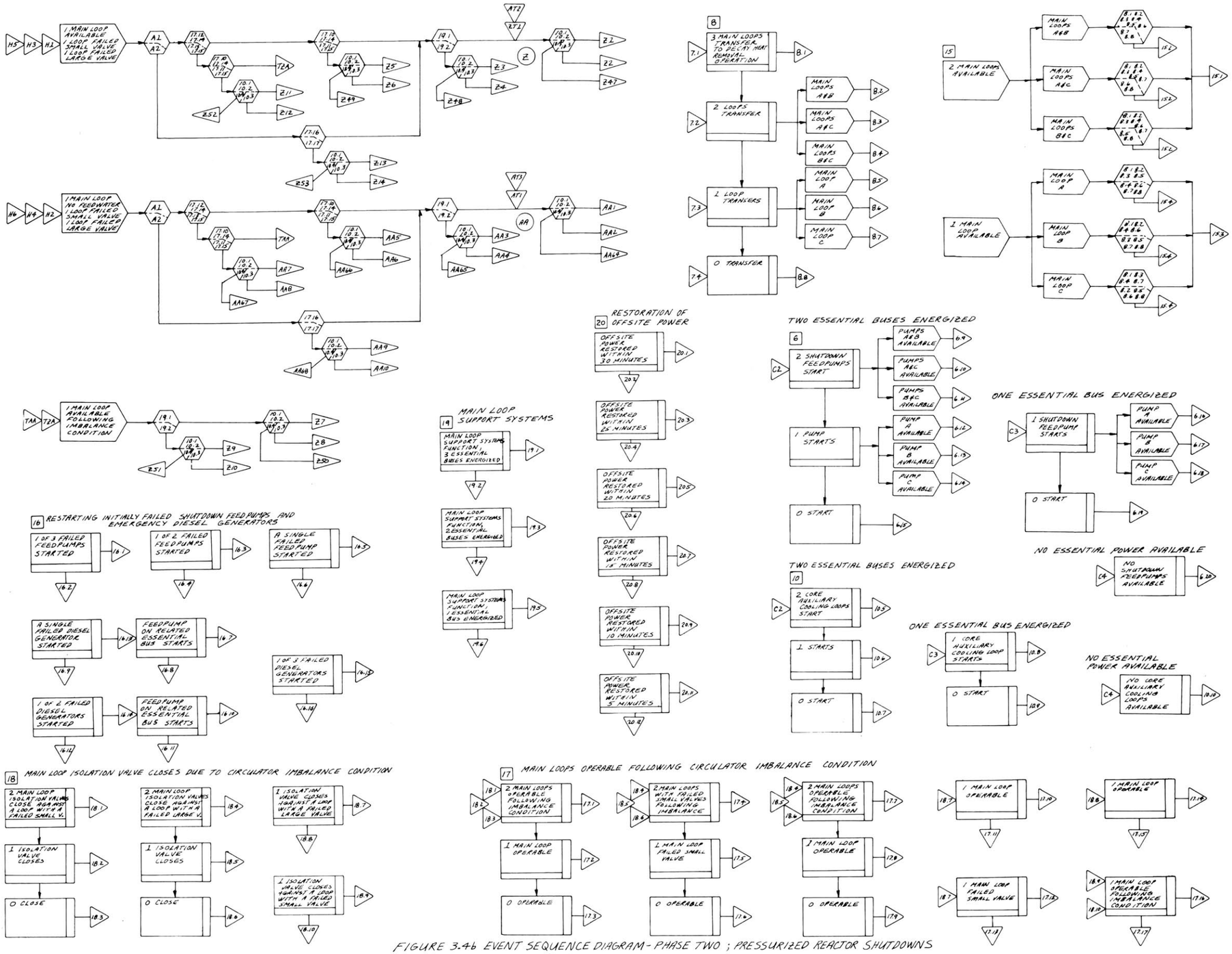


FIGURE 3.4b EVENT SEQUENCE DIAGRAM - PHASE TWO ; PRESSURIZED REACTOR SHUTDOWNS

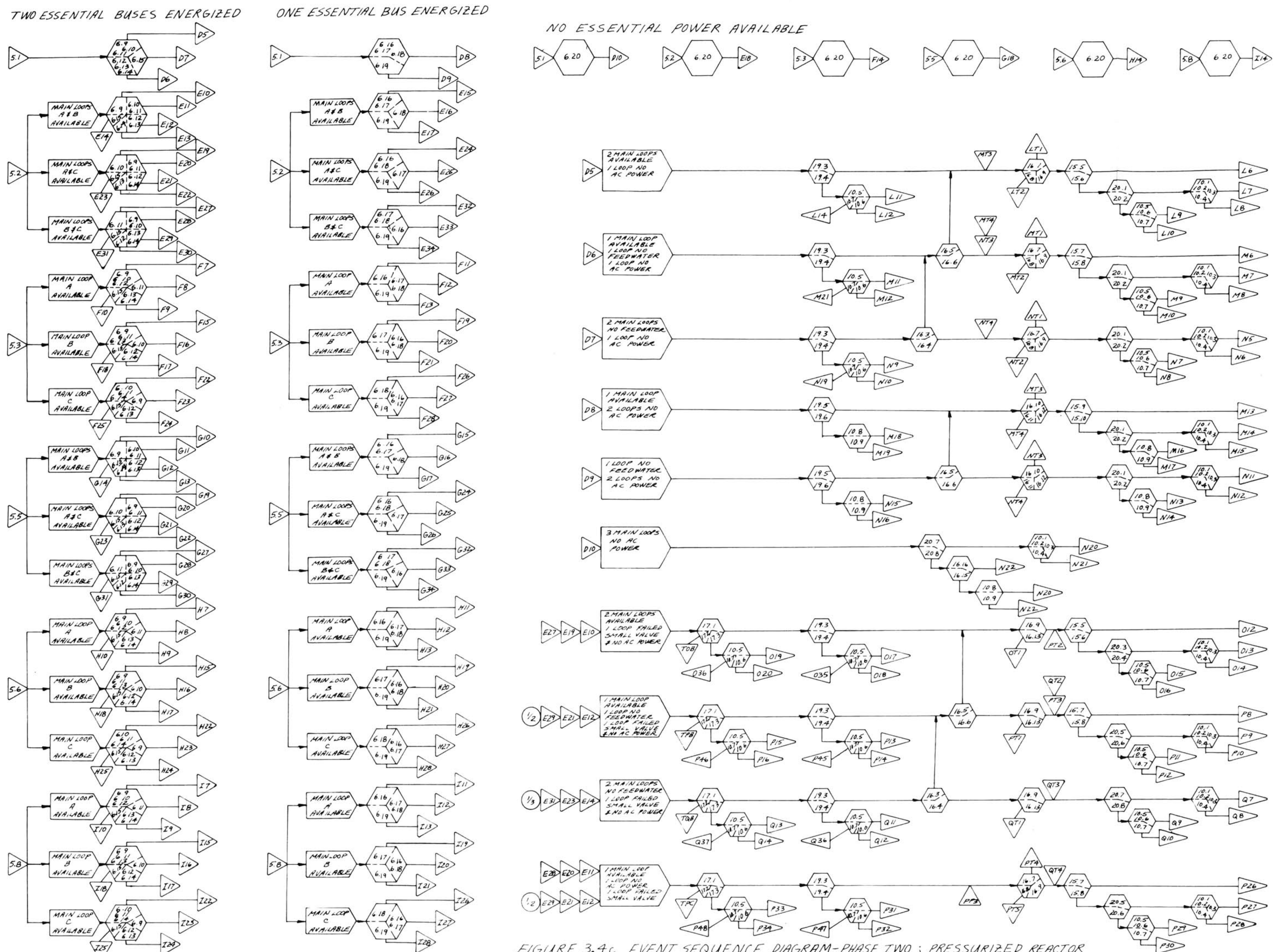


FIGURE 3.4c EVENT SEQUENCE DIAGRAM-PHASE TWO ; PRESSURIZED REACTOR SHUTDOWNS, OFFSITE POWER INITIALLY UNAVAILABLE

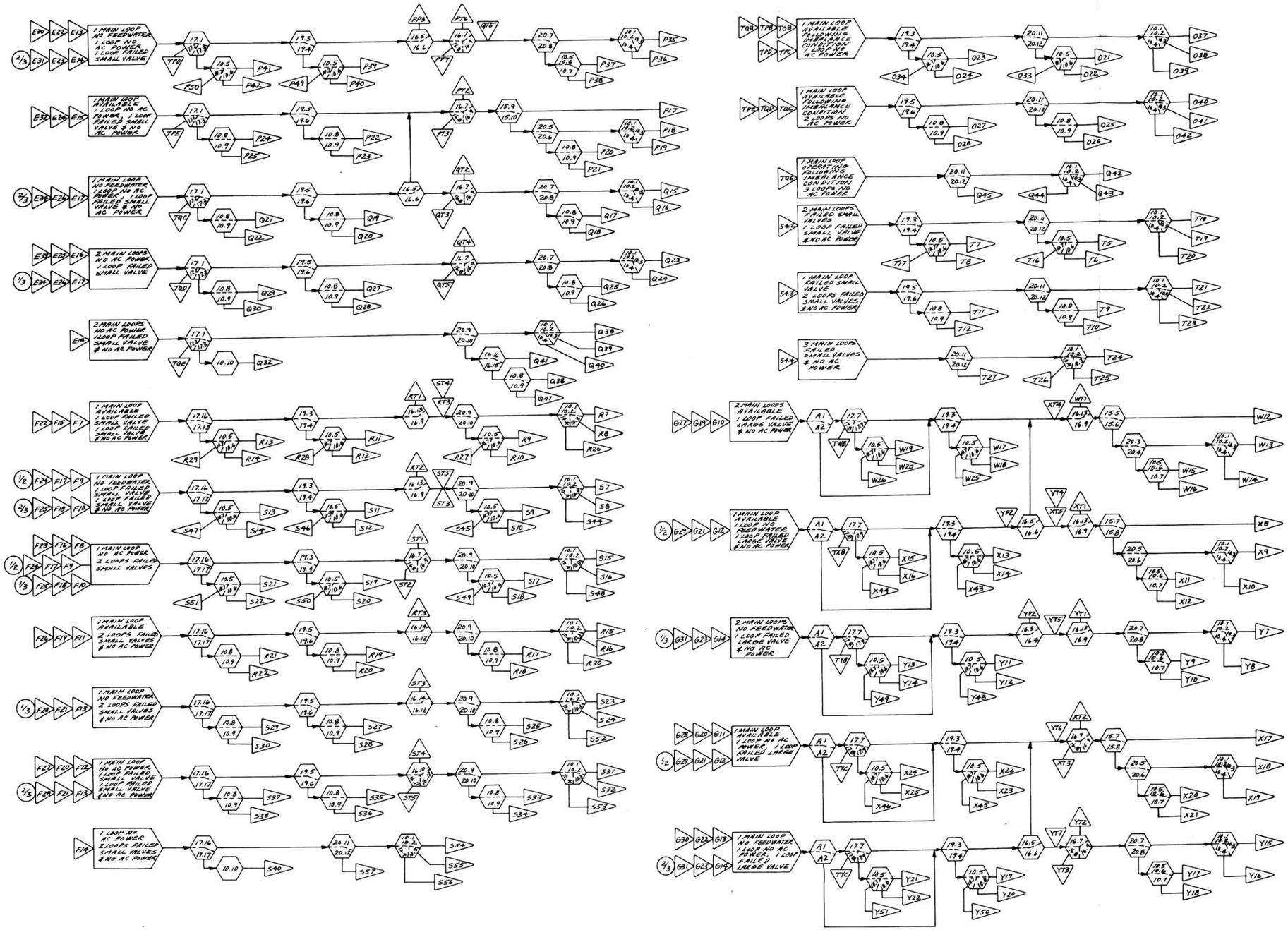


FIGURE 3.4d EVENT SEQUENCE DIAGRAM—PHASE TWO ; PRESSURIZED REACTOR SHUTDOWNS, OFFSITE POWER INITIALLY UNAVAILABLE

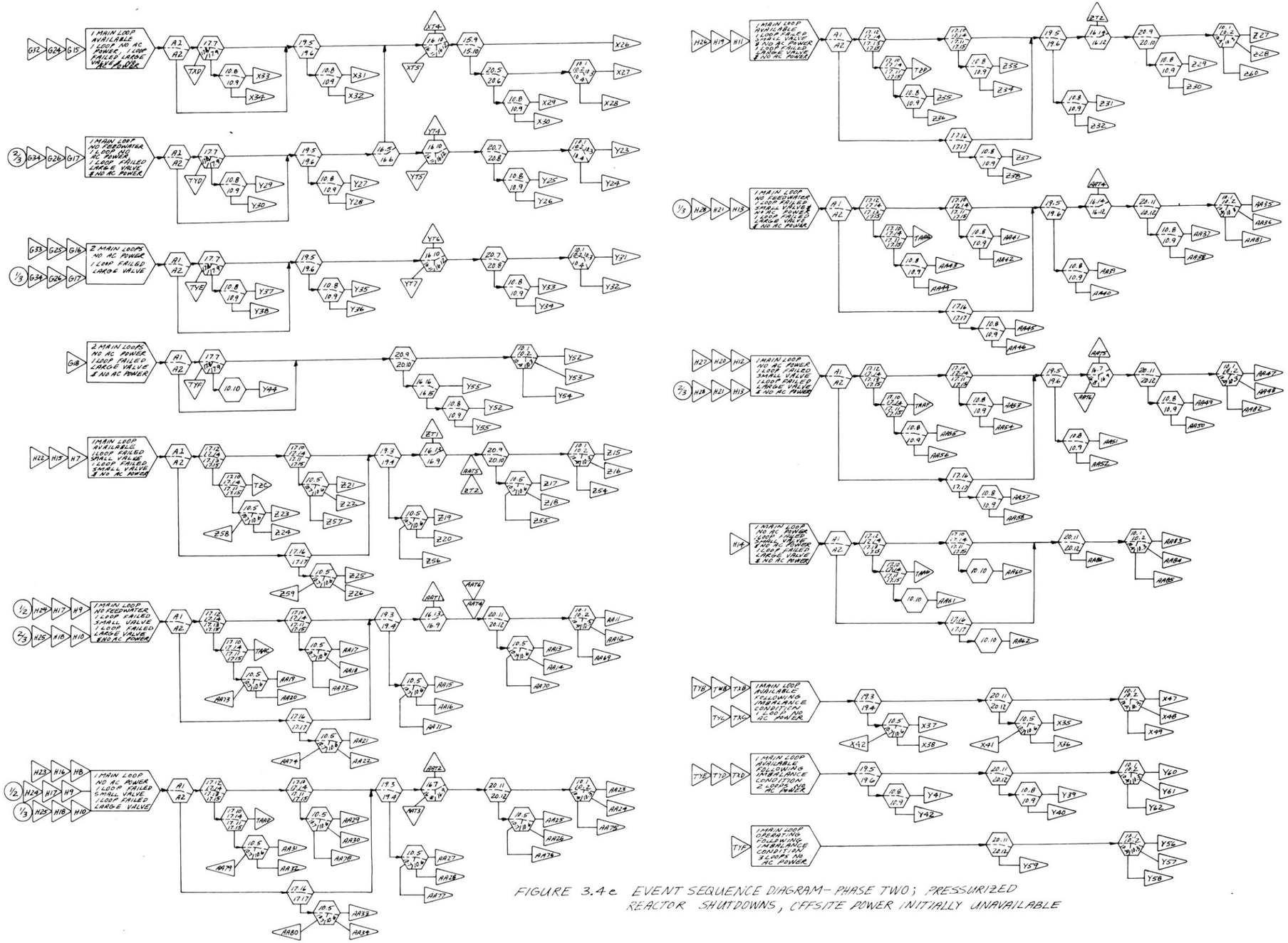


FIGURE 3.4c EVENT SEQUENCE DIAGRAM- PHASE TWO; PRESSURIZED REACTOR SHUTDOWNS, OFFSITE POWER INITIALLY UNAVAILABLE

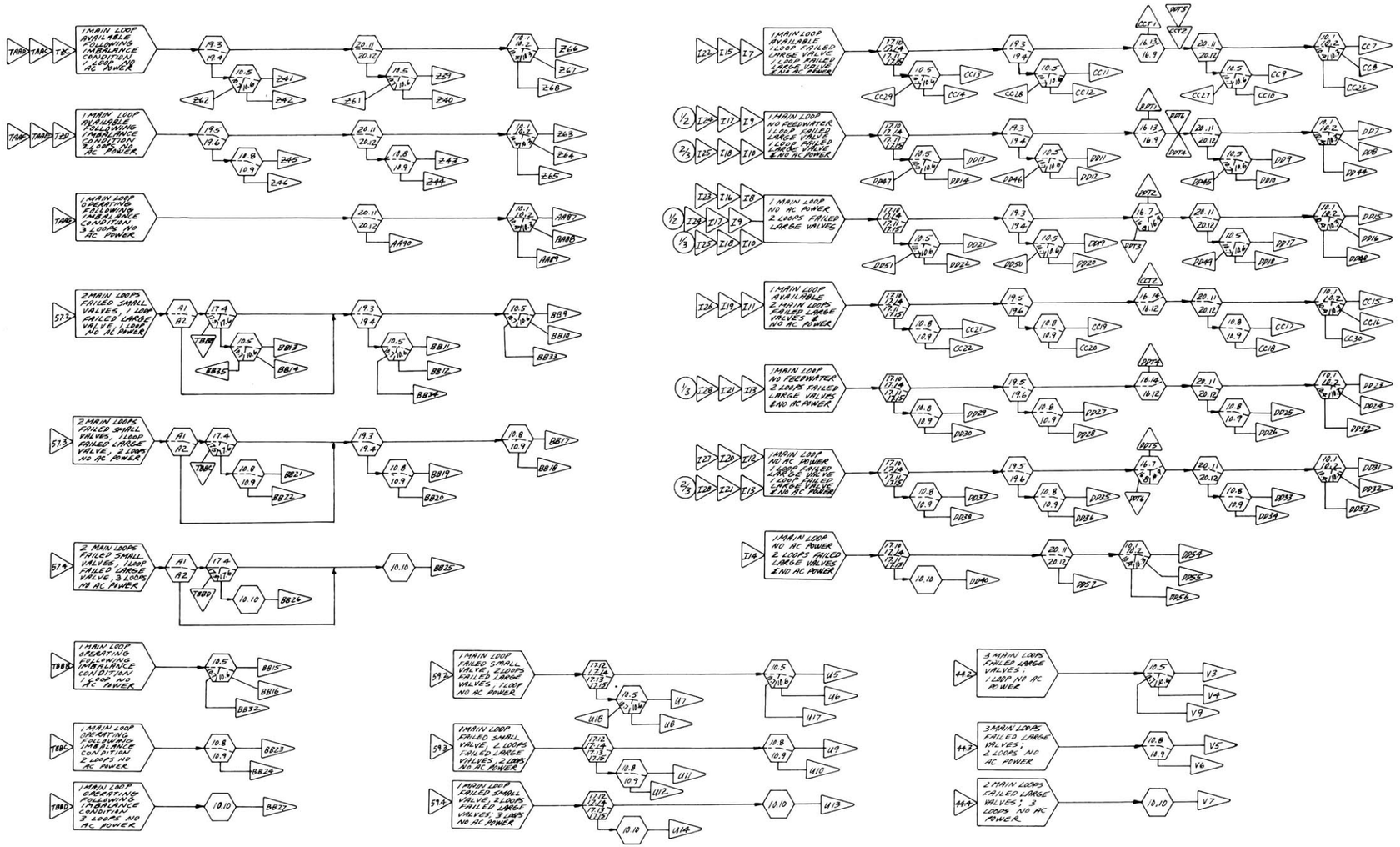


FIGURE 3.4f EVENT SEQUENCE DIAGRAM - PHASE TWO ; PRESSURIZED REACTOR SHUTDOWNS , OFFSITE POWER INITIALLY UNAVAILABLE

system capabilities, discussed in section 2.4, was utilized to model the shutdown event sequences. For each main loop operating state it was determined whether the main loops would be available for a sufficient time to allow the auxiliary boilers to reach their rated operating conditions. The available main loops were then correctly combined with the available auxiliary boilers. Also, it was determined when main loop failure actually would occur so that the number of CACS loops required for adequate core cooling was known. The actual main loop operating times utilized in the ESD modelling are listed in Table 3-IV. These times based on this author's best evaluation of the main loop cooling system operation, and they correspond to the worst condition of main loop isolation valve by-pass. The operation of the CACS was assumed to occur (if required) at the times listed, and if CACS failure occurred, core meltdown was assumed to occur immediately.

Subsystem 8 represents the transfer of a main cooling loop to decay heat removal operation using auxiliary boiler steam. This process requires an available auxiliary boiler and a number of valve operations. The correct combinations of available auxiliary boilers and available main loops is accomplished by item 15. The branch points containing index 15 describe event sequences ending in main loop decay heat removal operation. The CACS availability is described by branch points containing index 10. These branch points end those event sequences leading to either successful CACS operation or to core meltdown.

Table 3-IV

A List of the Main Loop Operating Times Used in the ESD for Pressurized Shutdowns

Number of Main Loops Available	Conditions of Unavailable Main Loops	Number of Available Main Loops With Feedwater	Main Loop Operating Time Used in ESD (minutes)
3		3 2 1 0	30 30 30 30
2	1 Main loop failed CT large CV, or shutdown	2 1 0	25 20 15
	1 Main loop failed CT large CV	2 1 0	27 22 17
1	2 Main loops failed CT large CVs	1 0	6 5
	1 Main loop failed CT large CV, 1 Main loop failed CT small CV	1 0	8 7
	1 Main loop available following CT imbalance condition	--	5
0	3 Main loops failed CT small CVs	--	10
	3 Main loops failed CT large CVs	--	2

All those individual event sequences resulting from a specific main loop operating state are given a similar index name. For example, event sequences K1 through K6 correspond to main loop operating state D1. Those event sequences resulting from main loop operating state D2 are labeled L. These event sequence indexes are given in Table 3-III.

3.3-5 ESD Additional Items

The auxiliary boiler availability, and the CACS availability complete the parallel of the ESD and the event tree of Figure 3.2. However, the ESD considers additional items not contained in the event tree. These are:

1) Main Loop isolation valve operations,
2) Main Loop cooling system dependence on support systems,
3) The possibility of starting initially failed shutdown feedpumps or diesel generators during the shutdown operations, and
4) The probability that off-site power is restored in those event sequence paths which begin without off-site power available.

These items are described briefly below. For a more detailed description, see Appendix A.

3.3-5-1 Main Loop Isolation Valve Operations

In the ESD modelling, main loop isolation valve operations were considered for their possible effects on the

core heat removal and on the main loop availability.

Failure to Close Resulting in Core By-Pass Flow

In the modelling of the reactor shutdown cooling operations, a main loop failure eventually causes the helium circulator of that main loop to cease functioning. If the isolation valve of this main loop fails to close, the pressure rise created by the operation of the other circulators will cause a backflow of helium through this failed main loop.

In a pressurized reactor shutdown, the amount of this by-pass flow (which is diverted from the reactor core) is not large, and it is compensated for slightly by an increase in the speed of the operable circulators due to the decreased overall helium flow resistance. In addition, the shutdown controllers on the operating loops function to maintain acceptable helium temperatures by increasing the circulator speed and thus the helium flow. These effects tend to minimize any temperature transient due to the isolation valve failure. However, the higher circulator speeds will result in shorter steam generator inventory depletion times, especially if no shutdown feedwater is provided.

The effect of main loop isolation valve failures on the main loop cooling system performance was analyzed in reference 2, and the resulting steam generator inventory depletion times are summarized in Table 2-VIII.

Instead of modelling a number of parallel event paths which were largely identical except for these main loop isola-

tion valve failures, a single path was drawn, and the steam generator inventory depletion time for the path was chosen to include those cases where main loop isolation valve failures occurred.

Main Loop Circulator Imbalance Conditions

During the shutdown cooling operations, a circulator-turbine control valve failure will cause an out-of-balance condition between the three main loop circulators. The circulator with the failed control valve will quickly be operating at a higher speed than the others because their control valves are acting to reduce their speed in accordance with the decreased heat lead following a shutdown. This may cause the loop isolation valves in the correctly functioning loops to close, or it may result in the circulators being overpowered or even reversed if their loop isolation valves fail to close.

Therefore, if the isolation valve in an operable loop closes, it must re-open after the out-of-balance condition if the loop is to remain operable. Also, the circulator and its drive turbine must not be damaged due to the period of operation behind the closed isolation valve. If the isolation valve fails to close, during the out-of-balance condition, then the circulator and drive turbine must remain operable after the condition is past.

These isolation valve operations (and the main circulator availabilities) are modelled on the appropriate event

sequence paths by the branch points containing the index 17. Both items 18 and 17 are combined to determine the number of main loops that remain operable following an out-of-balance condition.

3.3-5-2 Main Loop Support Systems

The continued operation of the main loop cooling system is dependent upon correct functioning of a number of support systems. These include the main circulator service systems, the service water system, the reactor plant cooling water system, and the instrument and service air system. Main loop cooling system failures due to support system faults are modelled in the event sequences by the branch points containing the index 19.

3.3.-5-3 The Restoration of Initially Failed Shutdown Feedpumps or Emergency Diesel Generators

In many event sequence paths, the operation of the main loop cooling system may continue for at least thirty minutes. In this interval, neither the availability of electrical power to the main loop, nor the operation of the shutdown feedpump are critical. In this time period, it was felt that the potential existed for corrective action which might start an initially failed shutdown feedpump, or where the emergency electrical supply is necessary, start

an initially failed diesel generator. The possible occurrence of this corrective action is included in those event paths where sufficient time exists (at least ten minutes) by the branch points containing index 16.

3.3-5-4 The Restoration of Off-site Power

The availability of off-site power was included in item B of the ESD. According to reference 3, there is a rather high likelihood of restoration of a lost off-site power source within the first thirty minutes of the loss. Therefore, for those accident sequences which last at least five minutes, the possibility of off-site power being restored was included.

The likelihood of off-site power being restored was estimated for six time intervals following the reactor shutdown. (In all cases where off-site power is lost, it was assumed lost concurrent with the reactor shutdown.) These are: 1) within 30 minutes, 2) within 25 minutes, 3) within 20 minutes, 4) within 15 minutes, 5) within 10 minutes, and 6) within 5 minutes.

The branch points containing index 20 allow the consideration of the restoration of off-site power. These are placed in the event paths just before main loop failure occurs. The restoration of off-site power could occur at any time during the period of main loop operation, but this was

assumed to make no difference to the main loop performance. Only the availability of the CACS was altered by the restoration of off-site power.

Because the auxiliary boilers are not powered from the essential buses, restoration of off-site power only affects the main loop performance if it occurs shortly after the reactor shutdown. It was assumed that twenty minutes of main loop operation following the restoration of off-site power was required to allow the boilers to reach their rated conditions. These possible event sequences were not modelled explicitly on the ESD, but they were considered in the final analysis. The manner in which they were included is discussed in Chapter 5. Powering the auxiliary boilers from the essential buses is a potential design option which was investigated. Therefore, for those accident sequences following the loss of off-site power, the auxiliary boilers were modelled so that they could be treated as being powered from either the non-essential bus or from the essential buses, and many of these event sequence paths contain branch points with the index 15.

3.3-6 ESD Outcome Categories - Pressurized Shutdowns

Each event sequence path ends with an index name for that path, and those event sequences which lead to similar outcomes are grouped into specific categories. These outcome categories describe the operating state of the shutdown cooling systems for decay heat removal operation. Specifically, for the pressurized reactor shutdowns, there are nine different outcome categories. Table 3-V summarizes these outcome categories.

Table 3-V

ESD Outcome Categories for the Pressurized Reactor Case

System Success

Category 1. Adequate decay heat removal is provided indefinitely by the main loop cooling system.

Category 2. Adequate decay heat removal is provided indefinitely by the CACS at 15 minutes or more after the shutdown.

Category 3. Adequate decay heat removal is provided indefinitely by the CACS starting in the interval between 2 and 15 minutes after shutdown.

System Failure

Category 4. Forced circulation provided by only one CACS loop in the interval between 2 and 15 minutes after the shutdown.

Category 5. Loss of adequate decay heat removal in the interval between 20 and 30 minutes after the shutdown,

Category 6. Loss of adequate decay heat removal in the interval between 15 and 20 minutes after the shutdown,

Category 7. Loss of adequate decay heat removal in the interval between 10 and 15 minutes after the shutdown,

Category 8. Loss of adequate decay heat removal in the interval between 5 and 10 minutes after the shutdown, and

Category 9. Loss of adequate decay heat removal within 5 minutes after the shutdown.

Three of the categories combine those event sequences which result in the successful decay heat removal operation of one of the shutdown cooling systems. Decay heat removal can be provided by either the main loop cooling system, two CACS loops before 15 minutes following the shutdown, or only one CACS loop after this time.

If only one CACS loop is available prior to 15 minutes following the shutdown, a core meltdown was assumed to occur. Present analyses by GA indicate that adequate helium circulation can be provided by a single auxiliary circulator, but the heat removal capability of one auxiliary heat exchanger is not sufficient to prevent core meltdown. All the event sequences leading to this outcome were combined into a single category.

Those event sequences leading to a complete loss of decay heat removal were grouped into categories depending upon the time interval in which cooling system failure was assumed to occur. These are mostly five minute intervals for the pressurized shutdowns.

A complete listing of the event sequences which comprise each outcome category is provided in Table 3-VI. It should be noted, that while outcome category 9 consists of core-melt accident sequences which occur within five minutes of the shutdown, no core meltdowns occur before two minutes. This can be seen from Table 3-IV. None of the failures modelled in the ESD eliminate the main loop cooling system in less than two minutes.

Table 3-VI

A List of the Categorization of the Individual

Event Sequences for Pressurzied Shutdowns

Category 1. Adequate decay heat removal is provided indefinitely by the main loop cooling system.

K1
L1, L6
M1, M6, M13
O1, O12
P1, P8, P17, P26
W1, W12
X1, X8, X17, X26

Category 2. Adequate decay heat removal is provided indefinitely by the CACS at 15 minutes or more after the shutdown.

K2
L2, L7, L9
M2, M7, M9, M14, M16
N1, N5, N7, N11, N13, N20
O2, O13, O15
P2, P9, P11, P18, P20, P27, P29, P35, P37
Q1, Q7, Q9, Q15, Q17, Q23, Q25, Q38
W2, W13, W15
X2, X9, X11, X18, X20, X27, X29
Y1, Y7, Y9, Y15, Y17, Y23, Y25, Y31, Y33

Category 3. Adequate decay heat removal is provided indefinitely by the CACS starting in the interval between 2 and 15 minutes after shutdown.

K4
L4, L11
M4, M11
N3, N9
O4, O6, O8, O10, O17, O19, O21, O23, O37, O40
P4, P6, P13, P15, P31, P33, P39, P41
Q3, Q5, Q11, Q13, Q42
R1, R3, R5, R7, R9, R11, R13, R15
S1, S3, S5, S7, S9, S11, S13, S15, S17, S19, S21, S23, S31, S54

Table 3-VI cont.

T1, T3, T5, T7, T18, T21, T24
U1, U3, U5, U7
V1, V3
W4, W6, W8, W10, W17, W19
X4, X6, X13, X15, X22, X24, X35, X37, X47
Y3, Y5, Y11, Y13, Y19, Y21, Y52, Y56, Y60
Z1, Z3, Z5, Z7, Z9, Z11, Z13, Z15, Z17, Z19, Z21, Z23, Z25, Z27, Z39, Z41, Z63, Z66
AA1, AA3, AA5, AA7, AA9, AA11, AA13, AA15, AA17, AA19, AA21, AA23, AA25, AA27, AA29, AA31, AA33, AA35, AA47, AA83, AA87
BB1, BB3, BB5, BB7, BB9, BB11, BB13, BB15
CC1, CC3, CC5, CC7, CC9, CC11, CC13, CC15
DD1, DD3, DD5, DD7, DD9, DD11, DD13, DD15, DD17, DD19, DD21, DD23, DD31, DD54

Category 4. Forced circulation provided by only one CACS loop in the interval between 2 and 15 minutes after shutdown.

K5
L5, L12
M5, M12, M18
N4, N10, N15
O5, O7, O9, O11, O18, O20, O22, O24, O25, O27, O38, O41
P5, P7, P14, P16, P22, P24, P32, P34, P40, P42
Q4, Q6, Q12, Q14, Q19, Q21, Q27, A29, Q43
R2, R4, R6, R8, R10 R12, R14, R16, R17, R19, R21
S2, S4, S6, S8, S10, S12, S14, S16, S18, S20, S22, S24, S25, S27, S29, S32, S33, S35, S37, S55
T2, T4, T6, T8, T9, T11, T19, T22, T25
U2, U4, U6, U8, U9, U11
V2, V4, V5
W5, W7, W9, W11, W18, W20
X5, X7, X14, X16, X23, X25, X31, X33, X36, X38, X48
Y4, Y6, Y12, Y14, Y20, Y22, Y27, Y29, Y35, Y37, Y39, Y41, Y53, Y57, Y61
Z2, Z4, Z6, Z8, Z10, Z12, Z14, Z16, Z18, Z20, Z22, Z24, Z26, Z28, Z29, Z31, Z33, Z35, Z37, Z40, Z42, Z43, Z45, Z64, Z67
AA2, AA4, AA6, AA8, AA10, AA12, AA14, AA16, AA18, AA20, AA22, AA24, AA26, AA28, AA30, AA32, AA34, AA36, AA37, AA39, AA41, AA43, AA45, AA48, AA49, AA51, AA53, AA55, AA57, AA84, AA88

Table 3-VI cont.

BB2, BB4, BB6, BB8, BB10, BB12, BB14, BB16, BB17, BB19, BB21, BB23
CC2, CC4, CC6, CC8, CC10, CC12, CC14, CC16, CC17, CC19, CC21
DD2, DD4, DD6, DD8, DD10, DD12, DD14, DD16, DD18, DD20, DD22, DD24, DD25, DD27, DD29, DD32, DD33, DD35, DD37, DD55

Category 5. Loss of adequate decay heat removal in the interval between 20 and 30 minutes after the shutdown.

K3
L3, L8, L10
M3, M8, M10, M15, M17
N2, N6, N8, N12, N14
O3, O14, O16
P3, P10, P12, P19, P21, P28, P30, P36, P38
W3, W14, W16
X3, X10, X12, X19, X21, X28, X30

Category 6. Loss of adequate decay heat removal in the interval between 15 and 20 minutes after the shutdown.

N21, N22
Q2, Q8, Q10, Q16, Q18, Q24, Q26
Y2, Y8, Y10, Y16, Y18, Y24, Y26, Y32, Y34

Category 7. Loss of adequate decay heat removal in the interval between 10 and 15 minutes after the shutdown.

Q39, Q40
R18, R23, R26, R27, R30
S26, S34, S41, S44, S45, S48, S49, S52, S53
Y54, Y55

Category 8. Loss of adequate decay heat removal in the interval between 5 and 10 minutes after the shutdown.

K6
L13, L14
M19, M20, M21
N16, N17, N18, N19
O26, O28, O29, O30, O31, O32, O33, O34, O35, O39, O42
P23, P43, P44, P45, P47, P49

Table 3-VI cont.

Q20, Q28, Q31, Q33, Q34, Q35, Q36, Q44, Q45
R20, R24, R25, R28
S28, S36, S39, S42, S43, S46, S50, S56, S57
T10, T12, T13, T14, T15, T16, T17, T20, T23, T26, T27
U10, U13, U17
W21, W23, W24, W25
X32, X39, X41, X42, X43, X45, X49
Y28, Y36, Y40, Y42, Y43, Y45, Y46, Y48, Y50, Y58, Y59, Y62
Z30, Z32, Z44, Z46, Z47, Z48, Z50, Z51, Z54, Z55, Z56, Z60, Z61, Z62, Z65, Z68
AA38, AA40, AA42, AA44, AA46, AA50, AA52, AA59, AA63, AA64, AA65, AA69, AA70, AA71, AA75, AA76, AA77, AA81, AA82, AA85, AA86, AA89, AA90
BB19, BB20, BB25, BB28, BB29, BB33, BB34
CC18, CC20, CC23, CC24, CC26, CC27, CC28, CC30
DD26, DD28, DD34, DD36, DD39, DD41, DD42, DD44, DD45 DD46, DD48, DD49, DD50, DD52, DD53, DD56, DD57

Category 9. Loss of adequate decay heat removal within 5 minutes after the shutdown.

O36
P25, P46, P48, P50
Q22, Q30, Q32, Q37
R22, R29
S30, S38, S40, S47, S51
U12, U14, U15, U16, U18
V6, V7, V8, V9
W22, W26
X34, X40, X47, X49, X51
Y38, Y40, Y47, Y49, Y51
Z34, Z36, Z38, Z49, Z52, Z53, Z57, Z58, Z59
AA54, AA56, AA58, AA60, AA61, AA62, AA66, AA67, AA68, AA72 AA73, AA74, AA78, AA79, AA80
BB22, BB24, BB26, BB26, BB30, BB31, BB32, BB35
CC22, CC25, CC29
DD30, DD38, DD40, DD43, DD47, DD51

3.4 ESD Modelling - Shutdowns Following a Depressurization Accident

3.4-1 Introduction

Failure of a PCRV penetration closure seal will result in the rapid depressurization of the reactor primary coolant. Because helium is a single phase fluid, it cannot be completely expulsed from the reactor. The high pressure helium inside the PCRV will expand into the containment volume, which contains air at atmospheric pressure, and an equilibrium pressure will be reached in the combined primary coolant and containment volumes.

The decrease in the helium density which occurs due to the depressurization has a large effect on the performance of the reactor cooling systems. A reactor shutdown is required, because the main circulators can no longer circulate a sufficiently large mass flow of helium. The main loop shutdown cooling capabilities and the CACS operating performance are both affected by the decrease in the helium density.

In order to account for the changes in the shutdown cooling system capabilities, a separate ESD was constructed which modelled the reactor shutdown cooling operations following a depressurization accident.

3.4-2 ESD - Phase One

For reactor shutdowns initiated by a PCRV depressurization accident, the initial shutdown operations, which are

modelled as Phase One of the ESD (Figure 3.3), are essentially the same as those resulting from any pressurized shutdown initiating event.

A single main cooling loop is not capable of providing adequate decay heat removal in the initial period following a depressurization accident. Thus, those operating states with only a single main loop available need not be combined with available shutdown feedpumps, and the main loop operating states F, H and I from the pressurized shutdowns do not exist. The output states with only a single main loop available (5.3, 5.6 and 5.8) each lead to only four shutdown cooling states which correspond to the number of essential buses energized. Table 3-VII describes only these three main loop operating states which differ from the pressurized shutdowns.

The depressurized accident sequences were all given index names similar to those in the pressurized shutdowns, but with a D prefix. For example, main loop operating state D1 leads to depressurized accident sequences labeled DK.

3.4-3 ESD - Phase Two

The modelling of the shutdown heat removal process in phase two of the ESD for the depressurized shutdowns follows the same logic used in the pressurized shutdowns. This modelling is shown in Figures 3.5 a,b and c. However, there are some major differences which will be described.

Table 3-VII

ESD Depressurized Phase I Output States Which Differ from the Pressurized Shutdowns

Main Loop Operating States Index and Description	Number of Main Loops With Essential AC Power; Shutdown Feedwater Not Considered	Depressurized Accident Sequence Index
53: 1 Main Loop Available; 2 Main Loops Failed CT Small CV's. From output state 5.3		
53.1	3	DR
53.2	2	
53.3	1	
53.4	0	
56: 1 Main Loop Available; 1 Main Loop Failed CT Large CV, or Shutdown. From output state 5.6		
56.1	3	DZ
56.2	2	
56.3	1	
56.4	0	
58: 1 Main Loop Available; 1 Main Loop Failed CT Large CV, or Shutdown. From output state 5.8		
58.1	3	DC
58.2	2	
58.3	1	
58.4	0	

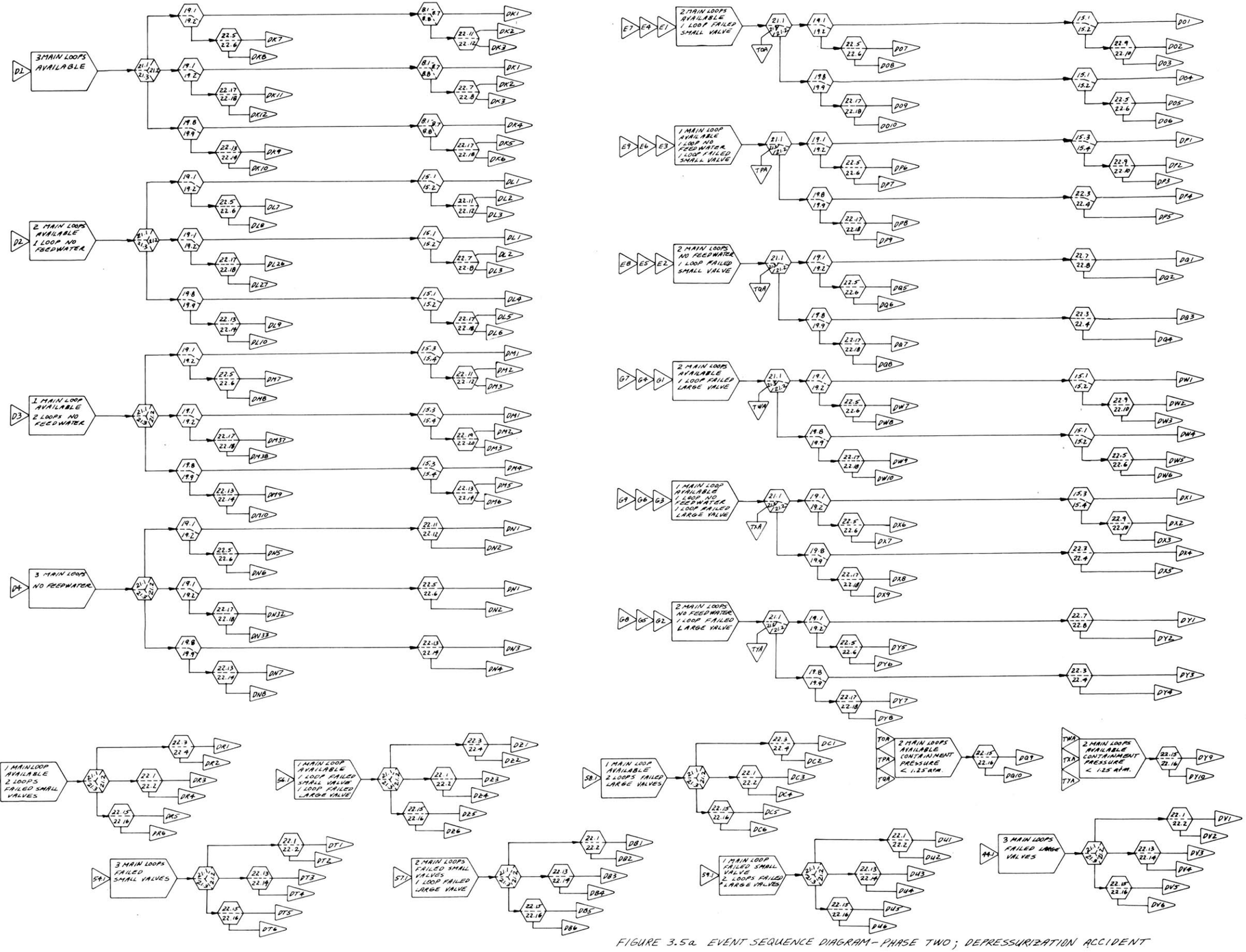


FIGURE 3.5a EVENT SEQUENCE DIAGRAM - PHASE TWO; DEPRESSURIZATION ACCIDENT

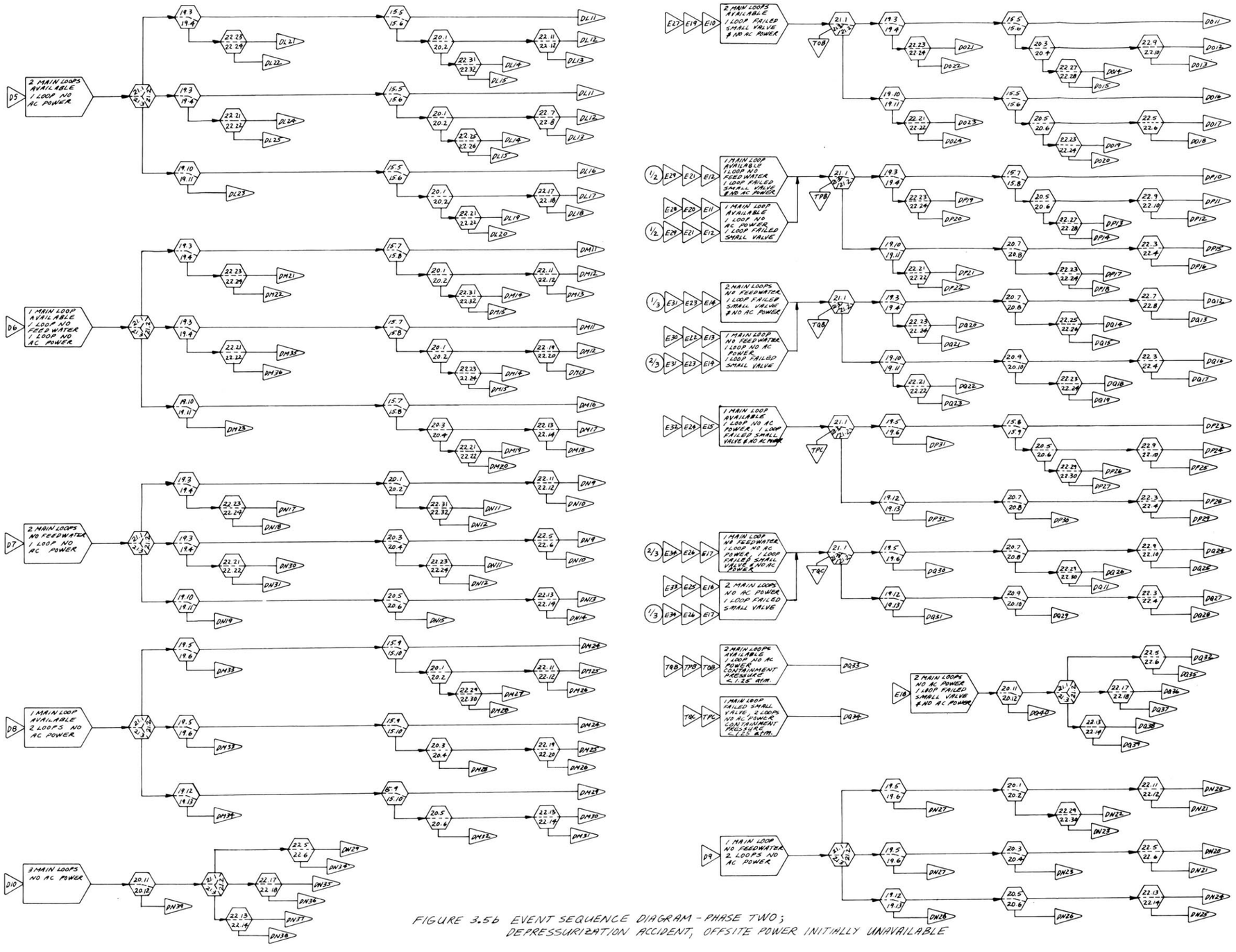


FIGURE 3.5b EVENT SEQUENCE DIAGRAM - PHASE TWO; DEPRESSURIZATION ACCIDENT, OFFSITE POWER INITIALLY UNAVAILABLE

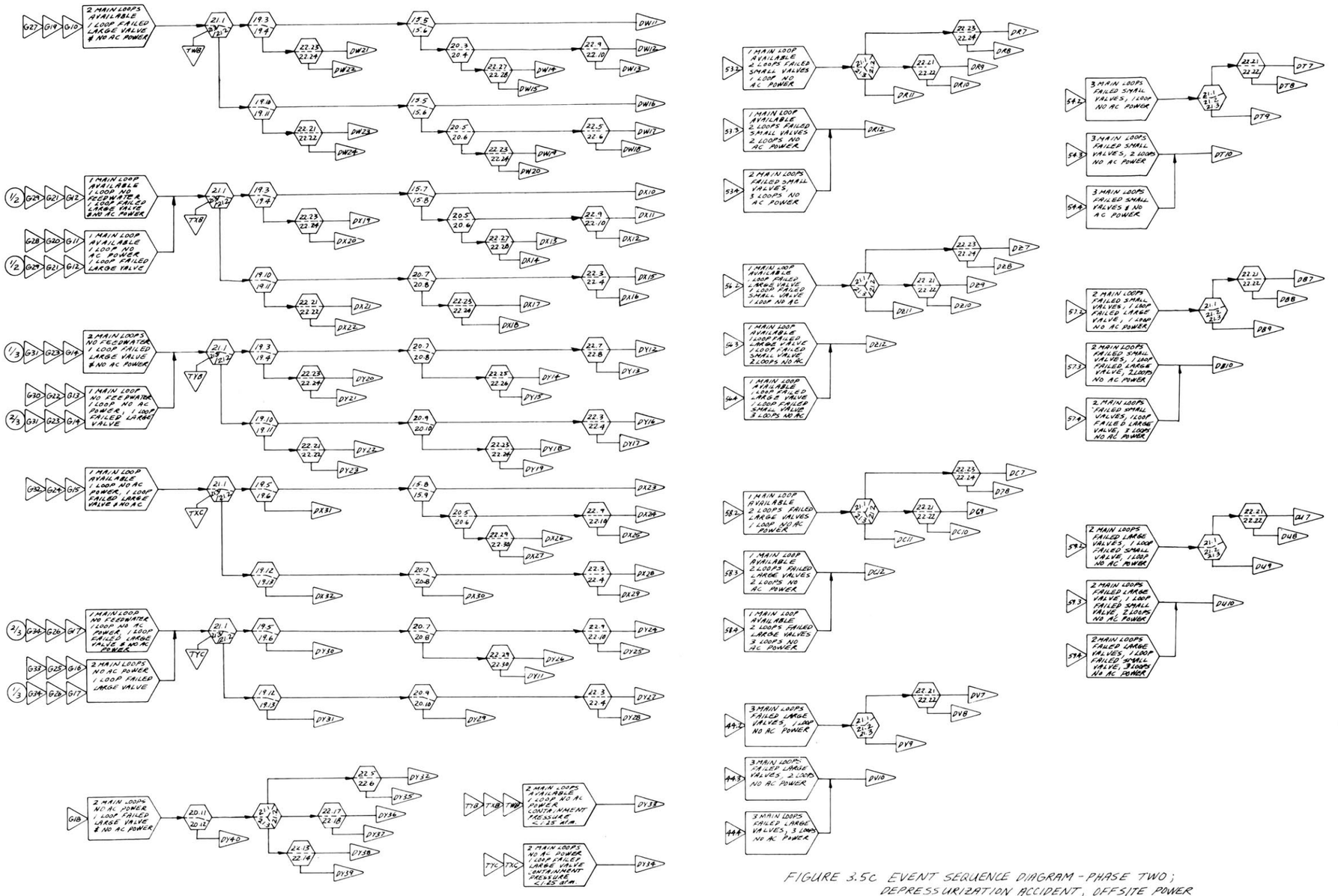


FIGURE 3.5c EVENT SEQUENCE DIAGRAM - PHASE TWO; DEPRESSURIZATION ACCIDENT, OFFSITE POWER INITIALLY UNAVAILABLE

3.4-3-1 Containment Equalization Pressure

The operating capabilities of both the main loop cooling system and the CACS are affected by the containment equalization pressure. Three ranges of containment equalization pressure were selected. The event sequence paths were branched according to the specific containment equalization pressure range, and the main loop capabilities and CACS capabilities could then be modelled accordingly.

Figure 3.6 [4] shows the variation in the maximum clad hot-spot temperature during a depressurization accident as a function of the PCRV leak size. Notice that over a large range of leak sizes, there is only a few hundred degree rise in the clad temperature. Plotted in the figure are curves for three main loops operating and for two main loops operating at a number of containment equalization pressures. Points off this figure were used to construct the lines on Figure 3.7. This latter figure shows the variation in the maximum clad hot-spot temperature as a function of the containment equalization pressure. Lines are plotted for three loop and for two loop operation and for 50 in^2 and 100 in^2 leak sizes.

From Figure 3.7, three ranges of the containment equalization pressure were chosen. These are:

1) greater than 1.50 atmosphere
2) between 1.25 and 1.50 atmospheres, and
3) less than 1.25 atmospheres.

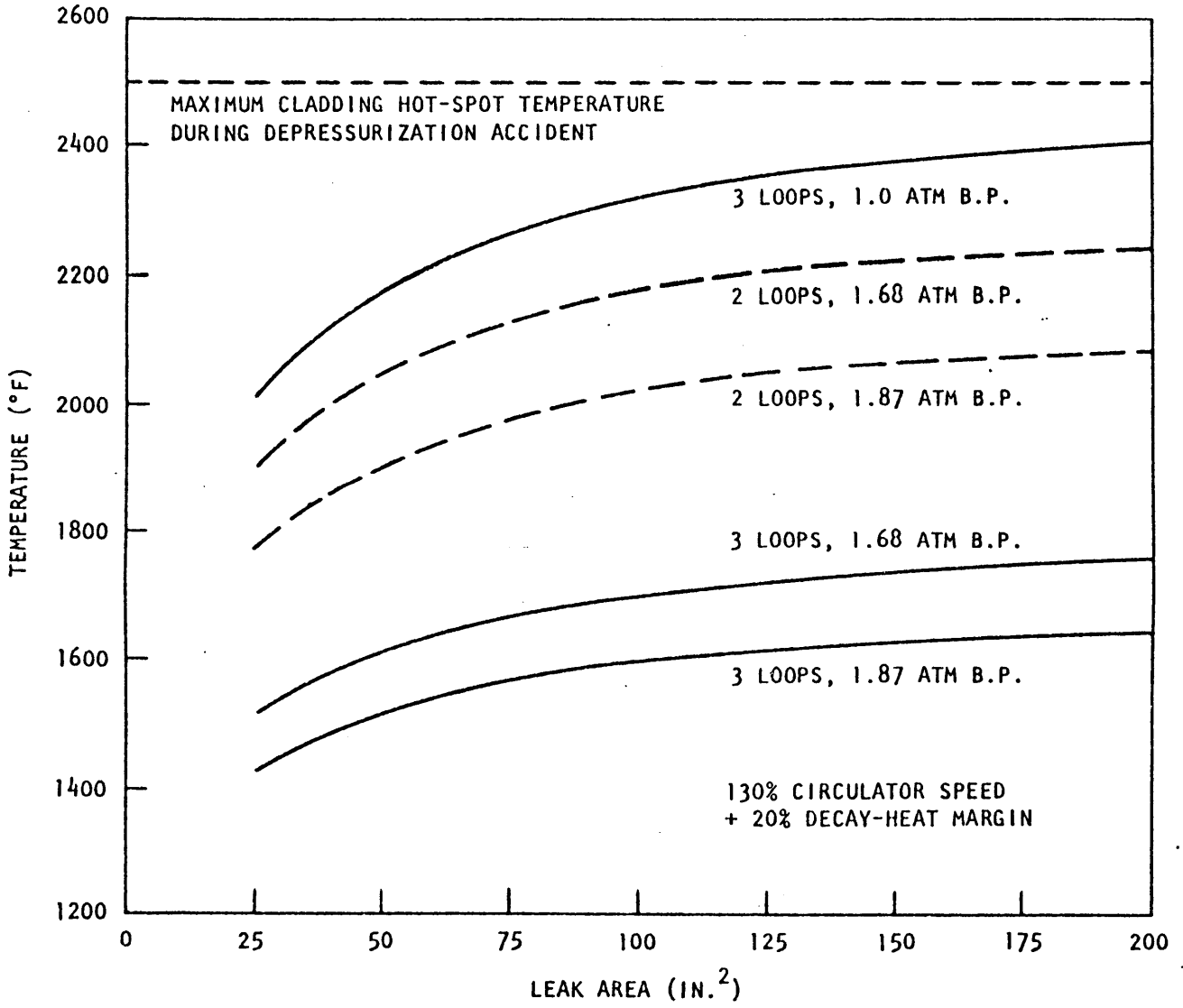


FIGURE 3.6 **Parametric survey of depressurization accidents beyond the design basis**

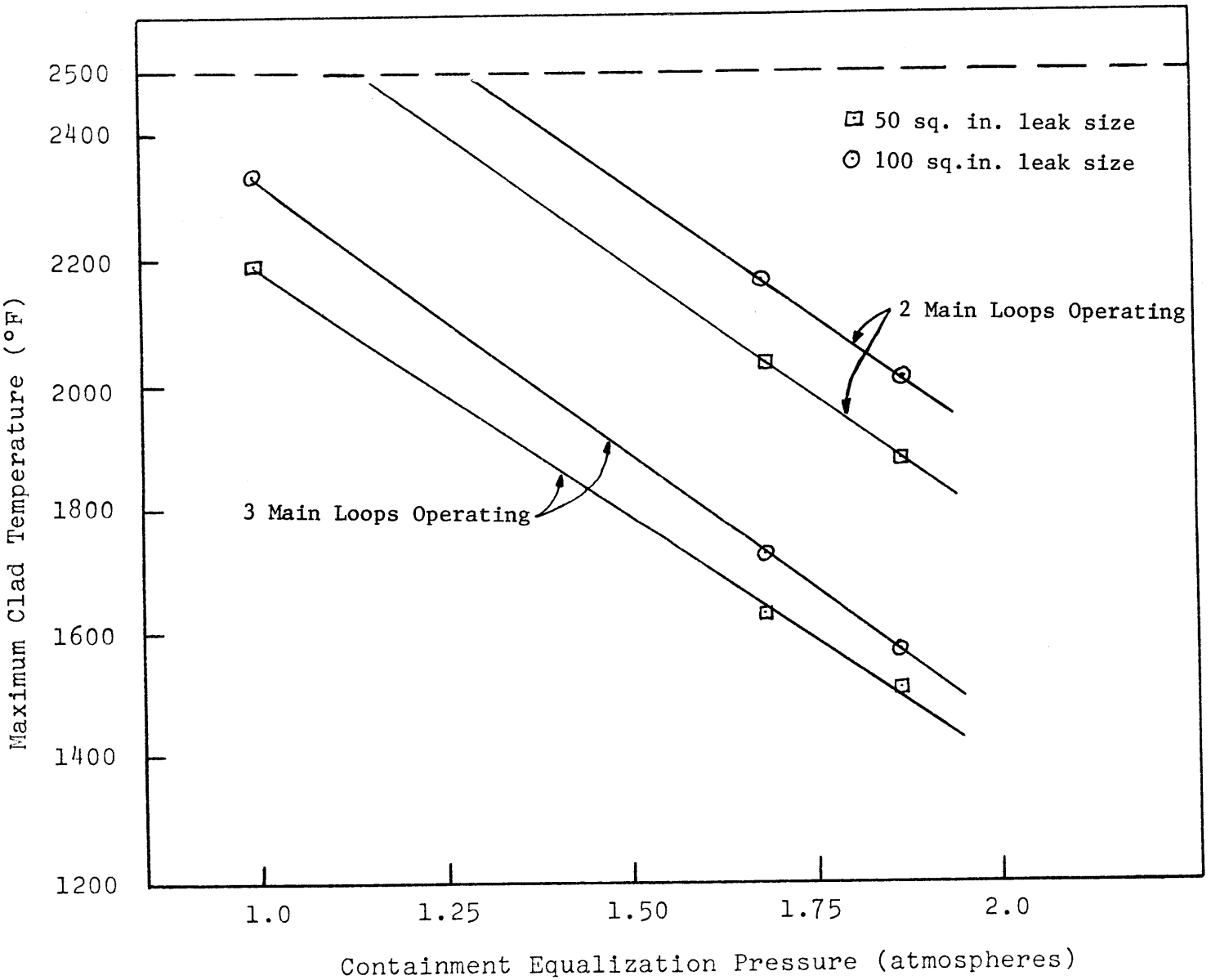


Figure 3.7 Maximum Clad Temperature Following a Depressurization Accident as a Function of the Containment Equalization Pressure

These were based upon the following considerations.

1) For a leak size greater than 50 in^2, the clad melting temperature (2500^oF) is exceeded if only two main loops are operating and the containment equalization pressure is less than 1.25 atmospheres.

2) In the range between 1.25 and 1.50 atmospheres two main loops may be able to prevent gross core melting, but because the circulators would most likely be operating near the overspeed trip setpoint, the operation of the circulator overspeed protection device becomes an important consideration.

3) Three main loops are adequate at any containment equalization pressure, however, below 1.25 atmospheres the circulator speed may approach the overspeed trip setpoint, and the possible operation of the overspeed protection device is considered.

The branching of the accident sequence paths according to the containment equalization pressure was accomplished in the ESD by those branch points containing index 21.

3.4-3-2 Main Loop Operating Capabilities

Table 2-IX summarized the steam generator inventory depletion times for main loop operation following a depressurization accident. It listed these times for the design containment equalization pressure of 1.8 atmospheres, and for a pressure of 1.0 atmospheres. In the ESD modelling, the accident paths with a containment equalization pressure greater than 1.5 were modelled using the depletion times corresponding to the design case. The depletion times for those accident paths in the

pressure range of 1.5 to 1.25 atmospheres were arbitrarily reduced by five minutes, and those paths with a pressure below 1.25 atmospheres were modelled using the values corresponding to 1.0 atmospheres.

These values are summarized in Table 3-VIII.

3.4-3-3 CACS Cooling Capabilities

The CACS cooling capabilities used in the modelling of the depressurization shutdown sequences are listed in Table 3-IX. For a containment equalization pressure greater than 1.50 atmospheres, the CACS capabilities at the design pressure of 1.8 atmospheres were used. These were taken from reference 2, which compared the CACS core flow capabilities against that core flow required to maintain a maximum clad temperature at or below 2200°F. The information in this reference was also used to extrapolate the CACS cooling capabilities at lower containment equalization pressures. Because the clad melting temperature is 2500°F, these core flow requirements give somewhat conservative results.

Figure 3.8 is a plot of the helium mass-flow through the core required to maintain the maximum clad temperature at or below 2200°F.[2] At 1.8 atmospheres, each CACS loop is capable of generating 11 lb/sec of helium flow. Between 1.50 and 1.25 atmospheres, a helium flow of 8 lb/sec per CACS loop was used, and below 1.25 atmospheres, a value of 6 lb/sec was employed. These values were based on the assumption that the auxiliary circulators are constant volume machines operating at a constant speed, and that the helium mass flow will decrease in direct proportion to the decrease in the helium density.

Table 3-VIII

Main Loop Operating Times Used in the ESD
Modelling of Shutdowns Following a Depressurization Accident

Number of Main Loops Available	Number of Available Main Loops With Feedwater	Main Loop Operating Time (minutes)		
		CEP>1.50atm.	CEP 1.50-1.25atm.	CEP<1.25atm.
3	3 2 1 0	30 30 30 30	30 30 25 20	30 25 20 15
2	2 1 0	25 20 15	20 15 10	4
1	--	4	3	2
0	--	2	2	2

CEP = containment equalization pressure

At the design containment equalization pressure, core-flow-bypass ratios were calculated from the core flows given in reference 2. These same ratios were used at the lower equalization pressures to generate the CACS capabilities in Table 3-IX a and b. Table 3-IXa gives the number of CACS loops capable of maintaining adequate core flow as a function of the time interval during which main loop failure occurs, the number of main loop isolation valves failed to open (allowing core-bypass flow), and the containment equalization pressure. Table 3-IXb lists the CACS capabilities given one CACS loop has failed and its loop isolation valve is open allowing core-bypass flow. Note that for this particular situation, the two remaining CACS loops are not capable of core cooling before 30 minutes if the containment equalization pressure is below 1.25 atmospheres.

The CACS availability for the various time intervals containment equalization pressures, and main loop isolation valve failures was determined separately and is modelled in the ESD by the hexagons containing the index 22. Appendix B contains a description of how these availabilities were modelled.

3.4-3-4 Main Loop Isolation Valve Operations

As in the pressurized shutdowns, the effect of core-flow-bypass, due to loop isolation valve failures, on the main loop cooling system performance was not explicitly modelled in the ESD. This effect was incorporated in the steam generator inventory depletion times used.

Table 3-IXa

CACS Cooling Capabilities Following a Depressurization Accident

Time Interval Following Shutdown During Which Main Loop Failure Occurs	Number of Main Loop Isolation Valves Bypassing	Number of CACS Loops Capable of Core Cooling		
		CEP> 1.50atm.	CEP 1.50-1.25atm.	CEP< 1.25atm.
Before 2 minutes	0	3,2	3	3
	1	3	3	--
	2	--	--	--
	3	--	--	--
2 to 5 minutes	0	3,2	3,2	3
	1	3,2	3	--
	2	3	--	--
	3	--	--	--
5 to 10 minutes	0	3,2	3,2	3
	1	3,2	3	3
	2	3	3	--
	3	3	--	--
10 to 15 minutes	0	3,2	3,2	3
	1	3,2	3,2	3
	2	3,2	3	--
	3	3	--	--
15 to 20 minutes	0	3,2,1	3,2	3
	1	3,2	3,2	3
	2	3,2	3	--
	3	3	3	--
20 to 25 minutes	0	3,2,1	3,2	3,2
	1	3,2	3,2	3
	2	3,2	3	3
	3	3	3	--
25 to 30 minutes	0	3,2,1	3,2	3,2
	1	3,2	3,2	3
	2	3,2	3,2	3
	3	3,2	3	--

CEP = containment equalization pressure

Table 3-IXb

CACS Cooling Capabilities Following a Depressurization Accident

One Auxiliary Circulator Failed and its Loop Isolation Valve Open Allowing Core Bypass Flow			
Time Interval Following Shutdown During Which Main Loop Failure Occurs	Number of Main Loop Isolation Valves Bypassing	Number of CACS Loops Capable of Core Cooling	
		CEP 1.50atm.	CEP 1.50-1.25atm.
0 to 10 minutes	0	--	--
	1	--	--
	2	--	--
	3	--	--
10 to 15 minutes	0	2	--
	1	--	--
	2	--	--
	3	--	--
15 to 20 minutes	0	2	--
	1	2	--
	2	--	--
	3	--	--
20 to 25 minutes	0	2	2
	1	2	--
	2	--	--
	3	--	--
25 to 30 minutes	0	2	2
	1	2	--
	2	2	--
	3	--	--

CEP = containment equalization pressure

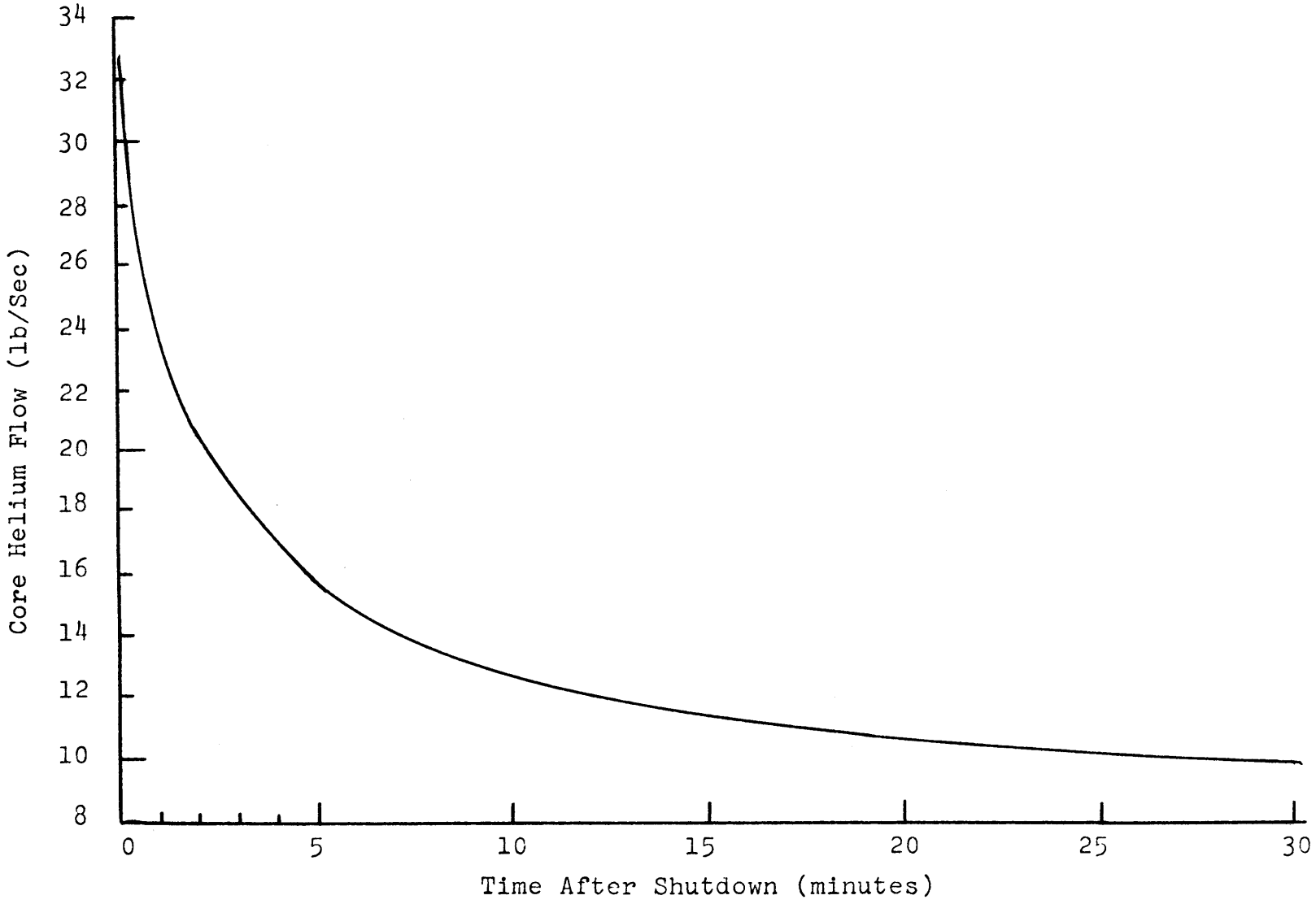


Figure 3.8 Core Flow Required to Maintain a Maximum Clad Temperature at or Below 2200°F

Circulator-turbine imbalance conditions were not modelled for shutdowns following a depressurization accident. Following any circulator-turbine control valve failure, the circulator was assumed to quickly overspeed and be tripped by the circulator overspeed protection device.

The effect of main loop isolation valve failures on the performance of the CACS was specifically incorporated into the CACS availability as described in the previous section.

3.4-3-5 Restart of Initially Failed Shutdown Feedpumps

The possibility of restarting initially failed shutdown feedpumps was not considered in the shutdown operations following a depressurization accident. The time available for such actions is somewhat shorter in this case, but more importantly, the results from the pressurized shutdowns indicated that the effect of restart operations on the probability of a core meltdown was small. Therefore the modelling effort for the depressurization shutdowns was not felt to be justified.

3.4.-3-6 Main Loop Support Systems

Main loop cooling system failures due to support system faults were modelled exactly as in the pressurized shutdown sequences by branch points containing the index 19. As in the pressurized shutdowns, the operation on the support

systems is dependent upon essential AC electrical power. However, the depressurization accident was felt to present an additional likelihood of main loop cooling system failure. This is especially important due to potential effects related to main circulators operating at speeds near their overspeed set point. Thus, for three main loops operating below a containment equalization pressure of 1.25 atmospheres, and for two main loops operating between 1.50 and 1.25 atmospheres, an additional term was included in the main loop cooling system failure probability. This is evidenced by the fact that the branch points for these event paths contain different index values. This term could then be varied to investigate the effect on the probability of a core meltdown of reduced circulator reliability when operating at or near the overspeed setpoint.

3.4-3-7 Additional Concerns

Of significant concern during a PCRV depressurization, is the effect of the depressurization forces on the PCRV internals. Both the main loop and auxiliary loop components, such as diffuser vanes, steam generator and heat exchanger shrouds, and loop isolation valves and valve structural supports are to be designed to withstand the depressurization forces due to a DBDA. The probability that the PCRV internals would remain intact following a DBDA was considered to be high. These failures were, therefore, not modelled in the ESD. However, because of this assumption, the ESD cannot be completely valid for depressuization accidents greater

than the DBDA.

3.4-4 PCRV Depressurization Leak Size

Depressurization accidents are assumed to result from failures of PCRV penetrations or penetration closures. These penetrations range in size from small instrument line connections to the reactor-cavity and steam-generator-cavity closures. Table 3-X is a list of the PCRV penetrations and the potential flow area through each penetration.

The present design basis depressurization accident (DBDA) is assumed to be initiated by the failure of the primary holddown mechanism of either the reactor-cavity closure, or one of the steam-generator-cavity closures. The arrangement of these two types of closures is shown in Figures 3.9 and 3.10. The primary holddown mechanism consists of a bolt and toggle arrangement. The secondary holddown is provided by the breech-lock arrangement of the closure and penetration which requires the rotation of the closure for engagement or disengagement. Each holddown system transfers the pressure load of the closure to a different portion of the PCRV.

With the failure of the primary holddown device, the closure plug will shift slightly but will remain essentially in place due to the secondary holddown mechanism. The closure seal is assumed broken and helium is free to escape along the annular passage between the penetration liner and closure plug. A piston-ring type of flow restrictor is provided in this

Table 3-X

A List of PCRV Penetrations and Potential Flow Areas

Penetration	Potential Flow Area (in^2)
Steam Generator	
Seal weld failure	8.9
Flow through seal rings	25.0
One superheater tube sheet	1.2
One resuperheater tube sheet	1.3
Circulator flow restrictor	4.1
Central Cavity	
Seal weld failure	7.5
Flow through seal rings	21.0
One control rod penetration	1.6
Auxiliary Heat Exchanger	
Flow restrictor	3.8
PCRV Bottom	
Fuel-handling machine	1.3
Fuel service machine	0.65
Fuel loading	0.33
Fuel unloading	0.33
Feedwater	1.4
Relief Valve	
One tube, 5 in. diameter and 40 ft. long	20

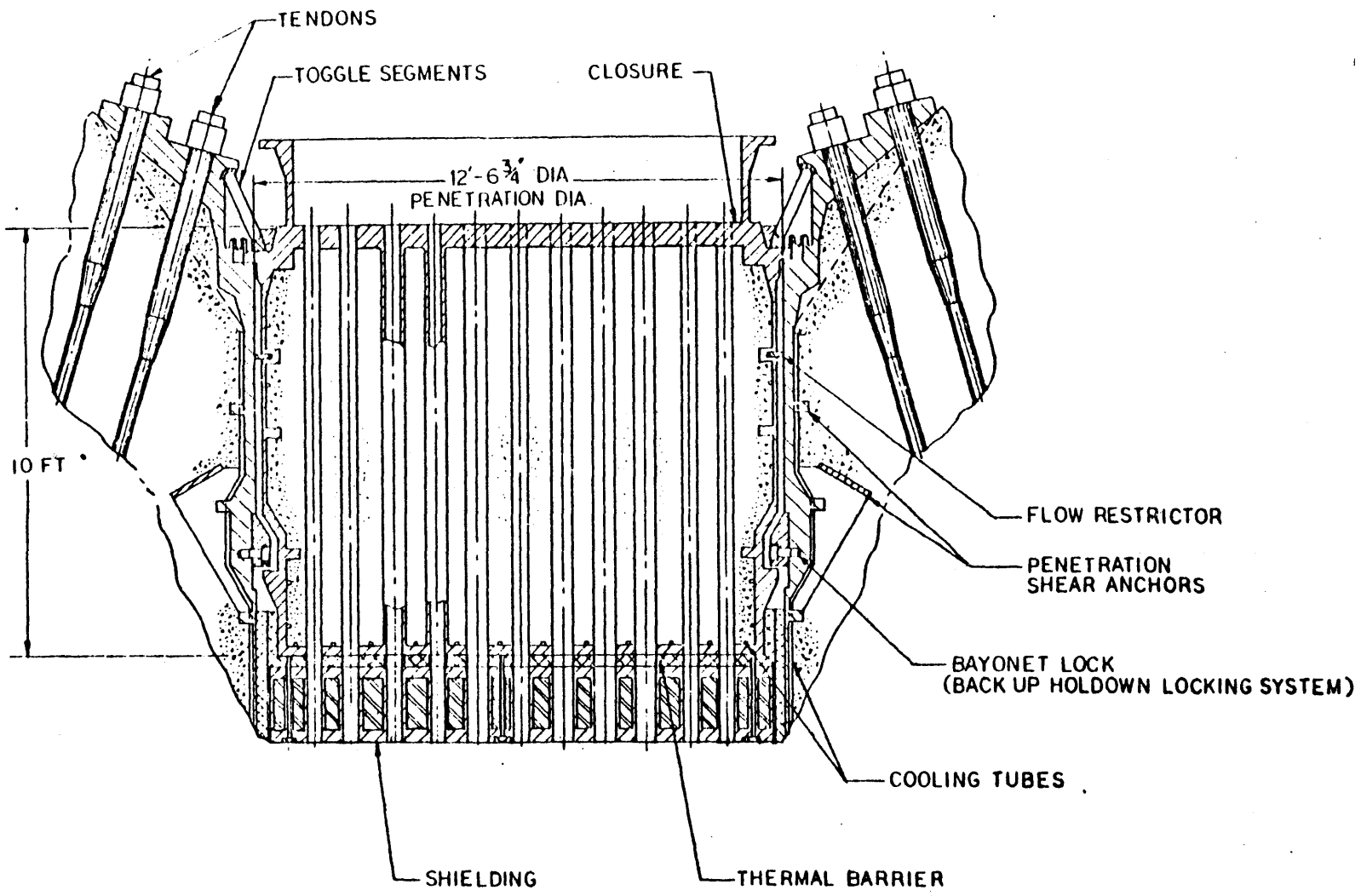


FIGURE 3.9 A Cross-section of the PCRV Central Cavity Closure

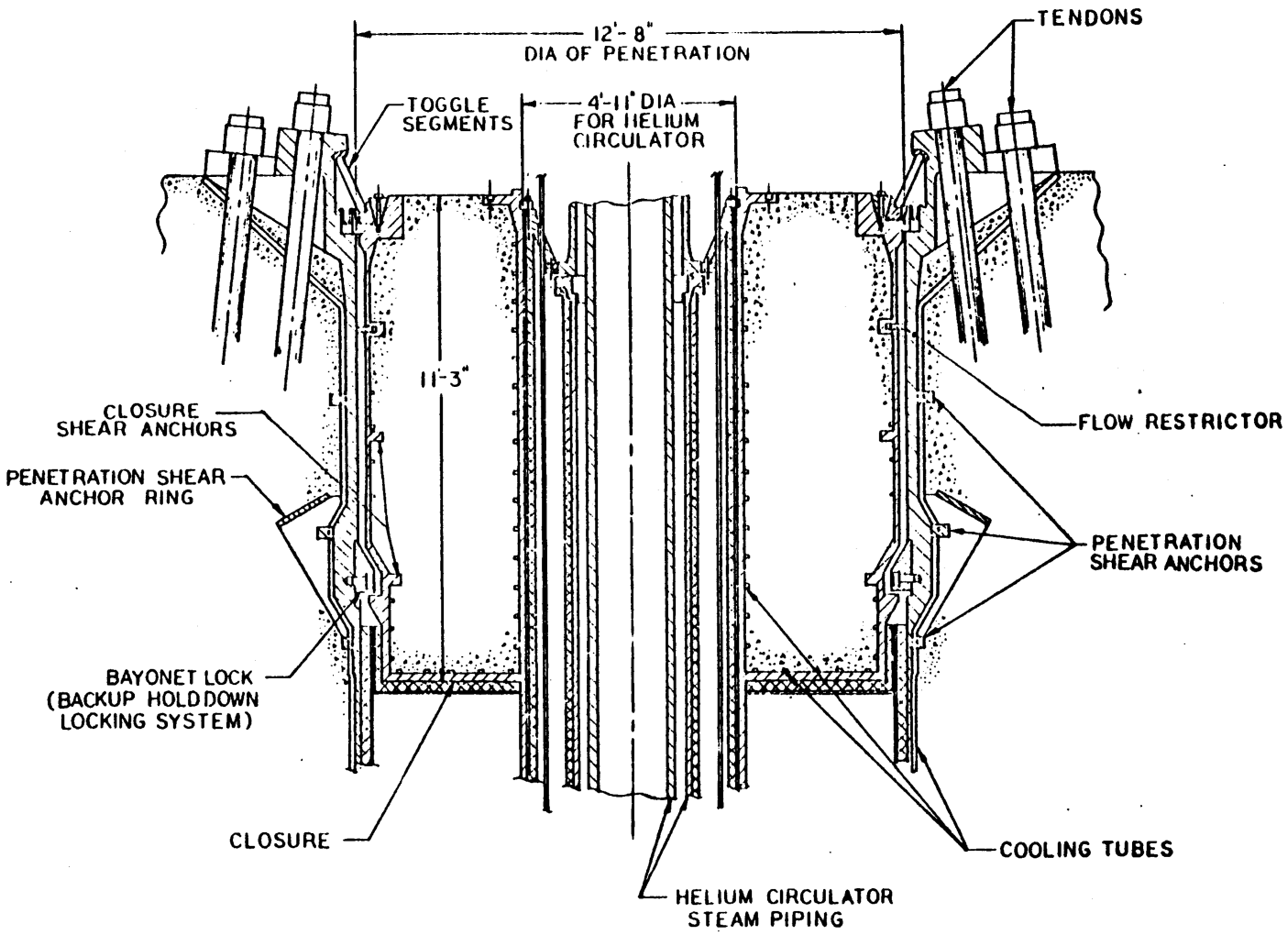


FIGURE 3.10 A Cross-section of a Steam Generator Cavity Closure

annular passage which is designed to limit the leak area for the depressurization. The present DBDA leak size of 25 in^2 requires a flow restrictor clearance around the 12 foot diameter penetrations of roughly 0.05 inches. However, a 100 in^2 leak size would require a clearance of over 3/16 of an inch around the entire circumference.

Large Leak Sizes

The ESD of the reactor shutdown operations following a depressurization accident was developed using information based on a PCRV leak size of 25 in^2. For this leak size, the depressurization is complete in approximately four minutes, and the bulk of the shutdown heat removal operations are carried out at the containment equalization pressure. However, the present modelling of the shutdown operations should be acceptable if a larger DBDA leak size, up to 100 in^2, is chosen. This is based on the following reasoning.

1) As shown in Figure 3.6, the increase in the maximum clad temperature with increasing leak size, for the acceptable main loop operating states is below the damage limit. Acceptable core temperatures can thus be maintained at these larger leak sizes.

2) The required main loop pumping power will increase slightly with the leak size, however, this effect on the steam generator inventory depletion times should be less than the present uncertainties in these values due to potential

shutdown controller design trade-offs.

3) CACS operating performance is affected through the increase in air ingress with larger leak sizes. Air ingress into the PCRV, due primarily to natural convection forces, increases the reactor coolant molecular weight and decreases its specific heat and thermal conductivity.[5] However, the effects of air ingress will be required to be fully considered in the design basis of the CACS.[6] Also, the modelling of the CACS only states the number of loops capable of core cooling. The present auxiliary cooling loop design bases may be changed to account for such effects as air ingress, but this should not greatly affect the modelling.

Intermediate Leak Sizes

PCRV leak sizes in the range between 1 in^2 and 25 in^2 will result in depressurizations which occur, to a varying extent, during the initial reactor shutdown heat removal operations. The PCRV depressurization time as a function of leak sizes in this range is shown in Figure 3.11.

The varying reactor coolant pressure results in an additional complexity in any attempt to model the reactor shutdown and decay heat removal operations. This modelling was not undertaken, and these leak sizes were conservatively analyzed using the ESD developed for the large PCRV leak sizes.

Small Leak Sizes

For leak sizes less than 1 in^2, the PCRV depressurization

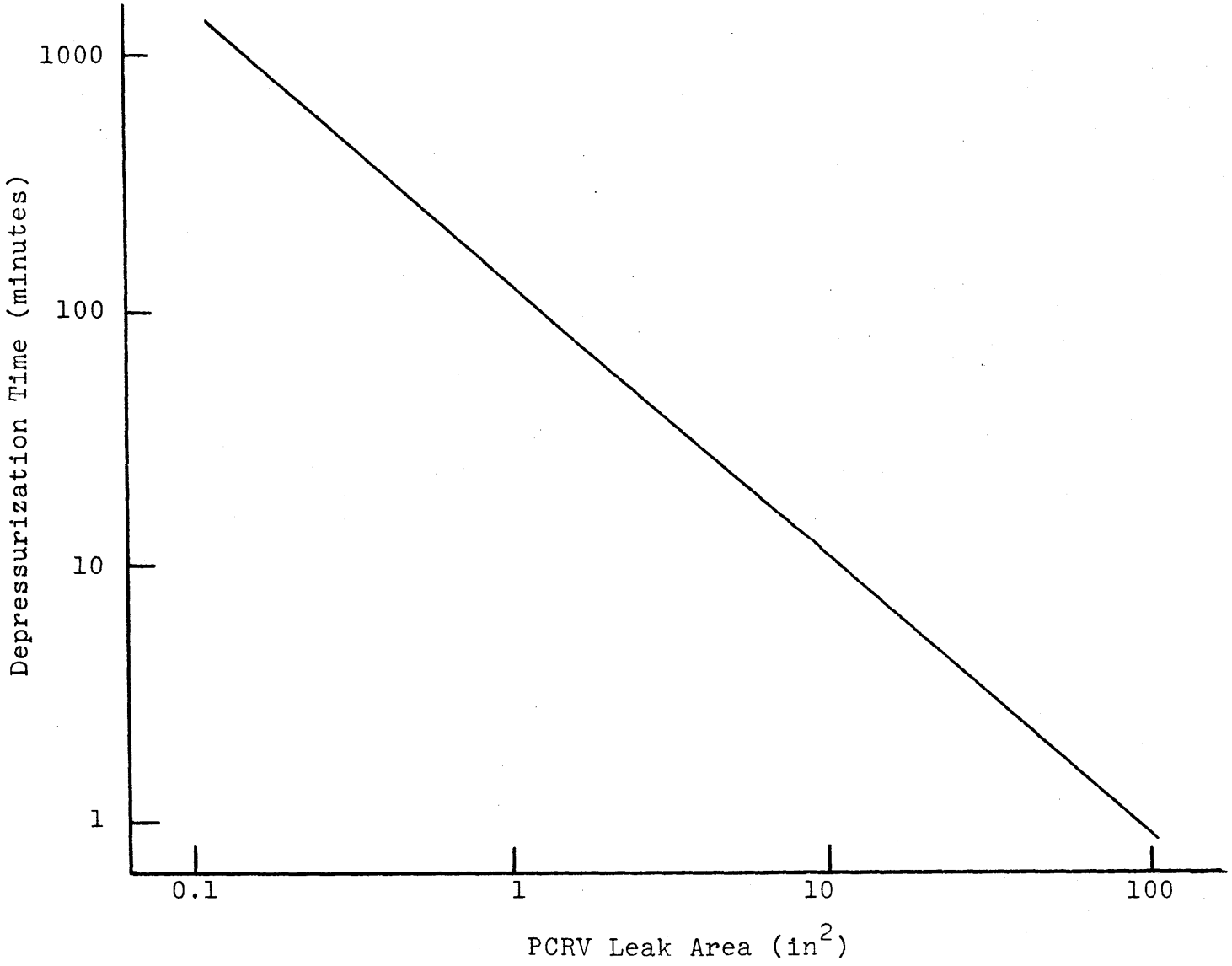


Figure 3.11 PCRV Depressurization Time as a Function of Leak Size

time is greater than 100 minutes. The initial shutdown and decay heat removal operations will occur in a partially pressurized reactor, and the main loop cooling system performance should not be greatly affected in at least the first 20 to 30 minutes. This range of PCRV leaks was not felt to cause any appreciable degradation of the main loop or CACS performance, and so no special modelling of these reactor shutdown sequences was done.

3.4-5 ESD Outcome Categories - Depressurized Case

The final event sequences for the depressurized shutdowns are grouped into 7 outcome categories. These are 3 system success categories and 4 system failure categories. These categories are summarized in Table 3-XI.

Table 3-XII lists the individual accident sequences, by their ESD index, for each of the outcome categories. As with ouctome category 9 for pressurized accident sequences, outcome category D7 does not contain core-melt accident sequences which occur before two minutes. This is because in the ESD modelling no main loop failures occur before this time.

3.5 Event Sequence Categories

As described in the previous sections, the final event sequences were all collapsed into a few outcome categories which describe the overall plant status. Lists of these categories are given in Tables 3-V and 3-XI. The event

sequences combined in these outcome categories lead to either success or failure of the shutdown cooling systems. Thus, the ESD results in the same general conclusions as the event tree of Figure 3.1, but in much greater detail.

The sum of the probability of all the system failure categories (categories 4 through 9 for the pressurized case, and categories D4 through D7 for the depressurized case) represents the probability that the shutdown cooling systems fail to provide adequate decay heat removal. The analysis of the shutdown and decay heat removal operations focused primarily on these events.

However, the event sequences which lead to the success of the main loop cooling system were also felt to be of significance. Unreliability of the main loop cooling system places greater importance on the reliability of the CACS. Therefore, outcome category 1 was watched closely in the analysis of the shutdown and decay heat removal operations.

Table 3-XI

ESD Outcome Categories for the Depressurized Reactor Case

System Success

Category D1. Adequate decay heat removal provided indefinitely by the main loop cooling system.

Category D2. Adequate decay heat removal provided indefinitely by the CACS, main loop failure occurs after 15 minutes of the shutdown,

Category D3. Adequate decay heat removal provided indefinitely by the CACS, main loop failure occurs between 2 and 15 minutes of the shutdown.

System Failure

Category D4. Loss of adequate decay heat removal in the interval between 20 and 30 minutes of the shutdown,

Category D5. Loss of adequate decay heat removal in the interval between 10 and 20 minutes of the shutdown,

Category D6. Loss of adequate decay heat removal in the interval between 5 and 10 minutes of the shutdown, and

Category D7. Loss of adequate decay heat removal within 5 minutes after the shutdown

Table 3-XII

A List of the Individual Shutdown Event

Sequence Following a Depressurization Accident

Category D1. Adequate decay heat removal provided indefinitely by the main loop cooling system.

DK1, DK4
DL1, DL4, DL11, DL16
DM1, DM4, DM11, DM16, DM24, DM29
DO1, DO4, DO11, DO16
DP1, DP10, DP23
DW1, DW4, DW11, DW16
DX1, DX10, DX23

Category D2. Adequate decay heat removal provided indefinitely by the CACS, main loop failure occurs after 15 minutes of the shutdown.

DK2, DK5
DL2, DL5, DL12, DL14, DL17, DL19
DM2, DM5, DM12, DM14, DM17, DM19, DM25, DM27, DM30
DN1, DN3, DN9, DN11, DN13, DN15, DN20, DN22, DN24
DO2, DO5, DO12, DO14, DO17, DO19
DP2, DP4, DP11, DP13, DP15, DP17, DP24, DP26, DP28
DQ1, DQ3, DQ12, DQ14, DQ16, DQ18, DQ24, DQ26, DQ27
DW2, DW5, DW12, DW14, DW17, DW19
DX2, DX4, DX11, DX13, DX15, DX17, DX24, DX26, DX28
DY1, DY3, DY12, DY14, DY16, DY18, DY24, DY26, DY27

Category D3. Adequate decay heat removal provided indefinitely by the CACS, main loop failure occurs between 2 and 15 minutes of the shutdown.

DK7, DK9, DK11
DL7, DL9, DL21, DL24, DL26
DM7, DM9, DM21, DM35, DM37
DN5, DN7, DN17, DN29, DN30, DN32, DN35, DN37
DO7, DO9, DO21, DO23
DP6, DP8, DP19, DP21
DQ5, DQ7, DQ9, DQ20, DQ22, DQ32, DQ36, DQ38
DR1, DR3, DR5, DR7, DR9
DT1, DT3, DT5, DT7
DU1, DU3, DU5, DU7
DV1, DV3, DV5, DV7

Table 3-XII cont.

DW7, DW9, DW21, DW23
DX6, DX9, DX19, DX21
DY5, DY7, DY9, DY20, DY22, DY32, DY36, DY38
DZ1, DZ3, DZ5, DZ7, DZ9
DB1, DB3, DB5, DB7
DC1, DC3, DC5, DC7, DC9

Category D4. Loss of adequate decay heat removal in the interval between 20 and 30 minutes of the shutdown.

DK3, DK6
DL3, DL6, DL13, DL15, DL18, DL20
DM3, DM6, DM13, DM15, DM18, DM20, DM26, DM28, DM31, DM32
DN2, DN4, DN10, DN12, DN14, DN16, DN21, DN23, DN25, DN26
DO3, DO6, DO13, DO15, DO18, DO20
DP3, DP12, DP14, DP25, DP27
DW3, DW6, DW13, DW15, DW18, DW20
DX3, DX12, DX14, DX25, DX27

Category D5. Loss of adequate decay heat removal in the interval between 10 and 20 minutes of the shutdown.

DP5, DP16, DP18, DP29, DP30
DQ2, DQ4, DQ11, DQ13, DQ15, DQ17, DQ19, DQ25, DQ28 DQ29
DX5, DX16, DX18, DX29, DX30
DY2, DY4, DY11, DY13, DY15, DY17, DY19, DY25, DY28, DY29

Category D6. Loss of adequate decay heat removal in the interval between 5 and 10 minutes of the shutdown.

DK8, DK10, DK12
DL8, DL10, DL22, DL23, DL25, DL27
DM8, DM10, DM22, DM23, DM33, DM34, DM36, DM38
DN6, DN8, DN18, DN19, DN27, DN28, DN31, DN33, DN34, DN36, DN38, DN39
DO8, DO10, DO22, DO24
DP7, DP9, DP20, DP22, DP31, DP32
DQ6, DQ8, DQ21, DQ23, DQ30, DQ31, DQ35, DQ37, DQ39, DQ40
DW8, DW10, DW22, DW24

Table 3-XII cont.

DX7, DX9, DX20, DX22, DX31, DX32
DY6, DY8, DY21, DY23, DY30, DY31, DY35, DY37, DY39, DY40

Category D7. Loss of adequate decay heat removal within 5 minutes after the shutdown.

DQ10, DQ34
DR2, DR4, DR6, DR8, DR10, DR11, DR12
DT2, DT4, DT6, DT8, DT9, DT10
DU2, DU4, DU6, DU8, DU9, DU10
DV2, DV4, DV6, DV8, DV9, DV10
DY10, DY34
DZ2, DZ4, DZ6, DZ8, DZ10, DZ11, DZ12
DB2, DB4, DB6, DB8, DB9, DB10
DC2, DC4, DC6, DC8, DC10, DC11, DC12

Chapter 4

Initiating Events and Accident Sequence Analysis Inputs

4.1 Introduction

The ESD is a generalized modelling of the reactor shutdown operations. It is the addition of the initiating event which changes these shutdown event sequences into accident sequences. The potential GCFR core-melt accidents were classified into two general types: 1) those resulting from severe power to heat removal imbalances following a reactor shutdown, and 2) those resulting from severe power to heat removal imbalances during power operation. This research has been mainly concerned with the first general class of accidents. These may result from losses of either adequate forced helium circulation or adequate decay heat removal following a reactor shutdown.

The second class of accidents may result either from losses of adequate helium circulation without reactor shutdown, or from reactor overpower transients. These accidents involve failure of the reactor to shutdown, and due to the high reliability that is expected for the reactor shutdown systems these accidents were not investigated in detail. Failure of the reactor shutdown systems does not automatically result in a core meltdown. Adequate core cooling may be maintained by the main loops following certain reactor shutdown initiating events. The probability of

a core meltdown due to the failure of the reactor to shutdown should then be less than the failure probability of the reactor shutdown systems. However, in this study, the failure of the reactor to shutdown was conservatively assumed to lead to a core meltdown, and the total core melt probability for a given initiating event can be described by the following equation:

$$P_i = (P_S + P_F)\ P_{IE},$$ where

P_i is the total probability of a core meltdown for a given initiating event;

P_S is the conditional probability of a meltdown following reactor shutdown, given the initiating event;

P_F is the conditional probability of a meltdown due to failure of the reactor shutdown systems, given the initiating event; and

P_{IE} is the probability **or** frequency of occurrence of the event requiring a reactor shutdown.

The initiating events for a possible core melt accident then become all events which can initiate a reactor shutdown. This includes innocuous shutdowns, shutdowns resulting from anticipated transcents, and shutdowns resulting from various accident initiating events.

The specific reactivity effects of different anticipated transients or accidents were not given special consideration based upon the results of a study by Torri and Driscoll.[1] The study analyzed the GCFR reactivity insertion mechanisms for the demonstration plant design. Their conclusion was

that the influence of reactivity effects on the normal operating and transient behavior of the GCFR design was mild. Their analyses included normal and anticipated operating occurrences, and a number of accident conditions including: steam inleakage; reactor coolant depressurization; control rod withdrawal; and earthquake induced core vibrations. The reactivity insertion accidents were included along with the other events requiring a reactor shutdown, and the reactor shutdown cooling operations were considered to be unaffected by reactivity induced effects.

This chapter includes a detailed discussion of the various reactor shutdown initiating events. It also discusses the manner in which the accident sequence probability calculations were performed, and it summarizes the failure date and other information used to establish the subsystem reliability valves and other probability inputs employed in the overall analysis.

4.2 Reactor Shutdown Initiating Event Categories

4.2-1 Introduction

In order to analyze the ability of the GCFR demonstration plant to provide adequate core cooling during the reactor shutdown and decay heat removal operations, appropriate reactor shutdown initiating events must be determined. Yet, a reactor shutdown may be initiated by many different types of events ranging from innocuous reactor trips to a

design basis type accident. Because of the large number of possible initiating events, the entire range of individual shutdown initiating events was divided into separate initiating event categories. Specifically, because the GCFR has two shutdown cooling systems (the main loop cooling system and the CACS), it was convenient to combine the initiating events according to their effect upon either shutdown cooling system. Those initiating events which do not affect the shutdown cooling performance of either system were combined into category I. Category II initiating events are those which degrade the shutdown cooling performance of the main loop cooling system but do not affect the performance of the CACS. Those initiating events which commonly degrade the shutdown heat removal capability of both the main loop cooling system and the CACS are combined in Category III. Table 4-I lists these categories along with their major subcategories.

4.2-2 Initiating Events not Affecting the Performance of Either Shutdown Cooling System

Category I initiating events are those events which lead to a reactor shutdown but do not affect the heat removal capability of either the main loop shutdown cooling system or the CACS. There are two subcategories associated with this category, and Table 4-II lists the most common events in each subcategory.

Table 4-I

Reactor Shutdown Initiating Event Categories

Category I:	Initiating events not affecting the performance of either shutdown cooling system.
Subcategory A:	Innocuous trips
Subcategory B:	Failures in systems unrelated to the shutdown cooling system performance.
Category II:	Initiating events degrading the main loop shutdown cooling performance.
Subcategory A:	Initiating events affecting only a single main cooling loop.
Subcategory B:	Initiating events commonly affecting more than one main cooling loop.
Category III:	Initiating events commonly degrading the performance of both the shutdown cooling systems.
Subcategory A:	External events
Subcategory B:	Internal events
Subcategory C:	Support system failures

Table 4-II

Initiating Events Not Affecting the Performance of Either Shutdown Cooling System (Initiating Event Category I)

Subcategory A:

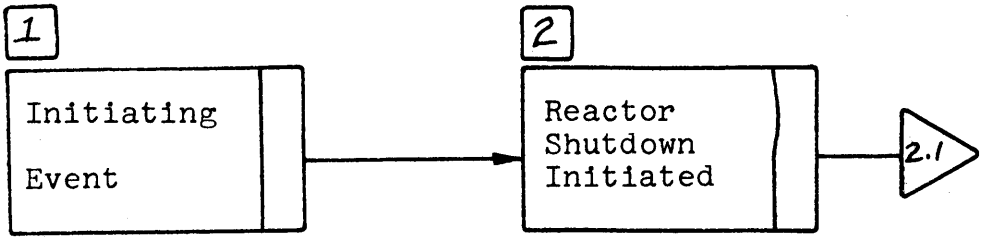
- Innocuous Trips

Subcategory B:

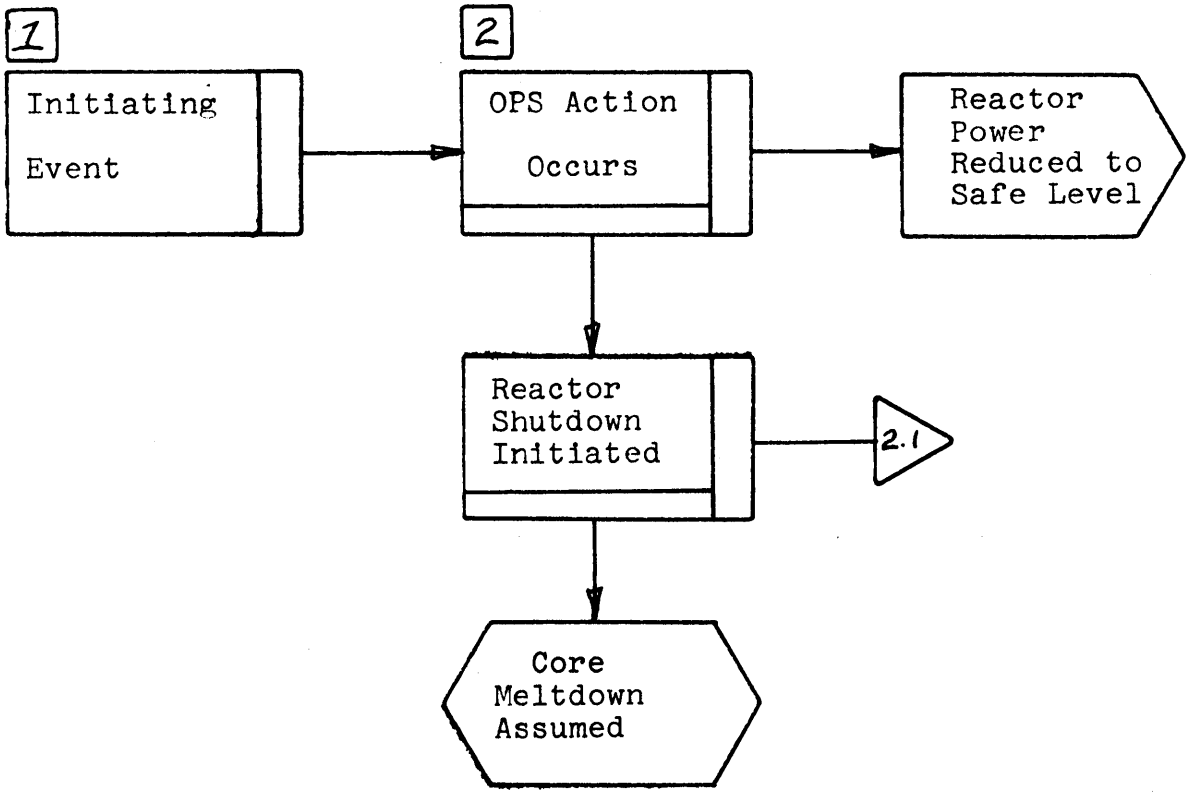
- Loss of offsite power and external load
- Turbine trip
- Loss of one main feed pump
- Inadvertent control rod withdrawal at power
- Small helium leak
- Loss of both main feed pumps

Figure 4.1

Initiating Events not Affecting the Performance of Either Shutdown Cooling System



Subcategory A. Innocuous Trips



Subcategory B. Failures in systems unrelated to the shutdown cooling system performance

Subcategory A includes those reactor shutdowns known as innocuous or spurious trips. Essentially, these are inadvertent forced reactor shutdowns which are initiated by such events as malfunctions in the reactor shutdown system, operator errors, or as the result of failures in portions of the plant unrelated to the reactor cooling systems. For this subcategory, the initiation of the reactor shutdown signal is assumed to be the initiating event, and a block diagram modelling of this event is shown in Figure 4.1.

Subcategory B includes those anticipated operating transients which do not directly affect the performance of the shutdown cooling systems. Typical events included in this subcategory are listed in Table 4-II. In all but one of the events listed (loss of both main feedpumps) the operational protection system (OPS) is designed to take corrective action which eliminates the need for a reactor shutdown. A block diagram modelling of these events is also included in Figure 4.1. The design of the OPS is not yet final, and so no evalution of its failure probability was made. A failure rate of 1×10^{-2} per demand was assumed. This value was felt to be very conservative for an operating control system.

In the event that OPS failure occurs and a reactor shutdown is initiated, the response of the shutdown cooling systems was considered to be identical to those following an innocuous trip. The plant response to these anticipated transients will be required to be well within the design margin

of the plant, and therefore, the shutdown and decay heat removal process should not be significantly affected.

The last event listed in Table 4-II is an example of more unlikely events which may require immediate reactor shutdowns but do not affect either shutdown cooling system.

Plant outages which result from an orderly shutdown of the reactor are considered in this category of initiating events, but they were not felt to be as significant as forced reactor shutdowns. These orderly shutdowns may be either scheduled or unscheduled, but they are essentially different from forced shutdowns. During an orderly reactor shutdown, both the reduction in reactor power level and the transition of the main cooling loops from their normal operating mode to the shutdown cooling mode are performed under the control and direction of the reactor operators. The reliability of the plant equipment to perform under these conditions would be quite high. Also, the operators would have more freedom during the shutdown process to either correct or counteract the faulty operation of some equipment. Therefore, orderly shutdowns were not included in the determination of the initiating event frequency of this category.

A study of the availability of the 19 nuclear power plants operating in the United States during 1972[2] indicated a total of 211 plant outages. Of these total outages, 167 involved shutdown of the reactor from an operating state, and only 91 of these involved a forced reactor shutdown

(scram or reactor trip). This represents an average of 5 reactor trips per year. The major causes of these reactor trips included failures of the primary and secondary coolant system equipment, the control rod system, the reactor protection instrumentation, the electrical generation and distribution systems, and operator errors. An investigation of these reactor trips indicated that for roughly half of these incidents, had they occurred in the GCFR, the OPS would have acted to prevent a forced reactor shutdown. Based on this information, an average of 3 forced reactor shutdowns per year was assumed to occur due to incidents of the type included in Category I.A. A similar frequency of occurrence was assumed for the more likely initiating events of Category I.B. However, due to the OPS, these events lead to a forced shutdown with a frequency of only 0.03 per year. Therefore, an average of 3 forced shutdowns per year was assumed due to all Category I initiating events.

Those events in subcategory I.B which require immediate reactor shutdown are unlikely to significantly increase the initiating event frequency for this category. For example, loss of both main feedpumps has a probability of occurrence of about 10^{-2} per year.

4.2-3 Initiating Events Degrading the Performance of the Main Loop Shutdown Cooling System

There are two specific subcategories for those events

which degrade the main loop cooling system performance but do not affect the CACS capabilities. The first subcategory combines all the events which independently affect the operation of only a single main cooling loop. The most common of these occurrences are listed in Table 4-III, and the ESD modelling for this subcategory is shown in Figure 4.2. For these occurrences the OPS acts both to shutdown that main loop in which the failure has occurred, and to initiate a programmed load reduction to 60% of full reactor power. This action allows the reactor to continue operating on only two main loops until either corrective action on the failed loop is taken, or an orderly reactor shutdown is performed.

The programmed load reduction is accomplished by the powered insertion of a set of three control rods, and the loop isolation is accomplished by closing the feedwater inlet valve, the resuperheater outlet valve and circulator-turbine large control valve for the loop. This stops the helium circulator and allows the loop isolation valves to close. Failure of the OPS to perform either function was assumed to initiate a reactor shutdown signal, and a failure rate for the OPS of 1×10^{-2} per demand was assumed.

Reference 2 indicated that approximately 20% of the total reactor trips were initiated by failures of primary coolant system equipment. This is a frequency of 1 event per year, and while this particular number cannot be totally applicable to the GCFR, it is indicative of the order of

Table 4-III

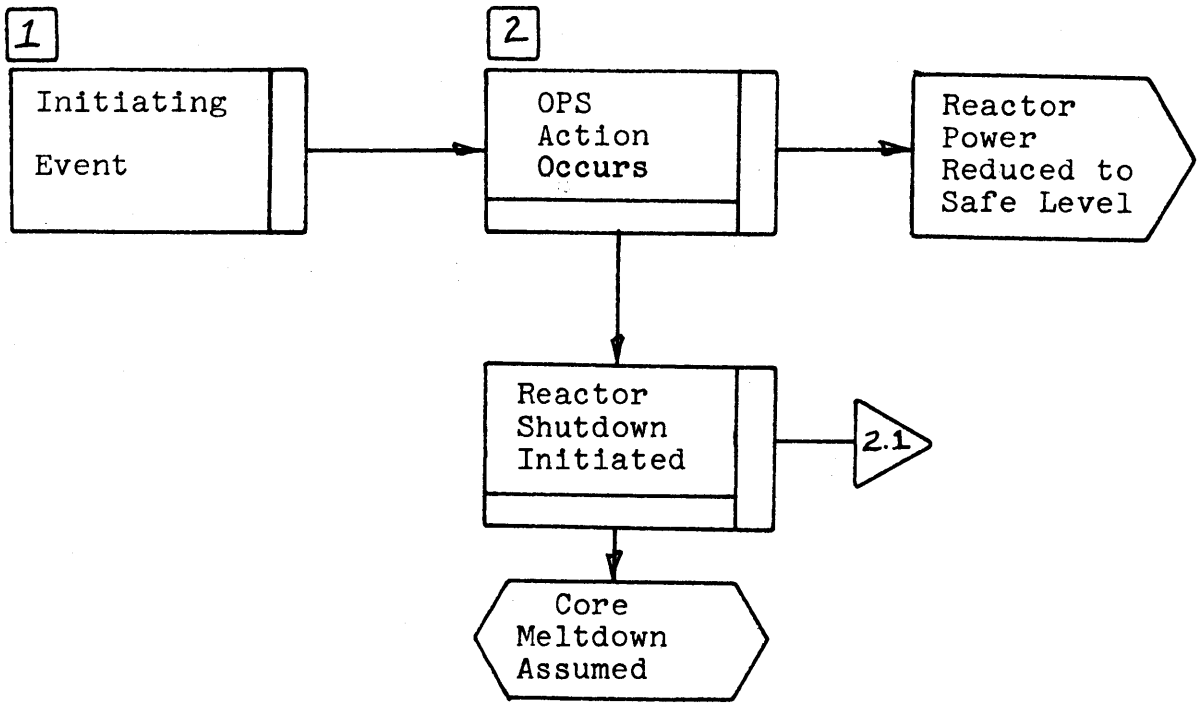
Initiating Events Leading to the Loss of a Single Main Cooling Loop (Initiating Event Category II.A)

1. Inadvertent closure of a feedwater control valve
2. Inadvertent full opening of a feedwater control valve
3. Inadvertent closure of a CT large CV
4. Inadvertent full opening of a CT large CV
5. Inadvertent opening of a resuperheater bypass control valve
6. Inadvertent opening of a relief or safety valve
7. Steam generator tube leak
8. Main circulator failure
9. Loop controller failure
10. Inadvertent loop isolation due to operator error or spurious protective system action
11. Steam line or feedwater are ruptured inside the containment building

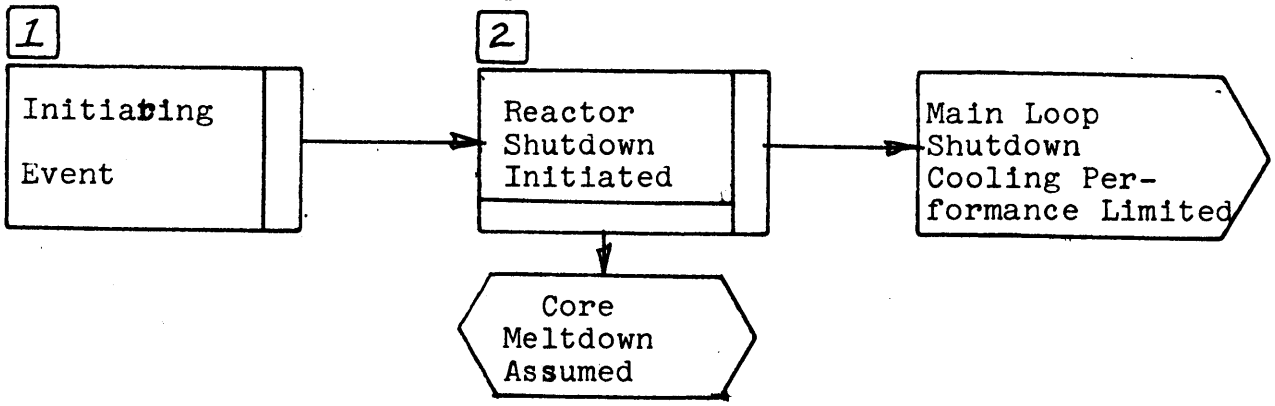
Figure 4.2

Initiating Events Degrading the Performance

of the Main Loop Shutdown Cooling System



Subcategory A: Events leading to the loss of a single main loop



Subcategory B: Events commonly degrading the shutdown performance of the main cooling loops

magnitude of the frequency of these events.

The last event listed in Table 4-III would require an immediate reactor shutdown with only two main loops available. However, the probability of a large pipe rupture inside the containment is on the order of 1×10^{-3} per year, and it does not significantly affect the total reactor shutdown initiation probability for this category which is about 1×10^{-2} per year.

The second subcategory includes those events which have a common effect on the shutdown heat removal performance of the main loop cooling system, but do not degrade the CACS performance. A block diagram modelling of this subcategory of events is also included in Figure 4.2. The main cooling loops are designed to be as independent as possible, however there are four areas in which they share some common dependence. These areas are described below:

1. Common Control Systems

   Potential failures of the main loop cooling system might arise from control system faults, however none were found in this analysis. While the plant regulator provides a common control of the main loop during normal operation, each main cooling loop has its own independent shutdown controller.

2. Common Heat Sink

The three main cooling loops share a common heat sink, which is the main condenser. However, if the condenser is unavailable, independent relief valves are provided in the exhaust path of each circulator-turbine to maintain steam flow and to allow heat rejection directly to the atmosphere. The overall effect on initial main loop operation is negligible, but the long term main loop operation may be limited by the condensate storage supply if the emergency feedwater supply is not available.

3. Common Feedwater Supply

Those items of the shutdown feedwater supply which are common to the main cooling loops are the condenser hotwell, the condensate storage tank and the piping on the suction side of the shutdown feedwater pumps. However, the effect of the loss of any one of these items is small, and even the loss of all feedwater does not immediately eliminate the main loops because of the stored inventory available in the steam generators.

4. Common Support Systems

The three support systems which are common to the main loop cooling system are the service water system, the instrument air system and the reactor

plant cooling water system. (The essential electrical supply is not considered here because it also affects the CACS.)

The reactor plant cooling water system provides cooling for the main circulator bearing water supplies. While the circulator bearing heat load is quite high during full power operation, the bearing friction during the reactor shutdown cooling operations is quite small. This is due to the significant decrease in circulator speed during the initial shutdown heat removal operations. The actual extent of the affect on main loop shutdown cooling, following a failure of the reactor plant cooling water supply is not precisely known, however, the time period before main loop failure occurs should be significantly long enough to allow for either remedial action on the cooling water supply, or an orderly transfer to the CACS.

The instrument air system provides clean, dry air for essential valve and control system operations. The system is equipped with air accumulator tanks which can supply all essential instrument air needs for about five minutes following failure of all the compressors.

These essential operations include closing the CT large CV's and any containment isolation valves as required by the plant protection system. However, the operation of the CT small CV's requires a continuous supply of instrument air. The accumulator air supply was assumed sufficient to initially throttle the CT small CV's, but main loop operation was limited to a maximum of 15 minutes operation before steam generator inventory depletion occurred due to incomplete throttling of the CT small CV's.

The service water system provides the ultimate heat rejection for a number of systems. The most important of these are the reactor plant cooling water system and the instrument and service air compressor jacket cooling system. Thus, failure of the service water system will eventually eliminate these two other systems, but on a longer time scale. The time scale for main loop failure will be determined by the failure of the instrument and service air compressors due to the loss of the jacket water coolant circulation. The time-scale for this failure was assumed to be on the order of 15 minutes, thus allowing a maximum of 30 minutes of main loop shutdown cooling operation.

There are some potential serious service water system dependencies which need to be discussed, but which have not been included in the modelling because it is assumed that they will be eliminated in the final demonstration plant design. These are the cooling water requirements for the emergency diesel generators and the auxiliary circulator motor units. The diesel generators require a jacket cooling water system to maintain appropriate cylinder wall temperatures, and the auxiliary circulator motor units require both stator cooling systems and bearing cooling units. To supply these cooling requirements with the service water system unnecessarily couples both the main loop cooling system and the CACS. A number of potential solutions to this problem have been suggested.[3] For the emergency diesel generators, the most practical solution would appear to be individual shaft-driven, circulating water pumps with natural or forced draft air heat exchangers. For the CACS, individual auxiliary circulator motor and bearing cooling water systems may be necessary, or it may be possible to simply direct cooling water from the core auxiliary cooling water system.

4.2-4 Initiating Events Commonly Degrading the Performance of Both Shutdown Cooling Systems

This last category of initiating events contains three specific subcategories. Figure 4.3 is the block diagram modelling for these events, and Table 4-IV lists the most typical events associated with each subcategory.

Subcategory A includes external events which can potentially affect both the main loop cooling system and the CACS. These events may be earthquakes, tornadoes, floods, aircraft impacts, or other similar events. Some of these events are discussed specifically below.

Earthquakes:

Commercial nuclear power plants must be designed to safely withstand the effects of the largest magnitude earthquake which may be expected based upon geological and historical evidence of the site and its surrounding area. This earthquake is designated the safe shutdown earthquake (SSE). The engineered safety systems required to safely shutdown the plant must be designed to withstand the stresses created by the ground motion of this earthquake and still remain operable. In addition, the plant must be able to remain in a safe operating condition during an earthquake which produces ground accelerations no smaller than half that of the SSE. This earthquake is designated the operating basis earthquake (OBE).

The Reactor Safety Study[4] gives an estimated proba-

Figure 4.3

Initiating Events Degrading the Performance of Both Shutdown Cooling Systems

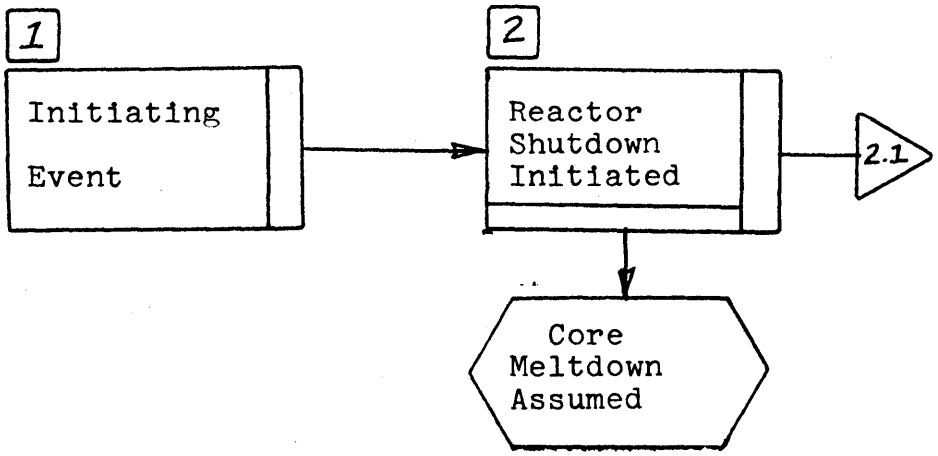


Table 4-IV

Initiating Events Commonly Degrading the Performance of Both Shutdown Cooling Systems (Initiating Event Category III)

Subcategory A. External Events

- o Earthquakes
- o Tornadoes
- o Floods
- o Aircraft Impact

Subcategory B. Internal Events

- o PCRV Depressurization Accidents
- o Core Flow Blockages
- o Internally Generated Missiles

Subcategory C. Support System Failures

- o Loss of Offsite Power Following a Reactor Trip

bility range of 10^{-4} to 10^{-6} per year of an earthquake producing 0.2 g ground acceleration for sites in the eastern U.S. This is roughly the SSE for many of the nuclear power plants in the eastern U.S., and the RSS further estimated that, based on an analysis of the seismic design of safety systems, the probability of survival of a system without mishap would be greater than 0.9.

It is reasonable to assume that the seismic design of GCFR subsystems will be at least as good as that for LWR systems. The likelihood of an SSE causing system failures leading to a core meltdown in the GCFR should be less than 0.01. The probability of a core meltdown due to the occurrence of an SSE is then in the range of 10^{-6} to 10^{-8} per year.

Were the GCFR to be located in a region of known seismic activity, it would be required to be designed to withstand larger magnitude earthquakes. For some regions of California, the SSE design acceleration may be as high as 0.67 g. The likelihood of an earthquake of this magnitude is low even for these regions, and the contribution to the probability of a core meltdown due to the occurrence of an SSE should be in about the same range as for less seismically active regions.

Tornadoes:

The GCFR, as with other U.S. nuclear power plants,

will be designed to withstand the effects of sizeable tornadoes. The typical design basis tornado for most of the U.S. is assumed to have wind speeds of 300 m.p.h. and a velocity of 60 m.p.h. All vital reactor systems must not only be designed to withstand the wind forces and pressure loadings due to the tornado, but they must also be protected from any missiles generated by the tornado. The probability of such a tornado striking a U.S. nuclear power plant was calculated to be less than 5×10^{-6} per year. (4)

Those structures in the GCFR considered to be most vulnerable to tornado effects are the auxiliary loop forced-air coolers and the service water system cooling towers. The auxiliary loop forced-air coolers are located in separate, shielded enclosures on the roof of the Reactor Auxiliary Building. These will be specifically designed as engineered safety features, and they will be required to withstand the effects of the design basis tornado. The likelihood of all the coolers failing due to tornado effects was felt to be less than 0.01. The service water cooling towers will also be designed to withstand tornado effects, however, their failure will only affect the main loop cooling system, and not the CACS performance.

The diesel generator building was also investigated with regard to possible tornado damage, and it is the author's opinion that adequate consideration has been taken in regard to potential missile damage to both the doors and the air intake vents.

The probability of a core meltdown initiated by a tornado is therefore considered to be quite small in comparison to other potential core melt accidents.

Other Events:

Events such as floods, aircraft impacts, turbine missiles and other events were considered in the RSS. All of these events were assessed, for light water reactors, to have a negligible contribution to the probability of a core meltdown. The impact of these events on a GCFR should be basically the same and it is reasonable to assume that they will also be negligible contributors to the probability of a core meltdown for the GCFR.

Subcategory B includes those events internal to the plant which can degrade the main loop and CACS performance. These events may involve the primary coolant circuit shared by the two cooling systems, their common function of circulating helium through the reactor core, or their common location within the PCRV and reactor containment. Specific events would be a PCRV depressurization accident, a severe core flow blockage, or damage due to internally generated missiles.

The reactor shutdown cooling operations following a PCRV depressurization accident were modelled in detail. The likelihood of such an accident will, in general, depend upon the size and location of the postulated PCRV failure.

Penetration closures are generally felt to be the weakest part of the PCRV structure, and Table 3-X listed the potential leak areas for the PCRV penetrations. Failure of either the central cavity closure or one of the steam generator cavity closures leads to the largest leak areas. However, these closures are fixed in place with two independent and redundant means of hold-down, and they are not removed except for major equipment repairs. The reliability of these closures should then approach that of a pressure vessel. The probability of failure of one of these major penetration closures was assumed to be less than 10^{-6} per year. This is the upper limit of pressure vessel failures probability given in the RSS. For the many smaller PCRV penetrations, such as the fuel handling penetration closures, the probability of failure was assumed to be in the range of 10^{-3} to 10^{-4} per year. This is equivalent to the probability of pipe ruptures leading to a small loss of coolant accident in an LWR given in the RSS. The large penetration closure failure was assumed to occur in the steam generator cavity closure, and due to uncertainty concerning the operation of the helium circulator located in the closure, that main cooling loop was conservatively assumed to be eliminated. This leads to a reactor shutdown with only two main loops initially available.

Core flow blockages resulting in gross core meltdown were judged to be extremely unlikely. Local flow blockages leading to melting of one or two sub-assemblies may be possible, however these were also judged to be extremely unlikely. If a local flow blockage were to occur, the initiation of fuel

damage would trigger a reactor shutdown. Even in the event that a shutdown was not initiated, present analyses [5] show that propagation of any fuel damage would be very unlikely. The melting of a few fuel assemblies while a serious enough event was not considered in the same class as gross core meltdown events.

The important GCFR safety equipment will be required to be adequately shielded from both internally and externally generated missiles. Considering this fact the physical separation of the important subsystem equipment, the potential damage due to missiles was assumed to be an insignificant contributor leading to core meltdown.

Subcategory C initiating events are possible failures of support systems which are common to both the main loop cooling system and the CACS. In section 4.2-3, the potential service water dependencies were discussed, and some possible solutions were outlined. It was assumed that knowledge of this potential common mode failure will allow it to be completely eliminated from the final design. The instrument air system is potentially another means of common mode failure of the main loops and CACS. The design of the auxiliary circulator support systems is not yet detailed enough to determine if instrument air requirements are necessary. However, there is no apparent reason why these requirements cannot either be eliminated or the equipment designed to "fail-safe" upon loss of instrument air.

The system which does tie the main loops and CACS togegether is the emergency electrical supply. Those initiating events which result in a simultaneous loss of offsite power and turbine trip require that both the main cooling loop and the CACS performance be dependent upon either proper operation of their corresponding diesel generators or the restoration of offsite power. A loss of offsite power may actually occur in two different ways. The loss of the plant offsite power source and external load will result in a turbine trip and forced reactor shutdown if the turbine load-reject mechanism fails to prevent the turbine trip. Alternatively, the turbine trip which accompanies any forced reactor shutdown may cause a transient in the electrical network which, if it exceeds the stability limit of the grid, will result in the loss of offsite power.

The probability of an interruption in the plant offsite power supply and external load is 0.1 per year.[6] The failure probability of the turbine load-reject mechanism was assumed to be 0.1 per demand. Therefore, the probability that this event leads to a forced reactor shutdown is 1×10^{-2} per year. The probability that a turbine trip would result in the loss of the electrical network was determined to be 10^{-3} per event for a 1000 MW(e) plant.[7] The 300 MW(e) GCFR will have less of an impact on the stability of an electrical network, and therefore such an event was not considered to be an important contributor to this initiating event.

4.3 ESD Computer Calculations

4.3-1 Introduction

Two computer codes were developed to perform the calculations of the accident sequence probabilities. One code performed the calculation of the event sequence probabilities modelled in the ESD for the pressurized reactors shutdowns, and the other code performed the same function for the depressurized accident sequences. Each of these codes performed four specific operations:

1) the calculation of the individual accident sequence probabilities,
2) the grouping of the individual accident sequences into the appropriate outcome categories, and the required bookkeeping to allow proper identification of each accident sequence,
3) the ordering of the individual accident sequence within each outcome category (in a descending array according to the accident sequence probabilities), and calculating the sum of the accident sequence probabilities for each outcome category and for all of the system failure outcome categories, and
4) the sequencing of the input variables in a predetermined fashion for use in the sensitivity analyses.

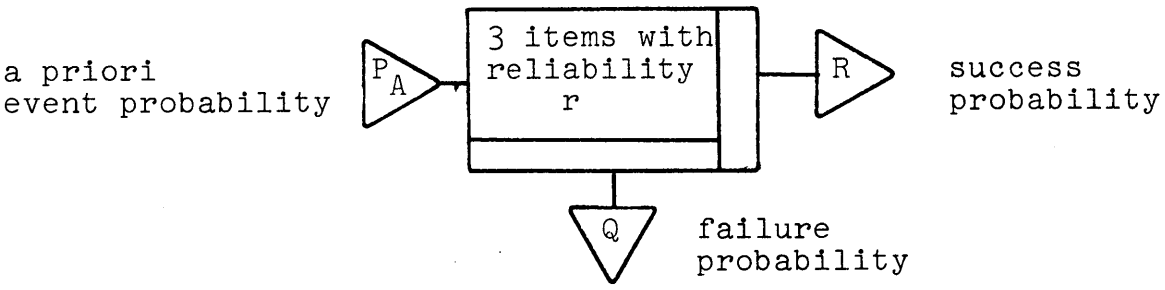
These codes are on file in the M.I.T Nuclear Engineering Department computer library.

This section includes a description of how the ESD's were converted into probability equations for the computer calculations. It also includes a short discussion of the failure data used in this study.

4.3-2 Calculation of the Individual Accident Sequence Probabilities

The modelling of the ESD's was used directly to create the probability equations for the computer calculations. For this transformation, the ESD symbology corresponds to specific probabilistic operators. These are described below.

System Action Block



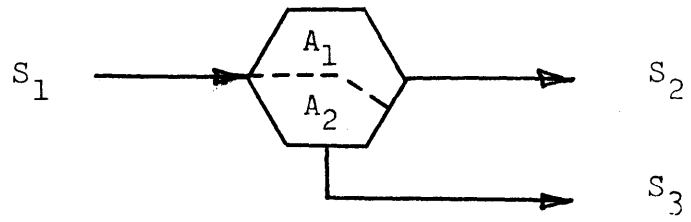
The system action blocks essentially correspond to the conditional probability of a specific operating mode of a system. The inputs to the block are the conditioning events for the individual system reliability value, and each block performs a specific operation on this value, which along with the probability of the conditioning event, gives the success and failure probability outputs for the block. For example, given the a priori event with probability P_A, the individual

items of a system may have a reliability of r . If the number of items in the system is three, then the probability that all three items function correctly, given the initiating event is

$$R = P_A \cdot r^3 \quad ,$$ and the probability of less than three functioning is

$$Q = P_A(1 - r^3) \quad .$$

Branch Point



Branch points correspond to the specific states of availability of a particular system. The values pertaining to each hexagon are also conditional probabilities, and the sum of these probabilities must always be unity. The numbers located in each hexagon are the variable names of the conditional output states for the particular system, and those variables which correspond to "success" or "failure" are conditioned further by the events preceding the branch point. For example, if the event sequence probability preceeding the branch point is S_1, and the availability and unavailability for system A, given that particular event path, are respectively A_1 and A_2, then

two event paths are now created leaving the branch point. These are

$$S_2 = S_1 \cdot A_1 \quad , \qquad \text{and} \qquad S_3 = S_1 \cdot A_2 \quad .$$

S_2 and S_3 are separate event paths which differ only by the availability of system A.

These two symbols along with the transfer triangle comprise the entire ESD's. The subsystem names and event sequence names in the ESD correspond directly to the variable names and event sequence names used in the computer codes. For example, the reliability input for subsystem 4, the CT large CV, is P(4), and the output from the system action blocks for this subsystem (4.1, 4.2 etc.) is labeled PR4(1), PR4(2), etc. In the same way, the final event sequences K1, etc., are labeled PRK(1), etc.

4.3-3 Intra-System Common Mode Failures

In the GCFR, redundancy in threes runs throughout the design. The essential electrical supply, the main loop cooling system, and the CACS all consist of three independent items. If complete independence of the individual system items is assumed, then the reliability of the system is greatly increased over the reliability of the single item. Experience, however, has shown that despite attempts to design completely independent redundant units, failure modes occur which violate the goal of independent failures.[7]

In general, these types of dependent failures are known

as common mode failures, but to distinguish these dependent failures of identical redundant items of a single subsystem from other types of common mode failures (such as those occurring between otherwise unrelated subsystems), the term intrasystem common mode failures will be used. Examples of some mechanisms which can result in these intra-system common mode failures are: undetected design errors, manufacturing or installation related errors, maintenance or operator errors, and failures caused by the failure of unrelated equipment or by unforseen environmental effects.

In order to prevent serious overestimation of the subsystem reliability values through the assumption of independent failures, a method of considering intra-system common mode failures was incorporated into the ESD computer codes. The logic of this method is described by Figures 4.4 and 4.5.

Independent, random failures of three items of a single subsystem can be described by a three trial Bernoulli process,[8] where the probability of success of a single trial (the reliability of a single item of the redundant system) is p. The probability of exactly k successes in the system is then described by the equation

$$P(k) = \frac{3!}{k!(3 - k)!} p^k (1 - p)^{3-k}$$

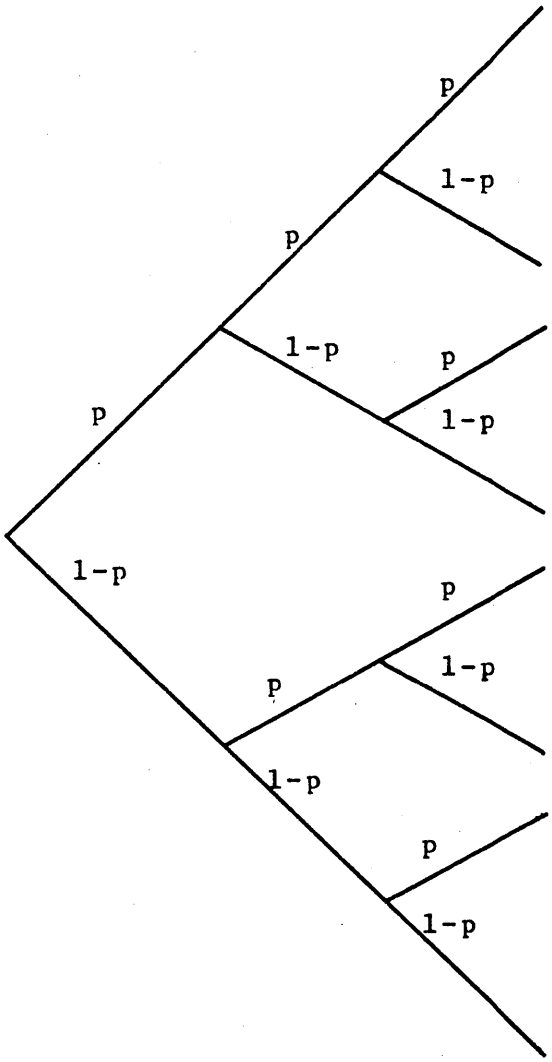
which is a binomial probability distribution function. This is graphically shown by the logic tree of Figure 4.4.

In order to include common mode failures, it was assumed

Figure 4.4

A Logic Diagram of Subsystem Availability States

with Random Failures of 3 Identical Items



No. Of Items Available	Probability Of Availability State
3	p^3
2	$p^2(1-p)$
2	$p^2(1-p)$
1	$p(1-p)^2$
2	$p^2(1-p)$
1	$p(1-p)^2$
1	$p(1-p)^2$
0	$(1-P)^3$

p = Individual system or component reliability

that the subsystems have two separate failure modes, either independent or common mode. The common mode failure probability is defined by z, and the logic tree can be modified as is shown in Figure 4.5. Essentially, if a common mode failure does not occur (probability 1-z), then independent, random failures can occur. The probability of success of exactly k items is then given by

$$P(k) = \frac{3!}{k!\ (3-k)!} p^k (1-p)^{3-k} (1-z)$$

where k = 3, 2, or 1, and for k = 0 by

$$P(0) = (1-p)^3\ (1-z) + z$$

A value of z for each redundant subsystem was then included in the computer calculation of the accident sequence probabilities.

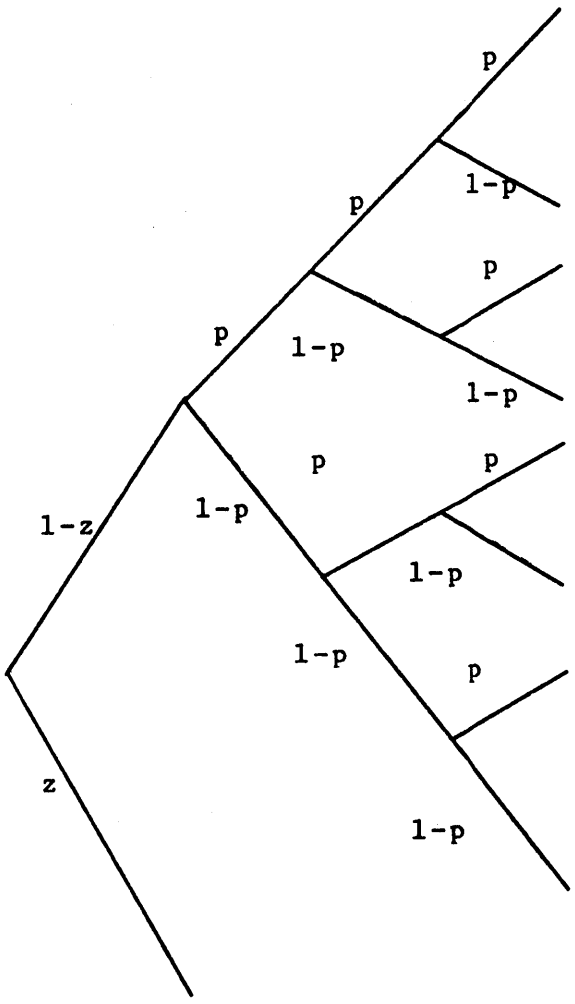
This same line of reasoning was followed independently by Fleming [9] in which a term β (the beta factor) was defined as the fraction of total unit failures which were common mode. Fleming used the beta factor to determine the common mode failure probability of redundant components. However, the concept can also be applied to redundant units (containing a number of components) of a particular subsystem. The common mode failure probability is then the probability of a single unit failure times the fraction of those failures which are common mode.

$$z = \beta\ (1-p)$$

This equation is a convenient method of determing the common mode failure probability. However, it is based upon an emperical relationship and not any fundamental understanding of common mode failures. Fleming applies the beta factor only at the component

Figure 4.5

A Logic Diagram of Subsystem Availability States With Random and Common Mode Failures of Three Identical Items



No. Of Items Available	Probability Of Availability State
3	$p^3(1-z)$
2	$p^2(1-p)(1-z)$
2	$p^2(1-p)(1-z)$
1	$p(1-p)^2(1-z)$
2	$p^2(1-p)(1-z)$
1	$p(1-p)^2(1-z)$
1	$p(1-p)^2(1-z)$
0	$(1-p)^3(1-z)$
0	z

p = Individual System or Component Reliability
z = Probability of a Common Mode Failure

level where failure data is generally applicable on a generic basis. In applying this relationship to the system level, caution must be used. Specifically, in this application to the GCFR subsystem, neither any possible functional relationships between β and p, nor the possible effects of design on the value of β are known. Therefore, β is presently assumed to be a constant with a sufficiently conversative value.

4.3-4 Equipment Unavailabilities Due to Test or Maintenance

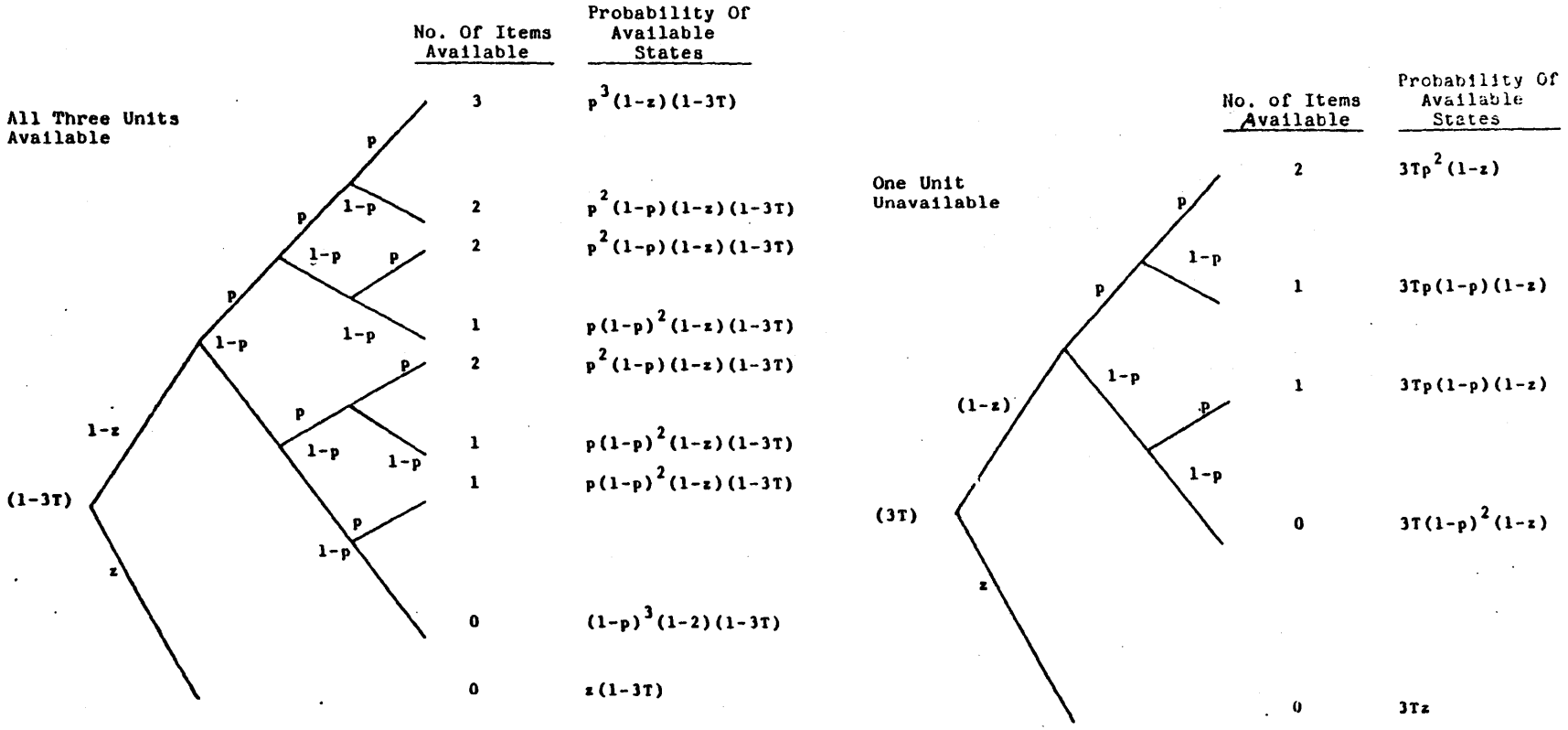
In redundant systems, the unavailability of one unit for either test or maintenance purposes may have a significant effect on the reliability of the subsystem. Assuming that the probability of one unit of a redundant system being unavailable at the time its operation is required is T and that only one unit of the system will be undergoing maintenance at any one time, then for a three unit system, the probability equations for successful operation of a given number of units become

$$P(3) = p^3(1 - z)\ (1 - 3T)$$
$$P(2) = 3p^2(1 - p)(1 - z)(1 - 3T) + 3Tp^2(1 - z)$$
$$P(1) = 3p(1 - p)^2(1 - z)(1 - 3T) + 6Tp(1 - p)(1 - z)$$
$$P(0) = (1 - p)^3(1 - z)(1 - 3T) + 3T(1 - p)^2(1 - z) + z$$

Given all three units are available (probability 1 - 3T), the system availability states are determined by the random failures of three items and the common mode failure probability. Given any one of the three units is unavailable (probability 3T), the system availability states are determined by the random failure of two items and the common mode failure probability. Figure 4.6 shows the logic diagrams for this situation.

Figure 4.6

Logic Diagrams of the Subsystem Availability States With Random Failures, Common Mode Failures, and Test and Maintenance Unavailability for Three Identical Items



p = Individual System or Component Reliability
z = Probability of a Common Mode Failure
T = Probability of One Unit Being Unavailable

In a situation in which only two items of the system are available for operation due to the previous failure of a related system, the probability of the system availability states are given by

$$P(2) = p^2(1 - z)(1 - 2T)$$

$$P(1) = 2p(1 - p)(1 - z)(1 - 2T) + 2TP$$

$$P(0) = (1 - p)^2(1 - z)(1 - 2T) + 2T(1 - p) + z(1-2T).$$

An example of this situation is the availability of the shutdown feedwater loops which, during a loss of offsite power, are dependent upon correct operation of their corresponding emergency diesel generator. If one diesel fails then only two shutdown feedpumps are available to start.

In these equations, the probability of a common mode failure is assumed to be the same whether two units or three units are available. This may be a conservative assumption, however there is not yet enough quantitative information concerning common mode failures to justify treating these potential common mode failure situations differently.

The above equations assume that only one redundant unit of a system may be unavailable at any one time without shutting down the reactor. During the construction of the ESD, the assumption was also made that test or maintenance would not be performed simultaneously on more than one main loop subsystem

if the units which would be unavailable corresponded to different shutdown cooling loops. For example, maintenance would not be performed simultaneously on both shutdown feed pump A and auxiliary boiler B.

4.3-5 Failure Data

In this study, three contributions to the subsystem failure probabilities were considered. These are hardware failures, test and maintenance equipment unavailabilities, and common mode failure contributions.

Generic component failure data from Appendix III of WASH-1400[7], the RSS, was employed for the hardware failure contributions. This data base includes U. S. nuclear power plant operating experience and equipment failure data from other related industries. The data should therefore be applicable to similar GCFR components. Table 4-V lists the median failure probabilities and the error factor for both mechanical and electrical components. The error factor represents the uncertainty in the data, and it is the ratio of the upper bound to the median failure probabilities.

Equipment outages for either test or maintenance purposes can have a significant effect on the subsystem failure probability. At present, test and maintenance requirements for GCFR subsystems are unknown. Therefore, equipment unavailabilities were considered on a generic basis, and maintenance acts were felt to be the major contributor to these unavailabilities.

Table 4-V

Basic Failure Data

MECHANICAL COMPONENTS			
DEVICE	FAILURE MODE	MEDIAN FAILURE PROBABILITY *	ERROR FACTOR
Air-Operated Valve	Failure to operate	3×10^{-4}/d	3
	Failure to remain open	1×10^{-4}/d	3
Motor-Operated Valve	Failure to operate	1×10^{-3}/d	3
	Failure to remain open	1×10^{-4}/d	3
Manuel Valve	Failure to operate	1×10^{-4}/d	3
Check Valve	Failure to open	1×10^{-4}/d	3
Relief Valve	Failure to open	1×10^{-5}/d	3
	Open Prematurely	1×10^{-5}/hr	3
Valve(general)†	Failure to remain open	1×10^{-6}/hr	10
Pump	Failure to start	1×10^{-3}/d	3
	Failure to run given start	3×10^{-5}/hr	10
Diesel System	Failure to start	3×10^{-2}/d	3
	Failure to run given start	3×10^{-3}/hr	3

* /d indicates probability per demand
/hr indicates probability per hour

† Not taken from WASH-1400

Table 4-V cont.

ELECTRICAL COMPONENTS			
DEVICE	FAILURE MODE	MEDIAN FAILURE PROBABILITY *	ERROR FACTOR
Motors	Failure to start	3×10^{-4}/d	3
	Failure to run given start	1×10^{-5}/hr	3
Circuit breakers	Failure to operate	1×10^{-3}/d	3
	Premature open	1×10^{-6}/hr	3
Pressure switch	Failure to operate	1×10^{-4}/d	3
Transformer	Opens or Shorts	1×10^{-6}/hr	10
Solid State Device	Failure to function	3×10^{-6}/hr	3
Battery Power Supply	Failure of proper output	3×10^{-6}/hr	3
Simple Control† System (1)	Failure to operate	1×10^{-3}/d 3×10^{-6}/hr	10 10
Complex Control† System (2)	Failure to operate	3×10^{-3}/d 1×10^{-5}/hr	10 10

* /d indicates probability per demand
/hr indicates probability per hour

(1) Performs a simple "on-off" function
(2) Performs a continuous control function

† Not taken from WASH-1400

Table 4-VI

Basic Component Unavailabilities

Component	Average Unavailability
Pumps	2×10^{-3}
Valves	2×10^{-3}
Diesels	6×10^{-3}
Instrumentation	2×10^{-3}

Table 4-VI lists these generic equipment unavailabilities, which are taken from Reference 7, page 118.

These unavailability values were applied to the major components of those subsystems which are not functioning during normal reactor operation. For each of these subsystems, only one of the redundant units was assumed to be down for test or maintenance purposes at any one time while the reactor was operating.

The probability of an intra-system common mode failure is related to the failure probability of one redundant unit of the subsystem.

$$z = \beta q = \beta (1 - p)$$

where z is the probability of an intra-system common mode failure,

q is the failure rate of one unit of the subsystem, and

β, the beta factor, is the fraction of total unit failures which are common mode failures.

In order to determine an estimate of the likely range of the beta factor for the GCFR subsystems, two types of data were investigated. The first was component failure data in which the fraction of multiple component failures for each component type was calculated. These results are shown in Table 4-VII.

The second type of data was the actual common mode failure contributions to system failure calculated in WASH-1400[10]

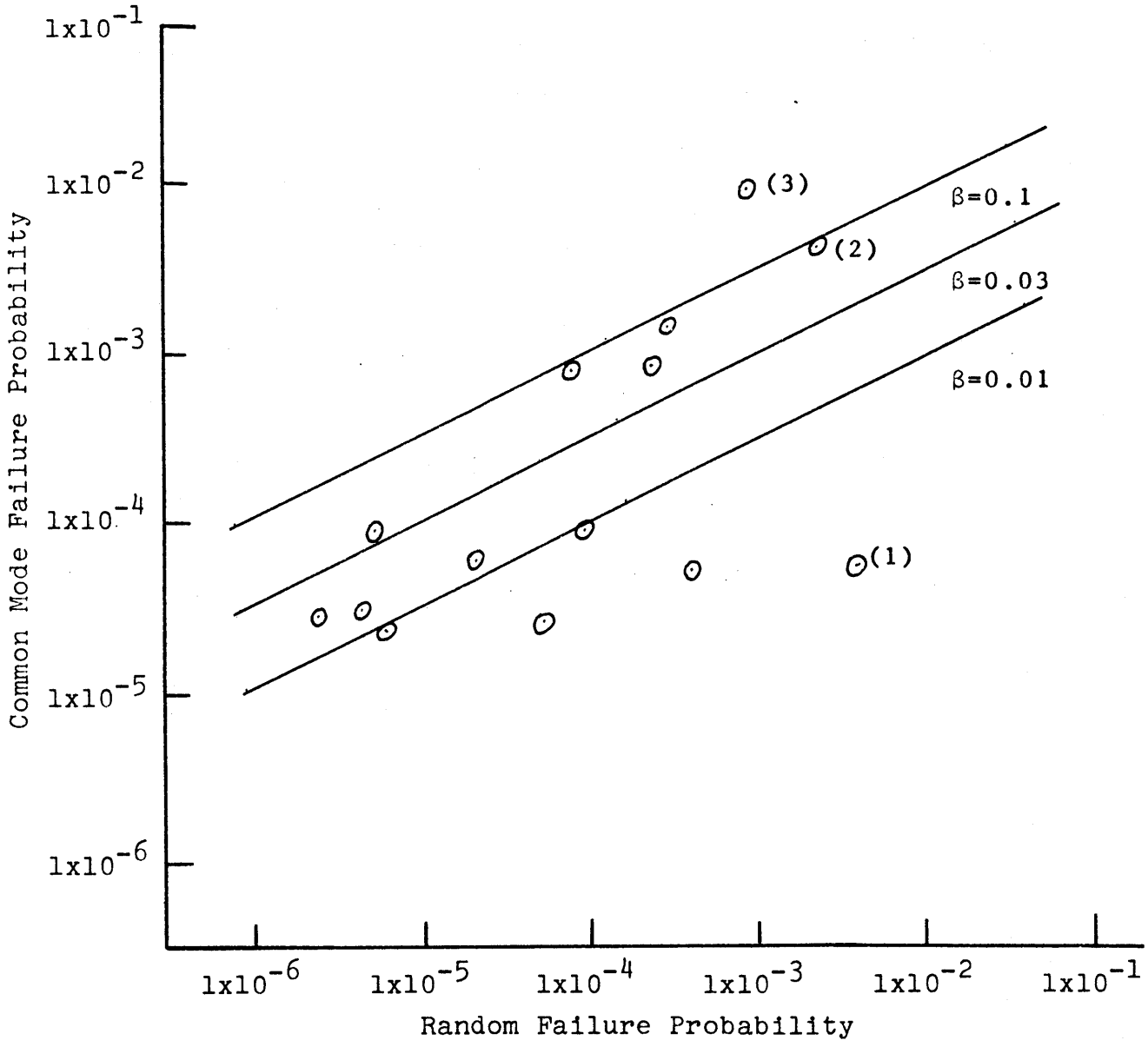
These common mode failure contributions are

Table 4-VII

Common Mode Failure Fractions

From Component Failure Data

Component	Number of Total Failures	Number of Common Mode Failures	Fraction of Common Mode Failures (β)
Pumps (Ref. 4)	24	0	.042
Valves (Ref. 4)	102	6	.059
Diesel Systems (Ref. 11)	87	5	.058
Instrumentation (Refs. 4,12)	203	28	.138



(1) Single failures dominate failure probability
(2) Double failures domonate random failure probability
(3) Diesel generator failure for one specific event (see text)

(From Tables II-1 and II-2, Reference 10)

Figure 4.7 A Plot of LWR Subsystem Common Mode Failure Contributions Versus the Total Random Failure Contributions

plotted as a function of the total random failure probability in Figure 4.7. Also shown on the figure are solid lines corresponding to beta factors, for a doubly redundant system, of 0.1, 0.03 and 0.1. Notice that the majority of the points lie between beta values of 0.01 and 0.1. This is also the range suggested by the component failure data. The only point significantly greater than 0.1 concerns failure of the diesel generators following a simultaneous loss of coolant accident and loss of offsite power for the PWR analyzed in the RSS. The potential common mode failure results from the inrush of current due to essential electrical loads which must be assumed upon starting. The likelihood that a common mode failure results is greater for the PWR due to the larger essential electrical loads required in this event. The beta factor for the diesel system of the BWR analyzed in the RSS is 0.03 for this event. In the GCFR demonstration plant design, the diesel generators are not required to assume large loads upon starting due to the capability of initially continuing main loop operation independent of the electrical supply. Therefore, this potential common mode failure should not be of significant concern.

None of this data was considered to be specific enough to apply to individual GCFR subsystems, however, it was felt to adequately establish a general range for the beta factor. This range was 0.01 to 0.1 and it was assumed to be the same for all

GCFR subsystems. Assuming a log-normal distribution for the beta factor range, the median beta factor value is 0.03. This median value was used for all the GCFR subsystems.

It needs to be emphasized, that most of the common mode failure data available pertains to doubly redundant systems. Because there is no evidence to the contrary, it was assumed that those common mode failures leading to the failure of both items of a doubly redundant system would also lead to the failure of all items of a triply redundant system. Thus the beta factors are taken to be the same. However, this may very well not be true; especially if potential common mode failures are given serious attention in the design of the system. Consider some potential common mode failure causes:

1) Maintenance related failures. The majority of common mode failures calculated in the RSS were due to human maintenance errors. For example, following test or maintenance, valves on all redundant units of a system are placed in a failed condition. For this type of event, if the failure is repeated twice, it will be most likely to be repeated three times. However, as the number of redundant units increases, it is less likely that a single person is responsible for work on all of the units. This reduces the likelihood of this type of common mode failure. Also, staggered test and maintenance schedules for redundant equipment also reduce this common mode failure possibility.

2) Design and Equipment related failures. It seems unlikely that design errors leading to common mode failures would have less of an impact in triply redundant systems. Certain types of equipment

failures would, however, tend to be less significant as the number of redundant items increases. For example, a common manufacturing defect can lead to premature failure of a certain piece of equipment. The greater the number of items, the less likely it is that a simultaneous (or near simutaneous) failure will occur.

3) Environment related failures. Greater physical separation is possible in a triply redundant system, and common mode failure of the system may be less likely for certain environmental effects. However, this is clearly dependent on the specific system involved, and no general judgment can be made.

4.4 Shutdown Event Sequence Analysis Variables

4.4-1 Introduction

In this section, the input variables to the ESD computer codes are presented. These essentially consist of 1) the subsystem unit reliability values, 2) the intra-system common mode failure values as determined by the beta factor, and 3) the probability values for the other occurrences modelled in the ESDs. These inputs are summarized in the following section, and a brief description of each of the inputs is included in the last section. A more detailed discussion of these items is included in Appendix A.

4.4-2 Summary of ESD Inputs

The eight major GCFR subsystems involved in the shutdown cooling and decay heat romoval operations each have three input variables. The first of the values is the reliability of one unit of these three-independent-unit subsystems. This is refered to as the subsystem unit reliability value. These values are median point estimates, and they are the compliment of the subsystem unit failure probabilities developed in Appendix A using the failure data presented in Section 4.3-5. The values are presented in Table 4-VIII along with the reliability ranges for each subsystem that were used in the sensitivity analysis. These sensitivity ranges correspond roughly to one order of magnitude changes in the subsystem unit failure probability on either side of the median value. For example, the median reliability value of .9987 for the CT large CV corresponds to a median point estimate of the failure probability of 1.3×10^{-3} per demand. The sensitivity range of .99 to .9999 corresponds to a failure probability range of 1×10^{-2} to 1×10^{-4} per demand.

The second input variable is the beta factor for the subsystem. The beta factor relates the common mode failure probability and the subsystem unit reliability value by the following equation.

$$z = \beta(1 - p)$$

The median value of the beta factor assumed for each subsystem are also listed in Table 4-VIII.

Table 4-VIII

GCFR Subsystem Unit Reliability

Values and Beta Factors

Subsystem Index and Name	Subsystem Unit Reliability		Common Mode Failure Fraction (Beta Factor)	
	Median Value	Range for Sensitivity Analysis	Median Value	Range
4: CT Large CV's	.9987	.99 - .9999	0.03	0.01-0.1
5: CT Small CV's	.9967	.97 - .9997	0.03	0.01-0.1
6: Shutdown Feedwater System	.9974	.96 - .9996	0.03	0.01-0.1
7: Auxiliary Boilers	.9919	.875- .999	0.03	0.01-0.1
8: Main Loop Decay Heat Removal Operation	.9938	.93 - .9993	0.03	0.01-0.1
9: Emergency Electrical Supply	.97	.9 - .997	0.03	0.01-0.1
10: Core Auxiliary Cooling System	.9917	.9 - .999	0.03	0.01-0.1
12: Resuperheater Bypass control Valves	.9986	.99 - .9999	0.03	0.01-0.1

The unavailabilities for each unit of those subsystems not functioning during normal full-power operation are listed in Table 4-IX. These are based upon the average component unavailabilities presented in Section 4.3-5. No sensitivity range is listed for these unavailability values. In the sensitivity analysis, the total contribution to the probability of core meltdown of the test and maintenance unavailabilities was investigated.

Table 4-X lists the median reliability values and the sensitivity range assumed for main loop isolation value operations and for main circulator performance during and following circulator-turbine imbalance conditions.

Table 4-XI lists the nominal probability values and the sensitivity range assumed for the restarting of initially failed shutdown feed pumps and emergency diesel generators.

Table 4-XII lists the upper and lower bounds assumed for the probability of a main loop support system failure leading to a main loop cooling system failure following a reactor shutdown. Note that for failures of the service water system leading to main loop failures in the 15 to 30 minute time interval, the values .333 and .667 are artificial failure probabilities. They are not the probabilities of system failure; they are the probabilities of failing to successfully combine the available essential buses with the operating service water system components. A more complete discussion of these values is included in Appendix A.

Table 4-IX

Subsystem Test and Maintenance Unavailabilities

Subsystem Index and Name	Test and Maintenance Unavailability
6: Shutdown Feedwater Loop	4×10^{-3}
7: Auxiliary Boiler	1.2×10^{-2}
8: Main Loop Transfer to Decay Heat Removal Operation	4×10^{-3}
9: Emergency Diesel Generator Set	6×10^{-3}
10: Core Auxiliary Cooling Loop	1.2×10^{-2}
12: Resuperheater Bypass Control Valve	2×10^{-3}

Table 4-X

Main Loop Isolation Valve Operating Reliability and Main Circulator Reliability During and Following Circulator-Turbine Imbalance Conditions

Main Loop Isolation Valve and Circulator Operation	Median Reliability Value	Sensitivity Range
P18: Main Loop Isolation Valve Closes due to a Circulator Imbalance Condition Caused by a failed		
CT Large CV	.995	.9995 - .95
CT Small CV	.975	.999 - .9
P17: Main Loop Isolation Valve Opens Following a Circulator Imbalance Condition	.999	.9999 - .99
P17: Main Circulator Remains Operable Following an Imbalance Condition (with loop isolation valve open) Caused by a Failed		
CT Large CV	.50	.95 - .10
CT Small CV	.95	.995 - .75

Table 4-XI

Probability Values for Restarting Initially Failed Shutdown Feedpumps and Emergency Diesel Generators

P16: Restoration of Initially Failed Feedpumps or Diesels	Nominal Values	Sensitivity Range
Given at least 15 minutes:		
Start 1 of 3 failed feedpumps	0.0	1.0 - .75 - .25
Start 1 of 2 failed feedpumps	0.0	1.0 - .60 - .20
start 1 of 1 failed feedpump	0.0	1.0 - .30 - .10
Given at least 10 minutes:		
Start 1 Of 3 failed diesels	0.0	1.0 - .75 - .25
Start 1 of 2 failed diesels	0.0	1.0 - .60 - .20
Start 1 of 1 failed diesel	0.0	1.0 - .30 - .10
Feedpump associated with a restarted diesel starts	.99	-------

Table 4-XII

Probability of a Main Loop Support System Failure
Leading to a Main Loop Failure Following a Reactor Shutdown

P19: Main Loop Support System Failure	Main Loop Failure in the Interval 5 to 15 Minutes Following Shutdown		Main Loop Failure in the Interval 15 to 30 Minutes Following Shutdown	
	Lower Bound	Upper Bound	Lower Bound	Upper Bound
3 Buses Energized	$1x10^{-7}$	$1x10^{-5}$	$1x10^{-5}$	$1x10^{-3}$
2 Buses Energized	$1x10^{-6}$	$1x10^{-4}$	$1x10^{-3}$	.333
1 Bus Energized	$1x10^{-4}$	$1x10^{-2}$	.333	.667
	Due to Instrument Air System Failure		Due to Service Water System Failure Leading to Instrument Air Compressor Failure	

Table 4-XIII

Probability of Restoration of Offsite Power

P20: Restoration of Offsite Power	Nominal Values	Sensitivity Range
o Within 30 minutes	.75	1.0 - 0.0
o Within 25 minutes	.70	1.0 - 0.0
o Within 20 minutes	.68	1.0 - 0.0
o Within 15 minutes	.65	1.0 - 0.0
o Within 10 minutes	.60	1.0 - 0.0
o Within 5 minutes	.35	1.0 - 0.0

Table 4-XIV

Probability Inputs for Reactor Shutdowns Following a PCRV Depressurization Accident

	Isolation Valve Reliability		Common Mode Failure Fraction (beta factor)	
	Median	Sensitivity Range	Median	Range
D18: Main Loop Isolation Valve Closes	.999	.99 - .9999	0.03	0.01 - 0.1

P21: Containment Equalization Pressure (CEP) Following a Depressurization Accident	Probability of a Given CEP Range Occuring	
	Nominal Value	Sensitivity Range
CEP 1.50atm.	.999	.9999 - .99
CEP 1.25atm.	$1x10^{-3}$	$1x10^{-4}$ - $1x10^{-2}$

	Nominal Value	Sensitivity Range
P23: Auxiliary Loop Isolation Valve Remains Open on a Failed Auxiliary Loop	$1x10^{-3}$	$1x10^{-4}$ - $1x10^{-2}$

Table 4-XIII lists the probability of restoration of offsite power following a simultaneous reactor trip and loss of offsite power. The nominal values are taken directly from Reference 7, and they were assumed to apply both to the case in which the loss of offsite power is the initiating event, and to the case in which the loss of offsite power is initiated by the turbine trip which accompanies all forced reactor shutdowns.

Table 4-XIV lists those inputs which pertain only to reactor shutdowns following a PCRV depresurization accident. These include the reliability of the main loop isolation valves to close following a loop failure, the probability that the containment equalization pressure is within a given range, and the probability of an auxiliary loop isolation valve failure.

4.4-3 Description of ESD Input Variables

Subsystem 4. The circulator-turbine large control valves

P(4) is the reliability of a circulator-turbine large control valve to close upon receipt of the shutdown initiation signal and the shutdown verification signal.

z(4) is the probability that a common mode failure causes all three valves to fail to close.

Subsystem 5. The circulator-turbine small control valves

P(5) is the reliability of a circulator-turbine small control valve to correctly throttle during

the shutdown heat removal operation.

z(5) is the probability that all three circulator turbine small control valves fail to throttle correctly, during the shutdown heat removal operation, due to a common mode failure.

Subsystem 6. The shutdown feedwater system

P(6) is the reliability of a shutdown feedwater pump to deliver feedwater to its steam generator during the shutdown and decay heat removal operations, given essential electrical power is available.

z(6) is the probability of a common mode failure which eliminates the shutdown feedwater system.

Subsystem 7. The auxiliary boilers

P(7) is the reliability of an auxiliary boiler to start and reach its rated steaming conditions in twenty minutes, given offsite power is available.

z(7) is the probability of a common mode failure which prevents all three boilers from starting or reaching rated conditions within twenty minutes.

Subsystem 8. Main loop transfer to the decay heat removal operating mode.

P(8) is the reliability of a main loop to perform the transfer to the decay heat removal operating mode and to provide long-term decay heat removal, given the auxiliary boiler is available.

z(8) is the probability that a common mode failure

prevents all three main loops from performing this function.

Subsystem 9. The emergency electrical supply

P(9) is the reliability of a single emergency diesel-generator to start and assume load, given the loss of offsite power.

z(9) is the probability of a common mode failure which causes all three diesel-generators to fail to start or to assume load.

Subsystem 10. The core auxiliary cooling system (CACS)

P(10) is the reliability of a single CACS loop to provide core cooling in the event of a main loop cooling system failure.

z(10) is the probability of a common mode failure which eliminates the core cooling capability of the entire CACS.

Subsystem 11. Turbine trip.

P(11) is the reliability of the turbine trip mechanism to close the main turbine throttle valve given a reactor shutdown initiation signal. The closing of the turbine throttle is the initiating signal to the resuperheater bypass control system. A failure in the turbine throttle mechanism which prevents the resuperheater bypass initiation signal is a common mode failure input for the resuperheater bypass system.

As such, it was not directly evaluated; but it was considered to be accounted for in the beta factor valve of Subsystem 12.

Subsystem 12. The resuperheater bypass control valve
P(12) is the reliability of this control valve to open and properly regulate the circulator-turbine exhaust pressure during shutdown and decay heat removal operations.
z(12) is the probability of a common mode failure which causes all three resuperheater bypass control valves to fail to open.

ITEM A. The number of loops in the main loop cooling system initially available to provide shutdown heat removal.
PR1(1) is the probability that all three of the main cooling loops are initially available for shutdown and decay heat removal.
PR1(2) is the probability that only two main cooling loops are initially available for shutdown and decay heat removal. The other loop is assumed to be shutdown and isolated.

ITEM B. The availability of offsite power
PR1(3) is the probability that offsite power is available following the reactor shutdown and turbine trip.

ITEM 20. The restoration of offsite power.

Given that the loss of offsite power either initiates the reactor shutdown, or occurs simultaneously with the shutdown:

P20(1) is the probability that offsite power is restored within 30 minutes after the shutdown.

P20(2) is the probability that offsite power is restored within 25 minutes after the shutdown.

P20(3) is the probability that offsite power is restored within 20 minutes after the shutdown.

P20(4) is the probability that offsite power is restored within 15 minutes after the shutdown.

P20(5) as the probability that offsite power is restored within 10 minutes after the shutdown.

P20(6) is the probability that offsite power is restored within 5 minutes after the shutdown.

In the sensitivity analyses, these valves were varied as a set.

The above list of variables is common to the computer codes of both the pressurized reactor shutdowns and the depressurization accident shutdowns. The following list of variables pertains only to the computer code for the pressurized reactor shutdowns.

ITEM 18. Main loop isolation valve operation: open to shut.

These isolation valve operations are the result of

imbalance forces during the shutdown heat removal operations arising from circulator-turbine control valve failures. (See Appendix A, Section A.17 for a more detailed explanation.).

P18(1) is the probability that a main loop isolation valve will close due to the imbalance force created by the failure of a CT small CV in one of the other loops.

P18(2) is the probability that a main loop isolation valve will close due to the imbalance force created by the failure of a CT large CV in one of the other loops.

ITEM 17. Main loop isolation valve operation: shut to open, and circulator-turbine operability.

These inputs also pertain to the imbalance condition mentioned in ITEM 18.

P17(1) is the probability that a main loop isolation valve in a normally function loop opens after being closed during an imbalance condition. This includes the probability that the circulator-turbine does not fail during the period of operation behind the shut valve.

P17(2) is the probability that a main loop isolation valve, in a loop with a CT small CV failed, opens after being closed due to an imbalance created by the CT large CV in another loop.

This includes the probability that the circulator-turbine does not fail during the period of operation behind the shut valve.

P17(3) is the probability that a circulator-turbine remains operable in a loop in which the isolation valve failed to close during an imbalance condition created by the failure of a CT large CV in one of the other loops.

P17(4) is the probability that a circulator turbine remains operable in a loop in which the isolation value failed to close during an imbalance condition created by the failure of a CT small CV in one of the other loops.

ITEM 16. The restoration of initially failed shutdown feedpumps or diesel generators.

P16(1) is the probability that given three initially failed shutdown feedpumps, one can be started within twenty minutes after the shutdown.

P16(2) is the probability that given two initially failed shutdown feedpumps, that one can be started within twenty minutes after the shutdown.

P16(3) is the probability that a single initially failed shutdown feed pump can be started within twenty minutes after the shutdown.

P16(4) is the probability that a single initially failed emergency diesel generator can be started

within fifteen minutes after the shutdown.

P16(5) with probability that given two initially failed emergency diesel generators, one can be started within fifteen minutes after the shutdown.

P16(6) is the reliability of the shutdown feed pump associated with a restarted diesel generator to deliver feedwater to its steam generator.

P16(7) is the probability that given all three emergency diesel generators have initially failed to start, one can be started within fifteen minutes after the shutdown.

These values were varied as a set in the sensitivity analyses.

The following variables pertain only to the computer code for the depressurized accident sequences.

ITEM D18. Main loop isolation valve operation: open to shut.

DP18 is the reliability of the main loop isolation valve to closes, during the shutdown heat removal operation, after main loop failure occurs.

Dz18 is the probability of a common mode failure that prevents all the main loop isolation valves from closing, given that all the main loops have failed.

ITEM 21. Containment isolation following a depressurization accident.

P21(1) is the probability that the containment equilazation pressure, following a depresurization accident, is greater than 1.50 atmospheres.

P21(2) is the probability that the containment equalization pressure, following a depresurization accident, is less than 1.25 atmospherees.

Chapter 5

Sensitivity Analyses

5.1 Introduction

5.1-1 Contributors to the Accident Probability

This chapter contains the results of the sensitivity analyses performed for each of the initiating event categories. A median valve for the probability of a core meltdown per reactor shutdown was determined for each category, and the sensitivity of this valve to changes in the three contributors to the subsystem failure rate was investigated in detail. The median core-melt probabilities are based on median point calculations, and they were determined utilizing the median subsystem reliability values, the test and maintenance unavailabilities, and the median beta factor value of 0.03. The sensitivity analysis results for each initiating event category are presented according to these three contributors:

1) the sensitivity to the shutdown cooling subsystem reliability values;
2) the sensitivity to the fraction of intra-system common mode failures, the beta factor; and
3) the contribution of the subsystem test and maintenance unavailabilities.

A simplified model of the reactor shutdown cooling operations is also provided as a guide to the basic shutdown cooling event sequences for each initiating event category.

The sensitivity to the subsystem unit reliability values was determined by varying these values between the high and low ends of the sensitivity ranges presented in Table 4-VIII. These sensitivity ranges should not be taken as an indication of the uncertainty in the subsystem unit reliability values. Large sensitivity ranges were specifically chosen for the purpose of determining the variation of the probability of a core meltdown over a wide range of subsystem unit reliability values. Also, the choice of large sensitivity ranges magnified the sensitivity values to allow easier comparison. The results are presented in both tables and plots. The latter allow easy extrapolation of the effect of possible changes in the subsystem unit reliabilities.

The change in the probability of a core meltdown for each initiating event category was investigated for different beta factor values. The beta factor value was assumed to be the same for all subsystems, however, the contribution to the core-melt probability due to common mode failures of the individual subsystems was also calculated.

The overall contribution to the probability of a loss of decay heat removal of equipment unavailabilities for test or maintenance purposes was determined for each reactor shutdown initiating event category. The contribution of the individual subsystem unavailabilities was also determined.

The effect of potential design changes is discussed throughout the chapter, and the effect of changes in the main loop

operating times is discussed in the last section.

5.1-2 Dominant Accident Sequence Inditification Code

For each initiating event category, the dominant accident sequences are presented and discussed. These dominant accident sequences are those with the highest probabilities of occurrence and they constitute the major contributors to the total core meltdown probability for the particular initiating event category.

An identification code was utilized to facilitate the discussion of the dominant accident sequences. In addition to its ESD name, each dominant sequence is identified by a short series of characters which represents the operating state of the main loops and the important failures involved in the accident sequence.

A: This represents a main loop in a fully available operating state. This character is preceeded by a number which indicates how many main loops are fully available. The number 1 is understood in this code.

A main loop failure is represented by the following characters with primes.

L' represents the failure of the CT large CV to close. It also represents failures of the resuperheater bypass control valve to open.

S' represents the failure of the CT small CV to throttle.

F' represents the failure of the shutdown feedwater supply

I' represents the failure of a main loop as the result of a circulator-turbine imbalance condition

X': This represents the failure of the main loop cooling system to provide long term decay heat removal. It includes failure of the auxiliary boilers and failure to transfer the main loops to their auxiliary steam supply.

B': For accident sequences in which offsite power is lost, this represents the failure of the diesel generator for one of the essential buses.

R: This represents offsite power. R denotes offsite power restoration and R' represents failure to restore offsite power. The time interval within which offsite power is either restored or not restored is indicated after the R. For example, R10' is failure to restore offsite power within 10 minutes. R30 is the restoration offsite power within 30 minutes.

SS': This represents a failure in a support system for the main loop cooling system that results in main loop failure.

C: This represents the CACS. C2' and C3' are different CACS failure modes. For pressurized accident sequences, C2' represents failure of two CACS loops in the interval 0 to 15 minutes after the shutdown, and C3' represents the failure of all three of the CACS loops. For depressurization accident sequences, C3' represents failure of the CACS to provide adequate decay heat removal following shutdown.

CP: For depressurized accident sequences only, this represents

the containment equalization pressure (CEP) range.

CP1 signifies CEP > 1.50 atm.

CP2 signifies 1.25 atm. $\leq$ CEP $\leq$ 1.50 atm.

CP3 signifies CEP < 1.25 atm.

A few examples of accident sequences leading to core meltdown are given to familiarize the reader with this identification code.

K3(3A-X'-C3'). For this accident sequence, all three main loops are fully available, but main loop transition to long term decay heat removal fails, and all three of the CACS loops also fail.

CC2(A-2L'-C3'). One main loop is fully available, but two main loops have failed CT large CVs. The failure of the CACS loops ends the sequence. (One main loop cannot operate long enough to allow the auxiliary boilers to start. Therefore, their failure is not included in the identification code.)

N9(A-L'-I'-C2'). For this accident sequence, one main loop is fully available, one main loop has a failed CT large CV, and one main loop has failed due to the circulator-turbine imbalance condition which followed the failure of the CT large CV. Core meltdown occurs due to only one CACS loop operating prior to 15 minutes after the shutdown.

M17(3A-2B'-R30'-C3'). This sequence involves the loss of offsite power. Three main loops are available, but with two diesels failed, two loops have no feedwater. Offsite power

is not restored within the main loop operational period, and the single available CACS loop fails.

L8(3A-B'-R30-C3'). Three main loops are available, and one diesel generator has failed. Offsite power is restored within the main loop operating time, and thus all three CACS loops are available but fail to start.

DK3(3A-CP1-X'-C3'). Following a depressurization accident, three main loops are available, the containment equalization pressure is greater than 1.50 atm., and both the auxiliary boilers and the CACS fail resulting in a core meltdown.

DK8(3A-CP3-SS'-C3'). For this depressurization accident sequence, three main loops are available, but the containment equalization pressure is below 1.25 atm. Failure of a main loop support system eliminates the main loops, and a core meltdown occurs due to failure of the CACS.

5.2 Initiating Events Not Affecting the Performance of Either Shutdown Cooling System.

5.2-1 Model of Events

Figure 5.1 is a simple diagram of the reactor shutdown cooling operations following an initiating event which does not degrade the performance of either shutdown cooling system. The shutdown cooling process begins with all three main loops available. Individual failures in subsystems 4,5,6 or 12 will eliminate the main loop in which they occur. Each of these

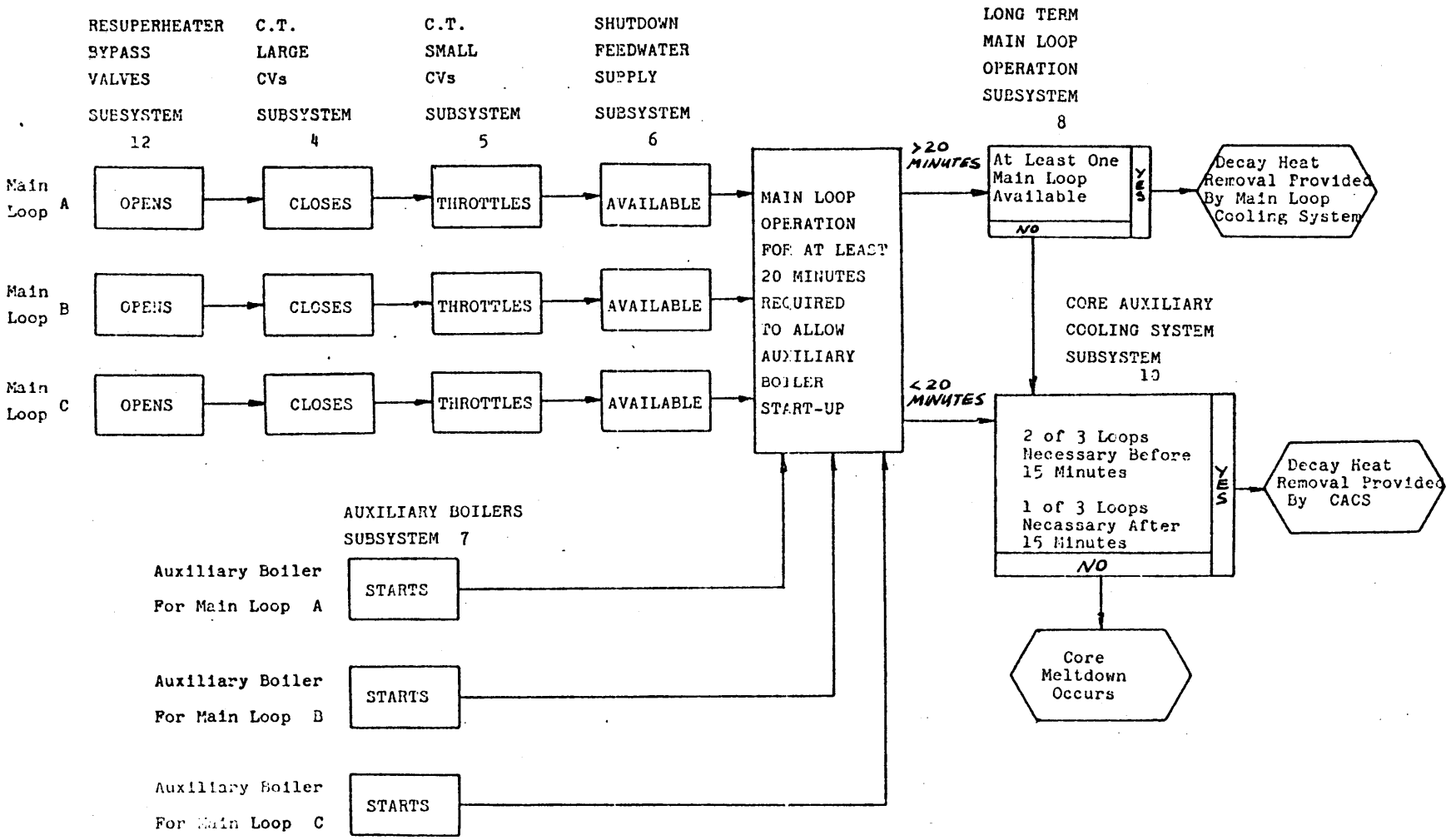


FIGURE 5.1 A Simple Diagram of a Reactor Shutdown Initiated By an Event Not Affecting the Performance of Either Shutdown Cooling System.

failures has a different effect on the main loop shutdown cooling performance as was discussed in Chapter 2. If main loop operation continues for at least twenty minutes, those auxiliary boilers which have started are assumed to be available to begin supplying steam to drive the main helium circulator-turbines. The correct combination of at least one available main loop and one auxiliary boiler is necessary for long term main loop operation. If at least one main loop is not available for long term decay heat removal, or if the main loops fail prior to twenty minutes, transfer to the core auxiliary cooling system will occur.

Two of the three CACS loops are necessary prior to fifteen minutes following the shutdown and only one of the three is necessary after this time. If both the main loops and the CACS fail, then a core meltdown is assumed to occur.

5.2-2 Sensitivity to the Subsystem Unit Reliability Values

The median probability of or loss of adequate decay heat removal determined for this initiating event category is 7×10^{-7} per shutdown. Table 5-I lists the change in this value as the unit reliability of a given subsystem is changed to the low or high end of its sensitivity range. The factor change indicated in the table represents the ratio of the category I core-melt probability calculated at the indicated reliability value to the median category I core-melt probability. For example, a

TABLE 5-I.
Core Meltdown Sensitivity to Subsystem Unit Reliability Values for Reactor Shutdowns Resulting from Category I Initiating Events

Subsystem Index and Name	Subsystem Unit Reliability Sensitivity Range (Low, High)	Factor Change in the Probability of a Loss of Decay Heat Removal*
4: CT Large CV's	.99 .9999	2.7 0.82
5: CT Small CV's	.97 .9997	7.9 0.62
6: Shutdown Feedwater System	.96 .9996	1.8 0.95
7: Auxiliary Boilers	.875 .999	3.8 0.90
8: Main Loop Transfer to Decay Heat Removal Operation	.93 .9993	2.1 0.93
10: Core Auxiliary Cooling System	.9 .999	31.6 0.10
12: Resuperheater Bypass Control Valves	.99 .9999	2.7 0.81

*Based on the median reliability values, the probability of a loss of decay heat removal is 7×10^{-7} per shutdown.

CT large CV reliability of .99 will result in a core-melt probability that is 2.7 times the median value. Increasing the CT large CV reliability to .9999 results in a core-melt probability that is 82% of the median value.

Notice that the reliability value of the CACS is by far the most sensitive. This is partly due to the fact that the vast majority of core meltdowns occur in the time interval in which two CACS loops are required. Table 5-II lists the percentage of the category I core-melt probability due to accident sequences which occur in the various EDS outcome categories. Just over 78% of the core-melt probability is due to accident sequences which occur prior to fifteen minutes following the shutdown, and of these accident sequences the largest part (over 58% of the total core-melt probability) occur with one CACS loop operating. This indicates that significant decreases in the core-melt probability for this category can be made by both increasing the CACS reliability, and by increasing the heat removal capability of the CACS loops.

Table 5-III lists the dominant accident sequences for this initiating event category. Those accident sequences in which only one CACS loop operates prior to fifteen minutes following the shutdown (ESD outcome category 4), are W9, T2, V2, Z2, CC2, 09 and R2. If one CACS loop were capable of adequate core cooling at 10 minutes following the shutdown, T2 and R2 would not lead to a core meltdown, and the probability of a meltdown decreases to 6×10^{-7} per shutdown. If one CACS loop were

TABLE 5-II.
A List of the Calculated Percent of Core Meltdowns Occurring in Different Time Intervals Following Reactor Shutdowns Due to Initiating Event Category I

ESD Outcome Category	Time Interval in Which Meltdown is Assumed to Occur	Percent of Core Meltdowns
4	0-15 minutes - only one auxiliary loop available	58.6
5	20-30 minutes - loss of decay heat removal	22.1
6	15-20 minutes - loss decay heat removal	0.1
7	10-15 minutes - loss of decay heat removal	1.2
8	5-10 minutes - loss of decay heat removal	14.8
9	within 5 minutes-loss of decay heat removal	3.2

TABLE 5-III.
A List of Dominant Accident Sequences For
Reactor Shutdowns Due to Category I Initiating Events

Accident Sequence	ESD Outcome Category	Probability of a Loss of Decay Heat Removal Per Shutdown
K3(3A-X'-C3')	5	1×10^{-7}
W9(A-L'-I'-C2')	4	8×10^{-8}
T2(3S'-C2')	4	8×10^{-8}
V2(3L'-C2')	4	7×10^{-8}
Z2(A-L'-S'-C2')	4	7×10^{-8}
CC2(A-2L'-C2')	4	4×10^{-8}
09(A-S'-I'-C2')	4	3×10^{-8}
T14(3S'-C3')	8	3×10^{-8}
W23(A-L'-I'-C3')	8	3×10^{-8}
Z47(A-L'-S'-C3')	8	2×10^{-8}
V8(3L'-C3')	9	2×10^{-8}
R2(A-2S'-C2')	4	2×10^{-8}
N2(3F'-C3')	5	2×10^{-8}
O31(A-S'-I'-C3')	8	1×10^{-8}
CC23(A-2L'-C3')	8	1×10^{-8}
R23(A-2S'-C3')	7	8×10^{-9}
L3(2A-F'-X'-C3')	5	6×10^{-9}
W3(2A-L'-X'-C3')	5	4×10^{-9}
03(2A-S'-X'-C3')	5	3×10^{-9}
Sum of all accident sequences for initiating event category		7×10^{-7}

capable of adequate core cooling at 8 minutes following the shutdown, Z2 and CC2 would also not lead to a core meltdown. This decreases the probability of a core meltdown to 5×10^{-7} per shutdown.

The CT small CV's are the most sensitive subsystem following the CACS for this initiating event category. The greater sensitivity of the CT small CV's in comparison to the CT large CV's should not be taken to imply that the CT small CV's are more important than the CT large CV's. The difference in sensitivities is mainly due to the fact that the CT small CV's have a lower median reliability in comparison to the CT large CV's. Intrinsically, the failure of a CT large CV is a more serious event because it eliminates the main loop much more quickly than the failure of a CT small CV. However, the greater sensitivity of the CT small CV's does indicate that improvements in the reliability of this subsystem can be beneficial.

Table 5-IV indicates the effect of changes in the operating reliability of the main loop isolation values and the main circulators during circulator-turbine imbalance conditions. Notice that large changes in the reliabilities of the isolation valves and main circulators to perform properly during imbalance conditions due to either a failed CT large CV or a CT small CV do not have a significant impact on the probability of a core meltdown.

Table 5-V shows the change in the probability of a core

TABLE 5-IV.
The Sensitivity of Main Loop Isolation Valve and Circulator Operating Reliability for Shutdowns Due to Category I Initiating Events

Isolation Valve or Circulator Function	Isolation Valve or Circulator Reliability (High, Low)	Factor Change in the Probability of a Loss of Decay Heat Removal
Main Loop Isolation Valve closes due to imbalance created by a failed	.9995 .999	0.87
CT Large CV	.95	1.2
CT Small CV	.9	
Main Loop Isolation Valve opens following an imbalance condition	.9999 .99	0.93 1.7
Main Circulator remains operable following an imbalance condition created by a failed	.95 .995	0.87
CT Large CV	.10	1.2
CT Small CV	.75	

TABLE 5-V.
The Effect of Restarting Initially Failed Shutdown Feed Pumps for Reactor Shutdowns Due to Category I Initiating Events

Probability of Re-Starting Initially Failed Shutdown Feed Pumps (Given at Least 15 Minutes)			Factor Change in the Probability of a Loss of Decay Heat Removal
Restart	1 of 3	1.0	0.96
Restart	1 of 2	1.0	
Restart	1 of 1	1.0	
Restart	1 of 3	.75	0.97
Restart	1 of 2	.60	
Restart	1 of 1	.30	
Restart	1 of 3	.25	0.99
Restart	1 of 2	.20	
Restart	1 of 1	.10	

meltdown given different probabilities of re-starting initially failed shutdown feedpumps. The table shows that only a very small decrease is gained even if all initially failed feedpumps can be started.

In addition to Table 5-I, the sensitivites of the subsystem unit reliability valves are illustrated in sensitivity plots. The purpose of these plots is to allow easy extrapolation of the effect of possible changes in the reliability of various subsystems. These changes may be due to either improvements in the subsystem component reliabilities, or changes in the subsystem configuration which do not affect its performances as modelled in the ESD's.

In each figure, the probability of a loss of decay heat removal (per shutdown) is plotted as a function of the subsystem unit reliability. Three curves are shown on each plot which correspond to different values of the beta factor. The middle curve corresponds to a beta factor for all subsystems of 0.03. The top and bottom curves respectively correspond to beta factors of 0.1 and 0.01 for all subsystems. The sensitivity plots for subsystems 4,5,6,7,8, 10 and 12 are included as Figures 5.2 through 5.8, respectively.

As an example of the use of these curves, each CACS loop air cooler contains two forced-air fans. The correct operation of both fans was assumed necessary for proper CACS loop performance. However, should the operation of only one fan be adequate, the unit reliability of the CACS would increase to

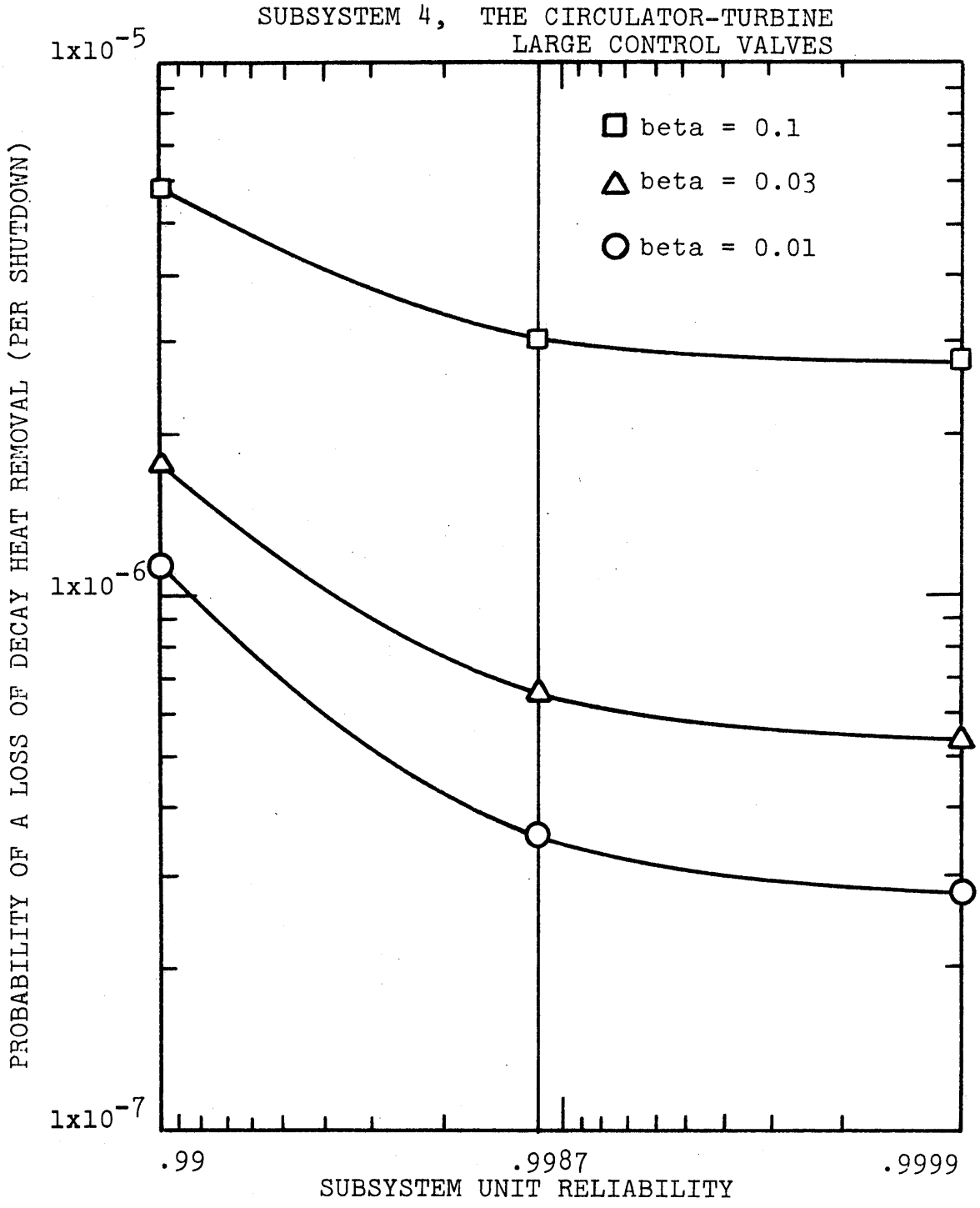


FIGURE 5.2 Sensitivity plot of subsystem 4 for shutdowns due to category I initiating events

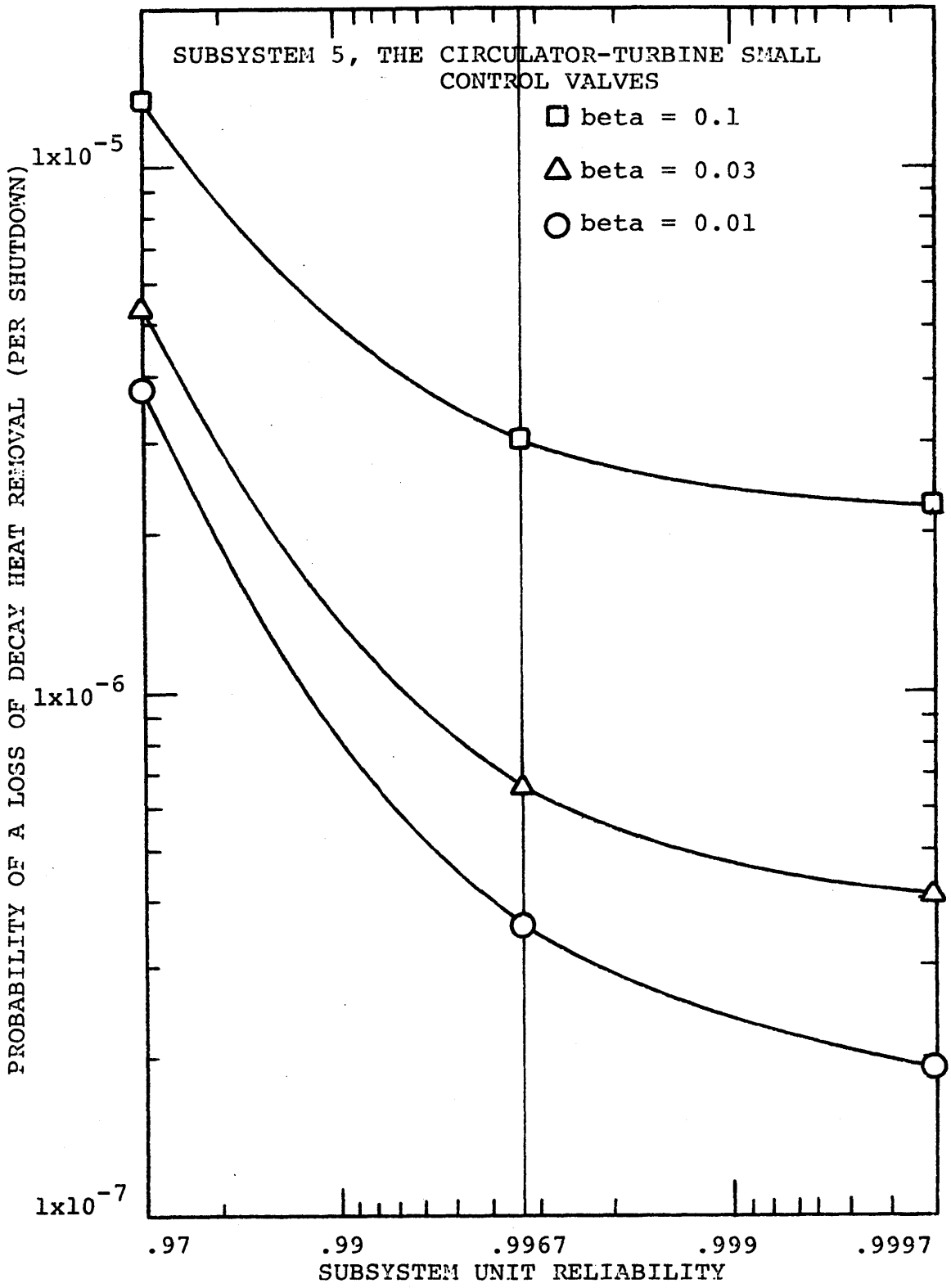


FIGURE 5.3 Sensitivity plot of subsystem 5 for shutdowns due to category I initiating events

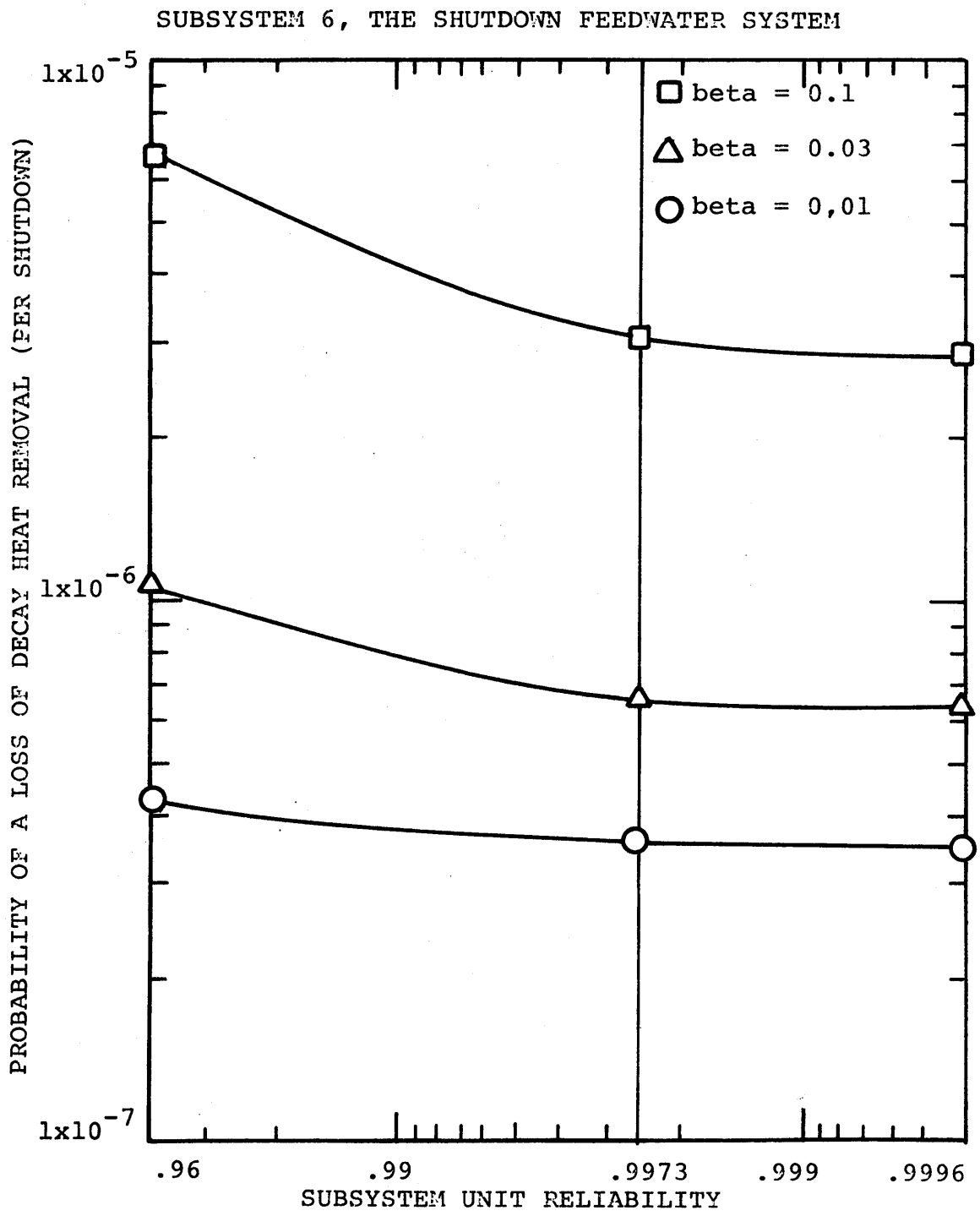


FIGURE 5.4 Sensitivity plot of subsystem 6 for shutdowns due to category I initiating events

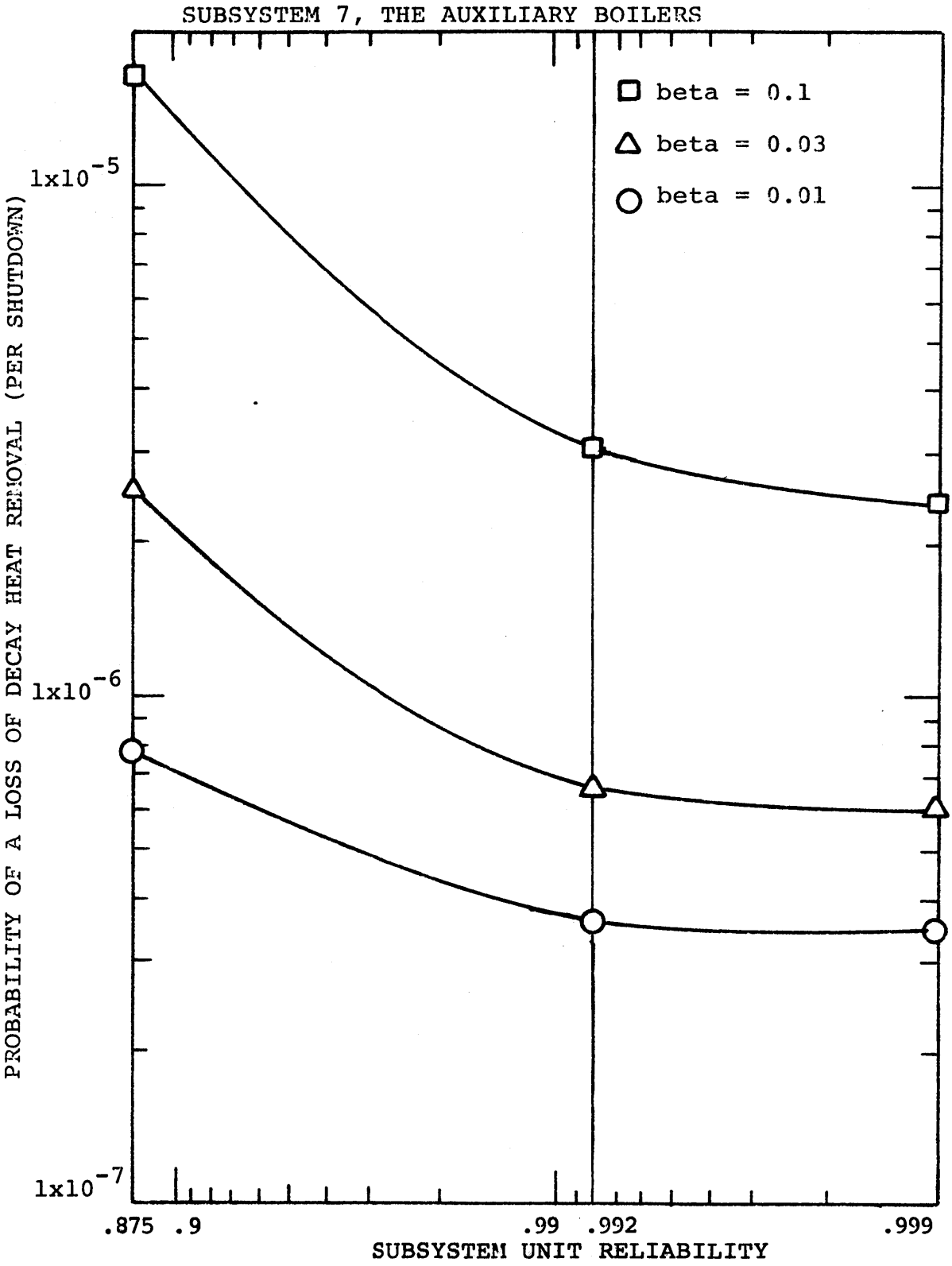


FIGURE 5.5 Sensitivity plot of subsystem 7 for shutdowns due to category I initiating events

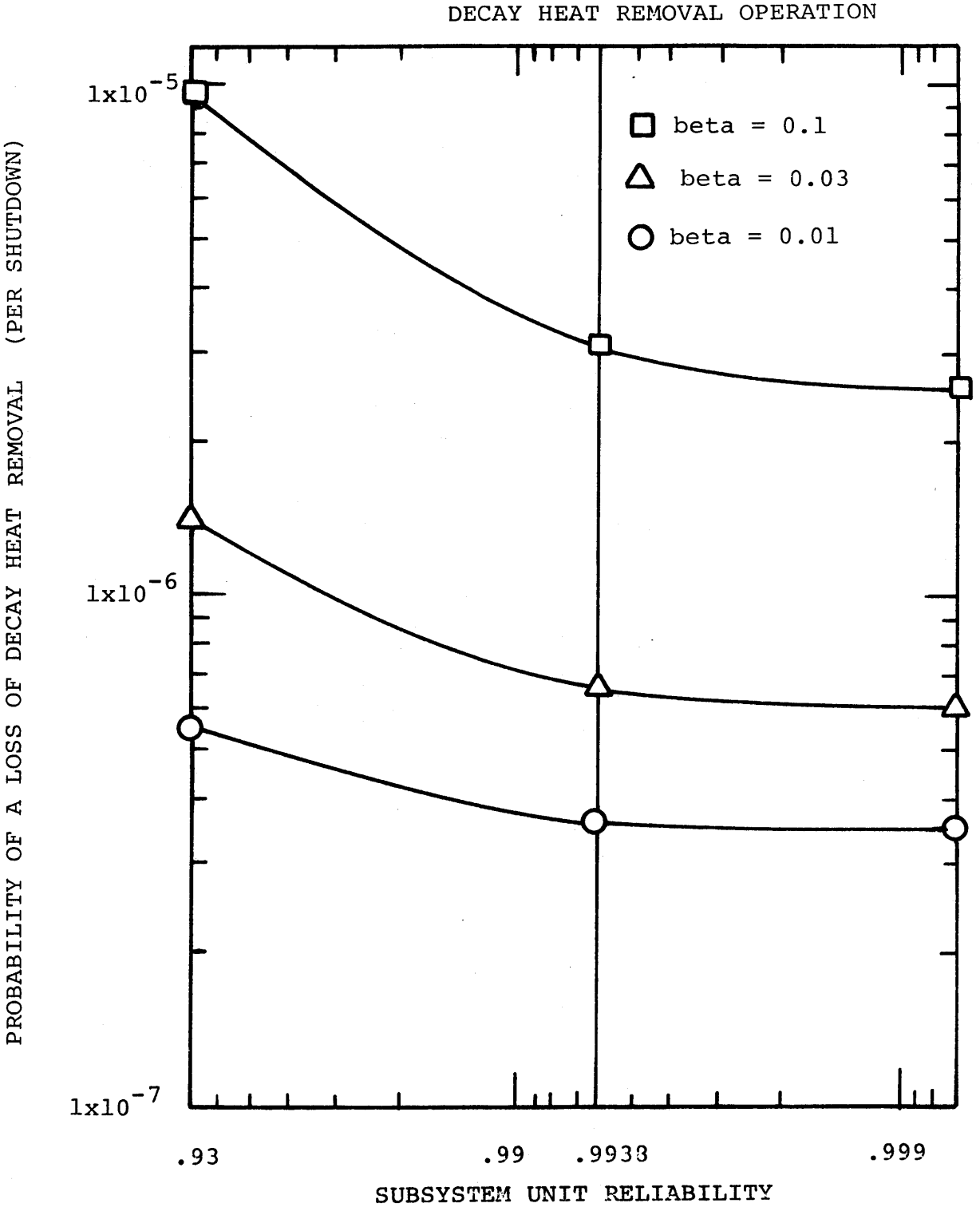


FIGURE 5.6 Sensitivity plot of subsystem 8 for shutdowns due to category I initiating events

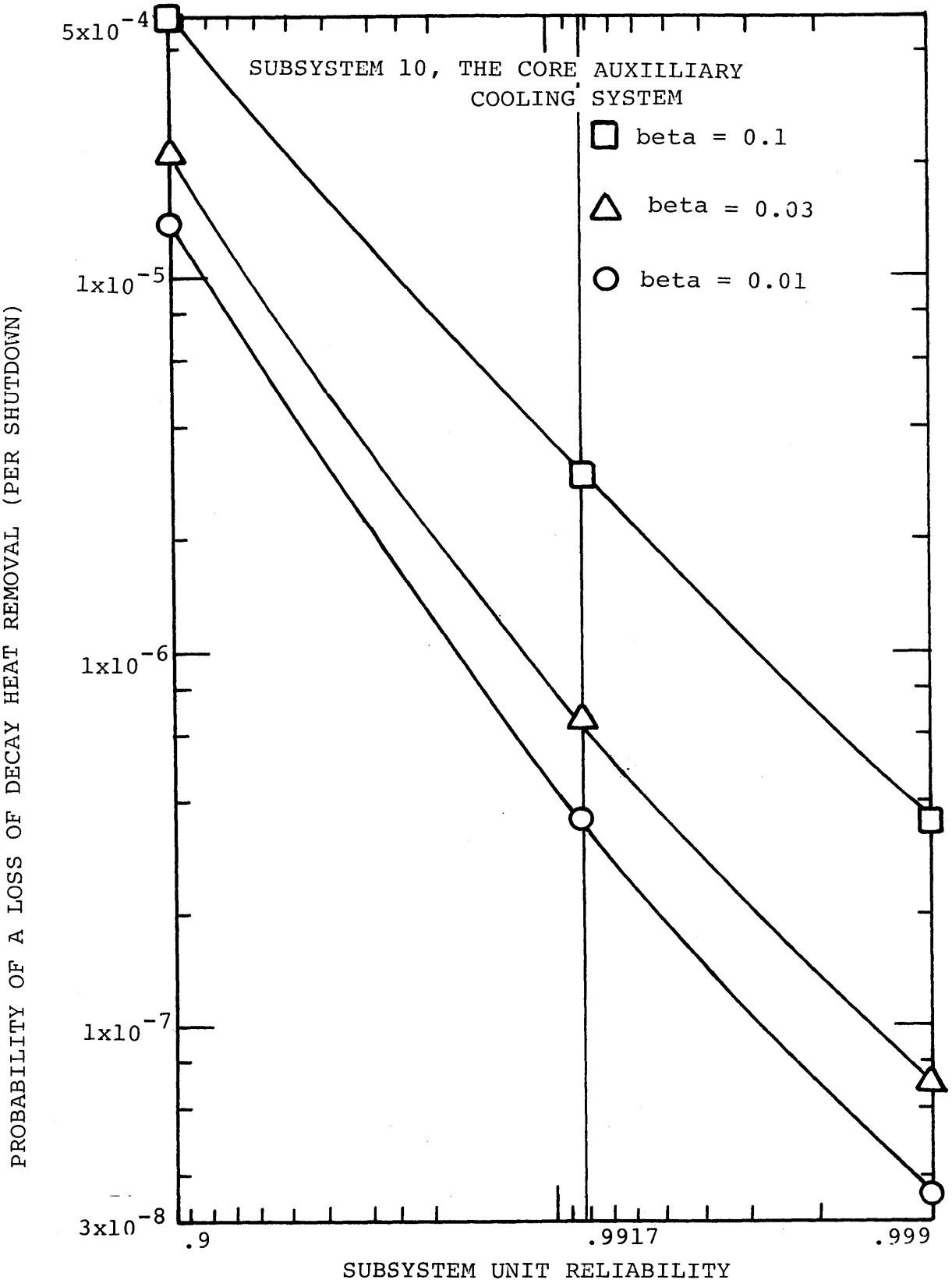


FIGURE 5.7 Sensitivity plot of subsystem 10 for shutdowns due to category I initiating events

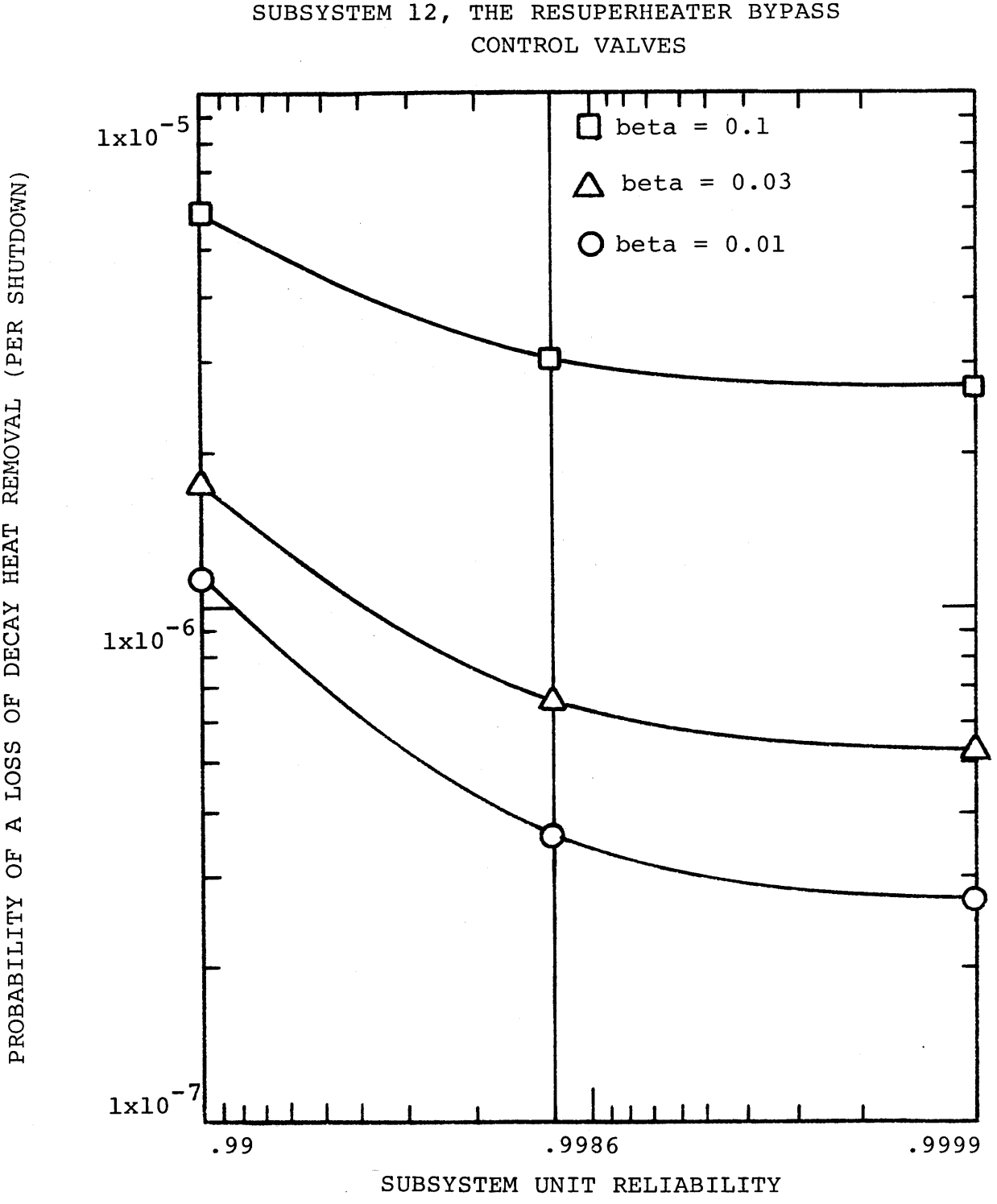


FIGURE 5.8 Sensitivity plot of subsystem 12 for shutdowns due to category I initiating events

.9943. Figure 5.7 is the sensitivity plot of the CACS, and for the median beta factor, this increase in the CACS unit reliability would result in a decrease in the probability of a core meltdown to about 4×10^{-7} per shutdown.

The importance of the component reliability of the main loop shutdown cooling system was also investigated for this initiating event category. The sensitivity of this value to changes in the main loop subsystem reliability valves was determined. Core meltdowns following a reactor shutdown occur due to failure of both the main loop cooling system and the CACS. It was felt that some main loop subsystems might be more important toward increasing the main loop reliability than to decreasing the core meltdown probability.

Table 5-VI shows the sensitivity of the main loop shutdown cooling subsystems toward the unreliability of main loop shutdown cooling. The median reliability of the main loop shutdown cooling system was determined to be .9989. The sensitivities are represented as changes in the unreliability (the compliment of the reliability) because this gives numbers that are more easily comparable. A decrease in the reliability from the median value to .9980 is only a .999 factor change. However, this same change is an increase by a factor of 1.8 in the unreliability.

The auxiliary boilers and the CT small CV's show the greatest senstivity, but on the whole, the subsystems have the same general effect. This would indicate that they all con-

TABLE 5-VI.
Sensitivity of the Subsystem Unit Reliability Values to the Reliability of Main Loop Shutdown Cooling for Reactor Shutdowns Due to Category I Initiating events

Subsystem Index and Name	Subsystem Unit Reliability Sensitivity Range (Low, High)	Factor Change in the Unreliability of the Main Loop Shutdown Cooling System*
4: CT Large CV's	.99 .9999	2.0 0.89
5: CT Small CV's	.97 .9997	5.2 0.76
6: Shutdown feed-water System	.96 .9996	2.4 0.93
7: Auxiliary Boilers	.875 .999	7.7 0.77
8: Main Loop Transfer to Decay Heat Removal Operation	.93 .9993	3.8 0.81
12: Resuperheater Bypass Control Valves	.99 .9999	2.0 0.93

*1.1×10^{-3} per shutdown based on median subsystem reliability values. Corresponds to a reliability of .9989.

tribute more or less equally to the main loop shutdown cooling reliability.

5.2-3 Sensitivity to Intrasystem Common Mode Failures

Due to the potentially serious effect of common mode failures on the reactor shutdown cooling operation, the sensitivity of the results to changes in the subsystem beta factors were investigated in detail. Table 5-VII lists the median probabilities of a loss of decay heat removal (per shutdown). at different beta factor values.

The relatively small change in the probability of a meltdown between $\beta = 0.0$ (no common mode failures) and $\beta = 0.01$ (1% of all unit failures are common mode failures) is due to the fact that at low values of the beta factor, the predominant means of core meltdown is due to the failure of two CACS loops prior to fifteen minutes following the shutdown. This can be seen from Table 5-VIII, which lists at different values of β, the percent of the core-melt probability due to accident sequences which occur in the various ESD outcome categories. At $\beta=0.01$, outcome category 4 still represents almost 85% of the core-melt probability. At higher values of the beta factor, those accident sequences involving common mode failures begin to appear and eventually dominate at $\beta=0.1$. This is seen by the increases in outcome categories 5,8 & 9.

Table 5-IX lists the dominant accident sequences according to their individual outcome categories. For outcome category 4,

TABLE 5-VII.
The Probability of a Loss of Decay Heat Removal at Different Beta Factor Values for Shutdowns Due to Category I Initiating Events

Common Mode Failure (Beta Factor)	Probability of a Loss of Decay Heat Removal (Per Shutdown)
0.0	3×10^{-7}
0.003	3×10^{-7}
0.01	4×10^{-7}
0.03	7×10^{-7}
0.1	3×10^{-6}

TABLE 5-VIII
A List of the Calculated Percent of Core Meltdown Occuring at Different Time Intervals Following A Shutdown Due to Category I Initiating Events.

ESD Outcome Category	Time Interval Following Shutdown in Which Meltdown is Assumed to Occur	Percent of Core Meltdowns				
		$\beta = 0.0$	$\beta = 0.003$	$\beta = 0.01$	$\beta = 0.03$	$\beta = 0.01$
4	0-15 minutes due to only one auxiliary loop available	99.5	99.5	84.8	58.6	23.9
5	20-30 minutes-loss of decay heat removal	0.07	1.1	5.7	22.1	50.1
6	15-30 minutes-loss of decay heat removal	0.001	0.009	0.03	0.1	0.2
7	10-15 minutes-loss of decay heat removal	0.04	0.3	0.8	1.2	0.9
8	5-10 minutes-loss of decay heat removal	0.4	3.0	8.0	14.8	17.3
9	within 5 minutes-loss of decay heat removal	0.002	0.1	0.7	3.2	7.7

TABLE 5-IX

A List of the Dominant Accident Sequences According to their Outcome Categories for Shutdowns due to Category I Initiating Events

OUTCOME CATEGORY 4: Only One CACS Loop Available 0 to 15 Minutes after the Shutdown					
Accident Sequence	Probability of a Loss of Decay Heat Removal (per shutdown)				
	β=0.0	β=0.003	β=0.01	β=0.03	β=0.1
W9(A-L'-I'-C2')	8×10^{-8}	← constant →			
Z2(A-L'-S'-C2')	7×10^{-8}		"		
O9(A-S'-I'-C2')	3×10^{-8}		"		
CC2(A-2L'-C2')	4×10^{-8}		"		
R2(A-2S'-C2')	2×10^{-8}		"		
V2(3L'-C2')	1×10^{-10}	7×10^{-9}	2×10^{-8}	7×10^{-8}	2×10^{-7}
T2(3S'-C2')	1×10^{-10}	3×10^{-9}	3×10^{-8}	8×10^{-8}	3×10^{-7}
Sum of all accident sequences for this category	3×10^{-7}	3×10^{-7}	3×10^{-7}	4×10^{-7}	7×10^{-7}

OUTCOME CATEGORY 5: Loss of Decay Heat Removal 20 to 30 Minutes after the Shutdown					
Accident Sequence	Probability of a Loss of Decay Heat Removal (per shutdown)				
	β=0.0	β=0.003	β=0.01	β=0.03	β=0.1
K3(3A-X'-C3')	1×10^{-10}	2×10^{-9}	1×10^{-8}	1×10^{-7}	1×10^{-6}
N2(3F'-C3')	$<1\times10^{-11}$	1×10^{-10}	2×10^{-9}	2×10^{-8}	2×10^{-7}
L3(2A-F'-X'-C3')	5×10^{-11}	4×10^{-10}	2×10^{-9}	6×10^{-9}	4×10^{-8}
W3(2A-L'-X'-C3')	$<1\times10^{-11}$	1×10^{-10}	1×10^{-9}	4×10^{-9}	3×10^{-8}
O3(2A-S'-X'-C3')	$<1\times10^{-11}$	1×10^{-10}	8×10^{-10}	3×10^{-9}	2×10^{-8}
Sum of all accident sequences for this category	2×10^{-10}	3×10^{-9}	2×10^{-8}	1×10^{-7}	2×10^{-6}

TABLE 5-IX (continued)

OUTCOME CATEGORY 8: Loss of Decay Heat Removal 5 to 10 Minutes after Shutdown					
Accident Sequence	Probability of a Loss of Decay Heat Removal (per shutdown)				
	β=0.0	β=0.003	β=0.01	β=0.03	β=0.1
T14(3S'-C3')	$<1\times10^{-10}$	3×10^{-10}	3×10^{-9}	3×10^{-8}	3×10^{-8}
W23(A-L'-I'-C3')	3×10^{-10}	1×10^{-9}	9×10^{-9}	3×10^{-8}	8×10^{-8}
Z47(A-L'-S'-C3')	$<1\times10^{-10}$	3×10^{-9}	8×10^{-9}	2×10^{-8}	8×10^{-8}
O31(A-S'-I'-C3')	$<1\times10^{-10}$	1×10^{-9}	4×10^{-9}	1×10^{-8}	4×10^{-8}
CC23(A-2L'-C3')	$<1\times10^{-10}$	2×10^{-9}	5×10^{-9}	1×10^{-8}	5×10^{-8}
Sum of all accident sequences for this category	9×10^{-10}	9×10^{-9}	3×10^{-8}	1×10^{-7}	5×10^{-7}

OUTCOME CATEGORY 9: Loss of Decay Heat Removal within 5 Minutes of the Shutdown					
Accident Sequence	Probability of a Loss of Decay Heat Removal (per shutdown)				
	β=0.0	β=0.003	β=0.01	β=0.03	β=0.1
V8(3L'-C3')	1×10^{-12}	3×10^{-10}	3×10^{-9}	2×10^{-8}	2×10^{-7}
Sum of all accident sequences for this category	4×10^{-12}	3×10^{-10}	3×10^{-9}	2×10^{-8}	2×10^{-7}

accident sequences W9, Z2, 09, C2 and R2 are all independent of common mode failures. At $\beta=0$ they are dominant, but as β increases, accident sequences V2 and T2 increase until they become dominant. These two accident sequences involve common mode failures of the CT large CV's and CT small CV's respectively.

For outcome category 5, no sequences contribute significantly until high beta factors. The accident sequence K3 is the dominant accident at $\beta=0.03$ and 0.1. It involves common mode failures of the auxiliary boilers and the CACS. The accident sequence N2 is the other major contributor in this category, and it involves common mode failures of the shutdown feedwater supply and the CACS.

The two dominant sequences from outcome categories 8 and 9, T14 and V8, involve common mode failures of the circulator-turbine control valves and the CACS.

The contribution of the individual subsystem common mode failures was investigated by varying the individual subsystem beta factor value while keeping the other subsystem beta factor values constant. The sensitivities were investigated at the low, median and high beta factor values. Table 5-X lists the factor change in the probability of a loss of decay heat removal for the two cases in which

1) all beta factor values are low and the individual beta factor values are high, and
2) all beta factor values are high and the individual beta factor values are low.

TABLE 5-X.
The Individual Subsystem Common Mode Failure Contributions at High and Low Beta Factor Values for Shutdowns Due to Category I Initiating Events

Subsystem Index and Name	Factor Change in the Probability of a Loss of Decay Heat Removal	
	Beta Value for Individual Subsystems is 0.1 While All Others Are 0.01	Beta Value for Individual Subsystems is 0.01 While All Others Are 0.1
4: CT Large CV's	1.3	0.94
5: CT Small CV's	1.8	0.84
6: Shutdown Feedwater Supply	1.1	0.93
7: Auxiliary Boilers	1.2	0.79
8: Main Loop Decay Heat Removal Operation	1.1	0.84
10: Core Auxiliary Cooling System	2.3	0.32
12: Resuperheater Bypass Control Values	1.3	0.93

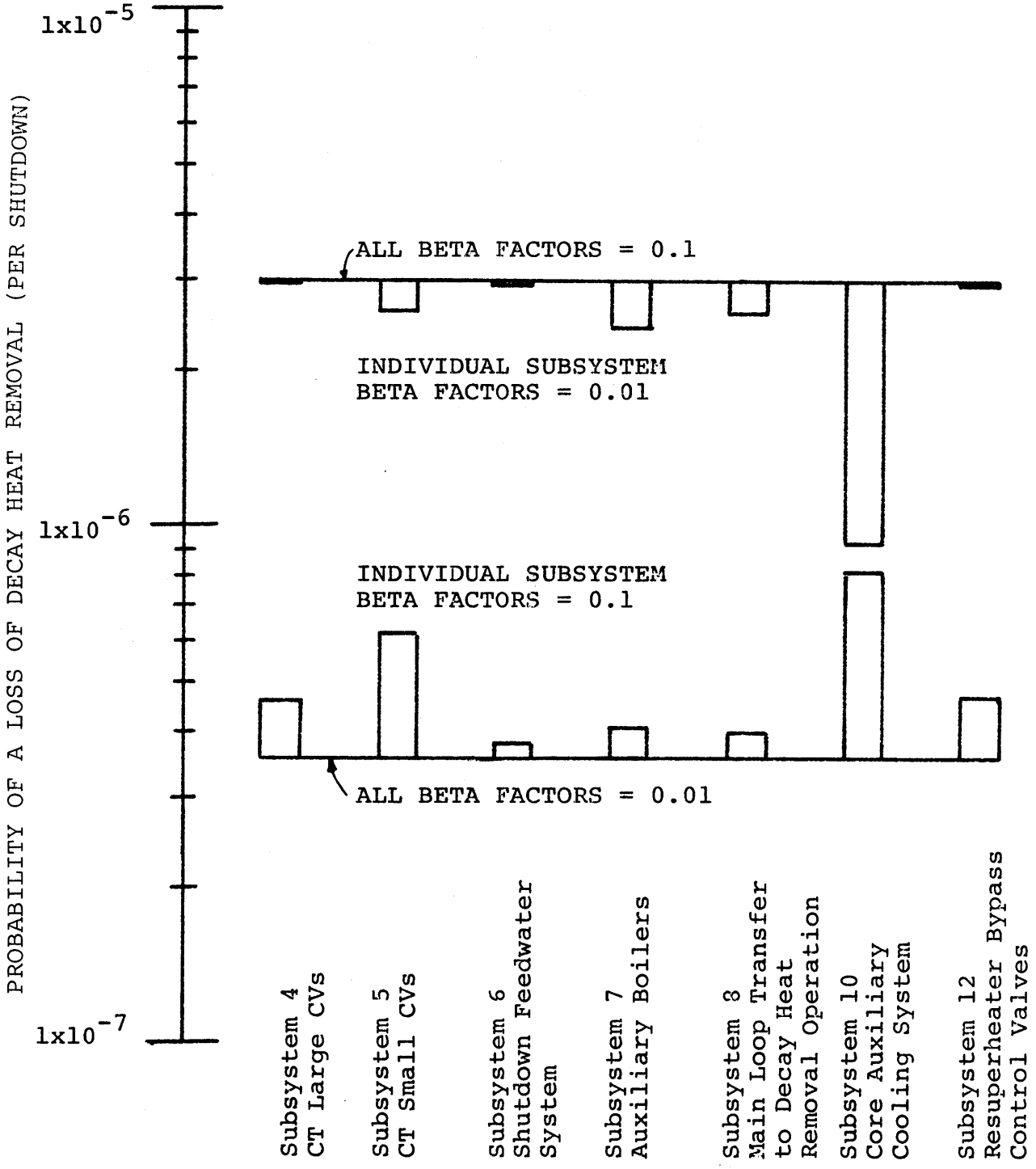


FIGURE 5.9 A bar graph of the individual subsystem common mode failure contributions at high and low beta factor values for shutdowns due to category I initiating events

In both cases, the common mode failure contribution of the CACS as the most significant. These common mode failure sensitivites are also shown in the bargraph representation of Figure 5.9. The upper line represents β=0.1 for all subsystems, and the lower line represents β=0.01 for all subsystems. The bars show the increase or decrease in the probability of a core meltdown as the individual beta factor is varied to 0.01 or 0.1.

Table 5-XI lists the change in the probability of a core meltdown as the individual subsystem beta factor values are varied to 0.01 and 0.1 and all other beta factor values are 0.03. Figure 5.10 is the bargraph representation. The common mode failure contribution of the CACS is the most important.

The effect of changes in the beta factor value on the sensitivity of the subsystem unit reliability values is shown in Table 5-XII. Notice that the sensitivity of subsystems 4, 5 & 12 decreases as the fraction of common mode failures increases. These subsystems essentilly determine the main loop availability states. As the reliability of these subsystems decreases, the initial main loop performance is degraded, and two CACS loops are required more often. At lower values of the beta factor, the percentage of failures that occur due to failure of two CACS loops prior to 15 minutes after the shutdown is higher. Therefore, changes in the reliability of subsystems 4,5 or 12 has a greater effect on the probability of a core meltdown. As the beta factor value increases, the percentage of the outcome

TABLE 5-XI.
The Individual Subsystem Common Mode Failure Contributions at Median Beta Factor Values for Shutdowns Due to Category I Initiating Events

Subsystem Index and Name	Factor Change in the Probability of a Loss of Decay Heat Removal	
	Beta Value for Individual Subsystems is 0.1 While All Others Are 0.03	Beta Value for Individual Subsystems is 0.01 While All Others Are 0.03
4: CT Large CV's	1.1	0.96
5: CT Small CV's	1.4	0.90
6: Shutdown Feedwater System	1.1	0.98
7: Auxiliary Boilers	1.2	0.94
8: Main Loop Decay Heat Removal Operation	1.7	0.97
10: Core Auxiliary Cooling System	2.0	0.73
12: Resuperheater Bypass Control Valves	1.2	0.96

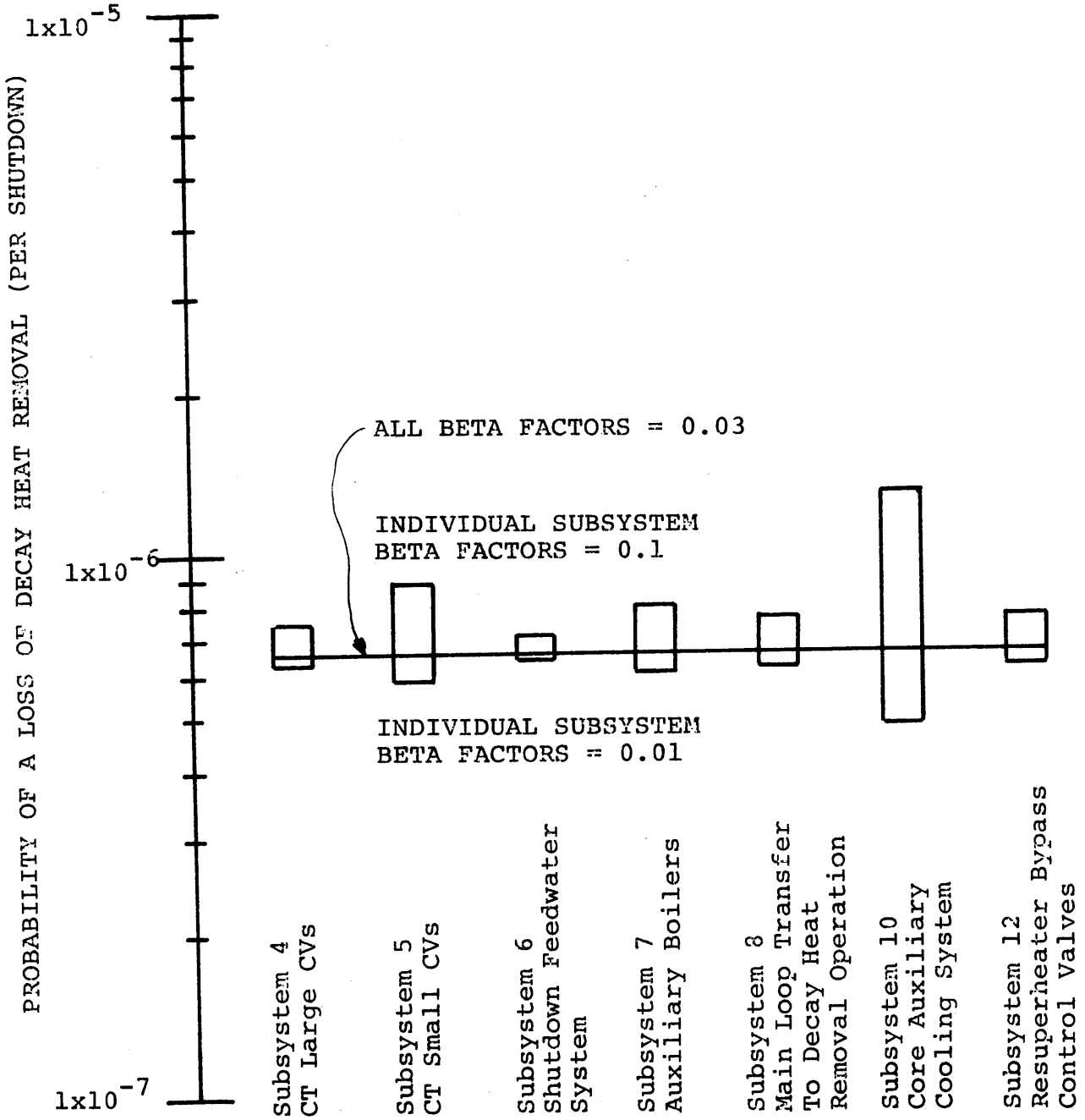


FIGURE 5.10 A bar graph of the individual subsystem common mode failure contributions at median beta factor values for shutdowns due to category I initiating events

TABLE 5-XII
The Sensitivity of the Subsystem Unit Reliability Valves at Different Beta Factor Values for Shutdowns Due to Category I Initiating Events.

Subsystem Index and Name	Subsystem Unit Reliability Sensitivity Range (low,high)	Factor Change in the Probability of A Loss of Decay Heat Removal		
		All Beta= 0.01	All Beta = 0.03	All Beta= 0.1
4:CT Large CV's	.99	3.2	2.7	1.9
	.9999	0.78	0.82	0.89
5:CT Small CV's	.97	10.7	7.9	4.4
	.9997	0.54	0.62	0.75
6:Shutdown Feedwater System	.96	1.2	1.8	2.2
	.9996	0.99	0.95	0.93
7: Auxiliary Boilers	.875	2.2	3.8	5.4
	.999	0.97	0.90	0.79
8: Main Loop Transfer to Decay Heat Removal Operation	.93	1.5	2.1	3.1
	.9993	0.98	0.93	0.84
10:Core Auxiliary Cooling System	.9	39.6	31.6	20.3
	.9999	0.76	0.81	0.88

category 4 failures decreases as the beta factor increases, and it is primarily due to this effect.

As the beta factor value increases, those accident sequences which involve a common mode failure in the main loops and in the CACS become dominant. Those accident sequences that involve common mode failures in the auxiliary boilers or the shutdown feedwater supply are the most likely, and this explains why the sensitivity of subsystems 6, 7 and 8 increases as the beta factor value increases. The common mode failure probability is tied to the subsystem unit reliability through the beta factor. Thus, changes in the reliability of subsystems 6, 7 and 8 are more important at higher beta factor values because of the greater contribution of their common mode failures to the probability of a core meltdown.

Lastly, Table 5-XIII shows that sensitivity of the main loop isolation valve and main circulator operating reliability during a circulator-turbine imbalance condition increases slightly as the beta factor value decreases. This is due to their contribution to ESD outcome category 4. However, their affect on the probability of a core meltdown is rather small.

5.2-4 The Contribution of Test and Maintenance Unavailabilities

The effect of equipment unavailabilities, due to test or maintenance purposes, on the probability of a loss of decay heat removal can be seen in both Table 5-XIV and Figure 5.11. At the median beta factor value, the probability of a core meltdown is 3×10^{-7} per shutdown with equipment failures only. The

TABLE 5-XIII

The Sensitivity of Main Loop Isolation Valve and Main Circulator Operating Reliability During Circulator-turbine Imbalances for Shutdowns Due to Category I Initiating Events

Function	Isolation Valve or Circulator Reliability (low, high)	Factor Change in the Probability of a Loss of Decay Heat Removal		
		β=0.01	β=0.03	β=0.1
Main Loop Isolation Valve Closes due to Imbalance Created by a failed	.9995 .999	0.79	0.87	0.95
CT Large CV	.95	1.3	1.2	1.1
CT Small CV	.9			
Main Loop Isolation Valve Opens Following an Imbalance Condition	.9999 .99	0.90 2.0	0.93 1.7	0.98 1.2
Main Circulator Remains Operable Following an Imbalance Created by a failed	.95 .995	0.79	0.87	0.95
CT Large CV	.10			
CT Small CV	.75	1.4	1.2	1.1

TABLE 5-XIV.
A List of Core Meltdown Probabilities for Equipment Failures Only and all Failure Contributions for Shutdowns Due to Category I Initiating Events

Intrasystem Common Mode Failure Fraction (Beta Factor)	Probability of a Loss of Decay Heat Removal (Per Shutdown)	
	Equipment Failures Only	Equipment Failures and Test and Maintenance Unavailabilities
0.0	4×10^{-8}	3×10^{-7}
0.003	5×10^{-8}	3×10^{-7}
0.01	9×10^{-8}	4×10^{-7}
0.03	3×10^{-7}	7×10^{-7}
0.1	2×10^{-6}	3×10^{-6}

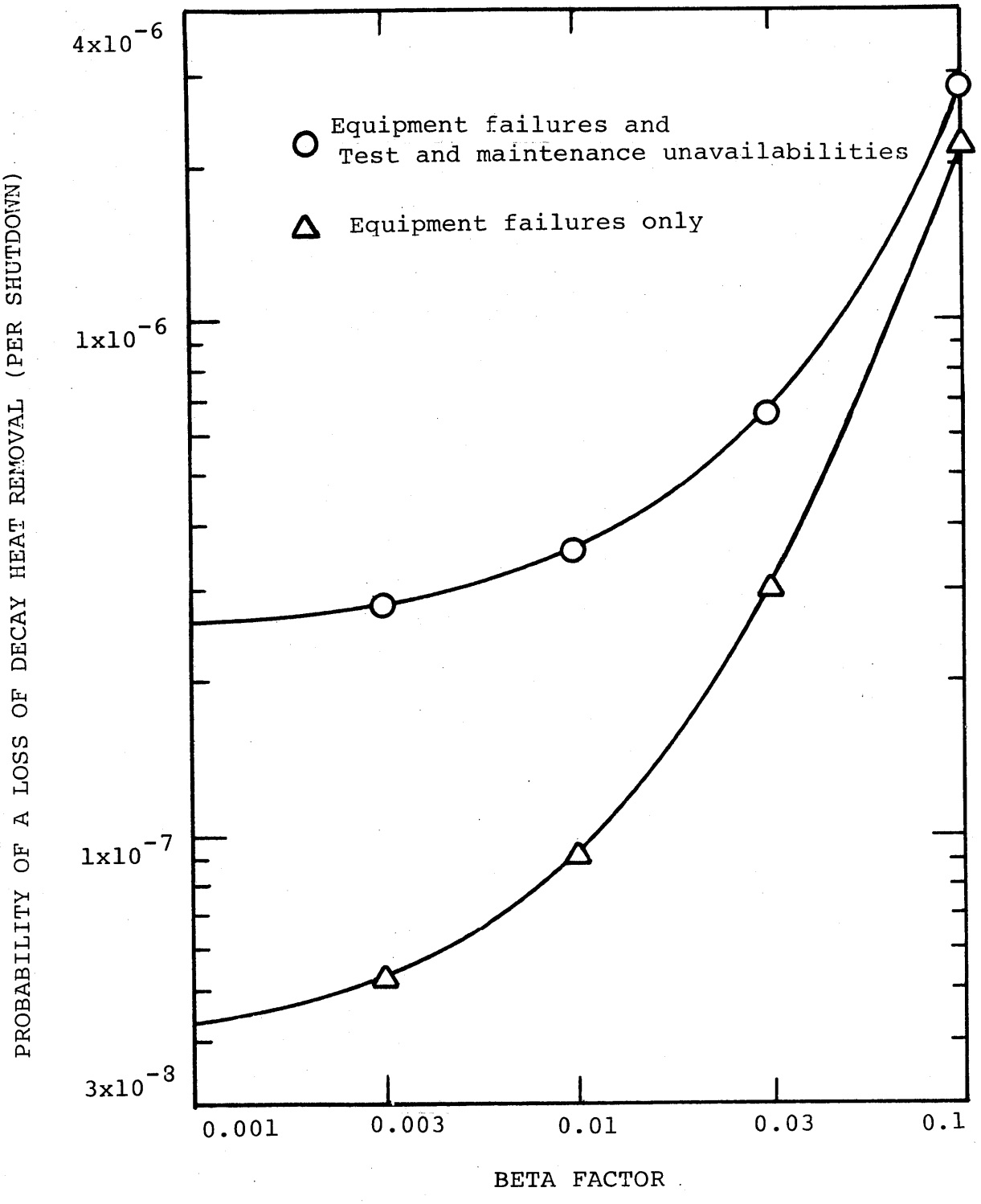


FIGURE 5.11 Probability of a Core Meltdown for shutdowns due to category I initiating events

inclusion of test and maintenance unavailabilities increases the core-melt probability by a factor of 2.2. The variation in the probability of a core meltdown can best be seen in Figure 5.11. At low beta factor values, the test and maintenance unavailability contribution is large, but as the beta factor value increases, this contribution decreases due to the dominance of common mode failures.

Table 5-XV lists the percentage of the core-melt probability due to accident sequences occurring in the different ESD outcome categories considering equipment failures only. In comparison to Table 5-VIII, it can be seen that including test and maintenance unavailabilities greatly increases the percent of core meltdowns which occur due to only one CACS loop operating prior to 15 minutes following shutdown. At the median beta factor value the percent of the core-melt probability due to outcome category 4 accident sequences is doubled by including test and maintenance unavailabilities.

A list of the dominant accident sequences considering no test and maintenance unavailabilities is shown in Table 5-XVI. The table lists the change in the accident sequence probability given in Table 5-III. A comparison with Table 5-III shows that the outcome category 4 sequences appear much lower in the order without test and maintenance unavailabilities. Also, their probability is most greatly decreased from the value in Table 5-III, which includes test and maintenance unavailabilities. It is interesting to note that in Table 5-XVI the first six accident sequences involve common mode failures.

TABLE 5-XV

A List of the Calculated Percent of Core Meltdowns Occuring at Different Time Intervals Following Shutdown. Subsystem Failures Due to Equipment Failure Only. Category I Initiating Events.

ESD Outcome Category	Time Interval Following Shutdown in Which Meltdown is Assumed to Occur	Percent of Core Meltdowns				
		β=0.0	β=0.003	β=0.01	β=0.03	β=0.1
4	0-15 minutes due to only one auxiliary loop available	99.7	86.4	59.5	26.1	7.4
5	20-30 minutes-loss of decay heat removal	0.01	2.9	16.1	42.1	62.5
6	15-20 minutes-loss of decay heat removal	0.0001	0.01	.05	0.01	0.1
7	10-15 minutes-loss of decay heat removal	0.04	1.5	3.0	2.7	1.2
8	5-10 minutes-loss of decay heat removal	0.2	8.8	18.8	22.4	18.7
9	within 5 minutes-loss of decay heat removal	0.0006	0.4	2.5	6.7	10.1

TABLE 5-XVI.
A List of the Dominant Accident Sequences Considering Equipment Failures Only for Shutdowns Due to Category I Initiating Events

Accident Sequence	ESD Outcome Category	Factor Change in the Individual Accident Sequence Probability Given in Table 5-III
K3(3A-X'-C3')	5	0.92
T14(3S'-C3')	8	0.96
V8(3L'-C3')	9	0.95
NZ(3F'-C3')	5	0.95
TZ(3S'-C2')	4	0.26
V2(3L'-C2')	4	0.25
W23(A-L'-I'-C3')	8	0.55
Z47(A-L'-S'-C3')	8	0.55
031(A-S'-I'-C3')	8	0.96
W9(A-L'-I'-C2')	4	0.15
Z2(A-L'-S'-C2')	4	0.15
09(A-S'-I'-C2')	4	0.27
R23(A-2S'-C3')	7	0.99
R2(A-2S'-C2')	4	0.26
CC2(A-2L'-C2')	4	0.10
CC23(A-2L'-C3')	8	0.39
03(2A-S'-X'-C3')	5	0.51
W3(2A-L'-X'-C3')	5	0.29
L3(2A-F'-X'-C3')	5	0.20

TABLE 5-XVII

The Contribution of Individual Subsystem Test and Maintenance Unavailabilities for Shutdowns due to Category I Initiating Events

Subsystem Index and Name	Test and Maintenance Unavailability (per unit)	Factor Change in the Probability of a Loss of Decay Heat Removal* T & M Unavailability Included on Specific Subsystem only		
		β=0.01	β=0.03	β=0.1
6:Shutdown Feedwater Supply	4×10^{-3}	1.0	1.0	1.0
7:Auxiliary Boilers	1.2×10^{-2}	1.0	1.0	1.0
8:Main Loop Transfer to Decat Heat Removal Operation	4×10^{-3}	1.0	1.0	1.0
10:Core Auxiliary Cooling System	1.2×10^{-2}	2.7	1.8	1.3
12:Resuperheater Bypass Control Valves	2×10^{-3}	1.4	1.2	1.1

* The core-melt probability considering equipment failures only is given in Table 5-XIV.

TABLE 5-XVIII.
Main Loop Shutdown Cooling Reliability With and Without Test and Maintenance Unavailabilities for Shutdowns Due to Category I Initiating Events

Intrasystem Common Mode Failure Fraction (Beta Factor)	Reliability of the Main Loop Shutdown Cooling System	
	Equipment Failures Only	Equipment Failures and Test and Maintenance Unavailabilities
0.0	.9998	.9996
0.003	.9997	.9996
0.01	.9996	.9994
0.03	.9991	.9989
0.1	.9975	.9973

The individual subsystem contributions due to test and maintenance unavailability are shown in Table 5-XVII. The table clearly shows that only the unavailability of the CACS and the resuperheater bypass control valves has any effect on the probability of a core meltdown. The resuperheater bypass unavailability, even though it is small compared to that of the CACS, is significant because failures of the resuperheater bypass circuit were assumed to quickly eliminate that main loop involved.

Table 5-XVIII shows that equipment test and maintenance unavailabilities do not have any significant effect on the main loop shutdown cooling reliability.

5.3 Initiating Events Affecting the Performance of a Single Main Cooling Loop

5.3-1 Model of Events

Figure 5.12 is a simplified diagram of the reactor shutdown cooling operations following a shutdown initiated by an event which eliminates a single main cooling loop. A forced shutdown results from these events only if an operational protection system failure also occurs. The shutdown cooling operations begin with two main loops available. Three auxiliary boilers are available, but both main loops must remain fully available in order to allow sufficient time for the boilers to

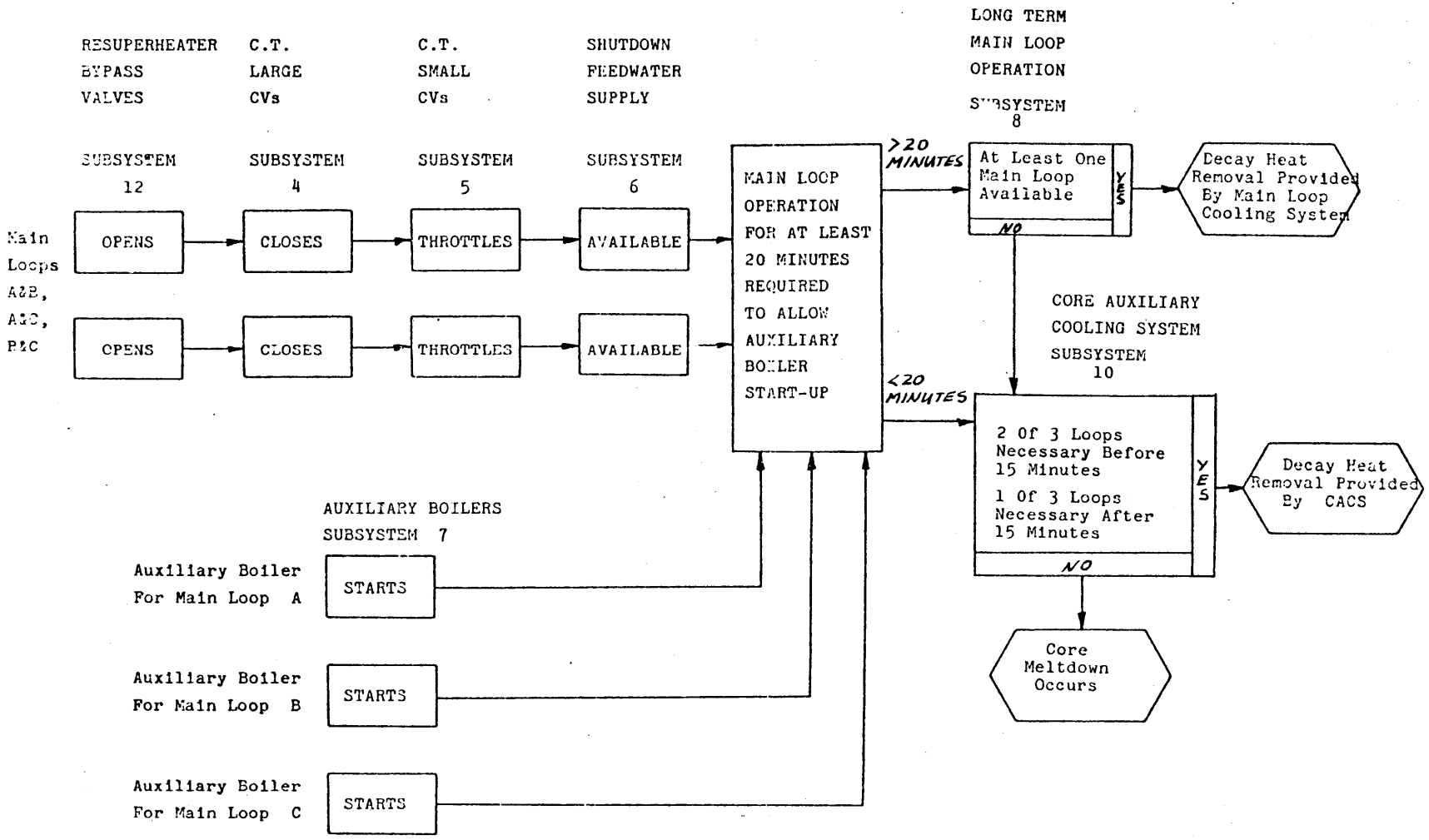


FIGURE 5.12 A Simple Diagram of a Reactor Shutdown Initiated By an Event Eliminating a Single Main Cooling Loop.

reach rated conditions. If at any time main loop failure occurs, all three CACS loops are available to take over the core cooling.

5.3-2 Sensitivity of the Subsystem Unit Reliability Values

The median value for the probability of a loss of decay heat removal for reactor shutdowns due to category II.A initiating events is 2×10^{-5} per shutdown. Table 5-XIX lists the sensitivities of the subsystem unit reliability values. For these reactor shutdowns, the subsystem sensitivities follow the same trend as the subsystem sensitivities for reactor shutdown due to category I initiating events. The reliability of the CACS is, by far, the most important factor determining the probability of a core meltdown. However, the reliability of the auxiliary boilers is not a significant factor.

Table 5-XX lists the dominant accident sequences for this initiating event category. The first four accident sequences are the most dominant contributors. These are CC2, Z2, CC23 and Z47. For these sequences only a single main loop is available due to a failure of either the resuperheater bypass control valve, the CT large CV, or the CT small CV on the other main loops. A single main loop cannot operate long enough to allow the auxiliary boilers to reach their rated conditions, and the CACS is required to operate. The small sensitivity of the auxiliary boiler reliability value is due to the fact that the

TABLE 5-XIX.
Core Meltdown Sensitivity of the Subsystem Unit Reliability Values for Shutdowns Due to Category II.A Initiating Events

Subsystem Index and Name	Subsystem Unit Reliability Sensitivity Range (Low, High)	Factor Change in the Probability of a Loss of Decay Heat Removal*
4: CT Large CV's	.99 .9999	2.0 0.85
5: CT Small CV's	.97 .9997	4.2 0.64
6: Shutdown Feed-water System	.96 .9996	1.1 1.0
7: Auxiliary Boilers	.875 .999	1.4 0.99
8: Main Loop Transfer to Decay Heat Removal Operation	.93 .9993	1.4 0.99
10:Core Auxiliary Cooling System	.9 .999	34.8 0.10
12:Resuperheater Bypass Control Values	.99 .9999	2.0 0.84

*Based on the median subsystem reliability values, the probability of a loss of decay heat removal is 2×10^{-5} per shutdown.

TABLE 5-XX.
A List of the Dominant Accident Sequences For
Reactor Shutdowns Due to Category II.A Initiating Events

Accident Sequence	ESD Outcome Category	Probability of a Loss of Decay Heat Removal Per Shutdown
CC2(A-L'-C2')	4	7×10^{-6}
Z2(A-S'-C2')	4	5×10^{-6}
CC23(A-L'-C3')	8	2×10^{-6}
Z47(A-S'-C3')	8	1×10^{-6}
W3(2A-X'-C3')	5	3×10^{-7}
X3(A-F'-X'-C3')	5	1×10^{-7}
BB2(2S'-C2')	4	9×10^{-8}
V2(2L'-C2')	4	8×10^{-8}
D2(L'-F'-C2')	4	5×10^{-8}
BB28(2S'-C3')	8	3×10^{-8}
V8(2L'-C3')	9	3×10^{-8}
Y2(2F'-C3')	6	3×10^{-8}
CC6(L'-I'-C2')	4	3×10^{-8}
AA2(F'-S'-C2')	4	3×10^{-8}
DD41(F'-L'-C3')	8	2×10^{-8}
U2(L'-S'-C2')	4	2×10^{-8}
Z14(S'-I'-C2')	4	1×10^{-8}
AA64(F'-S'-C3')	8	1×10^{-8}
Sum of all accident sequences for this initiating category		2×10^{-5}

auxiliary boilers do not operate in these four accient sequences. The large sensitivity of the CACS reliability value is due to the fact that it is required to operate prior to 15 minutes following the shutdown in all but three of the sequences listed in Table 5-XX. It is interesting that the two most likely accident sequences for this initiating event category (CC2 and Z2) could be eliminated by increasing the design capability of the CACS so that one auxiliary loop was adequate at eight minutes after the shutdown. This would decrease the probability of a core meltdown to about 5×10^{-6} per shutdown.

The median probability of a core meltdown for this initiating event category was not significantly affected by changes in the main loop isolation value operating reliability or main circulator operating reliability during circulator-turbine imbalance conditions. The effect of restarting initially failed shutdown feedpumps was also insignificant. This is due to the small contribution, for this initiating event category, of those accident sequences involving shutdown feedpump failures and main loop failures due to circulator-turbine imbalance conditions.

Figure 5.13 is the sensitivity plot of the CACS reliability value for shutdowns due to initiating events which eliminate one main loop. An increase in the CACS unit reliability to .9943 due to the design change mentioned in section 5.2-2 would decrease the probability of a core meltdown for this initiating event category to 1×10^{-5} per shutdown. Only a sensitivity plot of the CACS is provided due to the greater sensitivity

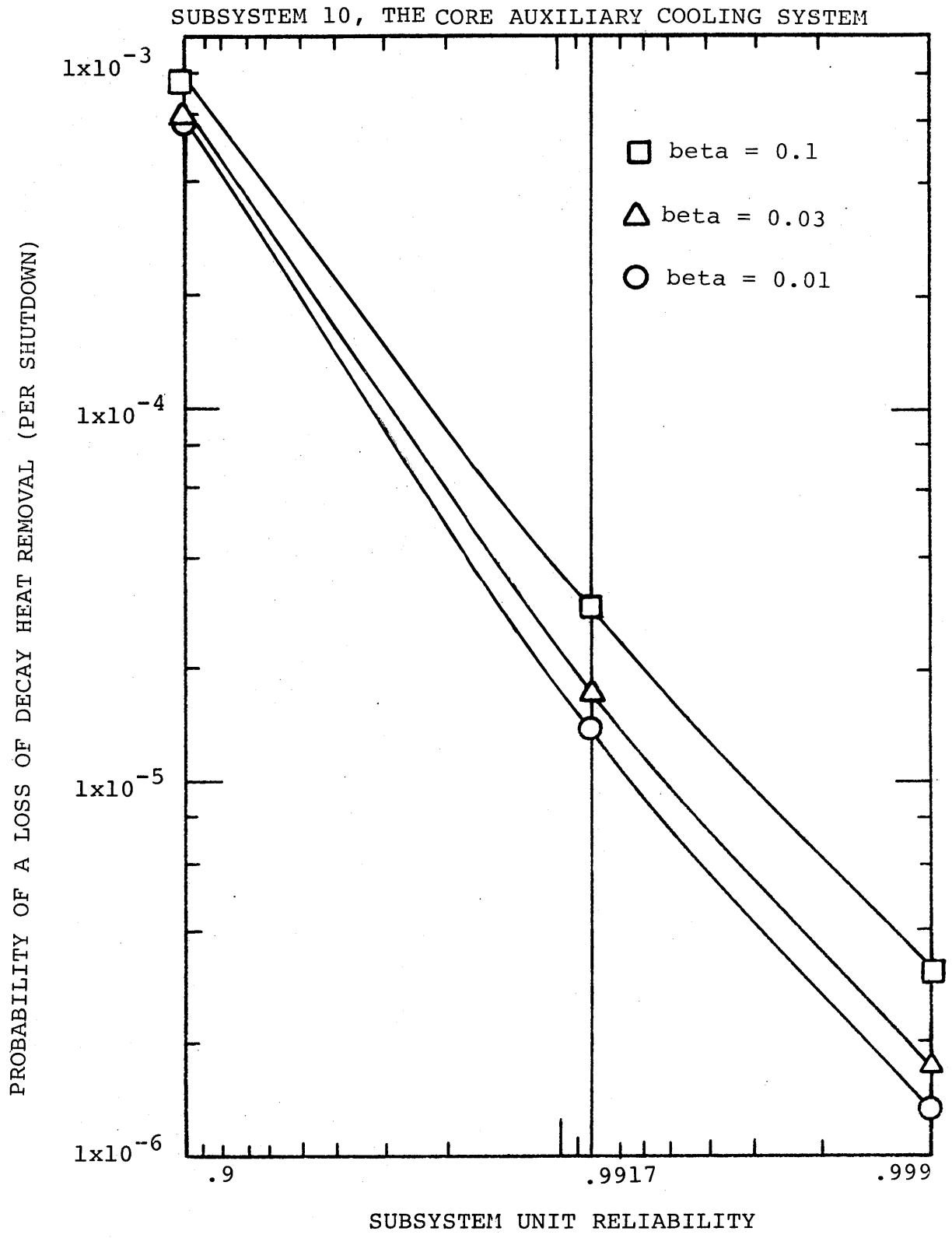


FIGURE 5.13 Sensitivity plot of subsystem 10 for shutdowns due to category II.A initiating events

of this subsystem over the others.

5.3-3 Sensitivity to Common Mode Failures and Test and Maintenance Unavailabilities

The variation in the probability of a loss of decay heat removal due to both common mode failures and test and maintenance unavailabilities is shown in Table 5-XXI. Notice that the probability of a core meltdown is increased more by the inclusion of the test and maintenance unavailabilities than by increases in the beta factor value.

It can be seen in Table 5-XXII, that the majority of core meltdowns occur with only a single CACS loop available prior to fifteen minutes following the shutdown. At the median beta factor value, 74% of the core-melt probability is due to accident sequences of this type. In Table 5-XXIII, the individual accident sequences for outcome categories 4 and 8 are listed. Many of the accident sequences from outcome category 4 are unaffected by common mode failures, but all are affected by test and maintenance unavailability of the CACS. The accident sequences of outcome category 8 all increase as the beta factor value increases due to common mode failure of the CACS.

After considering the dominant accident sequences, it is not too suprising that the investigation of the individual subsystem common mode failure contributions showed that only common mode failure of the CACS were significant. Also, the investigation

TABLE 5-XXI.
A List of Core-Melt Probabilities for Equipment Failures Only and for all Failure Contributions for Shutdowns Due to Category II.A Initiating Events

Intrasystem Common Mode Failure Fraction (Beta Factor)	Probability of a Loss of Decay Heat Removal (Per Shutdown)	
	Equipment Failures Only	Equipment Failures and Test and Maintenance Unavailability
0.0	2×10^{-6}	1×10^{-5}
0.003	3×10^{-6}	1×10^{-5}
0.01	4×10^{-6}	1×10^{-5}
0.03	6×10^{-6}	2×10^{-5}
0.1	1×10^{-5}	3×10^{-5}

TABLE 5-XXII

A List of the Calculated Percent of Core Meltdowns Occuring for the Various ESD Outcome Categories for Shutdowns due to Category II.A Initiating Events

ESD Outcome Category	Time Interval Following Shutdown in which Meltdown is Assumed to Occur	Percent of Core Meltdowns				
		β=0.0	β=0.003	β=0.01	β=0.03	β=0.1
4	0-15 minutes only one CACS loop available	99.6	96.3	89.5	74.0	44.8
5	20-30 minutes-loss of decay heat removal	0.03	0.3	0.8	2.2	7.2
6 & 7	10-20 minutes-loss of decay heat removal	0.0006	0.007	0.03	0.2	0.8
8	5-10 minutes-loss of decay heat removal	0.4	3.4	9.6	23.3	46.1
9	within 5 minutes-loss of decay heat removal	0.003	0.03	0.01	0.03	1.1

TABLE 5-XXIII

A List of the Dominant Accident Sequences According to Outcome Categories for Shutdowns due to Category II.A Initiating Events

OUTCOME CATEGORY 4: Only One CACS Loop Available 0 to 15 Minutes after the Shutdown					
Accident Sequence	Probability of a Loss of Decay Heat Removal (per shutdown)				
	β=0.0	β=0.003	β=0.01	β=0.03	β=0.1
CC2(A-L'-C2')	7×10^{-6}	← constant →			
Z2(A-S'-C2')	5×10^{-6}	"			
BB2(2S'-C2')	9×10^{-9}	2×10^{-8}	3×10^{-8}	9×10^{-8}	3×10^{-7}
V2(2L'-C2')	4×10^{-8}	5×10^{-8}	6×10^{-8}	1×10^{-7}	3×10^{-7}
DD2(F'-L'-C2')	5×10^{-8}	← constant →			
AA2(F'-S'-C2')	3×10^{-8}	3×10^{-8}	3×10^{-8}	3×10^{-8}	3×10^{-8}
CC6(L'-I'-C2')	2×10^{-8}	← constant →			
U2(L'-S'-C2')	2×10^{-8}	"			
Z14(S'-I'-C2')	1×10^{-8}	"			
Sum of all accident sequences for this category	1×10^{-5}	1×10^{-5}	1×10^{-5}	1×10^{-5}	1×10^{-5}

OUTCOME CATEGORY 8: Loss of Decay Heat Removal 5 to 10 Minutes after the Shutdown					
Accident Sequence	Probability of a Loss of Decay Heat Removal (per shutdown)				
	β=0.0	β=0.003	β=0.01	β=0.03	β=0.1
CC23(A-L'-C3')	3×10^{-8}	3×10^{-7}	8×10^{-7}	2×10^{-6}	8×10^{-6}
Z47(A-S'-C3')	2×10^{-8}	2×10^{-7}	6×10^{-7}	1×10^{-6}	5×10^{-6}
BB28(2S'-C3')	$<1\times10^{-10}$	6×10^{-10}	4×10^{-9}	3×10^{-8}	5×10^{-8}
DD41(F'-L'-C3')	1×10^{-10}	2×10^{-9}	5×10^{-9}	2×10^{-8}	5×10^{-8}
AA64(F'-S'-C3')	$<1\times10^{-10}$	1×10^{-9}	4×10^{-9}	1×10^{-8}	4×10^{-8}
Sum of all accident sequences for this category	5×10^{-8}	4×10^{-7}	1×10^{-6}	4×10^{-6}	1×10^{-5}

TABLE 5-XXIV
The Contribution of Individual Subsystem Test and Maintenance Unavailabilities For Shutdowns Due to Category II.A Initiating Events.

Subsystem Index and Name	T & M Unavailability Per Unit	Factor Change in the Probability of a Loss of Decay Heat Removal* T & M Unavailability included on Specific Subsystem Only.		
		Beta=0.01	Beta=0.03	Beta=0.1
10:Core Auxiliary Cooling System	$1.2X10^{-2}$	3.0	2.2	1.5
12:Resuperheater Bypass Control Valves	$2X10^{-3}$	1.3	1.3	1.3

* The core-melt probability considering equipment failures only is given in Table 5-XXI.

TABLE 5-XXV
The Sensitivity of the Subsystem Unit Reliability Values at Different Beta Factor Values for Shutdowns Due to Category II.A Initiating Events

Subsystem Index and Name	Subsystem Unit Reliability Sensitivity Range (low, high)	Factor Change in the Probability of a Loss of Decay Heat Removal		
		Beta=0.01	Beta=0.03	Beta=0.1
4:CT Large CV's	.99	2.1	2.0	2.0
	.9999	0.85	0.85	0.86
5:CT Small CV's	.97	4.2	4.2	4.0
	.9997	0.63	0.64	0.65
6:Shutdown Feedwater System	.96	1.0	1.1	1.2
	.9996	1.0	1.0	0.99
7:Auxiliary Boilers	.875	1.1	1.4	1.9
	.999	1.0	0.99	0.97
8: Main Loop Transfer to Decay Heat Removal Operation	.93	1.1	1.4	1.4
	.9993	1.0	0.99	0.97
10:Core Auxiliary Cooling System	.9	39.6	34.8	25.7
	.999	0.10	0.10	0.11
12: Resuperheater Bypass Control Valves	.99	2.1	2.0	2.0
	.9999	0.84	0.84	0.85

of the test and maintenance unavailability contributions showed that the major effect was due to CACS loop unavailability but that resuperheater bypass system unavailability also contributed. The test and maintenance unavailability contribution of these two subsystems is shown in Table 5-XXIV.

Table 5-XXV lists the sensitivities of the subsystem unit reliability values at the low, median and high beta factor values. Notice that the sensitivity of subsystems 4,5 & 12 do not change significantly as the fraction of common mode failures increases. This is due to their contribution to the accident sequences CC2(A-L'-C2') and Z2(A-S'-C2') which are not affected by common mode failures. The sensitivity of subsystems 6,7 & 8 is quite small over the entire range of beta factor values. The sensitivity of the CACS decreases as the beta factor value increases due to the decrease in the percentage of core meltdowns which occur in outcome category 4.

5.4 Losses of Offsite Power

5.4-1 Model of Events

Figure 5.14 is a simplified model of the reactor shutdown cooling operations in which the plant offsite power supply is initially unavailable. The reactor shutdown begins with three main loops available. However, the operation of the shutdown feedpumps is dependent upon the starting of their corresponding emergency diesel generators, and the auxiliary boilers which are

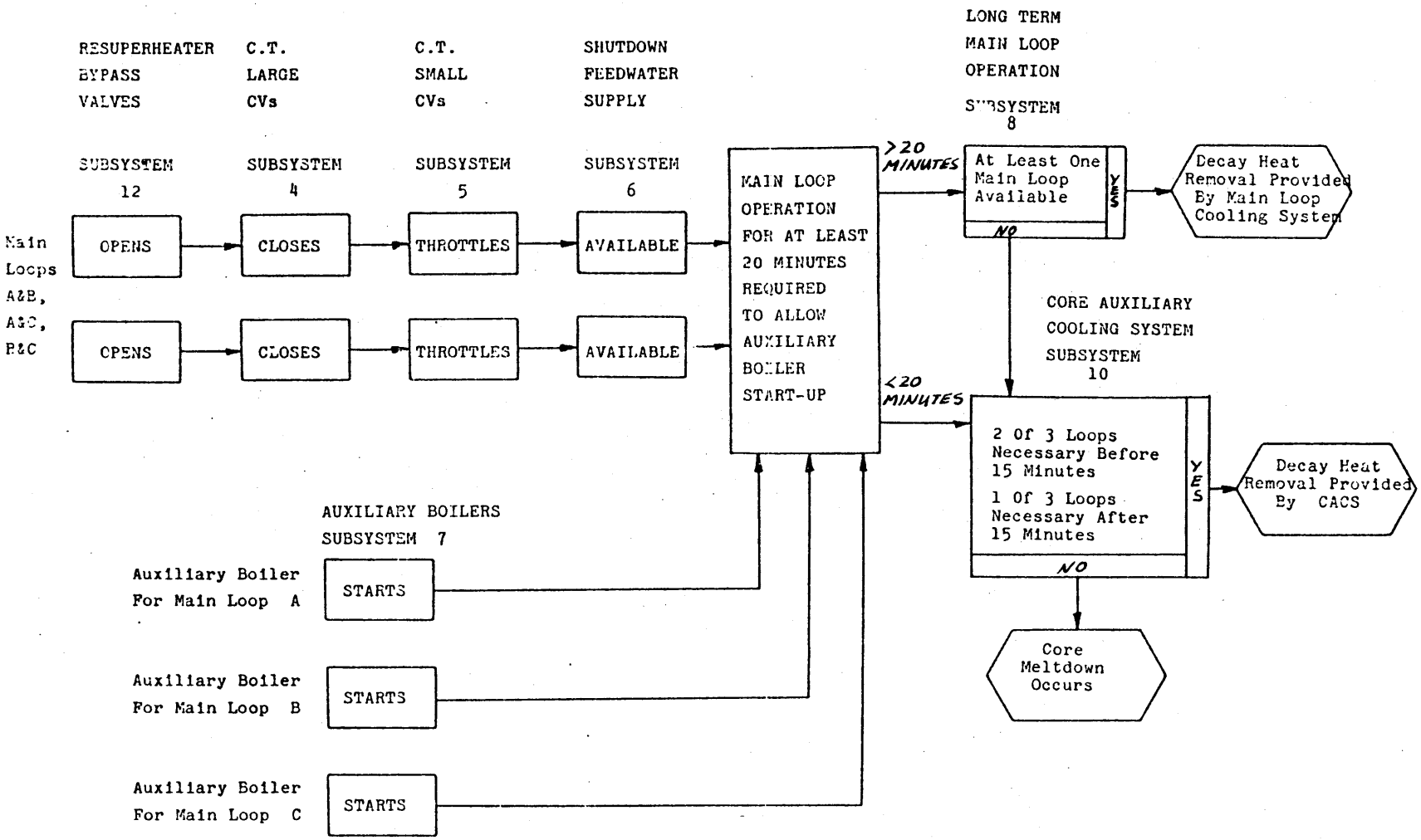


FIGURE 5.12 A Simple Diagram of a Reactor Shutdown Initiated By an Event Eliminating a Single Main Cooling Loop.

powered by the non-essential bus, are initially unavailable. Also, because main loop operation was assumed limited to 30 minutes due to steam generator inventory depletion, the auxiliary boilers cannot reach their rated operating conditions unless offsite power is restored within 5 to 10 minutes. Therefore, if offsite power is not restored early, the CACS must eventually take over core cooling, and the CACS operation is also dependent on the diesel generator performance.

Powering the auxiliary boiler electrical requirements from the essential buses is a possible design option which was explored in some detail. In the ESD, the auxiliary boilers were modelled so that they could be treated as being powered from either the essential buses or the non-essential bus. If the auxiliary boilers are powered from the essential buses, their availability is dependent on the operation of the emergency diesel generators, and long term main loop operation may occur even if offsite power is not restored. A model of the shutdown cooling operations for this design option is shown in Figure 5.15.

In the ESD modelling, the restoration of offsite power was assumed to have no effect on the main loops performance. This greatly facilitated the modelling of the two options of the auxiliary boiler operation. However, the effect of restoring offsite power on the main loop cooling system performance was considered in the analysis of the dominant accident sequences, and the final results do account for this effect.

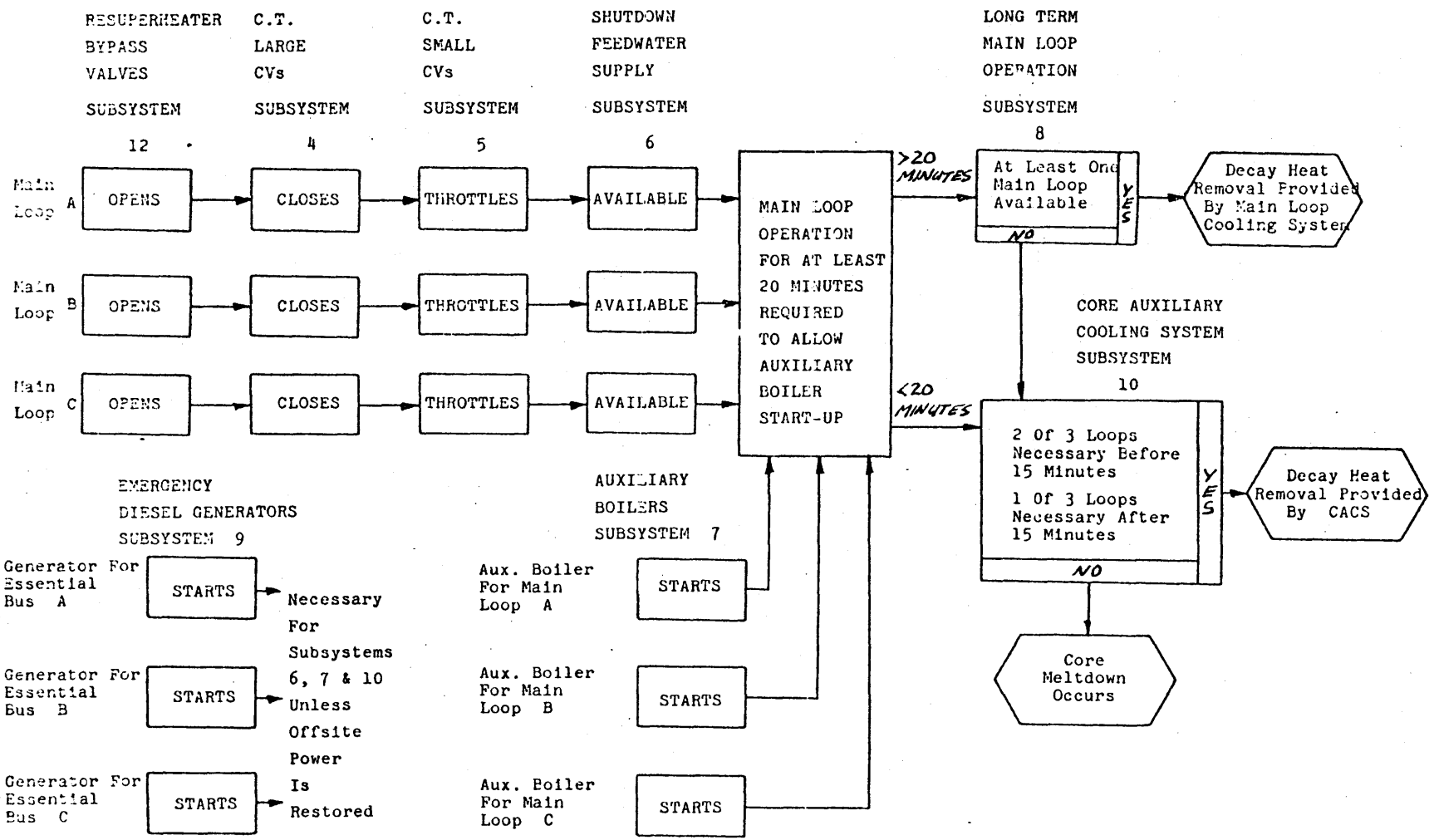


FIGURE 5.15 A Simple Diagram of the Reactor Shutdown Cooling Operations Following a Loss of Offsite Power With the Auxiliary Boilers Powered From the Essential Buses.

Specifically, for accident sequences named K, L and M, if offsite power is restored within 10 minutes following the shutdown, the auxiliary boilers will have sufficient time to reach their rated operating condition. The probability of offsite power being restored in this interval is about 0.6. This is also true for accident sequences named W and O if offsite power is restored within 5 minutes (probability 0.35). The probability of the dominant accident sequences with these index names was adjusted to account for the probability of not restoring offsite power in time to allow auxiliary boiler operation. Also, the accident sequence probability where offsite power is restored, was decreased by the failure probability of the auxiliary boilers.

5.4-2 Sensitivity of the Subsystem Unit Reliability Values

5.4-2-1 Auxiliary Boilers Powered From the Non-Essential Bus.

The sensitivities of the subsystem unit reliability values for shutdowns accompanied by the loss of offsite power are listed in Table 5-XXVI. The sensitivity values are the factor changes in the median value of the probability of a loss of decay heat removal due to changes in the subsystem unit reliability value. The table shows that only the emergency diesel generator reliability and the CACS reliability have any effect on the probability of a core meltdown.

The dominant accident sequences for this initiating event category are listed in Table 5-XXVII, and the median probability

TABLE 5-XXVI.
Core Meltdown Sensitivity to Subsystem Unit Reliability Values for Reactor Shutdowns Resulting From the Loss of Offsite Power

Subsystem Index and Name	Subsystem Unit Reliability Sensitivity Range (Low, High)	Factor Change in the Median Probability of a Loss of Decay Heat Removal*
4: CT Large CVs	.99 .9999	1.0 1.0
5: CT Small CV's	.97 .9997	1.0 1.0
6: Shutdown Feed-water System	.96 .9996	1.0 1.0
7: Auxiliary Boilers	.875 .999	1.0 1.0
8: Main Loop Transfer to Decay Heat Removal Operation	.93 .9993	1.0 1.0
9: Emergency Electrical Supply	.9 .997	3.1 0.47
10:Core Auxiliary Cooling System	.9 .999	8.3 0.61
12:Resuperheater bypass control valves	.99 .9999	1.0 1.0

*5×10^{-4} per shutdown based on median subsystem reliability values.

TABLE 5-XXVII.
A List of the Dominant Accident Sequences for Shutdowns Due to the Loss of Offsite Power

Accident Sequence	ESD Outcome Category	Probability of a Loss of Decay Heat Removal Per Shutdown
N22(3A-3B'-R15')	6	3×10^{-4}
K3(3A-R10'-C3')	5	1×10^{-4}
L8(3A-B'-R30-C3')	5	2×10^{-5}
M17(3A-2B'-R30'-C3')	5	1×10^{-5}
L10(3A-B'-R30'-C3')	5	7×10^{-6}
M19(3A-2B'-R30'-SS'-C3')	5	6×10^{-6}
Y55(2A-L'-3B'-R10')	7	5×10^{-6}
L3(2A-F'-R10'-C3')	5	3×10^{-6}
W3(2A-L'-R10'-C3')	5	2×10^{-6}
03(2A-S'-R10'-C3')	5	2×10^{-6}
M15(3A-2B'-R30-C3')	5	7×10^{-7}
V4(3L'-B'-C2')	4	3×10^{-7}
V5(3L'-2B'-C2')	4	3×10^{-7}
X36(A-L'-I'-B'-R5'-C2')	4	3×10^{-7}
T6(3S'-B'-R10'-C2')	4	3×10^{-7}
T9(3S'-2B'-R10'-C2')	4	2×10^{-7}
Y39(A-L'-I'-2B'-R5'-C2')	4	2×10^{-7}
N21(3A-3B'-R15-C3')	6	2×10^{-7}
M8(2A-F'-B'-R30-C3')	5	2×10^{-7}
X19(2A-L'-B'-R30-C3')	5	2×10^{-7}
Sum of all accident sequences for this initiating event category		5×10^{-4}

of a loss of decay heat removal is 5 X 10^{-4} per shutdown. For the most dominant accident sequence, sequence N22(3A-3B'-R15'), main loop operation was assumed limited to 15 minutes due to inadequate throttling of the CT small CV's. These valves are dependent on the instrument air supply which requires essential electric power. Offsite power restoration was assumed to have a minimal effect on main loop performance for this accident sequence because the initial steam generator depletion limits main loop operation even though instrument air is also restored. But, if each of the valves were equipped with air accumulators containing enough air for the full thirty minutes of main loop operation, the restoration of offsite power within 10 minutes following shutdown would allow auxiliary boiler operation for this sequence. Also, the restoration of offsite power within 30 minutes (probability 0.75) rather than 15 minutes (0.65) would reduce the accident sequence probability. Given these changes, the adjusted probability of accident sequence N22 would be 2 X 10^{-4}, and this would reduce the median probability of a loss of decay heat removal to 4 X 10^{-4} per shutdown.

The sensitivity plots of the emergency diesel generators and the CACS are included in Figures 5.16 and 5.17 respectively. From the CACS sensitivity plot, it can be seen that increasing the reliability of an auxiliary loop to .9943 by having redundant air cooler fans would decrease the probability of a core meltdown to just over 4 X 10^{-4} per shutdown.

With the auxiliary boilers powered by the non-essential bus,

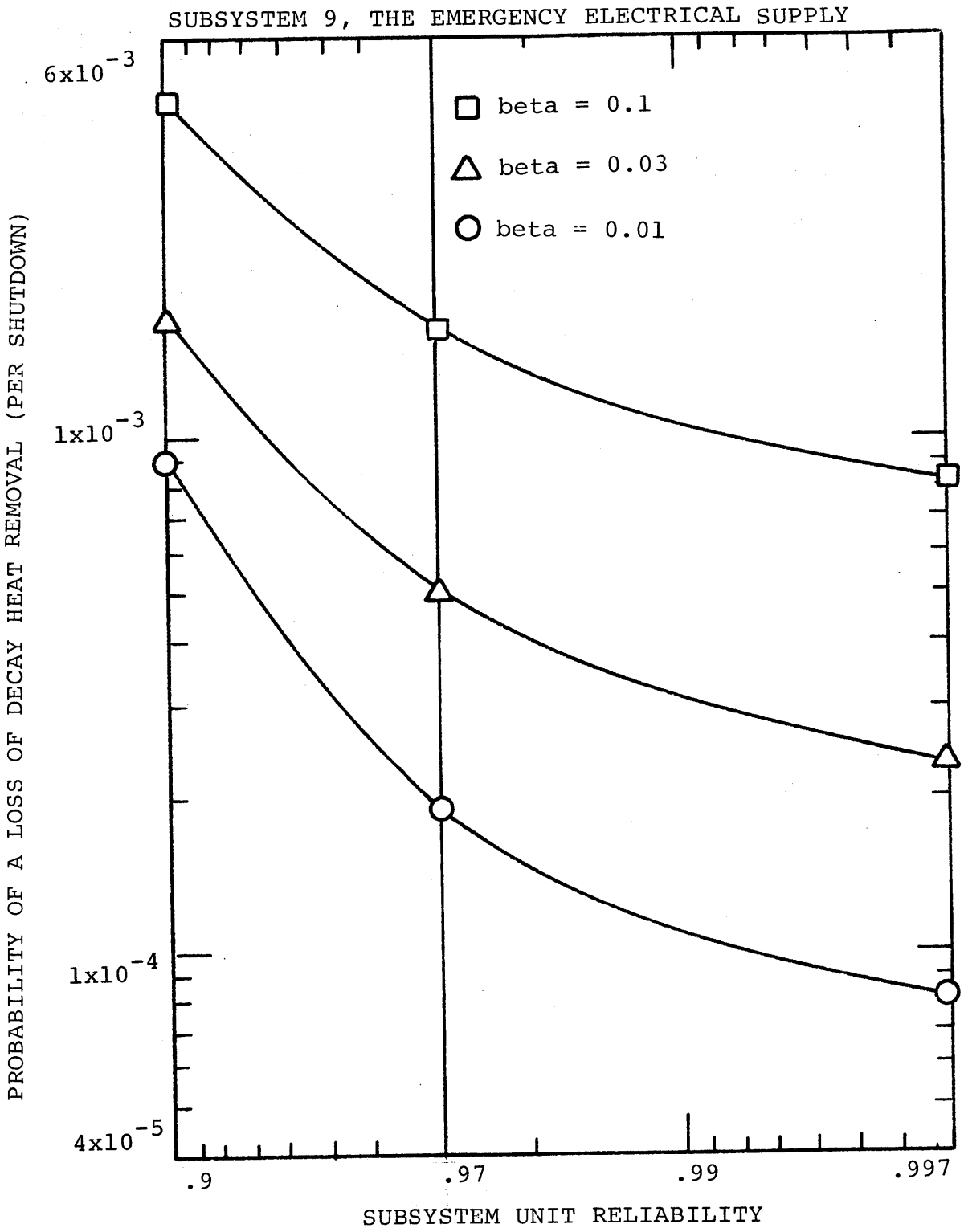


FIGURE 5.16 Sensitivity plot of subsystem 9 for shutdowns due to the loss of offsite power

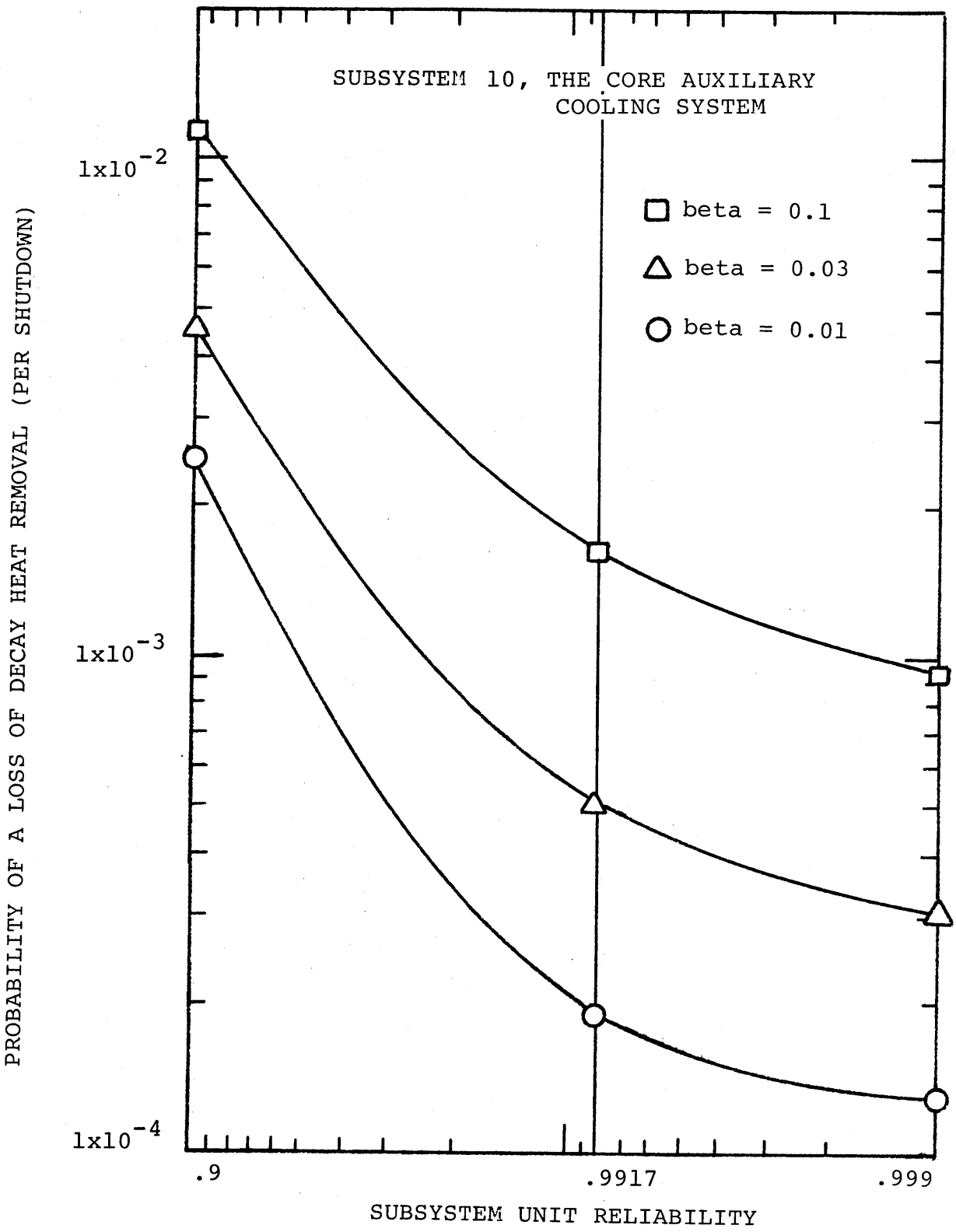


FIGURE 5.17 Sensitivity plot of subsystem 10 for shutdowns due to the loss of offsite power

only the diesel generator reliability and the CACS reliability have any effect on the median probability of a loss of decay heat removal. This is due to the dominance of accident sequences N22(3A-3B'-R15') and K3(3A-R10'-C3') which only involve diesel and CACS failures. It is not surprising then that the main loop isolation valve and circulator operating reliability during circulator imbalance conditions has no effect on the median probability of a core meltdown. Neither does the restarting of initially failed shutdown feedpumps. However, the restarting of initially failed diesel generators does affect the core-melt probability for this initiating event category.

The changes in the probability of a loss of decay heat removal is listed in Table 5-XXVIII for different probabilities of restarting initially failed diesel generators. An investigation of diesel generator failure data [1] showed that 63% of the reported failures were due to failure of the diesel system to start. Of these starting system failures, 52% were judged by this author to be of a nature which would easily be repairable within 10 to 15 minutes. Thus, the probability that an initially failed diesel could be restarted might be as high as 0.3. However, this assumes that the fault can be properly identified within this time period, and that the effort is actually made by an operator to attempt to restart a failed diesel following the reactor shutdown. The Table shows that a 10% likelihood of restarting any initially failed diesel has a negligible effect on the probability of a core meltdown. A 30% likelihood has a slight effect

TABLE 5-XXVIII
The Effect of Restarting Initially Failed Diesel Generators for Reactor Shutdowns Due to the Loss of Offsite Power

Probability of Restarting Initially Failed Diesel Generators Given at Least 10 Minutes (3 of 3 failed, 2 of 3 failed, 1 of 3 failed)	Factor Change in the Probability of a Loss of Decay Heat Removal
1.0 1.0 1.0	.44
.75 .60 .30	.82
.25 .20 .10	.94

and even the limiting case of starting all initially failed diesels allowed by the model, only changes the median probability by a factor of 0.44.

5.4-2-2 Auxiliary Boilers Powered From the Essential Buses.

The median probability of a loss of decay heat removal for reactor shutdowns following a loss of offsite power, if the auxiliary boilers are powered from the essential buses, is 3×10^{-4} per shutdown. The dominant accident sequences are listed in Table 5-XXIX. Notice that in this case, accident sequence N22 is almost two orders of magnitude greater than the next accident sequence. The only subsystem reliability value with any effect on the probability of a core meltdown is the emergency diesel generator reliability. The probability of a loss of decay heat removal is also sensitive to the main loop operating performance with no essential power available. The probability of accident sequence N22 and the median probability of a core meltdown would decrease to 2×10^{-4} if main loop operation for the full thirty minutes were possible with no essential power available.

Table 5-XXX lists the percentage of the core-melt probability due to accident sequences which occur in the various ESD outcome categories for both cases in which the auxiliary boilers are powered by the non-essential bus or by the essential buses. In both cases, almost 98% of the meltdowns occur between 15 and 30

TABLE 5-XXIX.
A List of the Dominant Accident Sequences for Shutdowns Due to the Loss of Offsite Power With the Auxiliary Boilers Powered From the Essential Buses

Accident Sequence	ESD Outcome Category	Probability of a Loss of Decay Heat Removal Per Shutdown
N22(3A-3B'-R15')	6	3×10^{-4}
M19(3A-2B'-R30'-SS'-C3')	5	6×10^{-6}
Y55(2A-L'-3B'-R10')	7	5×10^{-6}
M17(3A-2B'-Y'-R30-C3')	5	5×10^{-7}
V4(3L'-B'-C2')	4	3×10^{-7}
V5(3L'-2B'-C2')	4	3×10^{-7}
T6(3S'-B'-R10'-C2')	4	3×10^{-7}
X36(A'-L'-I'-B'-R5'-C2')	4	3×10^{-7}
T9(3S'-2B'-R10'-C2')	4	2×10^{-7}
Y39(A-L'-I'-2B'-R5'-C2')	4	2×10^{-7}
N21(3A-3B'-R15'-C3')	6	2×10^{-7}
N14(2A-F'-2B'-R30'-C3')	5	1×10^{-7}
K3(3A-X'-C3')	5	1×10^{-7}
AA49(F'-L'-S'-2B'-R5'-C2')	4	1×10^{-7}
022(A-S'-I'-2B'-R5'-C2')	4	1×10^{-7}
025(A-S'-I'-2B'-R5'-C2')	4	1×10^{-7}
X32(2A-L'-2B'-R30'-SS'-C3')	5	6×10^{-8}
L8(3A-B'-X'-R30'-C3')	5	2×10^{-8}
M15(3A-2B'-X'-R30'-C3')	5	2×10^{-8}
Sum of all accident sequences for this initiating event category with the auxiliary boilers powered from the essential buses		3×10^{-4}

TABLE 5-XXX.
A List of the Calculated Percent of Core Meltdowns
Occurring in Different Time Intervals Following Shutdowns
Due to the Loss of Offsite Power

ESD Outcome Category	Time Interval Following Shutdown in Which Meltdown is Assumed to Occur	Percent of Core Meltdowns	
		Aux. Boilers on Essential Buses	Aux. Boilers on Non-Essential Bus
4	0-15 minutes-only one CACS loop available	0.9	0.5
5	20-30 minutes-loss of decay heat removal	0.3	44.6
6	15-20 minutes-loss of decay heat removal	97.1	53.1
7	10-15 minutes-loss of decay heat removal	1.6	0.9
8	5-10 minutes-loss of decay heat removal	0.1	0.1
9	within 5 minutes-loss of decay heat removal	0.03	0.02

minutes. With the auxiliary boilers powered by the non-essential bus, less than half the core-melt probability is due to accident sequences which occur in the 20 to 30 minute interval involving combinations of emergency diesel and CACS loop failures. The remainder is due to accident sequences involving the common mode failure of the diesels. With the auxiliary boilers powered from the essential buses, the core-melt probability is dominated entirely by accident sequences involving the common mode failure of the diesels.

If the auxiliary boilers are powered by the essential buses, the diesel generator reliability is the dominating factor contributing to the probability of a core meltdown. Figure 5.18 is the sensitivity plot for the diesel generators for this design option. The probability of a core meltdown is also sensitive to restarting initially failed diesel generators. Table 5-XXXI shows the factor change in the median probability of a core meltdown for different probabilities of successfully restarting initially failed diesels. The impact of this possibility is slightly larger than in the case where the auxiliary boilers are powered from the non-essential bus. This is due to the fact that some diesel restarts will also allow auxiliary boiler operation. A 10% probability of successfully restarting an initially failed diesel has a negligible effect while at 30% probability has a slight effect. However, the limiting case of restarting all initially failed diesels allowed by the model has a very significant impact. This limiting case again emphasizes

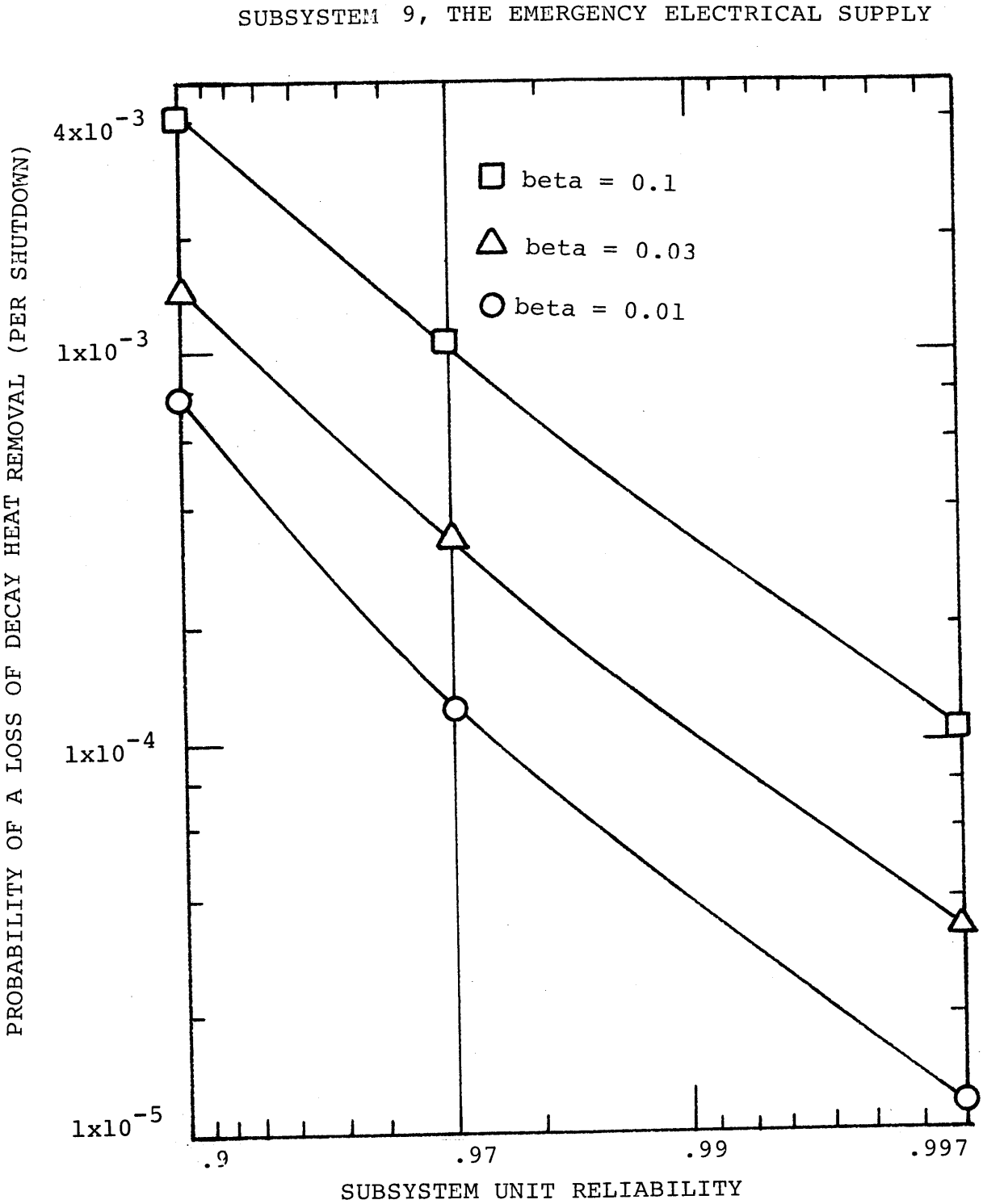


FIGURE 5.13 Sensitivity plot of subsystem 9 for shutdowns due to the loss of offsite power with the auxiliary boilers powered from the essential buses

TABLE 5-XXXI.
The Effect of Restarting Initially Failed Diesel Generators for Shutdowns Due to the Loss of Offsite Power With the Auxiliary Boilers Powered from the Essential Buses

Probability of Restarting Initially Failed Diesel Generators Given at Least 10 Minutes	Factor Change in the Probability of a Loss of Decay Heat Removal
1.0 1.0 1.0	0.06
.75 .60 .30	0.71
.25 .20 .10	0.90

the importance of the diesel generators for this design option following a loss of offsite power.

5.4-2-3 Restoration of Offsite Power

The effect of offsite power restoration was investigated by assuming two limiting cases. First, that offsite power is not restored within the thirty minute main loop operating period; and second, that offsite power is restored within 5 minutes of the reactor shutdown. The probability of a loss of decay heat removal for these two cases was 1×10^{-3} per event and 2×10^{-6} per event respectively.

Table 5-XXXII lists the dominant accident sequences for the case of no offsite power restoration. The dominant contributions to the probability of a core meltdown are the common mode failure of the diesel generators followed by the common mode failure of the CACS.

Table 5-XXXIII lists the dominant accident sequences for the case in which offsite power is restored in 5 minutes. The availability of the auxiliary boilers reduces the accident sequence probability for many of the sequences, and the list of dominant sequences begins with the sequences in which offsite power restoration makes no difference to the main loop performance. The first two accident sequences involve common mode failure of the CT large CV's. These eliminate the main loops in about two minutes. In the next three accident sequences, main loop operation is limited to less than 25 minutes. Thus,

Table 5-XXXII

A List of the Dominant Accident Sequences For Shutdowns Due to the Loss of Offsite Power if no Restoration Occurs in the 30 Minute Main Loop Operating Period

Accident Sequence	ESD Outcome Category	Probability of a Loss of Decay Heat Removal Per Shutdown
N22(3A-3B')	6	9×10^{-4}
K3(3A-C3')	5	2×10^{-4}
M17(3A-2B'-C3')	5	7×10^{-5}
L10(3A-B'-C3')	5	5×10^{-5}
Y55(2A-L'-3B')	7	1×10^{-5}
M19(3A-2B'-SS'-C3')	5	6×10^{-6}
L3(2A-F'-C3')	5	4×10^{-6}
W3(2A-L'-C3')	5	3×10^{-6}
O3(2A-S'-C3')	5	2×10^{-6}
X30(2A-L'-2B'-C3')	5	7×10^{-7}
M10(2A-F'-B'-C3')	5	7×10^{-7}
N14(2A-F'-2B'-C3')	5	5×10^{-7}
P21(2A-S'-2B'-C3')	5	5×10^{-7}
X21(2A-L'-B'-C3')	5	5×10^{-7}
T6(3S'-B'-C2')	4	4×10^{-7}
X36(A-L'-I'-B'-C2')	4	4×10^{-7}
T9(3S'-2B'-C2')	4	3×10^{-7}
Y39(A-L'-I'-2B'-C2')	4	3×10^{-7}
V4(3L'-B'-C2')	4	3×10^{-7}
V5(3L'-2B'-C2')	4	3×10^{-7}
Sum of all accident sequences for this initiating event category		1×10^{-3}

TABLE 5-XXXIII.
A List of the Dominant Accident Sequences For Shutdowns due to the Loss of Offsite Power if Restoration Occurs Within 5 Minutes Following the Shutdown

Accident Sequence	ESD Outcome Category	Probability of a Loss of Decay Heat Removal Per Shutdown
V4(3L'-B'-C2')	4	3×10^{-7}
V5(3L'-2B'-C2')	4	3×10^{-7}
X19(2A-L'-B'-R-C3')	5	2×10^{-7}
P28(2A-S'-B'-R-C3')	5	2×10^{-7}
N21(3A-3B'-R-C3')	6	2×10^{-7}
W14(2A-L'-B'-R-C3')	5	1×10^{-7}
K3(3A-R-X'-C3')	5	1×10^{-7}
014(2A-S'-B'-R-C3')	5	8×10^{-8}
V7(3L'-3B')	9	8×10^{-8}
T2(3S'-C2')	4	7×10^{-8}
W9(A-L'-I'-C2')	4	7×10^{-8}
Z2(A-L'-S'-C2')	4	6×10^{-8}
V2(3L'-C2')	4	6×10^{-8}
CC2(A-2L'-C2')	4	4×10^{-8}
X3(A-L'-F'-C3')	5	4×10^{-8}
P3(A-S'-F'-C3')	5	3×10^{-8}
09(A-S'-I'-C2')	4	3×10^{-8}
M3(A-2F'-C3')	5	2×10^{-8}
N2(3F'-C3')	5	2×10^{-8}
T14(3S'-C3')	8	2×10^{-8}
W23(A-L'-I'-C3')	8	2×10^{-8}
Z47(A-L'-S'-C3')	8	2×10^{-8}
V8(3L'-C3')	9	2×10^{-8}
R2(A-2S'-C2')	4	2×10^{-8}
Sum of all accident sequences for this initiating event category		2×10^{6}

the auxiliary boilers do not have sufficient time to become available.

5.4-3 Sensitivity to Common Mode Failures and Test and Maintenance Unavailabilities

The variation in the probability of a loss of decay heat removal due to both the fraction of common mode failures and test and maintenance unavailabilities is listed in Table 5-XXXIV and plotted in Figure 5.19. From these, it can be seen that for beta factor values greater than 0.01, test and maintenance unavailabilities make a negligible contribution to the probability of a core meltdown for this initiating event category. Notice also, that for beta factor values greater than 0.01, the probability of a core meltdown increases proportionally with the beta factor. This is due to the dominance of accident sequences N22(3A-3B'-R15') and K3(3A-R10'-C3') which involve common mode failures of the diesel generators and the CACS.

Table 5-XXXV lists the percent of the core-melt probability due to accident sequences occurring in each ESD outcome category for the different beta factor valves. The relatively small contribution of outcome category 4 (only one CACS loop available prior to 15 minutes following the shutdown) explains the unimportance of test and maintenance unavailabilities. Also, meltdowns occurring between 15 and 30 minutes following the shutdown account for over 95% of the total probability over the entire range of beta factor values.

TABLE 5-XXXIV.
A List of the Core Meltdown Probabilities Considering Equipment Failures Only, and all Failure Contributions for Shutdowns Due to the Loss of Offsite Power

Intrasystem Common Mode Failure Fraction (Beta Factor)	Probability of a Loss of Decay Heat Removel (Per Shutdown)	
	Equipment Failures Only	Equipment Failures and Test and Maintenance Unavailabilities
0.0	2×10^{-5}	4×10^{-5}
0.003	7×10^{-5}	1×10^{-4}
0.01	2×10^{-4}	2×10^{-4}
0.03	5×10^{-4}	5×10^{-4}
0.1	2×10^{-3}	2×10^{-3}

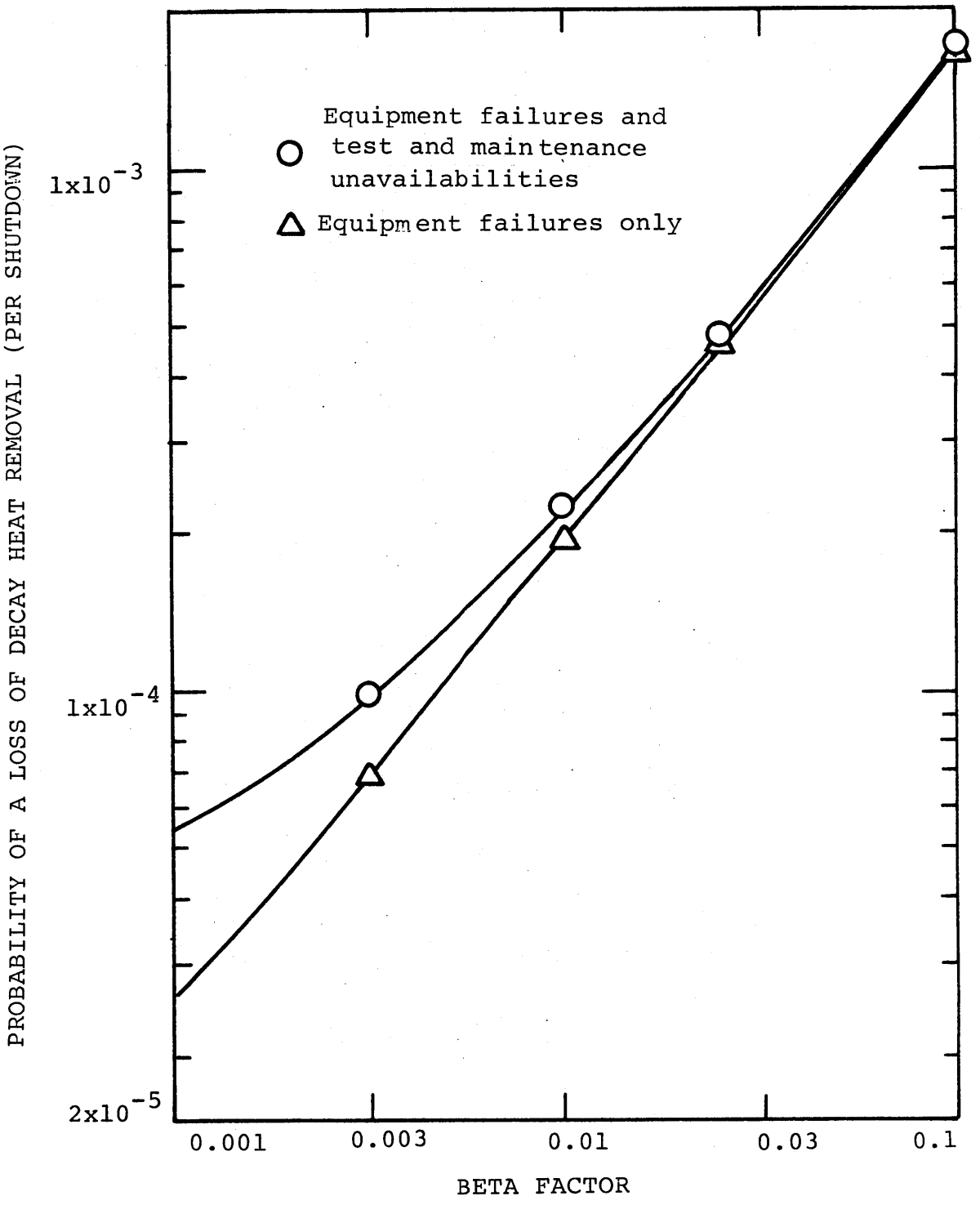


FIGURE 5.19 Probability of a core meltdown due to the loss of offsite power

TABLE 5-XXXV
A List of the Calculated Percent of Core Meltdowns Occuring in Different Time Intervals Following Shutdowns Due to the Loss of Offsite Power. For Different Beta Factor Values

ESD Outcome Category	Time Interval Following Shutdown in Which Meltdown is Assumed to Occur	Percent of Core Meltdowns				
		β=0.0	β=0.003	β=0.01	β=0.03	β=0.1
4	0 to 15 minutes only one CACS loop available	3.7	1.8	0.9	0.5	0.3
5	20 to 30 minutes-loss of decay heat removal	62.5	52.3	47.7	44.6	44.4
6	15 to 20 minutes-loss of decay heat removal	33.2	45.2	50.6	53.1	54.2
7	10 to 15 minutes-loss of decay heat removal	0.5	0.7	0.8	0.9	0.9
8	5 to 10 minutes-loss of decay heat removal	0.1	0.1	0.1	0.1	0.1
9	within 5 minutes-loss of decay heat removal	0.0001	0.001	0.01	0.02	0.06

TABLE 5-XXXVI.
A List of the Individual Subsystem Common Mode Failure Contributions at High and Low Beta Factor Values for Shutdowns Due to the Loss of Offsite Power

Subsystem Index and Name	Individual Subsystem Beta Factor Value	Factor Change in the Median Probability of a Loss of Decay Heat Removal
9: Emergency Electrical Supply	0.01 0.1	0.65 2.2
10:Core Auxiliary Cooling System	0.01 0.1	0.73 2.0

TABLE 5-XXXVII.
A List of the Sensitivity of the Subsystem Unit Reliability Values at Different Beta Factor Values for Shutdowns Due to the Loss of Offsite Power.

Subsystem Index and Name	Subsystem Unit Reliability Sensitivity Range	Factor Change in the Probability of a Loss of Decay Heat Removal		
		β=0.01	β=0.03	β=0.1
9: Emergency Electrical Supply	.9 .997	4.4 0.43	3.1 0.47	2.6 0.49
10:Core Auxiliary Cooling System	.9 .999	12.2 0.62	8.3 0.61	6.7 0.61

The investigation of individual subsystem common mode failure contribution showed that only common mode failures of the diesel generators and the CACS were significant. The factor change on the median probability of a loss of decay heat removal due to changes in the individual subsystem beta factor valves is listed in Table 5-XXXVI.

Table 5-XXXVII lists the variation in the sensitivity of the diesel generator and CACS unit reliability values due to changes in the beta factor valve. As beta increases, the sensitivity of both subsystems decreases. This is due to the dependence of the CACS on diesel generator operation, and to their relatively equal contributions to the probability of a core meltdown. As the fraction of common mode failures increases, the effect of changing the reliability of either system alone decreases due to the dominating effect of the common mode failure of the other subsystem.

5.5 PCRV Depressurization Accidents

5.5-1 Model of Events

In the analysis of the potential accident sequences due to PCRV depressurization accidents, two specific types of accident were considered. For large PCRV leaks involving one of the steam generator cavity closures, the main loop associated with the closure was assumed to be eliminated. The reactor shutdown cooling operations are then performed with only two

main loops initially available, and a simplified model of these events would be similar to that of Figure 5.12. For all other PCRV leaks, all three main loops were considered to be available, and a model of the shutdown cooling operations would be similar to that of Figure 5.1.

The major difference in the modelling of the reactor shutdown cooling operations following a depressurization accident is due to the effect of the decreased helium density on the design capabilities of the main loops and the CACS. After the depressurization is complete, the helium density is determined by the containment equalization pressure. Three ranges of containment equalization pressure were chosen, and the main loop and CACS capabilities were modelled according to the guidelines discussed in Chapter 3.

Also, losses of offsite power concurrent with the PCRV depressurization accident were considered. The loss of offsite power may occur due to the transient to the electrical network produced by the turbine trip which accompanies the shutdown. This occurrence was discussed in Chapter 4, and for the analyses of shutdowns following depressurization accidents, a probability of 1×10^{-3} per event was conservatively assumed.

5.5-2 Sensitivity to the Subsystem Unit Reliability Valves

Offsite Power Available

The median probability of a loss of decay heat removal for shutdowns following a depressurization accident with offsite power available was determined to be 9×10^{-7} per event

if three main loops are initially available. If only two main loops are initially available, the median probability is 2×10^{-5} per event. The dominant accident sequences for each of these types of accident are listed in Tables 5-XXXVIII and 5-XXXIX respectively.

With three main loops initially available, the first four accident sequences consist of a common mode failure of a main loop subsystem followed by the failure of the CACS. Notice also, the two sequences DY10 and DQ10. For these accident sequences, main loop operation is limited due to the low containment equalization pressure, and the probability of CACS failure is increased due to the more stringent operating requirements.

With only two main loops available, the two most dominant sequences involve main loop failures eliminating one of the loops. Because a single main loop is not capable of core cooling following a depressurization, these failures lead to an early dependence on the CACS.

Table 5-XL lists the percentage of the core-melt probability due to accident sequences in the various time intervals following the reactor shutdown. With three main loops available, over 25% of the meltdowns would occur in the 20 to 30 minute time interval. The remainder occur mostly within 5 minutes of the shutdown. However, if only two main loops are initially available, almost 98% of the meltdowns occur within the first five minutes following shutdown.

It is interesting that the probability of a loss of decay

heat removal following a depressurization accident, is not greatly different from that of shutdowns in which the reactor is pressurized. Core temperatures will generally be higher following shutdown due to a depressurization accident, and some core damage is more likely to occur. However this analysis shows that the present shutdown cooling system design is quite effective in preventing a core meltdown in both a pressurized and a depressurized reactor.

Table 5-XLI lists the factor change in the median probability of a core meltdown due to changes in the subsystem unit reliability values. In both cases (three main loops initially available, and two main loops initially available), the probability of a core meltdown is most affected by changes in the CACS reliability. It is interesting that the sensitivities of the subsystem reliability values follow the same trends as for pressurized reactor shutdowns with three or two main loops initially available. Notice also, that the reliability of the main loop isolation valves to close following main loop failure is included in the table. Isolation valve failures affect the CACS performance by allowing core bypass flow. However, they do not contribute significantly to the probability of a core meltdown.

There are two other items which need to be discussed in this section. The first is the probability that a CACS loop failure may lead to bypass flow through that loop. This was assumed to have a probability of 1×10^{-4} per CACS loop per

TABLE 5-XXXVIII.
A List of the Dominant Accident Sequences for Reactor Shutdowns Due to a Depressurization Accident With Three Main Loops Initially Available

Accident Sequence	ESD Outcome Category	Probability of a Loss of Decay Heat Removal Per Shutdown
DK3(3A-CP1-X'-C3')	D4	1×10^{-7}
DT2(3S'-CP1-C3')	D7	1×10^{-7}
DV2(3L'-CP1-C3')	D7	1×10^{-7}
DN2(3F'-CP1-C3')	D4	1×10^{-7}
DZ2(A-L'-S'-CP1-C3')	D7	1×10^{-7}
DY10(2A-L'-CP3-C3')	D7	9×10^{-8}
DQ10(2A-S'-CP3-C3')	D7	6×10^{-8}
DC2(A-2L'-CP1-C3')	D7	6×10^{-8}
DK10(3A-CP1-SS'-C3')	D6	6×10^{-8}
DR2(A-2S'-CP1-C3')	D7	3×10^{-8}
DK8(3A-CP3-SS'-C3')	D6	1×10^{-8}
DL3(2A-F'-CP1-X'-C3')	D4	6×10^{-9}
DT4(3S'-CP2-C3')	D7	5×10^{-9}
DV4(3L'-CP2-C3')	D7	4×10^{-9}
DW3(2A-L'-CP1-X'-C3')	D4	4×10^{-9}
D03(2A-S'-CP1-X'-C3')	D4	3×10^{-9}
DB2(L'-2S'-CP1-C3')	D7	2×10^{-9}
DY2(L'-2F'-CP1-C3')	D7	2×10^{-9}
Sum of all accident sequences for this initiating event		9×10^{-7}

TABLE 5-XXXIX.
A List of the Dominant Accident Sequences for Reactor Shutdowns Due to Depressurization Accidents With Only Two Main Loops Initially Available

Accident Sequence	ESD Outcome Category	Probability of a Loss of Decay Heat Removal Per Shutdown
DC2(A-L'-CP1-C3')	D7	1×10^{-5}
DZ2(A-S'-CP1-C3')	D7	7×10^{-6}
DY10(2A-CP3-C3')	D7	6×10^{-6}
DW3(2A-CP1-X'-C3')	D4	3×10^{-7}
DB2(2S'-CP1-C3')	D7	1×10^{-7}
DV2(2L'-CP1-C3')	D7	1×10^{-7}
DX3(A-F'-CP1-X'-C3')	D4	1×10^{-7}
DY2(2F'-CP1-C3')	D5	1×10^{-7}
DC6(A-L'-CP3-C3')	D7	6×10^{-8}
DZ6(2L'-CP3-C3')	D7	4×10^{-8}
DU2(L'-S'-CP1-C3')	D7	4×10^{-8}
DC4(A-L'-CP2-C3')	D7	1×10^{-8}
DX5(A-F'-CP2-C3')	D5	1×10^{-8}
DW10(2A-CP2-SS'-C3')	D6	1×10^{-8}
DW8(2A-CP1-SS'-C3')	D6	1×10^{-8}
Sum of all accident sequences for this initiating event		2×10^{-5}

TABLE 5-XL
A List of the Calculated Percentage of Core Meltdowns
Occuring in Various Time Intervals Following Shutdowns
Due to PCRV Depressurization Accidents.*

ESD Outcome Category	Time Interval Following Shutdown in Which Meltdown is Assumed to Occur	Percent of Core Meltdowns	
		Two Main Loops Initially available	Three Main Loops Initially Available
D4	20 to 30 minutes-loss of decay heat removal	1.6	25.6
D5	10 to 20 minutes-loss of decay heat removal	0.5	0.3
D6	5 to 10 minutes-loss of decay heat removal	0.1	8.0
D7	within 5 minutes-loss of decay heat removal	97.8	66.1

* Offsite power available following the shutdown

TABLE 5-XLI.
A List of the Sensitivity of the Subsystem Unit Reliability Valves for Reactor Shutdowns Following PCRV Depressurization Accidents

Subsystem Index and Name	Subsystem Unit Reliability Sensitivity Range (Low, High)	Factor Change in the Probability of a Loss of Decay Heat Removal*	
		Two Main Loops Initially Available	Three Main Loops Initially Available
4:CT Large CVS	.99	1.8	2.4
	.9999	0.89	0.85
5:CT Small CVS	.97	3.4	6.9
	.9997	0.73	0.66
6:Shutdown Feedwater System	.96	1.2	2.9
	.9996	1.0	0.89
7:Auxiliary Boilers	.875	1.2	3.1
	.999	0.99	0.93
8:Main Loop Transfer to Decay Heat Removal Operation	.93	1.1	1.9
	.9993	0.99	0.95
10:Core Auxiliary Cooling System	.9	26.1	23.0
	.999	0.27	0.28
12:Resuperheater Bypass Control Valves	.99	1.8	2.3
	.9999	0.88	0.84
D18:Main Loop Isolation Valves	.99	1.3	1.6
	.9999	0.97	0.95

* Based on median subsystem unit reliability values

shutdown. Mechanistically, it was felt that this occurrence would require the starting of an auxiliary circulator, in order to open the auxiliary loop isolation value, and then the subsequent circulator failure and isolation valve failure. However, this was not a significant contributor to the core-melt probability, and increasing the probability of this event to 1×10^{-2} per loop changed the median probability of a core meltdown in either case by at most a factor of 1.3.

The second item to be discussed is the operating reliability of the main circulators near their overspeed trip setpoint. The circulator overspeed control/protection device has not yet been designed. Also, just how close the circulator speed will come to the overspeed trip set point for certain accident sequences is unknown. Therefore, a term was included in the analysis which simulated main loop failure for accident sequences where the main circulators were operating near the overspeed trip setpoint. It was the author's estimate that the probability that the main loops would survive this operating condition was 0.99. The sensitivity analysis showed this to be a small contributor to the core-melt probability. A decrease in the probability of main loop survival to 0.9 only changed the probability of a core meltdown by a factor of 1.6. Likewise, increasing the main loop survival probability to 0.999 changed the median probability of a core meltdown by a factor of 0.93. Thus, this particular assumption concerning circulator reliability does not have a significant effect on the core-melt probability for this initiating

event category.

Offsite Power Unavailable

The contribution to the probability of a core meltdown due to a simultaneous PCRV depressurization accident and loss of offsite power was also investigated. Offsite power may be lost concurrent with a depressurization accident due to the transient in the electrical network caused by the turbine trip which accompanies the reactor shutdown. A list of the dominant accident sequences for this event is shown in Table 5-XLII.

With three main loops initially available, the median probability of a core meltdown due to this particular event is 9×10^{-7} per shutdown. The two most dominant accident sequences are DN39 and DK3 which involve common mode failures in the emergency diesel generators and CACS respectively. Including these accident sequences along with those listed in Table 5-XXXVII yields a median probability of 2×10^{-6} per shutdown for the loss of decay heat removal following a depressurization accident with three main loops initially available.

It is interesting that core-melt accident sequences due to the concurrent loss of offsite power are so significant for this depressurization accident. It indicates the dependence of the shutdown cooling systems on essential electric power.

If only two main loops are initially available, the contribution of core meltdowns due to the concurrent loss of offsite power is not very significant. The two most dominant

TABLE 5-XLII.
A List of the Dominant Accident Sequences for PCRV Depressurization Accidents and the Concurrent Loss of Offsite Power

Three Main Loops Initially Available

Accident Sequence	ESD Outcome Category	Probability of a Loss of Decay Heat Removal Per Shutdown
DN39(3A-3B'-R10')	D6	6×10^{-7}
DK3(3A-CP1-R10'-C3')	D4	2×10^{-7}
DM28(3A-CP1-2B'-R30'-C3')	D4	2×10^{-8}
DL13(3A-CP1-B'-R30-C3')	D4	2×10^{-8}
DL15(3A-CP1-B'-R30'-C3')	D4	2×10^{-8}
DY40(2A-L'-3B'-R5')	D6	9×10^{-9}
Sum of all accident sequences for this event		9×10^{-7}

Two Main Loops Initially Available

Accident Sequence	ESD Outcome Category	Probability of a Loss of Decay Heat Removal Per Shutdown
DY40(2A-3B'-R5')	D6	6×10^{-7}
DW3(2A-CP1-R5'-C3')	D4	2×10^{-7}
DC12(A-L'-2B')	D7	4×10^{-8}
DC8(A-L'-CP1-C3')	D7	4×10^{-8}
DZ12(A-S'-2B')	D7	3×10^{-8}
Sum of all accident sequences for this event		1×10^{-6}

accident sequences for this event both involve common mode failures. However, the dominant accident sequences from Table 5-XXXIX involve single failures, and they are therefore more significant.

Sensitivity Plots

For reactor shutdowns following PCRV depressurization accidents, the reliability of the CACS to operate is the most sensitive of the shutdown cooling subsystem inputs. A sensitivity plot for the CACS is provided for each depressurization accident case (i.e., three main loops initially available and two main loops initially available). These are Figures 5.20 and 5.21 respectively. Included in both these plots are the contributions from core-melt accident sequences with offsite power initially available and with offsite power initially unavailable.

5.5-3 Sensitivity to Common Mode Failures and Test and Maintenance Unavailabilities

For reactor shutdowns following PCRV depressurization accidents the variation in the probability of a loss of decay heat removal due to intrasystem common mode failures and test and maintenance unavailabilities is shown in Figure 5.22. Lists of these values for accidents with three main loops initially available and with two main loops initially available are given in Table 5-XLIII and 5-XLIV, respectively. These values include the contributions from core-melt accidents

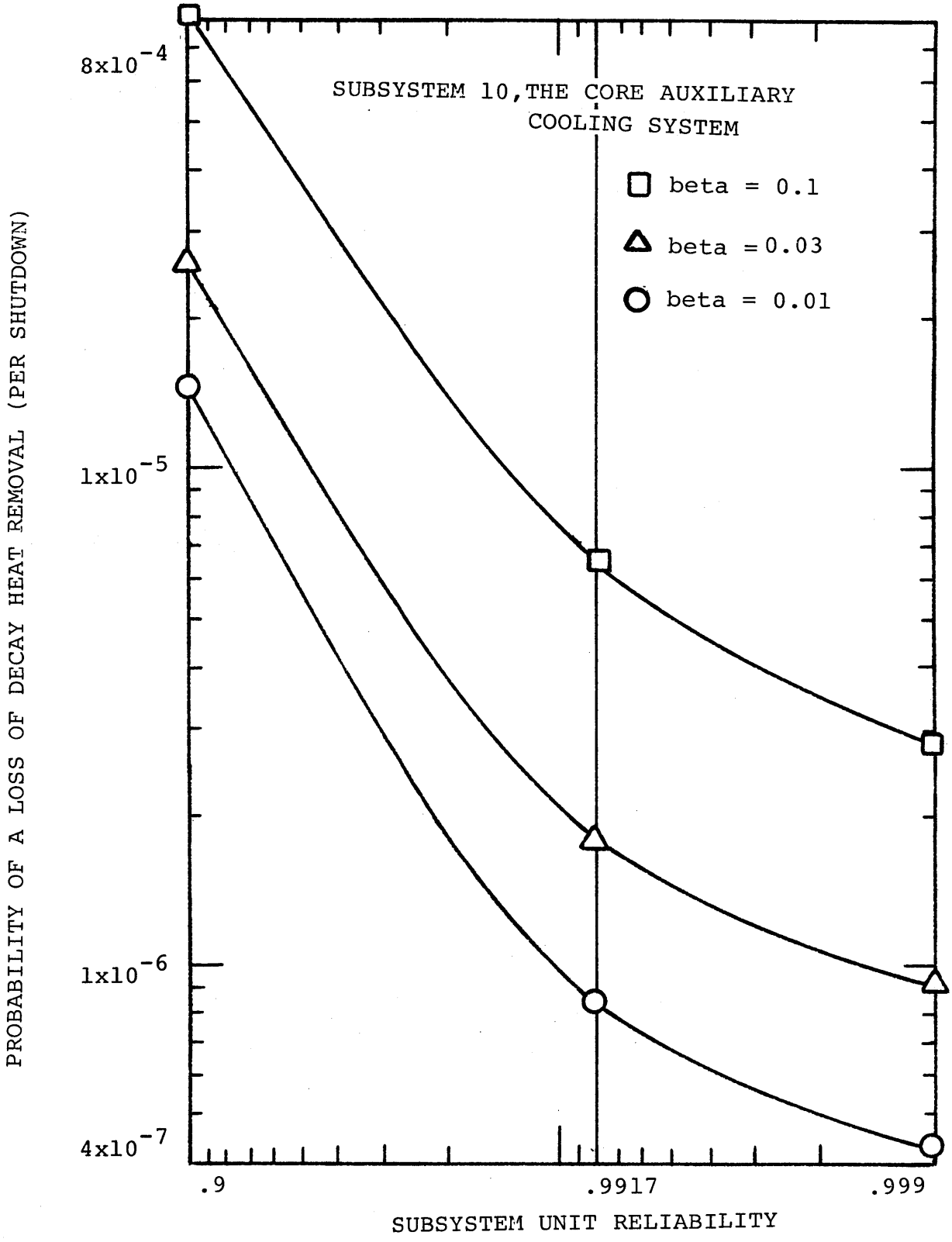


FIGURE 5.20 Sensitivity plot of subsystem 10 for shutdowns following PCRV depressurization accidents with three main loops initially available

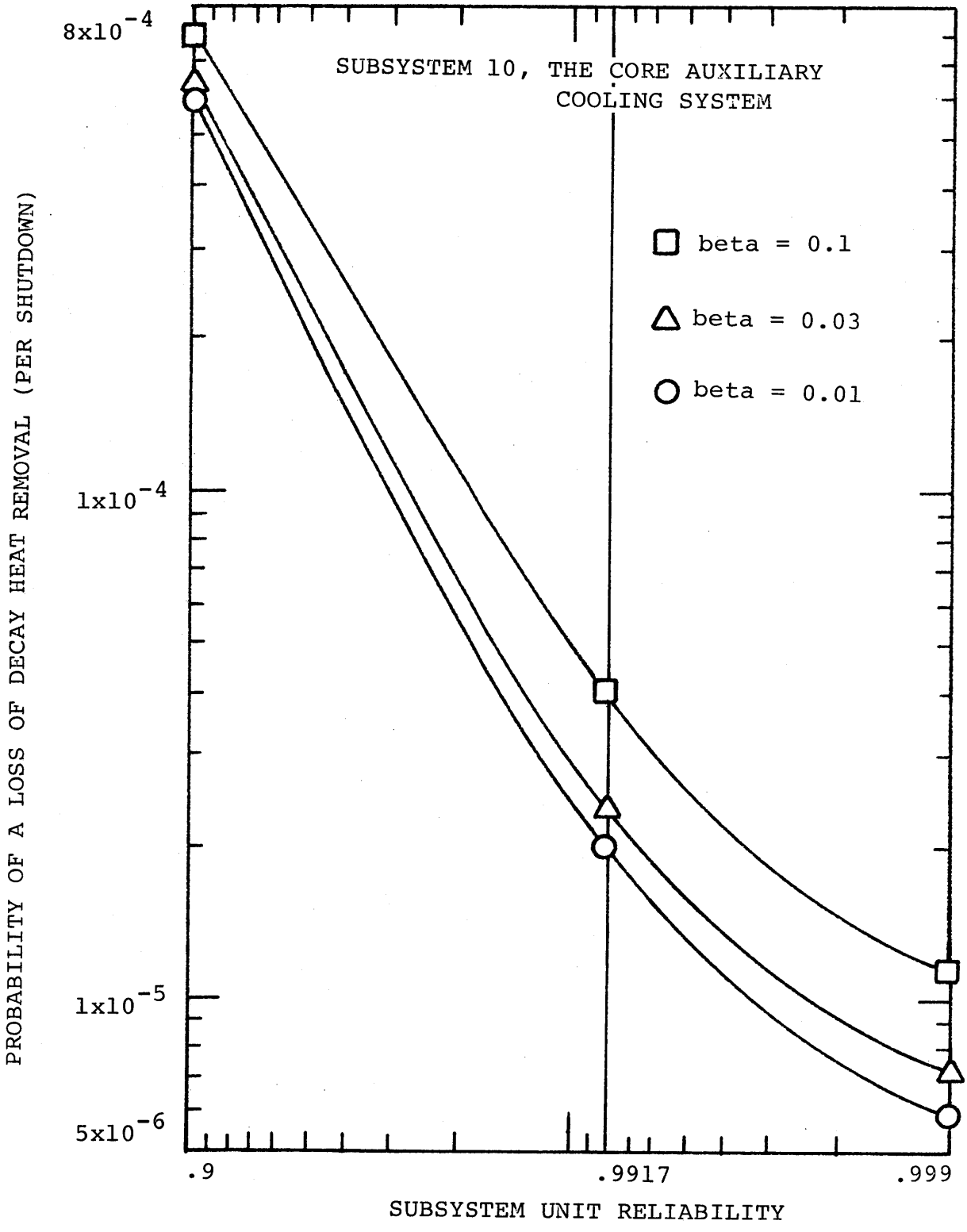


FIGURE 5.21 Sensitivity plot of subsystem 10 for shutdowns following PCRV depressurization accidents with two main loops initially available

TABLE 5-XLIII.
A List of Core-Melt Probabilities Considering Equipment Failure Only and all Failure Contributions for Shutdowns Following a Depressurization Accident With Three Main Loops Initially Available

Intrasystem Common Mode Failure Fraction (Beta Factor)	Probability of a Loss of Decay Heat Removal (Per Shutdown)	
	Equipment Failures Only	Equipment Failures and Test and Maintenance Unavailabilities
0.0	1×10^{-7}	4×10^{-7}
0.003	2×10^{-7}	6×10^{-7}
0.01	5×10^{-7}	8×10^{-7}
0.03	1×10^{-6}	2×10^{-6}
0.1	6×10^{-6}	7×10^{-6}

TABLE 5-XLIV.
A List of Core-Melt Probabilities Considering Equipment Failures Only and all Failure Contributions for Shutdowns Following Depressurization Accidents With Only Two Main Loops Initially Available

Intra-system Common Mode Failure Fraction (Beta Factor)	Probability of a Loss of Decay Heat Removal (Per Shutdown)	
	Equipment Failures Only	Equipment Failures and Test and Maintenance Unavailabilities
0.0	5×10^{-6}	2×10^{-5}
0.003	6×10^{-6}	2×10^{-5}
0.01	7×10^{-6}	2×10^{-5}
0.03	1×10^{-5}	2×10^{-5}
0.1	2×10^{-5}	4×10^{-5}

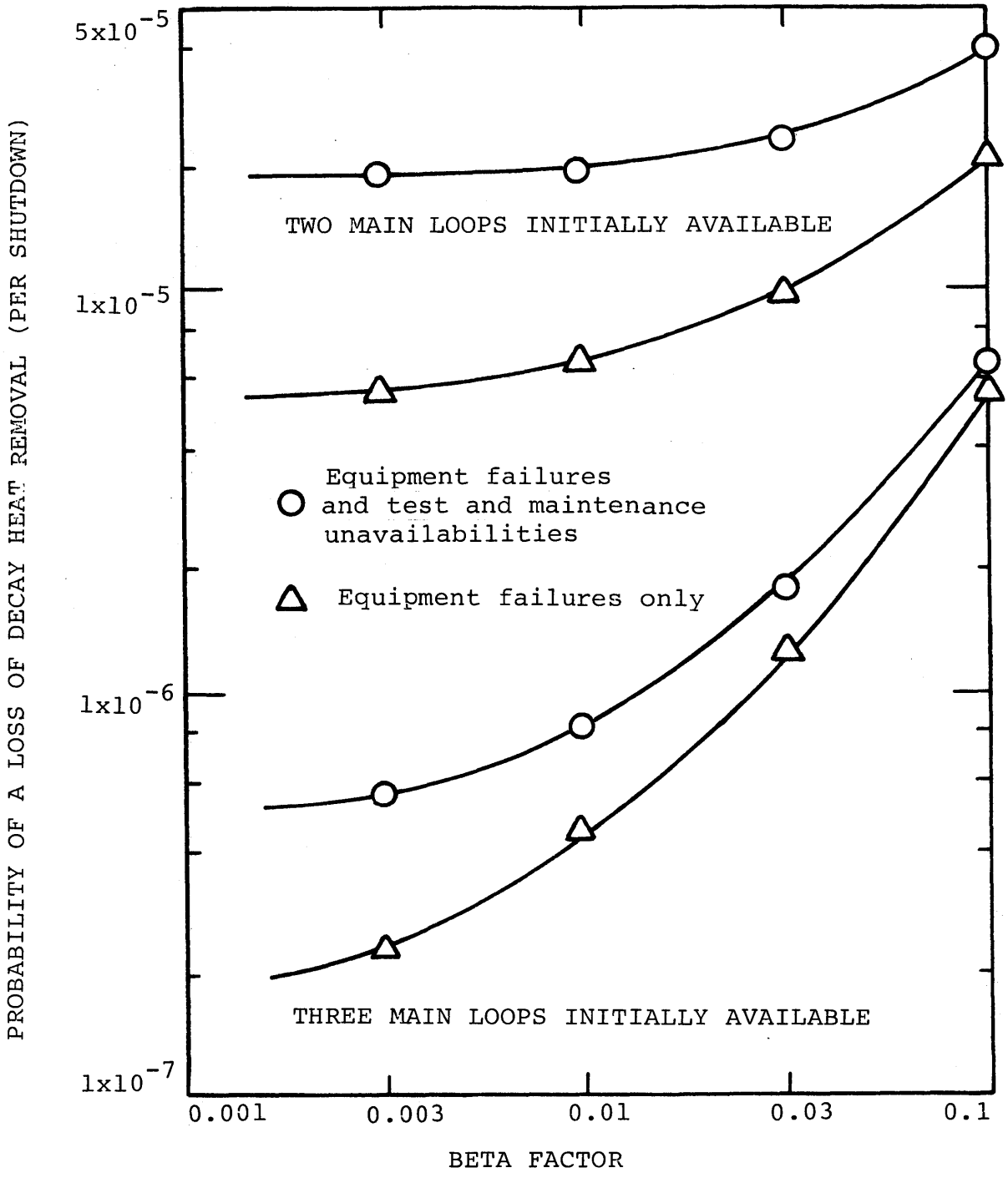


FIGURE 5.22 Probability of a core meltdown for shutdowns due to PCRV depressurization accidents

with offsite power initially available and with offsite power initially unavailable. For the case of three main loops initially available, common mode failures are more significant than the test and maintenance unavailabilities especially at higher beta factor values. However, with only two main loops initially available, common mode failures are less important, and the test and maintenance contribution is, therefore, more significant.

Table 5-XLV lists the percentage of the core-melt probability due to accident sequences occurring in the various time intervals following shutdown for three main loops initially available and for different beta factor values. As the beta factor valve increases, the percentage of core meltdowns occurring in the 20 to 30 minute interval increases while the percentage of meltdowns in the first 5 minutes decreases. Table 5-XLVI lists the dominant accident sequences at different beta factor values and according to their ESD outcome categories. The first three accident sequences in the 20 to 30 minute interval involve a common mode failure which eliminates the main loops and a common mode failure of the CACS. Thus, the contribution of this category increases as β increases. In outcome category D7, all the accident sequences except DT2 and DV2 do not involve common mode failures, and the contribution of this category decreases as β increases due to the increasing contribution of outcome category D4.

In outcome category D6, the important accident sequence is DN39, which involves the common mode failure of the diesel

TABLE 5-XLV
A List of the Calculated Percent of Core Meltdowns in Various Time Intervals Following Shutdowns Due to Depressurization Accidents With Three Main Loops Initially Available.

ESD Outcome Category	Time Interval Following Shutdown in Which Meltdown is Assumed to Occur	Percent of Core Meltdowns				
		β=0.0	β=0.003	β=0.01	β=0.03	β=0.1
D4	20 and 30 minutes-loss of decay heat removal	8.8	13.0	19.0	30.2	42.0
D5	10 to 20 minutes-loss of decay heat removal	0.2	0.2	0.2	0.2	0.2
D6	5 to 10 minutes-loss of decay heat removal	22.8	28.0	35.0	32.0	30.6
D7	within 5 minutes-loss of decay heat removal	68.2	58.0	45.8	37.2	26.2

TABLE 5-XLVI

A List of the Probability of the Dominant Accident Sequences at Different Beta Factor Values For Shutdowns Following Depressurization Accidents with Three Main Loops Initially Available

OUTCOME CATEGORY D4: Loss of Decay Heat Removal 20 to 30 Minutes after the Shutdown					
Accident Sequence	Probability of a Loss of Decay Heat Removal (per shutdown)				
	β=0.0	β=0.003	β=0.01	β=0.03	β=0.1
DK3(3A-CP1-X'-C3')	$1x10^{-10}$	$2x10^{-9}$	$1x10^{-8}$	$1x10^{-7}$	$1x10^{-6}$
DN2(3F'-CP1-C3')	$<1x10^{-10}$	$6x10^{-9}$	$2x10^{-8}$	$1x10^{-7}$	$6x10^{-7}$
*DK3(3A-CP1-R10'-C3')	$5x10^{-9}$	$3x10^{-8}$	$8x10^{-8}$	$2x10^{-7}$	$7x10^{-7}$
*DM28(3A-CP1-2B'-R30'-C3')	$2x10^{-8}$	← constant →			
*DL15(3A-CP1-B'-R30'-C3')	$1x10^{-8}$	$1x10^{-8}$	$1x10^{-8}$	$2x10^{-8}$	$3x10^{-8}$
Sum of all accident sequences for this category	$4x10^{-8}$	$7x10^{-8}$	$2x10^{-7}$	$5x10^{-7}$	$3x10^{-6}$

OUTCOME CATEGORY D6: Loss of Decay Heat Removal 5 to 10 Minutes after the Shutdown					
Accident Sequence	Probability of a Loss of Decay Heat Removal (per shutdown)				
	β=0.0	β=0.003	β=0.01	β=0,03	β=0.1
DK10(3A-CP3-SS'-C3')	$6x10^{-8}$	← constant →			
DK8(3A-CP1-SS'-C3')	$8x10^{-9}$		"		
*DN39(3A-3B'-R10')	$3x10^{-8}$	$8x10^{-8}$	$2x10^{-7}$	$6x10^{-7}$	$2x10^{-6}$
Sum of all accident sequences for this category	$1x10^{-7}$	$2x10^{-7}$	$3x10^{-7}$	$7x10^{-7}$	$2x10^{-7}$

* Loss of offsite power concurrent with depressurization accident

TABLE 5-XLVI (continued)

OUTCOME CATEGORY D7: Loss of Decay Heat Removal within 5 Minutes of the Shutdown					
Accident Sequence	Probability of a Loss of Decay Heat Removal (per shutdown)				
	β=0.0	β=0.003	β=0.01	β=0.03	β=0.1
DT2(3S'-CP1-C3')	1×10^{-10}	1×10^{-8}	3×10^{-8}	1×10^{-7}	6×10^{-7}
DV2(3L'-CP1-C3')	1×10^{-10}	8×10^{-9}	3×10^{-8}	1×10^{-7}	5×10^{-7}
DZ2(A-L'-S'-CP1-C3')	7×10^{-8}	8×10^{-8}	8×10^{-8}	1×10^{-7}	2×10^{-7}
DY10(2A-L'-CP3-C3')	9×10^{-8}	← constant →			
DQ10(2A-S'-CP3-C3')	6×10^{-8}		"		
DC2(A-2L'-CP1-C3')	4×10^{-8}	4×10^{-8}	5×10^{-8}	6×10^{-8}	9×10^{-8}
DR2(A-2S'-CP1-C3')	3×10^{-8}	3×10^{-8}	3×10^{-8}	3×10^{-8}	6×10^{-8}
Sum of all accident sequences for this category	3×10^{-7}	3×10^{-7}	4×10^{-7}	6×10^{-7}	2×10^{-6}

generators for concurrent losses of offsite power. This sequence increases as β increases. However, accident sequences DK10 and DB8 involve main loop support system falures and are not affected by the beta factor valve. Thus, the contribution of this outcome category only increases slightly as β increases.

For depressurization accidents with only two main loops initially available, the percentage of core meltdowns in each ESD outcome category is basically constant over the beta factor range. This is due to the dominance of accident sequences DC2(A-L'-CPI-C3') and DZ2(A-S'-CPI-C3') which are not very sensitive to the beta factor valve.

The individual subsystem common mode failure contributions, for the case of three main loops initially available, are listed in Table 5-XLVII. The table shows that the two major subsystem common mode failure contributions are due to the CACS and the emergency diesel generators (due to concurrent losses of offsite power). With only two main loops initially available, the only significant common mode failure contribution is due to the CACS. At the median beta factor value of 0.03 for all other systems, varying β for the CACS to 0.01 and 0.1 produced a change in the median probability of a core meltdown by factors of 0.88 and 1.4 respectively.

The contribution to the probability of a core meltdown due to the individual subsystem test and maintenance unavailability is listed in Table 5-XLVIII. In both cases where

TABLE 5-XLVII.
A List of the Individual Subsystem Common Mode Failure Contributions for Shutdowns Following Depressurization Accidents with Three Main Loops Initially Available

Subsystem Index and Name	Factor Change in the Probability of a Loss of Decay Heat Removal	
	Beta Factor for Individual Subsystem is 0.1 While All Others Are 0.03	Beta Factor for Individual Subsystem is 0.01 While All Others Are 0.03
4: CT Large CVs	0.98	1.1
5: CT Small CVs	0.95	1.2
6: Shutdown feed-water System	0.95	1.2
7: Auxiliary Boilers	0.98	1.1
8: Main Loop Transfer to Decay Heat Removal Operation	0.99	1.0
10:Core Auxiliary Cooling System	0.80	1.7
12:Resuperheater Bypass Control Valves	0.98	1.1
D18: Main Loop Isolation Valves	0.99	1.0
9: Emergency Electrical Supply	0.79	1.8

three main loops are initially available and where two main loops are initially available, only the contributions of CACS and resuperheater bypass control valve unavailability were significant.

5.5-4 The Effect of the Containment Equalization Pressure Range.

Following a depressurization accident, the event sequence paths were branched according to the containment equalization pressure range. The factor changes in the median probability of a core meltdown due to the upper and lower bounds of the probability values that these pressure ranges will occur are listed in Table 5-XLIX.

However, in order to better understand the contribution to the core-melt probability made by accident sequences in each containment equalization pressure (CEP) range, calculations were performed in which the probability of any one individual pressure range occuring was 1.0. The core meltdown probabilities for each of the CEP ranges, and as a function of the beta factor value, are listed in Table 5-L and 5-LI respectively for shutdowns with three main loops initially available and two main loops initially available. Notice that in both cases, the probability of a core meltdown, given the CEP is less than 1.25 atm., is quite high compared to the other two pressure ranges. The contribution of accident sequences in this low CEP range is the significant factor in the changes in the median core-melt probability values listed in Table 5-XLIX.

TABLE 5-XLVIII

A List of the Individual Test and Maintenance Unavailability Contributions for Shutdowns Following Depressurization Accidents with Three Main Loops Initially Available

Subsystem Index and Name	Subsystem Test and Maintenance Unavailability (per unit)	Factor Change in the Probability of a Core Meltdown due to Individual Subsystem T&M While all Other Subsystem Unavailabilities are zero	
		Three Main Loops Initially Available	Two Main Loops Initially Available
10:Core Auxiliary Cooling System	1.2×10^{-2}	1.9	2.2
12:Resuperheater Bypass Control Valves	2×10^{-2}	1.1	1.2

TABLE 5-XLIX

The Seneitivity of the Probability of Specific CEP Ranges for Shutdowns Following Depressurization Accidents

Containment Equalization Pressure Range	Probability of CEP being in Given Range	Factor Change in the Probability of a Loss of Decay Heat Removal	
		Three Main Loops Initially Available	Two Main Loops Initially Available
CEP>1.50atm.	.99	2.8	3.1
CEP<1.25atm.	1×10^{-3}		
CEP>1.50atm.	.9999	0.82	0.79
CEP<1.25atm.	1×10^{-5}		

TABLE 5-L

The Variation in the Probability of a Core Meltdown Given the Probability of Occurrence of Each Specific CEP Range is 1.0 for Depressurization Accidents with Three Main Loops Initially Available

Intrasystem Common Mode Failure Fraction, Beta Factor	Probability of a Loss of Decay Heat Removal (per shutdown) for each Specific CEP Range		
	CEP>1.50atm.	CEP 1.50-1.25atm.	CEP<1.25atm.
0.0	$2x10^{-7}$	$4x10^{-6}$	$2x10^{-3}$
0.003	$3x10^{-7}$	$5x10^{-6}$	$2x10^{-3}$
0.01	$6x10^{-7}$	$8x10^{-6}$	$2x10^{-3}$
0.03	$2x10^{-6}$	$2x10^{-5}$	$2x10^{-3}$
0.1	$6x10^{-6}$	$5x10^{-5}$	$2x10^{-3}$

TABLE 5-LI

The Variation in the Probability of a Core Meltdown Given the Probability of Occurrence of Each Specific CEP Range is 1.0 for Depressurization Accidents with Two Main Loops Initially Available

Intrasystem Common Mode Failure Fraction, Beta Factor	Probability of a Loss of Decay Heat Removal (Per Shutdown) For Each Specific CEP Range		
	CEP>1.50atm.	CEP 1.50-1.25atm.	CEP<1.25atm.
0.0	$1x10^{-5}$	$4x10^{-5}$	$6x10^{-2}$
0.003	$1x10^{-5}$	$4x10^{-5}$	$6x10^{-2}$
0.01	$1x10^{-5}$	$5x10^{-5}$	$6x10^{-2}$
0.03	$2x10^{-5}$	$6x10^{-5}$	$6x10^{-2}$
0.1	$3x10^{-5}$	$1x10^{-4}$	$6x10^{-2}$

5.6 Initiating Events Commonly Degrading Main Loop Shutdown Cooling Performance

5.6-1 Introduction

In this section, potential main loop common mode failures were investigated. The areas of common dependence of the main cooling loops were discussed in Section 4.3-2. In general, these main loop failures were treated as two types of events: either as initiating events which eliminated the main loop shutdown cooling system, or as common mode failures occuring after the shutdowns which were independent of the initiating event.

For initiating events which result in main loop cooling system failure, the CACS is the primary means of core cooling. If main loop failure occurs prior to 15 minutes following shutdown, the probability that two or more CACS loops fail to start is 8.2×10^{-4} per demand. This is determined using a beta factor of 0.03 and a test and maintenance unavailability of 1.2×10^{-2}. If the main loop failure does not occur until after this time, the probability that all three CACS loops will fail is 2.4×10^{-4} per demand. In section 5.6-2, an example of this type of event - the loss of all feedwater to the main loops - is discussed.

Main loop failures following the initiating event, but not due to the initiating event, were considered for all initiating event categories. These failures were primarily considered to occur as the result of main loop support system failures. However, the treatment of these failures was general

enough to include all potential main loop common mode failures. The results of these investigations are discussed in section 5.6-3.

5.6-2 Failure of the Feedwater Supply

Following a reactor shutdown, the main loops are supplied with feedwater by the shutdown feed pumps. The normal source of feedwater is the main condenser hotwell. However, should this source be unavailable, two back-up supplies exist. They are the condensate storage tanks and the emergency feedwater connection from the fire main.

In the event that all sources of feedwater are lost, main loop shutdown cooling operation is limited to 30 minutes by the steam generator inventory depletion. The probability of a loss of decay heat removal is just under 3×10^{-4} per shutdown event, and the dominant accident sequences are listed in Table 5-LII. The dominating event is the common mode failure of the CACS following main loop steam generator depletion. This is sequence N2, and it accounts for almost 98% of the total core-melt probability for this initiating event.

A sensitivity plot for the CACS is shown in Figure 5.23. Notice that the probability of a core meltdown is more sensitive to the CACS unit reliability than it is to the beta factor value. Also, an increase in the auxiliary loop reliability to .9943 due to redundant air cooler fans would decrease the probability of a loss of decay heat removal to below 2×10^{-4} per event.

TABLE 5-LII.
A List of the Dominant Accident Sequences for
Shutdowns Following the Loss of all Feedwater Supplies

Accident Sequence	ESD Outcome Category	Probability of a Loss of Decay Heat Removal Per Shutdown
N2(3F'-C3')	5	2×10^{-4}
Y2(2F'-L'-C3')	6	4×10^{-6}
Q2(2F'-S'-C3')	6	3×10^{-6}
T2(3S'-C2')	4	8×10^{-8}
W9(F'-L'-I'-C2')	4	8×10^{-8}
AA2(F'-L'-S'-C2')	4	7×10^{-8}
V2(3L'-C2')	4	6×10^{-8}
Sum of all accident sequences for this initiating event		3×10^{-4}

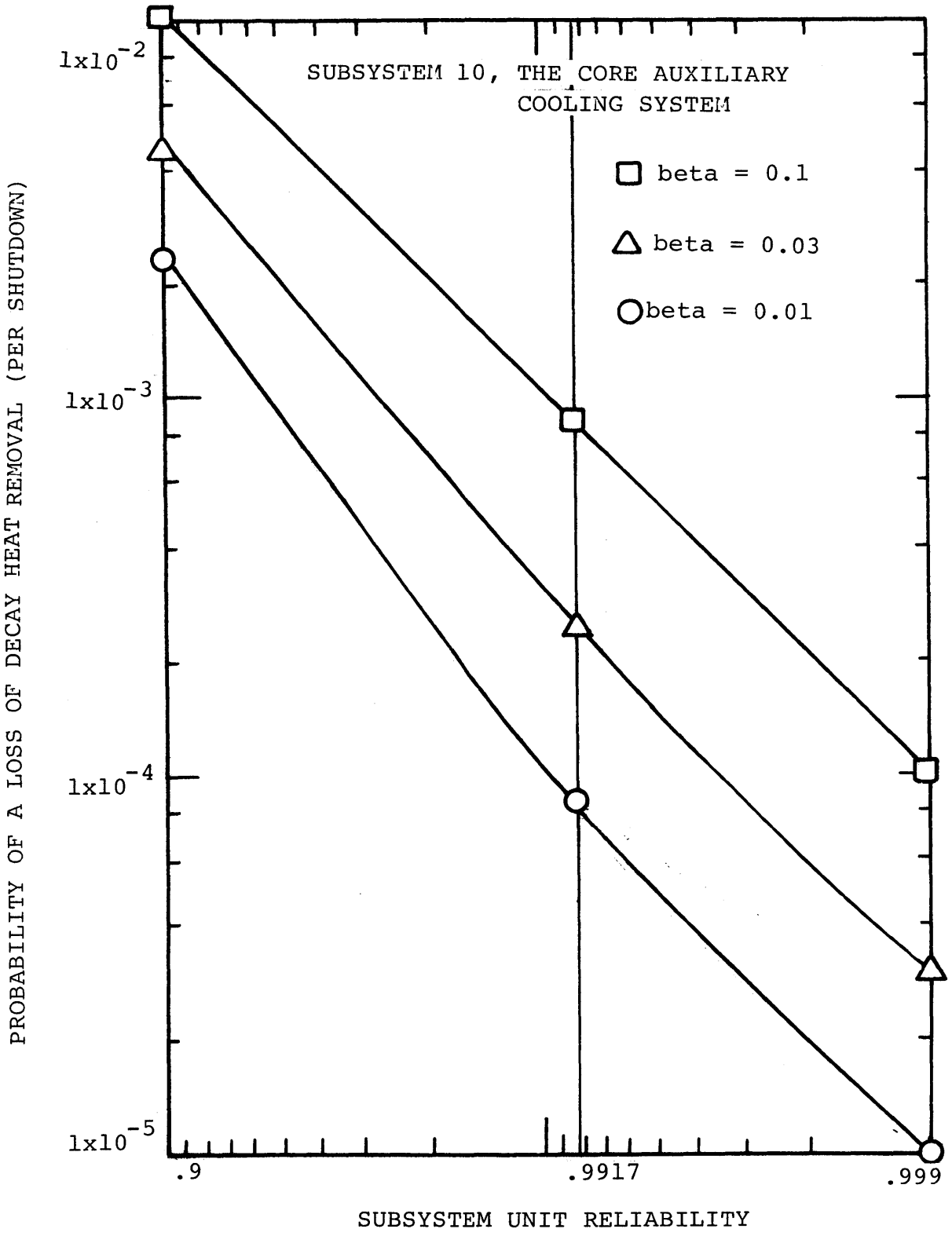


FIGURE 5.23 Sensitivity plot of subsystem 10 for shutdowns following the loss of all feedwater supplies

5.6-3 Support System Failures

Following any reactor shutdown, main loop failure may occur due to the failure of a common support system. The two primary support systems are the instrument air and the service water, and both systems are dependent upon essential electric power being available. The upper and lower failure probability values for these systems, given the number of essential buses energized were listed in Table 4-XII. The lower bound values were used in the calculations of the median core-melt probabilities for the different initiating event categories. Table 5-LIII lists the factor change in the median core-melt probability values due to applying the upper bound failure probabilities for the support systems.

The table shows that support system failures following pressurized reactor shutdowns are only very small contributors to the probability of a loss of decay heat removal. A check of the dominant accident sequences for pressurized reactor shutdowns (Table 5-III, 5-XX and 5-XXVII) shows that the only accident sequence involving support system failure is sequence M19 (3A-2B'-R30'-SS'-C3'). In this particular sequence, the service water system fails because it has only doubly redundant cooling water towers. For a reactor shutdown following a loss of offsite power, the failure of the two essential buses which power the two cooling water towers leads to service water system failure and eventually main loop failure unless offsite power

TABLE 5-LIII

A List of the Change in the Median Core-Melt Probability
Due to the Upper Bound Support System Failure Probabilities

Time Interval Following Shutdown in which Main Loop Failure is Assumed to Occur	Support System Failure	Factor Change in the Probability of a Loss of Decay Heat Removal (for each initiating event category) due to Upper Bound Support system Failure Probabilities				
		Shutdowns due to Category I. Initiating Events	Shutdowns due to Category II.A Initiating Events	Shutdowns due to the Loss of Offsite Power	Shutdowns Following a Depressurization Accident	
					3 Main Loops Initially Available	2 Main Loops Initially Available
5 to 15 Minutes	Instrument Air System Failure	1.0	1.0	1.1	---	---
	Service Water System Failure	---	---	---	1.0	2.2
15 to 30 Minutes	Service Water System Failure	1.1	1.0	1.1	---	---

is restored. However, this accident sequence is only a small contributor for this initiating event category, and this indicates that the present service water cooling tower arrangement does not significantly affect the probability of a core meltdown.

For reactor shutdowns following a depressurization accident, support system failures are somewhat more significant due to the fact that service water system failures were considered to lead to main loop failures in the 5 to 15 minute time interval following shutdown. Table 5-XXXVIII showed that for depressurization accidents with three main loops initially available the two accident sequences DK10(3A-CPI-SS'-C3') and DK8(3A-CP3-SS'-C3') are significant contributors to the probability of a core meltdown.

In this portion of the sensitivity analysis, some additional information regarding potential main loop common mode failures was gained. Specifically, following shutdowns due to category I initiating events, a main loop common mode failure with probability 1×10^{-4} which eliminated the main loops prior to 15 minutes following the shutdown, would only change the median probability of a core meltdown for this initiating event category by a factor of 1.2. Such an arbitrary common mode failure is quite unlikely due to the many main loop intrasystem common mode failures already taken into account. However, this small change in the median probability of a core meltdown indicates that any

unaccounted common mode failures would have to be more likely than 1×10^{-4} in order to significantly affect the results.

In this same regard, the median probability of a core meltdown for shutdowns due to category II.A initiating events is insensitive to main loop common mode failures even as likely as 1×10^{-3} per shutdown.

For reactor shutdowns following a loss of offsite power, support system failures were only slight contributors to the probability of a core meltdown. However, main loop common mode failures even as likely as 1×10^{-3} per shutdown would not significantly affect this initiating event category.

For reactor shutdowns following PCRV depressurization accidents, the upper bound of the support system failure probability is equivalent to a main loop common mode failure probability of 1×10^{-3} per shutdown. For depressurization accidents with three main loops available this increases the probability of a core meltdown by over a factor of 2. However, in the case in which only two main loops are initially available there is no change in the core-melt probability.

5.7 Other Analyses

5.7-1 The Effect of Changes in the Steam Generator Inventory

The design of the GCFR demonstration plant is not yet fixed, and possible future design changes may have some effect on the results presented in this chapter. One such possible design change would involve the steam generators. A redesign

of the steam generators which reduced the inventory of steam water would affect the main loop operating times used in the ESD modelling.

The effect of such a steam generator design change was analyzed by assuming a 20% reduction in all the main loop operating times. The only accident sequences which were significantly affected by this change were those for which the main loop operating time was close to either 15 or 20 minutes. Specifically, for pressurized accident sequences labeled P and X, the main loops were no longer able to operate long enough to allow auxiliary boiler operation. Also, for accident sequences labeled Q and Y, main loop operation was less than 15 minutes, and thus two CACS loops were required rather than only one. Similar changes were also made in the appropriate event sequences following depressurization accidents. The changes in the median probability of a core meltdown, for each initiating event category, due to a 20% reduction in the main loop operating times are listed in Table 5-LIV.

In all initiating event categories, the accident sequences most affected by such a design change were those labeled P or X. In these sequences the main loops no longer operate long enough to allow the auxiliary boilers to reach their rated operating conditions. However, the overall effect of this change is small due to the relatively minor contribution of these specific accident sequences.

TABLE 5-LIV.
The Effect of a 20% Reduction in Main Loop Operating Time on the Median Core-Melt Probabilities of the Various Initiating Event Categories

Initiating Event Category	Factor Change in the Median Probability of a Loss of Decay Heat Removal Due to a 20% Reduction in the Main Loop Operating Times
I. Reactor Shutdowns not affecting the performance of either shutdown cooling system	1.1
II.A Reactor Shutdowns affecting the performance of a single main loop	1.2
III.C Reactor Shutdowns due to the loss of offsite power	1.0
III.B Reactor Shutdowns following PCRV depressurization accidents.	
3 main loops initially available	1.1
2 main loops initially available	1.2

5.7-2 Increasing the Shutdown Feedpump Capacity

With the present design capacity of the shutdown feedpumps, a single available main cooling loop supplied with shutdown feedwater is operable for less than 15 minutes. The failure rate of the CACS, in this interval is 8.2×10^{-4} per demand. If the shutdown feedpump capacity were increased such that a single main loop were capable of operating at least 15 minutes, then the failure rate of the CACS for these accident sequences would decrease to 2.4×10^{-4} per demand.

The core-melt probability for initiating event categories I and II.A would be most affected by this design change, and the specific dominant accident sequences which would be affected can be seen in Tables 5-III and 5-XX. The more dominant accident sequences which are affected are CC2, Z2, W9, O9, CC23 and Z47. For inadvertent reactor shutdowns, the median core-melt probability would decrease to 5×10^{-7} per shutdown, and for reactor shutdowns due to the loss of a single main loop, the core-melt probability decreases to slightly over 1×10^{-5} per shutdown.

5.7-3 Other Possible CT Small CV Failure Modes

The failure mode of the CT small CV assumed in this study was the failure of the valve to throttle. This was considered to be the most likely failure mode because it does not involve any action on the part of the valve or its controller. Another possible failure mode, the valve fails closed, would required either that the valve had closed prior to the reactor shutdown, or that the shutdown controller function to close the valve.

The probability of a CT small CV failing closed and the failure remaining undetected prior to a reactor shutdown was considered to be about 1×10^{-4}. It was assumed that an electrical interlock device would require the CT small CV to be opened prior to the opening of the CT large CV. This would assure that the small valve was opened during the startup of the reactor. It was also assumed that the small valves would be equipped with monitoring devices which would detect valve closures during reactor operation. These CT small CV failures were investigated by assuming an unavailability for the values due to undetected valve closures. At 1×10^{-4}, this failure mode had no effect on the probability of a core meltdown for any initiating event category. Even if the probability of such a valve failure were 1×10^{-3}, the only initiating event categories for which the probability of a core meltdown would be affected are those for which only two main loops are initially available. For these initiating event categories, the

median probability of a core meltdown is changed by a factor of less than 1.2.

The probability that following a reactor shutdown the CT small CV would completely close, rather than throttle, was considered to be small compared to the probability that no action would occur. The ESD was therefore modelled according to the more likely failure mode. However, the results presented in this chapter would not change significantly if the "valve fails closed" failure mode had been modelled instead. For all the dominant accident sequences except those involving the common mode failure of the small valves. The difference in the main loop operating times between the two small valve failure modes would not affect either the auxiliary boiler availability or the CACS operating requirements. The common mode failure of all three small valves by failing closed would eliminate the main loops in about 30 seconds. this is roughly the coast-down time of the main circulators. With a CACS start-up time of two minutes, this particular event would result in a core meltdown. However, GA[2] is presently considering much shorter CACS starting times which would allow CACS operation even if such an unlikely event were to occur.

The probability of a common mode failure of all three valves by failing closed was considered to be at least one order of magnitude less than the common mode failure of the valves by failing to throttle. This would place it in the range of 10^{-5} to 10^{-6} per shutdown. If the CACS were not

capable of core cooling for this particular event, it would be a major contributor to the probability of a core meltdown. However, it appears likely that the CACS will be capable of starting quickly enough to prevent a core meltdown, and even if all three CACS loops were required to start successfully, this particular CT small CV common mode failure would not contribute significantly to the overall core-melt probability.

Chapter 6

Probability of a Core Meltdown

6.1 Introduction

6.1-1 Constituents of the Core-Melt Probability

The overall probability (per year) of a core meltdown is the sum of the core-melt probability values for all the initiating event categories. For each initiating event category, the probability of a core meltdown has a contribution from core meltdowns which occur following the reactor shutdown and a contribution from core meltdowns which occur due to failure of the reactor to shutdown. Thus,

$$P_{CM} = \sum_i P_i$$

where, P_{CM} is the overall probability (per year) of a core meltdown and the P_i's are the contributions from the various initiating event categories. Each P_i in turn is determined by the equation:

$$P_i = P_{IE} \, (P_S + P_F) \, .$$

P_{IE} is the frequency or probability of occurrence of the initiating event. These were discussed in Chapter 4. P_S is the conditional probability of a loss of decay heat removal following reactor shutdown given the initiating event. The

median core-melt probability for each of the initiating event categories and the sensitivity of these values to the different shutdown cooling system failure contributions was discussed in Chapter 5. P_F is the conditional probability that a core meltdown occurs due to failure of the reactor to shutdown for a given initiating event. Because accident sequences following failure to shutdown were not investigated, these accidents were all conservatively assumed to result in a core meltdown. This is a conservative assumption because the main loop heat removal capability is not immediately lost following all of the events which initiate reactor shutdown. It is therefore likely that a core meltdown can be prevented in certain of these accident sequences.

In Section 6.2, the total probability of a loss of decay heat removal following a reactor shutdown is discussed. Possible design changes are pointed out in Section 6.3 and discussed according to their effect on the overall probability of a core meltdown. In Section 6.4, the contribution of core meltdowns due to failure of the reactor to shutdown is discussed, and accident sequences following a failure of the reactor to shutdown are discussed briefly.

6.1-2 Absolute Versus Relative Probabilities

Due to the conceptual nature of the GCFR design, the core-melt probabilities presented in this study are a first-cut assessment. Lack of detail in specific areas of the design did not allow the depth of analysis necessary to

determine absolute probability values with a high degree of confidence. Conservative assumptions were made in the major areas of uncertainty, and the sensitivity of these assumptions was investigated to determine their impact on the results. But probably the most significant factor is that the design of the GCFR is still evolving and future design changes may affect the results of this study.

The thrust of this study has been to determine useful design information to aid in the further development of the GCFR. Thus, the relative values of the core-melt accident sequences do provide quantitative inputs to the overall design evaluation.

As work on the GCFR concept continues, and more detailed information becomes available, refinements in the accident sequence modelling and in the evaluation of the subsystem reliability values and common mode failure probabilities will allow better estimates of the absolute value of the core-melt probability.

6.2 The Probability of a Loss of Decay Heat Removal Following Reactor Shutdown

The initiating event frequencies and the calculated median probabilities of a loss of decay heat removal (per shutdown) for each initiating event category are listed in Table 6-I. The product of these two values yields the probability (per year) of a loss of decay heat removal for each initiating event category.

Table 6-I

A List of the Overall Core-Melt Probability
Contributions from each Initiating Event Category

Initiating Event Category	Frequency of Reactor Shutdowns (per year)	Median Probability of a Loss of Decay Heat Removal (per shutdown)	Probability of a Loss of Decay Heat Removal (per year)	
			Estimated Value	Range(1)
I. Inadvertant Forced Reactor Shutdowns	3	7×10^{-7}	2×10^{-6}	1×10^{-6}-9×10^{-6}
II.A Shutdowns following Failure of a Single Main Loop	10^{-2}	2×10^{-5}	2×10^{-7}	1×10^{-7}-3×10^{-7}
II.B Main Loop Common Mode Failures	10^{-4}	8×10^{-4}(2)	8×10^{-8}	6×10^{-8}-9×10^{-8}
III.A External Events(3)	10^{-4}-10^{-6}	10^{-2}(4)	---	1×10^{-8}-1×10^{-6}
III.B PCRV Depressurization Accidents				
3 Main Loops Available	10^{-3}(5)	2×10^{-6}	2×10^{-9}	8×10^{-10}-7×10^{-9}
2 Main Loops Available	10^{-6}	2×10^{-5}	2×10^{-11}	2×10^{-11}-4×10^{-11}
III.C Shutdowns following the Loss of offsite power	10^{-2}	5×10^{-4}	5×10^{-6}	2×10^{-6}-2×10^{-5}
Sum for all Initiating Event Categories			7×10^{-6}	3×10^{-6}-3×10^{-5}

(1) Corresponds to the upper and lower beta factor values

(2) Refers to the case of main loop failure in the first 15 minutes following shutdown

(3) Refers to the occurrence of an earthquake greater in magnitude than an SSE

(4) This value was discussed in Chapter 4

(5) Probability of a leak in one of the smaller PCRV penetration closures

This study has been a point estimate analysis with the major emphasis on the core-melt probability per shutdown as opposed to the core-melt probability per year. The core-melt probability, per reactor shutdown, is a median point estimate. It is based on the median subsystem unit reliability values, the test and maintenance unavailabilities, and the median beta factor value of 0.03. Of these three contributors to the subsystem failure probability, only the beta factor value was evaluated with an uncertainty range. While the other values do possess uncertainty ranges, the effect of uncertainty in the beta factor value was considered to outweigh the effect of uncertainty both in the failure data used to generate the subsystem unit reliability values, and in the test and maintenance unavailability values. Thus, a range of the median point estimate of the core-melt probability was determined based on the median subsystem unit reliability values, the test and maintenance unavailabilities and the upper and lower bounds of the beta factor value of 0.1 and 0.01 respectively.

However, the core-melt probability per year includes the initiating event frequency values which are not all median estimates. In all cases, except the frequency of inadvertent reactor shutdowns, the probability of a reactor shutdown due to the initiating event was determined as an order of magnitude estimate. This accuracy was considered

to be sufficient for an evaluation of the relative core-melt probabilities of the various initiating event categories. As more data on the various initiating events becomes available, a more refined estimate of these values can be made. This will aid in the attempt to determine a better value for the absolute probability of a core meltdown in a GCFR. Yet, it is unlikely that this would significantly change the relative importance of the various initiating event categories. Also, the probability of a core meltdown (per reactor year) is not a median value. It is the best estimate of that value for the purposes of this study, and while the range shown in the table is due to the beta factor uncertainty, it should be noted that for some of the initiating event categories, the uncertainty in the initiating event frequency may outweigh the beta factor uncertainty.

The sum of the estimated core-melt probabilities for each of the initiating event categories is slightly over 7×10^{-6} per year, and the sums of the upper and lower median estimates due the upper and lower beta factor values gives a range of 3×10^{-6} to 3×10^{-5} per year. The two major contributors to the core-melt probability are losses of decay heat removal following shutdowns due to category I initiating events (inadvertent reactor trips) and following shutdowns due to the loss of offsite power (category III.C). Losses of decay heat removal following shutdowns due to category II.A

initiating events (failures of one main loop) are only small contributors even at the conservative estimate of the operational protection system (OPS) failure rate of 1×10^{-2} per demand. For reactor shutdowns due to main loop support system failures (category II.B), an initiating event probability of 1×10^{-4} per year was estimated by the author. Losses of decay heat removal following shutdowns due to these initiating events are negligible contributors to the total probability of a core meltdown. However, even if the probability of occurrence of these initiating events were 1×10^{-3} per year, the total probability of a core meltdown would not be significantly affected.

The contribution to the probability of a core meltdown due to the occurrence of an earthquake of greater magnitude than a safe shutdown earthquake (SSE) is shown under initiating event category III.A. No median core-melt probability was selected for this event, but at most it is only a very small contributor to the median core-melt probability. However, the range of the probability of a core meltdown due to the occurrence of an SSE was included in the sum of the upper and lower values of the point estimate range, where it made only a small contribution.

The probability of a loss of decay heat removal following a depressurization accident has a negligible impact on the overall probability of a core meltdown. This is due in

part to the assumption that severe losses of containment integrity concurrent with the depressurization accident were very unlikely. This assumption was considered reasonable because the containment failure modes should be basically independent of the depressurization. However, even if the coupling between these two events were on the order of 10^{-1} to 10^{-2} per event, the probability of a core meltdown due to PCRV depressurization accidents would be at most 2×10^{-7} per year with three main loops initially available, and 6×10^{-9} per year if only two main loops were initially available. The total probability of a core meltdown would not be changed significantly even if this were the case.

The contribution of common mode failures and test and maintenance unavailabilities to the core-melt probability can be seen from Table 6-II. Considering only random equipment failures, the core-melt probability is 3×10^{-7} per year. Including intra-system common mode failures increases the probability of a core meltdown to 6×10^{-6} per year, while the addition of test and maintenance unavailabilities only increases this value to 7×10^{-6} per year. The significance of common mode failures is due to the dominance of accident sequences in initiating event categories I and III.C. Only in initiating event category II.B is the test and maintenance contribution much greater than that of common mode failures. This is because, for the event listed in the table, two CACS loops are required to operate.

Table 6-II

The Contributions of Intrasystem Common Mode Failures
and Test and Maintenance Unavailabilities to the Core-Melt Probability

Initiating Event Category	Probability of a Loss of Decay Heat Removal (per year)			Factor Increase Due to Common Mode Failures (a) Column (2) / Column (1)	Factor Increase Due to T&M Unavailabilities (a) Column (3) / Column (2)
	No T&M (1) $\beta = 0$	No T&M (2) $\beta = 0.03$	T&M Included (3) $\beta = 0.03$		
Inadvertent Forced Shutdowns I.	1×10^{-7}	9×10^{-7}	2×10^{-6}	8.3	2.2
Shutdowns Following Failure of a Single Main Loop II.A	2×10^{-8}	6×10^{-8}	2×10^{-7}	3.1	3.3
Main Loop Common Mode Failure (b) II.B	2×10^{-8}	3×10^{-8}	8×10^{-8}	1.4	3.0
PCRV Depressurization Accidents III.B					
3 Main Loops Available	1×10^{-10}	1×10^{-9}	2×10^{-9}	10.0	1.4
2 Main Loops Available	5×10^{-11}	1×10^{-10}	2×10^{-10}	2.0	2.4
Shutdowns Following the Loss of Offsite Power III.C	2×10^{-7}	5×10^{-6}	5×10^{-6}	28.8	1.0
SUM OF ALL INITIATING EVENT CATEGORIES	3×10^{-7}	6×10^{-6}	7×10^{-6}	17.6	1.2

(a) For these calculations, the exact values were used, while the numbers listed in columns 1, 2 and 3 are rounded to the nearest whole number.

(b) Main loop failure assumed in the first 15 minutes following shutdown.

It is important to note that the two most dominant accident sequences account for over half of the total core-melt probability. These are sequences N22 (3A-3B'-R10') and K3(3A-R10'-C3') which involve common mode failures of the diesel generators and the CACS respectively. The dominant accident sequences following inadvertent forced reactor shutdowns account for most of the remainder of the core-melt probability. These sequences are listed in Table 5-III and the most important of these also involve common mode failures.

6.3 The Effect of Potential Design Changes

A number of possible design changes were discussed throughout Chapter 5. These are summarized below and their overall effect on the probability of a core meltdown is discussed.

Table 6-III shows the calculated probability of a core meltdown due to inadvertent forced reactor shutdowns (category I initiating events) for three specific design changes. Two of these changes affect the CACS while the other concerns the shutdown feedpump capacity. For reactor shutdowns due to category I initiating events, a large percentage of the core-melt probability is due to accident sequences occurring prior to 15 minutes following the shutdown with only one CACS loop operating. If the CACS heat removal capability were increased such that one loop were capable of core cooling at 8 minutes after the shutdown, the probability of a loss of decay heat removal would be decreased.

TABLE 6-III
The Affect of Specific Design Changes
on the Core-Melt Probability Following Shutdown
Due to Category I Initiating Events

Potential Design Change	Probability of a Loss of Decay Heat Removal (per Shutdown) Due to Category I Initiating Events	
	Median	Range
Base Case	7×10^{-7}	3×10^{-7} - 3×10^{-6}
Increase CACS Heat Removal Capability	5×10^{-7}	2×10^{-7} - 3×10^{-6}
Increase CACS Reliability to .9943	4×10^{-7}	2×10^{-7} - 2×10^{-6}
Increase Shutdown Feedpump Capacity	5×10^{-7}	2×10^{-7} - 3×10^{-6}
Both Design Changes Above	3×10^{-7}	3×10^{-7} - 3×10^{-6}

In the determination of the CACS unit reliability, it was assumed that both of the air cooler fans were required to operate. The CACS unit reliability was then calculated at .9917. However, if only one fan were required to operate, the CACS of this increased CACS reliability was determined using the sensitivity plot of Figure 5.7. The combined effect of these two design changes was extrapolated from this sensitivity plot.

Increasing the shutdown feedpump capacity will decrease the core-melt probability for this category if a single main loop is capable of operating for at least 15 minutes. The effect of this design change is shown in Table 6-III. However, this design change is an alternative to increasing the CACS heat removal capability. In effect, either a single CACS loop can be capable of core cooling sooner to account for the operating time of a single main loop, or the operating time of a single main loop can be extended until one CACS loop is adequate. The decrease in the core-melt probability is effectively the same for these two changes, and in the remaining discussion the shutdown feedpump design change can be substituted for the CACS design change.

Other possible design changes which do not affect the subsystem performance as modelled in the ESD, but may affect its reliability of operation can be investigated through the sensitivity plots. After improvements in the CACS

reliability, possible design changes which might increase the reliability of the CT small CV's to throttle would be most beneficial.

The three design changes mentioned above, also have a significant impact on the probability of a loss of decay heat removal for shutdowns due to category II.A and category II.B initiating events. However, because of the small contribution to the overall probability of a core meltdown due to these events, no significant change in the overall value results. This is also the case for reactor shutdowns due to PCRV depressurization accidents.

For reactor shutdowns following the loss of offsite power, the effect of potential design changes is shown in Table 6-IV. The first potential design change concerns powering the auxiliary boilers from the essential buses rather than the non-essential bus. This change decreases the core-melt probability for this category from 5×10^{-4} to 3×10^{-4} per shutdown. The auxiliary boiler electrical loads are not large and could be easily incorporated into the essential electrical loads without significantly affecting the required diesel generator capacity.

The other significant design change involves increasing the operating time of the main loops when no essential power is available. In this study, main loop operation without essential power was limited to 15 minutes due to incomplete

TABLE 6-IV

The Effect of Specific Design Changes On the Core-Melt Probability Following Shutdowns Due to the Loss of Offsite Power

Potential Design Change	Adjusted Probability of a Loss of Decay Heat Removal (per shutdown) Due to Loss of Offsite Power Events	
	Auxiliary Boilers on Non-Essential Buses	Auxiliary Boilers on Essential Buses
	Median; Range	Median; Range
Base Case	5×10^{-4}; 2×10^{-4}-2×10^{-3}	3×10^{-4}; 1×10^{-4}-1×10^{-3}
Extend Main Loop Operation to 30 Minutes Without Essential Power	4×10^{-4}; 2×10^{-4}-2×10^{-3}	2×10^{-4}; 9×10^{-5}-9×10^{-4}
Increase CACS Reliability to .9943	4×10^{-4}; 2×10^{-4}-1×10^{-3}	3×10^{-4}; 1×10^{-4}-1×10^{-3}
Both Design Changes Above	3×10^{-4}; 1×10^{-4}-2×10^{-3}	2×10^{-4}; 9×10^{-5}-9×10^{-4}

throttling of the CT small CV's. These valves require a continuous supply of instrument air for correct operation. If each valve were equipped with a separate air accumulator to supply its air requirements, main loop operation without essential power could be extended until steam generator depletion (assumed to be 30 minutes). This design change decreases the probability of a loss of decay heat removal following shutdowns due to the loss of offsite power. Also, increasing the reliability of the CACS will decrease the probability of a loss of decay heat removal if the auxiliary boilers are powered by the non-essential bus. But if the auxiliary boilers are powered by the essential buses, the probability of a core meltdown is dominated entirely by the failure of the emergency diesel generators.

The separate and combined effect of these potential design changes is summarized in Table 6-V. The table lists the probability of a loss of decay heat removal (per year) as it is affected by the specific design change or changes. The single most significant design change is powering the auxiliary boilers from the essential buses. This decreases the median probability of a core meltdown to 5×10^{-6} per year with a range due to the beta factor range of 2×10^{-6} to 2×10^{-5} per year. If all of the design changes discussed above were made, the median probability of a loss of decay heat removal would decrease to 3×10^{-6} per year with a

TABLE 6-V

The Overall Effect of Potential Design Changes on the Core-Melt Probability

Potential Design Change	Adjusted Probability of a Loss of Decay Heat Removal (per year)	
	Estimated Value	Range
Base Case	7×10^{-6}	3×10^{-6} - 3×10^{-5}
1: Power Auxiliary Boilers From the Essential Buses	5×10^{-6}	2×10^{-6} - 2×10^{-5}
2: Increase CACS Heat Removal Capability	6×10^{-6}	3×10^{-6} - 3×10^{-5}
3: Extend Main Loop Operation to 30 Minutes Without Essential Power	6×10^{-6}	3×10^{-6} - 3×10^{-5}
4: Increase CACS Reliability to .9943	5×10^{-6}	3×10^{-6} - 2×10^{-5}
Design Changes 2, 3 and 4 Above	4×10^{-6}	2×10^{-6} - 2×10^{-5}
Design Changes 1, 2, 3 and 4 Above	3×10^{-6}	1×10^{-6} - 1×10^{-5}

range of 1×10^{-6} to 1×10^{-5} per year. However, if the above changes were made except for powering the auxiliary boilers from the essential buses, the median probability of a core meltdown would be 4×10^{-6} per year with a range of 2×10^{-6} to 2×10^{-5} per year.

The design changes discussed above only represent those changes which were investigated in the study and which were found to have some impact on the core-melt probability. They do not represent a complete analysis of all potential design changes. Furthermore, whether any design changes are warranted will depend on a complete consideration of all the various design trade-offs.

6.4 Probability of a Core Meltdown Due to Failure of the Reactor to Shutdown

An analysis of the accident sequences following failure of reactor shutdown systems was not performed in this study. The reliability of the reactor shutdown systems was considered to be sufficiently high such that core meltdowns due to their failure would not contribute significantly to the overall probability of a core meltdown.

There are two independent reactor shutdown systems in the GCFR. These are the control rod system and the shutdown rod system. The analysis of LWR reactor protection systems in the RSS indicates that a failure rate of 1×10^{-5} per demand is attainable for a single shutdown system [1].

Allowing for potential common failure modes due to the fact that both GCFR shutdown systems are rod-type systems, it is considered that a failure rate in the range of 10^{-7} to 10^{-8} per demand is reasonable for the two GCFR shutdown systems.

An upper bound on the failure rate for the GCFR shutdown systems can be obtained by conservatively assuming that failure of the reactor to shut down leads to a core meltdown. Assuming three forced reactor shutdowns are required per year and that core meltdowns due to failure should not contribute more than 10% of the overall probability of a core meltdown, the upper bound on the failure rate of the reactor shutdown systems would be 2×10^{-7} per demand. At a failure rate of 2×10^{-8} per demand, failure of the reactor to shut down would not contribute more than 1% to the probability of a core meltdown. Therefore, based on this analysis, failure of the reactor to shut down should not be a significant contributor to the core-melt probability.

However, failure of the reactor to shut down does not automatically result in a core meltdown. For example, the loss of condenser vacuum is a reactor trip parameter, but failure of the reactor to shut down does not immediately result in a core meltdown because main loop cooling is not lost. Operation of the main loops can be continued for a considerable period of time allowing for possible remedial actions.

Some important points regarding the plant response to this particular class of accidents are discussed below.

The input parameter sensors of the plant protection system are common to both reactor shutdown systems. If the reactor shutdown signal is not initiated, a reactor transient will result. Failure of the shutdown signal to be initiated is unlikely due to multiple input sensors for each reactor protection system parameter, and due to the fact that there is a primary trip parameter and at least one back-up trip parameter for each anticipated reactor shutdown situation. Also, for most of these situations operator action would result in a manual initiation of the reactor shutdown. Whether a core meltdown occurs, in the event that the shutdown signal is not initiated, will depend on the severity of the power to heat removal imbalance caused by the initiating event.

If following the initiation of a reactor shutdown signal the reactor is not shut down, a number of plant actions will occur. The turbine throttle is tripped and the resuperheater bypass control valves are opened, the auxiliary boilers and shutdown feedpumps are started, and the emergency diesel generator and the CACS are started in the event they may be needed. However, the CT large CV's do not close because the reactor shutdown verification signal is also required for this action. The main loop are still operating at full power pro-

viding core cooling. However, the steam generators will soon be exhausted unless a source of feedwater is established.

The main feedpump turbines are normally driven by extraction steam from the main turbine, and the turbine trip interrupts the feedwater supply. In order to continue full power main loop operation, the main feedpump turbines need to be driven by the steam exhaust in the resuperheater bypass line. The shutdown feedpumps are inadequate due to their low capacity. Provision is made for this mode of operation for the feedpumps both at startup and during orderly reactor shutdowns. Main loop operation could continue for some time in this operating mode.

The details of these plant responses are not final, but clearly the potential exists for preventing core meltdown in situations where the reactor shutdown systems have failed.

Chapter 7

Conclusions and Remarks

7.1 Summary

This study is an attempt to utilize the accident analysis techniques of the Reactor Safety Study (RSS) [1] toward a first-cut assessment of the gas-cooled fast-breeder reactor (GCFR) as typified by the conceptual design of the 300 MW(e) demonstration plant. The major thrust of the study was directed toward the investigation of the probability of potential accident sequences leading to core meltdowns. This involved the determination of the dominant accident sequences and the sensitivity of the results to the reliability values of the shutdown cooling subsystems. However, the potential consequences of core-melt accidents were not investigated.

In the analysis, those potential core meltdowns due to losses of decay heat removal following reactor shutdowns were investigated in detail. Probabilistic models were constructed of the plant responses following the initiation of the reactor shutdown signal. Two such models, called event sequence diagrams (ESD) were constructed. One modelled the plant responses following shutdowns in which the reactor remains pressurized. The other modelled the plant responses following shutdowns due to a prestressed concrete reactor vessel (PCRV) depressurization accident. These are shown in Figures 3.3, 3.4 a, b, c, d, e, f, and 3.5 a, b. c.

The reactor shutdown initiating events were grouped into categories according to their effect on the reactor shutdown cooling system performance. These categories are listed in Table 4-I. Category I. contains all those events which require a reactor shutdown but do not affect the performance of either the main cooling loops or the core auxiliary cooling system (CACS). Category II. contains those events which degrade the performance of the main loop cooling system only. This category contained two important subcategories. Subcategory II.A consisted of those events affecting the performance of a single main cooling loop, and subcategory II.B contained those events which commonly degraded the performance of all the main loops. Catgeory III included the events which commonly degraded the performance of both the main loop cooling system and the CACS. The major subcategories of this group were external events (III.A), internal events (III.B), and support system failures (III.C). The major initiating events in these three subcategories were respectively earthquakes, PCRV depressurization accidents, and reactor shutdowns due to the loss of offsite power.

The reliability of the GCFR shutdown cooling subsystems was evaluated utilizing generic failure data from the RSS. Three contributions to the subsystem failure rate were considered. These were random equipment failures, intra-system common mode failures and equipment unavailabilities due to test and maintenance purposes. The subsystem unit reliability

values and the subsystem test and maintenance unavailabilities are listed in Tables 4-VIII and 4-IX respectively. In order to determine the intrasystem common mode failure probability, a parameter, the beta factor, was utilized. The beta factor was defined as the fraction of unit failures which are common mode failures, and the intra-system common mode failure probability (z) is then determined in terms of the subsystem unit reliability (p) and the beta factor (β) using the following relationship:

$$z = \beta(1-p)$$

Two types of data were investigated in order to determine an appropriate value for the beta factor. These were component failure data, shown in Table 4-VII, and the common mode failure contributions calculated in the RSS for light water reactor systems, shown in Figure 4.7. Both of these types of data indicated a beta factor range of 0.01 to 0.1, but the information was not specific enough to allow a determination of a beta factor for each individual subsystem. Thus, this range was used for each subsystem, the median of this range of 0.03 (assuming a log-normal distribution) was used for each subsystem. These subsystem beta factor values are also given in Table 4-VIII.

For each of the initiating event categories a median point estimate of the probability of a loss of decay heat removal (per reactor shutdown) was calculated, and the sensitivity of this value to each of the three subsystem failure

contributors was investigated. The results of the sensitivity analysis determined those subsystem failures which contributed most to the calculated core-melt probability for each of the initiating event categories. The dominant accident sequences were determined, and the percentage of the core-melt probability, due to accident sequences occurring at different time intervals after shutdown, was investigated as an input to the evaluation of the core meltdown process and to the final accident consequence calculations. The results of the sensitivity analyses are included as Chapter 5.

For each initiating event category, the product of the frequency of the initiating event and the probability of a loss of decay heat removal (per shutdown) yields the probability of a core meltdown (per year). These values are listed in Table 6-I. An estimate of the overall probability of a core meltdown (per year) was determined from the sum of these values. This was evaluated to be 7×10^{-6} per year. It should be emphasized that while this study is a first-cut assessment of the absolute value of the GCFR core-melt probability, it is the relative values of these numbers that has provided quantitative inputs into the overall design evaluation.

The major uncertainty in the median point estimate of the core-melt probability (per shutdown) was considered to be contained in the range of the intra-system common mode failure probabilities as established by the range of the beta factor value. For each initiating event category, the beta

factor range of 0.01 to 0.1 results in a range of the median estimate of the core-melt probability. This uncertainty range was also used to determine a range of the estimated core-melt probability (per year). These ranges are shown in Table 6-I, and they yield a range of the overall core-melt probability of 3×10^{-5} to 3×10^{-6} per year.

Some results from the sensitivity analyses were applied to demonstrate the effect on this value of possible design changes. These are listed in Table 6-V, and given these design changes, it would be possible to reduce the median estimate of the core-melt probability to 3×10^{-6} per year with a range of 1×10^{-6} to 1×10^{-5} per year. However, the overall evaluation of the sensitivity studies indicated that the present design of the GCFR shutdown cooling systems is well balanced. This is discussed further in the next section.

7.2 Comments on the GCFR Shutdown Cooling Design

The results of this study show that the GCFR shutdown cooling system design, consisting of the main loop shutdown cooling system and the CACS, can be capable of maintaining adequate decay heat removal with a high degree of reliability over the entire range of reactor shutdown initiating events. The design feature of providing the initial shutdown heat removal by continued operation of the main loop cooling system is a significant factor contributing to the shutdown cooling reliability. The stored energy of the steam generators is available to drive the helium circulators with the capability

of continuing in this operating mode for at least 30 minutes. Main loop shutdown cooling operation is then continued by driving the helium circulators with auxiliary boiler steam. If at any time main loop failure occurs, the CACS is available to take over core cooling.

The main loop shutdown cooling system design is considered to be quite balanced. Following inadvertent forced reactor shutdowns, the main loop shutdown cooling reliability was slightly under .999, and Table 5-VI showed that the sensitivities of the various main loop shutdown cooling systems were within the same magnitude range. This indicates that the different subsystem failures all contribute more or less equally to main loop unreliability.

The largest contributor to main loop shutdown cooling unreliability is failure of the auxiliary boilers followed closely by the contribution of circulator-turbine small control valve (CT small CV) failures. However, comparison with Table 5-I shows that auxiliary boiler failures are not as significant to the core-melt probability for inadvertent reactor shutdowns. This is due to the fact that auxiliary boiler failures affect main loop operation in the 20 to 30 minute time interval, and in this interval, only a single CACS loop is required. Of the main loop shutdown cooling subsystems, the failure of the CT small CV's contributes most to the probability of a core meltdown. The correct operation of these valves is required to assure main loop availability, and their failure leads to

earlier dependence on the CACS. This is also true of the circulator-turbine large control valves (CT large CV's) and the resuperheater bypass control valves, but the reliability of these valves was determined to be higher than that of the small valve. Thus, these analyses indicate that more improvement can be gained by increasing the reliability of the CT small CV to throttle properly following a reactor shutdown.

The CACS is designed to provide core cooling in the event that main loop shutdown cooling system failure occurs. The contribution of CACS failures to the core-melt probability for most of the reactor shutdown initiating event categories is quite large. However, this is primarily due to two factors. First is that the CACS is more complex than any of the individual main loop shutdown cooling subsystems, and it therefore has a lower unit reliability. Second is that a large percentage of main loop failures occur in the first fifteen minutes after shutdown, and in this time interval, two of the three CACS loops are required for adequate core cooling.

In the final analysis, however, the major contributors to the overall core-melt probability are common mode failures. In fact, the two single largest contributors are the common mode failure of the diesel generators following a reactor shutdown due to a loss of offsite power, and the common mode failure of the CACS for this same event. Powering the auxiliary boilers from the essential electrical buses will reduce the contribution of the accident sequence involving common mode

failure of the CACS. However, the diesel generator dependence still remains.

This review would seem to indicate that a substantial improvement could be gained by design efforts directed at evaluating and reducing potential common mode failures. But this is a simplification of the problem. Considerable design effort has already been directed toward such a goal. In the normal design process, potential common failure modes are eliminated from the design whenever they are detected. The problem essentially lies in the inability to predict the probability of any undetected common mode failures. The beta factor approach to predicting intrasystem common mode failure probabilities is useful in that it provides a consistent methodology and it allows the analyst to utilize presently available failure data. However, while it allows potential common mode failures to be included in the analysis, it does not provide any useful design insight. The uncertainty range of the beta factor value of 0.01 to 0.1 determined the range of the median point estimate of the probability of a core meltdown. In fact, the calculated core-melt probability for the GCFR of 7×10^{-6} per year with a range of 3×10^{-6} to 3×10^{-5} per year compares will with the predicted core-melt probability for LWR's, which is a median value of 6×10^{-5} per reactor year with a 95%-5% confidence range of 2×10^{-5} to 4×10^{-4} per reactor year [1].

In addition to these general comments on the overall shutdown cooling system design, the analysis of the accident sequences has yielded other more specific information. These are summarized below:

(1) Main loop isolation valve failure, resulting in core bypass flow through a failed main loop, is not an important contributor to the probability of a core meltdown. Even following a PCRV depressurization accident, when core flow requirements are strictest, the contribution to the core-melt probability due to isolation valve failures is not predicted to be significant.

(2) Main loop failures due to circulator-turbine imbalance conditions were also not very significant contributors to the probability of a core meltdown.

(3) The effect of restarting initially failed shutdown feedpumps during the main loop operating period was insignificant.

(4) The potential effect of restarting initially failed diesel generators following a shutdown due to the loss of offsite power was determined to be quite significant. However, the realistic benefit to be gained by such efforts is likely to be small due to a relatively low probability of successfully starting an initially failed diesel in the time available.

(5) The core-melt probability is not sensitive to main loop support system faults following reactor shutdowns. In fact the level of arbitrary main loop common mode failures which would significantly affect the core-melt probability is quite high.

A number of potential design improvements have been analyzed in this study, and these are summarized below. Whether any design changes are warranted will depend upon the calculations of the accident sequence consequences, which are needed to complete the risk evaluation, and the analysis of economic (an other) trade-offs.

Auxiliary Boilers. Providing the auxiliary boiler electrical requirements from the essential buses results in a significant decrease in the probability of a core meltdown. These electrical loads are not large and will not cause any significant penalty by increasing the required diesel generator capacity.

Core Auxiliary Cooling System. Increasing the CACS heat removal capability can also result in a decrease in the core-melt probability by allowing successful operation of a single CACS loop sooner after the shutdown. However, this potential design change may not be economically justified until an overall study of the cost benefit of various design changes is evaluated.

Shutdown Feedpumps. Increasing the shutdown feedpump capacity to allow a single main loop to operate for at least 15 minutes produces effectively the same change in the core-melt prob-

ability as the CACS design change, mentioned above, by allowing a single main loop to operate until a single CACS loop is adequate.

Circulator-Turbine Small Control Valves. The continuous operation of these valves, following a reactor shutdown due to the loss of offsite power, is needed to assure proper operation of the main loops and the full conservative use of the stored energy of the steam generator inventories. Decoupling these valves from the instrument air supply, for example, by providing each with a separate air accumulator tank, would allow main loop operation for at least 30 minutes without essential power. This can result in a significant reduction in the probability of a core meltdown.

Throughout the analysis of the accident sequences, a number of design features were found to be quite important. These are summarized below.

(1) It was assumed that each of the CT small CV's was equipped with both an interlock and a monitoring device to assure that the valve is opened during reactor start-up, and to detect valve closings during normal power operation. These actions minimize the probability of a CT small CV being in a closed position prior to a reactor shutdown signal.

(2) It is recommended that the CACS have the capability of starting within 30 seconds. The likelihood that the CACS will be needed this quickly is low, but the potential may exist

for main loop failure within the presently assumed minimum of 2 minutes. For example, a common mode failure of the CT small CV's by failing closed cannot be dismissed. This particular event is very unlikely because it requires a specific failed action on the part of each independent small valve or shutdown controller. However, the probability of occurrence of this event may be likely enough to make it a significant contributor to the core-melt probability if the CACS cannot start quickly enough. GA has begun design investigations regarding the capability of the CACS to provide core cooling in the unlikely event of a sudden, instantaneous loss of the main loop cooling system [2]. It is recommended that these investigations be continued.

Even if all three CACS loops were required to operate for such an event, these would be sufficient to reduce the significance of early main loop cooling system failure events. Also, the 30 second CACS start-up need not be dependent on the diesel generator start-up time. For a simultaneous loss of offsite power and turbine trip, the early common mode failure of the main loop shutdown cooling system should be quite insignificant compared to the dominant accident sequence for this initiating event, which involves the common mode failure of the emergency diesel generators.

(3) One of the major areas of concern in this study involved potential dependencies between the main loops and the

CACS which might lead to a failure of both shutdown cooling systems. In general, the two cooling systems were found to be quite independent. Some potential dependencies involving the service water system and the instrument air system were discussed in Chapter 4, and it is assumed that these potential common mode failures will be eliminated from the design. The major link between the main loop shutdown cooling system and the CACS is their common dependence on essential electrical power. The dominant contribution of the core-melt accident sequences following the loss of offsite power is an indication of the significance of this dependence. Yet in the opinion of this author, the design of the essential electrical system is quite adequate. The essence of this dependence is the relatively short time (compared to light water reactors, and especially the high-temperature gas-cooled reactor) for which the GCFR can maintain core cooling with no essential electrical power available.

(4) Due to the large contribution to the core-melt probability of accident sequences due to reactor shutdowns initiated by the loss of offsite power, the capability of the turbine-generator to withstand a full-load rejection and continue powering the plant auxiliaries becomes increasingly important. Electrical-mechanical control systems for this purpose are utilized in fossil-fired power plants in this country and in

Great Britain. However, their present experience indicates a rather low reliability. Due to the importance of electric power to the ultimate shutdown cooling system performance, efforts to improve the reliability of a full-load rejection system - while not specifically part of a nuclear power plant design - could prove to be very beneficial.

7.3 Comments on the Study Methodology

The major advantage of the event sequence diagram (ESD) methodology is the detail which it allows in the construction of the accident sequences. Detail was included which properly accounted for the operating dependencies of the shutdown cooling subsystems. Also, the possible effect on the overall shutdown cooling performance of a number of operating uncertainties were able to be considered. The ESD identifies each individual accident sequence. This provides information regarding the specific failures which have occurred in the sequence, and the time at which the meltdown is assumed to occur. This is useful information concerning both the calculation of the mechanics of the initial core meltdown process and the calculation of the accident sequence consequences.

The disadvantage of the ESD modeling is the amount of time and effort which is required to model, in detail, the large number of potential accident sequences. The vast majority of the potential accident sequences are very unlikely and do not contribute significantly to the overall core-melt probability. However, it is not always easy to distinguish which accident

sequences are dominant before constructing and analyzing the model. Also, when determining sensitivities, some of the less likley sequences may be important contributors. Therefore, the detailed modelling of all the accident sequence possibilities allows some assurance of completeness.

While the initial investment of work is large, the final ESD model is a very flexible working tool, and modifications can be easily made as they become necessary. Thus, as the GCFR design evolves, the ESD's may be suitably modified as necessary. Also, the modelling is not very sensitive to changes in the specifications or operating requirements of the shutdown cooling subsystems. As long as the overall design bases of the subsystems remains the same, the effect of possible changes in the subsystem unit reliability values can be determined from the sensitivity plots. For example, it is likely that the CACS operating requirements, following a PCRV depressurization accident, will have to be modified to fully account for the effects of air ingress on their heat removal performance. But, as long as the basic CACS design basis of two loops equal to the decay heat load at 2 minutes after shutdown and one loop equal to the decay heat load at 15 minutes, the modelling is unaffected. Even if the overall subsystem design basis were changed, modifications in the ESD's could be easily made.

As the conceptual design of the GCFR progresses, and as more detailed information becomes available, additional

modelling efforts in a number of specific areas may be possible.

1) The ESDs can be extended to model the accident sequences following failure of the reactor to shut down.

2) The modelling of the resuperheater bypass control valve failures is considered to be very conservative. No benefit was allowed from continued main loop operation following failure of this valve to open. However, it may be likely that a main loop can continue operating for some period of time following this failure. For pressurized reactor shutdowns, the helium circulator-turbine steam exhaust pressure is maintained just above the reactor coolant pressure by the lifting of the resuperheater safety and relief valves. The extent of main loop operation in this condition is yet to be reasonably determined, and further modelling will have to await these analyses.

3) The present ESD's consider the plant responses in the first thirty minutes following the reactor shutdown. Extending the modelling to longer time periods after the shutdown would allow the operating reliability of the decay heat removal equipment to be explicitly included in the analysis.

Regarding the actual accident sequence probability calculations, the beta factor approach was used to calculate the intra-system common mode failure probabilities. While this approach is most applicable on a component level, with caution

and judgement, it can be applied to the subsystem level. The advantage of this approach is that it allows a justifiable estimation of the common mode failure probability based on failure data and other sources of failure rate information. However, many questions need to be answered before the beta factor approach can be better extended to the subsystem level. Some of these concerns are listed below:

1) How can a beta factor be better determined for a specific subsystem which may consist of a number of redundant valves and pumps?
2) Are there related effects between the beta factor and the subsystem reliability value? For example, a subsystem with a high reliability may also have a larger beta factor. Because the random failure rate has been decreased, the level of unforseen common mode failures may be proportionally higher. Conversly, a subsystem with a low reliability may have a low beta factor because the random failures may outweigh the potential common mode failures.
3) What is the relationship of the beta factor to the number of redundant items in the subsystem? As the number of redundant units increases, the penalty of applying the beta factor approach indiscriminately is very great and probably unrealistic.

As more failure data regarding multiple component failures becomes available, some of these questions may be answered. However, the effect of uncertainty in the beta factor approach

may be better handled by using more sophisticated calculational techniques. In general, a Monte Carlo calculational approach similar to that used in the reactor safety study could be applied to the entire ESD accident probability calculation. This approach is outlined below as a recommendation of possible future work.

1) The failure data uncertainty can be applied to the calculation of the subsystem unit reliability values to determine an appropriate confidence range and probability distribution function for each of these values.

2) Probability distribution functions can also be determined for each of the subsystem test and maintenance unavailability values.

3) The beta factor range established for each subsystem would then be treated as the confidence limits for the beta factor valve, and an appropriate probability distribution function can be applied to this range.

4) The convolution of all these probability distribution functions through all of the accident sequences of the ESD's can be performed for each of the initiating event categories by a Monte Carlo technique. This will yield a median core-melt probability with the appropriate upper and lower confidence limits.

Appendix A

GCFR Subsystem Descriptions and Failure Probability Quantifications

A.1 Introduction

In this appendix, those subsystems which function in the shutdown of the reactor and in the subsequent shutdown and decay heat removal operations are described in detail. Also presented here are the fault tree diagrams developed for the subsystem failure modes modelled in the event sequence diagram (ESD). Due to the conceptual nature of the GCFR design, the subsystem design bases or configurations may change as the design evolves. Therefore, the subsystem descriptions, which are mostly taken from the Bechtel balance-of-plant study mentioned in Chapter 2, should not be interpreted as final.

The ESD explicitly models the operational dependencies between the main loop shutdown cooling subsystems. Otherwise, the subsystem failures are assumed to be independent. In order to search for possible dependencies between the individual subsystems which were not explicitly modelled in the ESD, the fault tree diagrams were developed. These fault tree diagrams are basically qualitative in nature. They were drawn for the purpose of determining interrelationships which might lead to intersystem common mode failures. However,

these fault tree diagrams also served as guides for evaluating the subsystem unit reliabilities.

The following terms, which are used throughout this appendix, are defined below:

Reliability: This is the probability that a given system or component will perform a desired function in a certain time interval and under specific operating conditions.

Failure Probability: This is the probability that a system or component will suffer a defined failure in a specified period of time. In this study, this is the complement of the reliability.

Demand Probability: For those systems or components that are required to start, change state, or function following an initiating event, this is the probability that the system or component will fail to operate on demand.

Operating Failure Rate: For those systems or components required to operate for a specified period of time, this is the probability per unit time (normally per hour) of a failure occurring. The failure probability for the interval specified is then the operating failure rate multiplied by the time interval.

Unavailability: This is the probability that a system or component will not be capable of operating at a particular time, i.e., it is in a failed state. Availability is the complement of unavailability.

The subsystems to be described are:

- The reactor shutdown systems
- The circulator-turbine large control valve
- The shutdown feedwater system
- The auxiliary steam supply systems
- The emergency electrical supply
- The core auxiliary cooling system
- The resuperheater bypass system
- The service water system
- The service & instrument air system
- The reactor plant cooling water system
- The main circulator service systems.

The majority of these systems belong to the balance of plant (BOP), and their descriptions are taken from the Bechtel BOP design study.

This appendix also includes a description of the other ESD inputs and the range of their valves selected for the sensitivity analysis. These include:

- The loss and restoration of offsite power
- Main loop support systems, and
- Main loop isolation valve operations.

Failure Data

Median point estimates of the subsystem unit failure probabilities were calculated using generic failure data from WASH-1400 (Ref. 1). The median subsystem unit relia-

bilities listed in Chapter 4 are the complements of the valves calculated in this Appendix. A subsystem unit reliability is the reliability of a single independent path of a given subsystem. The basic failure data utilized is included in Table 4-V.

Test and Maintenance Unavailabilities

Equipment outages for either test or maintenance purposes can have a significant impact on the overall failure probability of a subsystem. This unavailability contribution to the subsystem failure probability can be written as

$$Q = \frac{f \times t_D}{720} \qquad \text{where}$$

f is the frequency of test or maintenance equipment outages in average acts per month,

t_D is the average duration of these acts in hours, and,

720 is the number of hours per month.

Because there are no definite test or maintenance schedules for the GCFR demonstration plant equipment, typical equipment unavailabilities from Reference 1 were used to obtain an overall unavailability for each subsystem. These are listed in Table 4-VI. Unavailability contributions were calculated only for those subsystems not operating during normal power operation. The major contribution to these unavailabilities is maintenance acts which were assumed to be

performed on a non-periodic - as needed - basis. Only one of the subsystem independent paths was assumed to be down for test and maintenance purposes at any one time. Also, it was assumed that test or maintenance would not be performed on items of two separate main loop subsystems simultaneously if these items corresponded to different shutdown cooling loops. For example, maintenance would not be performed simultaneously on the shutdown feedpump for main loop A and the auxiliary boiler for main loop B without shutting down the reactor.

Common Mode Failures

The GCFR subsystems have been designed such that single, random equipment failures cannot eliminate more than one of the independent paths. However, common mode failures of these independent paths may result from undetected design errors, manufacturing or installation related errors, maintenance or operator errors, and failures due to common environmental effects. The common mode failures of the independent paths of one subsystem are termed intra-system common mode failures, and a variable term z was incorporated into the random failure probabilities to represent these occurrences Section 4.3-3 includes a more complete description of this intra-system common mode failure term.

An evaluation of this common mode failure probability can be obtained by relating z to the subsystem unit failure

rate. Fleming (Reference 2) defined a term called the "beta factor" for evaluating common mode failures of redundant components.

β = the fraction of total component failures which are common mode failures.

This beta factor can be extended to cover independent paths of a particular subsystem. β then becomes the fraction of subsystem unit failures which result in a common mode failure, and thus

$$z = \beta q \ .$$

Two types of data were investigated in order to get an estimate of the likely range of beta. The first was component failure data from Refs. 1, 3 and 4. Table 4-VII summarizes the fraction of component failures in which more than one item failed. For the individual component types, this data is not statistically large enough for more than an order of magnitude estimate. The second type of information was the actual system failure rate calculations for LWR systems in WASH-1400 (Ref. 5). The failure rate contributions from random failures and from common mode failures were listed. For those subsystems in which there was a common mode failure contribution, a beta factor for that system was calculated. These are listed in Table A-I. However, these numbers are only approximate values, because most of these systems did

TABLE A-I

LWR System Common Mode Failure Fractions (Beta Values)

PWR Systems	Beta Factor
Auxiliary Feedwater System	
. Small LOCA	.003
. Loss of offsite power	.09
Containment Spray Injection System	.092
Consequence Limiting Control System	
Hl Mode	.008
Hl Hl Mode	.012
Low Pressure Injection System	.0009 (1)
High Pressure Injection System	.0009 (1)
Safety Injection Control System	.016
Containment Spray Recirculation System	.012
Low Pressure Recirculation System	.13 (2)
High Pressure Recirculation System	.13 (2)
Containment Heat Removal System	.0013
BWR Systems	
Automatic Depressurization System	.005
High Pressure Service Water System	.048
Emergency Service Water System	.0001
Diesel Generator Systems	
PWR	.33 (3)
BWR	0.03 (3)

(1) Single failures dominate total system failure rate.
(2) Double failures dominate random failure rate.
(3) Following a large LOCA and loss of offsite power only.

not consist of completely independent paths. For example, the Auxiliary Feedwater System has three redundant, diverse pumps feeding two headers which pass through the containment where each header then supplies the three main feed lines.

The majority of the component failure data indicated either design inadequacy or human error as the cause of the common mode failures. The common mode failure contributions calculated in WASH-1400 were mostly the result of human errors (i.e. all valves of a redundant system were left in a failed position following routine testing or maintenance). The range of beta factors is rather large due to the wide variety of system involved. However, the vast majority of the systems and component types have a beta factor between 0.003 and 0.1. The only beta factor which is significantly greater than 0.1 concerns diesel-generator failure following a simultaneous loss of offsite power and loss of coolant accident for a PWR. The potential common mode failure results from the inrush of current due to the essential electrical loads which must be assumed upon starting. The common mode failure probability is greater for the PWR than the BWR due to the larger electrical load for the PWR in this event.

In the GCFR demonstration plant design, the diesel generators are not required to assume large loads immediately upon starting due to the capability of initially continuing main loop operation independent of the electrical supply. Therefore, this potential common mode failure should not be a significant concern.

It is the author's feeling that a beta factor of 0.01 is reasonable for a system of redundant units in which considerable design effort has been spent toward minimizing potential common mode failures. However, a range of 0.01 to 0.1 was chosen as the range of beta for all the GCFR subsystems. This range of the beta factor is consistent with the available data and it allows for potential common mode failures due to unforeseen environmental effects. A median beta factor value of 0.03 was chosen for all GCFR shutdown cooling subsystems. While it is reasonable to assume that these subsystems would have different beta factors, the available data was not detailed enough to justify any distinction between the subsystem beta factor values. Table 4-VIII listed the subsystem beta factor values, and Table A-II summarizes the subsystem unit failure probabilities and test and maintenance unavailabilities of the shutdown cooling subsystems.

TABLE A-II

A List of Subsystem Unit Failure Probabilities and Test and Maintenance Unavailabilities

Subsystem Index and Name	Subsystem Unit Failure Probability	Test and Maintenance Unavailabilities
4: CT large* CVs	1.3×10^{-3}/d	---
5: CT small* CVs	3.3×10^{-3}/d	---
6: Shutdown Feed-water System	2.6×10^{-3}/d	4.0×10^{-3}
7: Auxiliary Boilers	8.1×10^{-3}/d	1.2×10^{-2}
8: Main Loop Decay Heat Removal Operation	6.2×10^{-3}/d	4.0×10^{-3}
9: Emergency Electrical Supply	3×10^{-2}/d	6.0×10^{-3}
10: Core Auxiliary Cooling System	8.3×10^{-3}/d	1.2×10^{-2}
12: Resuperheater Bypass Control Valves	1.4×10^{-3}/d	2.0×10^{-3}

* Normally operational, therefore no test and maintenance unavailability was assumed.

A.2 Fault Tree Analysis

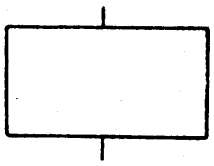
A fault tree is a logic diagram used to display the possible modes of occurrence of a particular undesired event. This event is the top fault event in the tree, and those fault events which lead to this undesired event are described below the top event and are logically linked to it.

Fault tree analysis is the formalized, deductive process for identifying and linking the possible failure paths which lead to the undesired event (Ref. 6).

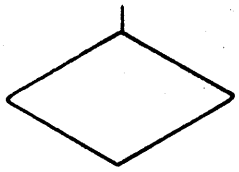
In simple terms, a fault tree is built by starting with the undesired event and then by determining which failure events will immediately cause the top event. This process of determining the failure events leading to a fault event already described in the tree can theoretically be continued until the basic attributable causes of the undesired event are determined. However, the degree of complexity to which the tree is developed is generally decided by the amount of information available concerning the system being analyzed, the purpose for which the fault tree is to be used, and the amount of time and effort the analyst is willing to put into developing the tree.

The types of symbols used in building a fault tree are described below.

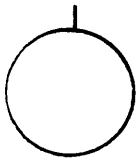
Symbols



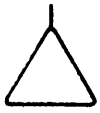
The Rectangle is used to identify an event, which is usually a failure event, that results from the combination of fault events through a logic gate. Thus an event described by a rectangle is always expanded further into failure events which result in its occurrence.



The Diamond describes a fault event which is considered basic to the particular fault tree in which it appears. The cause of the event has not been developed further. This may be due to a low probability of occurrence of the event, or lack of information, time or money.



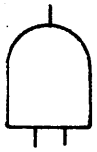
The Circle describes a basic fault event that requires no further development. The frequency and mode of failure of these events are derived from emperical data.



The Triangle is used as a transfer symbol. A line from the apex of the triangle denotes a transfer into the tree at this point. A line from the side of the triangle identifies that portion of the tree below the triangle with the transfer symbol indicated inside the triangle. Also, whenever a fault tree is spread over several pages, a number is often indicated

near a transfer in which indicates where the part of the tree indicated is located.

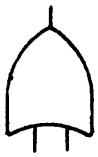
Logic Gates



The AND gate describes the logical operation which requires that all of the input events exist before the output event is produced. In boolean terms, it is the intersection of the events, and it is defined (for output event C and input events A and B) as

$$A \cap B = C \quad \text{or} \quad A \cdot B = C.$$

If the two events, A and B, are independent, then the probability of the output event is the product of the probability of the input events.



The OR gate describes the logical operation in which the output state will exist if any one or more of the input events exists. In boolean terms this is the union of the events, and it is defined as

$$A \cup B = C \quad \text{or} \quad A + B = C.$$

The probability expression for the output event is

$$P(C) = P(A) + P(B) - P(A \cdot B) .$$

However, if the probability of events A and B are both much less than one, then the probability

of the output event is, to a very good approximation the sum of the input events.

A.3 The Reactor Shutdown System

The reactor shutdown system in the GCFR consists of three sections. These are 1) the input parameter sensors and circuitry, 2) the reactor trip logic circuitry up to the rod trip mechanisms, and 3) the control rod and shutdown rod trip mechanisms.

The input parameter sensors are arranged in a two out of three voting logic, and there are at least two separate trip parameters for every anticipated plant event requiring a reactor shutdown. The present list of plant protection system trip parameters is included as Table 2-V (Reference 8).

The input parameter sensors are common to both the control rod system and the shutdown rod system. However, each rod system has its own trip logic circuitry leading to the rod trip mechanisms.

Shutdown of the nuclear reaction can be accomplished by either the control rod system or the shutdown rod system, and both systems are activated with every reactor shutdown signal. The control rod system is a set of 21 rods and drives. Each control rod is contained in a control fuel element, and each rod has a reactivity worth of 85¢. The neutron absorber material contained in the rods is boron

carbide (B_4C), and the constant rod worth (independent of the rod location in the core) is accomplished by varying the enrichment of isotope B-10 in the absorber material.

The control rods are connected to their drive mechanisms by electromagnetic couplings which are de-energized by the reactor shutdown signal. Control rod shutdown insertion is then accomplished by a gravity drop after an initial spring assist which helps to insure the de-coupling of the electromagnet. The rod kinetic energy is absorbed at the end of the insertion by a fly-wheel type absorber. There is also an impact energy absorber built into the control fuel element which can absorb the rod kinetic energy in the event of a fly-wheel failure. The stepping motor, which provides the normal rod control motion, also follows the rod.

The shutdown rod system is a set of six rods which are similar in design to the control rods. They are also located within control fuel elements, but they are always totally withdrawn from the core during normal reactor operation. Each shutdown rod has a reactivity worth of 1.60$, and the rods themselves are constructed without wearing rings to increase the diametral clearance upon insertion.

The shutdown rod drive mechanisms are quite diverse from the control rod drives. The shutdown rod drive mechanisms are high-speed direct current motors, and the shut-

down rod are mechanically coupled to their drivers. The power supply for these drive mechanisms comes from independent storage batteries for each drive mechanism.

The powered insertion of the shutdown rods, coupled with their larger diametral clearance, provides positive a assurance that the rods will be inserted even in the event of core distortions more severe than anticipated.

The fault tree diagram for the failure of the reactor to shutdown is included as Figure A.1. GA (Reference 9) estimates a failure rate of less than 10^{-9} per demand for the reactor shutdown system. This is based on the following:

1) A failure rate of 1×10^{-9} per demand for the input parameter sensors is assumed because of the availability of at least two separate trip parameters. It is based on a daily check-out of sensor values, a weekly check-out of the circuitry, and analyses done on similar HTGR protective circuitry.
2) A failure rate of 1×10^{-6} per demand for the logic circuitry leading to the trip mechanisms is also assumed from HTGR analyses.
3) A failure rate of 1×10^{-2} per demand per rod is assumed for both the control rod and shutdown rod trip mechanisms.

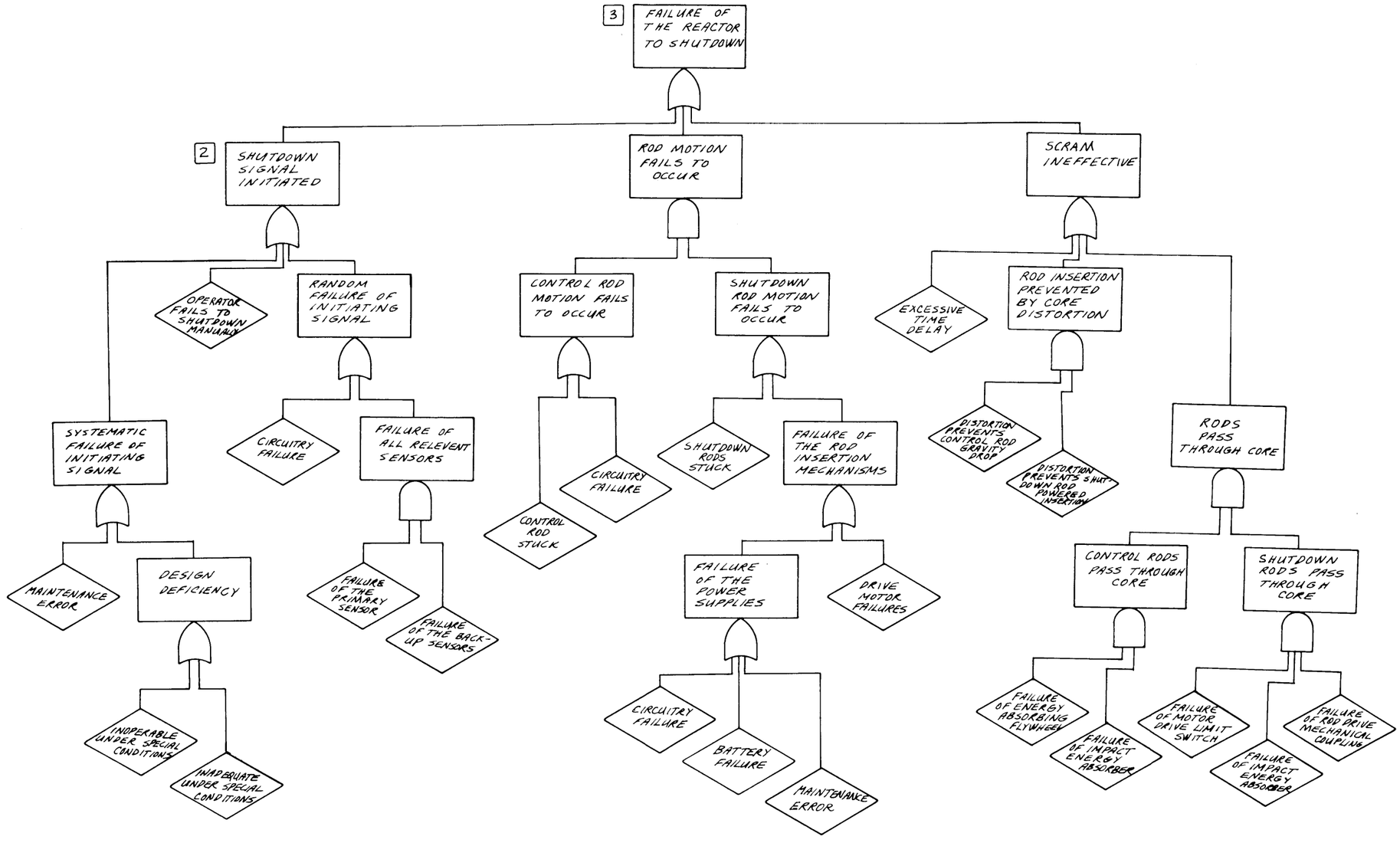


FIGURE A.1 FAULT TREE DIAGRAM: REACTOR SHUTDOWN SYSTEMS

Shutdown of the reactor at the most demanding condition, the beginning of cycle, requires the insertion of at least 5 of the 10 control rods that are entirely out of the core. Under these same conditions, insertion of 3 of the 6 shutdown rods are required for reactor shutdown. This leads to a probability of less than 3×10^{-10} per demand to fail to insert the necessary 5 control rods and to a probability of less than 2×10^{-7} per demand to fail to insert at least 3 shutdown rods.

Figure A.2 is a schematic of the plant protection system reactor shutdown logic. The control rod path requires both b_1 and c_1 and the probability of failing is 1×10^{-6}. The shutdown rod path requires both b_2 and c_2, and the probability of either failing is 1.2×10^{-7}. Failure to shutdown requires that either the input parameter sensors fail (1×10^{-9}) or that both rod systems fail (1.2×10^{-12} assuming no common mode failures). Thus, the input parameter sensors dominate the failure probability.

RSS analysis indicates that a failure rate of 1×10^{-5} per demand is attainable with a single shutdown system. The two diverse shutdown systems of the GCFR should be able to achieve a much lower failure rate, however because both systems are essentially rod-type systems, common mode failures will likely be the limiting factor in the shutdown reliability.

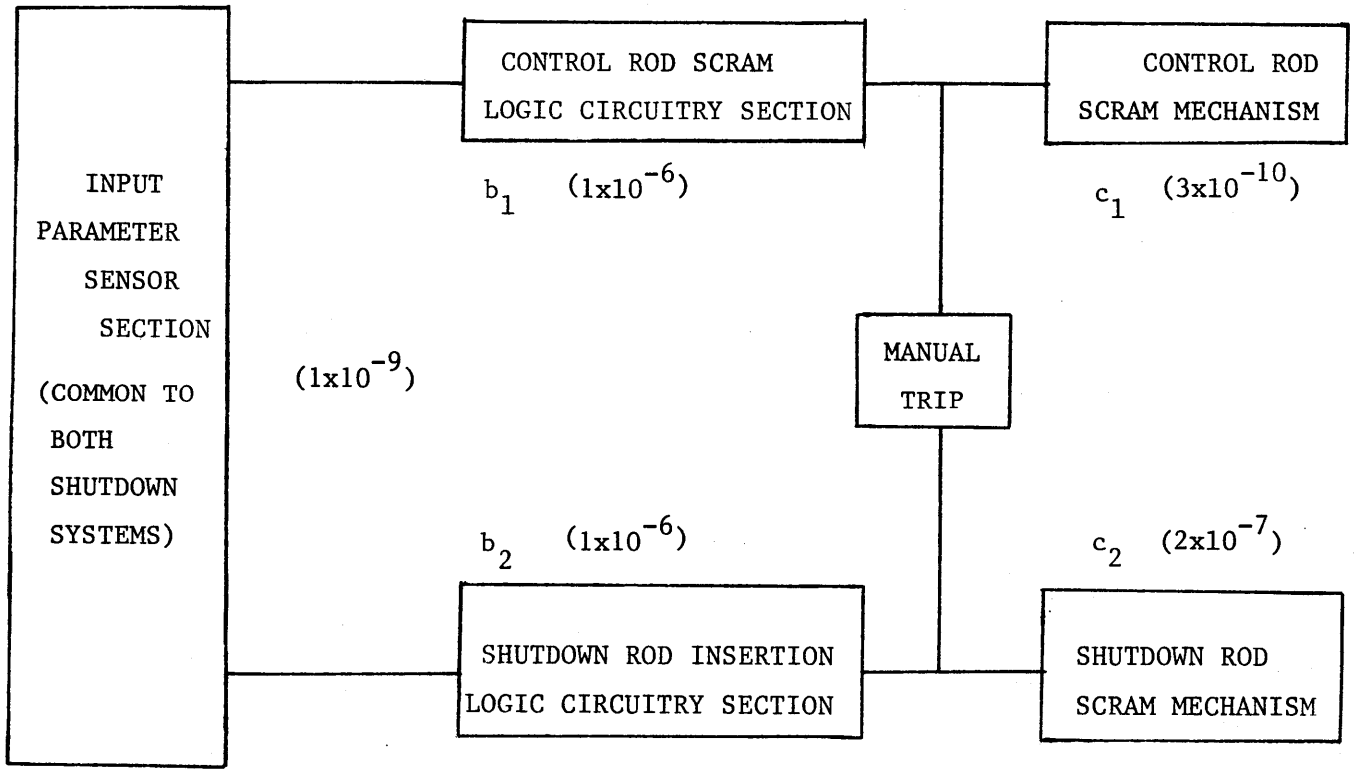


FIGURE A.2 Block diagram of the plant protection system reactor shutdown logic

A.4 The Circulator-Turbine Large Control Valves

These valves, one for each main loop, are designed to provide normal control of the circulator-turbine speed.

The pertinent valve design data are listed below:

Size and Rating	10" - 2500 lb ANSI
Type	"DRAG"
Material	2 - 1/4% CR; 1% Mo
Actuator	Air Piston
Nominal Flow Rating	100% loop flow (775,000 lb/hr)
Nominal Inlet Pressure	2900 psia
Nominal Inlet Temperature	875°F
ΔP at Rated Flow	120 psi
Valve Closing Time	3 seconds

During a reactor shutdown, these valves are designed to close rapidly (in three seconds) in order to prevent over-cooling of the core and to conserve the steam/water inventory in the steam generator. The "close" signal, which is generated by the plant protection system (PPS), requires both the shut-down initiation signal and a verification signal that the reaction has indeed stopped. The verification signal is by means of a neutron flux level sensor, and its purpose is to assure that the reactor is actually shutdown before the cooling capability of the main loops is reduced.

Failure of this valve to close during the initial phase of the shutdown process would cause the steam generator inventory for the loop to be depleted very quickly (about two minutes). This results in the loss of the shutdown cooling capability of this main loop, and so this particular failure mode of the valve was analysed.

The fault tree diagram for failure of this valve to close, given a reactor shutdown, is included as Figure A.3. Note that the valve requires instrument air to function, however, the amount of air normally in accumulator tanks should be more than sufficient to close all of these valves.

Both the circulator-turbine control valves along with the entire main loop steam piping system inside the containment building are designed to seismic category I specifications.

A failure rate of 1.3×10^{-3} per demand was calculated for each individual valve. This was based on the following:

Failure of valve to close	$3 \times 10^{-4}/d$
Failure of the valve control system	$1 \times 10^{-3}/d$
	$1.3 \times 10^{-3}/d$

No test and maintenance unavailability was assumed for these valves since they are normally operational. Two potential common mode failure contributors were identified. These

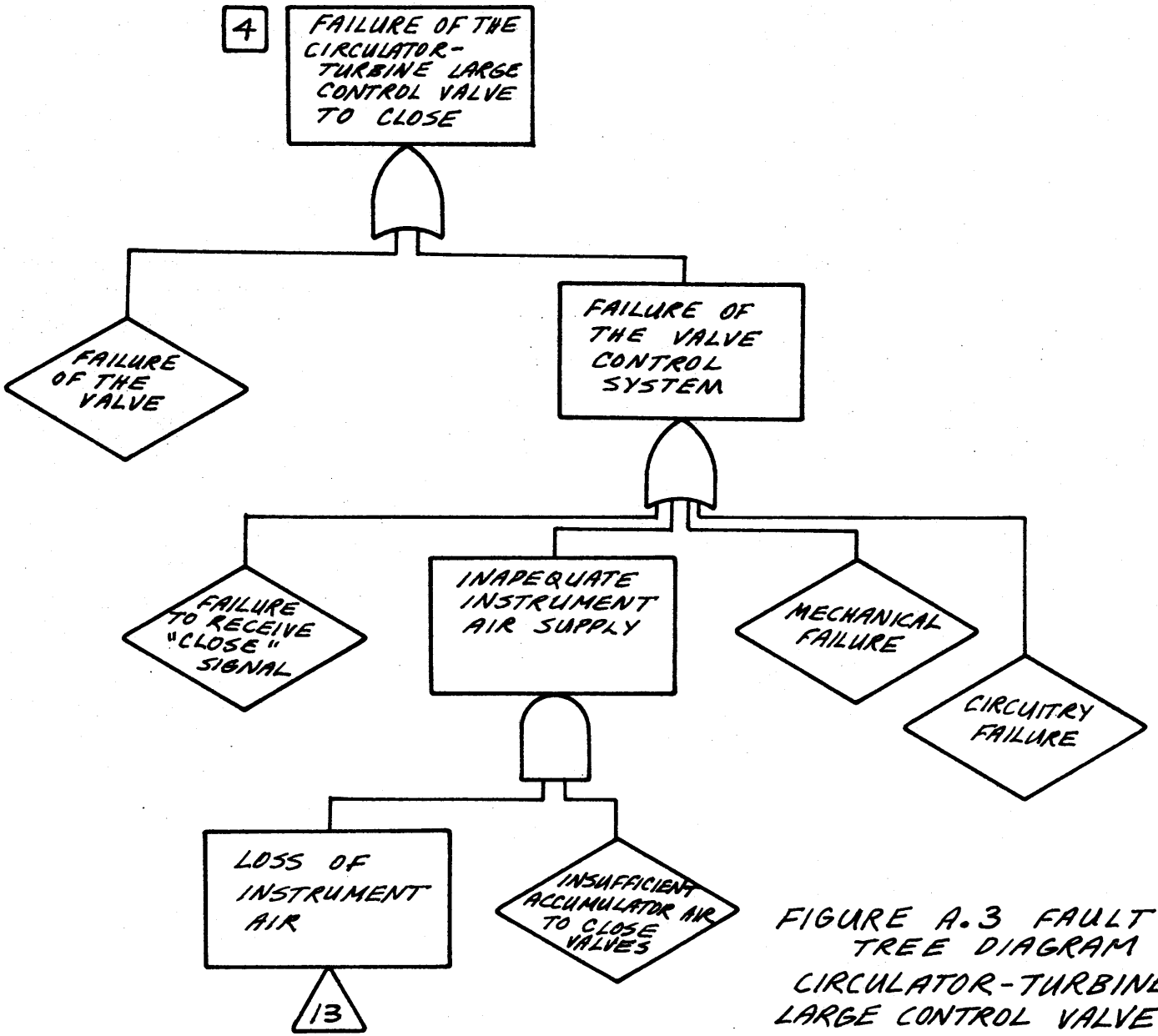


FIGURE A.3 FAULT TREE DIAGRAM : CIRCULATOR-TURBINE LARGE CONTROL VALVE

are the failure of the "close" signal and the interruption of instrument air to the valve. The latter would be eliminated by supplying each valve with an individual air accumulator.

A.5 The Circulator-Turbine Small Control Valves

These valves, one per each main loop, function during the shutdown heat removal operations (roughly that period following the reactor shutdown until the auxiliary steam supply is available) to control the circulator-turbine speed. These valves are located in a parallel flow circuit with the circulator-turbine large control valves, and they are fully open during the normal reactor operations. In the event of a reactor shutdown, the CT large CV for each loop is designed to quickly close. However, the CT small CV remains open in order to maintain the steam flow to the circulator-turbine.

The pertinent valve design data are listed below:

Size and Rating	3" - 2500 lb ANSI
Type	"DRAG"
Material	2-1/4% CR; 1% Mo
Actuator	Air Piston
Nominal Flow Rating	12% Loop Flow (106,000 lb/hr)
Nominal Inlet Pressure	2900 psia
Nominal Inlet Temperature	875°F
ΔP at Rated Flow	120 psi

During the shutdown heat removal process, the valve throttles close in order to control the circulator-turbine speed (thus the helium flow) and maintain core temperatures within acceptable limits.

The control of this valve is governed by two competing concerns. These are 1) conserving the steam generator inventory; thus prolonging the effective operation of the main loops; and 2) limiting the core temperature excursion. The first concern requires a quick throttling of the valve, but it results in higher core temperatures. The second requires a slower throttling rate to limit core temperatures, but it effectively limits the possible operating duration of the main loops. The presently proposed control of this valve is a compromise. The valve is initially quickly throttled to about 6% of the fuel loop flow followed by a slow ramp down to two percent of the loop flow at about fifteen minutes after the shutdown. The valve remains at two percent flow until auxiliary steam is available at which time the valve is closed.

Failure of the valve to throttle close (it is assumed that the valve remains full open) would result in the depletion of the steam generator inventory for the main loop involved. This failure eliminates the loop, however, the period of operation of the loop is longer than the case where the CT large CV fails to close. The fault tree

diagram for this failure mode - CT small CV fails to throttle, given a reactor shutdown - is included as Figure A.4. Note that the operation of the valve depends both on uninterruptable AC power and on a supply of instrument air. The accumulated air in the instrument air system was assumed to be sufficient to perform only the initial valve throttling, and the loss of instrument air results in the failure of the valve to fully perform its stated goal.

There is another failure mode for these valves which must be discussed. It is the failure of the valve by being closed prior to the shutdown signal, or failure of the valve by closing upon receipt of the shutdown signal. Either of these cases results in a rapid interruption of steam to the circulator-turbine which quickly eliminates the main loop. The design presently provides for procedures to minimize the possibility of the small valve being closed prior to a shutdown. This requires that the CT small CV always be opened before the CT large CV. An electrical interlock could also easily be provided which would inhibit the reverse action. However, the most promising method to minimize this occurrence would be an operational monitoring device which confirmed steam flow through the valve during power operation (during full power operation, only about 2% of the steam flow passes through the smaller valve due to its higher flow resistance).

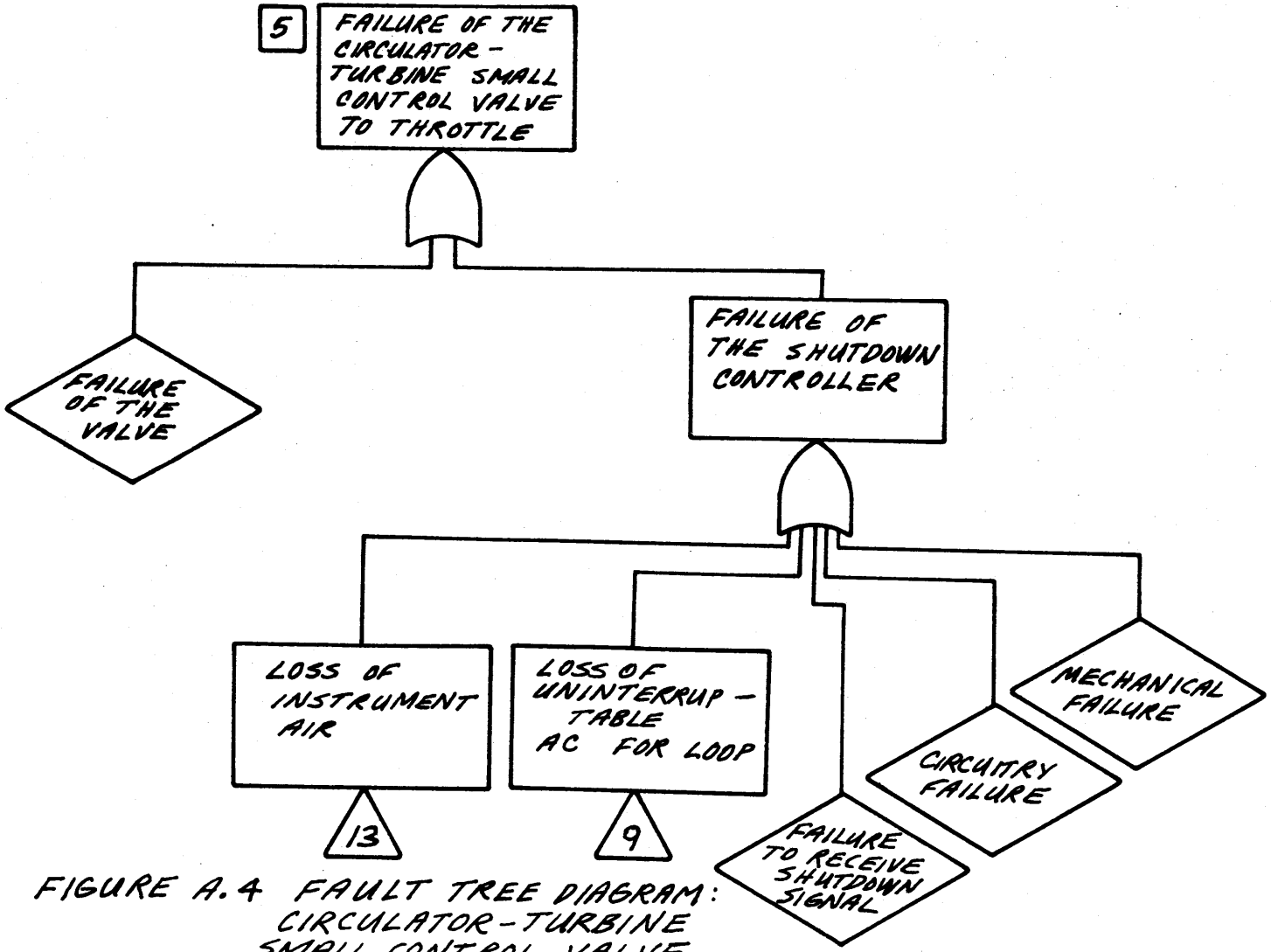


FIGURE A.4 FAULT TREE DIAGRAM: CIRCULATOR-TURBINE SMALL CONTROL VALVE

Concerning full closing of the valve following the shutdown signal, the shutdown controller is not designed in sufficient detail to determine any mechanisms for this failure mode. However, the probability that the valve would fail by this mode was considered to be much less than the failure to throttle mode. The impact of this assumption was discussed in Chapter 5.

A failure rate of 3.3×10^{-3} per demand was calculated for failure of this valve to throttle. This was based on the following:

Mechanical failure of the valve	3×10^{-4}/d
Failure of the shutdown controller	3×10^{-3}/d
	3.3×10^{-3}/d

No test and maintenance unavailability contribution was assumed for these values. Maintenance would require the loop to be shutdown, and testing should not inhibit the proper functioning of the valve.

A.6 The Shutdown Feedwater System

This subsystem is an independent feedwater supply for the main loop cooling system, and it is used during reactor start-up and also for shutdown and decay heat removal operations. The system, which is shown schematically in Figure A.5, consists of three separate feedwater circuits - one for each of the main loops. Each circuit is designed

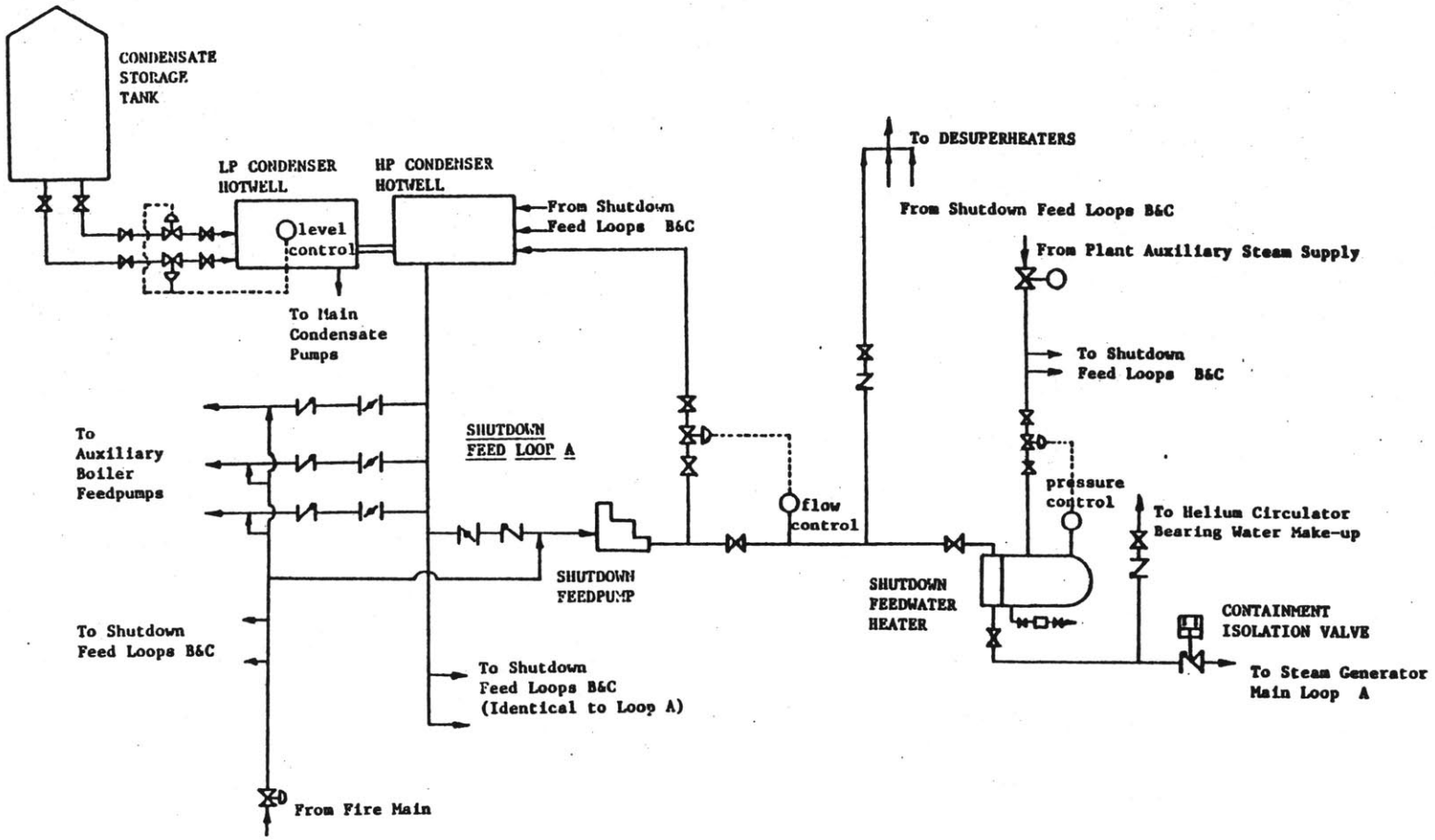


FIGURE A.5 A Schematic Flow Diagram of a Shutdown Feedwater Loop

to supply three percent of the full-load feedwater flow and each circuit consists of a feedwater heater and a positive displacement feedpump powered by an electric motor. The motor for each pump is energized from a separate essential electrical bus, and the feedwater heaters are pegged from the auxiliary steam system to prevent thermal shock to the steam generators following a reactor shutdown. This feedwater system also supplies the spray-water requirements for the desuperheaters.

Each shutdown feedpump takes a suction from a common line connected to the condenser hotwell. Feedwater flow control is accomplished by means of a bypass line back to the condenser hot well, and the feedwater, after passing through the heater, must pass through a containment isolation valve before entering the steam generator.

The common suction header from the condenser hotwell also supplies the auxiliary boiler feedpumps, and the condensate storage tank (400,000 gallon capacity) is available through the condenser and can provide the full required condensate flow through the make-up lines. An additional source of emergency feedwater is provided from the fire main.

The entire system, up to but not including the containment isolation valve is not designed as a seismic category I system.

The fault tree diagram for failure of the system to supply feedwater to the steam generators, given a reactor shutdown is included as Figure A.6.

Shutdown feedwater can be lost due to failures in the individual supply loops or due to failures in the condensate supply. The operation of the condensate make-up valves requires both instrument air and uninterruptable AC. However, these dependencies are unimportant due to the dominating failure of the CT small CV if either instrument air or uninterruptable AC is unavailable.

A failure rate of 2.6×10^{-3} per demand was calculated for each of the individual shutdown feedwater supply loops based on the following:

Shutdown feedwater pump fails to start	1×10^{-3}/d
Pump control system failure (circuit breaker failure dominates)	1×10^{-3}/d
Check valve failure	1×10^{-4}/d
Bypass flow control valve failure	3×10^{-4}/d
Isolation valve fails to remain open	1×10^{-4}/d
	2.6×10^{-3}/d
Test and Maintenance Unavailability	4×10^{-3}

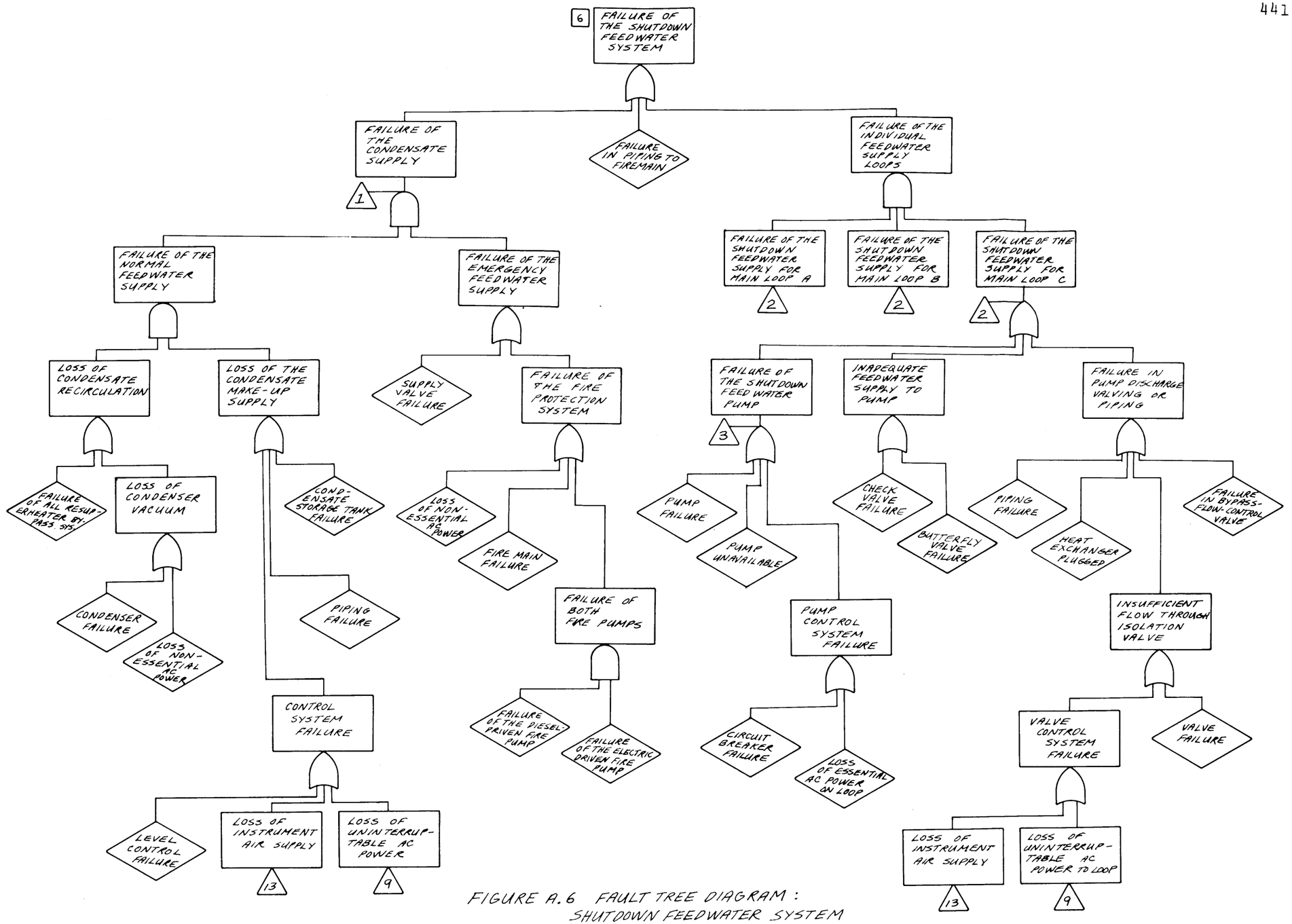


FIGURE A.6 FAULT TREE DIAGRAM : SHUTDOWN FEEDWATER SYSTEM

The test and maintenance unavailability used is based on the sum of unavailabilities for the major pieces of equipment in each shutdown feedwater supply loop. These are the shutdown feedwater pump and the shutdown feedwater heater. An unavailability of 2×10^{-3} was assumed for each due to test or maintenance purposes. This corresponds to a total unavailability of three hours per month for each shutdown feedwater loop. No unavailability contribution was assumed for the isolation valve because, it was assumed that the loop would have to be shutdown in order to perform maintenance on this valve.

A.7 The Auxiliary Steam Supply System

This system provides steam to drive the main helium circulator turbines and bearing water pump turbines during plant start-up and during decay heat removal operations following a reactor shutdown. It consists of three complete steam boiler units, and each unit provides steam for a single main loop circulator. During normal reactor operation, the boilers are maintained in a hot standby condition such that they can be brought to rated conditions in about twenty minutes.

Each auxiliary boiler is rated to supply 60,000 lb/hr of steam at 150 psig and 750°F, and each unit is equipped with an auxiliary boiler feedwater pump and an auxiliary boiler fuel oil pump. The boilers use No. 2 diesel oil as fuel,

and two separate fuel oil storage tanks provide enough fuel for five days of operation. A schematic diagram of this system is provided in Figure A.7.

The three auxiliary boilers are located in a single building adjacent to the control building. Each boiler is a package unit with integral superheaters, air atomizing equipment, piping and controls. The auxiliary boiler feedwater pumps are vertical multistage centrifugal type, and the feedwater supply is taken from the shutdown feed pump suction header leading from the condenser hotwell. The fuel oil pumps are screw type and take suction from the fuel oil tanks.

During normal operation, the boilers are maintained in a "hot standby condition by steam heater coils which are provided in the lower drum to pressurize the boiler and place it in a quick restart condition. Steam for these coils is provided from the main steam supply through a desuperheater.

The initiation of a reactor shutdown signal also initiates the process of bringing the auxiliary boilers to their rated condition. Failure of the boiler to reach its rated steaming conditions within twenty minutes of the shutdown signal was considered to constitute a failure of the system, and the fault tree diagram for this failure mode is included as Figure A.8.

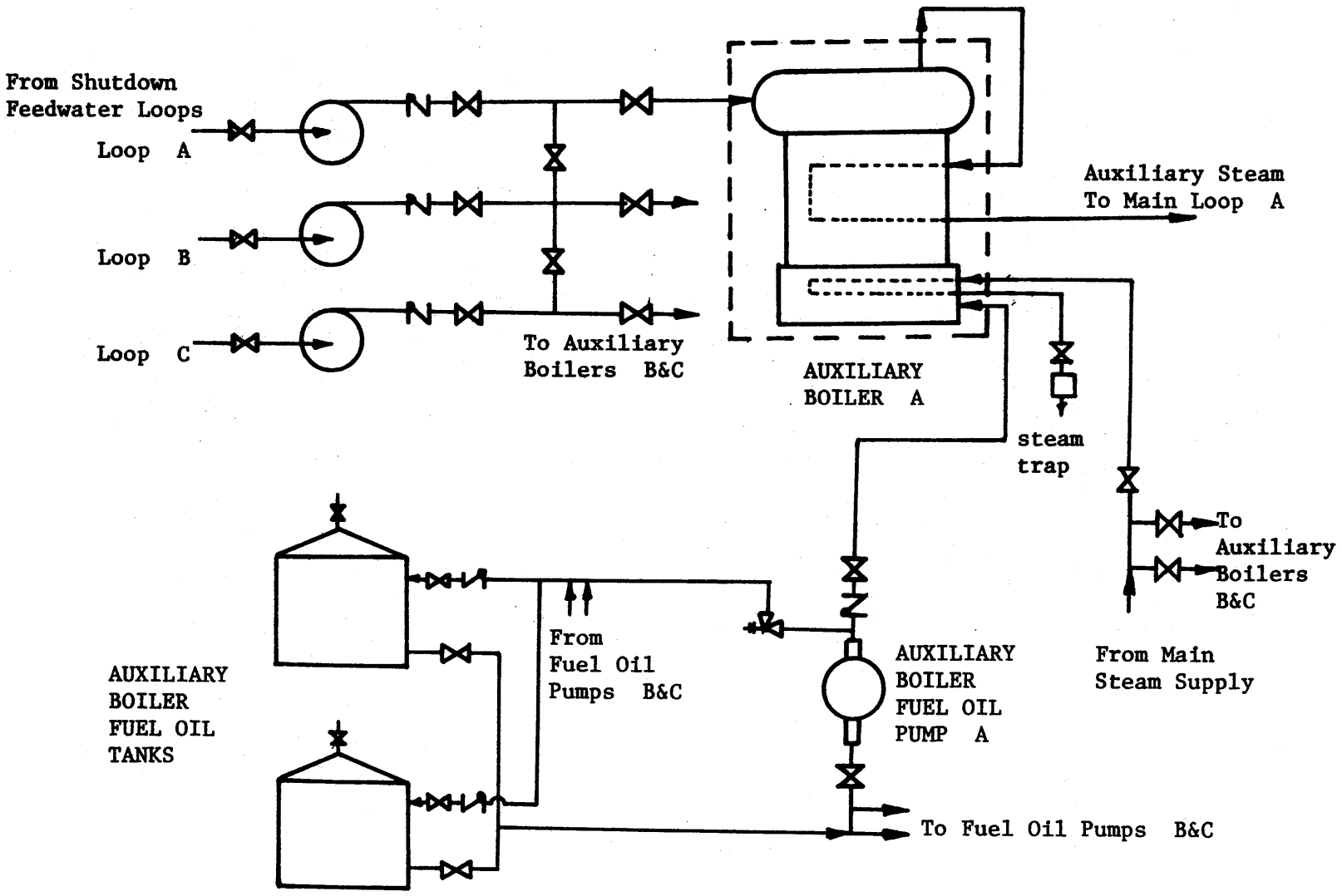


FIGURE A.7 Schematic Flow Diagram of an Auxiliary Boiler Steam Supply

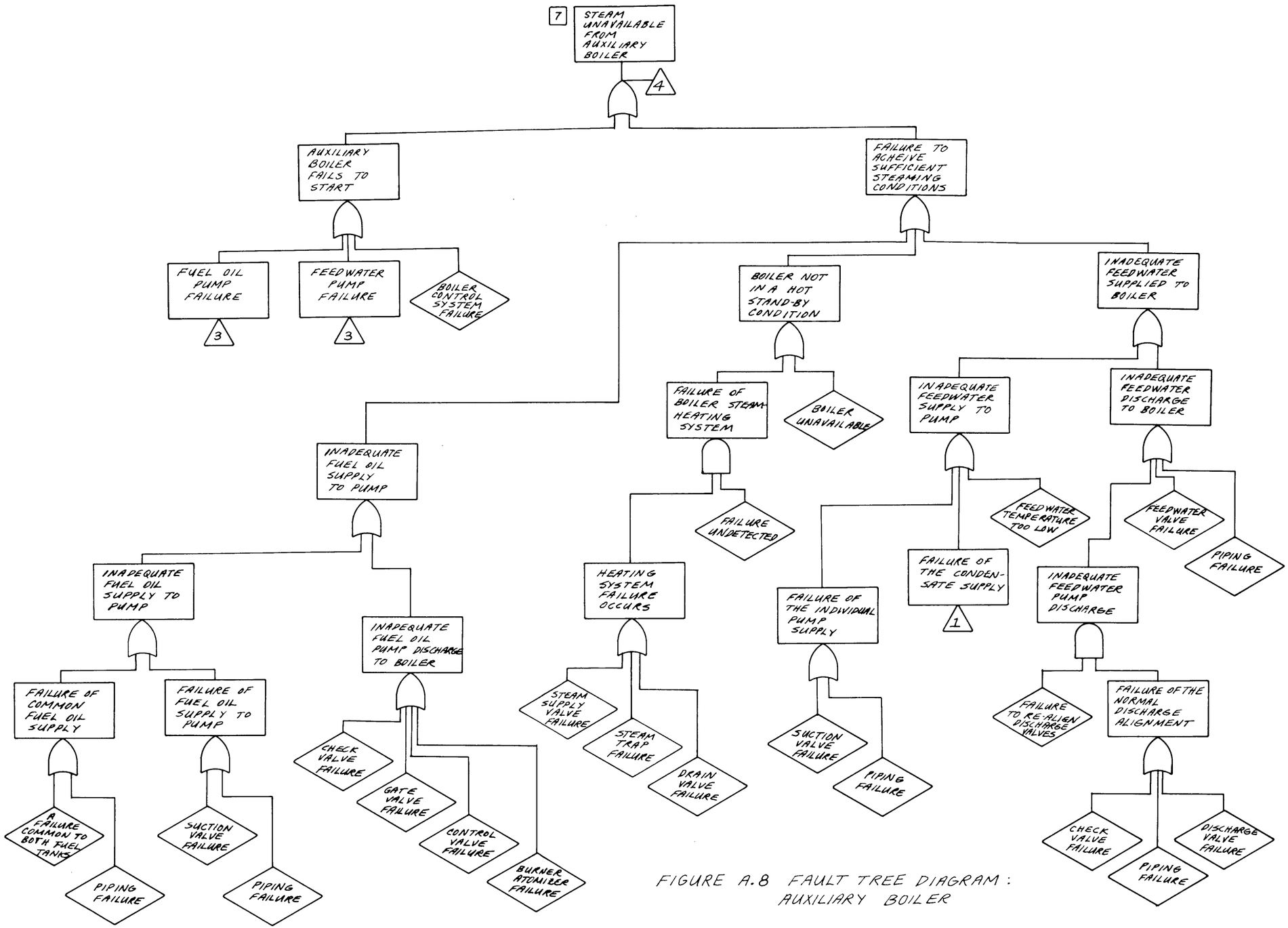


FIGURE A.8 FAULT TREE DIAGRAM: AUXILIARY BOILER

A failure rate of 8.1×10^{-3} per demand was calculated for each auxiliary boiler based upon the following contributions.

Fuel oil pump fails to start	1×10^{-3}/d
Fuel oil pump circuit breaker failure	1×10^{-3}/d
Feedwater pump fails to start	1×10^{-3}/d
Feedwater pump circuit breaker failure	1×10^{-3}/d
Fuel oil control valve failure	3×10^{-4}/d
Feedwater control valve failure	3×10^{-4}/d
Fuel oil check valve failure	1×10^{-4}/d
Feedwater check valve failure	1×10^{-4}/d
2 Feedwater gate valve failures	2×10^{-4}/d
Fuel oil gate valve failure	1×10^{-4}/d
	8.1×10^{-3}/d
Test and maintenance unavailability	1.2×10^{-2}

The test and maintenance unavailability is based on the sum of the unavailabilities of the major system components, with an unavailability of 2×10^{-3} assumed for the fuel oil pump, the fuel oil control valve, and the feedwater control valve. An unavailability of 6×10^{-3} was assumed for the boiler itself. The total unavailability is equivalent to almost nine hours of downtime a month for each auxiliary boiler unit. No maintenance unavailability was assumed for the boiler feedwater supply pumps, due to the valve cross-connections which

allow the two available pumps to supply all three boilers.

A.8 Main Loop Transfer To Long Term Decay Heat Removal Operation

Following a reactor shutdown, after the auxiliary boilers have reached their rated steaming conditions, auxiliary steam must be supplied to the main loops to drive the main helium circulator turbines and bearing water pumps. At the same time, the main steam generator discharge must be diverted around the circulator turbine and to the main condenser. A skematic flow diagram for this process, which indicates the required valve operations, is shown in Figure A.9. The sequence of these valve operations is as follows.

1) The steam generator alternate discharge valve is opened.
2) The auxiliary steam supply valve to the circulator-turbine is opened, and the auxiliary steam supply valve to the bearing-water pump turbine opened.
3) Lastly, the auxiliary steam supply is isolated from the steam generator alternate discharge path by closing the circulator-turbine small control valve, and the main steam supply valve to the bearing-water pump turbine.

The fault tree diagram for failure to supply auxiliary steam to the main loops to allow main loop long term decay heat removal is included as Figure A.10. Instrument air is required for some valve functions in this subsystem. However,

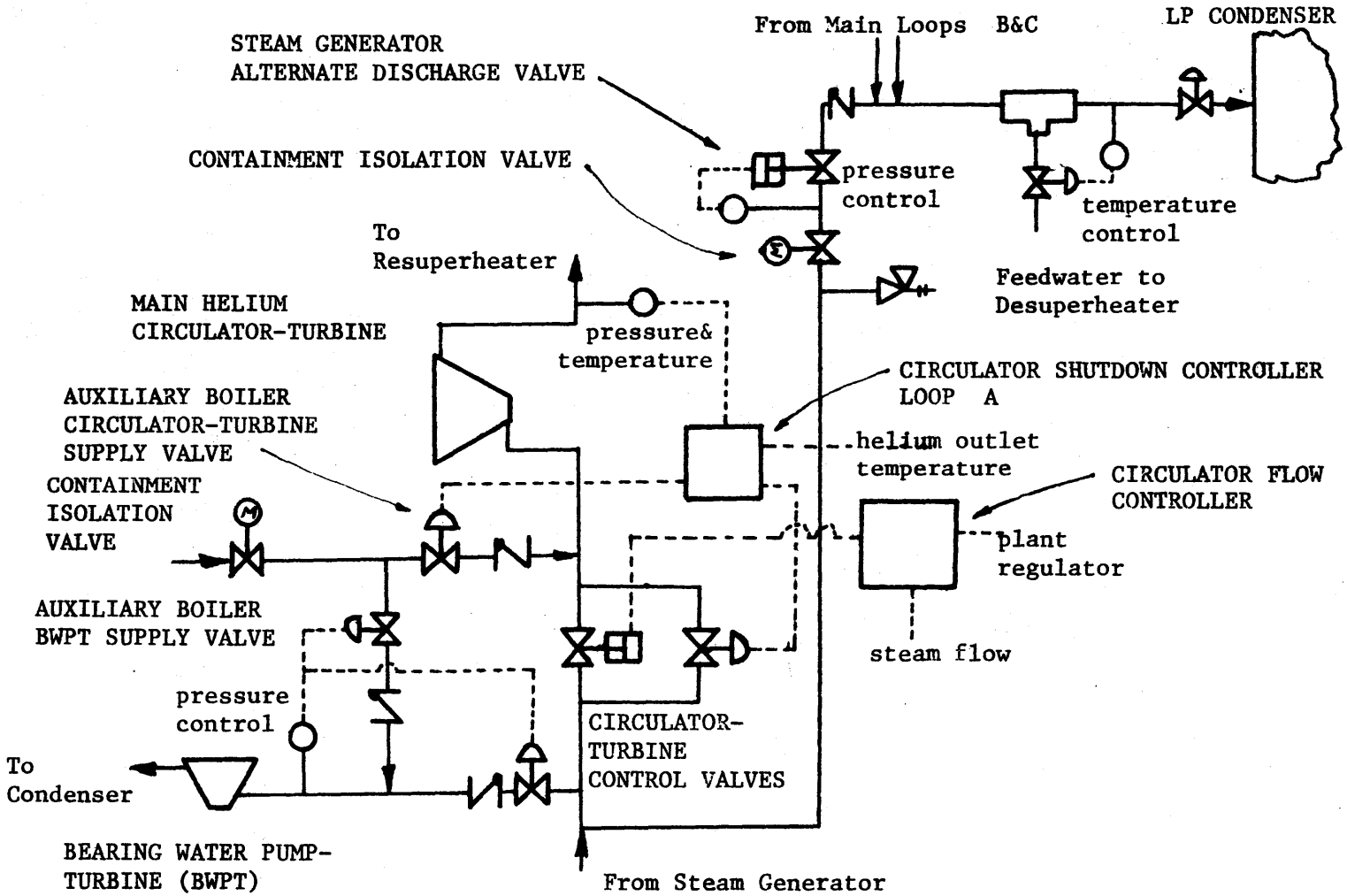


FIGURE A.9 A Schematic Diagram of Valves and Control Systems for Main Loop Transfer to Decay Heat Removal Operation

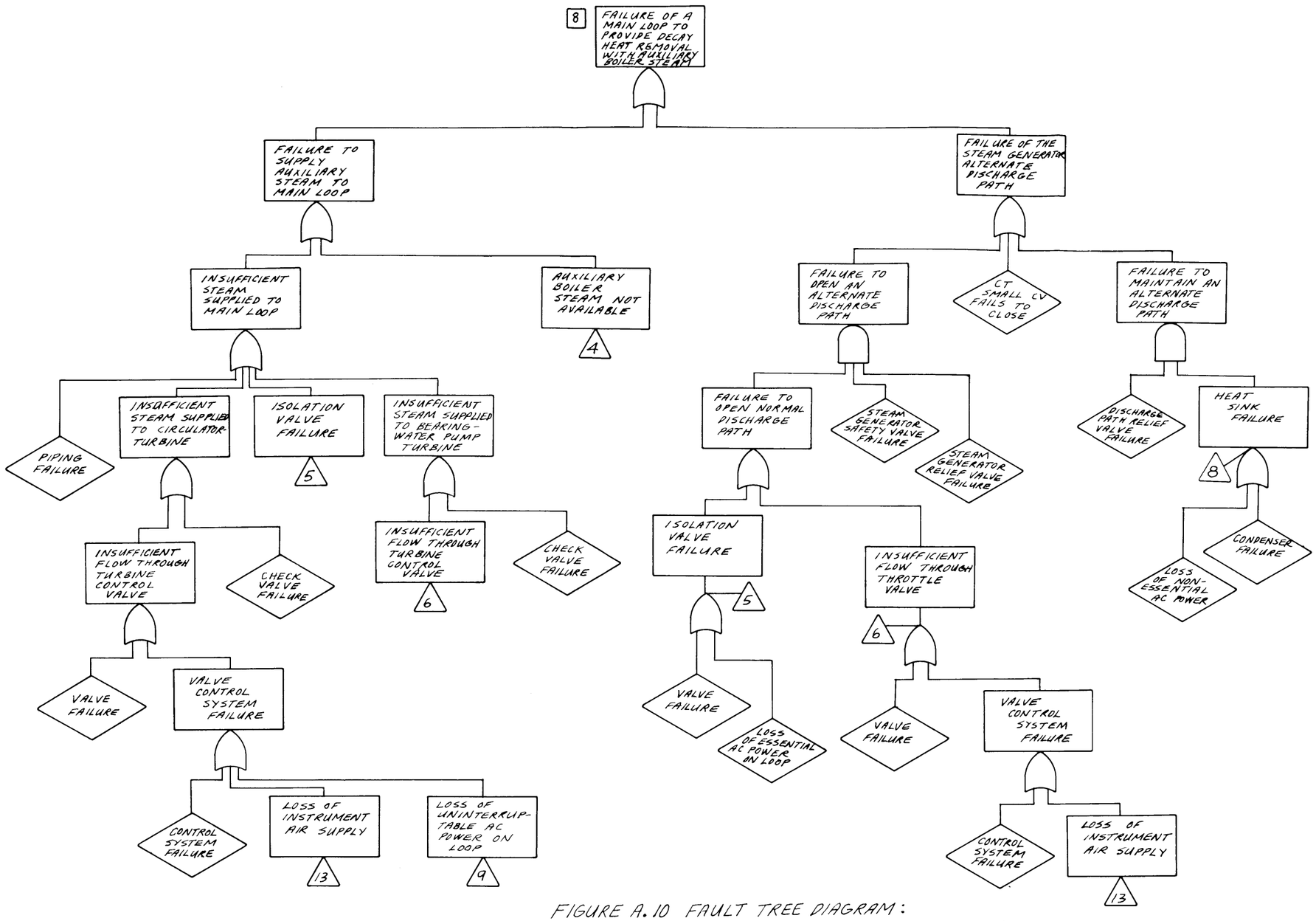


FIGURE A.10 FAULT TREE DIAGRAM:
MAIN LOOP TRANSFER TO DECAY HEAT REMOVAL OPERATION

for main loop operation to continue to this point, instrument air must already be available. Failure of the instrument air supply will eliminate the main loops before transfer to the auxiliary boilers can occur.

A failure rate of 6.2×10^{-3} per demand was calculated for each individual main loop based on the following.

Alternate discharge path control valve fails to open	3×10^{-4}/d
Circulator turbine control valve failure	3×10^{-4}/d
Bearing water pump control valve failure	3×10^{-4}/d
2 check valve failures (one associated with each control valve)	2×10^{-4}/d
CT small CV fails to close	1×10^{-4}/d
Shutdown controller failure	3×10^{-3}/d
2 isolation valves fail to open	2×10^{-3}/d
	6.2×10^{-3}/d
Test and maintenance unavailability	4×10^{-3}

The motor operated isolation valves were assumed to be closed during normal operation. If these were normally open, their failure rate would be 1×10^{-4}/d each to fail to remain open. The subsystem unit failure probability would then be 4.4×10^{-3}/d. Test and maintenance unavailability contributions were assumed for the isolation valve closest to the auxiliary boilers and for the alternate discharge path control valve. This corresponds to a total downtime of three hours a month.

A.9 The Essential Electrical Supply

The Class IE electrical power system consists of three independent 4160 volt AC subsystems and three 125 volt uninterruptable power systems. Each of the 4160 volt AC essential buses supplies a single main loop and a single auxiliary loop. Also, the essential support system loads are split between the essential buses. During normal operation, each essential bus is supplied from the unit auxiliary transformer. An alternate, off-site power source is also available for these buses, and upon loss of the normal power source, automatic, high-speed dead bus transfer will result. Each essential bus is also equipped with its own separate emergency diesel generator. These are designed to start automatically upon complete loss of off-site power, and they are sized to handle the entire essential bus load during the shutdown and decay-heat removal operations. A single line diagram of the essential and non-essential power supply system is shown in Figure A.11.

The diesel generators are each a complete unit for full operation. Each unit is located in a separate room which contains a control station, a 3000 gallon day tank and its own cooling system. The BOP design initially utilized service water for the diesel jacket cooling requirements, however, this dependence is to be eliminated in the final design.

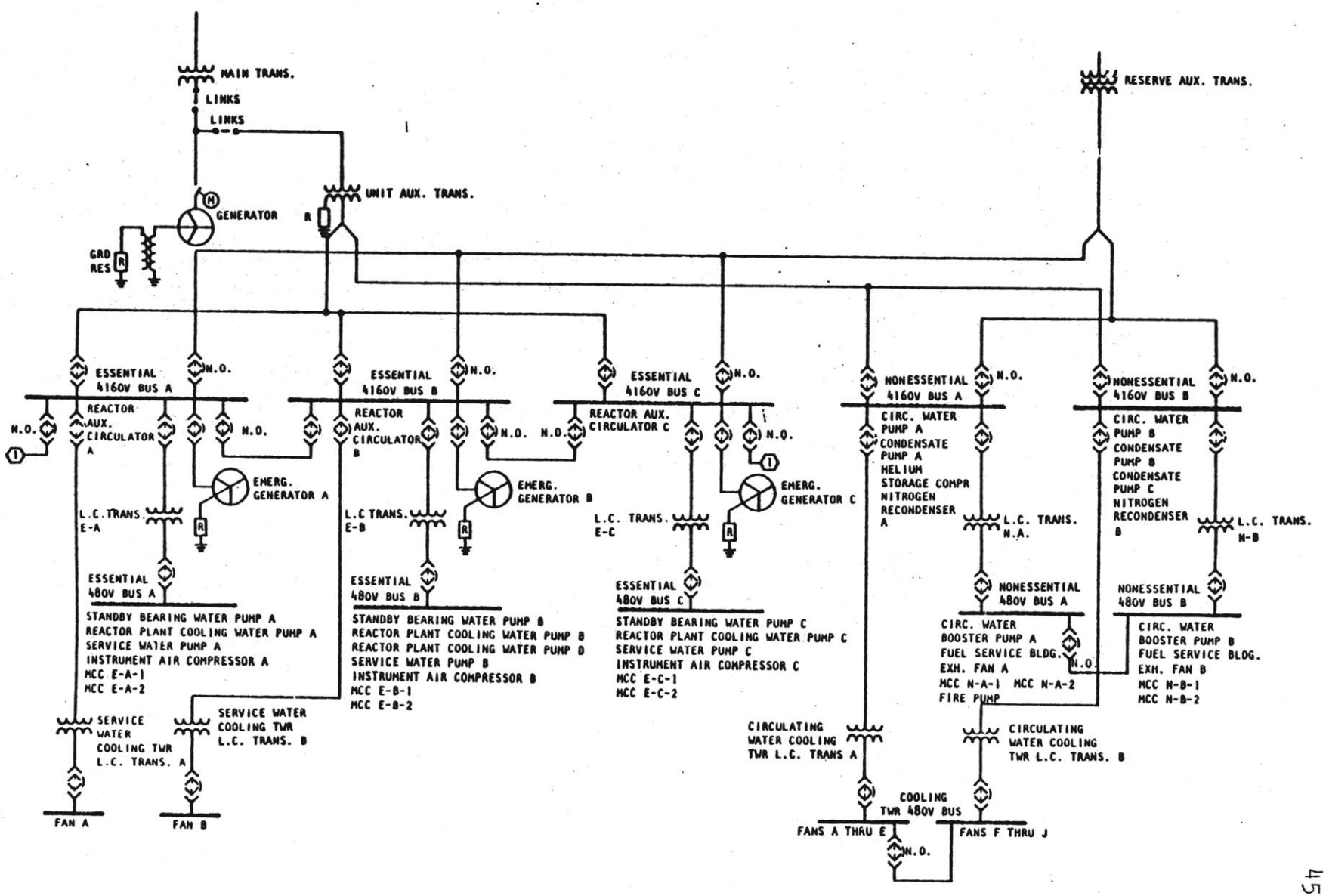


FIGURE A.11 Plant electrical system single line diagram

Each generator is rated at 2130 kw at 0.8 pf and is driven by a 3400 hp diesel motor. In the event of a loss of offsite power, each unit will start automatically, reach rated speed and voltage, and be ready to assume load in 10 seconds. This entire system is designed to seismic category I specifications except for the 15,000 gallon underground fuel, storage tank which is supplied for each generator.

A diesel generator system failure rate of 3×10^{-2} per demand was assumed for each unit. This value comes directly from WASH-1400. An unavailability for test and maintenance purposes of 6×10^{-3} is also taken from that source.

A line diagram of the uninterruptable power system is shown in Figure A.12. Each system consists of a 125 volt DC bus and a 125 volt AC uninterruptable bus, a battery charger, an inverter, a static switch and a bypass transformer for maintenance purposes. Each DC bus supplies power to the switchgear control annunciators and indicator lights for one of the main loops and one third of the emergency lights.

During normal operation, the DC loads and the inverter loads for the uninterruptable AC bus are carried through the battery charger, and the battery is floating. In the event of a loss of AC power, the battery automatically picks up the DC loads and the uninterruptable AC loads (through the inverter). The bypass transformer is provided to carry the

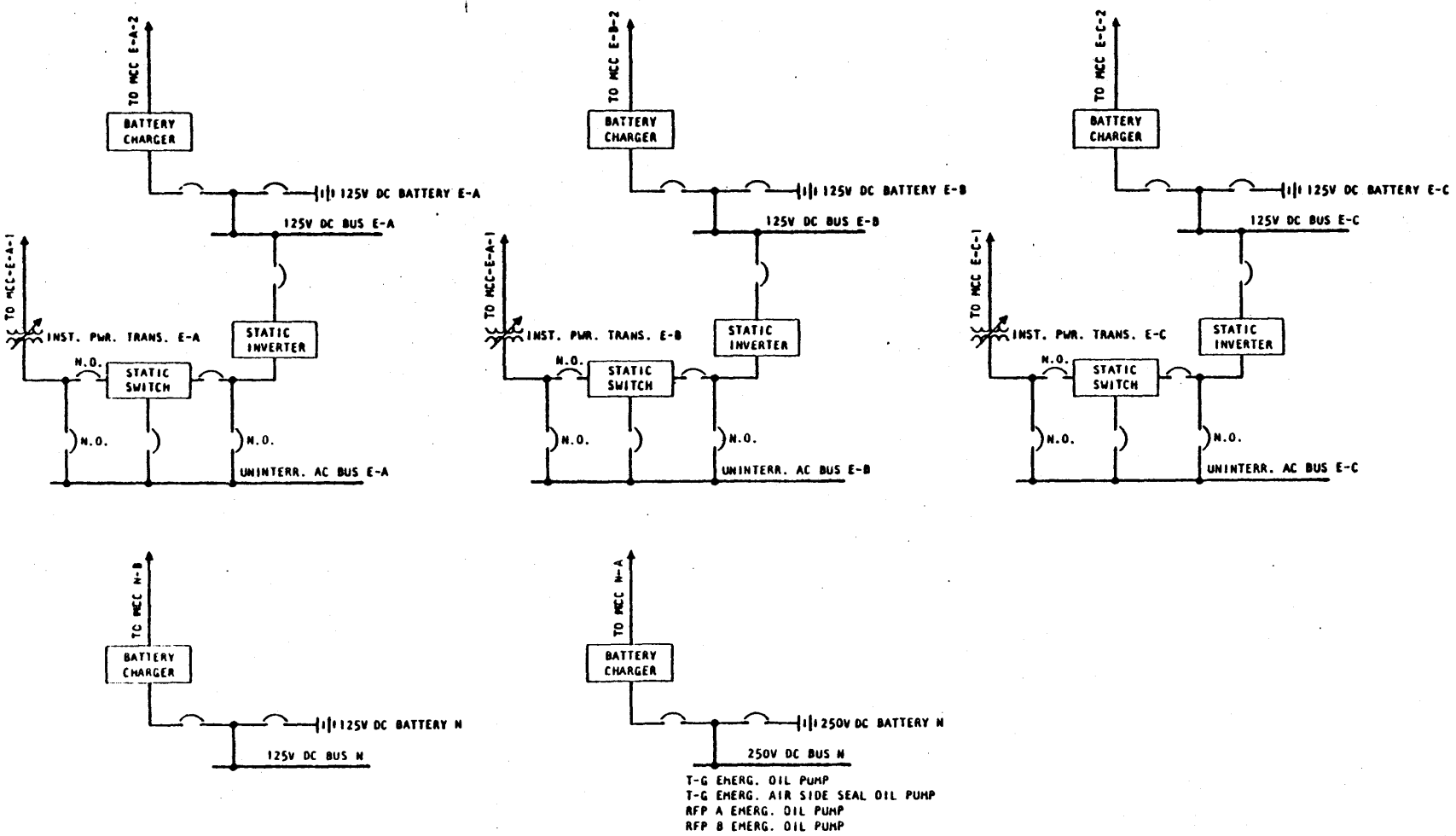


FIGURE A.12 dc and uninterruptible ac systems

load in the event any DC system components are out of service for maintenance or because of failure.

The battery is sized to carry all the loads on both the DC and uninterruptable AC bus for four hours, and the battery charger is sized to carry the full load and simultaneously recharge the battery in less than 8 hours.

The fault tree diagram for failure of an uninterruptable power supply is shown in Figure A.13. A failure rate of 1×10^{-5}/hr was calculated, given the loss of essential AC to the loop, based on the following:

Static switch failure	3×10^{-6}/hr
Static inverter failure	3×10^{-6}/hr
DC bus failure	1×10^{-6}/hr
DC battery supply failure	3×10^{-6}/hr
	1×10^{-5}/hr

This analysis is essentially concerned with the first thirty minutes following the shutdown. Failures of the uninterruptable power supply do not contribute to subsystem unit failure probabilities because these are already on the order of 1×10^{-3}/demand.

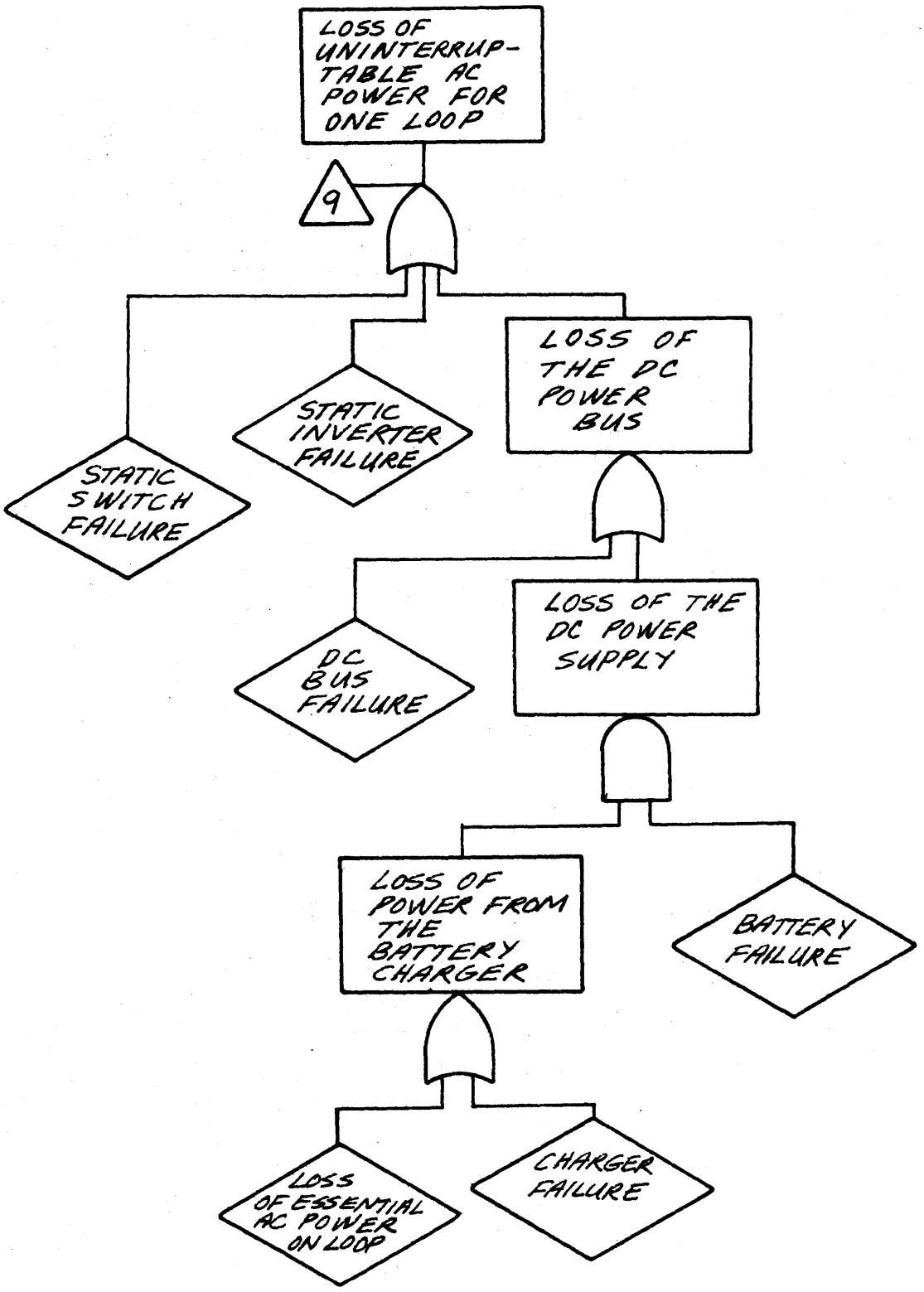


FIGURE A.13 FAULT TREE DIAGRAM: UNINTERRUPTABLE AC POWER SUPPLY

A.10 The Core Auxiliary Cooling System (CACS)

Each CACS loop consists of an auxiliary circulator, an auxiliary loop isolation valve, and a pressurized water heat exchanger which is connected to its own separate heat removal loop. Each loop is designed to remove two percent of the reactor full power heat load at the normal helium working pressure of 1305 psia and at the depressurized helium pressure (26.7 psia). The complete electrical needs for each CACS loop are supplied from a single essential bus.

Each auxiliary circulators unit consists of its electric motor drive, a centrifugal compressor and a diffuser. Because of the wide range of operating pressure levels, the electric motor drives will be capable of variable speed operation. The motors are the squirrel-cage induction type, and variable speeds will be produced by a variable-frequency power supply. Each auxiliary circulator is designed with its own independent power supply and control system. The auxiliary circulator design data for the depressurized case are given below:

Type	Centrifugal
Drive	Electric Motor
Fluid	Helium
Speed	4900 rpm
Inlet Temperature	400°F
Inlet Pressure	25.3 psia

Outlet Pressure	26.7 psia
Mass Flow	11.1 lb/sec
Power	460 hp

Each auxiliary circulator unit has its own independent service system which functions 1) to provide cooling water to the auxiliary circulator motor windings and bearings, 2) to supply purified buffer helium to prevent leakage of the bearing lubricant into the reactor coolant and to prevent leakage of the reactor coolant into the motor casing, 3) to remove and replace the motor bearing lubricant, and 4) to remove oil vapor from the purge helium from the circulators.

The motor cooling circuit consists of a helium-water heat exchanger, a water cooler, and a water circulation pump. Fans mounted on the auxiliary circulator shaft direct helium through the heat exchanger, which is located in the motor casing, and over the motor windings. It is assumed that the heat transferred from the motor casing will be rejected to an independent CACS cooling-water system.

Lubricating oil for the motor bearings is cooled by a water cooling coils located in the oil reservoir.

The auxiliary loop isolation valve is a self-actuating butterfly-type check valve. It is closed by the action of both the normal main loop operating pressure differential and by gravity. The valve is opened, given the main loops have failed, by the pressure rise created by the operation of its auxiliary circulator. These valves are similar to

those used in the Ft. St. Vrain primary cooling system.

The auxiliary heat exchanger is a helically wound, axial flow tube bundle. It is a pressurized-water type heat exchanger, and it operates at an average water pressure of 2100 psia. The helium flows up directly through the tube bundle, through the auxiliary loop isolation valve, to the auxiliary circulator.

The core auxiliary cooling-water system consists of the auxiliary heat exchangers and their associated heat removal equipment. There are three separate cooling-water loops (one for each CACS loop), and each loop provides the heat rejection for its CACS loop by means of a forced-convection air heat exchanger. A schematic flow diagram for one loop is shown in Figure A.14.

Each cooling water loop contains an auxiliary circulating water pump, a circulating water pump, a forced air cooler, a demineralizer and filter, and a pressurizer. During normal plant operation, the auxiliary circulating pump operates to provide a small flow through the auxiliary heat exchanger to prevent boiling. The forced-air cooler fans are not run, and natural air draft is sufficient to maintain the system at a constant sub-cooled temperature. This flow also acts to prevent thermal shock to the loop upon start-up of the CACS, however, it is small enough so that it does not represent a large thermal loss to the reactor.

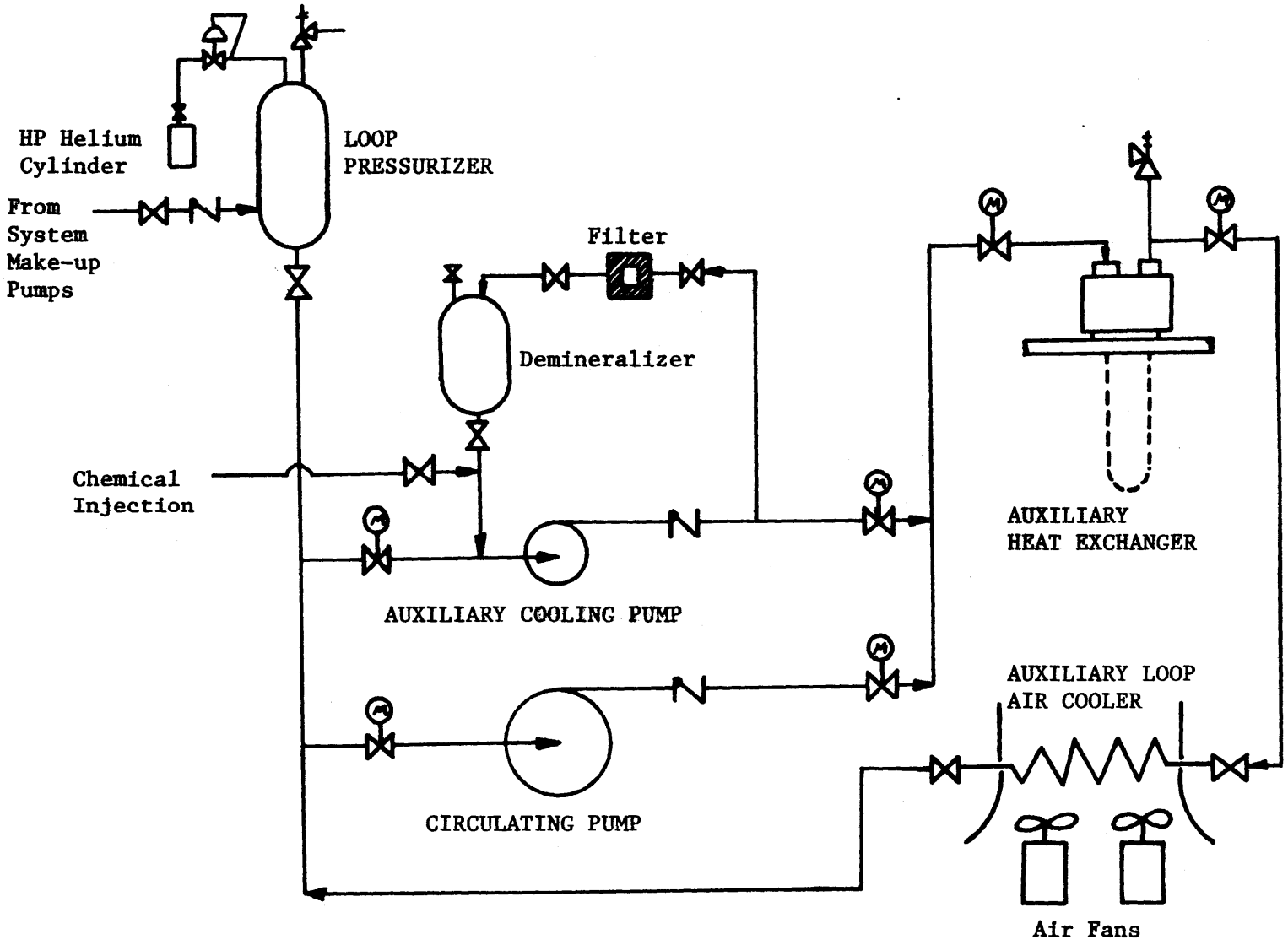


FIGURE A.14 A Schematic Flow Diagram of a Core Auxiliary Cooling Water Loop

The pressurizer maintains the system at 2100 psia by the addition of helium from gas cylinders, and water quality is maintained by a bypass filter and demineralizer unit provided around the auxiliary circulating pump and also by periodic chemical treatment.

Upon start-up of the CACS, the circulating water pump is started along with the air cooler fans. The auxiliary circulating pump is shutdown, and the system operates at full flow with no control required.

The air cooler consists of finned tubes which are arranged counter-current to the air flow. The cooler is designed to reduce the water temperature from 500°F to 180°F.

The entire CACS and the cooling water loops are designed to seismic category I specifications and are an engineered safeguard feature.

The fault tree diagram for failure of a CACS loop to provide adequate core cooling is included as Figure A.15. A failure rate of 8.3×10^{-3} per demand for each CACS loop was calculated from the following contributors.

Auxiliary circulator failure	1×10^{-3}/d
Auxiliary circulator power supply failure	3×10^{-4}/d
Circuit breaker to power supply failure	1×10^{-3}/d

Auxiliary circulator control system failure	1×10^{-3}/d
Auxiliary loop isolation valve failure	1×10^{-4}/d
Circulating water pump failure	1×10^{-3}/d
Pump control system failure (circuit breaker failure dominates)	1×10^{-3}/d
Check valve failure	1×10^{-4}/d
2 motor operated valves fail to remain open	2×10^{-4}/d
Air cooler fan failure	6×10^{-4}
and fan control system (circuit breaker failure)	2×10^{-3}
	8.3×10^{-3}/d
Test and maintenance unavailability	1.2×10^{-2}

The test and maintenance unavailability is based on contributions from the four motor operated valves, the circulating water pump and the two fans of each loop, and corresponds to almost 9 hours of downtime per month per loop.

The calculation above assumes that both air cooler forced draft fans are necessary. If only one is sufficient, then the random failure rate is 5.7×10^{-3}/d and the test and maintenance unavailability becomes 1.0×10^{-2}

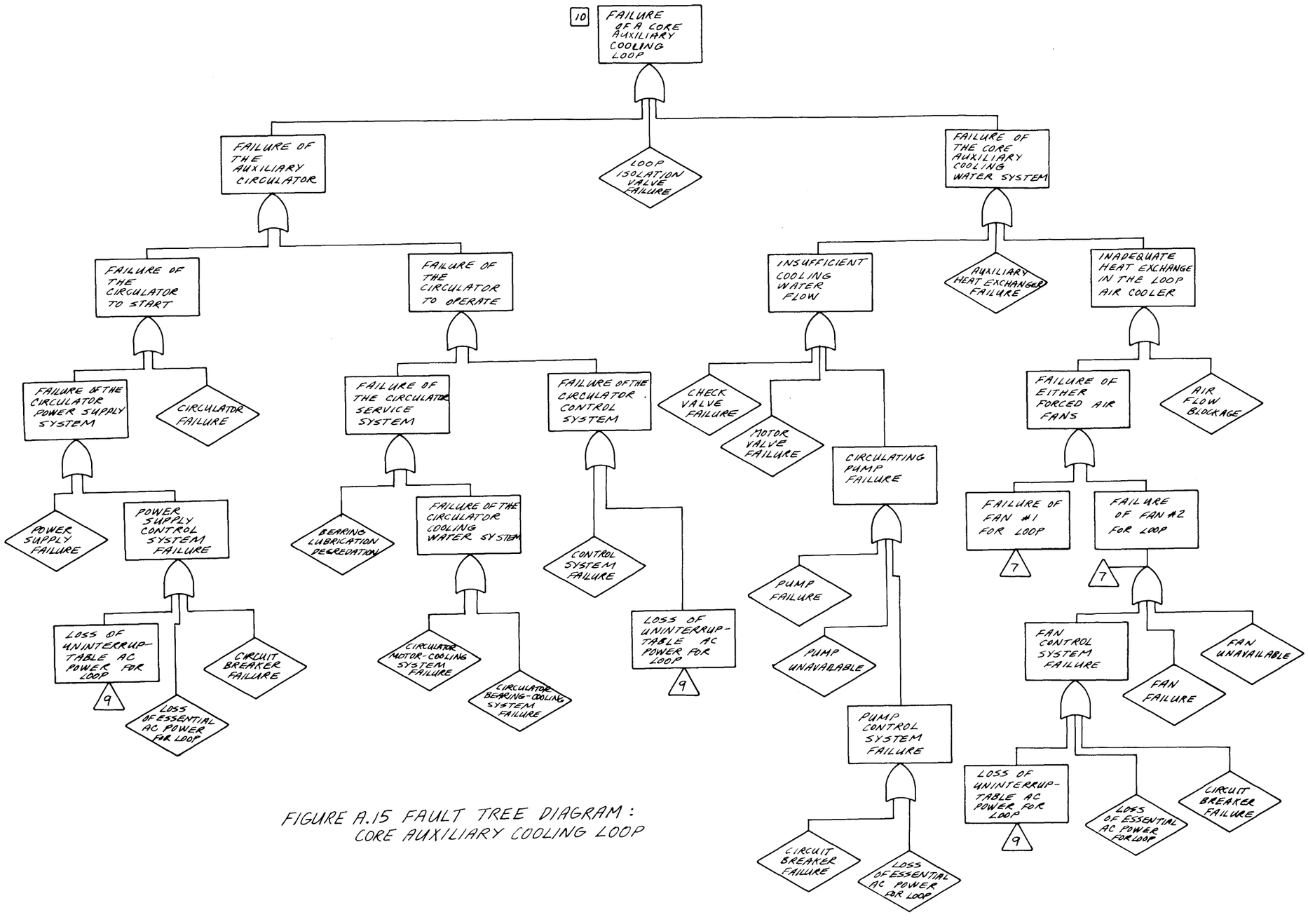


FIGURE A.15 FAULT TREE DIAGRAM: CORE AUXILIARY COOLING LOOP

A.11 The Resuperheater Bypass Circuits

The resuperheater bypass circuit for each main loop provides a path for the helium circulator-turbine exhaust steam around the resuperheater portion of the steam generator module to the main condenser. Each circuit consists of a resuperheater bypass control valve, an isolation valve, a check valve and resuperheater bypass circuit safety valves. The three circuits join before a common spray desuperheater, and the desuperheated steam is then directed to the main condenser. There is also a provision for providing the desuperheated steam to drive the main feed pump turbines during start-up and programmed shutdowns. A schematic of the circuit for one loop is shown in Figure A.16.

With the initiation of a reactor shutdown, the main turbine-generator throttle valve is closed, and the resuperheater bypass control valve is designed to open to provide a path for the circulator-turbine exhaust steam to the main condenser. Each circuit is sized to pass only 25% of the full loop flow, and so initially the resuperheater bypass circuit relief valves will lift to exhaust the excess steam to the atmosphere. Should the main condenser be unavailable, following the shutdown, then the relief valves would remain open to maintain the exhaust circuit for the helium circulator-turbine. The resuperheater bypass controller regulates the resuperheater bypass control valve in order to maintain

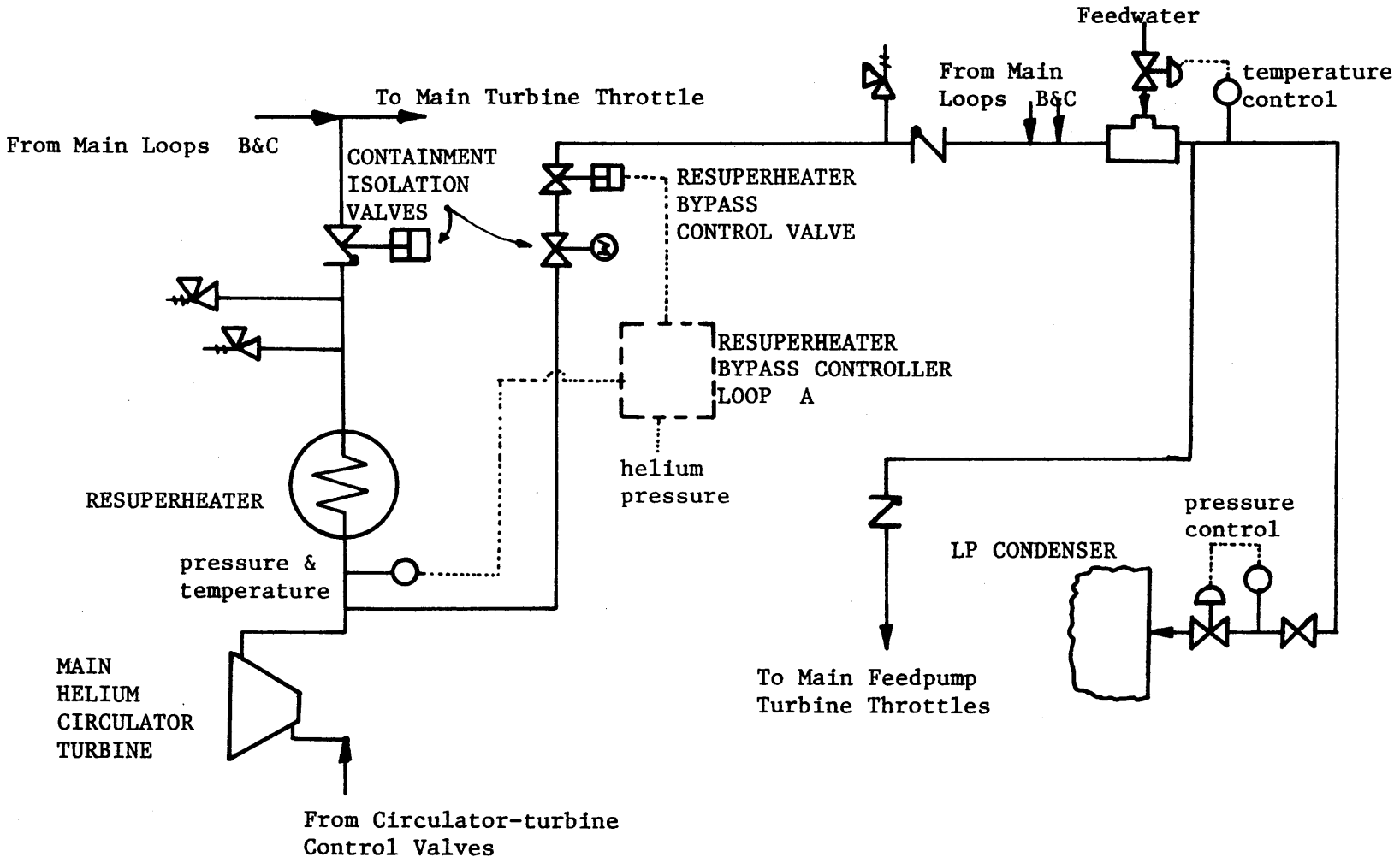


FIGURE A.16 A Schematic Flow Diagram of a Main Loop Circulator-turbine Exhaust Path Following Reactor Shutdown

the circulator-turbine exhaust pressure proportional to the reactor inlet helium pressure. This control action is most important in the event of a PCRV depressurization accident because it adjusts the circulator power, and thus the helium flow, in accordance with the reactor coolant pressure.

In the event that the resuperheater bypass control valve fails open, the circulator turbine exhaust is maintained by the resuperheater relief and safety valves which lift to prevent overpressurization of the resuperheater. This will also allow continued operation of the main circulators, however, the actual extent of circulator operation in this mode (exhausting through resuperheater safety and relief valves) is unknown. The steam generator inventory depletion times used in the ESD modelling assumed proper resuperheater bypass valve operation. Therefore, failure of this valve to correctly operate was assumed to fail the loop, and no credit was allowed for continued main loop operation as discussed above.

The fault tree diagram for the failure of the circulator-turbine exhaust circuit of one main loop is shown in Figure A.17. A failure rate of 1.4×10^{-3} per demand was calculated for failure of one resuperheater bypass system based on the following:

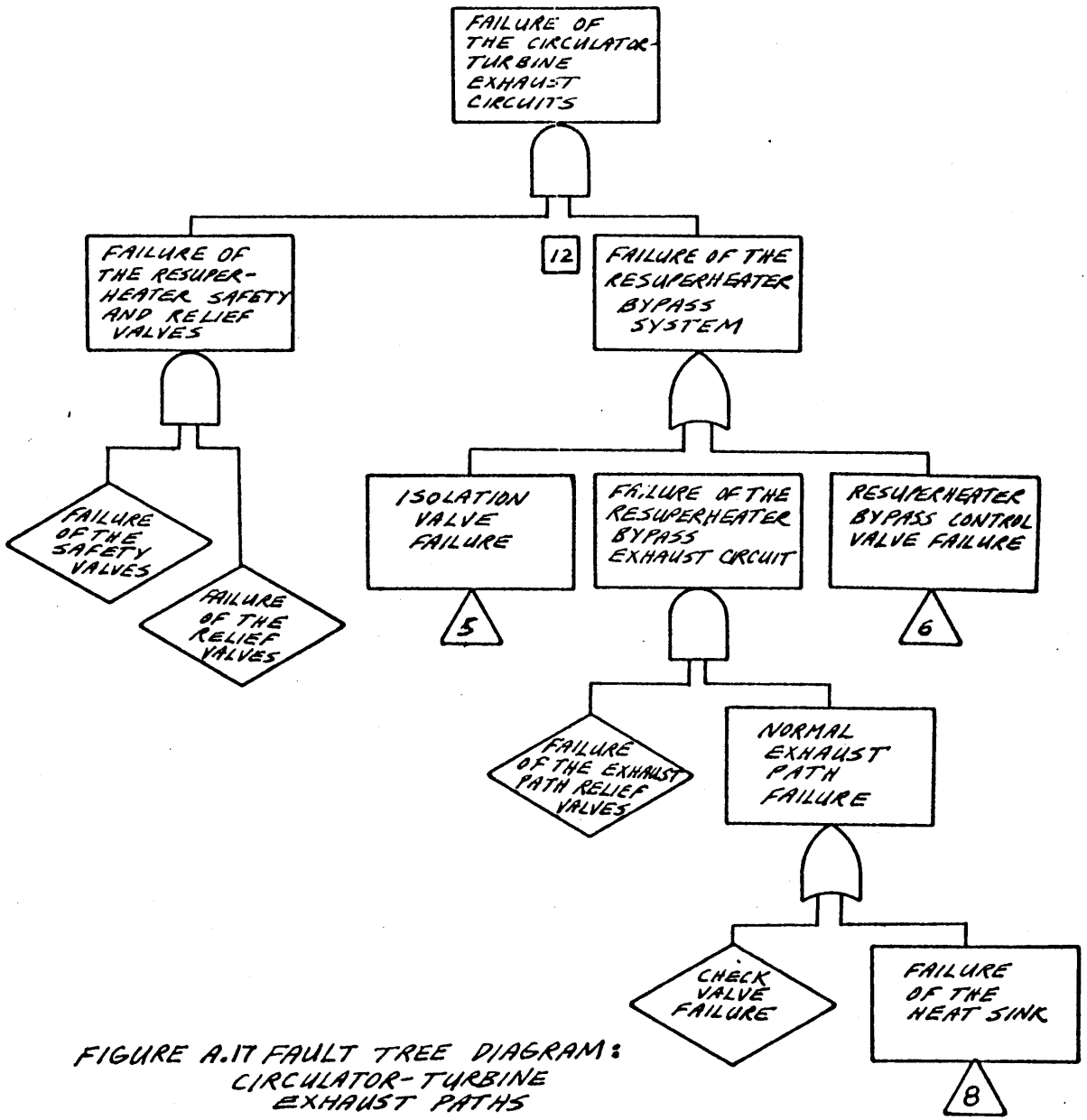


FIGURE A.17 FAULT TREE DIAGRAM: CIRCULATOR-TURBINE EXHAUST PATHS

Isolation valve failure to remain open	1×10^{-4}/d
Resuperheater bypass control valve failure	3×10^{-4}/d
Resuperheater bypass controller failure	1×10^{-3}/d
Resuperheater exhaust path relief valve failures (2)	1×10^{-6}/d
	1.4×10^{-3}/d
Test and maintenance unavailability	2×10^{-3}/d

The test and maintenance unavailability contribution was due to the resuperheater bypass control valve and is equivalent to a downtime of 1.5 hours a month.

A.12 The Service Water System

The service water system is designed to remove heat from reactor auxiliary equipment, emergency equipment and building cooling equipment. A schematic of the system is shown in Figure A.18. The system consists of three service water pumps each of which can supply either of the two parallel service water headers. Each of the parallel headers can independently supply the all of the essential service water loads.

Only one of the three pumps is necessary to provide all of the service water requirements for normal and abnormal operating conditions. The two parallel headers are equipped with check valves to prevent back-flow of water between them, and the standby pumps are started automatically by a low

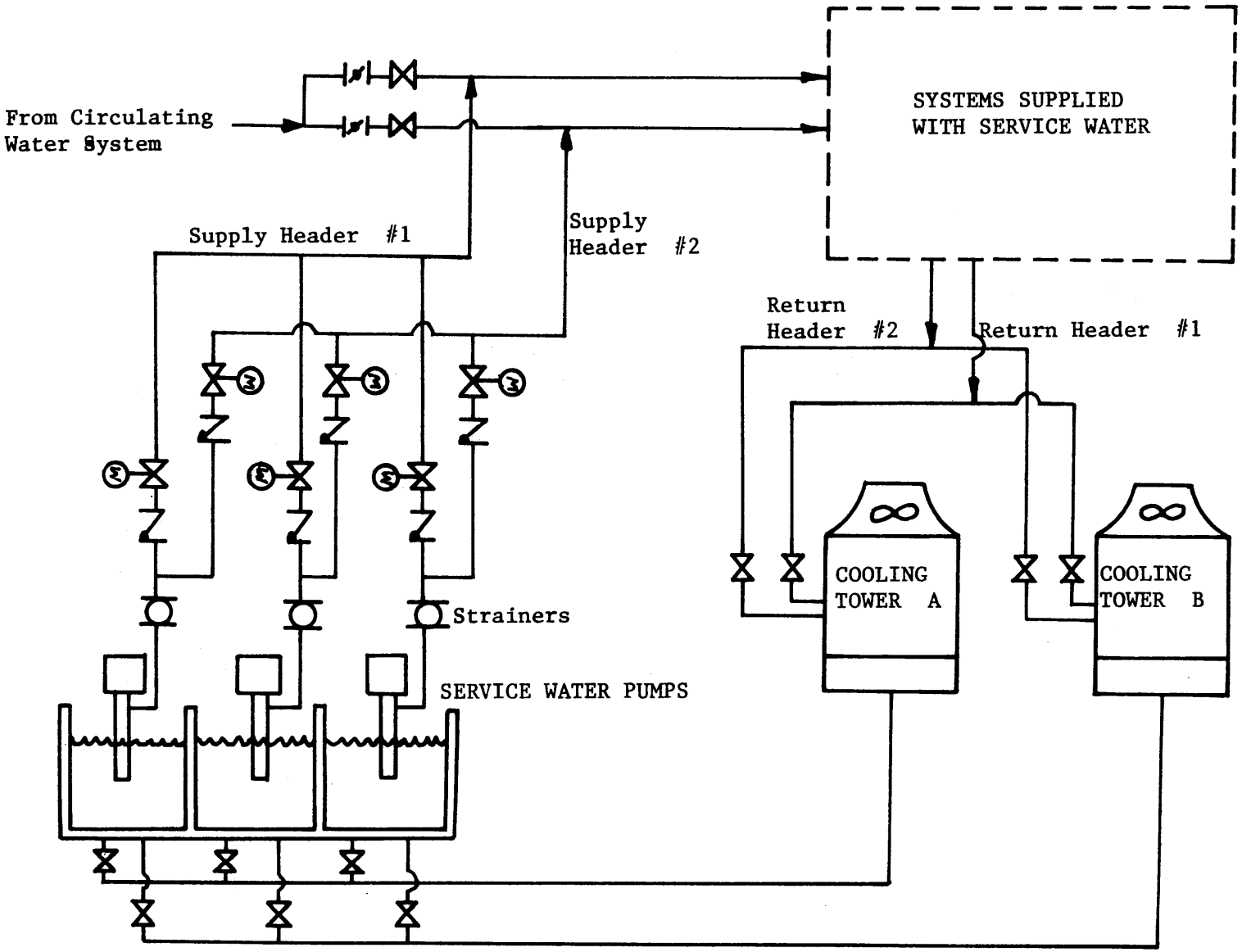


FIGURE A.18 A Schematic Flow Diagram of the Service Water System

pressure signal in the discharge headers. Heat rejection to the atmosphere is accomplished by a two-cell mechanical draft cooling tower. Either cell provides adequate heat rejection in all operating conditions, and either cell can be used with either of the two parallel service water paths.

This system is designed as a seismic category I system, and each of the service water pumps and cooling tower fans are powered by separate essential electrical buses.

The fault tree diagram for the failure of the service water system is included as Figure A.19. Failure of this system is dominated by failures eliminating the pumps, and by failures eliminating the cooling towers.

During the reactor shutdown, the failure probability of this system will depend upon 1) the number of essential buses energized, and 2) whether or not the standby cooling tower can be automatically started in the event of a failure of the operating tower.

The system failure probability is based upon the following data.

Failure of operating pump:

Failure of the motor-operated valve	1×10^{-6}/hr
Failure of the pump	3×10^{-5}/hr
	3.1×10^{-5}/hr

Failure of a standby pump:

Failure of the motor operated valve	1×10^{-3}/d
Failure of the check valve	1×10^{-4}/d
Filter plugged	1×10^{-4}/d
Pump failure	1×10^{-3}/d
Pump circuit breaker failure	1×10^{-3}/d
Pressure switch failure	1×10^{-4}/d
	3.3×10^{-3}/d

Failure of the operating tower:

Fan failure	1×10^{-5}/hr
Valve failures (2)	2×10^{-6}/hr
	1.2×10^{-5}/hr

Failure of the standby tower:

Fan failure	3×10^{-4}/d
Fan circuit breaker failure	1×10^{-3}/d
Valve failures (4)	4×10^{-3}/d
	5.3×10^{-3}/d

For the case in which all three essential buses are available, and the standby cooling tower can be automatically started, the failure probability is less than 1×10^{-7} per hour. When all three of the essential buses are not avail-

able, the subsystem failure probability will depend upon both the initial operating state of the service water system, and the actual essential buses energized. For example, if essential buses A and B are available, and the service water system is operating with the pump energized from bus A and the cooling tower fan energized from bus B, then the system should continue operating with its failure probability reduced slightly due to the loss of one standby pump (the one energized from bus C). If instead, only bus C were energized, then the service water system will always fail due to the fact that the cooling tower fans are energized from buses A and B only.

Assuming that all the initial operating states of the service water system are equally likely, an averaged failure probability can be calculated from all the cases of two buses energized and one bus energized. These are respectively 3×10^{-3} and .333 per shutdown. The latter is due to the fact that having only bus C available leads to failure of the system, and if only one bus is available, it will be bus C on the average one-third of the time.

In the case where cooling tower transfer is not possible, the system failure probability for three essential buses available, is dominated by failure of the cooling tower. With only two essential buses available, the failure proba-

bility is .333. This is due to the fact that with the cooling towers energized from buses A. and B, power will be lost to the buses on the average of one-third of the time if only two buses are energized. With one bus energized this will occur on the average of two-thirds of the time, and the failure probability is then .667.

These results are summarized in the table below.

Service Water System Failure Probability

No. of Essential Buses Energized	Standby Cooling Tower Transfer	No Standby Cooling Tower Transfer
3	1×10^{-7}	1×10^{-5}
2	3×10^{-3}	.333
1	.333	.667

In most of the analyses performed in this study, the standby service water cooling tower was assumed to be transferable in the event of failure of the operating tower, and the impact of this assumption was investigated in the sensitivity analyses. Note that for most cases where offsite power is available this analysis is conservative because no credit was allowed for the circulating water injection.

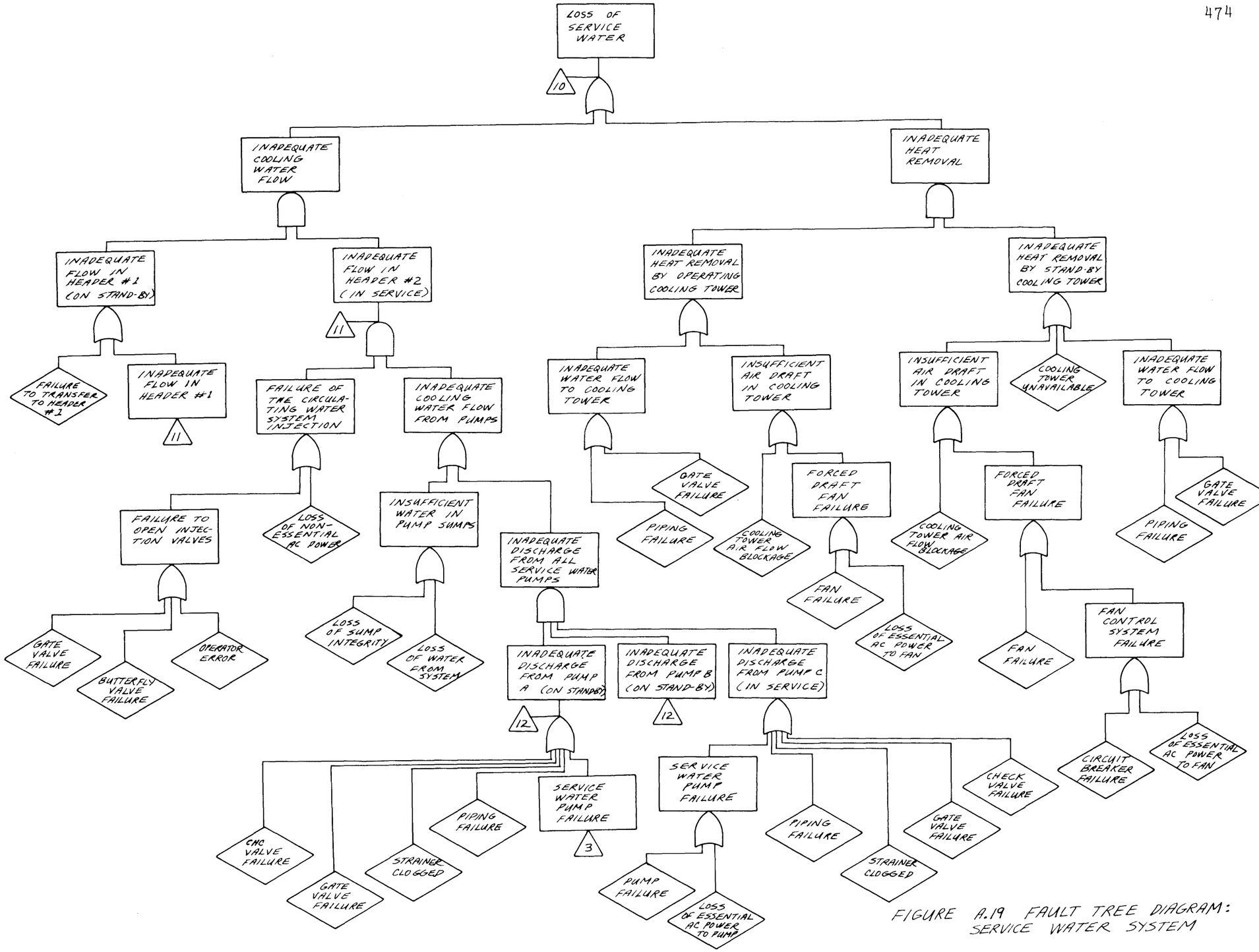


FIGURE A.19 FAULT TREE DIAGRAM: SERVICE WATER SYSTEM

A.13 The Instrument and Service Air System

This system provides clean, dry air to pneumatic valve operators and controllers and the other areas that require clean air. The system also provides service air for portable tools and the other pressurized air requirements throughout the plant. The system consists of three compressor units each of which contains a compressor, an after-cooler and a receiver. Each unit supplies a common header from which there are two independent instrument air supply circuits and the service air supply circuit. The instrument air supply lines also contain filters and a dryer. Figure A.20 is a skematic flow diagram for the system.

Each compressor unit is powered from a different essential bus, and two of the three compressor units are capable of providing full instrument and service air requirements. Also, each receiver is sized such that, when fully changed, it can supply the full instrument air demand for a period of one minute without power to the compressors.

During a reactor shutdown, the air accumulation in the receivers is sufficient to perform all necessary valve and controller operations. Also, a single operating compressor unit is assumed to provide sufficient instrument air to perform all vital valve operations and controller functions.

The system is designed to seismic category I specifications, and each compressor unit will be protected from missiles in the event of an accident coming from one of the adjacent units.

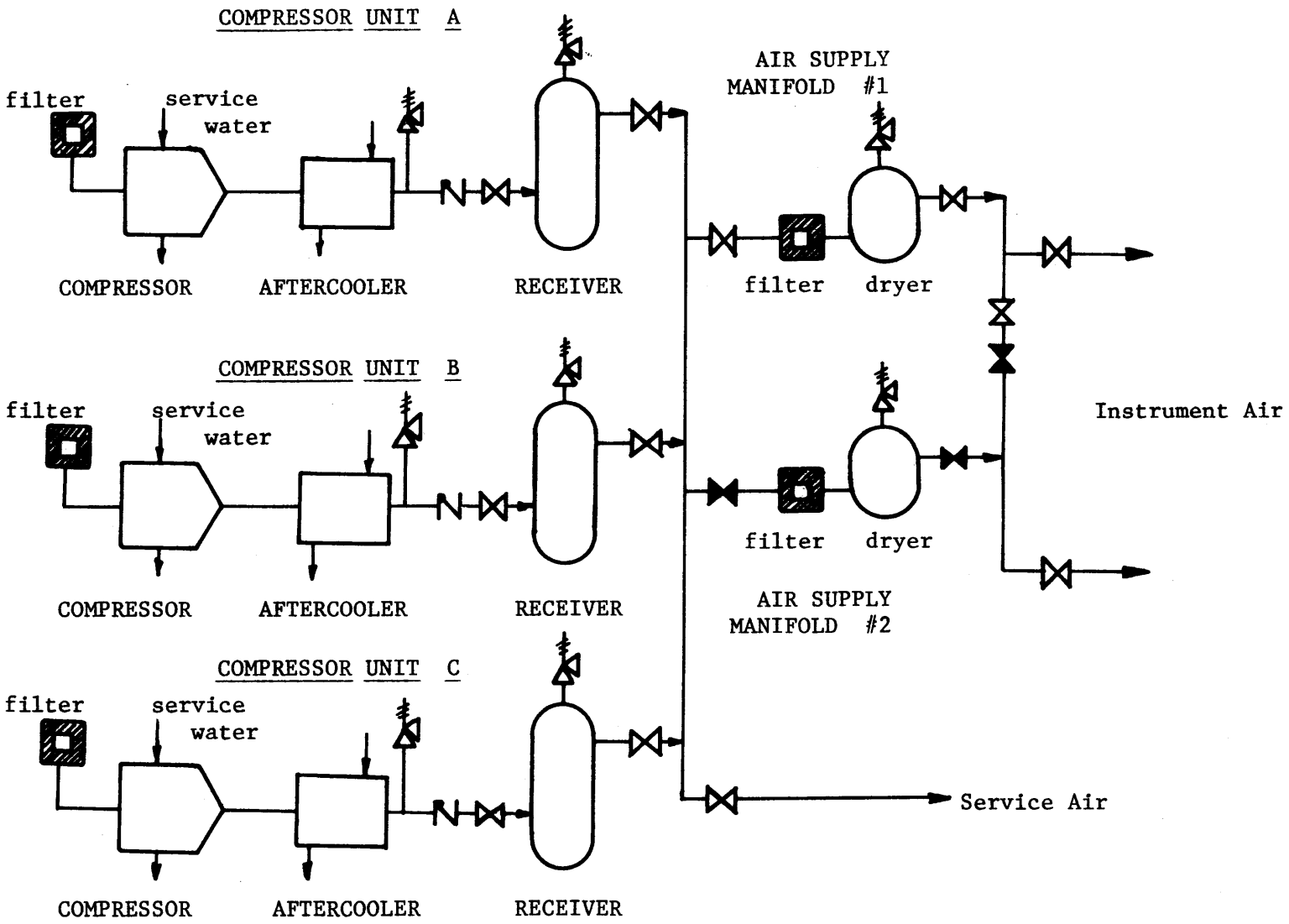


FIGURE A.20 A Schematic Flow Diagram of the Instrument and Service Air System

The fault tree diagram for failure of this system to function is shown in Figure A.21. It is important to note, that proper operation of each compressor unit is dependent upon adequate service water being supplied to its after-cooler.

The operating failure rate for each compressor unit (similar to a pump) is 3×10^{-5}/hr. A beta factor value of 0.03 was used to estimate the common mode failure probability, and the probability of a combination of valve and piping failures which would eliminate both supply lines was estimated to be less than 1×10^{-8}.

The operation of this system is dependent upon the essential electrical supply, and with three essential buses powered, its failure probability in the initial 30 minutes following reactor shutdown is 5×10^{-7}. Including the dependence of the service water system, reduces this to 1×10^{-6}. With only two buses energized, the failure probability is of the system reduces to 3×10^{-3} because of its dependence on service water, and with only one essential bus energized the failure probability of the one operating compressor unit is .333. However, failure of the instrument air compressors due to the loss of service water, is assumed to take place fifteen minutes after the shutdown.

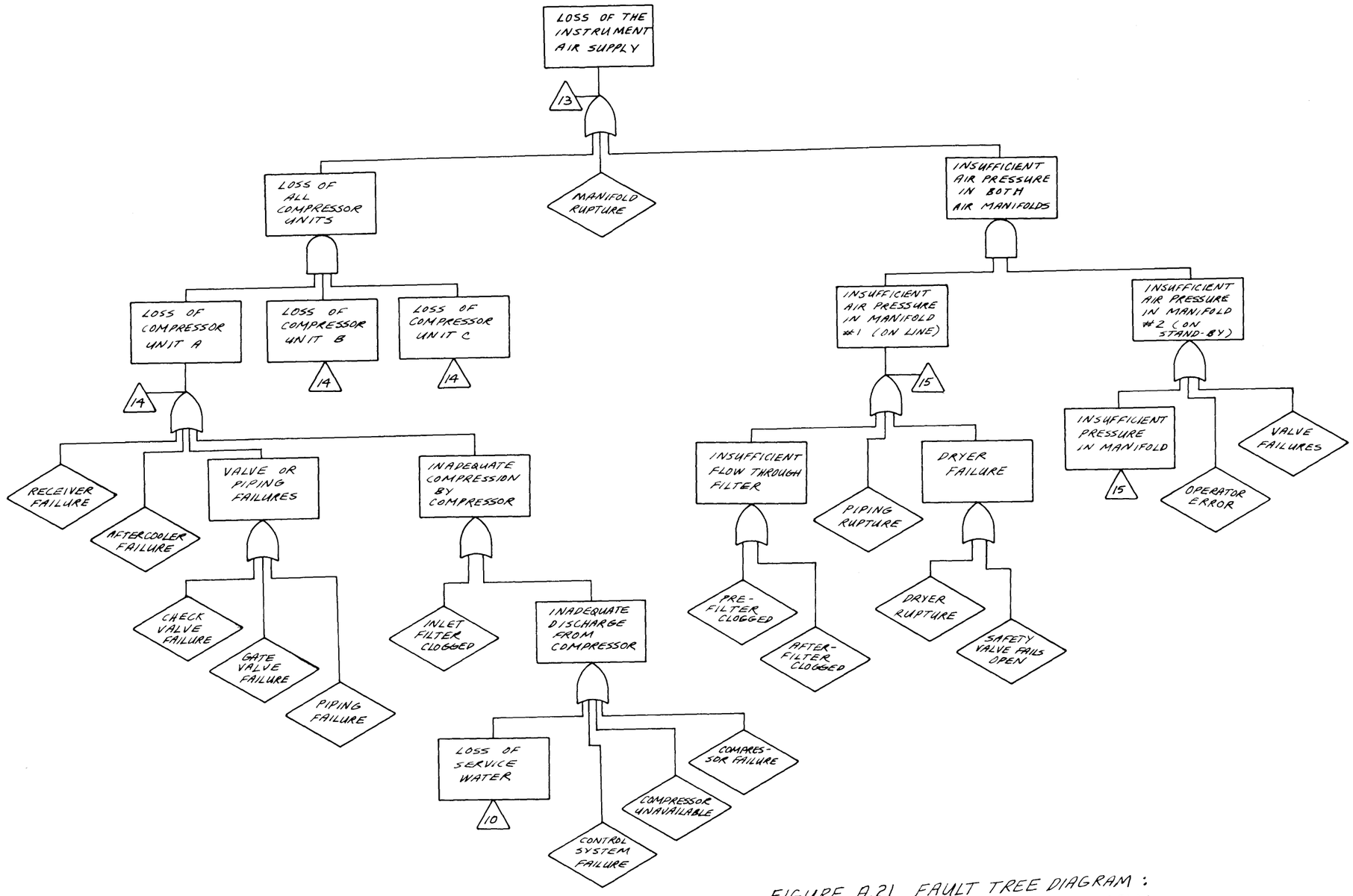


FIGURE A.21 FAULT TREE DIAGRAM : INSTRUMENT AIR SUPPLY

A.14 The Reactor Plant Cooling Water System

This system provides cooling water to those plant components which carry radioactive or potentially radioactive fluids. It provides a monitored intermediate barrier between these fluids and the service water system, in which the final heat rejection occurs.

The system consists of two independent closed loops, each of which contains two circulating water pumps and two heat exchangers to the service water system. Each loop provides 50 percent of the PCRV cooling load, and either loop can provide the remaining cooling load of the system. A schematic flow diagram of the system is provided in Figure A.22.

Each loop operates with one pump and one heat exchanger in service. The others remain in standby in case of failure of the operating items.

A fault tree diagram for failure of this system is included as Figure A.23.

Due to the doubly redundant nature of the reactor plant cooling water system, its failure probability was determined to be primarily dependent on the loss of the service water system. This is especially true if less than three essential buses are energized.

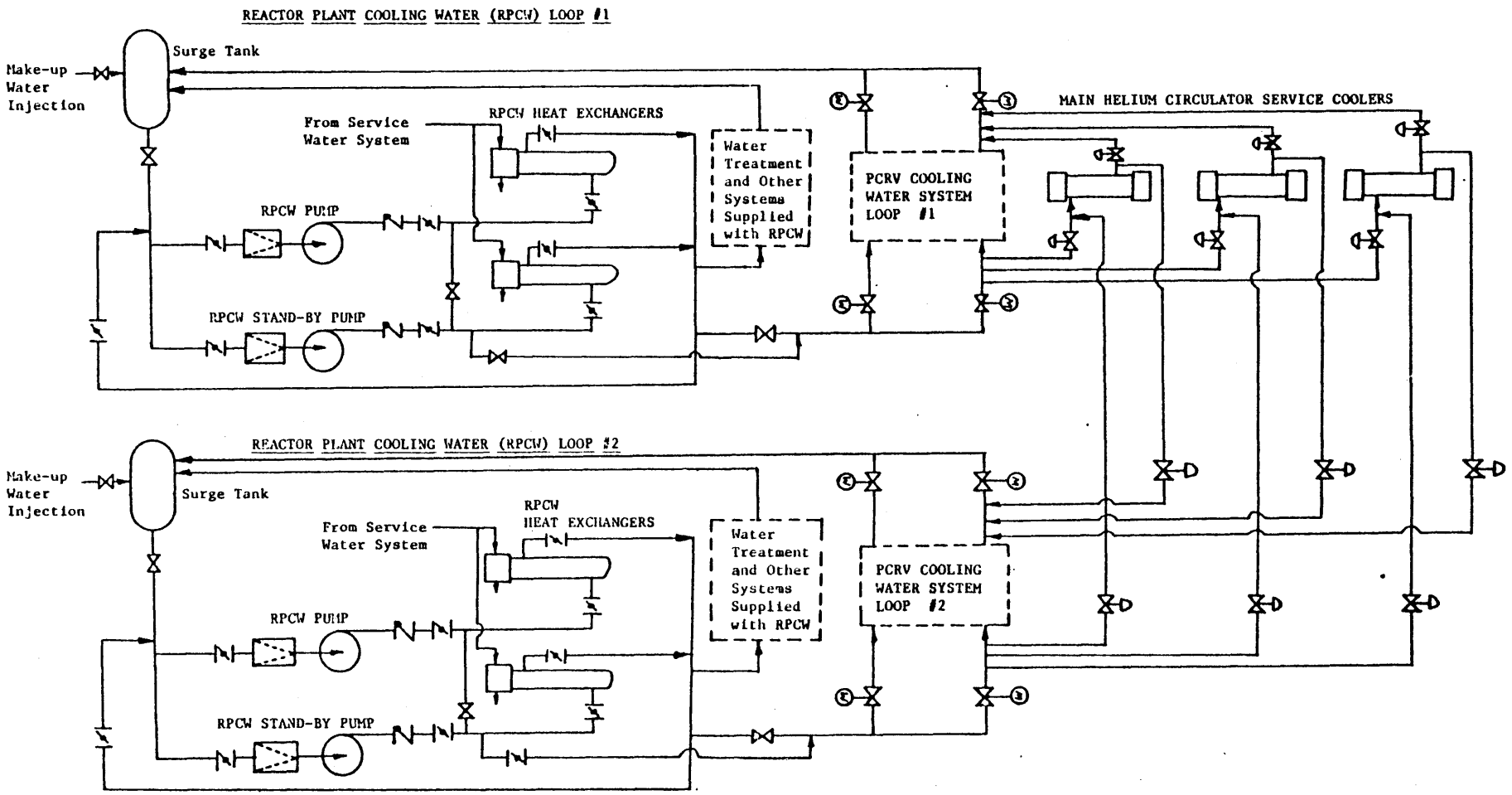


FIGURE A.22 A Schematic Flow Diagram of the Reactor Plant Cooling Water System

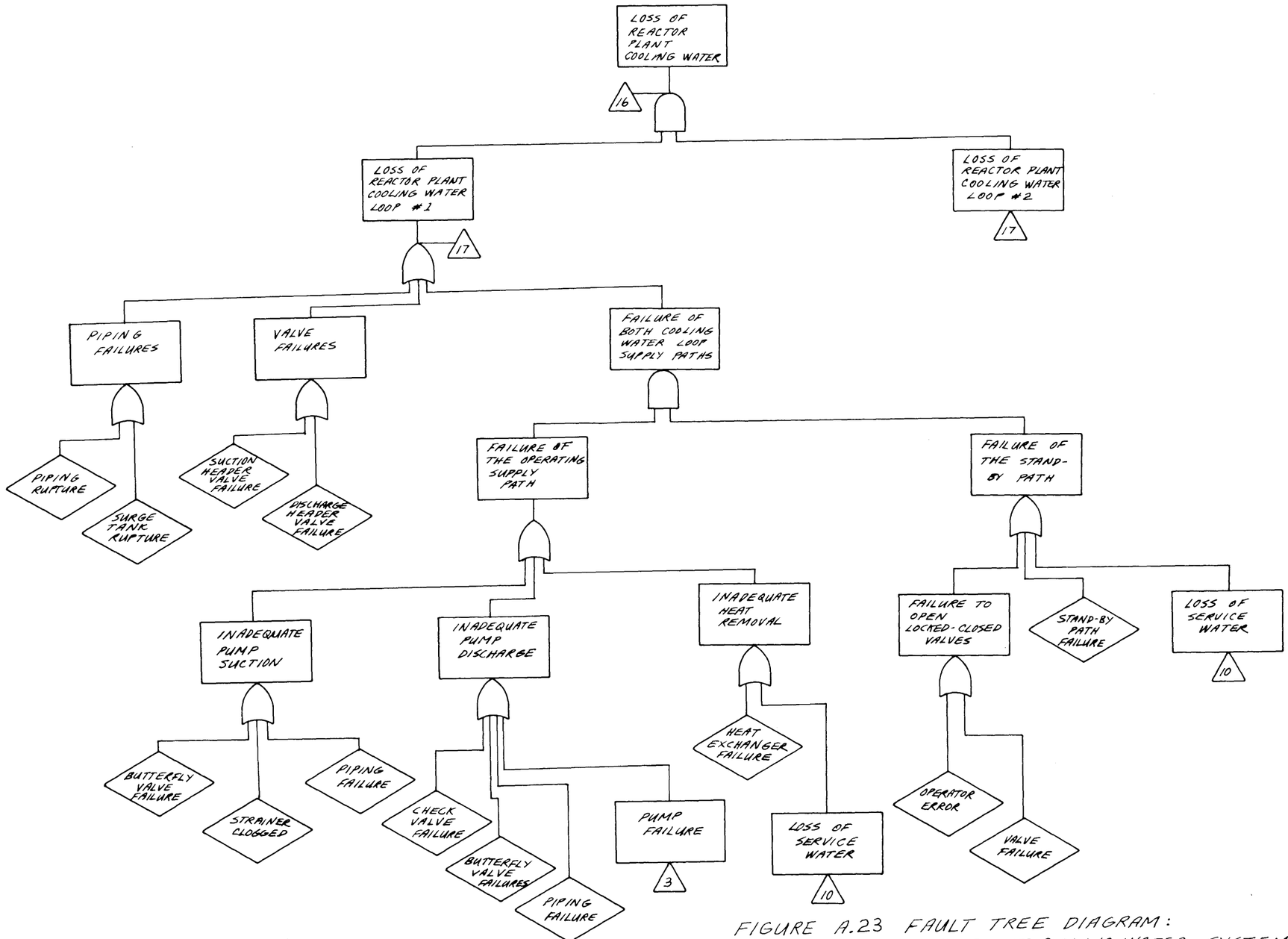


FIGURE A.23 FAULT TREE DIAGRAM:
REACTOR PLANT COOLING WATER SYSTEM

A.15 The Main Circulator Service System

This system supplies the main circulator-turbine with high-pressure water for bearing lubrication. It also supplies purified buffer helium to the lower shaft-seal of the circulator-turbine bearing unit to prevent both the in-leakage of bearing water to the reactor coolant, and the out-leakage of the reactor coolant. Cooled and filtered bearing water is supplied to each main circulator from an independent module. The purified buffer-helium is supplied from an integrated system which is common to all three circulators.

A schematic flow diagram for the system is shown in Figure A.24. The components of this system are located inside the reactor containment, and they must then be designed to perform properly at the pressures and temperatures associated with all containment atmosphere conditions.

During a reactor shutdown, the continued supply of high-pressure, clean, and cooled water to the circulator-turbine bearing is essential. The turbine-driven bearing-water pump supplies water a roughly 1000 psi above the reactor coolant pressure at all operating conditions. Thus, while the reactor coolant pressure may vary, and with it the bearing water supply pressure, the differential pressure will be maintained constant. The bearing water at the pump discharge if filtered before it is supplied to the bearing. In addition to the turbine-driven pump, each module contains an electric drive pump which is used during start-up.

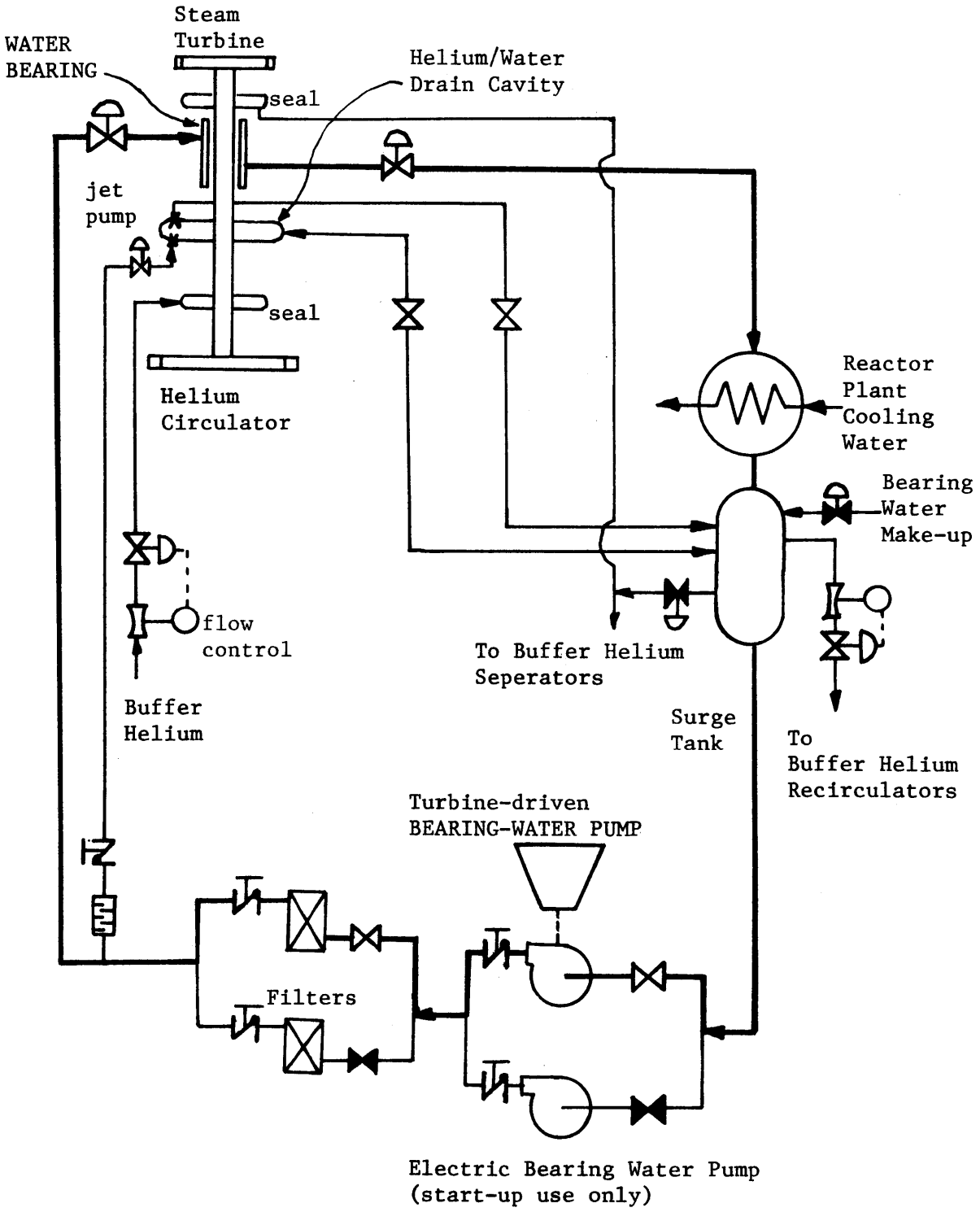


FIGURE A.24 A Schematic Flow Diagram of a Main Circulator Service System

The bulk of the water leaves the bearing through the main drain. The back pressure on this main drain is maintained at 20 psi above the reactor coolant pressure by a differential pressure control valve, and the drain water passes through a heat exchanger before it is returned to the surge-separator tank for recycle.

The bearing heat load is removed in the heat exchanger by water from the reactor plant cooling water system. The heat generated by bearing friction varies with the circulator speed, and during normal operation of the circulator, this amounts to 3×10^6 BTU/hr. During a normal pressurized shutdown, where the main helium circulators are quickly slowed down, the bearing heat load reduces greatly. At 10% circulator speed, the heat load is only 1954 BTU/hr and would require a reactor plant cooling water flow of less than 0.2 gpm at a $20^{\circ}F$ temperature rise through the heat exchanger. Because of the low heat load, the bearing water temperature should be relatively stable, and the continued supply of reactor plant cooling water to the heat exchanger was not considered to be critical during a reactor shutdown. However, during a PCRV depressurization accident, it was assumed that reactor plant cooling water was necessary to maintain acceptable bearing water temperatures. The main circulators operate at close to the design speed during a depressurization accident, and it was felt that this would generate considerable friction.

The buffer helium supply was also not considered to be crucial to the shutdown performance of the circulator. Neither the helium coolant out-leakage nor the bearing water in-leakage which might result should have any significant effect on the circulator operation.

The fault tree diagram for the circulator bearing water supply is shown in Figure A.25. The system failure probability was determined from the following contributors.

Failure of the bearing-water differential pressure control valve	1×10^{-6}/hr
Failure of the bearing drain-water differential pressure control valve	1×10^{-6}/hr
Bearing water pump failure	3×10^{-5}/hr
Bearing water pump control valve failure	3×10^{-6}/hr
	3.5×10^{-5}/hr

The probability of a circulator failure due to a bearing water supply failure is then $<2 \times 10^{-5}$ for the first 30 minutes following the shutdown. This failure probability is negligible compared to the failure rates of the other main loop subsystems. However, it is important to note that the correct operation of the three control valves is dependent on instrument air. The exact effect which loss of instrument air has on the performance of the bearing water supply is unknown, but instrument air failure already leads to main loop failure.

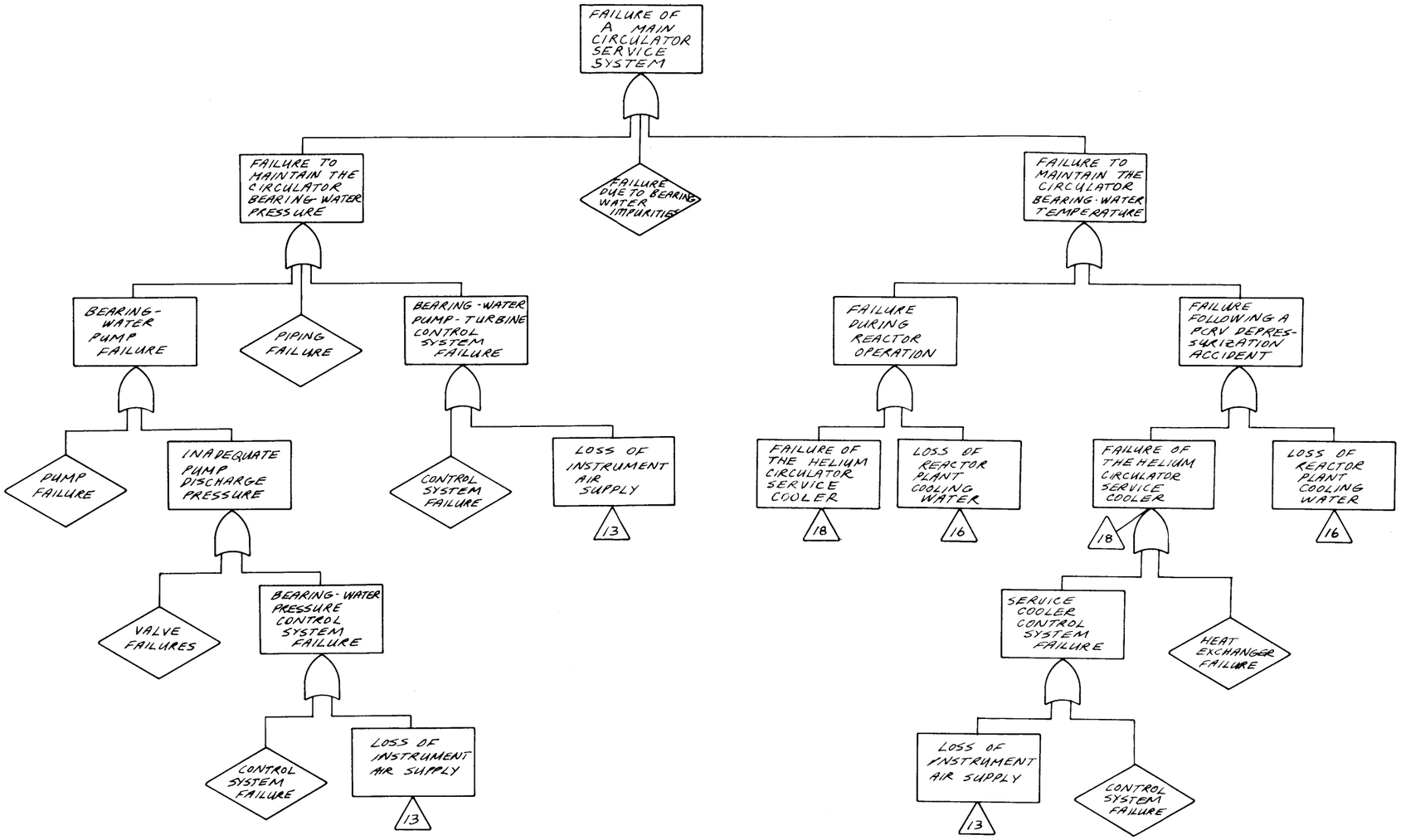


FIGURE A.25 FAULT TREE DIAGRAM:
MAIN CIRCULATOR SERVICE SYSTEM

Thus the additional failure of the bearing water supply should not significantly contribute to the main loop failure probability.

A.16 Off-Site Power Supply

The availability of AC electric power during a reactor shutdown is quite important. Without power to the main loop cooling system and the CACS, the loss of core heat removal capability will eventually occur.

During a reactor shutdown, the off-site power connection becomes the primary source of electricity to the essential plant loads because a turbine trip always accompanies a reactor shutdown. If this source of electrical power is lost, then only the emergency diesel generators remain.

A.16-1 The Loss of Off-Site Power

In general, the loss of off-site power can accompany a reactor shutdown by two methods.

The first mechanism begins with the initiation of a reactor shutdown, which also initiates a turbine trip. The loss of the main generator can cause a load transient in the electrical network which may exceed the stability unit of the system. If this limit is exceeded, then off-site power is lost. Off-site power may also fail to energize the essential electrical buses following a reactor shutdown due to a failure in the high-speed switching mechanism which transfers the load from the unit auxiliary transformer to the off-site power transformer.

The second mechanism is initiated by the loss of the external plant load and off-site power source. In this event, the turbine-load-reject mechanism functions to reduce the turbine-generator load in order that it continue operating to power the plant's electrical loads. If the turbine-load-rejection fails, a turbine trip and reactor shutdown will be initiated.

The probability of a loss of off-site power and external load to the power plant is 0.1 per year. This value is based on nuclear power plant experience between March 1969 and March 1974. An examination of the Abnormal Occurrence Reports filed with the Atomic Energy Commission between these dates was made by Fleming [10]. Eight occurrences of a loss of off-site power and external load were reported in this period, which represents over 690,000 reactor-hours of nuclear power plant operation. This is an average of 1 loss of off-site power event per over 86,000 reactor-hours, or just slightly over 0.1 events per reactor year.

In the GCFR, given a loss of off-site power event, a reactor trip need not occur unless the turbine load-reject mechanism fails. Fossil-fired power plants in the U.S., and nuclear units in Great Britian can successfully undergo full turbine-load-rejection and continuing operation to power the plant auxiliaries. Experience in the U.S., based on a limited number of power plant tests resulted in only 1

failure to full-load reject of the 7 plants tested [11]. In the U.K., 79 station years of nuclear power plant experience has resulted in 95 situations of "risk to the turbine," where a fault in the electrical network required the plant to be disconnected. Of these events, only 16 resulted in a turbine trip at the plant [12]. This is an average probability of 0.17 for failure of the turbine to successfully full-load-reject. This would indicate that the failure rate of turbine-load-reject mechanisms is on the order of 10^{-1} per demand.

Thus, the probability that a loss of off-site power will result in a reactor shutdown is on the order of 10^{-2} per year. Considering that this evaluation is concerned with the relative core-melt probabilities of the various initiating event categories, this order of magnitude estimate was thought to be most appropriate.

In the RSS a probability of 1×10^{-3} per turbine trip is given for the occurrence of a loss of offsite power as a result of the reactor shutdown. This was based on information supplied by the Federal Power Commission on transient stability for power plants east of the Rockies. This value pertains to a 1000 MW(e) generating plant. The effect on the electrical network of a 300 MW(e) GCFR would be much less severe, and the probability of this occurrence would be much less likely. Therefore, this occurrence was not considered to be a significant factor leading to a reactor shutdown with offsite power unavailable.

A.16-2 The Restoration of Off-Site Power

The likelihood that offsite power will be restored is a function of time. WASH-1400 utilized data from the Bonneville power administration on transmission line outages for the years 1970, 1971 and 1972 to determine a model for the restoration of offsite power. This curve is shown in Figure A.26. The curve is a cumulative plot of the percentage of repairs completed within a given time.

The curve is based on data from more than 1500 outages of transmission lines rated at 500, 345, 287, 230, 138 and 115 kV. While these outages did not all constitute a loss of offsite power, the repair data are directly applicable to the reapir of an offsite power line. The outages in the data were caused by such factors as falling trees, lightning, storm, fire, malicious damage, and accidental damage. This data can be seen more clearly in Figure A.27 which is taken directly out of Appendix III of the RSS. This is a histogram of the restoration times, and it also lists the major contributors to each category.

In the ESD, the restoration of off-site power was allowed to occur at specific time intervals following the shutdown. These are listed below with the values taken from Figure A.26.

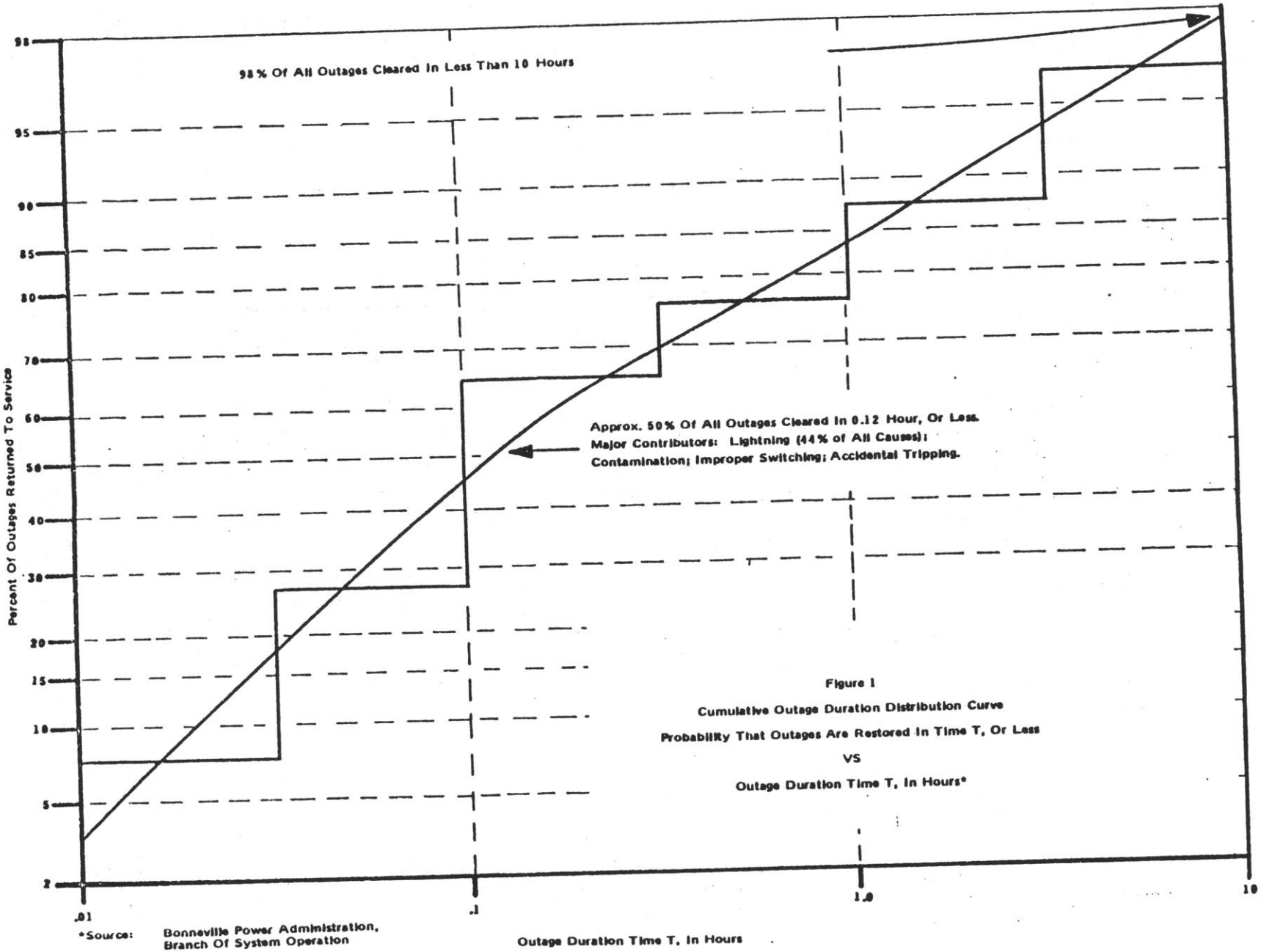


FIGURE A.26 **Cumulative Outage Duration Distribution Curve**

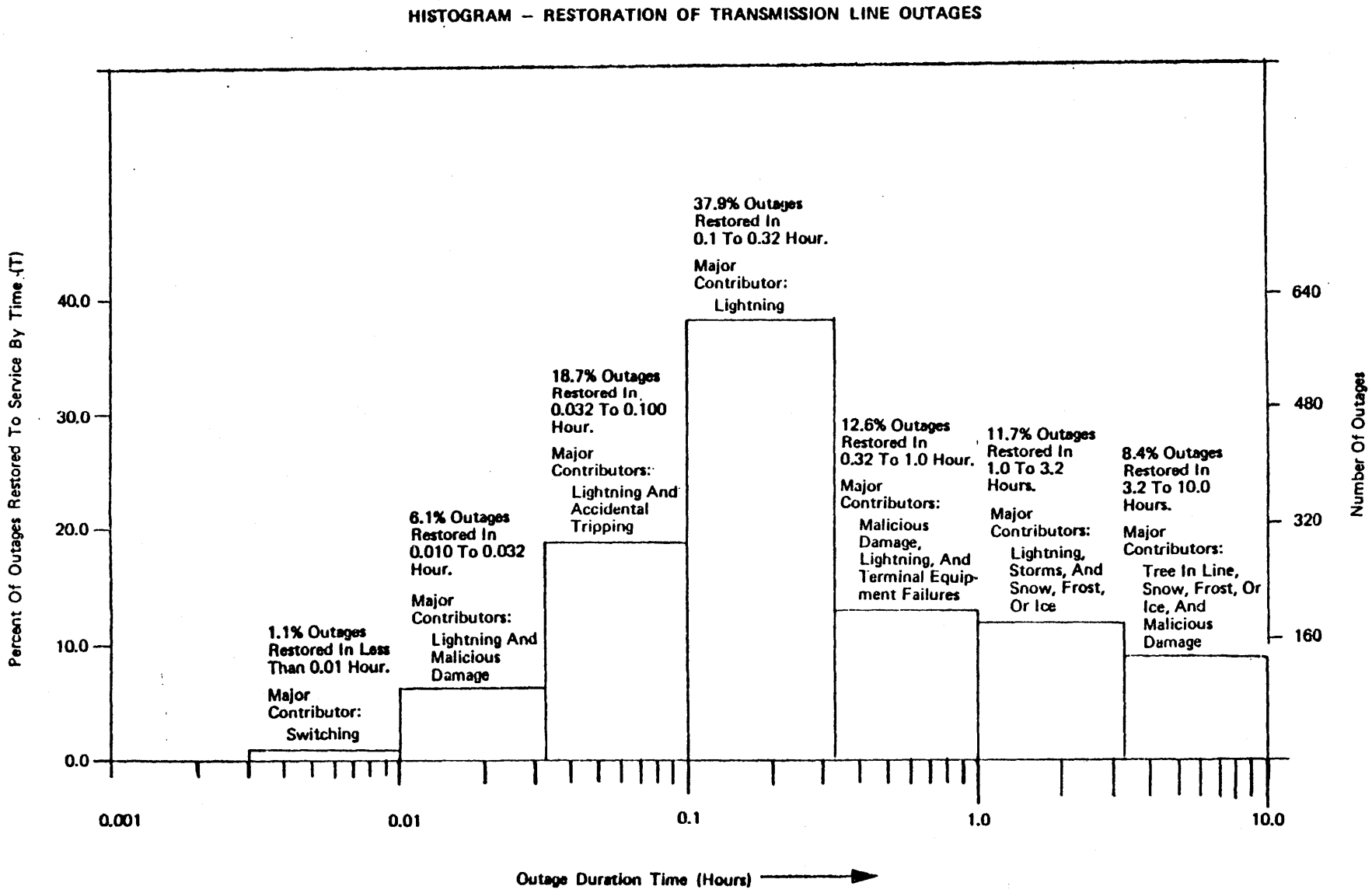


FIGURE A.27 **Histogram - Restoration of Transmission Line Outages**

Time Interval Within Which Offsite Power May Be Restored	Probability of the Restoration of Offsite Power to the Essential Buses Within the Time Interval
30 minutes	.75
25 minutes	.70
20 minutes	.68
15 minutes	.65
10 minutes	.60
5 minutes	.35

Restoration of offsite power after the initial thirty minute interval was not considered because the main loops were assumed to be capable of core cooling for at most thirty minutes. Thus, if electrical power was not available from at least one diesel generator, of if offsite power were not restored, then a loss of adequate core cooling was assumed to occur.

A.17 Main Loop Isolation Valves

Description

Each main cooling loop is supplied with a self-actuating isolation valve to prevent back-flow of helium through the loop in the event its main circulator is shutdown. The valve is located at the entrance to the cross duct leading from the main circulator outlet plenum to the reactor inlet plenum. This was shown in Figure 2.1 and in Figure 2.3.

Each valve consists of seven solid-steel air foil-shaped louvers which act independently of each other. The design of the louvers is such that, with the main circulator operating, aerodynamic lift forces hold the valves open. If the circulator is stopped, the helium flow will stop and may reverse; this eliminates the aerodynamic lift forces. The louver is then closed by gravitational forces and it is held closed by the pressure differential force across the closed valve.

The louvers rotate on self-lubricating spherical bushings that minimize binding even if the louver deflects under pressure loading or temperature differential. Also, the opening of each louver is limited by a stop pin which maintains the air foil at a small "angle of attack." This will minimize louver vibration under normal operation, and it will provide an additional design force for the valve.

Valve Reliability

The reliability of the main loop isolation valve was considered for both the closing of the valve and the opening of the valve. The design of the valve is such that the louvers operate independently, yet not all must be in the same position (all open, or all closed) for the valve to be effectively open or closed. This can be seen more clearly in Figure A.28 [13] which is a plot of the ratio of the valve flow resistance to the full open valve flow resistance as a function of the number of louvers open. From the figure, it is seen that with three louvers open, the flow resistance is not

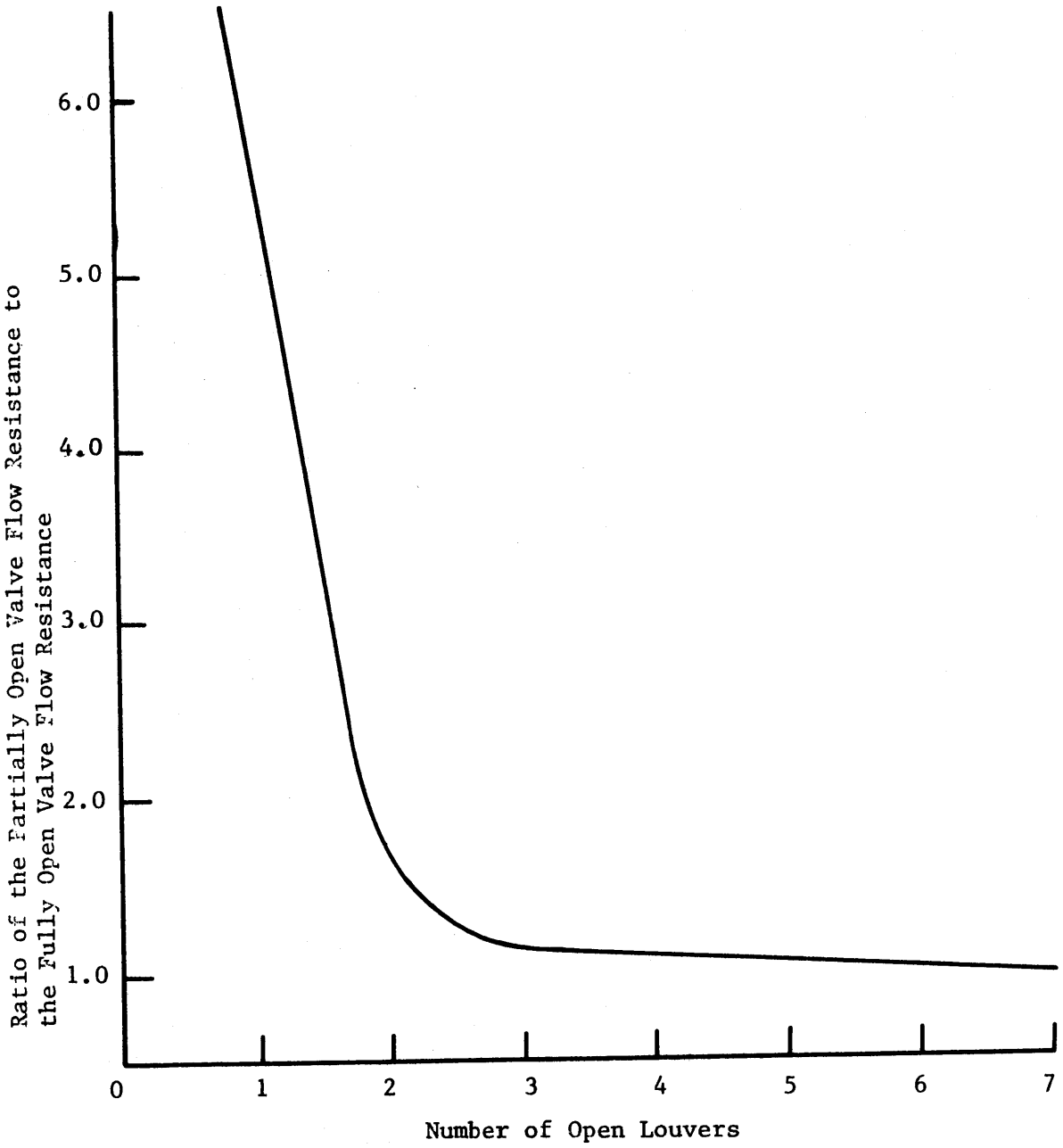


FIGURE A. 28 Main Loop Isolation Valve Flow Resistance as a Function of the Number of Open Louvers

significantly different from the full open flow resistance, and the valve was assumed to be fully open. Likewise, the valve flow resistance is not significantly increased until at least six louvers close. Thus, the failure of the valve to close was assumed to result from the failure of at least six louvers to shut, and the failure of the valve to open was assumed to result from the failure of at least three louvers to open.

The reactor safety study gives a check valve failure rate of 1×10^{-4} per demand. Assuming that each louver is an independent check valve, but allowing for potential common mode failures (Beta factor = 0.1) gives a valve failure rate on the order of 10^{-5} per demand. However, it was this author's opinion that the failure rate of the valve to close could be significantly higher. This is due to the fact that the valve may be full open in a high temperature environment for many months. Also, there are no present provisions for testing the valves during reactor operation. Thus, a conservative estimate of 1×10^{-3} per demand was used for failure of the valve to close. On the other hand, the reliability of the valve to open on demand was considered to be higher due to the fact that during a shutdown it does not remain in the closed position for any length of time before it is required to open. Also, the opening of the valve only requires the correct operation of three louvers, as opposed to six for the closing of the valve.

Following shutdowns in which the reactor remains pressurized, main loop isolation valve failures which result in core flow bypass were included in the ESD modelling by assuming the limiting steam generator inventory depletion times. These do not significantly affect the main loop reliability. However, there can be main loop isolation valve operations during a shutdown which may have a significant effect on the main loop reliability. In those shutdown sequences where a circulator-turbine control valve failure occurs in one or two operating loops, an out-of-balance condition will exist between the three main cooling loops. This situation can be created by a failure of either the large control valve or the small control valve, and the circulator for the loop with the failed valve (this loop is called the failing loop) will operate at a higher speed than the loops with correctly functioning valves (these loops are called the normal loops). The helium flow in the normal loops may then stop or even reverse due to the pressure rise created by the circulator in the failing loop, and the main loop isolation valves for these normal loops may close.

If the isolation valves do close, then when the failing loop stops, the isolation valves for the normal loops must re-open to allow heat removal to continue with the main loop cooling system. It is also required that the helium circulator remain operable after the period of running behind its

closed isolation valve. In the event the isolation valve does not close, then the helium circulators in the normal loops must not fail due to the increased pressure differential, or possible reverse flow against which they are operating.

These events are modelled explicitly in the ESD for those shutdown sequences in which they can occur. A distinction is made in the probability that an isolation valve will close for sequences in which the failing loop has a failed large control valve and those in which the small control valve is failed. This was due to the fact that the closing force on the valve should be much greater if a circulator is being driven at its full rated speed. Also, the forces imposed on a normally operating circulator, whose isolation valve failed to close, would be much greater. A distinction was also made in the modelling of the isolation valve openings depending upon whether the loop was normally operating or if it had a failed CT small CV. However, in the final analysis, no distinction was made in the valve for reliability of the valve to open for these two cases.

The reliability values used for each of these valve or circulator functions were presented in Table 4-X along with the ranges assumed for the sensitivity analysis. Summarized below are those considerations made in arriving at these values.

A main loop isolation valve closes given:

1) A CT large CV fails on another loop.

The closing forces in this case should be relatively large (about that available in a normal loop shutdown), however, due to fact that the loop circulator is still operating there will be a combination of forces acting on the valve. Therefore, the probability that the valve closes was assumed to be 5×10^{-3}.

2) A CT small CV fails on another loop.

The closing forces in this case are relatively small, especially compared to the case above, and the probability for this event was assumed to be 2.5×10^{-2}.

A main loop isolation valve opens and the circulator is operable:

The pressure rise created by the circulator in its shutdown mode is not as great as that normally available to open the valve. However, sufficient positive opening force should be available. The valve has just been shut and it should not be subject to any conditions which might cause it to stich in the short period before it is re-opened. Also, the out-of-balance condition which closed the valve should be within the design margin of the valve, and it should not significantly affect the re-opening of the valve. However, the circulator must remain operable after the period of operation behind its closed valve. This was assumed to

be the limiting factor, and the failure probability for this event was assumed conservatively to be 1×10^{-3}. A main helium circulator remains operable after an out-of-balance condition in which its isolation valve failed to close. The condition caused by:

1) A CT large CV fails to close in another loop.

While the out-of-balance condition will last only a minute or two, the pressure forces against which the circulator must operate are large. It was assumed that the circulator had a 50 percent change of surviving this condition. This is felt to be conservative, but there is no basis for judgement. The range in the sensitivity analysis was from a 95 percent chance of survival to only a 10% chance of survival.

2) A CT small CV fails to throttle in another day.

In this case, the out-of-balance condition may last as long as 3 or 4 minutes. However, the pressure forces against which the circulator must operate are much less than in the case above. The circulator was assumed to have a 95 percent chance of surviving these conditions, and the range used in the sensitivity analysis was from .995 to .75.

A.18 Main Loop Support System Dependencies

Those systems which perform support functions for the main loop cooling system are:

- The main circulator service systems,
- The service water system,
- The instrument and service air systems, and
- The uninterruptable AC power supplies.

The dependence of the main loop cooling system on the functioning of its support systems was lumped into a single input variable. It was assumed that a failure in a support system caused the elimination of the main loop cooling system heat removal capability in either the interval between five and fifteen minutes after the shutdown, or some time after 15 minutes.

Individual failures of the main circulator service systems and uninterruptable AC power supplies were not considered to be important contributors to the failure of the main loop cooling system following a shutdown. For the main circulator service system, no change in function occurs and so the failure probability of the system during the shutdown and decay heat removal operations is low compared to the failure rate of the other main loop shutdown cooling subsystems. For the uninterruptable AC power supplies, failures independent of loss of power to the essential buses were not considered because no change in function occurs. Also, in

most cases, loss of essential AC power eliminates the main loop irrespective of the uninterruptable AC power on the loop.

For the pressurized reactor shutdowns, the service water system was also not considered essential to initial operation of the main loop cooling system. The service water system provides the ultimate heat rejection for the main circulator-turbine bearing heat load. This heat duty is quite small in a pressurized shutdown and operation of the main loop cooling system should continue unaffected for a considerable period of time. The actual time period will depend on the water inventory of the bearing-water system if no consideration of the reactor plant cooling water system is allowed.

However, in a depressurized shutdown, the bearing friction was assumed to be somewhat more significant that in a pressurized shutdown, and the operation of the reactor plant cooling water system and the service water system were required. The probability of main loop cooling system failure due to the loss of either of these systems was determined to be limited by the service water system failure probability.

The most important dependence of the main loop cooling system, following any shutdown, is with the instrument air system. The main loops depend on instrument air for vital valve actions and valve controller functions. These include,

most importantly, the CT small control valve and shutdown controller, the resuperheater bypass control valve, the bearing-water pump turbine control valve, and the bearing water differential pressure control valves. Of these valves, the turbine control valves are required to perform important regulating functions during the shutdown and they therefore need a continuous supply of instrument air. The operation of the CT small CV was assumed to be the limiting factor in the functioning of the main loops. With the loss of instrument air, a maximum of 15 minutes of main loop cooling system operation was allowed due to partial valve action using the accumulator air supply early in the shutdown process. At the end of this time the steam generators of all the loops were assumed to be depleted due to incomplete throttling of the CT small CV's.

The instrument air system is also dependent on the service water system for the cooling-water requirements of the air compressors. Thus, failures of the service water system will eliminate the instrument air compressors after a time lag, and this was assumed to occur in the interval of 15 to 30 minutes following the shutdown.

A range of the failure probability of the main loop cooling system due to support system failures following a reactor shutdown was determined based on the above considerations and the failure rates of the support systems.

These ranges were listed in Table 4-XII for pressurized shutdowns and depressurized shutdowns, and for each of the availability states of the essential electrical supply.

A.19 Containment Equalization Pressure Ranges

Following a PCRV depressurization accident, the containment equalization pressure range may have a significant effect on the main loop and the CACS heat removal capabilities. Three ranges of the containment equalization pressure range were selected as was discussed in Section 3.4-3. The design equalization pressure is 1.8 atmospheres, and the three pressure ranges chosen for modelling the shutdown cooling accident sequences were 1) >1.50 atmospheres, 2) 1.50 to 1.25 atmospheres, and 3) <1.25 atmospheres.

In order to estimate the probability of occurrence of these pressure ranges, the containment isolation system and the containment purge system were investigated. The presently available information on these system indicates that they should be capable of acting to maintain the containment integrity with a high degree of reliability. Also, no attempt was made to estimate the likelihood of containment failure due to a missile generated during the PCRV depressurization. The probability of the containment equalization pressure ranges was determined based solely on the judgement of this author.

The reliability of the containment to be properly isolated following the receipt of a high containment pressure signal was considered to be at least as high as .999. Thus, the probability that the containment equalization pressure would be greater than 1.50 atmospheres was assumed to be .999.

For the containment pressure to equalize below 1.25 atmospheres would require a rather large opening in the containment. This might result from a complete failure of the containment purge system to isolate the inlet or exhaust ducts. It might also result from a large, missile-produced breech in the containment. However, the probability of any of these occurrences following a PCRV depressurization was considered to be less than 1×10^{-4} per event.

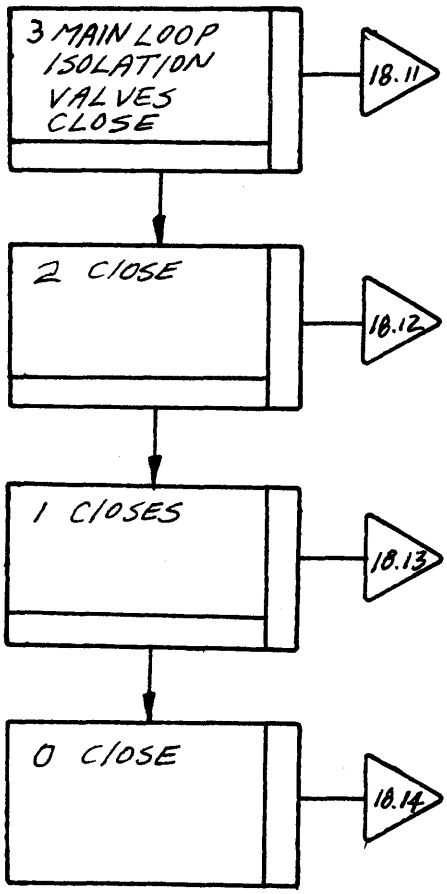
The probability that the containment equalization pressure range is between 1.50 and 1.25 atmospheres was simply assumed to be the probability that it was not in either of the other two ranges.

The sensitivity of these assumptions was investigated in some detail in the sensitivity analyses, and this is discussed in Chapters 5 and 6.

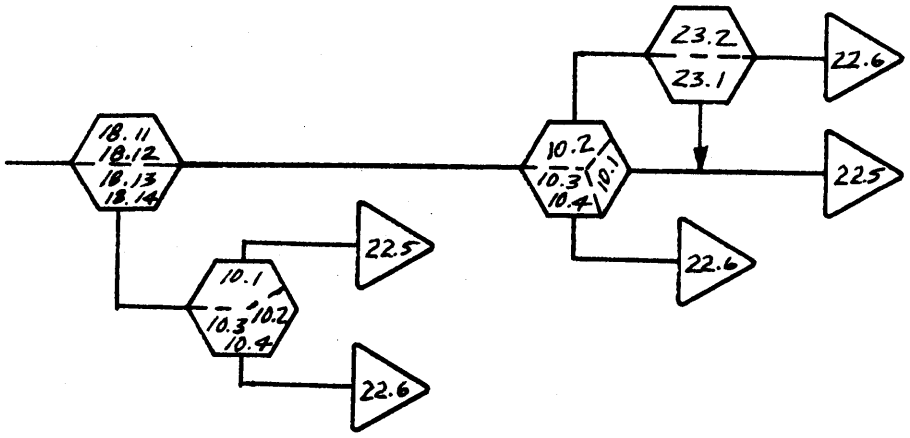
Appendix B
CACS Operating States Following a Depressurization Accident

Following a PCRV depressurization accident, the CACS operating states were described by a single variable with index number 22. This variable described the properly combined operating states of the CACS for each condition of main loop isolation valve failure and for different time intervals following the shutdown.

The four possible combinations of main loop isolation valve bypass were described as shown below.



The overall CACS operating states, as described in Table 3-IXa&b, were combined as shown in the example below for the case of 3 essential buses energized and main loop failure occuring in the interval 5 to 10 minutes following the shutdown.



The overall CACS operating states as described by the index numbers are summarized in Table B-I.

Table B-I
CACS Operating States Following a Depressurization Accident (a)

Time Interval in which Main Loop Failure Occurs	Three Essential Buses Energized			Two Essential Buses Energized			One Essential Bus Energized	
	CEP 1.50atm.	CEP 1.50 1.25atm.	CEP 1.25atm.	CEP 1.50atm.	CEP 1.50 1.25atm.	CEP 1.25atm.	CEP 1.50atm.	CEP 1.25atm.
0 to 2 minutes	22.1 22.2	22.13 22.14	22.15 22.16	22.21 22.22	*	*	*	*
2 to 5 minutes	22.3 22.4	22.1 22.2	22.15 22.16	22.23 22.24	22.21 22.22	*	*	*
5 to 10 minutes	22.5 22.6	22.17 22.18	22.13 22.14	22.23 22.24	22.21 22.22	*	*	*
10 to 15 minutes	22.7 22.8	22.3 22.4	22.13 22.14	22.25 22.26	22.23 22.24	*	*	*
15 to 20 minutes	22.9 22.10	22.5 22.6	22.13 22.14	22.27 22.28	22.23 22.24	*	22.29 22.30	*
20 to 25 minutes	22.9 22.10	22.19 22.20	22.17 22.18	22.27 22.28	22.23 22.24	22.21 22.22	22.29 22.30	*
25 to 30 minutes	22.11 22.12	22.7 22.8	22.17 22.18	22.31 22.32	22.25 22.26	22.21 22.22	22.29 22.30	*

(a) Top index is the success state and the bottom index is the failure state.

* No successful CACS operating state

Appendix C
Nomenclature

ACRS	Advisory Committee on Reactor Safeguards
AEC	Atomic Energy Commission
	the beta factor, fraction of common mode failures
CEP	containment equalization pressure
CT large CV	circulator-turbine large control valve
CT small CV	circulator-turbine small control valve
DBDA	design basis depressurization accident
ERDA	Energy Research and Development Administration
GA	General Atomic Company
GCFR	gas-cooled fast breeder reactor
HTGR	high temperature gas-cooled reactor
LMFBR	liquil-metal-cooled fast breeder reactor
LOCA	loss of coolant accident
LWR	light water reactor
NSSS	nuclear steam supply system
OPS	operational protection system
p	subsystem unit reliability
PCRV	prestressed concrete reactor vessel
PCS	plant control system
PPS	plant protection system
PSID	Preliminary Safety Information Document
q	subsystem unit failure probability
RSS	Reactor Safety Study
T	test and maintenance unavailability of
z	subsystem common mode failure probability

References

Chapter 1 Scope and Intent of Research

(1) U.S.A.E.C., "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Draft Report. WASH-1400, August, 1974.

(2) Green, A.E., and Bourne, A.J., Reliability Technology, Chapter 1. Wiley-Interscience, London, 1972.

(3) Steward, R.M. "The Application of Modern Safety and Reliability Methods to the Design and Operation of Protective Systems for Large Potentially Hazardous Chemical Plants," Presented to the 1974 Engineering Foundation Conference at Henniker, New Hampshire, July 21-26, 1974.

(4) General Atomic Company, "300MW(e) Gas-cooled Fast Breeder Reactor Demonstration Plant," Report GA-A13045, July 15, 1974.

(5) Rasmussen, N. C., Director: Reactor Safety Study, Statement before the Joint Committee on Atomic Energy Hearings on Nuclear Reactor Safety: September 25, 1973.

(6) Lambert, M.E., "Systems Safety Analysis and Fault Tree Analysis, "Lawrence Livermore Laboratory, Report UCID-16238, May, 1973.

Chapter 2 The Gas-cooled Fast-breeder Reactor

(1) General Atomic Company, "Preliminary Safety Information Document (PSID); Gas-cooled Fast-breeder Reactor (GCFR)," Report GA-10298, Volumes I and II with Amendements 1 through 6, San Diego, California, March, 1971, through June, 1974.

(2) General Atomic Company, "Supplement to the PSID; GCFR, Additional Information on the GCFR concept Requested by the Advisory Committee on Reactor Safeguards," Report GA-10298 Supplement, San Diego, California, June, 1972.

(3) General Atomic Company, "Responses to AEC Questions on the PSID for the GCFR," Report GA-10298 Supplement II, Volumes I and II, San Diego, California, October, 1973.

References

Chapter 2 (cont'd)

(4) U.S. Atomic Energy Commission, Directorate of Licensing, "Preapplication Safety Evaluation for the Gas-cooled Fast-breeder Reactor," Project No. 456, August 2, 1974.

(5) Bechtel Corporation, "300 MWe GCFR Balance of Plant Preliminary Engineering and Cost Estimate," and "300 MWe GCFR Balance of Plant Follow-on-study," San Francisco, California, Job 10437, August, 1973, and November, 1973.

(6) Perkins, R., "Core Cooling Capabilities in the 300 MW(e) GCFR Demonstration Plant Following Various Combinations of Main Loop, Auxiliary Loop, and Check Valve Failures." Unpublishec Data, August, 1974.

(7) General Atomic Company, "Responses to AEC Questions on the PSID for the GCFR," Report GA-10298 Supplement II, Question 6.3-6, San Diego, California, October, 1973.

Chapter 3 Thesis Methodology

(1) U.S.A.E.C., "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Appendix I, Event Tree Methodology, Draft Report Wash-1400, August, 1974.

(2) Perkins, R., "Core Cooling Capabilities in the 300 MW(e) GCFR Demonstration Plant Following Various Combinations of Main Loop, Auxiliary Loop, and Check Valve Failures," unpublished Data, August 13, 1974.

(3) U.S.A.E.C. "Reactor Safety Study: An assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Appendix III, Failure Data, Draft Report Wash-1400, August, 1974.

(4) General Atomic Company, Presentation Before the Advisory Committee on Reactor Safeguards, Washington, D.C., September 5, 1974.

(5) General Atomic Company, "Responses to AEC Questions on the PSID for tbe GCFR," Report GA-10298 Supplement II, Questions 6.3-4 and 6.3-5, San Diego, California, October, 1973.

References

Chapter 3 (cont'd)

(6) U.S.A.E.C., Directorate of Licensing, "Preapplication Safety Evaluation for the GCFR," Project No. 456, August 1, 1974.

Chapter 4 Initiating Events and Accident Sequence Analysis Inputs

(1) Torri, A., and Driscoll, M.J., "Reactivity Insertion Mechanisms in the GCFR," Report GA-A12934, April 1974.

(2) U.S.A.E.C., Office of Operations Evaluations, "Evaluation of Nuclear Power Plant Availability," Report 00E-ES-001, January, 1974.

(3) Personal Communication with A. Kelley, General Atomic Company, San Diego, California.

(4) U.S.A.E.C., "Reactor-Safety Study; An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Draft Report WASH-1400, August 1974.

(5) General Atomic Company, "Preliminary Safety Information Document; GCFR," Section 14, Report GA-10298, San Diego, California, June 1974.

(6) Personal correspondence with K.N. Fleming, General Atomic Company, San Diego, California, December, 1975.

(7) U.S.A.E.C., "Reactor Safety Study; An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Appendix III, Failure Data, Report WASH-1400, August, 1974. Draft.

(8) Drake, A.W., Fundamentals of Applied Probability Theory, McGraw-Hill Book Company, New York, 1967.

(9) Fleming, K.N., "A Reliability Model for Common Mode Failures in Redundant Safety System," Report GA-A13284, December, 1974.

(10) U.S.A.E.C., "Reactor Safety Study; An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Appendix II, Fault Tree Methodology, Draft Report, WASH-1400, August, 1974.

References

Chapter 4 (cont'd)

(11) U.S.A.E.C., Office of Operations Evaluations "Diesel Generator Operating Experience at Nuclear Power Plants," Report 00E-ES-002, June, 1974.

(12) Epler, E., "Common Mode Failure Considerations in the Design of Systems for Protection and Control, "Nuclear Safety, Vol. 10, No. 1, January-February, 1969.

Chapter 5 Sensitivity Analysis

(1) U.S.A.E.C., Office of Operations Evaluation, "Diesel Generator Operating Experience at Nuclear Power Plants," Report 00E-ES-002, June, 1974.

(2) Personal correspondence with J.A. Larrimore, General Atomic Company, San Diego, California.

Chapter 6 Probability of a Core Meltdown

(1) U.S.A.E.C., "Reactor Safety Study; An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Appendix II, Fault Tree Methodolody, Draft Report WASH-1400, August, 1974.

Chapter 7 Conclusions and Remarks

(1) U.S.A.E.C., "Reactor Safety Study, An assessment of Accident Risks in Commercial Nuclear Power Plants," Draft Report WASH-1400, August, 1974.

(2) General Atomic Company, "Gas-Cooled Fast Reactor Safety Program, Annual Progress Report for the Period Ending December 31, 1974," Report GA-A13490, August, 1975.

Appendix A

(1) U.S.A.E.C., "Reactor Safety Study; An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Appendix III, Failure Data, Draft Report WASH 1400, August, 1974.

(2) Fleming, K.N., "A Reliability Model for Common Mode Failures in Redundant Safety Systems," Report GA-13284 December, 1974.

(3) U.S.A.E.C., Office of Operations Evaluation, "Diesel Generator Operating Experience at Nuclear Power Plants," Report 00E-ES-002, June, 1974.

(4) Epler, E., "Common Mode Failures, Considerations in the Design of Systems for Protection and Control," Nuclear Safety, Vol. 10, No. 1, January-February, 1969.

(5) U.S.A.E.C., "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Appendix II, Fault Tree Methodology, Draft Report WASH-1400, August, 1974.

(6) Lambert, M.E., "Systems Safety Analysis and Fault Tree Analysis," Lawrence Livermore Laboratory, Report UCID-16238, May, 1973.

(7) McLaughlin, M.A., Preliminary Fault Tree Analysis for the FFTF," Battelle Memorial Institute, Pacific Northwest Laboratory, BNWL-874, May, 1969.

(8) General Atomic Company, "Additional Information on the GCFR Concept Requested by the Advisory Committee on Reactor Safeguards," Answer to Question 12, Report GA-10298 Supplement, San Diego, California, June, 1972.

(9) General Atomic Company, "Additional Information on the GCFR Concept Requested by the Advisory Committee on Reactor Safeguards," Answer to Question 10, Report GA-10298 Supplement, San Diego, California, June, 1972.

(10) Personal correspondence with K.N. Fleming, General Atomic Company, San Diego, California, December, 1975.

(11) Olken, M.I. and Woelfle, W.T., "Load Rejection of Subcritical Steam Turbine-Generator Units," IEEE Transaction Paper No. T72580-9, July, 1972.

(12) Fleming, K.N., "British Turbine Trip Data," Unpublished Data, December, 1975.

References

Appendix A (cont'd)

(13) Kelley, A.P., "Reliability of Self-Actuating Main Loop Isolation Valves," Unpublished Data, July, 1974.