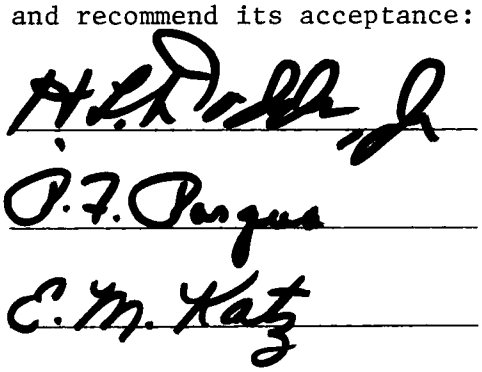
To the Graduate Council:

I am submitting herewith a thesis written by David F. Montague entitled "A Procedure for Determining the Expected Number of Failures of a Phased Mission." I recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Engineering, with a major in Nuclear Engineering.



L. B. Fussell, Major Professor

We have read this thesis
and recommend its acceptance:



Accepted for the Council:



Vice Chancellor
Graduate Studies and Research

Thesis
79
.M645
cop. 2

A PROCEDURE FOR DETERMINING THE EXPECTED NUMBER OF FAILURES OF A PHASED MISSION

A Thesis

Presented for the

Master of Engineering

Degree

The University of Tennessee, Knoxville

David F. Montague

August 1979

1397110

ACKNOWLEDGEMENTS

The author wishes to express his sincere appreciation to his advisor, Dr. J. B. Fussell, whose support and advice were vital to the completion of this thesis.

The author also wishes to thank Dr. P. F. Pasqua for supporting this thesis through a research assistantship. Dr. B. B. Chu of the Electric Power Research Institute is also gratefully acknowledged for his support.

Special appreciation is reserved for Miss L. S. Baker and Mr. H. A. Stiles for their assistance in the final stages of this task. The author also thanks, Barbara Klopatek, who typed this thesis.

The author would like to thank Dr. H. L. Dodds and Dr. E. M. Katz for their support in the completion of this thesis.

The work reported herein was performed under a contract between the Nuclear Engineering Department, The University of Tennessee, and Electric Power Research Institute.

ABSTRACT

A procedure for determining the expected number of failures of systems undergoing phased missions is described. Approximations to this procedure are also presented. The emergency core cooling system of a boiling water reactor is analyzed to demonstrate this methodology. The results of this analysis show that these procedures have practical application and the approximations provide a close estimate to the exact expected number of failures.

TABLE OF CONTENTS

CHAPTER		PAGE
1.	INTRODUCTION	1
	1.1 Motivation	1
	1.2 Objective	3
	1.3 Organization of Text	4
2.	MATHEMATICAL FORMULATION OF THE EXPECTED NUMBER OF FAILURES OF A PHASED MISSION	6
	2.1 Basic Reliability Concepts	6
	2.2 Assumptions	10
	2.3 Notation	10
	2.4 Calculation of the Phased Mission Expected Number of Failures	11
	2.5 Characteristics of the Boundary Jump	20
3.	APPROXIMATIONS TO THE PHASED MISSION EXPECTED NUMBER OF FAILURES	26
	3.1 Approximation I: Using Bracketing	26
	3.2 Approximation II: Using Conditional Basic Events	27
	3.3 Approximation III: Using Unconditional Basic Events	30
	3.4 Sample Problem	31
	3.5 Assessment of the Approximations	34
4.	ANALYSIS OF A BOILING WATER REACTOR EMERGENCY CORE COOLING SYSTEM	35
	4.1 Mission Description	35
	4.2 Analysis Procedure	38
	4.3 Results and Conclusions	38
5.	CONCLUSIONS AND RECOMMENDATIONS	47
	5.1 Summary and Conclusions	47
	5.2 Recommendations for Future Work	48
LIST OF REFERENCES		50
APPENDICES		53
I.	INPUT DESCRIPTION FOR ENFPHORM	54
II.	RATE OF FAILURE METHODOLOGY	62
III.	INPUT DATA FOR THE BOILING WATER REACTOR EMERGENCY CORE COOLING SYSTEM ANALYSIS	74
VITA		80

LIST OF FIGURES

FIGURE		PAGE
2-1	Fault Tree for Phase 1 of Example Problem 2.1	7
2-2	Fault Tree for Phase 2 of Example Problem 2.1	7
2-3	Fault Tree for Phase 1 of Example Problem 2.2	17
2-4	Fault Tree for Phase 2 of Example Problem 2.2	18
2-5	Fault Tree for Phase 2 of Example Problem 2.3	22
3-1	Fault Tree for Phase 1 of the Sample Problem	32
3-2	Fault Tree for Phase 2 of the Sample Problem	32
4-1	BWR Emergency Core Cooling System	37
4-2	Nonrepairable Case TOP Event Expected Number of Failures Versus Time Using the Exact Methodology ($P(\bar{S}_- \cap S_+)$)	39
4-3	Approximation II: Nonrepairable Case TOP Event Expected Number of Failures Versus Time	40
4-4	Approximation III: Nonrepairable Case TOP Event Expected Number of Failures Versus Time	41
4-5	Repairable Case TOP Event Expected Number of Failures Versus Time Using the Exact Methodology ($P(\bar{S}_- \cap S_+)$)	42
4-6	Approximation II: Repairable Case TOP Event Expected Number of Failures Versus Time	43
4-7	Approximation III: Repairable Case TOP Event Expected Number of Failures Versus Time	44
A-II-1	Example Problem II.1 Fault Tree	71
A-III-1	BWR ECCS Phase 1 Logic Model	77
A-III-2	BWR ECCS Phase 2 Logic Model	78
A-III-3	BWR ECCS Phase 3 Logic Model	79

CHAPTER 1

INTRODUCTION

1.1 Motivation

The study of the behavior of complex nuclear systems has become increasingly important in recent years. This is particularly true with respect to engineered safety systems within the nuclear power industry. Reliability engineering methods provide the technology to make such a study. Results of a reliability analysis provide an objective basis for analyzing system design, performing trade-off studies, and justifying system design changes or additions.

One of the results often obtained in the quantitative reliability analysis of a system is the expected number of failures of the TOP event (that is, the system failure of interest). The expected number of failures of a system is statistically the expected number of times a system will fail during a given time interval. The expected number of failures is used in calculating the risk (expected number of failures; consequence/failure) associated with a particular accident. The expected number of failures can also be used as input to economic studies and to aid with decisions concerning maintenance scheduling and system planning.[1]

A phased mission analysis is a special type of reliability analysis. A phased mission is a task, to be performed by a system, during the execution of which the system is altered such that the failure logic model changes at specified times.[2] A fault tree is an example of a failure logic model and is a graphical representation of the Boolean logic associated with the development of a TOP event to system

component failures, called basic events.[3] A system component, in this case, is the smallest unit of the system as developed in the system logic model. A component may be a single item, such as a relay, a complex entity, such as a flux monitoring system, or some specific operator action.

The need for phased mission techniques to analyze complex changing systems is not new. During the 1960's and early 1970's a great deal of work was done in developing methods to calculate the reliability of a phased mission.[4,5,6] In 1974, J. D. Esary and H. Ziehms developed a transformation procedure that enables one to determine the exact unreliability of a phased mission with nonrepairable statistically independent basic events.[7] Several approximations to the phased mission unreliability have also been presented by Esary, Ziehms, and Proschan.[8,9]

Since 1974, little work has been published on phased mission analysis techniques. In 1977, G. R. Burdick et al., reviewed current phased mission analysis techniques and expressed a need for new analysis techniques in this field, such as methodology to calculate the expected number of failures of a phased mission.[2] This need was also expressed in a study done by The University of Tennessee on the reliability of a hypothetical power grid.[1]

Renewed interest in the reliability analysis of phased missions is now being shown because of the large number of systems that undergo phased missions. Conventional reliability analysis techniques are not generally applicable to phased mission problems. For example, it is not correct to add the expected number of failures of each phase of a mission. Doing so could give results that underestimate the expected number of failures of the mission and lead to erroneous conclusions

about a system.

1.2 Objective

In this thesis, the phased mission problem considered refers to the following situation:

> A system has failure logic consisting of several independent basic events, each of which can be in one of two states, functioning or failed. The system performs a mission which can be divided into consecutive time periods or phases. During each phase it has to accomplish a specified task such that the failure logic model describing the system changes from phase to phase. At any point in time the TOP event for the failure logic of the system either exists or it does not exist.

The phased mission problem to be solved is to:

> Calculate the expected number of failures of the TOP event as a function of time throughout the phased mission, given the reliability characteristics of the basic events, the failure logic models of the system for each phase of the mission, and the duration of the phases.

Specifically, the objective of this thesis is to present an analytical solution to the expected number of failures for a system during a phased mission. Some approximations are also developed that

overpredict this expected number of failures (usually only slightly). To demonstrate the methodology developed, the emergency core cooling system of a boiling water reactor is analyzed.

1.3 Organization of Text

A procedure to determine the expected number of failures of a system experiencing a phased mission is developed in Chapter 2. Several sample problems are also presented to illustrate this methodology and some of the characteristics of the expected number of failures of a phased mission.

Chapter 3 describes some approximations to the expected number of failures of a phased mission. All but one of these approximations are proven to overpredict the phased mission expected number of failures. A sample problem demonstrating the procedure involved in applying one of these approximations is also presented.

The methodology developed in this thesis is used to determine the expected number of failures of an emergency core cooling system of a boiling water reactor. This example problem has previously been used in the IEEE Transactions on Reliability to demonstrate techniques for determining the unreliability of a phased mission.[3] A description of this problem and the pertinent results of this analysis are presented in Chapter 4.

Chapter 5 presents general conclusions and recommendations concerning the phased mission analysis techniques developed in this thesis.

Appendix I contains a description of the input data required to run the ENFPHORM computer program. ENFPHORM uses the conditional basic event approximation described in Chapter 3 to estimate the expected number of failures of a phased mission.

Appendix II contains a description of the methodology used to determine the rate of failure and expected number of failures of a TOP event within a single phase.

Appendix III contains a list of the basic events used in the BWR ECCS analysis, their failure rates and mean down times, and a list of the minimal cut sets and minimal path sets for each phase of the problem.

CHAPTER 2

MATHEMATICAL FORMULATION OF THE EXPECTED NUMBER OF FAILURES OF A PHASED MISSION

The expected number of failures of a single phase mission is determined by integrating over the time interval of interest the rate of failure of the TOP event. Methodology for this calculation is presented in Appendix II. With a phased mission, however, determination of the expected number of failures is different. Since the basic events used in the failure logic models for the different phases of the mission may be common to several of these models, the TOP event can occur immediately upon entering a new phase. To illustrate this concept, the following example problem is given.

Example 2.1. The fault tree for a specific system malfunction has two statistically independent basic events, X_1 and X_2. The system undergoes a two-phased mission. The fault trees for the two phases are shown in Figures 2-1 and 2-2. At the end of phase 1 the TOP event is in the unfailed state if either X_1 or X_2 is in the unfailed state. If either X_1 or X_2 is failed at the end of phase 1, the TOP event will occur immediately upon entering phase 2. This failure is not accounted for if we simply add the expected number of failures of the TOP event for each phase to get the expected number of failures of the TOP event over the mission. Accounting for this possible phase boundary failure is a major subject of this chapter.

2.1 Basic Reliability Concepts

Before venturing into the evaluation of the expected number of failures of a phased mission problem, some basic definitions and

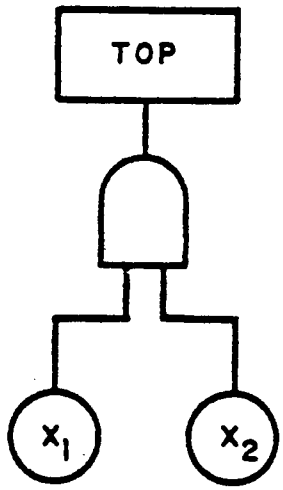


Figure 2-1: Fault Tree for Phase 1 of Example Problem 2.1.

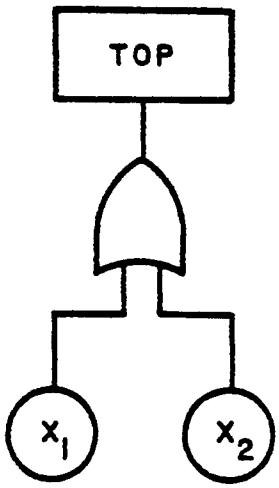


Figure 2.2: Fault Tree for Phase 2 of Example Problem 2.1.

general probability relationships must be established. From basic probability theory,

$$P(A_1 \cap A_2) = P(A_1)P(A_2|A_1) \tag{2.1.1}$$

and

$$P(A_1 \cup A_2 \ldots \cup A_N) = \underbrace{\sum_{i=1}^{N} P(A_i)}_{1} - \underbrace{\sum_{i=2}^{N} \sum_{j=1}^{i-1} P(A_i \cap A_j)}_{2} + \underbrace{\sum_{i=3}^{N} \sum_{j=2}^{i-1} \sum_{k=1}^{j-1} P(A_i \cap A_j \cap A_k)}_{3} + \ldots, \tag{2.1.2}$$

where A = an event,

$\cap$ = the intersection of events,

$\cup$ = the union of events.[10]

In equation (2.1.2), the probability of the union of events involves the probabilities of all the various combinations of the intersections of the events. If these intersections are taken into account such that intersections of an increasing number of events are considered (that is, term 1 alone, term 1 - term 2, term 1 - term 2 + term 3, etc.), then successive upper and lower bounds are obtained for $P(A_1 \cup A_2 \ldots \cup A_N)$ until, finally, its exact value is reached.

Some other relationships that will be used are

$$A \cap \bar{A} = \phi, \tag{2.1.3}$$

$$A \cap A = A, \tag{2.1.4}$$

$$A \cup (B \cup C) = (A \cup B) \cup C, \tag{2.1.5}$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \tag{2.1.6}$$

and

$$A \cap (B \cup C) = (A \cap B) + (A \cap C) - (A \cap B \cap C). \tag{2.1.7}$$

Equations (2.1.4) through (2.1.7) are the adsorption, associative, and

distributive properties from Boolean algebra. Equation (2.1.3) states that the intersection of an event and its complement is the empty set.

The expected number of failures is statistically the expected number of times a failure will occur in some specified time interval. By definition, the expected value of a random variable is the sum (or integral) of the product of all possible values of the variable and the probability they take on that value.

A cut set is a collection of basic events such that if all these basic events exist, then the TOP event is guaranteed to exist. If when any basic event is removed from this collection it is no longer a cut set, the cut set is minimal. For example, if the basic events X_1 and X_2 form cut set K_1, then $K_1 = (X_1 \cap X_2)$ would guarantee the existence of the TOP event. If X_1 alone will not cause the TOP event and neither will X_2, then X_1, X_2 is a minimal cut set. Several computer programs, such as PREP and MOCUS, exist that will determine minimal cut sets for a fault tree.[11,12]

A path set, on the other hand, is a collection of basic events such that if none of these basic events exist then the TOP event is guaranteed not to exist. If when any basic event is removed from this collection it is no longer a path set, the path set is minimal. For example, if basic events $\bar{X}_2$ and $\bar{X}_3$ form path set R_2, then $R_2 = (\bar{X}_2 \cap \bar{X}_3)$ would guarantee the nonexistence of the TOP event. If $\bar{X}_2$ alone or $\bar{X}_3$ alone do not guarantee the nonexistence of the TOP event, then $\bar{X}_2, \bar{X}_3$ is a minimal path set. The computer program MOCUS is also capable of finding the minimal path sets for a fault tree.

2.2 Assumptions

The methodology in this thesis to determine the expected number of failures of a phased mission problem is developed under the following assumptions:

1. The logic model is coherent.[13]
2. The basic events are statistically independent (s-independent) in both failure and repair.
3. The failure and repair distribution of the basic events are known.
4. The transition time between any two consecutive phases is instantaneous.

Assumptions 1 through 3 are standard assumptions for the quantitative time-dependent evaluation of fault trees. Assumption 4 restricts to one the number of possible system failures during a transition from one phase to the next one. It does not, however, preclude imposing failure and repair conditions on the system components at the phase boundary.

2.3 Notation

The following notation will be used to describe the expected number of failures of a phased mission.

$\bar{X}_i(t)$ = event basic event X_i does not exist at time t,

$X_i(t)$ = event basic event X_i exists at time t,

$R_i(t)$ = event minimal path set R_i exists at time t,

$K_i(t)$ = event minimal cut set K_i exists at time t,

$\bar{S}(t)$ = event the TOP event does not exist at time t,

$S(t)$ = event the TOP event exists at time t,

$W_T(t)$ = the rate of failure of the TOP event at time t,

and $ENF(t_1,t_2)$ = the expected number of failures of the TOP event over the time interval t_1 to t_2.

2.4 Calculation of the Phased Mission Expected Number of Failures

For a single phase mission, the expected number of failures of the TOP event over the time interval t_o to t is given by

$$ENF(t_o,t) = \int_{t_o}^{t} W_T(t)dt. \qquad (2.4.1)$$

For a phased mission, the expression for the rate of failure of the TOP event, $W_T(t)$ (see Appendix II), will change if the failure logic model describing the system changes within the time interval t_o to t. If the failure logic model changes N times within the time interval (that is, there are N phases in the mission), then equation (2.4.1) can be rewritten as

$$ENF(t_o,t_N) \geq \sum_{i=1}^{N} \int_{t_{i-1}}^{t_i} W_T(t)dt + \text{other terms}, \qquad (2.4.2)$$

where t_{i-1} = time phase i begins,

t_i = time phase i ends,

and N = number of phases.

Equation (2.4.2) now accounts for the changing logic models encountered in phased mission problems and the "other terms" account for the TOP event occurring as a phase boundary is crossed. To evaluate these other terms, the definition of expected value is used. Let Δt be an arbitrarily small length of time spanning across the "ith" phase boundary. The expected number of failures in this Δt time interval is

$$ENF_i = 0P[\bar{S}(t_i - \tfrac{\Delta t}{2}) \cap S(t_i + \tfrac{\Delta t}{2})] + 1P[\bar{S}(t_i - \tfrac{\Delta t}{2}) \cap S(t_i + \tfrac{\Delta t}{2})] + \text{higher order terms,} \quad (2.4.3)$$

where the higher order terms account for the system failing more than one time during the Δt time interval. Since Δt spans a phase boundary, the failure logic models used to determine $\bar{S}(t_i - \frac{\Delta t}{2})$ and $S(t_i + \frac{\Delta t}{2})$ are different. Taking the limit of equation (2.4.3) as Δt approaches zero so that

$$\lim_{\Delta t \to 0} t_i - \frac{\Delta t}{2} = t_{i-} \quad (2.4.4)$$

and

$$\lim_{\Delta t \to 0} t_i + \frac{\Delta t}{2} = t_{i+}, \quad (2.4.5)$$

equation (2.4.3) now becomes

$$ENF_i = 0P[\bar{S}(t_{i-}) \cap S(t_{i+})] + 1P[\bar{S}(t_{i-}) \cap S(t_{i+})]. \quad (2.4.6)$$

Since the transition between phase boundaries is now considered instantaneous, it is impossible for the system to fail more than once upon crossing into a new phase. Therefore, the higher order terms in this case are identically zero.

Using equation (2.4.6) to account for the possibility of the TOP event occurring as a phase boundary is crossed, the expected number of failures of the TOP event for a phased mission can now be expressed as

$$ENF(t_o,t_N) = \sum_{i=1}^{N} \int_{t_{i-1}}^{t_i} W_T(t)dt + \sum_{i=1}^{N-1} P[\bar{S}(t_{i-})\cap S(t_{i+})], \qquad (2.4.7.)$$

where again t_{i-1} = time phase i begins,

t_i = time phase i ends,

$\bar{S}(t_{i-})$ = event the TOP event does not exist at the end of phase i,

$S(t_{i+})$ = event the TOP event does exist at the beginning of phase i+1,

and N = number of phases.

The first term in the right hand side of equation (2.4.7) is the sum of the expected number of failures during each phase of the phased mission. The rate of failure of the TOP in this integral term is given by

$$W_T(t)dt = P(\bigcup_{i=1}^{M} C_i) - P[B\cap(\bigcup_{i=1}^{M} C_i)], \qquad (2.4.8)$$

where C_i = the event the ith minimal cut set fails in time t to t + dt,

B = the event one or more of the minimal cut sets is failed at time t,

and M = the number of minimal cut sets for the particular phase in question.

Equation (2.4.8) is readily understood if we consider the individual terms on the right hand side. The first contribution to $W_T(t)dt$, $P(\bigcup_{i=1}^{M} C_i)$, is the contribution of one or more of the minimal cut sets failing in the interval t to t + dt and causing the TOP event to occur. The second term, $P(B \cap (\bigcup_{i=1}^{M} C_i))$, accounts for those cases in which one or more minimal cut sets fail in this interval while other minimal cut sets are already failed. A more detailed explanation of this quantity and how it is serived is given in Appendix II.

The second right hand side term of equation (2.4.7) is the sum of the expected number of failures at the phase boundary due to the logic model changing. Calculation of these quantities requires using the minimal path sets of the failure logic model of one phase and the minimal cut sets of the failure logic model of the next consecutive phase. Using Boolean algebra, an expression for the TOP event not existing at the end of one phase and existing at the beginning of the next can be written in terms of the basic events using these minimal cut sets and path sets.

The procedure for calculating this "boundary jump" in the expected number of failures is as follows. Consider a phased mission in which one of the phase boundaries occurs at time t_i. The minimal path sets for the TOP event in phase i are $(R_1, R_2, \ldots, R_P)$. With these minimal path sets the TOP event not existing at the end of phase i (that is, at time

t_{i-}) can be expressed as

$$\bar{S}(t_{i-}) = R_1(t_{i-}) \cup R_2(t_{i-}) \cup \ldots \cup R_p(t_{i-}). \tag{2.4.9}$$

The TOP event existing at the start of phase i+1 can be expressed in terms of its minimal cut sets $(K_1, K_2, \ldots, K_m)$ as

$$S(t_{i+}) = K_1(t_{i+}) \cup K(t_{i+}) \cup \ldots \cup K_m(t_{i+}). \tag{2.4.10}$$

Equations (2.4.9) and (2.4.10) are now used to express the TOP event not existing at the end of phase i and existing at the beginning of phase i+1 as

$$\bar{S}(t_{i-}) \cap S(t_{i+}) = [R_1(t_{i-}) \cup R_2(t_{i-}) \cup \ldots \cup R_p(t_{i-})] \cap [K_1(t_{i+}) \cup K_2(t_{i+}) \cup \ldots \cup K_m(t_{i+})]. \tag{2.4.11}$$

Dropping the time arguments from the variables and using equations (2.1.6) and (2.1.7), this expression can be expanded to

$$\bar{S}_- \cap S_+ = (R_{1-} \cap K_{1+}) \cup \ldots \cup (R_{1-} \cap K_{m+}) \cup (R_{2-} \cap K_{1+}) \cup (R_{2-} \cap K_{2+}) \cup \ldots \cup (R_{p-} \cap K_{m+}). \tag{2.4.12}$$

where the "+" and "-" signs indicate from which side of the phase boundary the path sets or cut sets were obtained.

Note that if any pair of minimal path sets and cut sets (that is, $R_- \cap K_+$) contain a common basic event, then the coexistence of that pair is not possible. For example, if minimal path set R_1 contained basic events $\bar{X}_1$ and $\bar{X}_3$ and minimal cut set K_1 contained basic events X_1 and X_2, then the first term on the right hand side of equation (2.4.12) would be

$$R_{1-} \cap K_{1+} = \bar{X}_{1-} \cap \bar{X}_{3-} \cap X_{1+} \cap X_{2+} \tag{2.4.13}$$

$$= \phi .$$

The event $(R_{1-} \cap K_{1+})$ is the empty set because $\bar{X}_{1-}$ and X_{1+} are mutually exclusive events. That is, basic event X_1 cannot exist and not exist at one time. If basic event X_1 does not exist at the phase boundary, then all the terms in equation (2.4.12) containing the event X_1 will be the empty set. The reason for this is that guaranteeing the working state of basic event X_1 at the start of the next phase guarantees the nonexistence of the minimal cut sets containing this basic event. Thus, the intersection of a path set at the end of one phase with a nonexistent cut set at the beginning of the next phase is the empty set.

Finally, calculating the probability of the event described by equation (2.4.12) gives the expected number of failures of the TOP event as the phase boundary is crossed. Therefore, the "boundary jump" in the expected number of failures is

$$ENF_i = P(\bar{S}_- \cap S_+) = P\ (R_{1-} \cap K_{1+}) \cup (R_{1-} \cap K_{2+}) \cup \ldots \cup (R_{p-} \cap K_{1+}) \cup$$

$$(R_{p-} \cap K_{2+}) \cup \ldots \cup (R_{p-} \cap K_{m+}) \ . \tag{2.4.14}$$

The following example illustrates the procedure for calculating the expected number of failures across a phase boundary.

Example 2.2. A system composed of four s-independent basic events is designed for a two phase mission. Fault trees describing the failure logic for the TOP event for each phase are shown in Figures 2-3 and 2-4. The minimal path sets for the TOP event in phase 1 are $(\bar{X}_1, \bar{X}_2)$ and

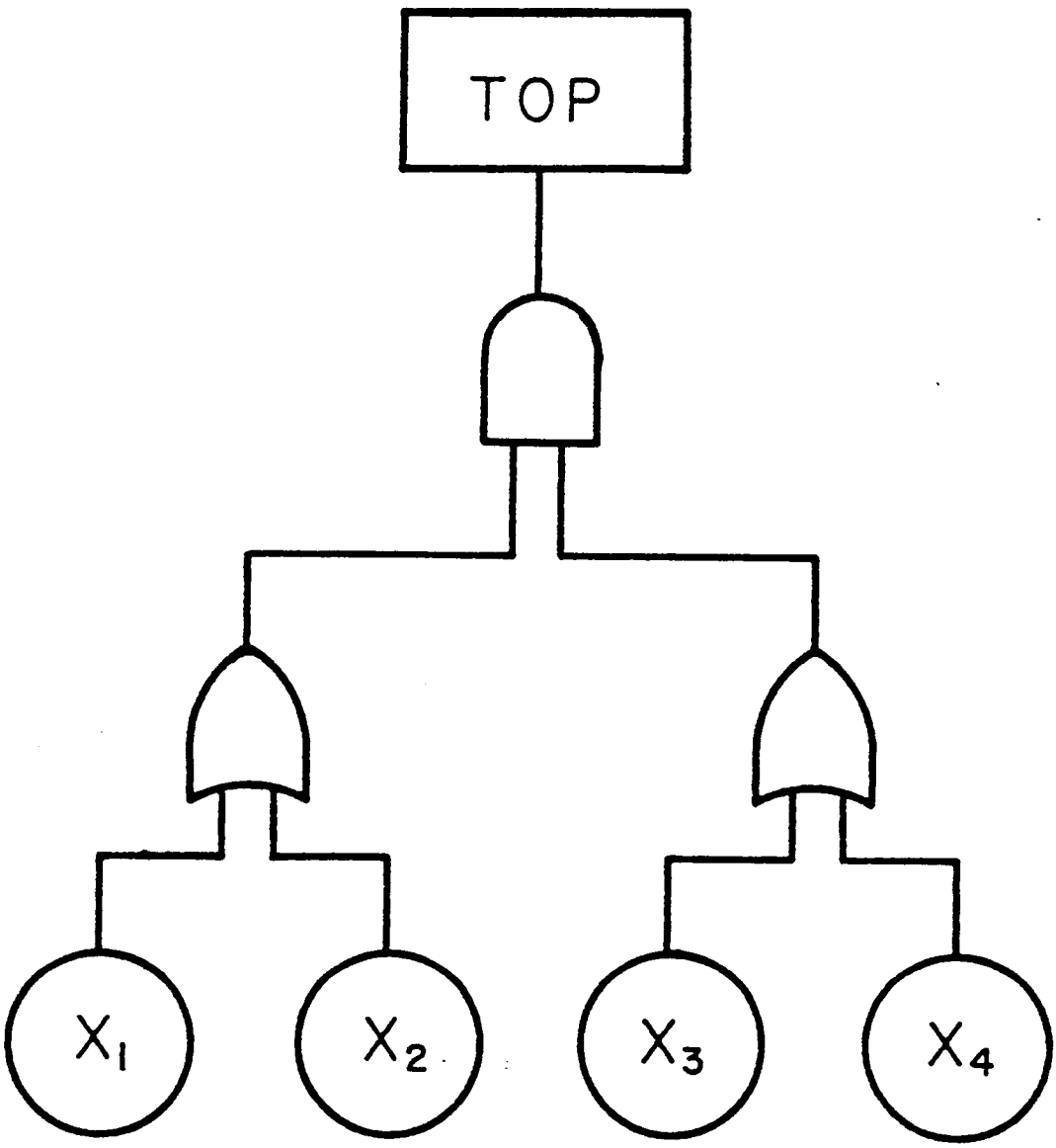


Figure 2-3: Fault Tree for Phase 1 of Example Problem 2.2.

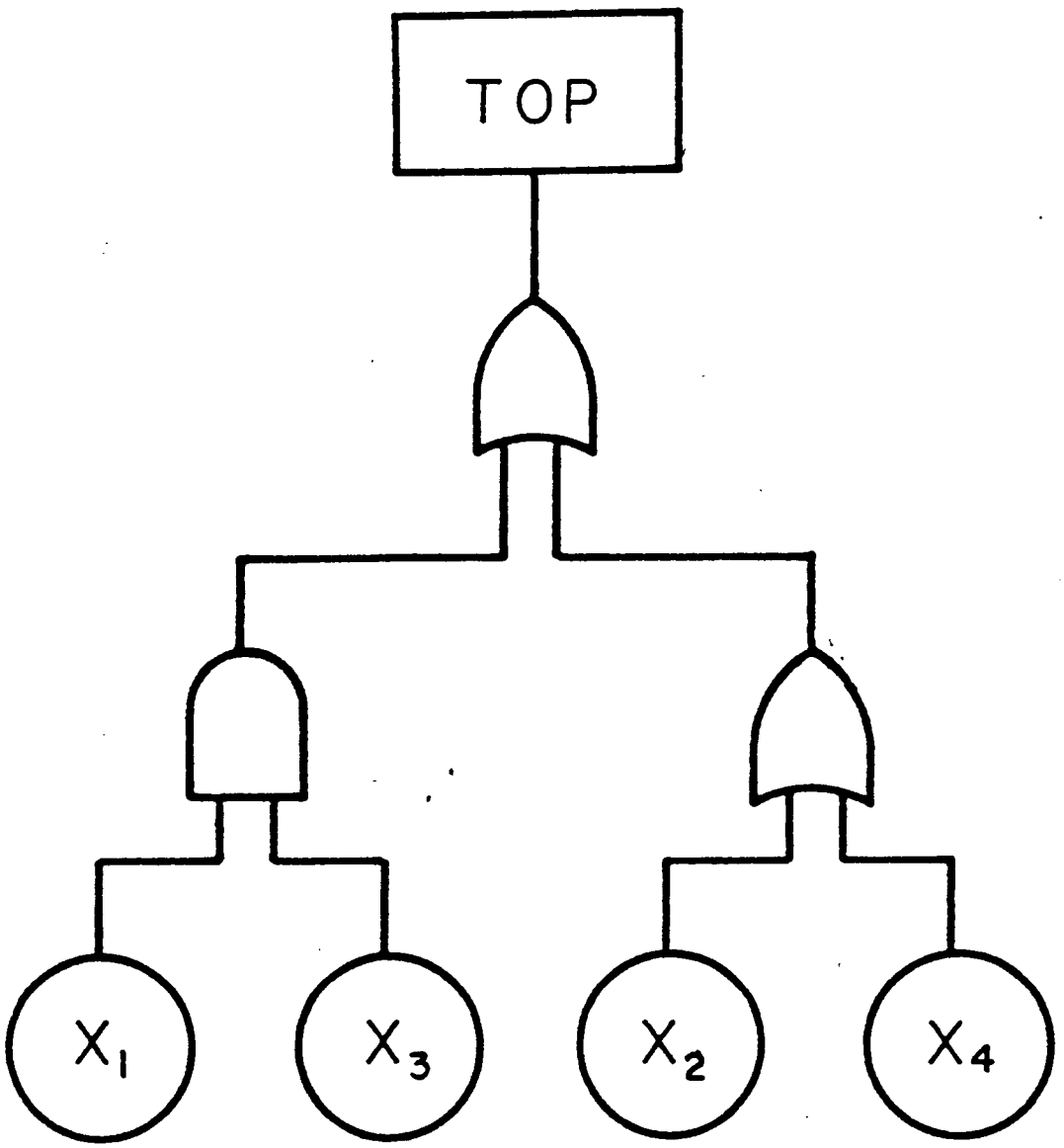


Figure 2-4: Fault Tree for Phase 2 of Example Problem 2.2.

$(\bar{X}_3,\bar{X}_4)$. By definition of minimal path set then, the TOP event not existing at the end of phase 1 can be expressed as

$$\bar{S}(t_{1-}) = [\bar{X}_1(t_{1-})\cap\bar{X}_2(t_{1-})]\cup[\bar{X}_3(t_{1-})\cap\bar{X}_4(t_{1-})]. \qquad (2.4.15)$$

In a similar manner, the minimal cut sets describe the failure modes of the TOP event. The minimal cut sets for the TOP event in phase 2 are (X_1,X_3), (X_2), and (X_4). The TOP event existing at the beginning of phase 2 can be expressed as

$$S(t_{1+}) = [X_1(t_{1+})\cap X_3(t_{1+})] \cup X_2(t_{1+}) \cup X_4(t_{1+}). \qquad (2.4.16)$$

Now, using equations (2.4.15) and (2.4.16), we can express the TOP event not existing at the end of phase 1 and existing at the beginning of phase 2 in terms of the basic events as

$$\bar{S}(t_{1-})\cap S(t_{1+}) = \{[\bar{X}_1(t_{1-})\cap\bar{X}_2(t_{1-})]\cup[\bar{X}_3(t_{1-})\cap\bar{X}_4(t_{1-})]\}\cap$$
$$\{[X_1(t_{1+})\cap X_3(t_{1+})] \cup X_2(t_{1+}) \cup X_4(t_{1+})\}. \qquad (2.4.17)$$

Applying equations (2.1.3) through (2.1.5) to this equation and dropping the time arguments of the variables, equation (2.4.17) becomes

$$\bar{S}_-\cap S_+ = (\bar{X}_{1-}\cap\bar{X}_{2-}\cap X_{1+}\cap X_{3+})\cup(\bar{X}_{1-}\cap\bar{X}_{2-}\cap X_{2+})\cup(\bar{X}_{1-}\cap\bar{X}_{2-}\cap X_{4+})$$
$$\cup(\bar{X}_{3-}\cap\bar{X}_{4-}\cap X_{1+}\cap X_{3+})\cup(\bar{X}_{3-}\cap\bar{X}_{4-}\cap X_{2+})$$
$$\cup(\bar{X}_{3-}\cap\bar{X}_{4-}\cap X_{4+}). \qquad (2.4.18)$$

Eliminating the terms that contain the intersection mutually exclusive events reduces equation (2.4.18) to

$$\bar{S}_{-} \cap S_{+} = (X_{1-} \cap X_{2-} \cap X_{4+}) \cup (X_{3-} \cap X_{4-} \cap X_{2+}). \qquad (2.4.19)$$

Thus, the expected number of failures resulting from the phase boundary where the failure logic model changes is

$$ENF_1 = P(\bar{S}_{-} \cap S_{+}) = P[(\bar{X}_{1-} \cap \bar{X}_{2-} \cap X_{4+}) \cup (\bar{X}_{3-} \cap \bar{X}_{4-} \cap X_{2+})] \; . \qquad (2.4.20)$$

Reducing equation (2.4.20) gives

$$ENF_1 = P(\bar{X}_{1-})P(\bar{X}_{2-})P(X_{4+}) + P(\bar{X}_{3-})P(\bar{X}_{4-})P(X_{2+}). \qquad (2.4.21)$$

Since the failure and repair distributions of the basic events are known (assumption 3), a numerical result to equation (2.4.21) can be obtained.

2.5 Characteristics of the Boundary Jump

The expected number of failures is an integral characteristic of a system; thus, it can never decrease. The size boundary jump in the expected number of failures is dependent on the minimal path sets and minimal cut sets for that particular phase boundary. In this section, characteristics of the phase "boundary jump" are examined. Understanding these characteristics is important to those involved in system design when a design objective is to reduce this jump.

2.5.1 System Redundancy

One of the simplest, although not often practical, ways to reduce the size of a boundary jump is to increase the redundancy in a system as it enters a new phase of the mission. By making the system more redundant in the next phase, the size of each minimal cut set (that is, the number of basic events in each set) is increased while the path sets of the

previous phase are unaffected. Thus, the expression for the phase jump in terms of the intersections of path sets and cut sets is not changed, but the existence probability at the phase boundary of some or all of the cut sets involved has now been decreased due to the redundant basic events. The following example illustrates this point.

Example 2.3. Again consider the problem described by Example 2.1 and Figure 2-1 (Pg. 7). The phase 1 failure logic model has path sets $R_1 = (\bar{X}_1)$ and $R_2 = (\bar{X}_2)$. The phase 2 minimal cut sets are $K_1 = (X_1)$ and $K_2 = (X_2)$. The expression for the phase 1 - phase 2 boundary jump is

$$P(\bar{S}_- \cap S_+) = P[(R_{1-} \cup R_{2-}) \cap (K_{1+} \cup K_{2+})]. \tag{2.5.1}$$

Expanding equation (2.5.1) and then reducing it to a form containing only basic events gives

$$\begin{aligned} P(\bar{S}_- \cap S_+) &= P[(R_{1-} \cap K_{1+}) \cup (R_{1-} \cap K_{2+}) \cup (R_{2-} \cap K_{1+}) \cup (R_{2-} \cap K_{2+})] \\ &= P\,(\bar{X}_{1-} \cap X_{2+}) \cup (\bar{X}_{2-} \cap X_{1+}) \\ &= P(\bar{X}_1)P(X_{2+}) + P(\bar{X}_{2-})P(X_{1+}). \end{aligned} \tag{2.5.2}$$

Now consider this same problem again. In this case, however, we will provide a backup to basic event X_1 in phase 2. That is, basic event X_1 will be replaced in phase 2 with basic events X_1 and X_1'. The failure logic model describing phase 2 is shown in Figure 2-5. The path sets for phase 1 of this problem are the same as before (that is, $R_1 = (\bar{X}_1)$ and $R_2 = (\bar{X}_2)$). The minimal cut sets for phase 2, however, are now $K_1 = (X_1, X_1')$ and $K_2 = (X_2)$. Using this information, the equation for the phase 1 - phase 2 boundary jump becomes

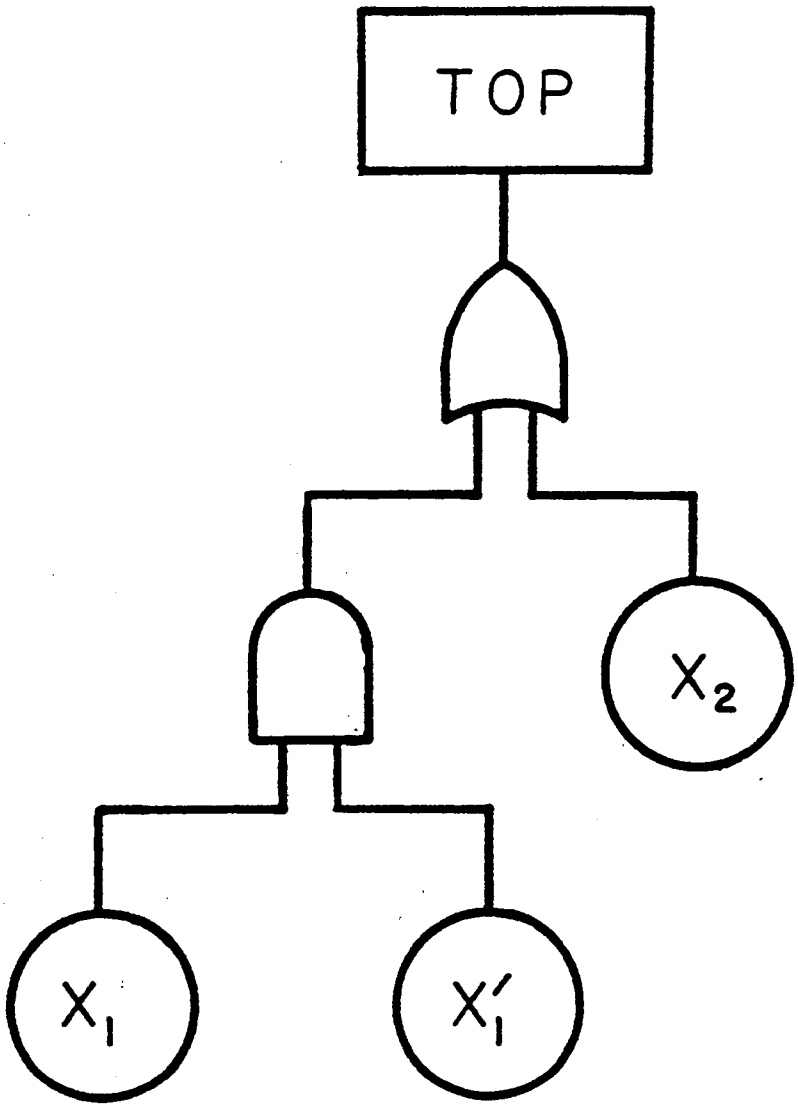


Figure 2-5: Fault Tree for Phase 2 of Example Problem 2.3 .

$$P(\bar{S}_{-} \cap S_{+}) = P[(R_{1-} \cap K_{1+}) \cup (R_{1-} \cap K_{2+}) \cup (R_{2-} \cap K_{1+}) \cup (R_{2-} \cap K_{2+})]$$

$$= [(\bar{X}_{1-} \cap X_{2+}) \cup (\bar{X}_{2-} \cap X_{1+} \cap X'_{1+})]$$

$$= P(\bar{X}_{1-})P(X_{2+}) + P(\bar{X}_{2-})P(X_{1+})P(X'_{1+}). \qquad (2.5.3)$$

Since the probability of an event existing (or not existing) is always less than or equal to one, the value of equation (2.5.3) is always less than or equal to the value of equation (2.5.2), the boundary jump of the less redundant system. If the redundancy of the system had been further increased by making basic event X_2 redundant in phase 2, the boundary jump would have decreased even further. In this case, the expression for the phase 1 - phase 2 jump would be

$$P(\bar{S}_{-} \cap S_{+}) = P[(\bar{X}_{1-} \cap X_{2+} \cap X'_{2+}) \cup (\bar{X}_{2-} \cap X_{1+} \cap X'_{1+})]$$

$$= P(\bar{X}_{1-})P(X_{2+})P(X'_{2+}) + P(\bar{X}_{2-})P(X_{1+})P(X'_{1+}). \qquad (2.5.4)$$

Thus, making one or more basic events more redundant (that is, providing more backups) as the system progresses through the mission will decrease the size of the boundary jump. Another possible method of reducing the boundary jump is by assuring the nonexistence of the basic events during the transition between phases.

2.5.2 Basic Event Testing and Repair

Although one of the assumptions used to develop this methodology is the instantaneous transition between phases, testing and the instantaneous repair of basic events at the phase boundaries is allowed. This permits one to reduce the boundary jump by repairing a few "key" basic events at

the phase boundary. These "key" basic events could be determined by one of two criteria.

One criteria for determining a "key" basic event is the magnitude of the path-cut intersection term (that is, $R_i \cap K_j$) in relation to the magnitude of the other intersection terms in the boundary jump expression (equation 2.4.13). If only a few intersection terms dominate the magnitude of the boundary jump, then these quantities could be eliminated from the boundary jump calculation by simply guaranteeing the nonexistence of the minimal cut sets in these terms. This can be accomplished by assuring one or more basic events common to these minimal cut sets does not exist. For example, suppose that in calculating a boundary jump it is determined that the terms $(R_1 \cap K_2)$, $(R_3 \cap K_7)$, and $(R_7 \cap K_4)$ are the main contributors to the jump. It is also found that minimal cut sets K_2, K_4, and K_7 have a common basic event X_3. If we assure basic event X_3 does not exist at the beginning of the next phase (through testing and repair at the boundary), then the TOP event cannot exist at the beginning of the next phase by cut sets K_2, K_4, and K_7. Thus, the three main contributors to the boundary jump have been eliminated by assuring only one basic event is working.

If no intersection term dominates the boundary jump or if a further reduction in the boundary jump is desired, a second criterion for choosing a "key" basic event can be used. A basic event may be considered "key" if it is common to several of the minimal cut sets in the intersection terms $(R_i \cap K_j)$ in the boundary jump equation. In this case, a large number of the intersection terms are again eliminated by guaranteeing the nonexistence of the minimal cut sets. For example, suppose there are sixteen minimal cut sets for phase i+1 that are used in determining the

phase i - phase 1+1 boundary jump. Assume also that half of these minimal cut sets have basic event X_i in common and the other half have basic event X_j in common. By assuring these two basic events do not exist at the beginning of phase i+1 (through testing and repair), the boundary jump will become zero because all the phase i+1 minimal cut sets are guaranteed to be nonexistent at this time. This criterion is easy to implement since the minimal path sets for a phase provide all the various collections of basic events which will "disable" the minimal cut sets of that phase.

Either or both of these criteria will be useful in reducing the expected number of failures boundary jump. If the boundary jumps are a major contributor to the total expected number of failures of the mission, then they should also prove useful in developing maintenance and repair schemes to be carried out during the phase transition period.

CHAPTER 3

APPROXIMATIONS TO THE PHASED MISSION EXPECTED NUMBER OF FAILURES

In calculating the phased mission expected number of failures, it is necessary to calculate the expected number of failures for each phase of the mission and for each phase boundary (equation 2.4.7). A method to determine exactly the expected number of failures of a single phase mission and approximations to this method were developed by W. E. Vesely (Appendix II).[14] These approximations can be used to overestimate (usually only slightly) the value of the first term in the right hand side of equation (2.4.7). This chapter will focus on approximations to the second right hand side term in equation (2.4.7), the boundary jump $P(\bar{S}_- \cap S_+)$. These approximations are useful because they often require less computational effort than the exact method and the results are usually accurate enough for the purpose at hand.

3.1 Approximation I: Using Bracketing

The expression for a phase boundary jump was the union of all the possible intersections between one minimal path set and one minimal cut set of the two consecutive phases in question. This was expressed algebraically as (equation 2.4.13)

$$P(\bar{S}_- \cap S_+) = P[(R_{1-} \cap K_{1+}) \cup (R_{1-} \cap K_{2+}) \cup \ldots \cup (R_{1-} \cap K_{m+}) \ldots$$

$$\ldots \cup (R_{p-} \cap K_{1+}) \cup (R_{p-} \cap K_{2+}) \cup \ldots \cup (R_{p-} \cap K_{m+})], \qquad (3.1.1)$$

where all the variables are the same as they were defined in section 2.3.

Representing each of the intersection terms in this equation with the variable A_i (for example, $A_1 = R_{1-} \cap K_{1+}$)), equation (3.1.1) can be rewritten as

$$P(\bar{S}_- \cap S_+) = P(A_1 \cup A_2 \ldots \cup A_{pxm}). \qquad (3.1.2.)$$

From basic probability theory (equation 2.1.2), equation (3.1.2) can be expanded to

$$\bar{P}(S_- \cap S_+) = \sum_{i=1}^{pxm} P(A_i) - \sum_{i=1}^{pxm} \sum_{j=1}^{i-1} P(A_i \cap A_j) +$$

$$\sum_{i=3}^{pxm} \sum_{j=2}^{i-1} \sum_{k=1}^{j-1} P(A_i \cap A_j \cap A_k) + \ldots +$$

$$(-1)^{pxm-1} P(A_1 \cap A_2 \cap A_3 \cap \ldots \cap A_{pxm}). \qquad (3.1.3)$$

Basic probability theory has shown that if these intersection terms in equation (3.1.3) (for example, $A_i \cap A_j \cap A_k$) are taken into account such that intersections of an increasing number of events are considered, then successive upper and lower bounds or brackets are obtained for $P(\bar{S}_- \cap S_+)$, the boundary jump. Thus, if the right hand side of equation (3.1.3) is truncated after an odd number of terms the boundary jump will be overestimated and if it is truncated after an even number of terms the boundary jump will be underestimated. For most problems, the first upper bracket (that is, truncating equation (3.1.3) after the first term) should give a reasonably accurate estimate of the boundary jump.

3.2 Approximation II: Using Conditional Basic Events

Another estimate of the boundary jump is the product of the probability the TOP event does not exist at the end of one phase and the

conditional probability it exists at the beginning of the next phase. The approximation in this procedure comes in estimating the conditional probability the TOP event exists at the beginning of the next phase.

The expression for the boundary jump can be written as

$$P(\bar{S}_- \cap S_+) = P(\bar{S}_-)P(S_+|\bar{S}_-). \tag{3.2.1}$$

The procedure to calculate the probability the TOP event does not exist (that is, $P(\bar{S}_-)$) is well-documented (Appendix II).[15] The probability the TOP event exists at the beginning of the next phase given it did not exist at the end of the previous phase (that is $P(S_+|\bar{S}_-)$) is more difficult to determine. A suitable approximation to this conditional probability is the probability the TOP event exists at the beginning of the next phase in which this failure probability is calculated using the failure probabilities of the basic events conditioned on the TOP event not existing immediately prior to crossing a phase boundary. This approximation, which the author believes always overestimates the conditional probability $P(S_+|\bar{S}_-)$, is expressed as

$$P(S_+^*) \geq P(S_+|\bar{S}_-), \tag{3.2.2}$$

where $P(S_+^*)$ = the probability the TOP event exists at the beginning of a phase. This probability is calculated using basic event failure probabilities that are conditioned on the TOP event not existing immediately prior to crossing the phase boundary.

The conditional basic event failure probabilities that are used

to get the probability the TOP event exists in equation (3.2.2) ($P(S_+^*)$) are given by

$$P(X_{i+}|\bar{S}_-) = \frac{P(\bar{S}_-|X_{i+})P(X_{i+})}{P(\bar{S}_-)}, \tag{3.2.3}$$

where all the variables are the same as those defined in section 2.3.

The implementation of equation (3.2.3) is straightforward. Using the methodology described in Appendix II, the probability the TOP event exists $P(S_-)$ at any point in time can be expressed as the product and sum of the failure probabilities of the basic events. The probability the TOP event does not exist is simply

$$P(\bar{S}_-) = 1 - P(S_-). \tag{3.2.4}$$

To determine the value of $P(\bar{S}_-|X_{i+})$, equation (3.2.4) is again used. In this case, however, the probability that the TOP event does not exist is calculated with the failure probability of basic event X_i set to 1.

Two observations can be made about the calculation of the conditional failure probability of a basic event. First, if the basic event is instantaneously repaired at the phase boundary, then the failure probability of this basic event used to calculate $P(S_+^*)$ is zero. Second, if the basic event is not instantaneously repaired at the phase boundary, then requiring X_i to be failed at the beginning of a phase (that is, requiring X_{i+} to exist) implies that it is also failed at the end of the prior phase (that is, X_{i-} exists). The following example illustrates this approximation procedure.

Example 3.1. Consider again the system described in Example 2.1 (Pg. 7). The expressions for the TOP event not existing at the end of phase 1 and existing at the beginning of phase 2 are

$$\bar{S}_- = \bar{X}_{1-} U \bar{X}_{2-} \tag{3.2.5}$$

and

$$S_+ = X_{1+} U X_{2+} . \tag{3.2.6}$$

In order to calculate $P(S_+^*)$, the conditional failure probabilities of the basic events must be determined. These are

$$P(X_{1+}|\bar{S}_-) = P(X_{1+}^*) = \frac{P(\bar{X}_{2-})P(X_{1+})}{P(\bar{X}_{1-} U \bar{X}_{2-})} \tag{3.2.7}$$

and

$$P(X_{2+}|\bar{S}_-) = P(X_{2+}^*) = \frac{P(\bar{X}_{1-})P(X_{2+})}{P(\bar{X}_{1-} U \bar{X}_{2-})} . \tag{3.2.8}$$

Using equations (3.2.5) through (3.2.8), the approximate boundary jump is

$$P(\bar{S}_-)P(S_+^*) = P(\bar{X}_{1-} U \bar{X}_{2-})P(X_{1+}^* U X_{2+}^*). \tag{3.2.9}$$

This approximation method is used by ENFPHORM to calculate the boundary jump. For most problems, this approximation method should overestimate the boundary jump. For the general case, however, it has not been shown to always overpredict the boundary jump.

3.3 Approximation III: Using Unconditional Basic Events

Perhaps the simplest approximation to the phase boundary jump is the product of the probability the TOP event does not exist at the end of one phase and the probability it exists at the beginning of the next. That is

$$P(\bar{S}_-)P(S_+) \geq P(\bar{S}_-)P(S_+|\bar{S}_-) . \tag{3.3.1}$$

To prove equation (3.3.1), recall that $P(\bar{S}_- \cap S_+)$ can be written as

$$P(\bar{S}_- \cap S_+) = P(\bar{S}_-)P(S_+|\bar{S}_-) . \tag{3.3.2}$$

However, since it is assumed that the logic models are coherent, then

$$P(S_+|\bar{S}_-) \leq P(S_+) . \tag{3.3.3}$$

Thus, equation (3.3.1) always overpredicts the phase boundary jump. This approximation is very similar to the one in section 3.2 except that now the probability that the TOP event exists at the beginning of a new phase is calculated using unconditional failure probabilities for the basic events.

3.4 Sample Problem

To illustrate these approximations, consider a system that undergoes a two-phased mission. Fault trees for a specific system malfunction for the two phases are shown in Figures 3-1 and 3-2. The basic event failure data is listed in Table 3-1.

The expected number of failures of the TOP event was calculated for a 200 hour mission (each phase is 100 hours) using the KITT1 computer program and the methods presented in the previous sections. The results are listed in Table 3-2.

All the approximations are adequate for calculating the total expected number of failures of the TOP event in this problem. Approximation I largely overestimated the boundary jump. This is because this problem is relatively small and has few terms in each of the brackets. Including only one more bracket gave the exact value of the boundary jump. In general, higher order bracketing terms contribute less to the

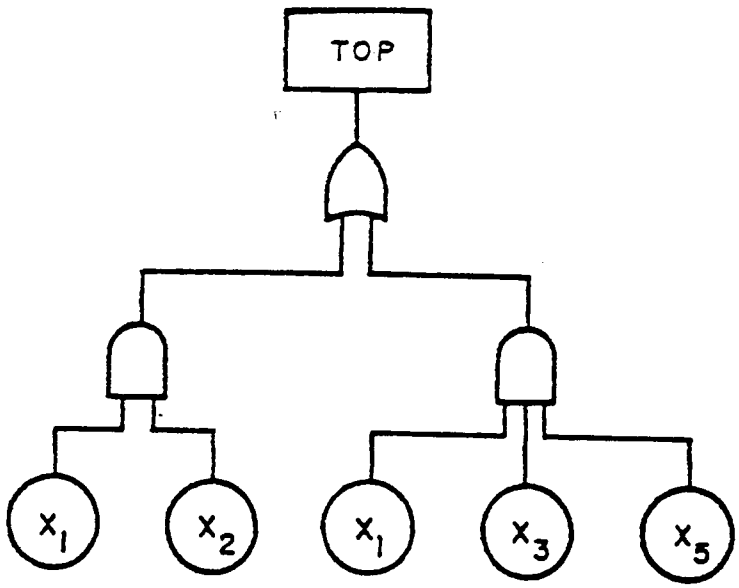


Figure 3-1: Fault Tree for Phase 1 of the Sample Problem.

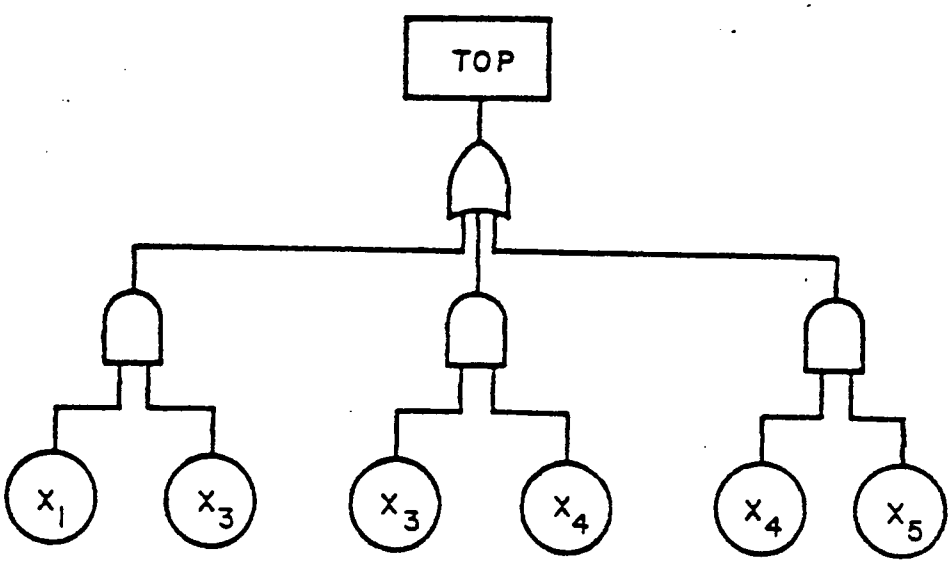


Figure 3-2: Fault Tree for Phase 2 of the Sample Problem.

TABLE 3-1

SAMPLE PROBLEM BASIC EVENT FAILURE DATA

Basic Event	Failure Rate ($hr.^{-1}$)	Mean Down Time (hr.)
1	10^{-3}	100
2	10^{-4}	100
3	10^{-4}	100
4	10^{-2}	10
5	10^{-2}	10

TABLE 3-2

SAMPLE PROBLEM EXPECTED NUMBER OF FAILURES

Method	Expected Number of Failures	Boundary Jump (%)
Exact	0.18471	0.90915
Approximation I (2 brackets)	0.18471	0.90915
Approximation I (1 bracket)	0.19294	1.73228
Approximation II	0.18474	0.91181
Approximation III	0.18475	0.91277

total boundary jump as the size of the problem (i.e., the length and number of minimal cut sets and minimal path sets) increases.

3.5 Assessment of the Approximations

The approximations presented in this chapter vary in degree of accuracy and the amount of computational effort required. The bracketing approximation provides the most accurate estimate of the boundary jump but also requires a large amount of computational effort. The conditional basic event failures approximation also requires a large amount of computational effort and in addition, does not necessarily overpredict the boundary jump.

The unconditional basic even failures approximation is the easiest to implement. This approximation requires the least computational effort of the three and should provide accurate results. Another advantage of this approximation is that currently available computer programs such as KITT1 and SUPERPOCUS already calculate the quantities used by this approximation.[16]

CHAPTER 4

ANALYSIS OF A BOILING WATER REACTOR EMERGENCY CORE COOLING SYSTEM

Phased mission techniques are required for proper analysis of problems when switching procedures are carried out, equipment is reassembled into new systems (by say, valve position changes), or the load demand changes at predetermined times. One system in the nuclear power industry that must be analyzed using phased mission techniques in the emergency core cooling system (ECCS) of a boiling water reactor (BWR) during a loss of coolant accident (LOCA).

This system has been previously analyzed by G. R. Burdick et al., to determine its mission unreliability, where mission unreliability is defined as the probability the system fails to function successfully in at least one phase.[7] In this analysis, however, the basic events were required to be nonrepairable and no attempt was made to calculate the expected number of failures.

In this chapter, the ECCS of a boiling water reactor is analyzed to demonatrate the methodology developed in this thesis. The system is analyzed for two cases: in case 1 the basic events are considered nonrepairable and in case 2 the basic events are considered as repairable. The fault trees for this mission, the minimal path sets and minimal cut sets of these fault trees, and the basic event failure rates and mean down times appear in Appendix III.

4.1 Mission Description

The mission of a BWR ECCS is to prevent excessive heating of the fuel rods within the reactor vessel as soon as possible after a large

loss of coolant accident and then to keep water circulating to and from the reactor vessel until the rods are cool. A schematic of this system is shown in Figure 4-1. Following a LOCA, three phases can be identified for the mission of the ECCS. These are initial core cooling, suppression pool cooling, and residual heat removal.

For phase 1 (initial core cooling) either the high pressure core spray (HPCS) alone, the automatic depressurization system (ADS) and one of the low pressure core injection systems (LPCI), or the automatic depressurization system and the low pressure core spray (LPCS) are needed. The purpose of phase 1 is to reflood the core and cool the fuel as soon as possible following a loss of coolant accident. During the 0.5 hour time period of phase 1, valve V-1 is open and valves V-2 and V-3 are closed (Figure 4-1).

During phase 2 (suppression pool cooling), the automatic depressurization system (ADS) is required to limit the pressure buildup in the reactor vessel. One of the heat exchangers (HX) and the corresponding low pressure coolant injection system (LPCI) are needed to cool the water in the suppression pool. Also needed is the low pressure core spray (LPCS), the high pressure core spray (HPCS), or a second low pressure coolant injection system (LPCI) to circulate the water from the suppression pool to the reactor vessel. In this phase, valve V-3 is open and the other valves are closed (Figure 4-1). The duration of this phase is 36 hours.

Throughout phase 3 (residual heat removal), the break is assumed to be repaired or isolated so that the system can operate normally. Residual heat removal requires the operation of one heat exchanger (HX) and one LPCI. Valve V-2 will be open and valves V-1 and V-3 will be closed during this phase (the complete flow loop is not shown in Figure 4-1). The

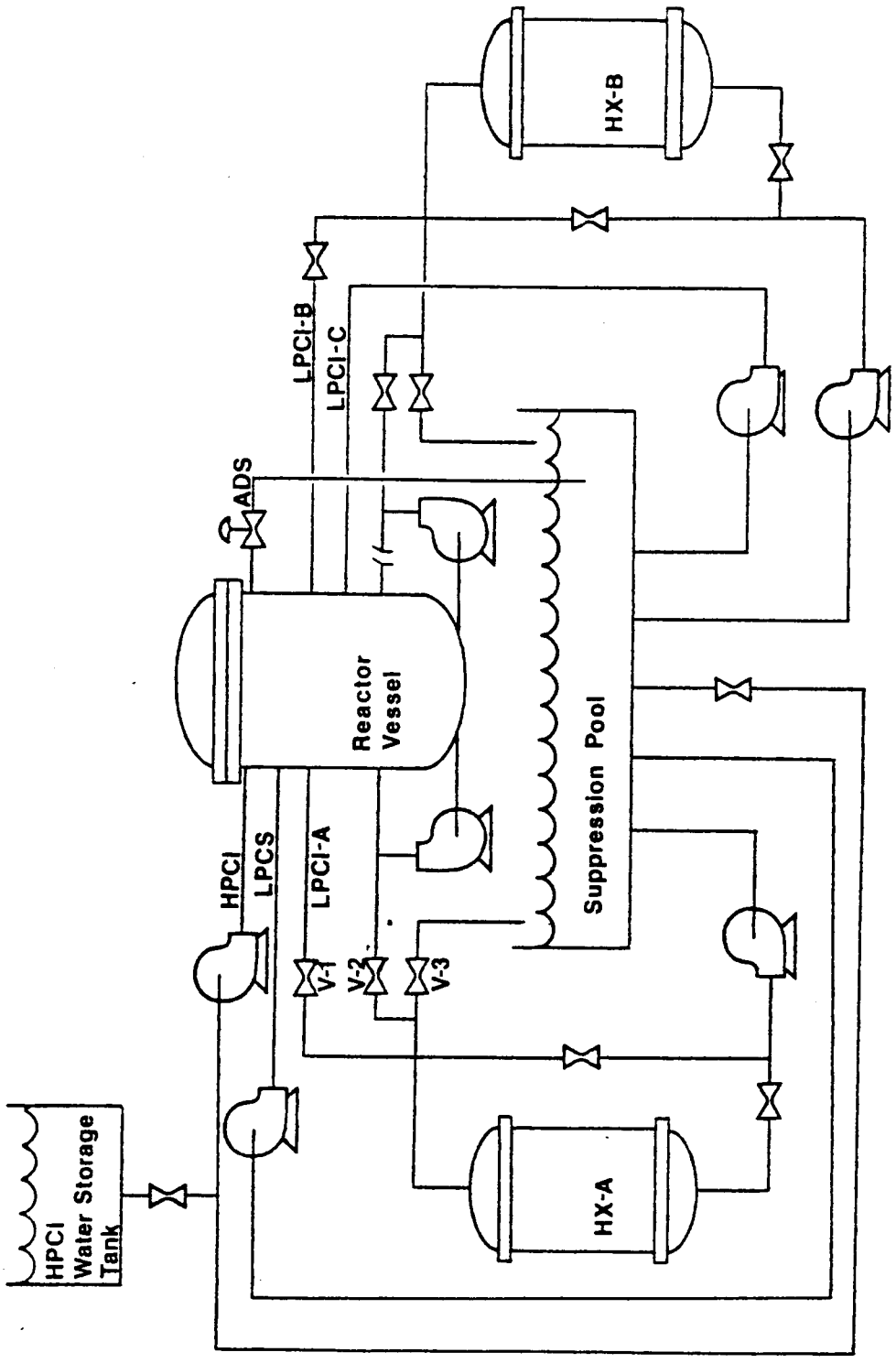


Figure 4-1: BWR Emergency Core Cooling System.

length of phase 3 is 84 hours.

The TOP event in this analysis is the "Emergency Core Cooling System Fails to Cool the Core Following a Loss of Coolant Accident." At the beginning of the mission, all the basic events are assumed to be in the unfailed state and no boundary conditions are imposed of the basic events at the phase boundaries.

4.2 Analysis Procedure

In this analysis, the basic events are assumed to have exponential failure and repair distributions. The assumptions listed in section 2.2 are also used. The KITT 1 and ENFPHORM computer programs were used to determine the expected number of failures of the TOP event. In the cases where the exact expected number of failures was determined, hand calculations were used to find the values of the "boundary jumps."

4.3 Results and Conclusions

The result of this analysis is the expected number of failures of the TOP event. The expected number of failures of the TOP event as a function of time for both the repairable and nonrepairable cases is shown in Figures 4-2 through 4-7. For the nonrepairable case, the exact methodology gives the expected number of failures of the TOP event at the end of the mission as 5.221×10^{-4}. The two approximations using conditioned and unconditioned basic event failures without bracketing gave the expected number of failures of the TOP event as 5.223×10^{-4} and 5.231×10^{-4}, respectively.

For the repairable case, the expected number of failures of the TOP event using the exact methodology is 5.17×10^{-4}. Both of the approximations methods without bracketing gave the expected number of failures in this case as 5.18×10^{-4}.

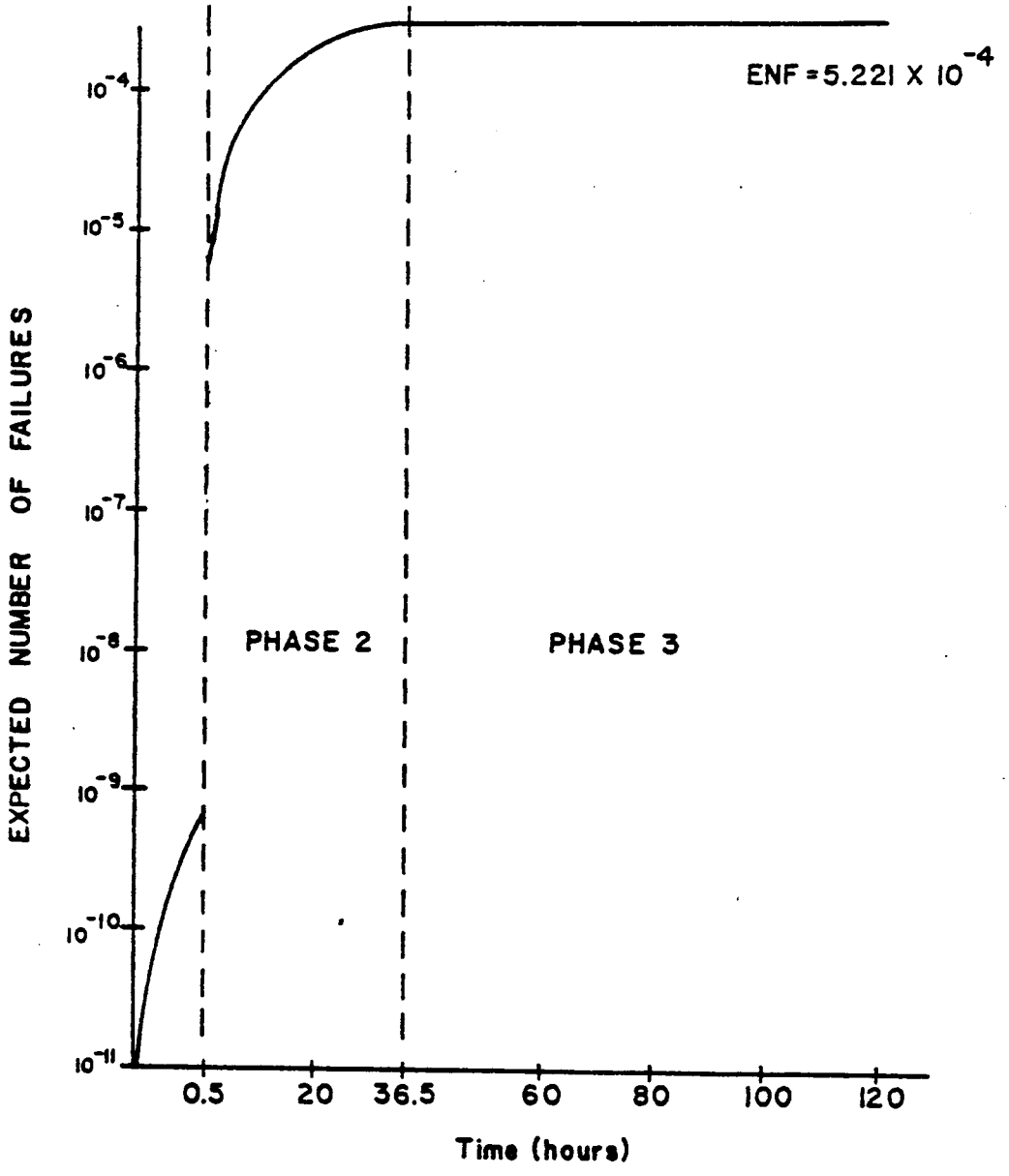


Figure 4-2: Nonrepairable Case TOP Event Expected Number of Failures Versus Time Using the Exact Methodology ($P(\bar{S}_- \cap S_+)$).

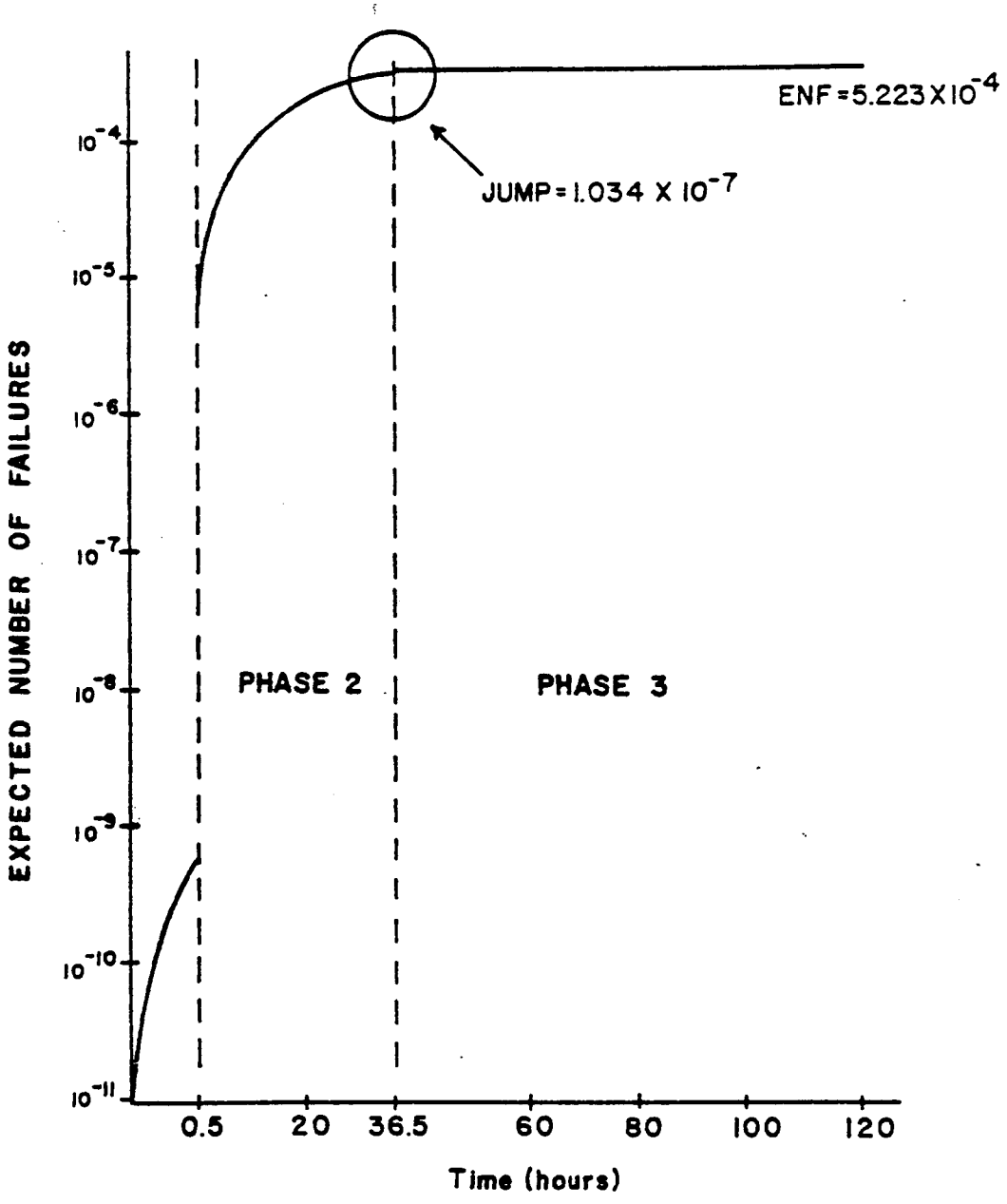


Figure 4-3: Approximation II: Nonrepairable Case TOP Event Expected Number of Failures Versus Time.

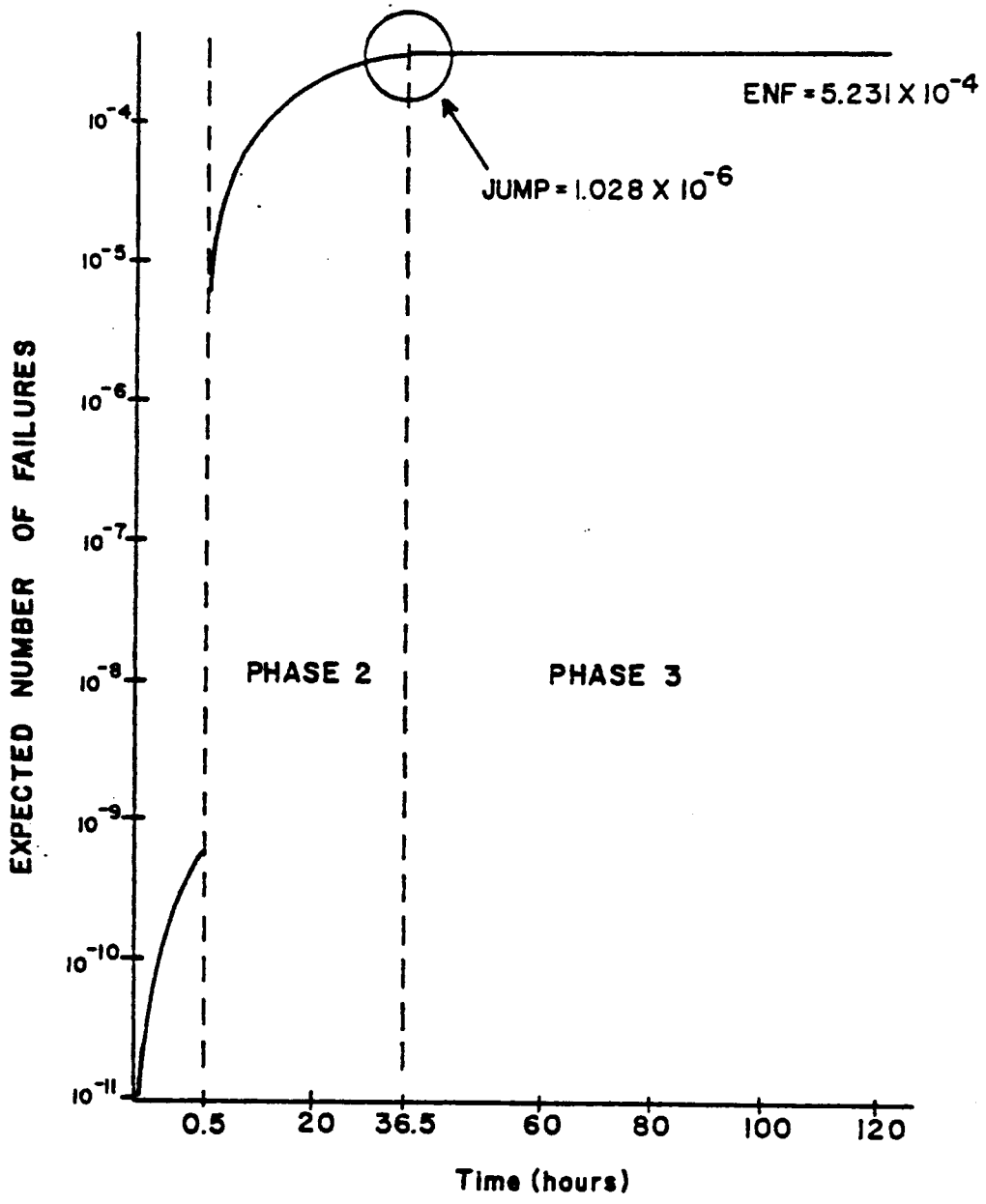


Figure 4-4: Approximation III: Nonrepairable Case TOP Event Expected Number of Failures Versus Time.

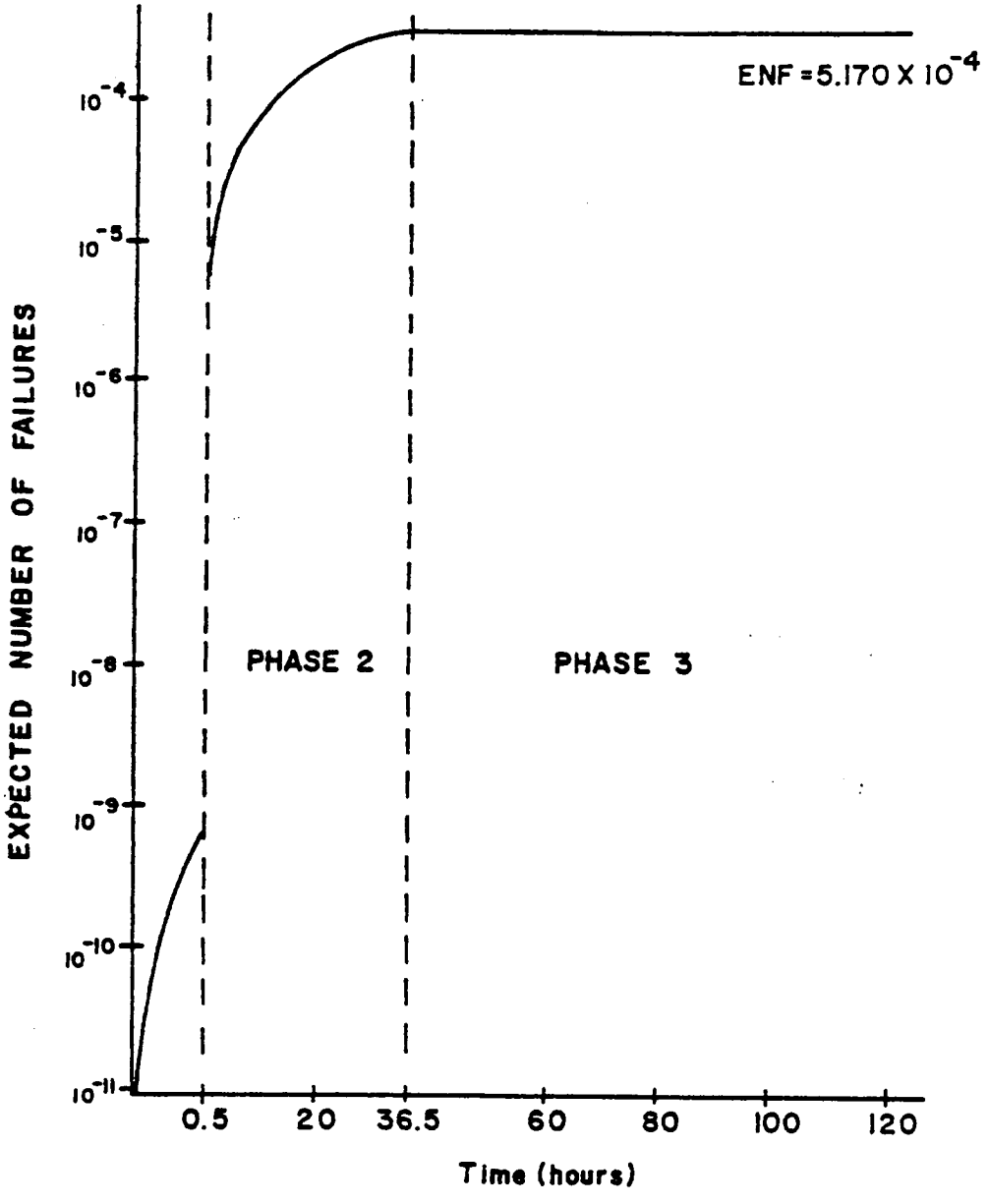


Figure 4-5: Repairable Case TOP Event Expected Number of Failures Versus Time Using the Exact Methodology ($P(\bar{S}_{-} \cap S_{+})$).

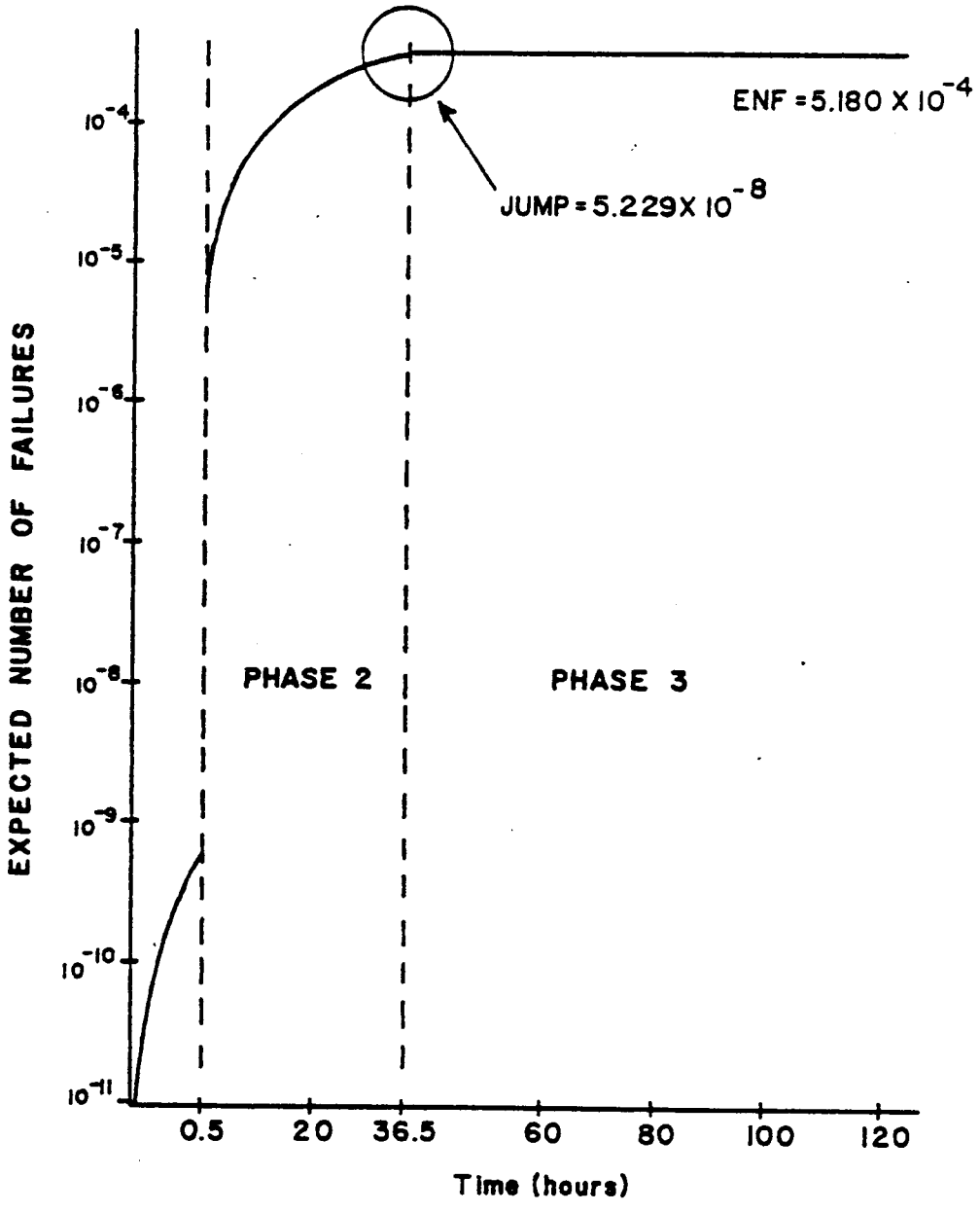


Figure 4-6: Approximation II: Repairable Case TOP Event Expected Number of Failures Versus Time.

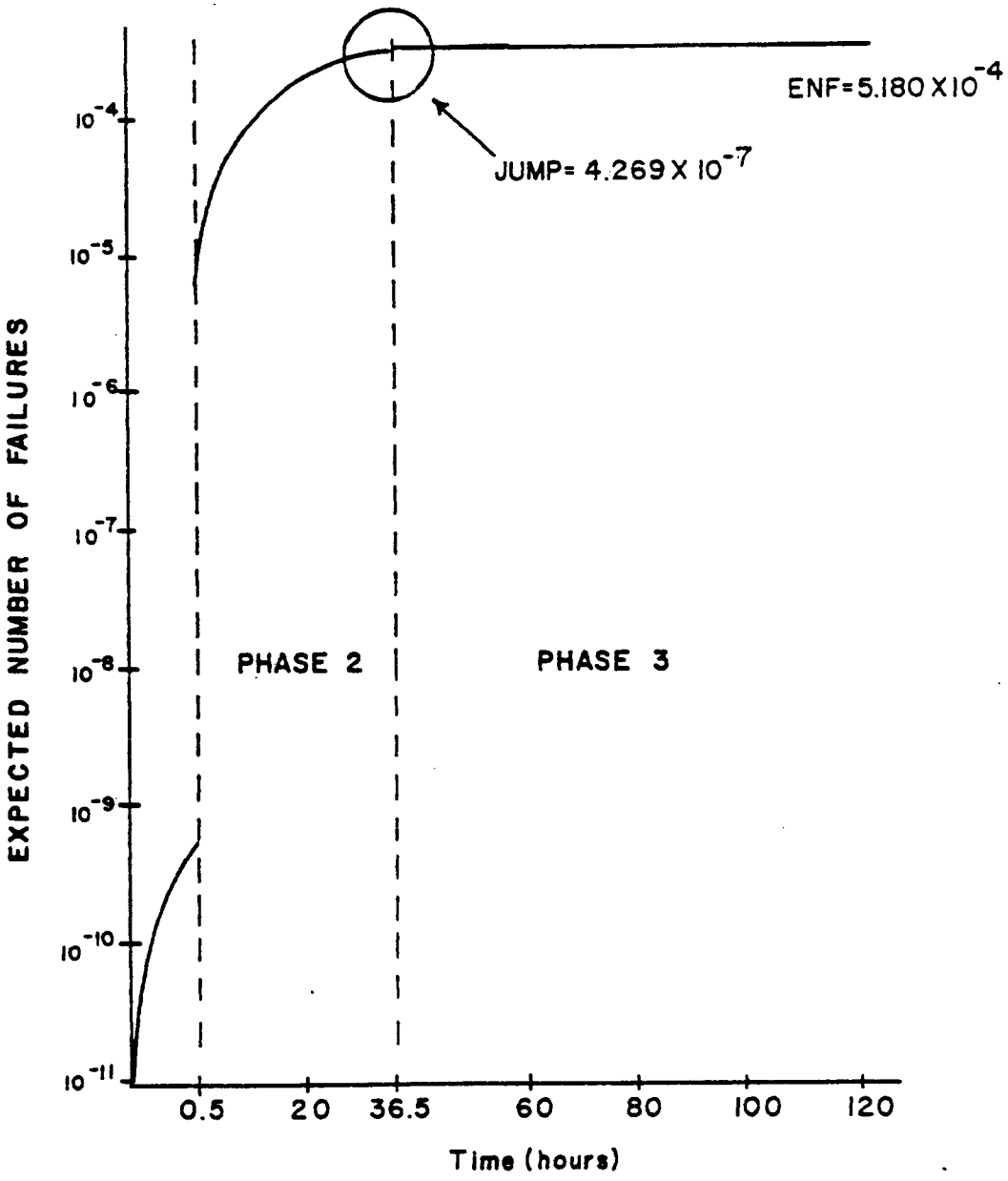


Figure 4-7: Approximation III: Repairable Case TOP Event Expected Number of Failures Versus Time.

Both the repairable and nonrepairable cases were analyzed using the approximations with bracketing. There was no significant difference in the results obtained with these approximations and the results obtained using the approximations without bracketing.

The values obtained for the expected number of failures of a BWR ECCS are not realistic since the failure rates and mean down times of the basic events used in this problem are fictitious. However, the purpose of this analysis was not to obtain some value for the expected number of failures of a BWR ECCS, but to demonstrate a new methodology. Several observations can be made about this methodology from the analysis procedures and results.

The procedures for determining the phased mission expected number of failures using either the exact method or the approximations are easy to implement. There are several computer programs (for example, KITT 1 and SUPERPOCUS) available which calculate the probability a TOP event exists or does not exist at any point in time. These same programs also calculate the expected number of failures of the TOP event for a single phase. With only a few alterations and additions, the capability of these programs could be extended to handle the phased mission expected number of failures. For example, if the unconditional basic event failures approximation were used to estimate the boundary jump, then only a minor alteration to these programs would be necessary since they already calculate all the quantities needed by this approximation technique.

The expected number of failures of the TOP event is lower in the repairable case. Although this result is obvious, it is also significant. Before the development of the methodology presented in this thesis, no methods were available to determine any integral reliability characteristic

of a repairable phased mission. With this methodology, phased mission analysis is no longer restricted by the assumption of the system being nonrepairable. Noting that accounting for repair reduced the expected number of failures, this methodology could possibly be useful in developing an optimal maintenance and repair scheme.

Another point to notice in this analysis is the small difference between the values obtained with the exact method and the approximations. There was less than a 2% error with any of the approximations used. Although the size of this error is problem dependent, it does indicate that the approximation techniques can be used with the assurance of giving an accurate estimate of the expected number of failures of a system.

One final observation to be made involves imposing failure and repair conditions on the basic events at the phase boundary. The phase 1 - phase 2 boundary jump in Figures 4-2 through 4-7 is approximately 6.999×10^{-6}. During the hand calculation of this value, it was observed that several of the intersection terms between the minimal path and cut sets were zero (because they contained mutually exclusive events) and that the size of the jump is due mainly to one intersection term (the event $\overline{HPCS} \cap ADS_+$). By assuring that the ADS is not failed during the transition from phase 1 to phase 2, the magnitude of the boundary jump would be reduced to an order of 10^{-10}. Although this would not be possible during an accident situation, it does suggest that it may be desirable to develop maintenance procedures that minimize the unavailability of the ADS. Guaranteeing the working order of other basic events that are contained in remaining intersection terms (that is, the intersections that are left after those that contain mutually exclusive events have been eliminated) can further reduce this boundary jump.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Summary and Conclusions

The expected number of failures of a system can be useful to a systems analyst for several purposes. It can be used in justifying system changes and additions during design efforts, in determining the risk associated with a particular accident, and in determining the economic feasibility of operating a system. It was shown in this thesis how, under suitable assumptions, the expected number of failures of a phased mission can be calculated. This methodology represents a new addition to phased mission analysis techniques and offers many advantages over existing phased mission methods.

1. This method is applicable to both nonrepairable and repairable systems. All previously existing methods for determining the integral characteristics of phased missions required the system to be nonrepairable.
2. The amount of information handled in the analysis of a system is not increased by this procedure. The methods developed by Esary and Ziehms to calculate the unreliability of a phased mission require using a transformation procedure that often increases the size of a problem to unmanageable proportions.
3. The procedure for determining the "boundary jump" and the approximations to this procedure are straightforward to implement.

4. If the boundary jumps are major contributors to the total expected number of failures over a mission, then the "boundary jump" calculation could suggest optimal maintenance routines to the systems analyst.

5.2 Recommendations for Future Work

Full automation of the procedures described in this thesis is recommended. A computer program, ENFPHORM, has been developed which uses the conditional basic event approximation. However, computer programs which implement the other approximations and the exact method for calculating the phased mission expected number of failures have not been developed.

Investigation into the accuracy and computational effort of the approximations for large problems is also recommended. The BWR ECCS problem studied in this thesis is relatively small and does not adequately illustrate the advantages or disadvantages of the approximations.

It should be determined if the conditional basic event approximation always overpredicts the "boundary jump." Although this method overpredicted the "boundary jump" for all the problems considered in this work, it has not been shown to overpredict the result for the general case.

Investigation into the possible elimination of the instantaneous transition between phases assumption is also recommended. Although this assumption is not overly restrictive, many systems will have transition times between phases which are long enough for the system to fail more than once during the transition.

It is recommended that the validity of the methods presented in

this thesis be checked. This might be accomplished by using "good" data from the electronics industry to calculate the expected number of failures of a piece of equipment and comparing this result with the operational history ENF of this equipment.

LIST OF REFERENCES

LIST OF REFERENCES

1. Broadhead, B. L., et al., "A Reliability Assessment of a Hypothetical Power Grid Using Phased Mission Methodology," NERS-78-05, The University of Tennessee, Knoxville, August 1978.

2. Burdick, G. R., Fussell, J. B., Rasmuson, D. M., and Wilson, J. R., "Phased Mission Analysis: A Review of New Developments and an Application," IEEE Transactions on Reliability, Vol. R-26, April 1977.

3. Fussell, J. B., "A Formal Methodology for Fault Tree Construction," Nuclear Science and Engineering, Vol. 52, 1973, pp. 421-432.

4. Rubin, J. C., "The Reliability of Complex Networks," Proceedings of the 1961 National Aerospace Electronics Conference, Dayton, Ohio, pp. 262-266.

5. Muth, E. J., "Reliability Assessment of Multiphase Missions," General Electric Company, Daytona Beach, Florida, 1964.

6. Weisburg, S. A., and Schmidt, J. H., "Computer Techniques for Estimating System Reliability," Proceedings of the 1966 Annual Symposium on Reliability, IEEE 7C26, 1966.

7. Ziehms, H., "Reliability Analysis of Phased Missions," Thesis, Naval Postgraduate School, Monterey, California, December 1974.

8. Ziehms, H., "Approximations to the Reliability of Phased Missions," Naval Research Logistics Quarterly, Vol. 25, No. 2, June 1978.

9. Barlow, R. E., and Proschan, F., Statistical Theory of Reliability and Life Testing, Holt, Rinehart and Winston, New York, 1975.

10. Brunk, H. D., An Introduction to Mathematical Statistics, Ginn and Company, Boston, 1960, p. 23.

11. Vesely, W. E., and Narum, R. E., PREP and KITT: Computer Codes for the Automatic Evaluation of a Fault Tree, IN-1349, August 1970.

12. Fussell, J. B., Henry, E. B., and Marshall, N. A., MOCUS - A Computer Program to Obtain Minimal Sets from Fault Trees, ANCR-1156, August, 1974.

13. Esary, J. D., and Proschan, F., "Coherent Structures of Nonidentical Components," Technometrics, Vol. 5, 1963, pp. 191-209.

14. Vesely, W. E., "A Time-Dependent Methodology for Fault Tree Evaluation," Nuclear Engineering and Design, Vol. 13, 1970, pp. 337-360.

15. Fussell, J. B., "How to Hand Calculate System Reliability and Safety Characteristics," IEEE Transactions on Reliability, Vol. R-24, August, 1975.

16. Fussell, J. B., et al., "SUPERPOCUS - A Computer Program for Calculating System Probabilistic Reliability and Safety Characteristics," NERS-77-01, Nuclear Engineering Department, The University of Tennessee, Knoxville, Tennessee 37916, May 1977.

17. Burdick, G. R., Fussell, J. B., Rasmuson, D. M., and Wilson, J. R., "The Implementation of Phased Mission Techniques to Nuclear Systems Analysis," Methods for Reliability and Safety Engineering, MAP#0015, Aerojet Nuclear Company, June 1975.

18. Taylor, J. R., "The Relationship Between Sequential Fault Trees, Coherent Systems, Phased Missions, Stochastic Diagrams, and Cause Consequence Diagrams," RISO-N-38-77, November 1977.

19. Fussell, J. B., "Fault Tree Analysis - Concepts and Techniques," Generic Techniques in System Reliability Analysis, Noordhoff, Leyden, 1976, pp. 133-162.

20. Fussell, J. B., and Wagner, D. P., "Fault Tree Analysis as a Part of Mechanical System Design," NBS Special Publication 487, 25th Meeting of Mechanical Failures Prevention Group, August 1977, pp. 289-308.

21. Worrell, R. B., and Burdick, G. R., "Qualitative Analysis in Reliability and Safety Studies," IEEE Transactions on Reliability, Vol. R-25, No. 3, August 1976.

APPENDICES

APPENDIX I

INPUT DESCRIPTION FOR ENFPHORM

ENFPHORM is a program that will determine the expected number of failures of a phased mission. It is written in FORTRAN IV for the IBM 360/65 computer. The methodology used in this program is not exact, but will usually give an overestimate of the expected number of failures. Approximation Method II (Chapter 3) is used in this program to calculate the boundary jump in the expected number of failures.

The input deck has the following format:

1. TITLE CARD
2. CONTROL CARD
3. BASIC EVENT INFORMATION
4. NUMBER OF PHASES AND TIME COORDINATES
5. BOUNDARY CONDITIONS
6. MINIMAL CUT SET INFORMATION
7. BASIC EVENT FAILURE RATE AND REPAIR TIME CHANGES

Input groups 1 through 5 are included once for each problem. Input groups 6 and 7 are included for each phase of the problem.

1. INPUT GROUP 1

   Contents ----------Title card (1 card)

   Array Name ----------TITLE

   Format ----------(10A8)

   Description ----------Any alphanumeric information describing the problem.

2. INPUT GROUP 2

   Contents ----------Control card (1 card)

Array Name ----------IPRINT

Format ----------(10I8)

IPRINT (1) ----------Basic event print option: (Columns 1-8)
If IPRINT (1) = 0, print basic event information. If IPRINT (1) > 0, do not print basic event information.

IPRINT (2) ----------Cut set print option: (Columns 9-16)
If IPRINT (2) = 0, print cut set information. If IPRINT (2) > 0, do not print cut set information.

IPRINT (3) ----------Time coordinate option: (Columns 17-24)
If IPRINT (3) = 0, the number of time intervals into which the phase is divided and the time the phase ends must be supplied, for each phase, by the user. If IPRINT (3) = 1, the number of time coordinates and the time coordinates must be supplied, for each phase, by the user.

IPRINT (4) ----------Basic event and cut set unit option: (Columns 25-32) IPRINT (4) allows the user to denote the computer logical unit number from which basic event and cut set data is read. If IPRINT (4) = 0, ENFPHORM defaults to 5 (unit 5), the card reader on most computers.

IPRINT (5) ----------Basic event importance rank option: (Columns 33-40) If IPRINT (5) $\leq$ 0, perform basic event rank calculations as a function of time and print this information. (This information is not calculated if IPRINT (1) > 0.) If IPRINT (5) > 0, do not perform basic event importance rank calculations.

IPRINT (6) ----------Cut set importance rank option: (Columns 41-48) If IPRINT (6) $\leq$ 0, perform cut set rank calculations as a function of time and print this information. (This information is not calculated if IPRINT (2) > 0.) If IPRINT (6) > 0, do not perform cut set importance rank calculations.

IPRINT (7) ----------Basic event name option: (Columns 49-56) If IPRINT (7) = 0, all the basic event names must be supplied by the user. If IPRINT (7) $\neq$ 1, basic event names are not used.

IPRINT (8) ----------Basic event phase boundary condition option: (Columns 57-64) If IPRINT (8) = 0, all the basic events are assigned an initial failed probability of 0.0 and no boundary conditions are imposed on the basic events for the other phases of

the missions. If IPRINT (8) = 1, a user supplied initial failed probability is assigned to each basic event at the start of the mission. No boundary conditions are imposed on the basic events for the other phases of the mission. If IPRINT (8) = 2, all the basic events are assigned an initial failed probability of 0.0 at the beginning of each phase of the mission. If IPRINT (8) = 3, the basic events are assigned an initial failed probability by the user for the beginning of each phase.

IPRINT (9) ----------Basic event data change option: (Columns 65-72) IPRINT (9) allows the user to change the failure rate and repair time for any basic event between phases. If IPRINT (9) = 0, no changes are made in the failure rates or repair times during the mission. If IPRINT (9) $\neq$ 0, the failure rate and repair time for one or more basic events is changed during the mission.

3. INPUT GROUP 3

A. Contents ----------Basic event count (1 card)

Variable name ----------NCOMP

Format ----------(I10)

Description ----------Number of basic events used in the analysis. This number is constant over all phases and must be the total number of different basic events in the logic models for all phases.

B. Contents ----------Basic event failure rates (varies)

Array name ----------XLMDA

Format ----------(8F10.0)

Description ----------Failure rates for corresponding basic events. For example, XLMDA(K) is the failure rate for basic event K.

C. Contents ----------Basic event mean time to repair (varies)

Array name ----------TAU

Format ----------(8.F10.0)

Description ----------Mean time to repair for corresponding basic events.

D. ******This input group is supplied only if IPRINT (7) = 1. If IPRINT (7) $\neq$ 1, go to input group 4.

Contents ----------Basic event names (varies)

Variable name ----------NAM

Format ----------(10A8)

Description ----------Alphanumeric names for the basic events.

4. INPUT GROUP 4

The input to this group is determined by the time coordinate control option (IPRINT (3)) as follows:

I. IPRINT (3) = 0: ENFPHORM calculates the time points for each phase.

A. Contents ----------Phase and time coordinate count (1 card)

Variable names ----------NPH, NTPT

Format ----------(10I8)

Description ----------NPH is the number of phases in the mission. NTPT is the number of intervals into which a particular phase is divided. NTPT must be supplied for each phase.

B. Contents ----------Time coordinates (1 card)

Array name ----------PHB

Format ----------(10F8.0)

Description ----------PHB is the time point at which each phase ends. NPH times must be supplied.

II. IPRINT (3) = 1: Time points are user supplied.

A. Contents ----------Phase and time coordinate count (1 card)

Variable names ----------NPH, NTPT

Format ----------(10I8)

Description ----------Time coordinates to be used for the analysis. NTPT (K) is the number of time points supplied for Phase K.

B. Contents ----------Time coordinates

Array name ----------TOT

Format ----------(8F10.0)

Description ----------Time coordinates to be used for the analysis. NTPT (K) is the number of time points supplied for phase K.

5. INPUT GROUP 5

The input for this group depends on whether any boundary conditions are to be applied to the unavailability of any of the basic events at the beginning of the phase under consideration. IF IPRINT (8) = 0 or 2, go to Input Group 6.

I. IPRINT (8) = 1

Contents ----------Basic event boundary conditions (varies

Array name ----------BCCOMP

Format ----------(8F10.0)

Description ----------The initial failed probability of each basic event at the beginning of the mission. NCOMP probabilities must be supplied by the user.

II. IPRINT (8) = 3

Contents ----------Basic event boundary conditions (varies)

Array name ----------BCCOMP

Format ----------(8F10.0)

Description ----------The initial failed probability of each basic event at the beginning of each phase. The boundary conditions for all the basic events for phase 1 must be supplied, then phase 2, etc.

Input Groups 6 and 7 are supplied for each phase of the analysis. The user should supply input groups 6 and 7 for phase 1, then supply Input Groups 6 and 7 for phase 2 and so forth.

6. INPUT GROUP 6

A. Contents ----------Cut set count (1 card)

Array name ----------Item, ICUT (I), I = 1, ITEM

Format ----------(8I10)

Description ----------ITEM is the number of basic events in the cut set and ICUT is an array containing the basic event indices for the cut set.

7. INPUT GROUP 7

******This input group is supplied only if IPRINT (9) ≠ 0. If IPRINT (9) = 0, go to Input Group 6 for the next phase.

A. Contents ----------Basic event information change count (1 card)

Variable name ----------NCHANG

Format ----------(I10)

Description ----------The number of basic events whose failure and repair information is changed.

B. Contents ----------New basic event information

Array name ----------J, XLMDA, TAU

Format ----------(I10, 2F10.0)

Description ----------J is the basic event number whose failure rate and mean time to repair is to be changed. XLMDA is the new failure rate and TAU is the new mean time to repair.

APPENDIX II

RATE OF FAILURE METHODOLOGY

The expected number of failures of the TOP event during any one particular phase of a mission is determined by integrating the rate of failure of the TOP event for that particular phase from the time that phase started to time t. In 1970, W. E. Vesely developed the methodology to determine the exact rate of failure of the TOP event.[14] The only assumptions required by his procedure are that the basic events (that is, components or subsystems) of the fault tree be s-independent and that the minimal cut sets for the fault tree of each phase are known.

II.1 Notation

The following symbols will be used in describing the rate of failure of the TOP event (system failure of interest):

$\bar{a}_i(t)$ = probability basic event i exists at time t (unavailability),

$\lambda_i(t)dt$ = probability basic event i fails in the time interval t to t+dt given it has survived to time t (failure rate),

$w(t)$ = expected number of times the basic event failure occurs at time t per unit time,

$\mu_i(t)dt$ = probability basic event i is repaired in time t to t+dt given it exists at time t (repair rate),

$W_K(t; 1,2,\ldots,m)$ = rate of failure of the set of basic events which are common members to all the minimal cut sets $1,\ldots,m$,

$W_T(t)$ = rate of failure of the TOP event.

II.2 Rate of Failure Methodology

II.2.1 Basic Event Information

The basic events used in the fault trees may be repairable or non-repairable. If it is assumed that the basic events have constant failure rates and constant repair rates (an assumption commonly used in practice), the probability a non-repairable basic event i is failed at time t is

$$\bar{a}_i(t) = 1-e^{-\lambda_i t}. \qquad \text{(II.2.1.1)}$$

For a repairable basic event i, the failed probability at time t is

$$\bar{a}_i(t) = \frac{\lambda_i}{\mu_i+\lambda_i}\,[1-e^{-(\mu_i+\lambda_i)t}]. \qquad \text{(II.2.1.2)}$$

The rate of failure of a basic event i at time t was shown by Vesely to be

$$w_i(t)dt = (1-\bar{a}_i(t))\lambda_i(t)dt. \qquad \text{(II.2.1.3)}$$

The rate of failure and the unavailability of the basic events are used to determine the rate of failure of each of the minimal cut sets.

II.2.2 Minimal Cut Set Information

A minimal cut set is a collection of basic events such that if all the basic events in the set exist, then the TOP event is guaranteed to exist. If any of the basic events in the set do not exist, then the TOP

event may or may not exist.

In order for a minimal cut set K to enter the failed state in the time interval t to t+dt given it is not failed at time t, one or more of the basic events in the minimal cut set must not exist at time t. Validly neglecting the occurrence of two or more basic events occurring in the "dt" time interval (since the probability of two or more basic events failing in the same "dt" time interval is of order dt^2 or smaller), the rate of failure of minimal cut set k is just the summation of the "ith" basic event occurring in t to t+dt ($w_i(t)dt$) with the remaining basic events existing at time t. The rate of failure of a minimal cut set K with n basic events is

$$W_K(t) = \sum_{i=1}^{n} w_i(t) \prod_{\substack{j=1 \\ j\neq i}}^{n} \bar{a}_j(t). \qquad \text{(II.2.2.1)}$$

Thus, the rate of failure of the minimal cut sets can be determined by using equations (II.2.1.1) through (II.2.2.1). The characteristics of the minimal cut sets and the basic events that compose them are used to determine the characteristics of the TOP event.

II.2.3 TOP Event Information

The rate of failure of the TOP event is the expected number of times the TOP event occurs at time t per unit time. This rate of failure depends on the rate of failure of the minimal cut sets, the rate of failure of the intersections of these minimal cut sets, and the probability of the minimal cut sets simultaneously failing in t to t+dt with one or more of the minimal cut sets already failed at time t.

To describe the TOP event rate of failure, let

u_i = event of the ith minimal cut set being in the unfailed

state at time t,

b_j = event of the ith minimal cut set being failed at time t,

A = event none of the minimal cut sets are failed at time t;

$A = u_1 \cap u_2 \cap \ldots \cap u_n$,

B = event of one or more of the minimal cut sets is failed at time t; $B = \bigcup_{j=1}^{N} b_j$,

C_i = event the ith minimal cut set fails in time t to t+dt.

By definition, the rate of failure of the TOP event is

$$W_T(t) = P[A \cap (\bigcup_{i=1}^{N} C_i)], \qquad \text{(II.2.3.1)}$$

where $\bigcup_{i=1}^{N} C_i$ = event one or more of the N C_i's occurring.

The right hand side of equation (II.2.3.1) can be rewritten as

$$W_T(t)dt = P[\bigcup_{i=1}^{N} C_i] - P[B \cap (\bigcup_{i=1}^{N} C_i)] . \qquad \text{(II.2.3.2)}$$

Equation (II.2.3.2) is readily understood if we consider the individual terms on the right hand side. The first contribution to $W_T(t)dt$, $P[\bigcup_{i=1}^{N} C_i]$, is the contribution of one or more of the minimal cut sets failing in the interval t to t+dt and causing the TOP event to occur. The second term, $P[B \cap (\bigcup_{i=1}^{N} C_i)]$, accounts for those cases in which one or more minimal cut sets fail while other minimal cut sets are already failed.

From basic probability theory [19] the first term on the right hand

side of equation (II.2.3.2) can be expanded to

$$P[\overset{N}{\underset{i=1}{U}}C_i] = \overset{N}{\underset{i=1}{\Sigma}}P(C_i) - \overset{N}{\underset{i=2}{\Sigma}}\overset{i-1}{\underset{j=1}{\Sigma}}P(C_i \cap C_j) + \ldots$$

$$+(-1)^{N-1}P(C_1 \cap C_2 \cap \ldots \cap C_N). \qquad \text{(II.2.3.3)}$$

The terms in this equation are simply the contributions from individual or simultaneous failures of minimal cut sets. Since the probability of two or more basic events failing in t to t+dt is of order dt^2 or smaller and is therefore neglected, the simultaneous failure of two or more minimal cut sets can only be caused by the failure of a basic event that is common to the minimal cut sets.

Consider the general event $(C_1 \cap C_2 \cap \ldots \cap C_M)$, the simultaneous failure of M minimal cut sets. Let there be k unique basic events that are common members to the M minimal cut sets. If k is zero, then the event $(C_1 \cap C_2 \cap \ldots \cap C_M)$ cannot occur and its associated probability is zero. Therefore, assume k is greater than zero.

If all the basic events in the M minimal cut sets are failed at time t except for one of the k common basic events and that one common basic event fails in time t to t+dt, then the event $(C_1 \cap C_2 \cap \ldots \cap C_M)$ will occur. The probability of the event $(C_1 \cap C_2 \cap \ldots \cap C_M)$ can be expressed as

$$P(C_1 \cap C_2 \cap \ldots \cap C_M) = W_o(t;1,\ldots,M)dt \overset{1\ldots M}{\underset{}{\Pi}} \bar{a}_i(t), \qquad \text{(II.2.3.4)}$$

where

$\overset{1\ldots M}{\underset{}{\Pi}} \bar{a}_i(t)$ = product of the unavailability of the basic events in the M minimal cut sets, excluding

the k common basic events

and $W_o(t;1,\ldots,M)$ = rate of failure of the set of k common basic events.

The term $P(\bigcup_{i=1}^{N} C_i)$ can therefore be determined by finding all the combinations of two, three, four,...through N minimal cut sets that have one or more common basic events and using equations (II.2.3.3) and (II.2.3.4). The quantity $W_o(t;1,\ldots,M)$ is determined using equation (II.2.2.1).

The term $P(\bigcup_{i=1}^{N} C_i)$ is known as the outer bracket to the rate of failure of the TOP event in the KITT programs.[5] Usually the first term of the right hand side of equation (II.2.3.3) is of sufficient accuracy for the determination of $W_T(t)$. However, in order to determine the exact value of $W_T(t)$ the quantity $P[B(\bigcup_{i=1}^{N} \cap C_i)]$ must also be determined. Expanding this term yields

$$P((\bigcup_{i=1}^{N} \cap C_i) \cap B) = P(C_i \cap B) - \sum_{i=2}^{N} \sum_{j=1}^{i-1} P(C_i \cap C_j \cap B) + \ldots + (-1)^{N-1} P(C_1 \cap C_2 \cap \ldots \cap C_3 \cap B). \qquad \text{(II.2.3.5)}$$

Consider a general term in this expansion, $P[B \cap C_1 \cap C_2 \cap \ldots \cap C_M]$. This is the probability of M minimal cut sets failing in time t to t+dt with one or more minimal cut sets existing at time t (event B).

Recall that event B can be written as

$$B = \bigcup_{j=1}^{N} b_j. \qquad \text{(II.2.3.6)}$$

We can now define the rate of occurrence of M minimal cut sets simultaneously failing in time t to t+dt with one or more minimal cut sets being failed at t as

$$W_I(t;1,2,\ldots,M)dt = \sum_{i=1}^{N} P(C_1 \cap C_2 \cap \ldots \cap C_M \cap b_i)$$
$$- \sum_{i=2}^{N} \sum_{j=1}^{i-1} P(C_1 \cap C_2 \cap \ldots \cap C_M \cap b_i \cap b_j) \ldots$$
$$+(-1)^{N-1} P(C_1 \cap C_2 \cap \ldots \cap C_M \cap b_1 \cap \ldots \cap b_N), \quad \text{(II.2.3.7)}$$

where again b_i = event of the ith minimal cut set being failed at time t. With equation (II.2.3.7) we can now rewrite equation (II.2.3.5) as

$$P[(\bigcup_{i=1}^{N} C_i) \cap B] = \sum_{i=1}^{N} W_I(t;i)dt - \sum_{1=2}^{N} \sum_{j=1}^{i-1} W_I(t;i,j)dt + \ldots$$

$$\ldots + (-1)^{N-1} W_I(t;1,2,\ldots,N)dt. \quad \text{(II.2.3.8)}$$

The value of the terms in the right hand side of equation (II.2.3.7) are determined in a similar manner as the terms were in equation (II.2.3.3). The quantity $P(C_1 \cap C_2 \cap \ldots \cap C_M \cap b_1 \cap b_2 \cap \ldots \cap b_N)$ is determined using the following steps:

1. All the basic events in the 1,...,N minimal cut sets are in the failed state at time t.

2. All the basic events in the 1,...,M minimal cut sets which are not common to all the 1...M minimal cut sets are in the failed state at time t.

3. Any of the basic events which are common to all the 1...M minimal cut sets and are also a member of any one of the 1...N minimal cut sets are in the failed state at time t.

4. The rate of failure of the remaining set of common basic events of the 1...M minimal cut sets is calculated using equation (II.2.2.1). If there are no remaining basic

events, this rate of failure is identically zero.

Thus, $P(C_1 \cap C_2 \cap \ldots \cap C_m \cap b_1 \cap b_2 \cap \ldots \cap b_n)$ can be expressed as

$$P(C_1 \cap \ldots \cap C_m \cap b_1 \ldots \cap b_n) = W(t;1\ldots M--1\ldots N) \prod_{1\ldots M}^{1\ldots N} \bar{a}_i(t), \quad \text{(II.2.3.9)}$$

where $W(t;1\ldots M--1\ldots N)$ = rate of failure of the set of basic events common to all M minimal cut sets, deleted from which are those basic events also in any of the minimal cut sets 1...N,

and $\prod_{1\ldots M}^{1\ldots N} \bar{a}_i(t)$ = the product of unique basic event unavailabilities, where the basic event is a member of any of the 1...N minimal cut sets or of the 1...M minimal cut sets, but not a common member of all m minimal cut sets.

The computation of $P[(\bigcup_{i=1}^{N} C_i) \cap B]$ is therefore straightforward using equations (II.2.3.8) and (II.2.3.9). This quantity is called the inner bracket in the KITT programs. For fault trees with a large number of minimal cut sets this quantity, $P[(\bigcup_{i=1}^{N} C_i) \cap B]$ usually provides only a minor correction to the rate of failure of the TOP event.

Thus, the rate of failure of the TOP event is easily determined using equations (II.2.3.2), (II.2.3.3), and (II.2.3.8). Upper and lower bounds to the exact rate of failure of the TOP event can be determined

limiting the number of intersections (that is, simultaneous failures of minimal cut sets) in the inner and outer bracket equations. The expected number of failures of the TOP event for the time interval t_1 to t_2 is

$$ENF_T = \int_{t_1}^{t_2} W_T(t)dt. \qquad (II.2.3.10)$$

The KITT programs approximate this integral using the trapezoidal rule.

II.2.4 Example Problem II.1

The following problem is presented to demonstrate the rate of failure methodology. Consider the fault tree of Figure A-II-1. The minimal cut sets for this fault tree are $K_1 = (X_1,X_2)$, $K_2 = (X_1,X_3)$, and $K_3 = (X_1,X_4)$. The rate of failure of the TOP event was given by equation (II.2.3.2) as

$$W_T(t)dt = P[\bigcup_{i=1}^{N} C_i] - P[B\cap(\bigcup_{i=1}^{N} C_i)]. \qquad (II.2.3.2)$$

The first term in the right hand side of this equation for the particular fault tree we are analyzing is determined using equation (II.2.3.3). This yields

$$P[\bigcup_{1=1}^{3} C_i] = P(K_1^*) + P(K_2^*) + P(K_3^*) - P(K_1^*\cap K_2^*) - P(K_1^*\cap K_3^*) -$$

$$P(K_2^*\cap K_3^*) + P(K_1^*\cap K_2^*\cap K_3^*), \qquad (II.2.4.1)$$

where K_i^* = event the minimal cut set K_i fails in time t to t+dt. Using equations (II.2.2.1) and (II.2.3.4) to express this last equation in terms of basic events gives us

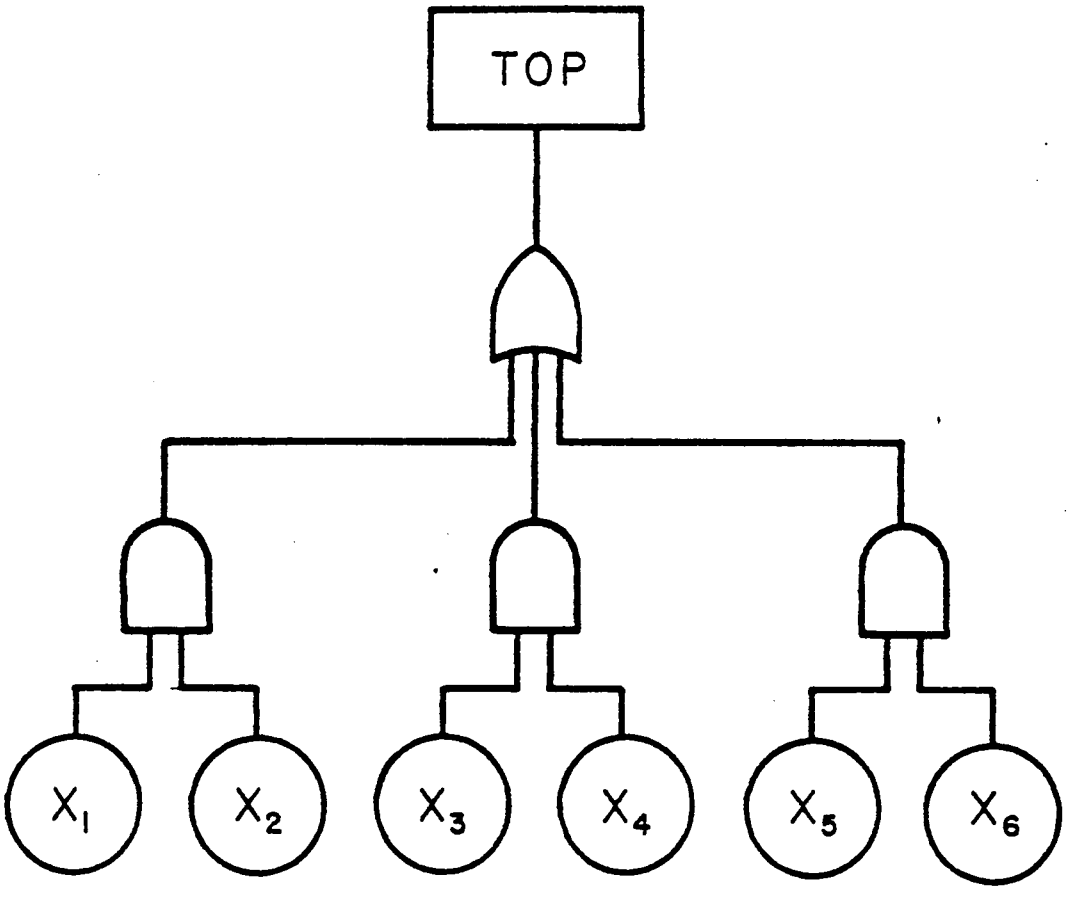


Figure A-II-1: Example Problem II.1 Fault Tree.

$$P[\bigcup_{i=1}^{3} C_i] = (1-\bar{a}_1(t))\bar{a}_2(t)\lambda_1(t)dt + (1-\bar{a}_2(t))\bar{a}_1(t)\lambda_2(t)dt +$$

$$(1-\bar{a}_1(t))\bar{a}_3(t)\lambda_1(t)dt + (1-\bar{a}_3(t))\bar{a}_1(t)\lambda_3(t)dt +$$

$$(1-\bar{a}_1(t))\bar{a}_4(t)\lambda_1(t)dt + (1-\bar{a}_4(t))\bar{a}_1(t)\lambda_4(t)dt -$$

$$(1-\bar{a}_1(t))\bar{a}_2(t)\bar{a}_3(t)\lambda_1(t)dt -$$

$$(1-\bar{a}_1(t))\bar{a}_2(t)\bar{a}_4(t)\lambda_1(t)dt -$$

$$(1-\bar{a}_1(t))\bar{a}_3(t)\bar{a}_4(t)\lambda_1(t)dt +$$

$$(1-\bar{a}_1(t))\bar{a}_2(t)\bar{a}_3(t)\bar{a}_4(t)\lambda_1(t)dt . \qquad \text{(II.2.4.2)}$$

The terms accounting for the simultaneous failure of two or more minimal cut sets involve the product of the unavailability of two or more basic events while the single cut set failure terms involve only one basic event unavailability. For basic events with relatively good reliability characteristics, the terms accounting for the simultaneous failure of cut sets are usually insignificant with respect to the term accounting for single cut set failures.

Calculation of the second term, $P(B\cap(\bigcup_{i=1}^{3} C_i))$ in equation (II.2.3.2) is also straightforward. Applying equation (II.2.3.8) to this particular problem yields

$$P[(\bigcup_{i=1}^{3} C_i)\cap B] = W_I(t;K_1)dt + W_I(t;K_2)dt + W_I(t;K_3)dt -$$

$$W_I(t;K_1,K_2)dt - W_I(t;K_1,K_3)dt - W_I(t;K_2,K_3)dt +$$

$$W_I(t;K_1,K_2,K_3). \qquad \text{(II.2.4.3)}$$

Expanding the terms in this equation according to equation (II.2.3.7)

gives

$$P[(\bigcup_{i=1}^{3} C_i)\cap B] = P(K_1^*\cap K_2) + P(K_1^*\cap K_3) - P(K_1^*\cap K_2^*\cap K_3) + P(K_2^*\cap K_3) +$$

$$P(K_2^*\cap K_3) - P(K_3^*\cap K_1\cap K_3) + P(K_3^*\cap K_1) + P(K_3^*\cap K_2) -$$

$$P(K_3^*\cap K_1\cap K_2) - P(K_1^*\cap K_2^*\cap K_3) - P(K_1^*\cap K_3^*\cap K_2) -$$

$$P(K_2^*\cap K_3^*\cap K_1) + 0 , \qquad \text{(II.2.4.4)}$$

where K_i = event minimal cut set K_i is failed at time t. The terms in the above equation can easily be rewritten in terms of basic event unavailabilities and failure rates using equation (II.2.3.9). For illustrative purposes, we will expand two of the terms in equation (II.2.4.4). This yields

$$P(K_1\cap K_2^*) = (1-\bar{a}_2(t))\bar{a}_1(t)\bar{a}_3(t)\lambda_2(t)dt \qquad \text{(II.2.4.5)}$$

and

$$P(K_3\cap K_1^*\cap K_2^*) = (1-\bar{a}_4(t))\bar{a}_1(t)\bar{a}_2(t)\bar{a}_3(t)\lambda_4(t)dt. \qquad \text{(II.2.4.6)}$$

The other terms are expanded in a similar manner. Note that even in this simple example all the terms in equation (II.2.4.4) will include the product of the unavailability of at least two basic events. Thus, if the basic event unavailabilities are small, the value of the quantity $P[B\cap(\bigcup_{i=1}^{N} C_i)]$ should be insignificant relative to the value of $P(\bigcup_{i=1}^{N} C_i)$.

The equation (II.2.4.2) and (II.2.4.4) provide an analytical solution to the rate of failure of the TOP event. The expected number of failures of the TOP event is just the integral of these two equations over the time interval of interest.

APPENDIX III

INPUT DATA FOR THE BOILING WATER REACTOR EMERGENCY CORE COOLING SYSTEM ANALYSIS

The input data needed to analyze the BWR ECCS appears in Tables A-III-1 and A-III-2. Table A-III-1 is a list of the basic events used in the analysis and their respective failure rates (λ) and mean down times (τ). Table A-III-2 lists the minimal cut sets and minimal path sets for each phase of the mission. Figures A-III-1 through A-III-3 are the fault trees for the three phases of the mission.

TABLE A-III-1

BASIC EVENT FAILURE DATA

Basic Event Name	Description	Failure Rate (Hr.-1)	Mean Down Time (Hr.)
ADS	Automatic Depressurization System	1.4E-5	10
HPCS	High Pressure Core Spray System	2.7E-4	20
LPCS	Low Pressure Core Spray	2.6E-6	48
LPCI-A	Low Pressure Core Injection System A	2.5E-5	25
LPCI-B	Low Pressure Core Injection System B	2.5E-5	25
LPCI-C	Low Pressure Core Injection System C	2.5E-5	25
HX-A	Heat Exchanger A	2.8E-6	72
HX-B	Heat Exchanger B	2.8E-6	72

TABLE A-III-2

BWR ECCS MINIMAL CUT SETS AND MINIMAL PATH SETS

Phase	Minimal Path Sets	Minimal Cut Sets
1	HPCS	HPCS ADS
	ADS LPCS	HPCS LPCS LPCI-A LPCI-B LPCI-C
	ADS LPCI-A	
	ADS LPCI-B	
	ADS LPCI-C	
2	ADS HX-A LPCI-A LPCI-B	ADS
	ADS HX-A LPCI-A LPCI-C	LPCI-A LPCI-B
	ADS HX-A LPCI-A HPCS	HX-A HX-B
	ADS HX-A LPCI-A LPCS	HX-A LPCI-B
	ADS HX-B LPCI-B LPCI-A	HX-B LPCI-A
	ADS HX-B LPCI-B LPCI-C	LPCI-A LPCI-C LPCS HPCS
	ADS HX-B LPCI-B HPCS	LPCI-B LPCI-C LPCS HPCS
	ADS HX-B LPCI-B LPCS	
3	HX-A LPCI-A	HX-A HX-B
	HX-B LPCI-B	HX-A HX-B
		HX-B LPCI-A
		LPCI-A LPCI-B

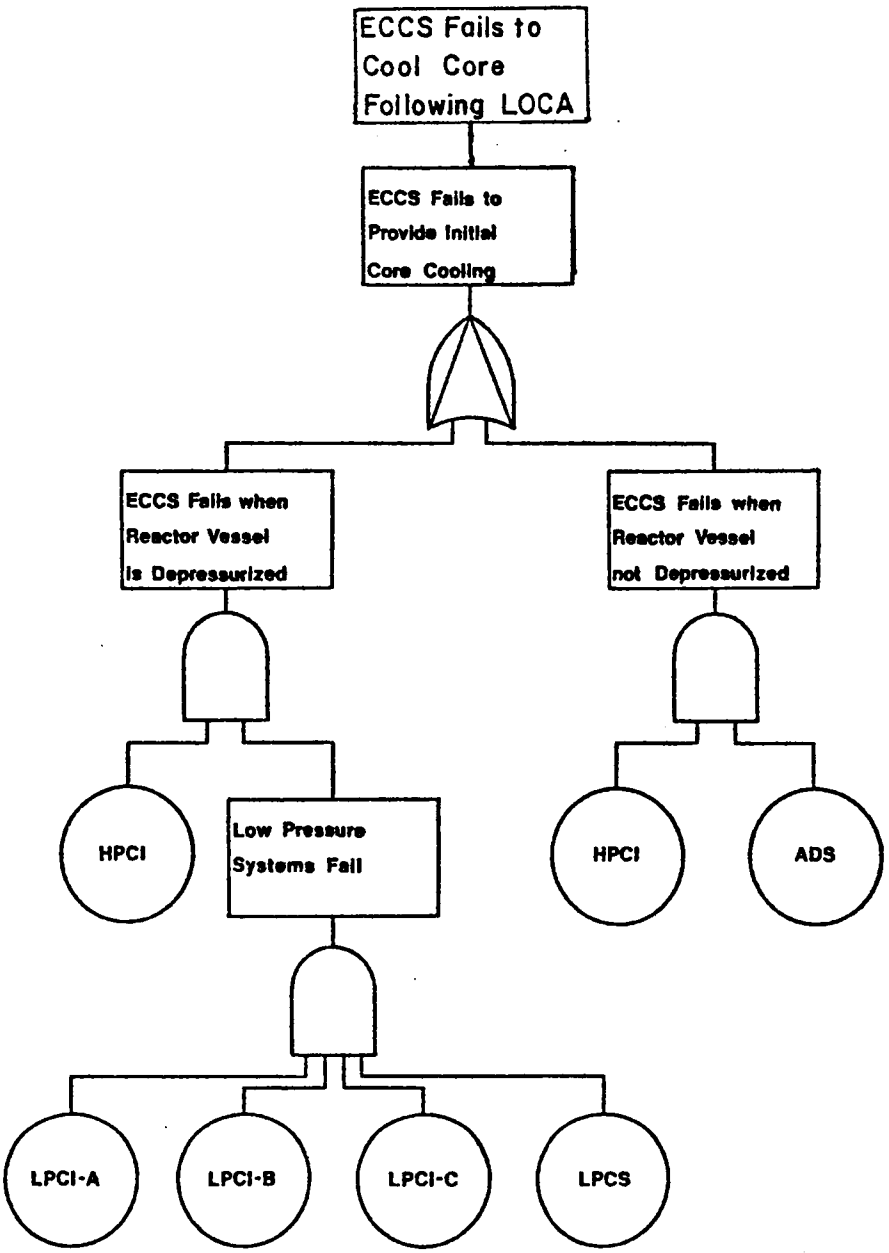


FIGURE A-III-1: BWR ECCS Phase 1 Logic Model

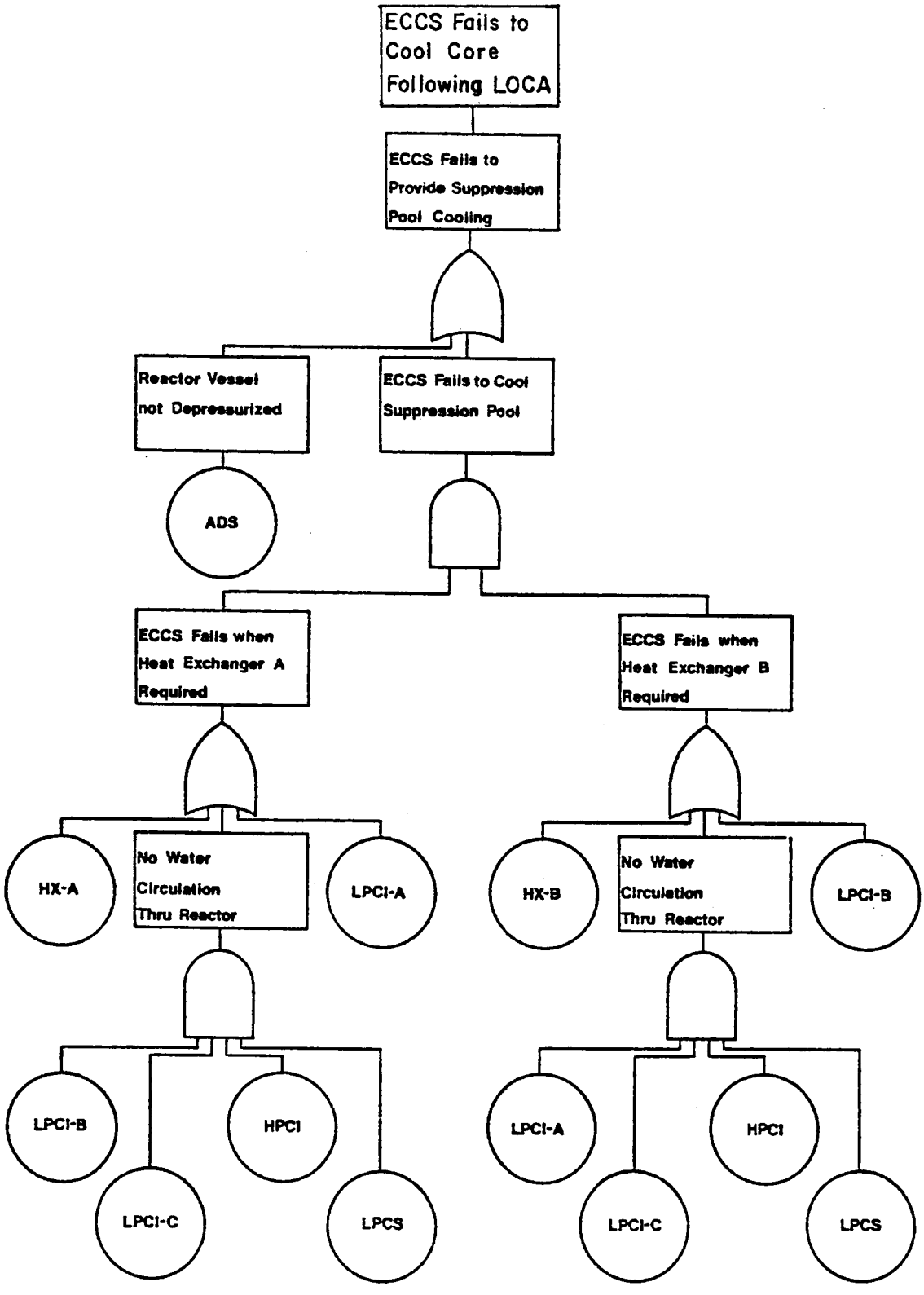


FIGURE A-III-2: BWR ECCS Phase 2 Logic Model

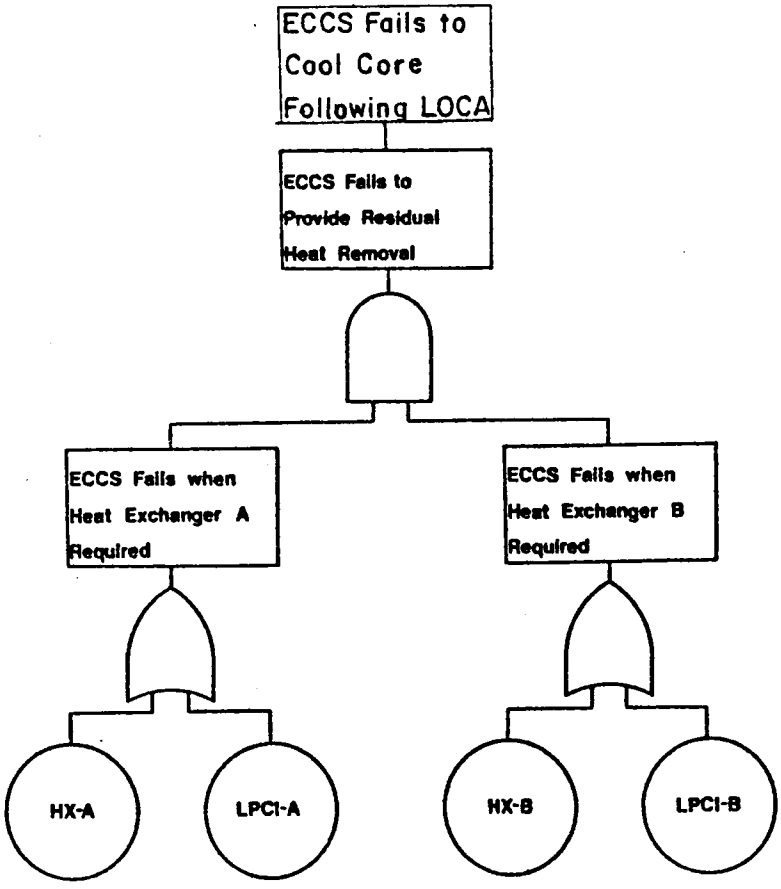


FIGURE A-III-3: BWR ECCS Phase 3 Logic Model

VITA

David Fairfax Montague was born in Atlanta, Georgia on January 27, 1956. He is the son of the late Dr. F. E. Montague and Mrs. F. E. Montague. He was raised in Palatka, Florida. After graduating from Palatka South High School in June 1974, he entered the Georgia Institute of Technology where he received a Bachelor of Nuclear Engineering degree in September 1977.

David entered the graduate program in nuclear engineering at the University of Tennessee, Knoxville in September 1977. After receiving the Master of Engineering degree in 1979, he will pursue a Doctor of Philosophy degree in the field of nuclear systems reliability engineering and risk assessment.