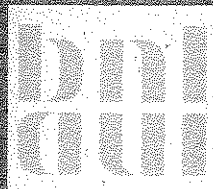


# MARKOVIAN RELIABILITY ANALYSIS UNDER UNCERTAINTY WITH AN APPLICATION ON THE SHUTDOWN SYSTEM OF THE CLINCH RIVER BREEDER REACTOR

I.A. Papazoglou and E.P. Gyftopoulos

DATE PUBLISHED - SEPTEMBER 1978

ENGINEERING AND ADVANCED REACTOR SAFETY DIVISION  
DEPARTMENT OF NUCLEAR ENERGY, BROOKHAVEN NATIONAL LABORATORY  
UPTON, NEW YORK 11973



Prepared for the U.S. Nuclear Regulatory Commission  
Contract No. EY-76-C-02-0016

# **MARKOVIAN RELIABILITY ANALYSIS UNDER UNCERTAINTY WITH AN APPLICATION ON THE SHUTDOWN SYSTEM OF THE CLINCH RIVER BREEDER REACTOR**

**Ioannis A. Papazoglou**  
**Engineering and Advanced Reactor Safety Division**  
**Department of Nuclear Energy**  
**Brookhaven National Laboratory**  
**Associated Universities, Inc.**  
**Upton, New York 11973**

**Elias P. Gyftopoulos**  
**Department of Nuclear Engineering**  
**Massachusetts Institute of Technology**  
**Cambridge, Massachusetts 02139**

**Manuscript Completed: August 1978**  
**Date Published: September 1978**

**Prepared for**  
**U.S. Nuclear Regulatory Commission**  
**Offices of Nuclear Reactor Regulation and**  
**Nuclear Regulatory Research**  
**Washington, D.C. 20555**  
**Contract No. EY-76-C-02-0016**  
**Fin Nos. A-3000 and A-3047**

#### NOTICE

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

The views expressed in this report are not necessarily those of the U.S. Nuclear Regulatory Commission.

Available from  
U.S. Nuclear Regulatory Commission  
Washington, D.C. 20555

Available from  
National Technical Information Service  
Springfield, Virginia 22161

MARKOVIAN RELIABILITY ANALYSIS UNDER UNCERTAINTY  
WITH AN APPLICATION ON THE  
SHUTDOWN SYSTEM OF THE CLINCH RIVER BREEDER REACTOR

ABSTRACT

A methodology for the assessment of the uncertainties about the reliability of nuclear reactor systems described by Markov models is developed, and the uncertainties about the probability of loss of coolable core geometry (LCG) of the Clinch River Breeder Reactor (CRBR) due to shutdown system failures, are assessed.

Uncertainties are expressed by assuming the failure rates, the repair rates and all other input variables of reliability analysis as random variables, distributed according to known probability density functions (pdf). The pdf of the reliability is then calculated by the moment matching technique. Two methods have been employed for the determination of the moments of the reliability: the Monte Carlo simulation; and the Taylor-series expansion. These methods are adopted to Markovian problems and compared for accuracy and efficiency. Three techniques have also been developed for reducing the calculation effort. These are: (1) Systematic ordering of the system states - resulting in a simpler structure of the transition probability matrix; (2) Systematic merging of Markov processes describing systems exhibiting symmetries - resulting in smaller transition probability matrix dimensions; and (3) Systematic choice of the maximum possible time step for the process and introduction of an approximation that permits the use of large time steps in the Monte Carlo simulation.

Computer codes have been written to perform the calculations necessary for the implementation of the developed methods.

A Markovian reliability analysis under uncertainty for the shutdown system of the CRBR has also been performed. A Markov model has been used including common cause failures, interdependences between the unavailability of the system and the occurrence of transients, and inspection and maintenance procedures that depend on the state of the system and include the possibility of human errors. The failure rates, the repair rates, the rates at which transients occur and all other input variables have been assumed randomly distributed in such a way that their upper 90% confidence limit is one order of magnitude higher than the lower 90% confidence limit. The latter limit is of the same order of magnitude as the most probable value of the quantity in question.

The consideration of common cause failures, human errors, and uncertainties has a significant effect on the calculated probability of LCG due to shutdown system failures. The calculated probability of LCG is distributed lognormally with median  $2 \times 10^{-6}$  and upper and lower 90% confidence limits  $2 \times 10^{-5}$  and  $2 \times 10^{-7}$ , respectively. This probability band represents a considerable difference from the  $1 \times 10^{-9}$  point estimate of the same probability if common cause failures are not considered, the inspection is perfect, and the input variables are fixed at their mean values.

## ACKNOWLEDGEMENTS

This report is based on a dissertation submitted by Ioannis A. Papazoglou to the Department of Nuclear Engineering of the Massachusetts Institute of Technology in partial fulfillment of the requirements for the degree of Doctor of Science.

The research for this dissertation was performed at Brookhaven National Laboratory while Dr. Papazoglou was associated with the Fast Reactor Safety Division. Dr. Papazoglou would like to thank all the people who helped him in various ways during the two and one-half years he spent there. In particular, special thanks go to Drs. Robert A. Bari and Arthur Buslik for many fruitful discussions.

Financial support from the United States Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, and Office of Nuclear Reactor Regulation, is gratefully acknowledged.

## TABLE OF CONTENTS

	<u>Page</u>
ABSTRACT . . . . .	iii
ACKNOWLEDGMENTS . . . . .	v
TABLE OF CONTENTS . . . . .	vii
LIST OF ACRONYMS . . . . .	xi
LIST OF FIGURES . . . . .	xii
LIST OF TABLES . . . . .	xiv
CHAPTER I: INTRODUCTION . . . . .	1
CHAPTER II: MARKOV PROCESSES AND RELIABILITY ANALYSIS . . . . .	7
2.1 Introduction . . . . .	7
2.2 Basic Assumptions and Definitions . . . . .	8
2.3 Linearization of Probabilities and Ordering of States . . . . .	12
2.4 Repair Policies and Special Systems . . . . .	16
2.5 An Application . . . . .	17
CHAPTER III: MERGEABLE MARKOV PROCESSES . . . . .	21
3.1 Introduction . . . . .	21
3.2 Mergeable Markov Processes and the Merge- ability Criterion . . . . .	22
3.3 On the Mergeability of Markov Processes of Systems Exhibiting Symmetries . . . . .	27
3.3.1 Systems Exhibiting Symmetries at the Component Level . . . . .	28
3.3.2 Systems Exhibiting Symmetries at the Subsystem Level . . . . .	28
3.4 Automated Merging of a Markov Process by a Computer . . . . .	42

TABLE OF CONTENTS (Cont.)		Page
CHAPTER IV:	MARKOVIAN RELIABILITY ANALYSIS UNDER UNCERTAINTY . . .	48
4.1	Introduction . . . . .	48
4.2	Objectives of the Reliability Analysis Under Uncertainty . . . . .	49
4.3	Statement of the Problem . . . . .	51
4.3.1	Functions of Random Matrices . . . . .	53
4.3.2	Need for Approximate Solutions . . . . .	54
4.4	On the Distribution of the Input Variables . . .	56
4.4.1	Gamma Probability Density Function . . . .	56
4.4.2	The Log-Normal Probability Density Function . . . . .	57
4.4.3	The Beta Probability Density Function . .	58
4.4.4	Log-Gamma Probability Density Function . .	59
4.5	Quantification of Common Cause Failure Rates and Interdependences of Transition Rates . . . .	59
4.6	Analytical Results of the 2x2 Case . . . . .	62
4.6.1	The pdf of the Steady-State Availability of a Two-State Component . . . . .	65
4.6.2	Conditional pdf of the Transient Part of the Availability of Two-State Component .	69
4.6.3	Expected n-Step Transition Probabilities .	70
CHAPTER V:	THE MOMENT-MATCHING METHOD . . . . .	73
5.1	Introduction . . . . .	73
5.2	The Moment-Matching Method . . . . .	73
CHAPTER VI:	MONTE CARLO SIMULATION . . . . .	77
6.1	Introduction . . . . .	77
6.2	Straightforward Monte Carlo Sampling . . . . .	78



	<u>Page</u>
TABLE OF CONTENTS (Cont.)	
6.2.1 Numerical Example of the Straight-forward Monte Carlo Simulation . . . . .	84
6.3 On the Size of the Time Step . . . . .	88
6.4 The Choice of the Size of the Time Step in a Monte Carlo Simulation . . . . .	91
6.4.1 A Numerical Example . . . . .	97
CHAPTER VII: THE TAYLOR SERIES APPROXIMATION . . . . .	113
7.1 Introduction . . . . .	113
7.2 Approximate Evaluation of the System-Moments by Taylor Series Expansion . . . . .	114
7.3 Evaluation of the Derivatives . . . . .	117
7.4 Numerical Example of a Two-State System . . . . .	121
7.4.1 Time-Dependent Unavailability . . . . .	122
7.4.2 Steady-State Unavailability . . . . .	122
7.5 An Example of the General Case . . . . .	124
CHAPTER VIII: RELIABILITY ASSESSMENT OF THE CLINCH RIVER BREEDER REACTOR SHUTDOWN SYSTEM UNDER UNCERTAINTY . . . . .	133
8.1 Introduction . . . . .	133
8.2 System Description . . . . .	134
8.2.1 Introduction . . . . .	134
8.2.2 Primary Electrical Subsystem . . . . .	135
8.2.3 Secondary Electrical Subsystem . . . . .	139
8.2.4 Primary Mechanical Subsystem . . . . .	140
8.2.5 Secondary Mechanical Subsystem . . . . .	145
8.3 System Mission and Reliability Duty Cycle . . . . .	148
8.4 System Model and Assumptions . . . . .	151

TABLE OF CONTENTS (Cont.)		<u>Page</u>
8.5	Detailed Subsystem Models . . . . .	162
8.5.1	Mechanical Subsystem . . . . .	162
8.5.2	Primary Output Logic . . . . .	168
8.5.3	Electrical Subsystem . . . . .	171
8.5.4	System Inspection . . . . .	185
8.6	Data Base . . . . .	190
8.7	Presentation and Discussion of the Results . .	198
CHAPTER IX:	SUMMARY AND CONCLUSIONS . . . . .	210
9.1	Methodology . . . . .	210
9.2	Reliability Assessment of the CRRR RSS . . . .	214
CHAPTER X:	RECOMMENDATIONS FOR FURTHER RESEARCH . . . . .	219
REFERENCES	. . . . .	225
APPENDIX A:	STAGEN-MARELA: A Computer Code for Markovian Reliability Analysis . . . . .	230
APPENDIX B:	SSTAGEN-MMARELA: A Computer Code for Mergeable Markovian Reliability Analysis . .	232
APPENDIX C:	Modification of MMARELA for Use in Monte Carlo Simulations . . . . .	236

## LIST OF ACRONYMS

CRBR	Clinch River Breeder Reactor
LCG	Loss of Core Coolable Geometry
LRT	Limited Response Transients
MFT	Major Flow Transients
PCA	Primary Control Rod Assembly
PCRD	Primary Control Rod Driveline
PCRDM	Primary Control Rod Drive Mechanism
PFN	Protective Function Network
PMS	Primary Mechanical Subsystem
POL	Primary Output Logic
PPF	Primary Protective Function
PPFN	Primary Protective Function Network
PSAR	Preliminary Safety Analysis Report
PSS	Primary Shutdown System
RSS	Reactor Shutdown System
RT	Reactivity Transients
SCA	Secondary Control Assembly
SCRD	Secondary Control Rod Driveline
SCRDM	Secondary Control Rod Drive Mechanism
SCRS	Secondary Control Rod System
SMS	Secondary Mechanical Subsystem
SOL	Secondary Output Logic
SPF	Secondary Protective Function
SPFN	Secondary Protective Function Network
SSS	Secondary Shutdown System

# LIST OF FIGURES

<u>Figure</u>		<u>Page</u>
2.1	Sample system . . . . .	19
2.2	Time-dependent unavailability of the sample system . . .	20
2.3	Time-dependent unreliability of the sample system . . . .	20
3.1	Equivalent system to system shown in Figure 2.1 . . . . .	42
4.1	Overlapping of the pdf's of h and h* . . . . .	61
5.1	Regions in $(\beta_1, \beta_2)$ plane for various distributions . . .	76
6.1	Pdf of failure probability without repair at t=1000 hr. Beta pdf resulting from the moment-matching technique and histogram of 1200 Monte Carlo trials . . . . .	87
6.2	Histograms of the negative common logarithm of some transition rates of components of the sample system . . .	99
6.3	Expected value of future probability for various cutoff values $x_0$ . . . . .	101
7.1	Pdf of failure probability without repair at t=1000 hr. .	132
8.1	Primary electrical logic diagram . . . . .	136
8.2	Typical primary electrical subsystem . . . . .	137
8.3	Primary electrical shutdown subsystem block diagram . . .	138
8.4	Secondary electrical logic diagram . . . . .	141
8.5	Typical primary electrical subsystem . . . . .	142
8.6	Secondary electrical shutdown subsystem block diagram . .	143
8.7	Primary control rod system . . . . .	144
8.8	Collapsible motor roller nut drive . . . . .	146
8.9	Secondary control rod system . . . . .	147
8.10	Simplified logic block diagram of CRBR reactor shutdown system . . . . .	152
8.11	State flow chart for CRBR and shutdown system . . . . .	155

# LIST OF FIGURES (Cont.)

<u>Figure</u>		<u>Page</u>
8.12	Logic flow chart of the reactor shutdown system model . .	158
8.13	Control assembly conditions in core layout . . . . .	163
8.14	Logic block diagram for primary output logic . . . . .	169
8.15	Functional block diagram of the flux-square root of pressure subsystem, one channel of three shown . . . . .	173
8.16	Functional block diagram of the flux-total flow protective subsystem, one channel of three shown . . . . .	173
8.17	State flow chart for typical protective function network.	176
8.18	Simplified state flow chart for typical primary protective function network . . . . .	176
8.19	Simplified state flow chart for typical secondary protective function network . . . . .	176
8.20	Unavailability of primary protective function network . .	179
8.21	Histograms of the negative common logarithm of some transition rates of components of the shutdown system . .	192
8.22	Median and 90% confidence limits of the RSS failure probability as a function of time . . . . .	200
8.23	Pdf of the negative common logarithm of the RSS failure probability per year. Taylor series approximation and Monte Carlo diagram . . . . .	204
A.1	Flow chart of programs STAGEN and MARELA . . . . .	231
B.1	Flow chart of program SSTAGEN-I . . . . .	234
B.2	Flow chart of program SSTAGEN-II . . . . .	235

# LIST OF TABLES

<u>No.</u>		<u>Page</u>
2.1	Conditional failure and repair rates of the components of the system in Figure 2.1 . . . . .	19
3.1	Comparison of the computer program and computer time required for solving the original and the merged Markov processes for system in Figure 2.1 . . . . .	47
4.1	Summary of important distributions . . . . .	60
6.1	Confidence levels for the expected value of the failure probability without repair of the sample system . . . . .	85
6.2	Cumulative probabilities for the failure probabilities without repair at $t=1000$ hr . . . . .	86
6.3	Expected failure probability with repair for various cutoff values $x_0$ . . . . .	100
6.4	Expected failure probability without repair: regular run ( $x_0=\infty$ ) and $x_0=.01$ . . . . .	100
6.5	Random sample for $\lambda_1$ . . . . .	102
6.6	Random sample for $\mu_1$ . . . . .	103
6.7	Random sample for $\lambda_2$ . . . . .	104
6.8	Random sample for $\mu_2$ . . . . .	105
6.9	Random sample for $h_5=k_1 \cdot \lambda_1$ . . . . .	106
6.10	Random sample for $h_6=k_2 \cdot \mu_1$ . . . . .	107
6.11	Random sample for $h_7=k_3 \cdot \lambda_2$ . . . . .	108
6.12	Random sample for $h_3=k_4 \cdot \lambda_2$ . . . . .	109
6.13	Random sample for $h_9=k_5 \cdot \lambda_2$ . . . . .	110
6.14	Random sample for $h_{10}=k_6 \cdot \mu_2$ . . . . .	111
6.15	Random sample for $h_5=k_1 \cdot \lambda_1$ . . . . .	112

# LIST OF TABLES (Cont.)

<u>No.</u>		<u>Page</u>
7.1	Moments of gamma distributed failure and repair rates of a two-state system . . . . .	123
7.2	Expected value and variance of dynamic failure probability of a two-state system . . . . .	123
7.3	Conditional transition rates for the components of system in Figure 2.1 . . . . .	126
7.4	Expected values and central moments of transition rates and dependence coefficients . . . . .	129
7.5	Expected value and central moments of failure probability with repair . . . . .	130
7.6	Expected value and central moments of failure probability without repair . . . . .	131
7.7	Taylor series expansion coefficients for the expected value and variance of the failure probability without repair at T=1000 hr . . . . .	132
7.8	Cummulative probability for the failure probability without repair at T=1000 hr . . . . .	132
8.1	Superstate groups for mechanical subsystem . . . . .	167
8.2	RSS-state subspaces to which combination of mechanical and electrical subsystem superstates belong . . . . .	183
8.3	Failure rates and associated uncertainties. Primary and secondary protective function networks . . . . .	193
8.4	Dependence coefficients and associated uncertainties . . . . .	195
8.5	Transient arrival rates, reactor repair rate, and the associated uncertainties . . . . .	197
8.6	Failure detection probability, inspection error probability, and associated uncertainties . . . . .	197
8.7	Median and 90% confidence limits of the failure probability as functions of time . . . . .	199

# LIST OF TABLES (Cont.)

<u>No.</u>		<u>Page</u>
8.8	Mean, variance, and coefficients $\beta_1, \beta_2$ of the negative common logarithm of the failure probability at various times . . . . .	202
8.9	Median and 90% confidence limits of the interval unavailabilities (mean over 48 weeks) of the system to respond to reactivity, major flow, and limited response transients . . . . .	202
8.10	Classification of input variables according to their contribution to the uncertainties of the failure probability . . . . .	205
8.11	Point estimate median and 90% confidence limits of the RSS failure probability per year under various assumptions . . . . .	209



## CHAPTER ONE

### INTRODUCTION

The objectives of this dissertation are: the development of a methodology for the calculation of uncertainties about the reliability of nuclear reactor systems described by Markov models and the assessment of the uncertainties in the reliability of the Shutdown System of the Clinch River Breeder Reactor.

Reliability of a system is the probability that the system will perform a required function under stated conditions and for a stated period of time. For complex systems (as nuclear reactors), this probability is calculated from existing information about subsystems or components of the system. This information is usually expressed in terms of failure and repair rates of components. Hence, the reliability of the system is a function of the failure and repair rates of the components. The complexity of this function and of the methods for its evaluation vary with the complexity and the stochastic character of the system.

Very often in reliability analyses of nuclear systems, statistical dependences among either failures or repairs or both must be considered. Such statistical dependences are introduced by both common cause failures and by maintenance procedures that are contingent on the state of the components, on the state of the system, and on the test method. Many aspects of statistical dependence can be analyzed if the probabilistic behavior of the system can be simulated by a Markov process.

If the failure and repair rates of the components are exactly known, the Markovian method (as well as any other method) yields a unique answer for the reliability of the system. In many instances, however, uncertainties exist about the various failure and repair rates. These uncertainties exist either because our knowledge of these quantities is incomplete (existing components that will operate in a different environment, new design, limited testing, etc.) or because these quantities are inherently uncertain. Uncertainties exist in particular for newly designed systems as the advanced reactor systems of the Liquid Metal Fast Breeder Reactor, the High Temperature Gas Cooled Reactor, the Gas Cooled Fast Breeder Reactor, etc. It follows that an uncertainty exists about the reliability of such systems, and an important question is "how does one calculate the uncertainty about the reliability of a system from the uncertainties about the reliability of the components of the system?" We will attempt to answer this question as follows.

We will assume that the uncertainties about the failure and repair rates of the components can be quantified by considering them as random variables, namely, variables with a range of values and probabilities associated with this range. Thus, the reliability of a system being a function of random variables becomes itself a random variable. We are interested then in calculating the range of values of the reliability and the probabilities associated with this range. The reason we want to determine the reliability (and the associated uncertainties) is because reliability is an important factor in evaluating the usefulness of a system.

Although all information about the reliability of the system would be included in the range of the values and the corresponding probabilities, reliability is seldom used in this form for evaluation or comparison purposes. Usually, other more compact evaluators of the reliability and the associated uncertainties are used. The problem of reliability analysis under uncertainty can be divided into the following three subproblems:

- (a) Determination of the probability density functions (pdf) of the transition rates of the components of a complex system;
- (b) Calculation of the pdf of the reliability of the complex system from the pdf's of the transition rates;
- (c) Derivation of evaluators from the random variable reliability.

For the purposes of this work we assumed that the nature of pdf's of the transition rates are given, and we developed methods for addressing subproblems (b) and (c).

As an illustration of the methodology that we developed, we evaluated the uncertainties about the reliability of the Shutdown System of the Clinch River Breeder Reactor (CRBR). In particular, we calculated the uncertainties associated with the probability of loss of coolable core geometry due to failure to scram on transient. Since the CRBR is a newly designed system, our knowledge about the failure rates of the components and other required statistical information is rather limited. For this reason, we expressed uncertainties by considering the various transition rates and probabilities as random variables distributed according to given probability density functions. Then we calculated the probability density function (pdf) of the failure probability of

the Shutdown System, and from this pdf we derived a confidence interval or probability band for the failure probability.

A Markov model was used for these calculations. The use of such a model permits the modeling of:

- (1) Common cause failures by allowing interdependences among the failure rates and the states of the components;
- (2) Interdependences between the unavailability of the Shutdown System and the occurrence of transients;
- (3) Inspection and maintenance procedures that depend on the state of the system and include the possibility of human errors.

The consideration of uncertainties and the inclusion of the above cited features in the model have a significant effect on the calculated failure probability of the Shutdown System of the CRBR. The failure rates, the repair rates, the rates at which transients occur, and all other input variables were assumed distributed in such a way that their upper 90% confidence limit is one order of magnitude higher than the lower 90% confidence limit. The latter limit is of the same order of magnitude as the most probable value of the quantity in question. The calculated lower 90% confidence limit, median, and upper 90% confidence limit of the CRBR Shutdown System failure probability per year are, respectively,  $2.1 \times 10^{-7}$ ,  $1.9 \times 10^{-6}$ , and  $1.8 \times 10^{-5}$ . This probability band is to be compared with the  $1 \times 10^{-9}$  point estimate of the failure probability when interdependences are not considered, the inspection is perfect, and the input variables are fixed at their mean values.

The dissertation is organized as follows.

Chapter 2 presents the basics of Markovian reliability analysis. In particular, it is shown how Markov processes can be used in the calculation of the time-dependent reliability and other related probabilities of an engineering system. Furthermore, a technique is presented for simplifying the structure of the transition probability matrix in order to reduce the numerical difficulties associated with models of large systems.

Chapter 3 presents another technique for further reducing the numerical difficulties of the problem by reducing the dimensions of the transition probability matrix. This is possible if the Markov process is mergeable, i.e., if its states can be merged to form superstates and if the resulting superstate-transition probabilities can be expressed only in terms of the transition probabilities of the process. It is shown that the Markov processes describing systems exhibiting symmetries (such as the safety systems of nuclear reactors) are mergeable and a systematic procedure for achieving the merging is presented.

Chapter 4 presents the mathematical statement of the problem of Markovian reliability analysis under uncertainty. The unfeasibility of an analytical solution and the need for numerical approximate solutions are discussed, the quantification of the uncertainties about the common cause failures is examined, and some analytical results for the 2x2 case are presented.

Chapter 5 deals with the moment matching technique for the approximate determination of the pdf of a random variable for which

only the first few moments are known. The various types of distributions fitted to the existing information, as well as a short discussion of the use of this technique in other studies for the description of uncertainties in the reliability of nuclear systems, are presented.

Chapter 6 presents the use of the Monte Carlo simulation technique for the determination of the moments of the reliability, and of other reliability evaluators. Techniques for reducing the necessary computing time by an appropriate choice of the time step of the process are also presented.

Chapter 7 presents the Taylor-series method for the calculation of the first few central moments of a function of random variables. The particular problems arising from the specific mathematical form of the reliability function in Markovian analyses are examined, and the advantages and limitations of this technique versus those of the Monte Carlo simulation are discussed.

Chapter 8 presents the assessment of the uncertainties about the failure probability of the Clinch River Breeder Reactor due to failure of the Shutdown System to scram on a transient. A description of the system, its mission, its reliability duty cycle, and of the model is given. The uncertainties about the failure rates and other input variables are defined and the pdf of the failure probability is derived.

Chapter 9 gives the summary and the conclusions of this work.

Finally, Chapter 10 presents recommendations for further studies.

## CHAPTER TWO

### MARKOV PROCESSES AND RELIABILITY ANALYSIS

#### 2.1 Introduction

In this chapter the basics of Markovian reliability analysis are presented. In particular, it is shown how the probabilistic behavior of an engineering system can be described by a Markov process and how the dynamic reliability and other related probabilities can be calculated from the resulting mathematical model. Furthermore, since the reliability analysis of large systems is of particular importance to this work, a technique is also presented for reducing the numerical difficulties associated with models of large systems. The material in this chapter is a summary of definitions of basic concepts, symbols, and assumptions that will be needed in the sequel. For a complete treatment of Markov processes, the reader is referred to Howard (1972) and Kemeny and Snell (1960). The application of Markov processes to reliability analysis is also discussed by Shooman (1969), Barlow and Prochan (1965), Billinton (1973), Sandler (1963), Green and Bourne (1972), Buzacott (1970), and Lee (1971). For a more detailed exposition of the technique for large systems see Papazoglou and Gyftopoulos (1974).

The chapter is organized as follows: Section 2 presents the basic assumptions, concepts, and definitions of Markovian reliability theory; Section 3 describes a technique for reducing the numerical difficulties of Markovian models of large systems; Section 4 discusses the analytical formulation of specific repair policies; and Section 5 presents the calculations of the time-dependent reliability and availability of a simple system.

## 2.2 Basic Assumptions and Definitions

- (i) A system consisting of  $N$  components is considered.
- (ii) Each component can be in  $k_v$  ( $v=1,2,\dots,N$ ) component-states.
- (iii) A component-state is defined by the way the component is functioning as well as by the way this functioning affects the function of the system and the other components.
- (iv) A system-state is defined by the component-states of the  $N$  components. The number  $z$  of possible system-states is given, therefore, by the number of permutations of  $k_v$  taken  $N$  at a time, or

$$z = \prod_{v=1}^N k_v . \quad (2.1)$$

If all the components can be in the same number of states, i.e., if  $k_1=k_2=\dots=k_N=k$ , then

$$z = k^N . \quad (2.1a)$$

The system changes its state, performs a state-transition, whenever one or more of its components change state.

- (v) The components (and therefore the system) can change state only at discrete times  $t_n$  where

$$t_n = t_{n-1} + \Delta t(n) , \quad (2.2)$$



or with  $\Delta t(n) = \text{constant}$ :

$$t_n = t_0 + n\Delta t \quad . \quad (2.2a)$$

- (vi) The process of changing the state of components is a random process and therefore the process of changing the system-state is also a random process.
- (vii) The probability that a component will change its state at time  $t_n$  depends only on the initial and final state of the component, on the time  $t_n$ , and on the states of the other components of the system at time  $t_n$ .

From assumptions (v) and (vii) it follows that the probability that the system will perform a state-transition from system-state  $i$  to system-state  $j$  at  $t_n$ , depends only on  $i$ ,  $j$ , and  $t_n$ . This probability is called the transition probability from state  $i$  to state  $j$  at  $t_n$  and is denoted by  $p_{ij}(n)$ .

From assumptions (iv), (v) and the property of the transition probabilities just cited, it follows that the random process of changing system-states is a discrete-state, discrete-time Markov process.

- (viii) The probability that the system will be in state  $i$  at  $t_n$  is called the state-probability and is denoted by  $\pi_i(n)$ .
- (ix) The  $z$  state-probabilities  $\pi_i(n)$  ( $i=1,2,\dots,z$ ), define a row vector with elements  $\pi_i(n)$ , called the state-probability vector and denoted by  $\underline{\pi}(n)$ .
- (x) The  $z^2$  transition probabilities  $p_{ij}(n)$   $i=1,2,\dots,z$ ,  $j=1,2,\dots,z$  define a square matrix of elements  $p_{ij}(n)$  called the

transition probability matrix and denoted by  $\underline{P}(n)$ . It can be shown that  $\underline{\pi}(n)$  obeys the relation: [see Howard (1972)]

$$\underline{\pi}(n + 1) = \underline{\pi}(n) \cdot \underline{P}(n) \quad , \quad (2.3)$$

where

$$0 \leq p_{ij}(n) \leq 1, \quad \sum_{j=1}^z p_{ij}(n) = 1 \quad (2.3a)$$

for  $i, j = 1, 2, \dots, z$  and  $n = 0, 1, 2, \dots$ ,

and

$$0 \leq \pi_i(n) \leq 1, \quad \sum_{i=1}^z \pi_i(n) = 1 \quad (2.3b)$$

for  $i = 1, 2, \dots, z$  and  $n = 0, 1, 2, \dots$ ,

If the transition probabilities are independent of time, then (2.3) yields

$$\underline{\pi}(n) = \underline{\pi}(0) \cdot \underline{P}^n \quad . \quad (2.4)$$

The set of the  $z$  possible states of the system is partitioned into two subsets  $X$  and  $Y$  such that:

- (xi) The set  $X$  contains all the states of the system in which its operation is considered successful. This set is called the set of operating states.
- (xii) The set  $Y$  contains all the states in which the system is considered failed. This set is called the set of failed states. Then, with the corresponding partition of  $\underline{\pi}(n)$  into subvectors  $\underline{\pi}(n+1, X)$  and  $\underline{\pi}(n+1, Y)$ , and of  $\underline{P}(n)$  into submatrices  $\underline{P}(n, X, X)$ ,  $\underline{P}(n, X, Y)$ ,  $\underline{P}(n, Y, X)$ ,  $\underline{P}(n, Y, Y)$  (2.3) can be written as

$$[\underline{\pi}(n+1, X), \underline{\pi}(n+1, Y)] = [\underline{\pi}(n, X), \underline{\pi}(n, Y)] \begin{bmatrix} \underline{P}(n, X, X) & \underline{P}(n, X, Y) \\ \underline{P}(n, Y, X) & \underline{P}(n, Y, Y) \end{bmatrix}. \quad (2.5)$$

- (xiii) The probability that the system will be operating at time  $n$  is equal to the probability that the system will occupy any of the operating states at time  $n$ . It is the availability,  $A(n)$ , at time  $n$  and is given by

$$A(n) = \sum_{i \in X} \pi_i(n, X). \quad (2.6)$$

- (xiv) The probability that the system will not leave the subset of operating states  $X$  during the time period from 0 up to  $n$  is equal to the probability that the system will occupy any of the operating states at time  $n$  given that transitions from subset  $Y$  back to subset  $X$  are not possible. It is the reliability,  $R(n)$ , at time  $n$  and is given by

$$R(n) = \sum_{i \in X} \pi_i(n, X), \quad (2.7)$$

where now  $\pi(n, X)$  is the solution of (2.5) with  $\underline{P}(n, Y, X) = \underline{0}$ ,  
i.e., the solution of

$$\pi(n+1, X) = \pi(n, X) P(n, X, X) \quad . \quad (2.8)$$

### 2.3 Linearization of Probabilities and Ordering of States

The solution of (2.5) requires the aid of a computer. When the number of possible states of a system is large, however, the necessary computer storage and computer time are prohibitive because of the large size of the transition probability matrix. For example, for a system consisting of 10 components, each having two possible states and constant failure and repair rates, the transition probability matrix has more than  $10^6$  elements.

The computational effort associated with (2.3) can be reduced by linearization of probabilities and by ordering states. Specifically, we will assume that each transition probability  $p_{ij}(n)$  is a linear function of the time step  $\Delta t$ , or that the size of  $\Delta t$  is such that transition probabilities among system-states differing in the states of two or more components can be neglected. Thus,

$$p_{ij}(n) = \begin{cases} h_{rg}^v(n|s(n)=i) \Delta t & \text{if } i \neq j \text{ and states } i \text{ and } j \text{ differ} \\ & \text{only in the state of component } v; \\ 0 & \text{if } i \neq j \text{ and states } i \text{ and } j \text{ differ in} \\ & \text{the state of more than one component;} \\ 1 - \sum_{\substack{m=1 \\ m \neq i}}^z p_{im}(n) & \text{if } i=j; \end{cases} \quad (2.9)$$

where  $h_{rg}^v(n|s(n)=i)$  is the conditional transition rate (probability per unit time) of the  $v$ -th component from component-state  $r$  to component-state  $g$  at time  $n$ , given that the state of the system at time  $n$   $[s(n)]$  is  $i$ . The conditional transition rate  $h_{rg}^v$  is of course equal to various conditional failure rates and repair rates of component  $v$ . The transition rate of each component at time  $n$  depends on the state of the system, namely, on the states of the other components, so common-cause failures are allowed. For example, the common-cause failure of two components can be modeled by assuming a certain conditional failure rate when both components are operating and a properly higher conditional failure rate when only one component is operating. (See also Section 2.6.)

The ordering of system-states is accomplished by partitioning the sets  $X$  of operating states and  $Y$  of failed states into subsets  $X(K)$ , for  $K=0,1,2,\dots,M$ , and  $Y(K)$ , for  $K=1,2,\dots,N$ , respectively, so that each state in either  $X(K)$  or  $Y(K)$  contains  $K$  failed components; in other words,  $X$  and  $Y$  are represented by the unions

$$X = X(0) \cup X(1) \cup \dots \cup X(M) , \quad (2.10)$$

$$Y = Y(1) \cup Y(2) \cup \dots \cup Y(N) , \quad (2.11)$$

where  $M$  is the maximum number of failed components with which the system can operate and  $N$  the total number of components. Similarly, we can order the state probability vectors  $\pi(n,X)$  and  $\pi(n,Y)$  into subvectors, and the transition probability submatrices  $P(n,X,X)$ ,  $P(n,X,Y)$ ,  $P(n,Y,X)$ , and  $P(n,Y,Y)$  into submatrices corresponding to the various subsets  $X(K)$  and  $Y(K)$ . Thus (2.5) becomes

$$[\underline{\pi}^0(n+1,X), \dots, \underline{\pi}^N(n+1,Y)] = [\underline{\pi}^0(n,X), \dots, \underline{\pi}^N(n,Y)] \begin{bmatrix} [\underline{p}^{IJ}]_{XX} & [\underline{p}^{IL}]_{XY} \\ [\underline{p}^{KJ}]_{YX} & [\underline{p}^{KL}]_{YY} \end{bmatrix}, \quad (2.12)$$

where  $I, J = 0, 1, 2, \dots, M$ ,  $K, L = 1, 2, \dots, M, \dots, N$ , and  $\underline{\pi}^K(n, X)$  corresponds to subset  $X(K)$ .

Moreover, by virtue of (2.9), it follows that

$$\underline{p}^{IJ} = \underline{p}^{IJ}(n, X, X) \begin{cases} \neq \underline{0} & \text{if } I=J-1 \text{ or } I=J \text{ or } I=J+1 \\ = \underline{0} & \text{otherwise;} \end{cases} \quad (2.13a)$$

$$\underline{p}^{KJ} = \underline{p}^{KJ}(n, Y, X) \begin{cases} \neq \underline{0} & \text{if } K=J+1 \\ = \underline{0} & \text{otherwise;} \end{cases} \quad (2.13b)$$

$$\underline{p}^{IL} = \underline{p}^{IL}(n, X, Y) \begin{cases} \neq \underline{0} & \text{if } I=L-1 \\ = \underline{0} & \text{otherwise;} \end{cases} \quad (2.13c)$$

$$\underline{p}^{KL} = \underline{p}^{KL}(n, Y, Y) \begin{cases} \neq \underline{0} & \text{if } K=L-1 \text{ or } K=L \text{ or } K=L+1 \\ = \underline{0} & \text{otherwise;} \end{cases} \quad (2.13d)$$

and that

$$\underline{P}(n) = \begin{bmatrix}
 \begin{array}{cccc|cccc}
 \underline{p}^{00} & \underline{p}^{01} & 0 & \dots & 0 & \underline{p}^{01} & 0 & 0 & \dots & 0 & \dots & 0 \\
 \underline{p}^{10} & \underline{p}^{11} & \underline{p}^{12} & \dots & 0 & 0 & \underline{p}^{12} & 0 & \dots & 0 & \dots & 0 \\
 \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
 0 & \cdot & \cdot & \cdot & \dots & \underline{p}^{MM} & 0 & \cdot & \cdot & \cdot & \dots & \underline{p}^{M,M+1} & \dots & 0
 \end{array} \\
 \hline
 \begin{array}{cccc|cccc}
 \underline{p}^{10} & 0 & 0 & \dots & 0 & \underline{p}^{11} & \underline{p}^{12} & 0 & \dots & 0 & \dots & 0 \\
 0 & \underline{p}^{21} & 0 & \dots & 0 & \underline{p}^{21} & \underline{p}^{22} & \underline{p}^{23} & \dots & 0 & \dots & 0 \\
 \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
 0 & \cdot & \cdot & \cdot & \dots & \underline{p}^{M+1,M} & 0 & \cdot & \cdot & \cdot & \dots & \underline{p}^{M+1,M+1} & \dots & 0 \\
 \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
 0 & \cdot & \cdot & \cdot & \dots & 0 & \cdot & \cdot & \dots & \dots & \dots & \dots & \dots & \underline{p}^{NN}
 \end{array}
 \end{bmatrix}, \quad (2.14)$$

where  $I, J = 0, 1, \dots, M$ , and  $K, L = 1, 2, \dots, M, \dots, N$ , and, for convenience, the time and subset dependence of the submatrices of matrices  $\underline{P}(n, X, X)$  etc. have been omitted from both (2.12) and (2.14).

From (2.13) and (2.14) it can be seen that linearization of probabilities and ordering of states reduce the numerical complexity of the problem in a systematic manner. For example, (2.13c) indicates that transitions from an operating state with  $I$  failed components to a failed state with  $L$  failed components is not possible if: (1)  $|I-L| > 1$ , namely, if more than one component-state transition must occur; and (2)  $I=L+1$ , namely, if a failed component is repaired, since such a repair in an operating state cannot bring the system into a failed state. Again (2.14) indicates that only  $5M+3N-1$  submatrices of the ordered  $\underline{P}(n)$  need be stored instead of the  $(M+N+1)^2$  submatrices of the unordered  $\underline{P}(n)$ . Moreover, the ordering results in computing-time savings because the solution of (2.5) is much faster when  $\underline{P}(n)$  is ordered than when it is not.

## 2.4 Repair Policies and Special Systems

For certain repair policies and certain special systems, some of the submatrices  $\underline{P}^{KL}$  in (2.14) are equal to zero. Four examples are given below.

a) No-online repair: If online repair is not possible, then submatrices  $\underline{P}^{IJ}$  of the lower diagonal stripe of  $\underline{P}(n, X, X)$  in (2.14), are equal to zero:

for no-online repair: in  $\underline{P}(n, X, X)$ ,  $\underline{P}^{I+1, I} = \underline{0}$  for  $1 \leq I \leq M$ . (2.15)

b) "Cold" standby operation: If the standby operation of a system is assumed "cold," that is if no components can fail while the system is not operating, then submatrices  $\underline{P}^{KL}$  of the upper diagonal stripe of  $\underline{P}(n, Y, Y)$  in (2.14) are equal to zero:

for "cold" standby operation: in  $\underline{P}(n, Y, Y)$ ,  $\underline{P}^{K-1, K} = \underline{0}$  for  $2 \leq K \leq N$ . (2.16)

c) Selective repair: In general, if a system is failed, the first component to be repaired can be any of the failed components. Under a selective repair policy, however, it might be possible to repair that particular component which brings the system back into operation. When a selective repair policy is possible, then submatrices  $\underline{P}^{K+1, K}$  of  $\underline{P}(n, Y, Y)$  in (2.14) are equal to zero for  $K \leq M + 1$ :

for a selective repair: in  $\underline{P}(n, Y, Y)$ ,  $\underline{P}^{K+1, K} = \underline{0}$  for  $K \leq M + 1$ . (2.17)

d) Components with one operating state: If a system consists of components that cannot transit between failed states and have only one operating state, then submatrices  $\underline{P}^{II}$  of  $\underline{P}(n, X, X)$  and  $\underline{P}^{KK}$  of  $\underline{P}(n, Y, Y)$  are diagonal because a system transition from a given state to another with the same number of failed components requires at least the simultaneous repair and failure of two different components:



for systems consisting of components with one operating state:

$$\text{in } \underline{P}(n, X, X), \underline{P}^{II} = [\delta_{ij} p_{ij}(n)]^{II} \text{ for } I = 0, 1, 2, \dots, M$$

and

$$\text{in } \underline{P}(n, Y, Y), \underline{P}^{KK} = [\delta_{ij} p_{ij}(n)]^{KK} \text{ for } K = 1, 2, \dots, N, (2.18)$$

where  $\delta_{ij}$  is the Kronecker delta.

## 2.5 An Application

As an illustration of the methodology developed in Sections 2.2 to 2.4, the time-dependent availability and reliability of the system shown in Figure 2.1 has been calculated. The following assumptions were made about the system:

1) The system consists of two pumps and four valves. Each pump can supply the required flow rate, but when both are operating each is operating at half capacity. The pumps can be in two states: operating and failed. Two valves are associated with each pump. The function of the valves is to isolate the corresponding pump when it fails. Each valve can be in three states: operating, failed in the open position, and failed in the closed position.

2) The mission of the system is to supply point B with water at a certain flow rate and for a certain period of time T, and under a known environment.

3) The various failure and repair rates are listed in Table 2.1. They do not correspond to real data but have been selected solely for illustration purposes. The following statistical dependences due to different operating conditions, repair capabilities, and possible

common cause failures, have been assumed:

a) The failure rate of each pump is equal to  $k_{pi}\lambda(i=0,1)$ , where  $i$  is the number of failed pumps and  $k_{p0}=1$ . Similarly, the failure rate of each valve is equal to  $k_{vi}\lambda_{vj}(i=0,1,2,3 \text{ and } j=1,2)$ , where  $i$  denotes the number of failed valves,  $j$  the failure mode (open or closed position), and  $k_{v0}=1$ ;

b) Every repair is perfect. The repair rate of each pump is equal to  $d_{pi}r_p(i=1,2 \text{ and } d_{p1}=1)$ , where  $i$  denotes the number of failed pumps. The repair rate of each valve is equal to  $d_{vi}r_{vj}(i=1,2,3,4; j=1,2 \text{ and } d_{v1}=1)$ .

A computer code, described briefly in Appendix A, has been written to perform the calculations according to the methodology developed in Sections 4 and 5. The results are summarized in Figures 2.2 and 2.3. In Figure 2.2, curves 1 and 2 represent the unavailability of the system as a function of time with or without statistical dependences among the failure repair rates, respectively, and curve 3 represents the unavailability of the system if online repair is not possible. Figure 2.3 presents analogous results for the unreliability of the system.

TABLE 2.1 Conditional failure and repair rates of the components of system in Figure 2.1

	Conditional failure rates (per $10^6$ hr)		Conditional repair rates (per $10^6$ hr)	
Pumps				
Two Up	30		-	
One Up	3000		10000	
None Up	-		5000	
Valves	to the "open position"	to the "closed position"	from the "open position"	from the "closed position"
Four Up	1	1	-	-
Three Up	5	5	1000	1000
Two Up	10	10	500	500
One Up	100	100	300	300
None Up	-	-	100	100

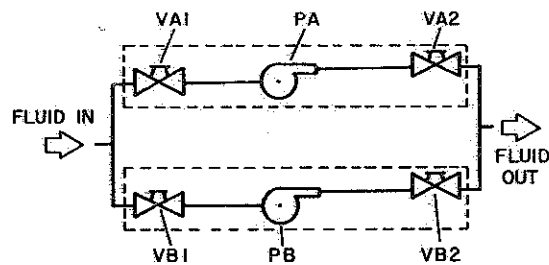


Figure 2.1. Sample system.

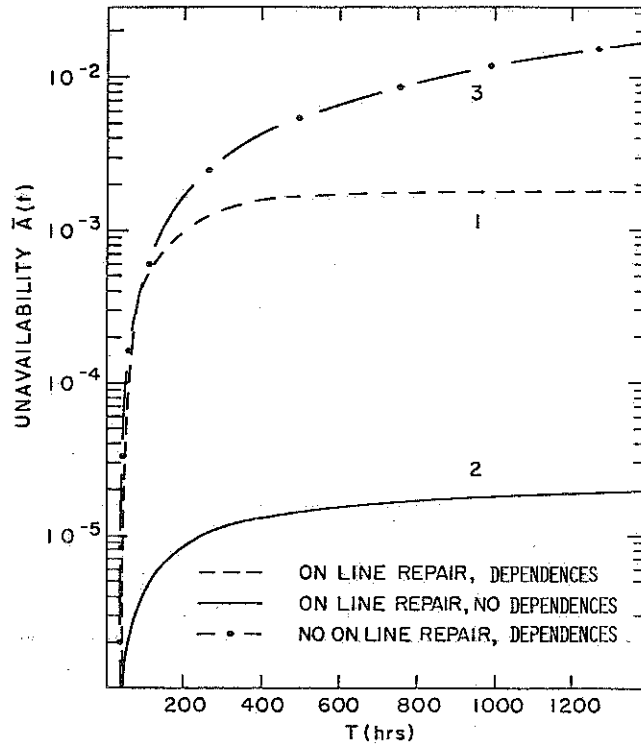


Figure 2.2. Time-dependent unavailability of the sample system.

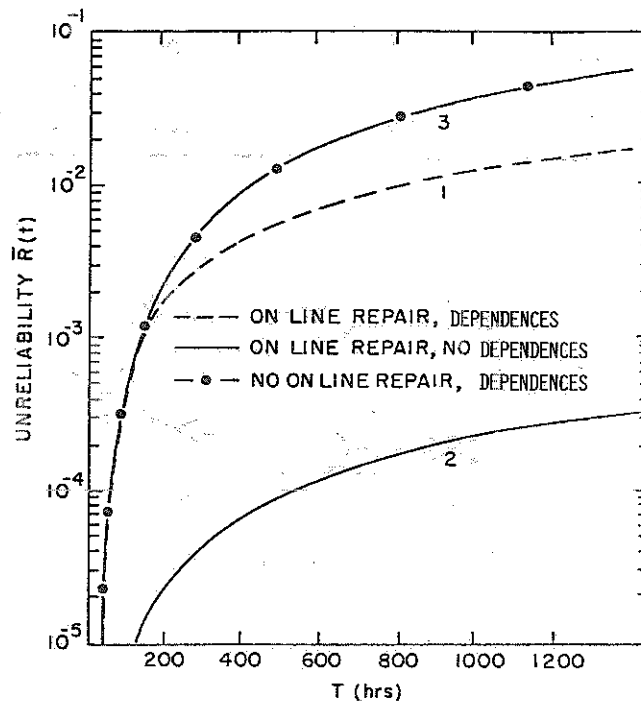


Figure 2.3. Time-dependent unreliability of the sample system.

## CHAPTER THREE

### MERGEABLE MARKOV PROCESSES

#### 3.1 Introduction

The computational effort involved in evaluations of the reliability and availability can be substantially reduced if the Markov process describing the probabilistic behavior of the system is mergeable. The theory of mergeable Markov processes is presented in this chapter.

From (2.6) and (2.7) it follows that the reliability of a system can be calculated if partial sums of  $\pi_i(n, X)$ 's can be obtained. A sum of state-probabilities  $\pi_i(n, X)$ 's is equal to the probability that the system will be in any of the individual states that form this sum. If a new process could be formed, therefore, such that its states consist of groups of states of the original process and if this new process is Markovian, then the new state-probabilities would provide the partial sums necessary for the calculation of  $A(n)$  or  $R(n)$  in (2.6) or (2.7). A Markov process, the states of which can be grouped together to form superstates in such a way that the result is also a Markov process, is called mergeable (for a more complete definition see Subsection 3.2). Because the number of superstates of a merged Markov process is much smaller than the number of original states, the dimensions of the probability vector and transition matrix of the superstates are much smaller than those of the original states, and, therefore, the computational effort is substantially reduced.

Given a certain grouping of states of a process, there is a necessary and sufficient condition that the transition probabilities of the

original process must satisfy for the resulting merged process to be Markovian. This condition, called henceforth the mergeability criterion, has been presented by Buzacott (1970), Bacon (1964), Singh and Billinton (1975), Howard (1972), Papazoglou and Gyftopoulos (1974), and Kemeny and Snell (1960). The creation of all possible combinations in which the states of a Markov process can be grouped into superstates, and the testing for the satisfaction of the mergeability criterion, is for all practical purposes impossible. It is shown in this chapter, however, that the Markov processes describing systems exhibiting certain symmetries are mergeable. In addition, a systematic way for achieving the merging is presented.

This chapter is organized as follows: Section 3.2 presents the definition of mergeable Markov processes and derives the mergeability criterion; Section 3.3 gives the definition of system-symmetries and the proof that the corresponding Markov processes are mergeable; Section 3.4 provides a brief description of a computer code that achieves the merging and a numerical example.

### 3.2 Mergeable Markov Processes and the Mergeability Criterion

Let the random process describing the probabilistic behavior of a system be a  $z$ -state Markov process. Let  $T = (T_1, T_2, \dots, T_I, \dots, T_M)$  denote a partition of the set of the  $z$  states into  $M$  groups of states. In terms of these  $M$  groups a new random process can be defined as follows: the system is in the  $I$ -th state of the new process whenever it is in any of the states that belong to subset  $T_I$  (that form group  $I$ ). If  $s(n)=i$  denote the event "system is in state  $i$  at  $t_n$ " and  $S(n)=I$  the

event "system is in state I of the new process at  $t_n$ ", then the new process can be defined symbolically as

$$\{S(n) = I\} \text{ if and only if } \{s(n) = i \text{ and } i \in T_I\} . \quad (3.1)$$

This new process is called the collapsed process, and its states are called superstates. In general, the prefix super will refer to the collapsed process. The definition of a mergeable Markov process is now possible.

Definition 3.2.1 A Markov process is called mergeable with respect to a partition  $T = \{T_1, T_2, \dots, T_M\}$  if for every initial state-probability vector  $\pi(0)$ , the collapsed process defined in (3.1) is a Markov process and the new supertransition probabilities do not depend on the choice of  $\pi(0)$ .

It will be seen later that requiring the supertransition probabilities to be independent of  $\pi(0)$  is equivalent to requiring that they be calculated from the transition probabilities of the original process only. Before deriving the mergeability criterion for a Markov process, the following definitions and lemma are necessary.

Let  $p_{ij}(n)$  denote the probability that the system will transit from state  $i$  to superstate  $J$  at  $t_n$ . Then

$$p_{iJ}(n) \equiv \Pr \{S(n+1) = J \mid s(n) = i\} = \sum_{j \in J} p_{ij}(n) . \quad (3.2)$$

Let  $p_{IJ}(n)$  denote the probability that the system will transit from superstate I to superstate J at  $t_n$ . We will show that:

Lemma 3.2.1 The superstate transition probability of collapsed process,  $p_{IJ}(n)$ , is expressed in terms of the state probabilities and the transition probabilities of the original process by the relation:

$$p_{IJ}(n) = \frac{\sum_{i \in T_I} \pi_i(n) \sum_{j \in T_J} p_{ij}(n)}{\sum_{i \in T_I} \pi_i(n)} . \quad (3.3)$$

Proof Let event A be the transition of the system from superstate I to superstate J, or symbolically:

$$A \equiv \{S(n) = I \text{ and } S(n+1) = J\} . \quad (3.4)$$

The probability of occurrence of A can be expressed in two ways:

(1) Since the system is in superstate I whenever it is in any of the states of subset  $T_I$ , it follows from (3.4) that

$$\Pr\{A\} = \sum_{i \in T_I} \Pr\{s(n) = i \text{ and } S(n+1) = J\} ,$$

which in view of the relation

$$\Pr\{B \cdot C\} = \Pr\{B\} \cdot \Pr\{C/B\} \quad (3.5)$$

can be written as



$$\Pr\{A\} = \sum_{i \in T_I} \Pr\{s(n) = i\} \cdot \Pr\{S(n+1) = J | s(n) = i\}$$

or

$$\Pr\{A\} = \sum_{i \in T_I} \pi_i(n) p_{iJ}(n) \quad . \quad (3.6)$$

(2) By virtue of (3.4) and (3.5), it follows that

$$\Pr\{A\} = \Pr\{S(n) = I\} \cdot \Pr\{S(n+1) = J | S(n) = I\} \quad , \quad (3.7)$$

or

$$\Pr\{A\} = \pi_I(n) \cdot p_{IJ}(n) \quad , \quad (3.8)$$

where

$$\pi_I(n) \equiv \Pr\{S(n) = I\} \quad . \quad (3.9)$$

The combination of (3.6) and (3.8) yields

$$p_{IJ}(n) = \frac{\sum_{i \in T_I} \pi_i(n) p_{iJ}(n)}{\pi_I(n)} \quad (3.10)$$

which in view of (3.2) and (3.1) is equivalent to (3.3). The following proposition can now be proved about mergeable processes.

Proposition 3.2.1 A necessary and sufficient condition for a Markov process to be mergeable with respect to a partition  $T = \{T_1, T_2, \dots, T_I, \dots, T_M\}$  is that for every pair of sets

$T_I, T_J$ , the transition probability  $p_{ij}(n)$ , from a state  $i$  of  $I$  to superstate  $J$  has the same value for all the states of superstate  $I$ . Symbolically:

$$\sum_{j \in T_J} p_{ij}(n) = \sum_{j \in T_J} p_{kj}(n) \text{ all } i, k \in I, \text{ all } T_I, T_J \in T. \quad (3.11)$$

Proof We first prove the necessity. From Definition 3.2.1 it follows that the value of the transition probabilities of the new process is independent of the initial state-probability vector  $\underline{\pi}(0)$ . Considering a  $\underline{\pi}(0)$  with all its elements equal to zero but the element corresponding to the  $i$ -th state of  $T_I$ , which is equal to one, (3.3) for  $n=0$  yields

$$p_{IJ}(0) = \sum_{j \in T_J} p_{ij}(0). \quad (3.12)$$

Since  $p_{IJ}(0)$  has the same value for all  $\underline{\pi}(0)$  and  $i$  was arbitrary, (3.12) holds for all  $i$  in  $T_I$ , and the necessity of (3.11) has been proved.

For the sufficiency of (3.11) we notice that from (3.10) it follows that  $p_{IJ}(n)$  depends only on superstates  $I, J$  and, therefore, the new process is a Markov process. Furthermore, by virtue of (3.11) and (3.3), it follows that

$$p_{IJ}(n) = \sum_{j \in T_J} p_{ij}(n) \frac{\sum_{i \in T_I} \pi_i(n)}{\sum_{i \in T_I} \pi_i(n)} = \sum_{j \in T_J} p_{ij}(n),$$

and, therefore, the  $p_{IJ}(n)$ 's depend only on the  $p_{ij}(n)$ 's of the initial process and not on  $\pi(0)$ .

Whenever a partition  $T = \{T_1, \dots, T_M\}$  of the set of states of a Markov process can be found such that the mergeability criterion (3.11) is satisfied, then the transition probability matrix of the merged process can be defined in terms of the transition probabilities of the original process only. The solution of (2.3) for the new process is then possible, and since the number of superstates is substantially smaller than the number of the original states, the computational effort associated with the solution of (2.6) and (2.7) is greatly reduced. Throughout this section it was assumed that the partition  $T$  was given and the question of whether the process is mergeable or not with respect to this particular partition was answered. A much more difficult question to answer is whether, given a Markov process, there is a partition with respect to which the process is mergeable, and if the answer is yes, how this partition can be found. A general answer to this question is not known, and a straightforward approach of creating all the possible partitions of the set of states and testing each one against criterion (3.11) is self-defeating. In the next two sections it is shown, however, that for Markov processes describing systems exhibiting certain properties there is a partition with respect to which these processes are mergeable. A systematic way to create this partition is also presented.

### 3.3 On the Mergeability of Markov Processes of Systems Exhibiting Symmetries

In this section it is shown that for systems exhibiting certain

symmetries there exists a partition of the set of possible states with respect to which the corresponding Markov process is mergeable. For a given system, symmetries may exist between components, or between subsystems of varying degrees of complexity. We will define these symmetries explicitly in the next two subsections. Here we would like to indicate that highly redundant systems such as the safety systems of a nuclear reactor exhibit these two kinds of symmetries.

### 3.3.1 Systems exhibiting symmetries at the component-level

Whenever symmetries in a system exist among its components, they are called symmetries at a component-level. These symmetries are defined as follows:

Definition 3.3.1 Two components of a system are symmetrical

if and only if:

- (1) each component can be in the same number of states as the other;
- (2) each component has the same conditional failure rates and conditional repair rates as the other;
- (3) for any operating (failed) system-state, interchanging only the states of the two components results in an operating (failed) system-state.

Note that a component is trivially symmetrical to itself.

Definition 3.3.2 A group of components each of which is symmetrical to all the others in the group forms a class of components.

A system can have many classes. Note that a class may contain only one component.

Definition 3.3.3 A system is exhibiting symmetries at a component level if and only if it has at least one class containing more than one component.

Symmetries at a component-level are demonstrated in the following example.

Example 3.1 The sample system considered in Section 2.5 has symmetries at a component-level. Indeed, valve VA1 is symmetrical to valve VA2 and valve VB1 is symmetrical to valve VB2 (see figure 2.1). The system has four classes of components; class 1 containing pump PA, class 2 containing pump PB, class 3 containing valves VA1 and VA2, and class 4 containing valves VB1 and VB2. It must be noted that pumps PA and PB are not symmetrical since condition (3) of Definition 3.3.1 does not hold. Indeed, if system-state *i* and *j* are as shown in listings (a) and (b) below, then we note *i* is an operating state, *j* a failed state, and yet *j* is generated from *i* by interchanging the states of pumps PA and PB.

COMP	PA	PB	VA1	VA2	VB1	VB2	SYSTEM	
STATE	UP	FAILED	UP	UP	UP	FAILED CLOSED	OPERATING	(a)

COMP	PA	PB	VA1	VA2	VB1	VB2	SYSTEM	
STATE	FAILED	UP	UP	UP	UP	FAILED CLOSED	FAILED	(b)

We will now prove that systems symmetrical at a component level are described by mergeable Markov processes. This will be proved by Proposition 3.3.1 and for that purpose the following definitions and lemmas are necessary.

Let a system have  $c$  classes of components, where

$$1 \leq c \leq N, \quad (3.13)$$

$N$  being the total number of components. Let  $t(r)$  denote the number of states of the components of the  $r$ -th ( $r=1, \dots, c$ ) class. Then for each system-state, let  $a_m^r$  for  $r=1, 2, \dots, c$ , and  $m=1, 2, \dots, t(r)$ , denote the number of the components that belong to the  $r$ -th class and are in the  $m$ -th state.

Definition 3.3.4 The one-dimensional array  $L_v$ , where

$$L_v = \{a_1^1, a_2^1, \dots, a_{t(1)}^1, \dots, a_m^r, \dots, a_1^c, a_2^c, \dots, a_{t(c)}^c\},$$

is called a state-label where  $v$  is an index varying over all the possible state labels.

Thus, to each system-state a label  $L_v$  can be assigned where  $v=1, 2, \dots, M$ ,  $M$  being the total number of different labels. Note that if there are no symmetrical components in the system, then there are  $c=N$  classes of components each containing one component,  $a_m^r$  can only have the value of zero or one, and there are as many state-labels as system-states.

Example 3.2 The labels of the system-states of the sample system have the following form

$$L_v = \{a_1^1, a_2^1 | a_1^2, a_2^2 | a_1^3, a_2^3, a_3^3 | a_1^4, a_2^4, a_3^4\}, \quad (a)$$

since the system has four classes and the components of the first two classes can be in two states while the components of the last two classes can be in three states. The labels of states  $i$  and  $j$  considered in example 3.1 are, respectively,

$$L_\mu = \{1, 0 | 0, 1 | 2, 0, 0 | 1, 0, 1\} \quad (b)$$

$$L_\rho = \{0, 1 | 1, 0 | 2, 0, 0 | 1, 0, 1\} . \quad (c)$$

The following lemmas are now proved.

Lemma 3.3.1 A transition between two states of a Markov process is possible only if the labels of these states differ in the values of only two of their elements that correspond to components of the same class, one of these differences being equal to unity and the other being equal to minus unity.

Proof Let  $i$  be a system-state with label  $L_v$ , where

$$L_v = \{a_1^1(v), a_2^1(v), \dots, a_m^r(v), \dots, a_h^r(v), \dots, a_1^c(v), \dots, a_{t(c)}^c(v)\} .$$

Let  $j$  be a system-state that can be reached from  $i$  in one transition. Since only one component can change state at the end of each time step [see Section 2.3, Eq. (2.9)], let system state  $j$  be the state that results if a component of class  $r$  in component-state  $m$  changes its state to  $h$ . Thus, system-state  $j$  differs from system-state  $i$  only in that it

has one fewer component of class  $r$  in component-state  $m$ , while it has one more component of class  $r$  in component-state  $h$ . Its label is, therefore,

$$L_\rho = \{a_1^1(\rho), a_2^1(\rho), \dots, a_m^r(\rho), \dots, a_h^r(\rho), a_1^c(\rho), \dots, a_{t(c)}^c(\rho)\} ,$$

where

$$a_k^t(\rho) \left\{ \begin{array}{ll} = a_m^r(v) - 1 & \text{if } t = r \text{ and } k = m \\ = a_h^r(v) + 1 & \text{if } t = r \text{ and } k = h \\ = a_k^t(v) & \text{if } t \neq r, k \neq m \text{ and } k \neq h \end{array} \right. \quad (3.14)$$

Equation (3.14) shows that the label of system-state  $j$  differs from the label of system-state  $i$  in the values of only two elements. Furthermore, these elements correspond to components belonging to the same class ( $r$ ), and have values that differ by  $\pm 1$  from those for state  $i$ . Since class  $r$  and states  $m$  and  $h$  were completely arbitrary, it has been proved that the labels of all the states that can be reached by one transition from system-state  $i$  have the characteristics cited in Lemma 3.3.1. This completes the proof.

Example 3.3 The states that can be reached from state  $i$  considered in Example 3.1 and the corresponding labels are given below, and indeed Lemma 3.3.1 holds for the label of state  $i$  and the labels of the 9 states that can be reached from state  $i$  by one transition.



STATE	PA	PB	VA1	VA2	VB1	VB2	STATE LABEL
i	UP	Failed	UP	UP	UP	FC	{1,0 0,1 2,0,0 1,0,1}
i <sub>1</sub>	UP	UP	UP	UP	UP	FC	{1,0 1,0 2,0,0 1,0,1}
i <sub>2</sub>	Failed	Failed	UP	UP	UP	FC	{0,1 0,1 2,0,0 1,0,1}
i <sub>3</sub>	UP	Failed	FO	UP	UP	FC	{1,0 0,1 1,1,0 1,0,1}
i <sub>4</sub>	UP	Failed	UP	FO	UP	FC	
i <sub>5</sub>	UP	Failed	FC	UP	UP	FC	{1,0 0,1 1,0,1 1,0,1}
i <sub>6</sub>	UP	Failed	UP	FC	UP	FC	
i <sub>7</sub>	UP	Failed	UP	UP	FO	FC	{1,0 0,1 2,0,0 0,1,1}
i <sub>8</sub>	UP	Failed	UP	UP	FC	FC	{1,0 0,1 2,0,0 0,0,2}
i <sub>9</sub>	UP	Failed	UP	UP	UP	UP	{1,0 0,1 2,0,0 2,0,0}

Lemma 3.3.2 States with the same label  $L_v$  are all either operating or failed and belong to the same group  $X(K)$  or  $Y(K)$ , respectively.

Proof Lemma 3.3.2 will be first proved for two system-states  $i$  and  $j$  which differ in the component-states of only class  $r$ . Let  $b(r)$  ( $r=1,2,\dots,c$ ) denote the number of components that belong to the  $r$ -th class. Since the system-states  $i$  and  $j$  have the same label  $L_v$ , it follows from Definition 3.3.4 that they both have  $a_m^r$  components of the  $r$ -th class in the  $m$ -th state for  $m=1,2,\dots,t(r)$ . Furthermore, since

$$b(r) = \sum_{m=1}^{t(r)} a_m^r ,$$

the components of the  $r$ -th class in these two states can be viewed as two different permutations of a collection of  $b(r)$  items,  $a_m^r$  ( $m=1,2,\dots,t(r)$ )

of which are of the same kind. It is known from the theory of permutations that given any two permutations of  $N$  items, the second can always be constructed from the first by successive interchanges of the position of the elements of the first taken two at a time. This means that system-state  $j$  can always be constructed from system-state  $i$  by successively interchanging the states of the components of class  $r$ , taken two at a time. But since all the components of a class are symmetrical, it follows from Definition 3.3.1, part (3), that all the states generated according to this procedure are of the same kind as state  $i$  (operating or failed). Therefore, system-state  $j$  is of the same kind as  $i$ .

We will now prove that Lemma 3.3.2 is true for two system-states  $i, j$  differing in the component-states of any number  $\alpha$  of classes. Indeed, as already shown starting with system-state  $i$ , we can construct a system-state  $i_1$  that differs from  $j$  in the component-states of  $\alpha-1$  classes. Then a system-state  $i_2$  can be constructed that differs from  $j$  in  $\alpha-2$  classes and so on, until  $j$  itself will be constructed. But according to part one of this proof the pairs of system-states  $(i, i_1)$ ,  $(i_1, i_2), \dots, (i_{\alpha-1}, j)$  are all of the same kind and, therefore, states  $i$  and  $j$  are of the same kind.

We will now show that states with the same label belong to the same subset  $X(k)$  or  $Y(K)$  (see Section 2.2). Since it has been proved that states with the same label are of the same kind, we need only to show that they have the same number of failed components. If  $K$  denotes this number, then for a state  $i$

$$K = \sum_{r=1}^c \sum_m a_m^r, \quad (3.15)$$

where the second summation extends over all the failed component-states of class  $r$ .

But since any two states with the same label have the same  $a_m^r$ s (all  $r$  and  $m$ ), it follows from (3.15) that they have the same number of failed components. This completes the proof of Lemma 3.3.2.

Example 3.4 As an illustration of Lemma 3.3.2, the following two states of the sample system having the same label are considered

STATE	PA	PB	VA1	VA2	VB1	VB2	LABEL
i	UP	Failed	FO	UP	UP	FC	{1,0 0,1 1,1,0 1,0,1}
j	UP	Failed	UP	FO	FC	UP	

State  $j$  can be constructed from state  $i$  by successive interchanges of state of symmetrical components. Indeed:

STATE	PA	PB	VA1	VA2	VB1	VB2	SYSTEM	COMMON LABEL
i	UP	Failed	FO	UP	UP	FC	Operating	{1,0 0,1 1,1,0 1,0,1}
i <sub>1</sub>	UP	Failed	UP	FO	UP	FC	Operating	
j	UP	Failed	UP	FO	FC	UP	Operating	

The following proposition can now be proved.

Proposition 3.3.1 Let each of the states of a system exhibiting symmetries at a component level be labeled with a label  $L_v$ , and let  $T = \{T_1, T_2, \dots, T_v, \dots, T_M\}$  be a partition of the set of system-states such that a system-state belongs to  $T_v$  if and only if it has a label  $L_v$ . Then

(1) the Markov process describing the system is mergeable with respect to partition  $T$ ,

and

(2) the superstates generated by partition  $T$  are either operating or failed.

Proof To prove part (1) of this proposition, it suffices to show that criterion (3.11) is satisfied by any two superstates created by partition  $T$ . Let  $I_v, J_\rho$  be any two superstates containing system-states with labels  $L_v$  and  $L_\rho$ , respectively. If labels  $L_v$  and  $L_\rho$  are such that a transition is not possible between system-states of superstates  $I_v$  and  $J_\rho$  (see Lemma 3.3.1), criterion (3.11) is trivially satisfied. Let now  $L_v$  and  $L_\rho$  be such that a transition is possible between  $I_v$  and  $J_\rho$  (see Lemma 3.3.1). More explicitly, let

$$L_v = \{a_1^1, \dots, a_{t(1)}^1, \dots, a_1^r, \dots, a_m^r, \dots, a_k^r, \dots, a_{t(r)}^r, \dots, a_1^c, \dots, a_{t(c)}^c\} , \quad (3.16)$$

and

$$L_\rho = \{a_1^1, \dots, a_{t(1)}^1, \dots, a_1^r, \dots, a_m^{r-1}, \dots, a_k^{r+1}, \dots, a_{t(r)}^r, \dots, a_1^c, \dots, a_{t(c)}^c\} . \quad (3.17)$$

Let  $i$  be a system-state of superstate  $I_v$ . The transition probability  $p_{ij}(n)$  from system-state  $i$  to superstate  $J_\rho$  can be calculated as follows. System-state  $i$  has a label  $L_v$  given in (3.16). If, therefore, one of the components of class  $r$  changes its state from component-state  $m$  to component-state  $k$ , the system performs a state transition from system-state  $i$  to system-state  $j$  having label  $L_\rho$  given in (3.17). The transition probability for this transition is given by [see (2.9)]

$$p_{ij}(n) = h_{mk}(n|S(n)=I_v)\Delta t \quad . \quad (3.18)$$

There are  $a_m^r$  different system-states with label  $L_\rho$  that can be reached from system-state  $i$ , since the latter has  $a_m^r$  components of class  $r$  in component-state  $m$  [see (3.16)]. In addition, because of the way superstate  $J_\rho$  was formed, all  $a_m^r$  system-states are contained in  $J_\rho$ . Furthermore, the transitions from system-state  $i$  to any of the  $a_m^r$  system-states have the same transition probabilities, namely, that given in (3.18). This is true because these transitions correspond to changes in component-states of components that are symmetrical since they belong to the same class, and therefore by virtue of Definition 3.3.1 they have the same transition rates. The transition probability from state  $i$  to any other state of superstate  $J_\rho$  is equal to zero because it would require the change of state of more than one component. It has been proved, therefore, that

$$p_{ij}(n) = \sum_{j \in J} p_{ij}(n) = a_m^r \cdot h_{mk}^r(n|I_v)\Delta t \quad \text{for all } i \in I_v \quad . \quad (3.19)$$

Since labels  $L_v$ ,  $L_p$  were arbitrary, criterion (3.11) is satisfied by any pair of superstates created by partition  $T$  and the proof of part (1) has been completed.

Part (2) of this proposition follows immediately from Lemma 3.3.2. Furthermore, from the same lemma it follows that each superstate contains system-states that belong to the same group  $X(K)$  or  $Y(K)$  (see Section 2.3).

Part (2) of Proposition 3.3.1 is of major importance to reliability analysis because it proves that the merging procedure does not mix operating with failed system-states and, therefore, the resulting Markov process is suitable for reliability calculations [see (2.6) and (2.7)]. Furthermore, since each superstate is formed within the subsets  $X(K)$  or  $Y(K)$ , the transition probability matrix of the merged process retains the simple structure of (2.14).

### 3.3.2 Systems exhibiting symmetries at the subsystem level

Whenever symmetries among groups of components rather than among individual components exist in a system, they are called symmetries at a subsystem-level. These symmetries are formally defined as follows:

Definition 3.3.5 Any partial collection of components of a system forms a subsystem.

Note that a subsystem may consist of only one component.

Definition 3.3.6 A subsystem-state is defined whenever the states of the components that belong to the subsystem are defined.

In a complete analogy to symmetrical components and classes of

components, symmetrical subsystems and classes of subsystems can now be defined.

Definition 3.3.7 Two subsystems are symmetrical if and only if:

- (1) There is a one-to-one correspondence between the components of the two subsystems such that two corresponding components can be in the same number of states and have the same failure and repair rates.
- (2) For any operating (failed) system-state, interchanging only the states of the corresponding components of the two subsystems results in an operating (failed) system-state.

Definition 3.3.8 A group of subsystems each of which is symmetric to all the others is said to form a class of subsystems.

A system can have many classes of subsystems. Note that a class may contain only one subsystem.

Definition 3.3.9 A system exhibits symmetries of a subsystem level if and only if it has at least one subsystem class containing more than one subsystem.

Example 3.5 The sample system considered in Section 2.6 also exhibits symmetries at subsystem level. Indeed, each leg of the system can be considered as a subsystem. The sample system consists, therefore, of subsystem A containing components PA, VA1 and VA2 and subsystem B containing components PB, VB1, VB2. Furthermore, these two subsystems are symmetrical and form the only class of subsystems of the sample system.

To prove that the Markov processes describing systems with symmetries at a subsystem level are mergeable, a procedure completely parallel to the one for systems with symmetries at a component level could be followed. This would require the definition of state labels describing the states of subsystems and so on (see Section 3.3.1). Instead, an equivalency between the two kinds of symmetries will be shown.

Definition 3.3.10 Two systems are equivalent if and only if:

- (1) They can be in the same number of states.
- (2) A one-to-one correspondence exists among the states of the two systems such that corresponding transition probabilities are equal and corresponding states are of the same kind (operating or failed).

The following proposition follows immediately from Definition 3.3.10.

Proposition 3.3.1 Two equivalent systems are described by the same Markov process.

Proposition 3.3.2 For every system exhibiting symmetries at a subsystem level there exists an equivalent system exhibiting symmetries at a component level.

Proof Let  $Q$  be a system exhibiting symmetries of a subsystem level.

A new system  $W$  is then defined as follows:

- (1) Every subsystem of system  $Q$  is substituted by an equivalent component such that:



- (1.a) the component can be in as many states as the states of the subsystem;
  - (1.b) the transition probabilities among the states of the component are equal to the transition probabilities of the corresponding states of the subsystem;
  - (1.c) the function of the component in each state is exactly the same as the function of the subsystem in the corresponding states.
- (2) The equivalent components defined in step (1) are logically connected to form system W in exactly the same way as the subsystems are connected in system Q.

In other words, the subsystems of system Q are replaced with "black boxes," i.e., the components of system W. By virtue of Definitions 3.3.7 and 3.3.1, it follows then that to symmetrical subsystems of system Q correspond symmetrical components of system W. From Definitions 3.3.9 and 3.3.3, it follows, therefore, that if system Q exhibits symmetries at a subsystem level, system W exhibits symmetries at a component level.

Corollary 3.3.2 The Markov process describing a system exhibiting symmetries at a subsystem level is mergeable.

Indeed, from Propositions 3.3.1 and 3.3.2, it follows that the Markov processes describing a system exhibiting symmetries at a subsystem level is the same with the Markov process describing a system exhibiting symmetries at a component level which by Proposition 3.3.1 is mergeable.

Example 3.6 The equivalent to the sample system is shown in Figure 3.1. System W consists of two components, each of which can be in 18 states (as many as each subsystem). The number of system-states for W is, therefore, equal to

$$z = 18^2 = 324 \quad (\text{see 2.1a})$$

equal to number of states of the original system.

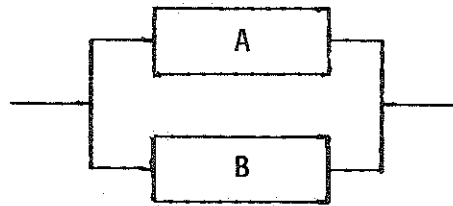


Figure 3.1 Equivalent System to System Shown in Figure 2.1.

#### 3.4 Automated Merging of a Markov Process by a Computer

Based on the theory developed in Section 3.3, a computer code has been written that performs the merging of a Markov process describing systems with symmetries at a component and/or a subsystem level. Two versions of this code are available, one being faster than the other but requiring more information as an input. Once the transition probability matrix of the merged process is defined, Eq. (2.3) is solved as in any other case (see Chapter 2). Therefore, only the steps necessary for the creation of the transition probability matrix will be described in this section. A more detailed description of this code can be found in Appendix B.

Version 1 is based on the fact that the transition probabilities among superstates depend only on the labels of the initial and final superstates [see (3.19)].

Version 1. The input for version 1 consists of:

- (1) a description of the symmetries of the system, namely:
  - (1a) the number of classes of components;
  - (1b) the number of components in each class;
  - (1c) the number of states and each component in each class as well as the corresponding transition rates.
- (2) a test subroutine providing the criterion of whether a superstate is operating or failed.

The code then proceeds in the following steps:

- (1) It generates all possible state labels.
- (2) By virtue of the "test" subroutine, it partitions the set of labels into a set of "operating" labels  $X$ , and a set of "failed" labels  $Y$ .
- (3) It classifies the labels into subsets  $X(K)$  and  $Y(K)$  containing, respectively, "operating" or "failed" labels with  $K$  failed components.
- (4) It defines the transition probability matrix according to (3.19).

Since the number of state labels is equal to the number of superstates, this procedure is very fast. It requires, nevertheless, the correct identification of symmetrical components. For a given system, it is rather easy to identify potentially symmetrical components

satisfying conditions (1) and (2) of Definition 3.3.1. For large systems, however, it might be difficult to verify the validity of condition (3). In such cases if the classes of symmetrical components are wrongly defined, the merged transition probability matrix that will be produced by version 1 of the code will not be equivalent to the original Markov process. Therefore, whenever the analyst is not sure if two or more components are actually symmetrical, version 2 should be used.

Version 2. The input of this version consists of the following information:

- (1) A description of the system, namely:
  - (1a) the number of the components of the system;
  - (1b) the number of the states of each component, and the corresponding transition rates;
  - (1c) a "test" subroutine providing a criterion of whether a system-state is operating or not.
- (2) A description of the symmetries, namely, the number of classes of (potentially) symmetrical components as well as the individual components belonging to each class.\*

Then the code proceeds as follows:

- (1) It generates all the possible states of the system.
- (2) It classifies the states into operating and failed, using the "test" subroutine.
- (3) It partitions the sets of operating and failed states into

---

\* Note that while in version 1 it would have been sufficient to specify that class 1, for example, contains 3 components; in version 2 it must be specified that components #1, #2, and #7 belong to class 1.

subsets  $X(K)$  and  $Y(K)$ .

- (4) Within each subset  $X(K)$  or  $Y(K)$ , the state label of each state is generated and states with the same label are lumped to form superstates.
- (5) For a pair of superstates  $I$  and  $J$ , criterion (3.11) is checked as follows:
  - (5a) for every state  $i$  of superstate  $I$  the transition probability  $p_{ij}(n)$  is computed as in (3.2);
  - (5b) if criterion (3.11) is satisfied by all the  $p_{ij}(n)$ 's the program proceeds in step (5c), if not, it proceeds to step (7);
  - (5c) steps (5a) and (5b) are repeated for all states  $j$  of superstate  $J$ .
- (6) Step (5) is repeated for all pairs  $I$  and  $J$  of superstates. If all of them satisfy (3.11), the merging has been achieved, if not, the program proceeds in step (7).
- (7) The superstate that does not satisfy criterion (3.11) is split into two or more superstates, and steps (5), (6), and (7) are repeated until the original process is obtained.

Version 2 obviously requires more computing time as well as more memory space, but it guarantees a correct result. With a fairly reasonable definition of the symmetries, the merging is achieved within few iterations. An example of the use of both versions follows.

Example 3.7 The Markov process describing the system shown in Figure 2.1 has been merged with the help of the computer code described in

this section. The necessary computing-storage and computing-time requirements are given in Table 3.1 for the two versions of the code, as well as for the original process.

For version 1, the input stated that (1) the system consists of one class of subsystems containing two subsystems (Leg A and Leg B); and (2) each subsystem consists of two classes of components; class 1 containing the pump, and class 2 containing the two valves.

For version 2, the input stated that the system consists of two classes of components, the first containing the two pumps and the second the four valves. Since this definition of classes is not correct (see Example 3.1), the code needed several trials before the merging was achieved.

TABLE 3.1 Comparison of the computer storage and computer time required for solving the original and merged Markov processes for system in Figure 2.1.

	NUMBER OF STATES <sup>a</sup>	NUMBER OF ELEMENTS OF $P_a$	NUMBER OF ELEMENTS THAT NEED BE STORED <sup>a</sup>	TIME REQUIRED FOR GENERATION OF $P_b$ (sec)	TIME REQUIRED FOR SOLUTION OF (2.12) FOR 300 TIME STEPS <sup>b</sup> (sec)	TOTAL TIME <sup>b</sup> (sec)
Original Process	287	82,369	17,676	1.0	13.0	14.0
Merged Process Version 1	67	4,489	967	0.6	0.8	1.4
Merged Process Version 2	67	4,489	967	1.7	0.8	2.5

(a) With zero standby failure rates (Section 2.4).

(b) CDC, CYBER 70/Model 76 Computer System (7600).

## CHAPTER FOUR

### MARKOVIAN RELIABILITY ANALYSIS UNDER UNCERTAINTY

#### 4.1 Introduction

This Chapter presents the mathematical form of the problem examined in this dissertation, namely, the problem of Markovian reliability analysis under uncertainty.

As discussed in Chapter One, whenever the uncertainties in the reliability analysis are expressed by regarding the failure rates\* and the repair rates\* of the components of a system as random variables, the whole problem can be decomposed in the following three subproblems.

- (a) Determine the probability density functions (pdf) of the transition rates of the components of a complex system.
- (b) Calculate the pdf of the reliability (availability) of the complex system from the pdf of the transition rates.
- (c) Derive evaluators of the system from the random variable reliability (availability).

Subproblem (a) per se is not examined in this dissertation. For the purposes of this work it is assumed that the types of the pdfs of the transition rates as well as the numerical values of their parameters are given. The various forms of distributions considered in the numerical applications are, however, presented in this chapter. Subproblem (b) is a formidable one. Its exact mathematical form is presented in this chapter, and the unfeasibility of an analytical solution is discussed. The complexity of the problem suggests the

---

\* From now on and for the rest of Chapter Four the failure rates and repair rates will be collectively referred to as transition rates.



use of approximate methods for its solution. Subproblem (c) deals with the derivation of evaluators of the reliability (availability) from its pdf. The discussion of subproblem (c) precedes the others since the nature of the evaluators suggests ways of calculating them without the direct use of the pdf of the reliability.

The chapter is organized as follows: In Section 4.2, the objectives of the reliability analysis under uncertainty are presented. In Section 4.3, the mathematical statement of the problem is derived and the difficulties of an analytical solution are discussed. In Section 4.4, the forms of the pdf's considered in the numerical applications of this work are presented. In Section 4.5, the quantification of the uncertainties about the common-cause failure rates and in general of the interdependences of the transition rates is examined. And, finally, in Section 4.6, some analytical results for the 2x2 case are given.

## 4.2 Objectives of the Reliability Analysis Under Uncertainty

As already stated, the purpose of the reliability analysis (under uncertainty or not) is to provide evaluators (performance indices) to compare a given system to others or with given standards. Whenever a system is complicated and information exists only about its components, its reliability\* is a function of the transition rates of the components. Let the number of the transition rates be equal to  $m$ , and let  $x_i$  for  $i=1,2,\dots,m$  denote the  $i$ -th rate. Then, the

---

\*Throughout this chapter we will use the term reliability for collective reference to the reliability, failure probability, availability, unavailability or any other reliability index of a system. Whatever will be said about the reliability holds for any other reliability index.

reliability of the system at time  $n$ , is a function of the form

$$R(n) = R(x_1, \dots, x_m, n) \quad (4.1)$$

Whenever the  $x_i$ 's are known with certainty,  $R(n)$  is a deterministic function. In the presence of uncertainties, however, the  $x_i$ 's and  $R(n)$  are random variables. Then the problem is: Calculate the pdf of the random variable  $R(n)$  given the pdf's of the random variables  $x_i$ ,  $i=1,2,\dots,m$ .

The reliability  $R(n)$  is used in the calculation of several evaluators such as:

- (1) The expected value of the reliability defined by

$$E[R] \equiv \int_0^1 R(n) f(R) dR \quad (4.2)$$

where  $f(R)$  is the pdf of  $R$ .

- (2) The variance defined by

$$\text{var}[R] \equiv \int_0^1 \{R - E[R]\}^2 f(R) dR \quad (4.3)$$

- (3) The probability interval, the probability,  $\alpha$ , that the reliability of a system will be less than a given value  $Q$ , defined by

$$\alpha \equiv \Pr\{R \leq Q\} \equiv \int_0^Q f(R) dR \quad (4.4)$$

- (4) The expected utility of the reliability  $R$ , the expected value of a function  $u(R)$  that emphasizes the relative importance of each particular value of  $R$ ,

$$E[u(R)] \equiv \int_0^1 u(R) f(R) dR \quad . \quad (4.5)$$

It is noteworthy that the first three evaluators are special cases of the fourth. Indeed, the first implies a linear utility function for  $R$ , the second a quadratic, and the third a step function. Since almost always one of the above cited quantities is used in reliability evaluations of systems, we can say that the general objective of the reliability analysis under uncertainty is to calculate the expected value of a given function of  $R$ .

#### 4.3 Statement of the Problem

It was said in Section 4.2 that the objective of the reliability analysis under uncertainty is to calculate the expected value of a given function,  $u(R)$ , of the reliability  $R$ . From (4.2) to (4.5) it follows that  $E[u(R)]$  can be easily calculated if the pdf  $f(R)$  of  $R$  is known.

By virtue of (2.7) and (2.4), it follows that in Markovian analyses the reliability function has the form

$$R(n) = \sum_{i \in X} \sum_{j=1}^Z \pi_j(0) p_{ji}^{(n)} \quad , \quad (4.6)$$

where  $p_{ij}^{(n)}$  denotes the  $ij$  element of matrix  $\underline{P}^n$ . Since the vector  $\underline{\pi}(0)$

is assumed to be known with probability 1, it follows from (4.2) that  $R(n)$  is a linear combination of the  $p_{ij}^{(n)}$ 's. The pdf of  $R(n)$  could be, therefore, calculated if the pdf's of the  $p_{ij}^{(n)}$ 's were known (see, for example, Green and Bourne, or Hahn and Shapiro). The main problem of this work can be stated, therefore, as:

Given the pdf's of the  $z^2$  random variables  $p_{ij}$ , find the pdf's of the  $z^2$  random variables  $p_{ij}^{(n)}$ ,

where

$$p_{ij}^{(n)} = y(p_{kr}) \quad \text{for } i, j = 1, 2, \dots, z \text{ and } k, r = 1, 2, \dots, z, \quad (4.7)$$

the function  $y$  being

$$\underline{p}^{(n)} = y(\underline{p}) = \underline{p}^n. \quad (4.8)$$

Further examination of this problem requires the following definition of a random matrix.

Definition 4.1 A  $z \times z$  matrix  $\underline{P}$  is called random if its elements are random variables. The joint pdf of the elements  $p_{ij}$  is called the pdf of the random matrix  $\underline{P}$ .

A random\* matrix can be viewed as a  $z^2$ -dimensional variable taking values in the  $z^2$ -dimensional Euclidean space  $S$ .

---

\* A random matrix must not be confused with a stochastic matrix. A stochastic matrix is a matrix the elements of which satisfy (2.3a). The matrices with which we work in this dissertation are both stochastic and random.

From Definition 4.1, (4.7), and (4.8) it follows that the problem of determining the pdfs of  $p_{ij}^{(n)}$ 's is equivalent to determining the pdf of a function of a random matrix. This problem is delineated in the following subsection.

#### 4.3.1 Functions of random matrices

Let  $\underline{G}$  be a  $z \times z$  matrix function of a  $z \times z$  matrix  $\underline{P}$

$$\underline{G} = y(\underline{P}) \quad . \quad (4.9)$$

If  $\underline{P}$  is a random matrix,  $\underline{G}$  is also a random matrix if the function  $y(\underline{P})$  satisfies certain conditions. For details the reader is referred to Wilks (1962), p. 58. Here it suffices to say that these conditions are met by the functions considered in this work.

The pdf of  $\underline{G}$  can be calculated from the pdf of  $\underline{P}$  with the help of the following proposition. This proposition is stated without proof. For a proof, the reader is referred to Wilks (1962), p. 58.

Proposition 4.1 Let  $\underline{P}$  be a continuous random matrix with pdf

$$f(p_{11}, p_{12}, \dots, p_{zz}) = f(\underline{P}) \quad (4.10)$$

in some open region A of the space of  $p_{ij}$ 's, let  $g_{ij} = y_{ij}(p_{11}, p_{12}, \dots, p_{zz})$   $i=1,2,\dots,z$  and  $j=1,2,\dots,z$  have a unique inverse

$$p_{ij} = y^{-1}(g_{11}, g_{12}, \dots, g_{zz}) \quad i,j=1,2,\dots,z \quad , \quad (4.11)$$

where the  $y_{ij}$  possess continuous first derivatives such that the Jacobian  $(z^2 \times z^2)$

$$J = \left| \frac{\partial p_{ij}}{\partial g_{kr}} \right| \neq 0 \quad \text{in } A.$$

Let the image of  $A$  in the space of  $(g_{11}, g_{12}, \dots, g_{zz})$  be denoted by  $B$ . Then  $\underline{G}$  is a continuous random matrix having pdf at a point  $(g_{11}, g_{12}, \dots, g_{zz})$  in  $B$  given by

$$h(g_{11}, g_{12}, \dots, g_{zz}) = f(p_{11}, p_{12}, \dots, p_{zz}) |J| = f[y^{-1}(\underline{G})] |J| \quad (4.12)$$

or

$$h(\underline{G}) = f[y^{-1}(\underline{G})] |J|, \quad (4.13)$$

where it is understood that the  $p_{ij}$ 's are given by (4.11) and that, therefore, the  $p_{ij}$ 's are to be expressed in terms of the  $g_{ij}$ 's in the righthand side of (4.13).

#### 4.3.2 Need for approximate solutions

An analytical solution to the problem of determining the pdf of the reliability  $R(n)$  could consist, therefore, of the following steps:

- (1) The pdf's of the elements  $p_{ij}$  of the transition probability matrix  $\underline{P}$  are derived from the pdf's of the failure rates and repair rates through (2.9).
- (2) The pdf's of  $p_{ij}^{(n)}$ 's, the elements of the matrix  $\underline{P}^n$ , are then

determined from the pdf's of  $p_{ij}$ 's and (4.12).

- (3) The pdf of  $R(n)$  is determined from the pdf's of  $p_{ij}^{(n)}$ 's through (4.6).

The completion of step (2) is, nevertheless, extremely difficult. The difficulty lies mainly in the determination of the inverse functions [see also (4.11)]

$$p_{ij} = y_{ij}^{-1} (p_{11}^{(n)}, p_{12}^{(n)}, \dots, p_{zz}^{(n)}) \quad (4.14)$$

that are required in (4.12).

Equation (4.14) implies the availability of a closed expression for the  $ij$ -th element of the  $n$ -th root of a square matrix or, equivalently, the availability of closed, inversable expressions of the elements of the  $n$ -th power of a square matrix in terms of the elements of this matrix. To our knowledge this problem can be solved only in the following cases:

- (a) Small dimensionality of  $\underline{P}$  (e.g.,  $2 \times 2$  case)
- (b) Very simple structure of  $\underline{P}$  (e.g., diagonal, tridiagonal).

For more general structures of  $\underline{P}$ , (4.13) can be used only when  $\underline{G}$  is a linear transformation of  $\underline{P}$ , i.e., when

$$\underline{G} = \underline{Q} \cdot \underline{P} \cdot \underline{I} \quad (4.15)$$

The matrices encountered in Markovian reliability analyses are, however, both of greater dimension than two and more complex than diagonal. We, therefore, think that the application of the analytical

method described in this section is not possible and that other approximate methods should be employed. Two such methods used in this work are presented in Chapters Five, Six, and Seven.

#### 4.4 On the Distribution of the Input Variables

This section is devoted to a description of the various forms of distributions that are used in this work for the expression of the uncertainties of the input variables, i.e., the transition rates. The question of how these forms can be obtained from existing information, theoretical models, engineering judgement, or subjective considerations is not addressed in this dissertation.

The transition rates of the various components of a system are assumed to be positive random variables taking values in any interval of the positive real axis. In the numerical applications, two types of pdf's were considered, the gamma distribution and the log-normal distribution. The methods developed in Chapters Five, Six, and Seven, are, nevertheless, independent of the nature of the pdf's of the input variables.

A list of the pdf's considered in various parts of this work follows.

##### 4.4.1 Gamma probability density function

The gamma pdf is used to describe the distribution of continuous random variables bounded at one end. The gamma pdf is defined by

$$f_{\gamma}(x|r,y) = \frac{\exp[-yx](yx)^{r-1}}{\Gamma(r)} y \quad , \quad (4.16)$$



where  $\Gamma(r)$  is the complete gamma function defined by

$$\Gamma(r) \equiv \int_0^{\infty} x^{r-1} e^{-x} dx \quad . \quad (4.16a)$$

If  $r$  is a positive integer

$$\Gamma(r) = (r-1)! \quad (4.16b)$$

The first four moments of this distribution are given in Table 4.1.

Equation (4.16) gives the form of a gamma pdf for a random variable bounded from below by zero. If the lower bound is a positive number  $a$ , then the generalized gamma pdf is given by

$$f_Y(x|r, y, a) \equiv \frac{\exp[-y(x-a)][y(x-a)]^{r-1}}{\Gamma(r)} y \quad . \quad (4.17)$$

#### 4.4.2 The log-normal probability density function

The log-normal pdf describes the distribution of a continuous random variable bounded from below by zero, with a logarithm distributed according to a normal pdf. Thus, the log-normal pdf is defined by

$$f_{LN}(x|\mu, \sigma) \equiv \frac{1}{\sigma x \sqrt{2\pi}} \exp \left[ \frac{-(\ln x - \mu)^2}{2\sigma^2} \right] \quad (4.18)$$

$$x > 0, \sigma > 0 \quad -\infty < \mu < \infty \quad .$$

The generalized log-normal distribution describes a random variable that covers an interval other than  $(0, \infty)$  and it is defined by

$$f_{LN}(x|\mu, \sigma, a) \equiv \frac{1}{\sigma(x-a)\sqrt{2\pi}} \exp \left[ \frac{-[\ln(x-a)-\mu]^2}{2\sigma^2} \right] \quad (4.19)$$

$$x \geq a, \quad \sigma > 0 \quad -\infty < \mu < \infty$$

The first four moments of this distribution are given in Table 4.1.

#### 4.4.3 The Beta probability density function

The Beta pdf is used to describe the distribution of continuous random variables bounded at both ends. The Beta pdf for the interval  $[0,1]$  is defined by

$$f_p(x|p,q) = \frac{1}{B(p,q)} x^{p-1} (1-x)^{q-1} \quad (4.20)$$

$$0 \leq x \leq 1 \quad p, q > 0,$$

where  $B(p,q)$  is the complete Beta function

$$B(p,q) = \frac{\Gamma(p)\Gamma(q)}{\Gamma(p+q)} \quad (4.20a)$$

The generalized Beta pdf describes a positive continuous random variable varying in an interval  $[a,b]$ . It is defined by

$$f_{\beta}(x|p,q,a,b) \equiv \frac{1}{(b-a)} \frac{1}{B(p,q)} \left[ \frac{x-a}{b-a} \right]^{p-1} \left[ 1 - \frac{x-a}{b-a} \right]^{q-1} \quad (4.21)$$

$$a \leq x \leq b \quad p, q > 0$$

The first four moments of this distribution are given in Tabl 4.1.

#### 4.4.4 The log-gamma probability density function

The log-gamma distribution is used to describe random variables taking values in the interval  $[0,1]$ . A random variable,  $x$ , is distributed according to a log-gamma distribution if its negative logarithm ( $z = -\ln x$ ) is distributed according to a gamma distribution. It is defined by

$$f_{LY}(x|r,y) = \frac{(x)^{y-1} [-y \ln x]^{r-1}}{\Gamma(r)} y \quad (4.22)$$

$$0 \leq x \leq 1 \quad r, y > 0$$

#### 4.5 Quantification of Common Cause Failure Rates and Interdependences of Transition Rates

As discussed in Chapters One and Two, the use of a Markov chain permits the incorporation in the model of interdependences among the transition rates and the states of the various components. Thus, if the transition rate from system state  $i$  to system state  $j$  is  $h$ , the transition rate from system state  $i'$  to system state  $j'$  might be  $h^*$  ( $h^* \neq h$ ) even though the latter transition involves the change of the state of the same component. This is because this transition rate

TABLE 4.1 Summary of important distributions

		Expected Value	Variance	$\sqrt{\beta_1}$	$\beta_2$
Gamma	$\frac{\exp[-yx](yx)^{r-1}}{\Gamma(r)}y$	$\frac{r}{y}$	$\frac{r}{y^2}$	$\frac{2}{\sqrt{r}}$	$\frac{3(r+2)}{r}$
Lognormal	$\frac{\exp[-(\ln x - \mu)^2/2\sigma^2]}{\sigma x \sqrt{2\pi}}$	$e^{\mu + \frac{1}{2}\sigma^2}$	$(e^{2\mu} + \sigma^2)(e^{\sigma^2} - 1)$	$(e^{\sigma^2} - 1)^{\frac{1}{2}}(e^{\sigma^2} + 2)$	$3 + (e^{\sigma^2} - 1)(e^{3\sigma^2} + 3e^{2\sigma^2} + 6e^{\sigma^2} + 6)$
Beta	$\frac{x^{p-1}(1-x)^{q-1}}{B(p,q)}$	$\frac{p}{p+q}$	$\frac{pq}{(p+q)^2(p+q+1)}$	$\frac{2(q-p)(p+q+1)^{\frac{1}{2}}}{(pq)^{\frac{1}{2}}(p+q+2)}$	$\frac{3(p+q+1)[2(p+q)^2 + pq(p+q-6)]}{pq(p+q+2)(p+q+3)}$

(h) might depend on the states of the other components which can be different in system states  $i$  and  $i'$ . Since uncertainties might exist about both  $h$  and  $h^*$ , a first approach to quantify them would be to consider both  $h$  and  $h^*$  as random variables taking values in the interval  $[0, \infty)$ . In general, an overlap of the pdf's (see Figure 4.1) may exist so that both

$$h < h^*$$

and

$$h > h^*$$

could be true, albeit with different probability. In most instances, however, the relation between  $h$  and  $h^*$  is monotonic. If, for example,

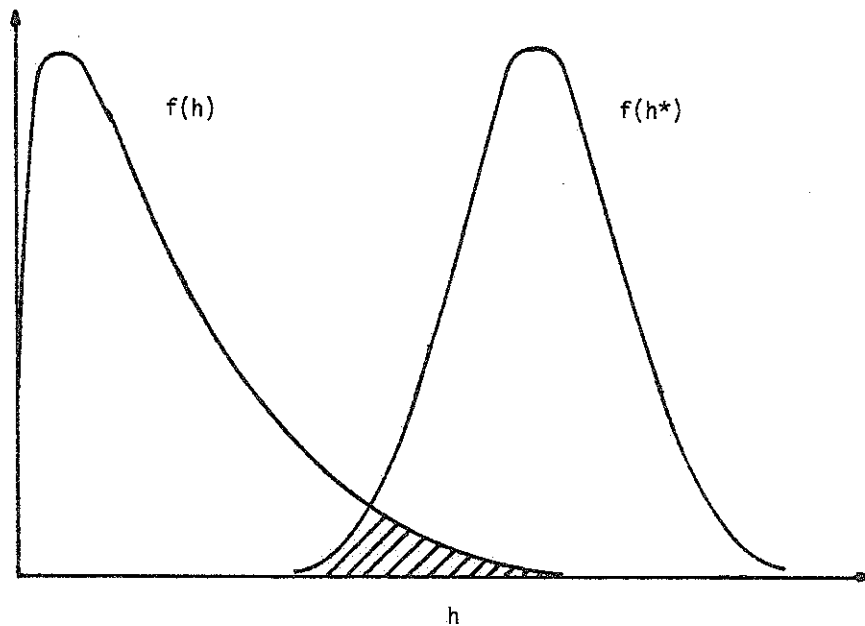


Figure 4.1. Overlapping of the pdf's of  $h$  and  $h^*$ .

$h^*$  represents a common cause failure rate, we want always to have  $h^* > h$ . Of course this condition could be added in the pdf of  $h^*$ . In an idealization of the process we could say that the value of  $h$  is first chosen from  $f(h)$  and, then, the value of  $h^*$  is chosen from  $f(h^*)$  with the condition  $h^* > h$ . But this introduces a statistical dependence among the values of the transition rates  $h$  and  $h^*$ . Although the existence of such dependences is not prohibitive for the methods employed in this work, it unnecessarily increases the complexity of the problem. Alternatively stated, we would like to have  $R$  as a function of independent random variables [see (4.1)]. To achieve this, we define  $h^*$  to be

$$h^* = kh, \quad (4.23)$$

where  $k$  is a random variable taking values in the interval  $[1, \infty)$ , is statistically independent of  $h$ , and it is called dependence coefficient. Thus, the set of variables  $x_i$ s in (4.1) consists of the generic transition rates  $h$  that characterize the independent operation of the components and of the dependence coefficients  $k$ . It is, therefore, a set of statistically independent random variables.

#### 4.6 Analytical Results for the 2x2 Case

In this section specific analytical results for a two-state Markov process are presented. The reasons for this presentation are:

- (1) these analytical results can serve as a means of checking the accuracy of the numerical methods presented in Chapters Five and Six, and
- (2) the complexity of the results supports our claim that an analytical

solution for the general case (where the order of the matrices involved rises in the hundreds) is unfeasible.

A single two-state component is considered having failure rate  $\lambda$  and repair rate  $\mu$ . The equation of the state probability vector  $\underline{\pi}(t)$  in the continuous-time case is then given by

$$\frac{d\underline{\pi}(t)}{dt} = \underline{\pi}(t) \cdot \underline{A} \quad , \quad (4.24)$$

where  $\underline{A}$  is the transition rate probability matrix

$$\underline{A} = \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix} \quad . \quad (4.25)$$

In the discrete-time case the equation of  $\underline{\pi}(n)$  is

$$\underline{\pi}(n+1) = \underline{\pi}(n) \cdot \underline{P} \quad , \quad (4.26)$$

where  $\underline{P}$  is the transition probability matrix given by [see also (2.9)]

$$\underline{P} = \underline{I} + \underline{A} \Delta t \quad . \quad (4.27)$$

The solutions of (4.24) and (4.26) are, respectively,

$$\underline{\pi}(t) = \underline{\pi}(0) \cdot e^{\underline{A} t} \quad (4.28)$$

and

$$\underline{\pi}(n) = \underline{\pi}(0) \cdot \underline{p}^n, \quad (4.29)$$

where  $\underline{\pi}(0) = [1,0]$  is the state probability vector at time zero. It can be easily shown that the availability of the system (i.e., the probability that it occupy state 1) is given for the continuous time case by

$$A(t) \equiv \pi_1(t) = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda} \exp[-(\mu+\lambda)t], \quad (4.30)$$

and for the discrete-time case by

$$A(n) = \pi_1(n) = \frac{p_{21}}{p_{12}+p_{21}} + \frac{p_{12}}{p_{12}+p_{21}} [1-(p_{12}+p_{21})]^n, \quad (4.31)$$

where [see (2.9), (4.27)]

$$p_{12} = \lambda \Delta t \quad \text{and} \quad p_{21} = \mu \Delta t. \quad (4.32)$$

The steady-state availability for both cases is

$$A(\infty) = \frac{\mu}{\mu+\lambda}. \quad (4.33)$$

If the failure and repair rates  $\mu, \lambda$  are random variables, so are the variables  $A(t)$ ,  $A(n)$ , and  $A(\infty)$ . Given the pdf's of  $\mu, \lambda$  we would like to calculate the pdf's of  $A(t)$ ,  $A(n)$ ,  $A(\infty)$ , and/or important parameters of these pdf's. For convenience, we start with  $A(\infty)$ .



#### 4.6.1 The pdf of the steady-state availability of a two-state component

It is assumed that  $\mu, \lambda$  are statistically independent and each is distributed according to a gamma density function. Then, the joint pdf of those variables is the product of the individual pdf's or

$$f(\lambda, \mu | r_1, r_2, y_1, y_2) = f_\gamma(\lambda | r_1, y_1) f_\gamma(\mu | r_2, y_2)$$

or [see (4.16)]

$$f(\lambda, \mu) = \frac{1}{\Gamma(r_1) \Gamma(r_2)} \lambda^{r_1-1} \mu^{r_2-1} \exp[-(y_2 \lambda + y_2 \mu)] y_2^{r_1} y_2^{r_2}. \quad (4.34)$$

We now denote  $A(\infty)$  by  $w$ , define the variable  $s=(\lambda+\mu)$  and consider the transformation [see also (4.9)]

$$(s, w) = y(\lambda, \mu), \quad (4.35)$$

where

$$s = \lambda + \mu, \quad (4.35a)$$

$$w = \frac{\mu}{\mu + \lambda}. \quad (4.35b)$$

If  $h(s, w)$  denotes the pdf of the random variables  $s, w$ , it follows from (4.13) that

$$h(s, w) = f[y^{-1}(s, w)] \begin{vmatrix} \frac{\partial \lambda}{\partial s} & \frac{\partial \lambda}{\partial w} \\ \frac{\partial \mu}{\partial s} & \frac{\partial \mu}{\partial w} \end{vmatrix} \quad (4.36)$$

By virtue of (4.35a) and (4.35b), it follows that the transformation  $(\lambda, \mu) = y^{-1}(s, w)$  is given by

$$\lambda = (1-w)s \quad , \quad (4.37a)$$

$$\mu = ws \quad , \quad (4.37b)$$

and that the Jacobian in (4.36) is equal to  $s$ :

$$|J| = s \quad . \quad (4.38)$$

The combination of (4.34) and (4.36) through (4.38) yields

$$h(s, w) = \frac{y_1^{r_1} y_2^{r_2}}{\Gamma(r_1) \Gamma(r_2)} s^{r_1+r_2-1} w^{r_2-1} (1-w)^{r_1-1} \exp\{-y_1(1-w) + y_2 w\} s \quad (4.39)$$

The pdf of  $A(\infty)$  or  $w$  can now be derived from (4.39) by integrating out the variable  $s$  or

$$f(w) = \int_0^\infty h(s, w) ds \quad . \quad (4.40)$$

The integration in (4.40) results in

$$f(w) = \frac{1}{B(r_1, r_2)} \frac{y_1(1-w)^{r_1-1} y_2 w^{r_2-1}}{[y_1(1-w) + y_2 w]^{r_1+r_2}} y_1 y_2 \quad , \quad (4.41)$$

a pdf that can be called generalized-inverted-Beta distribution. This name is suggested by the fact that whenever a random variable  $w$  is distributed according to (4.41) then the random variable  $z$ , where

$$z \equiv \frac{y_1(1-w)}{y_1(1-w) + y_2 w} \quad (4.42)$$

is distributed according to a Beta-density function.

The expected value of the steady-state availability  $E[A(\infty)]$ , is defined by

$$E[A(\infty)] = \int_0^1 w f(w) dw ,$$

which in terms of the substitution (4.42) can be written as

$$E[A(\infty)] = \frac{1}{B(r_1, r_2)} \int_0^1 z^{r_1-1} (1-z)^{r_2-1} [1-yz]^{-1} dz , \quad (4.43)$$

where

$$y \equiv 1 - \frac{y_2}{y_1} . \quad (4.44)$$

As will be seen shortly, it is important that  $y$  be defined in such a way that the following holds

$$y^2 < 1 . \quad (4.44a)$$

Since  $y_2$  is the scale parameter of the pdf for the repair rate while  $y_1$  is the scale parameter of the pdf for the failure rate, we assume that  $y_2 < y_1$ , and therefore that (4.44a) is true. If for any reason  $y_1 < y_2$ , then the mean value of the random variable  $1-w$  (unavailability) can be calculated in terms of the value  $1-y_1/y_2$ .

The integration in (4.43) is not easy to perform. The integral has been evaluated and tabulated numerically in terms of the hypergeometric function (see, for example, Morse and Feshbach, p. 591) but only for values of  $y_1, y_2, r_1, r_2$  that are of interest to problems of theoretical physics. A series representation of this integral is presented here in terms of the hypergeometric coefficients defined by

$$(x)_k \equiv \frac{\Gamma(x+k)}{\Gamma(x)} \quad . \quad (4.45)$$

Because of (4.44a) we can expand the term  $(1-yz)^{-1}$  into an infinite series

$$(1-yz)^{-1} = \sum_{k=0}^{\infty} y^k z^k$$

and therefore write (4.43) as

$$E[A(\infty)] = \frac{1}{B(r_1, r_2)} \sum_{k=0}^{\infty} y^k \int_0^1 (1-z)^{r_2-1} z^{r_1+k-1} dz \quad ,$$

or in terms of (4.45)

$$E[A^{(\infty)}] = \frac{r_2}{r_1+r_2} \sum_{k=0}^{\infty} y^k \frac{(r_1)_k}{(r_1+r_2+1)_k} \quad (4.46)$$

The series (4.46) converges absolutely.

In a similar way it can be shown that the second moment of  $A^{(\infty)}$  is given by

$$E[A^2(\infty)] = \frac{1}{B(r_1, r_2)} \int_0^1 z^{r_1-1} (1-z)^{r_2+1} (1-yz)^{-2} dz ,$$

which in terms of (4.46) can be written as

$$E[A^2(\infty)] = \frac{r_2(r_2+1)}{(r_1+r_2)(r_1+r_2+1)} \sum_{k=0}^{\infty} (k+1)y^k \frac{(r_1)_k}{(r_1+r_2+2)_k} \quad (4.47)$$

#### 4.6.2 Conditional pdf of the transient part of the availability of two-state component

Let the transient part of the availability at time  $t$  be denoted by  $u$  where [see (4.29), (4.35a), and (4.35b)]

$$u \equiv A(t) - w = (1-w)e^{-s t} \quad (4.48)$$

Then it can be shown, as in Subsection 4.6.1, that the transformation  $(u, w) = y(s, w)$  yields

$$g(u, w) = K(w) t^{-r} \left[ -1 \ln \left( \frac{u}{1-w} \right) \right]^{r-1} \left[ \frac{u}{1-w} \right]^{a-1} , \quad (4.49)$$

where

$$K(w) \equiv \frac{y_1^{r_1} y_2^{r_2}}{\Gamma(r_1) \Gamma(r_2)} (1-w)^{r_1} w^{r_2-1}, \quad (4.49a)$$

$$a \equiv - \frac{[y_1(1-w) + y_2 w]}{t}, \quad (4.49b)$$

$$r = r_1 + r_2. \quad (4.49c)$$

By virtue of (4.42) and (4.49) it follows that the conditional (on the steady-state availability) pdf of the transient part of the availability is given by

$$g(u|w) = \frac{1}{\Gamma(r)} a^r [-\ln(\frac{u}{1-w})]^{r-1} [\frac{u}{1-w}]^{a-1}. \quad (4.50)$$

#### 4.6.3 Expected n-step transition probabilities\*

For this case we assume that the random variables  $\lambda, \mu$  are distributed in such a way that the variables  $p_{12}$  and  $p_{21}$  [see (4.31)] are independently distributed according to Beta distributions. This means that for constant  $\Delta t = h$ ,  $\lambda$  and  $\mu$  vary in the interval  $[0, 1/h]$  instead of the interval  $[0, \infty)$ . For convenience we will calculate the expected value of the unavailability at time  $n$  defined by

$$U(n) = 1 - A(n) = \frac{a}{a+b} \{1 - [1 - (a+b)]^n\}, \quad (4.51)$$

where

$$p_{12} = a \text{ and } p_{21} = b, \text{ and}$$

---

\* In this section we present results of Martin (1964).

where

$$f(a,b) = \frac{1}{B(r,s) B(p,q)} a^{r-1}(1-a)^{s-1} b^{p-1}(1-b)^{q-1} . \quad (4.52)$$

Equation (4.51) can be written as

$$U(n) = a \frac{\{1-[1-(a+b)]^n\}}{\{1-[1-(a+b)]\}} = a \sum_{k=0}^{n-1} (1-a-b)^k ,$$

which can be written with the binominal expansion of the term  $(1-a-b)^k$  as

$$U(n) = \sum_{k=0}^{n-1} \sum_{v=0}^k \binom{k}{v} (-1)^v b^v a (1-a)^{k-v} ,$$

and therefore

$$E[U(n)] = \sum_{k=0}^{n-1} \sum_{v=0}^k \binom{k}{v} \int_0^1 \int_0^1 (-1)^v b^v a (1-a)^{k-v} da db ,$$

which in view of (4.52) and (4.45) can be written as

$$E[U(n)] = \frac{s}{r+s} \sum_{k=0}^{n-1} \sum_{v=0}^k \binom{k}{v} (-1)^v \frac{(r)_{k-v} (p)_v}{(r+s+1)_{k-v} (p+q)_v} . \quad (4.53)$$

In a similar way it can be shown that

$$E[U^2(n)] = \frac{(s)_2}{(r+s)_2} \sum_{j=0}^{n-1} \sum_{v=0}^{j+k} \binom{j+k}{v} (-1)^v \frac{(r)_{j+k+v} (p)_v}{(r+s+2)_{j+k+v} (p+q)_v} . \quad (4.54)$$

Furthermore it can be shown that the expected steady-state availability is given by

$$E[A(\infty)] = \sum_{k=0}^{\infty} \sum_{v=0}^k \binom{k}{v} (-1)^v \frac{\binom{r}{k-v} \binom{p}{v+1}}{\binom{r+s}{k-v} \binom{p+q}{v+1}}, \quad (4.55)$$

and

$$E[A^2(\infty)] = \sum_{\substack{j=0 \\ k=0}}^{\infty} \sum_{v=0}^{j+k} \binom{j+k}{v} (-1)^v \frac{\binom{r}{j+k-v} \binom{p}{v+2}}{\binom{r+s}{j+k-v} \binom{p+q}{v+2}}. \quad (4.56)$$

It is noteworthy that the infinite series in (4.55) and (4.56) are conditionally convergent, and that the difference in the expressions for  $E[A(\infty)]$  and  $E[A^2(\infty)]$  in the discrete-time and continuous-time case stems from the different distributions considered for the  $\lambda$  and  $\mu$  in each case.



## CHAPTER FIVE

### THE MOMENT-MATCHING METHOD

#### 5.1 Introduction

This chapter presents a method for approximating the pdf of the reliability when its first few moments are available.

If the first few moments of a random variable are known, its pdf can be approximated by fitting an appropriate distribution to the existing information (expressed collectively in the form of the first few moments). Usually the first four moments are adequate for fitting two-parameter pdf's. The third and fourth moments determine the "shape" or the form of the distribution while the first two moments define its parameters. This procedure is called the moment-matching method and it has been widely used in uncertainty analysis, in nuclear and nonnuclear applications. In the Reactor Safety Study (1975), for example, the pdf of the top-event of a fault-tree was approximated by a lognormal distribution, while Apostolakis and Lee (1976) considered for the same purpose a wider class of distributions.

The moment-matching method for approximating the pdf of a random variable is described in the following section.

#### 5.2 The Moment-Matching Method

The pdf of a bounded random variable is uniquely determined by its moments [see Wilks (1962, p. 127)]. It follows, therefore, that pdf's of bounded random variables with a finite number of the lower moments in common exhibit similarities, since in the limit (all

moments the same) they would coincide in a unique pdf. Let us now suppose that only the first few moments of a bounded random variable are known. Then if a pdf is chosen in such a way that it has as its first few moments these known moments, it would constitute an approximation to the pdf of the random variable. This method of approximating a pdf is called the moment-matching method.

The reliability of a system, being a probability, is bounded since it can take values only in the interval  $[0,1]$ , and therefore the moment-matching method can be applied if its  $n$  first moments are known. Obviously, the more moments available, the more exact the approximation would be. In most instances, however, the first four moments are adequate. This is the case when a two-parameter pdf (like the ones presented in Section 4.4 or a member of the Johnson or Pearson families) is chosen as an approximation. The third and fourth moments determine the shape or the "type" of the distribution and the first two its parameters. More precisely, the shape of a distribution is partly characterized by: (1) its third central moment or skewness which is a measure of the asymmetry of the distribution, and (2) its fourth central moment or kurtosis which is related to its peakedness. In order to make these two "measures" of the shape of a pdf independent from its scale, the following coefficients are defined:

$$\text{coefficient of skewness: } \sqrt{\beta_1} \equiv \frac{\mu_3}{(\mu_2)^{3/2}} \quad (5.1)$$

and

$$\text{coefficient of kurtosis: } \beta_2 \equiv \frac{\mu_4}{\mu_2^2} , \quad (5.2)$$

where  $\mu_k$  denotes the k-th central moment of a random variable or

$$\mu_k \equiv \int_0^1 \{R - E[R]\}^k f(R) dR \quad (5.3)$$

If, furthermore,  $\mu'_k$  denotes the k-th moment about the origin or

$$\mu'_k \equiv \int_0^1 R^k f(R) dR , \quad (5.4)$$

we have

$$\mu_2 = \mu'_2 - (\mu'_1)^2 , \quad (5.5a)$$

$$\mu_3 = \mu'_3 - 3\mu'_2\mu'_1 + 2(\mu'_1)^3 , \quad (5.5b)$$

$$\mu_4 = \mu'_4 - 4\mu'_3\mu'_1 + 6\mu'_2(\mu'_1)^2 - 3(\mu'_1)^4 . \quad (5.5c)$$

Thus, if the coefficients  $\beta_1$  and  $\beta_2$  can be obtained, the shape of the distribution is approximately defined. Figure 5.1 gives numerical values of the coefficients  $\beta_1$  and  $\beta_2$  of the various "theoretical" types of densities presented in Chapter Four. [See also Hahn and Shapiro (1967)]. From this figure, the type of density that has the same  $\beta_1$  and  $\beta_2$  with the sought pdf can be obtained. The remaining two parameters (defining the location and the scale of the pdf) are then determined by the first two moments.

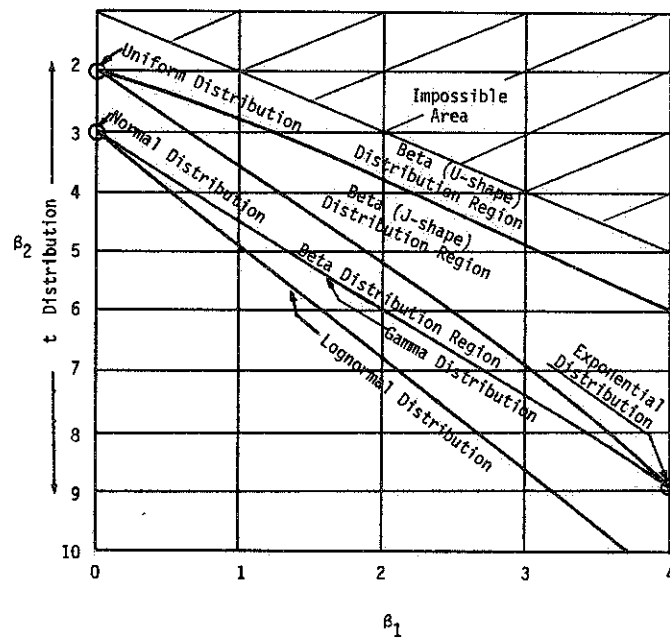


Figure 5.1. Regions in  $(\beta_1, \beta_2)$  plane for various distributions.

## CHAPTER SIX

### MONTE CARLO SIMULATION

#### 6.1 Introduction

This Chapter discusses the use of the Monte Carlo simulation technique in the evaluation of the uncertainties about the reliability of a system.

As already told, the objective of any reliability analysis under uncertainty is the calculation of a reliability evaluator containing, in some form, a measure of the uncertainties. In most cases these evaluators are the expected values of functions of the reliability [see (4.2) through (4.5)], and therefore the Monte Carlo technique is suitable for their estimation. Even when the pdf of the reliability is required, the Monte Carlo method can be used to estimate the moments of the distribution, and then the moment-matching technique described in Chapter 5 can be applied. The Monte Carlo technique consists in the generation of a sample of values of the random variable  $R$  (or a function of  $R$ ) by repeatedly solving (2.4) and (2.7), each time using randomly selected values of the input variables. The required quantities can then be statistically estimated from this sample. The precision of this method is limited only by the size of the sample, and therefore by the computing time necessary for its generation. For a given sample size (and hence, for a given degree of precision), the required computing time is directly proportional to the time necessary for each individual calculation. This latter time is controlled by three factors: 1) The complexity of the

structure of the transition probability matrix  $\underline{P}$ ; 2) the dimensions of  $\underline{P}$ ; and 3) the size of the time step  $\Delta t$  which determines the value of the exponent in (2.4) for a given time horizon. Methods for reducing the necessary computing time by simplifying the structure of  $\underline{P}$  and by reducing its dimensions were presented in Chapters Two and Three, respectively. In this chapter the question of the size of the time step is addressed.

This chapter is organized as follows: Section 6.2 presents the straightforward Monte Carlo technique along with a numerical example; Section 6.3 discusses the problem of determining the required size of the time step for a given set of transition rates; and Section 6.4 examines problems arising from the fact that each individual trial determines a different size of time step, as well as the problem of very small time steps. A numerical example is also presented.

## 6.2 Straightforward Monte Carlo Sampling

Let us suppose that we want to calculate the integral

$$E[u(R)] = \int_0^1 u(R) f(R) dR \quad , \quad (6.1)$$

where  $R$  is a function of  $m$  random variables

$$R = R(x_1, \dots, x_m) \quad , \quad (6.2)$$

where the  $x_i$ 's have a joint pdf  $g(x_1, \dots, x_m)$ . Equation (6.1) can then be written as

$$E[u(R)] = \int \cdots \int u(R) g(x_1, \dots, x_m) dx_1 \dots dx_m . \quad (6.3)$$

Let us now assume that a sample of  $N$   $m$ -tuples  $(x_{1i}, x_{2i}, \dots, x_{mi})$   $i=1, \dots, N$  is randomly generated from the pdf  $g(x_1, \dots, x_m)$ . These  $N$   $m$ -tuples provide, through (6.2), a sample of  $N$  values of the random variable  $R$ , and this in turn, a sample of  $N$  values of the random variable  $u$ . Then, we say that the quantity  $\hat{u}_1$ , where

$$\hat{u}_1 = \frac{1}{N} \sum_{i=1}^N u_i , \quad (6.4)$$

provides an estimator of  $E[u]$  in the sense that  $\hat{u}_1$  approaches, almost always,  $E[u]$  as  $N$  approaches  $\infty$ . This follows from the Central Limit theorem\* which states that: If  $u_1, u_2, \dots, u_N$  is a sequence of independent and identically distributed random variables with common mean  $m$  and standard deviation  $\sigma$ , then the average

$$\hat{u}_1 = \frac{1}{N} \sum_{i=1}^N u_i \quad (6.5)$$

is asymptotically normal  $(m, \sigma/\sqrt{N})$ ; i.e.,

$$\lim_{N \rightarrow \infty} P_r \{ |\hat{u}_1 - m| \leq \frac{x \sigma}{\sqrt{N}} \} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-t^2/2} dt . \quad (6.6)$$

It must be noted that the Central Limit theorem holds regardless of the distribution of  $u$  as long as  $m$  and  $\sigma$  exist. Alternatively, by

---

\* See for example Cramer (1946).

denoting  $x\sigma/\sqrt{N}$  by  $\epsilon$ , (6.6) can be written as

$$P_r\{|\hat{u}_i - m| \leq \epsilon\} = \sqrt{\frac{2}{\pi}} \int_0^{\epsilon\sqrt{N}/\sigma} e^{-t^2/2} dt + O\left(\frac{1}{\sqrt{N}}\right) \quad (6.7)$$

Equation (6.7) implies that as  $N$  approaches  $\infty$ , the probability that  $|u_1 - m|$  will be less than or equal to any nonnegative real number  $\epsilon$  is equal to one. If the standard deviation  $\sigma$  of the distribution of  $u$  were known, (6.7) could provide the required size  $N$  for a desired precision level. In other words, (6.7) would provide confidence levels or an interval that would contain  $m$  with certain probability. Of course, it is rather rare that  $\sigma$  should be known and  $m$  unknown. Then an estimator  $s^2$  of the variance  $\sigma$  could be used in (6.7). This estimator is given by

$$s^2 = \frac{N}{N-1} [\hat{u}_2 - (\hat{u}_1)^2] \quad , \quad (6.8)$$

where, of course,

$$\hat{u}_2 \equiv \frac{1}{N} \sum_{i=1}^N u_i^2 \quad . \quad (6.9)$$

As noted by Kahn (1956), p. 87, the estimate  $s$  of  $\sigma$  in (6.8) is often unreliable unless  $N$  is sufficiently large. How much is sufficiently large cannot be specified, however, and it depends heavily on the particular application. The estimator  $s$  in (6.8) can be, nevertheless, used in (6.5) to provide negative information, in the sense that



if the results of (6.7) with  $s$  in the place of  $\sigma$  are not acceptable, then this information is usually reliable. One way to get around this difficulty is suggested by Gelbard(b). This procedure is based on the fact that if  $z$  is a random variable normally distributed (mean  $m$  and standard deviation  $\sigma$ ) and a sample of size  $n$  is drawn from this distribution, then the quantity

$$\bar{z} = \sqrt{n} (\bar{z}_1 - m) , \quad (6.10)$$

where

$$\bar{z}_1 = \frac{1}{n} \sum_{i=1}^n z_i ,$$

is distributed normally with mean 0 and standard deviation  $\sigma$  (see Central Limit theorem), and the quantity

$$\hat{\sigma} = \left\{ \frac{n}{n-1} [\hat{z}_2 - (\hat{z}_1)^2] \right\}^{1/2} = \left( \frac{n}{n-1} \right)^{1/2} s , \quad (6.11)$$

where

$$\hat{z}_2 = \frac{1}{n} \sum_{i=1}^n z_i^2 ,$$

is distributed according to a  $\chi^2$  distribution with  $(n-1)$  degrees of freedom and parameter  $1/2\sigma^2$ . If we now define the quantity

$$t \equiv \frac{\bar{z}}{\hat{\sigma}} = (n-1)^{1/2} \frac{\hat{z}_1 - m}{s} , \quad (6.12)$$

it can be shown that the distribution of  $t$  is a Student's  $t$  distribution with  $n-1$  degrees of freedom, or

$$S_{n-1}(t) = \frac{1}{\sqrt{(n-1)\pi}} \frac{\Gamma(n/2)}{\Gamma(\frac{n-1}{2})} \left(1 + \frac{t^2}{n-1}\right)^{-n/2} . \quad (6.13)$$

Since  $S_{n-1}(t)$  depends only on the sample size  $n$ , it can be used to provide confidence levels for  $t$ , and therefore for  $m$  [see (6.12)]. In other words, we have that

$$\Pr\{a \leq t \leq b\} = \int_a^b S_{n-1}(x) dx ,$$

or

$$\Pr\{\hat{z}_1 - \frac{bs}{\sqrt{n-1}} \leq m \leq \hat{z}_1 - \frac{as}{\sqrt{n-1}}\} = \int_a^b S_{n-1}(x) dx , \quad (6.14)$$

where the right-hand side of (6.14) can be found from probability tables.

Of course, (6.14) holds only when the sample is drawn from a normal population. This procedure can be applied in the general case, however, as follows. Let us divide the total number of trials ( $N$ ) of a Monte Carlo simulation in  $I$  groups, each containing  $n$  trials, so that

$$N = n \cdot I . \quad (6.15)$$

Let  $\hat{z}_j$  denote the mean of the  $j$ -th group, or

$$\hat{z}_j \equiv \frac{1}{n} \sum_{i=1}^n u_i, \quad (6.16)$$

and let  $\hat{u}_1$  denote the mean of the I estimators  $\hat{z}_j$ , or

$$\hat{u}_1 \equiv \frac{1}{I} \sum_{j=1}^I \hat{z}_j \quad (6.17)$$

and

$$(\hat{\sigma}_{I,n})^2 = \frac{1}{I(I-1)} \sum_{j=1}^I (\hat{z}_j - \hat{u}_1)^2. \quad (6.18)$$

If n is large enough that the Central Limit theorem holds, then the  $\hat{z}_j$  are normally distributed, and therefore the variable

$$t \equiv \frac{\hat{u}_1 - m}{\hat{\sigma}_{I,n}} \quad (6.19)$$

where m denotes the expected value of u,  $E[u]$ , is distributed according to a Student's t distribution, and from (6.14) it follows that

$$\Pr\{\hat{u}_1 - b\hat{\sigma}_{I,n} \leq m \leq \hat{u}_1 + b\hat{\sigma}_{I,n}\} = 1 - 2 \int_b^\infty S_{n-1}(x) dx. \quad (6.20)$$

In using (6.20) one must be sure that the  $\hat{z}_j$  are normally distributed. Usually if n is not sufficiently large, a test of normality should be applied.

The procedure described above is followed in this work for the

estimation of confidence levels of any of the evaluators presented in Section 4.2. Whenever the whole pdf of  $R$  is desired, the first four moments are estimated and the moment-matching technique described in Chapter Five is applied.

A computer code has been written to carry out the Monte Carlo simulation, and it is described in Appendix C. A numerical example is provided in the following subsection.

#### 6.2.1 Numerical example of the straightforward Monte Carlo simulation

As an illustration of the straightforward Monte Carlo simulation, we calculated the expected value of the dynamic failure probability ( $F$ ) without repair of the sample system described in Section 2.5. The transition rates and the dependence coefficients were assumed randomly distributed according to gamma pdfs, the parameters of which are given in Table 7.4. A random sample of 1200 12-tuples of transition rates was generated. The corresponding histograms are presented in numerical form in Tables 6.4 through 6.15 and schematically in Figure 6.2. Equation (2.7) was solved repeatedly 1200 times, and the  $E[F]$  was estimated as in (6.4). Confidence levels for  $E[F]$  were estimated according to the two methods described in Section 6.2. Method I consists in using (6.7), considering the 1200 trials as one sample, and the placing of  $\sigma$  with its estimation  $s$  given by (6.8). Method II consists in considering the 1200 trials as 20 samples each of magnitude 60. Then Equations (6.17) through (6.20) were used. The results are presented in Table 6.1. The confidence levels provided by Method II are tighter than those provided by Method I.

TABLE 6.1 Confidence levels for the expected value of the failure probability without repair of the sample system.

TIME (HR)	METHOD	90% INTERVAL	95% INTERVAL	99% INTERVAL
200	I	$(.84 \pm .05) \times 10^{-2}$	$(.84 \pm .06) \times 10^{-2}$	$(.84 \pm .08) \times 10^{-2}$
	II	$(.84 \pm .04) \times 10^{-2}$	$(.84 \pm .05) \times 10^{-2}$	$(.84 \pm .07) \times 10^{-2}$
400	I	$(1.47 \pm .10) \times 10^{-2}$	$(1.47 \pm .12) \times 10^{-2}$	$(1.47 \pm .15) \times 10^{-2}$
	II	$(1.47 \pm .07) \times 10^{-2}$	$(1.47 \pm .09) \times 10^{-2}$	$(1.47 \pm .13) \times 10^{-2}$
600	I	$(2.53 \pm .15) \times 10^{-2}$	$(2.53 \pm .18) \times 10^{-2}$	$(2.53 \pm .24) \times 10^{-2}$
	II	$(2.53 \pm .10) \times 10^{-2}$	$(2.53 \pm .13) \times 10^{-2}$	$(2.53 \pm .19) \times 10^{-2}$
800	I	$(3.60 \pm .20) \times 10^{-2}$	$(3.60 \pm .24) \times 10^{-2}$	$(3.60 \pm .32) \times 10^{-2}$
	II	$(3.60 \pm .14) \times 10^{-2}$	$(3.60 \pm .18) \times 10^{-2}$	$(3.60 \pm .26) \times 10^{-2}$
1000	I	$(4.68 \pm .25) \times 10^{-2}$	$(4.68 \pm .30) \times 10^{-2}$	$(4.68 \pm .39) \times 10^{-2}$
	II	$(4.68 \pm .17) \times 10^{-2}$	$(4.68 \pm .22) \times 10^{-2}$	$(4.68 \pm .32) \times 10^{-2}$
1200	I	$(5.74 \pm .30) \times 10^{-2}$	$(5.74 \pm .36) \times 10^{-2}$	$(5.74 \pm .47) \times 10^{-2}$
	II	$(5.74 \pm .20) \times 10^{-2}$	$(5.74 \pm .26) \times 10^{-2}$	$(5.74 \pm .37) \times 10^{-2}$
1400	I	$(6.79 \pm .34) \times 10^{-2}$	$(6.79 \pm .41) \times 10^{-2}$	$(6.79 \pm .54) \times 10^{-2}$
	II	$(6.79 \pm .23) \times 10^{-2}$	$(6.79 \pm .30) \times 10^{-2}$	$(6.79 \pm .43) \times 10^{-2}$
1600	I	$(7.83 \pm .39) \times 10^{-2}$	$(7.83 \pm .46) \times 10^{-2}$	$(7.83 \pm .60) \times 10^{-2}$
	II	$(7.83 \pm .26) \times 10^{-2}$	$(7.83 \pm .33) \times 10^{-2}$	$(7.83 \pm .48) \times 10^{-2}$
1800	I	$(8.84 \pm .43) \times 10^{-2}$	$(8.84 \pm .51) \times 10^{-2}$	$(8.84 \pm .67) \times 10^{-2}$
	II	$(8.84 \pm .29) \times 10^{-2}$	$(8.84 \pm .37) \times 10^{-2}$	$(8.84 \pm .53) \times 10^{-2}$
2000	I	$(9.84 \pm .47) \times 10^{-2}$	$(9.84 \pm .56) \times 10^{-2}$	$(9.84 \pm .73) \times 10^{-2}$
	II	$(9.84 \pm .31) \times 10^{-2}$	$(9.84 \pm .40) \times 10^{-2}$	$(9.84 \pm .57) \times 10^{-2}$

The pdf of  $F$  at a given time can be approximated via the moment-matching technique. The estimations of  $\beta_1, \beta_2$  [see (5.1) and (5.2)] provide a type of distribution through Figure 5.1 and then the estimation of the first two moments of  $F$  can be used for the determination of the parameters of the distribution. For example, the estimations of  $\beta_1$  and  $\beta_2$  for  $F(1000 \text{ hr})$  are, respectively,

$$\beta_1 = 2.75 \quad ,$$

$$\beta_2 = 6.33 \quad .$$

The point  $(\beta_1, \beta_2)$  in the  $(\beta_1, \beta_2)$  plane indicates (see Figure 5.1) a Beta pdf. The parameters of the pdf were determined from the estimation of the first moment and the variance (see Table 4.1) and the results are presented in Table 6.2 and Figure 6.1.

TABLE 6.2 Cumulative probabilities for the failure probabilities without repair at  $t=1000 \text{ hr}$ .

$F_0 \text{ (} \times 10^{-1} \text{)}$	$\text{Pr}\{F \leq F_0\}$	
	Monte Carlo	Fitted Beta
0.184	0.399	0.388
0.368	0.563	0.574
0.552	0.682	0.697
0.736	0.772	0.782
0.920	0.842	0.844
1.100	0.878	0.887
1.290	0.915	0.919
1.470	0.944	0.942
1.660	0.958	0.959
1.840	0.968	0.971
2.020	0.980	0.979
2.210	0.987	0.986
2.400	0.992	0.990
2.580	0.995	0.993
2.760	0.999	0.995

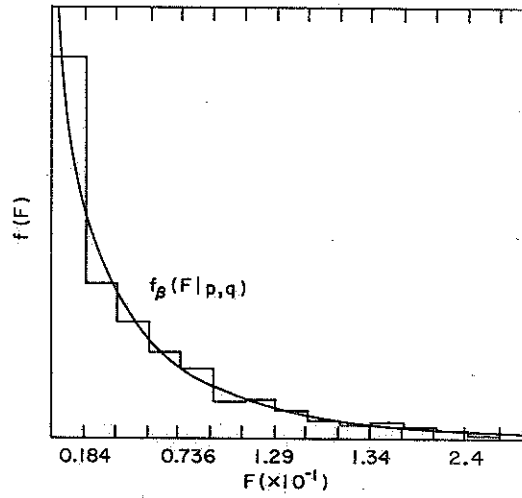


Figure 6.1. Pdf of failure probability without repair at  $t=1000$  hr. Beta pdf resulting from the moment-matching technique and histogram of 1200 Monte Carlo trials.

### 6.3 On the Size of the Time Step

For a given transition probability matrix  $\underline{P}$  and a given time-horizon  $t$ , the calculational effort associated with the solution of (2.4) is directly proportional to the number of time steps  $n(t=n\Delta t)$ . It is, therefore, desirable to use the largest possible time step. On the other hand, it was said in Section 2.3 that the time step must be such that assumptions (2.9) are valid. Since the smaller the time step the more accurate Equations (2.9) are, this second condition requires the use of the smallest possible time step. The problem of choosing the size of the time step can be viewed, therefore, as one of choosing the maximum time step for which assumptions (2.9) are valid. To further explore this question, we consider the discrete-time Markov model used in this work as an approximation of a continuous-time Markov model and examine for how large a  $\Delta t$  this approximation is valid.

A continuous-time Markov process is one in which the system can change state at any instant of time. Again, the basic assumption will be made that a direct transition between two system-states differing in the states of more than one component is not possible. In other words, two or more components cannot change state at the same instant. Let  $\tau_{ij}$  denote the time that the system spends in system state  $i$  before it transits to system-state  $j$  ( $i \neq j$ ). The Markovian assumption that the transition probability between states  $i$  and  $j$  depends only on  $i$  and  $j$ , implies that the times  $\tau_{ij}$  are generated according to a Poisson random process. It can then be shown that the  $\tau_{ij}$ 's are distributed exponentially or, if  $f(\tau_{ij})$  denotes their pdf, that



$$f(\tau_{ij}) = h_{ij} e^{-h_{ij} \tau_{ij}}, \quad i \neq j, \quad (6.21)$$

where  $h_{ij}$  characterizes the particular transition  $i \rightarrow j$ , and therefore it is equal to the transition rate of the component that changed state. If we now consider a finite period of time  $\Delta t$ , it follows from (6.21) that the probability that system will remain in state  $i$  for a time period  $\Delta t$  without transferring into state  $j$  is given by

$$\Pr\{\tau_{ij} > \Delta t\} = e^{-h_{ij} \Delta t}, \quad i \neq j, \quad (6.22)$$

and therefore the probability that the system will transit some time during  $\Delta t$  into  $j$  is given by

$$\Pr\{\tau_{ij} \leq \Delta t\} = 1 - e^{-h_{ij} \Delta t}, \quad i \neq j. \quad (6.23)$$

The probability that the system will remain at the same time  $i$  for the whole period  $\Delta t$ , is equal to the probability that it won't transit to any other state during this period, and therefore by virtue of (6.22) it follows that

$$\Pr\left\{\begin{array}{l} \text{system won't} \\ \text{leave state } i \end{array}\right\} = \prod_{\substack{j=1 \\ j \neq i}}^z e^{-h_{ij} \Delta t} = \exp\left\{-\sum_{\substack{j=1 \\ j \neq i}}^z h_{ij} \Delta t\right\}. \quad (6.24)$$

By discretizing the process we assume that: 1) the system can perform state transitions only at the end of time intervals of

length  $\Delta t$ ; and 2) the probability that a transition will take place is equal to the probability that such a transition would have taken place during this interval if the process were continuous in time. Then, it follows from (6.23) and (6.24) that

$$p_{ij} = \begin{cases} 1 - e^{-h_{ij} \Delta t}, & \text{if } i \neq j \\ \exp\left\{-\sum_{\substack{j=1 \\ i \neq j}}^z h_{ij} \Delta t\right\} & \text{if } i=j, \end{cases} \quad (6.25a)$$

$$(6.25b)$$

and from (2.9) and (6.25) that  $\Delta t$  should be such that

$$1 - e^{-h_{ij} \Delta t} \approx h_{ij} \Delta t, \quad i, j=1, 2, \dots, z, \quad (6.26a)$$

and that

$$\exp\left\{-\sum_{\substack{j=1 \\ i \neq j}}^z h_{ij} \Delta t\right\} \approx 1 - \sum_{\substack{j=1 \\ i \neq j}}^z h_{ij} \Delta t, \quad i=1, 2, \dots, z \quad (6.26b)$$

holds.

By denoting

$$s_i \equiv \sum_{\substack{j=1 \\ i \neq j}}^z h_{ij} \quad (6.27a)$$

and

$$s \equiv \max_i \{s_i\} \quad , \quad (6.27b)$$

it follows from (6.26) that  $\Delta t$  should be such that

$$e^{-s\Delta t} \approx 1 - s\Delta t \quad (6.28)$$

is approximately true. If, for example,  $s\Delta t = 10^{-1}$ , then  $e^{-0.1} = 0.9048$  while  $1.0 - 0.1 = 0.9$ .

An alternative analysis of the size of  $\Delta t$  could be done based on purely mathematical grounds by considering (2.4), a first-order difference equation, as an approximation to a first-order differential equation of the continuous time process. This analysis is more involved, however, and since it leads to similar conclusions it won't be presented here. The interested reader is referred to Henrici (1964) and Hildebrand (1968).

We conclude this section by noting that the difference between the discrete-time and continuous-time solutions lies only in the transient part, since both yield exactly the same steady-state solution.

#### 6.4 The Choice of the Size of the Time Step in a Monte Carlo Simulation

The Monte Carlo simulation is performed by a computer code that repeats  $N$  times the following steps:

1. Randomly select a set of transition rates from their respective pdf's.
2. The transition-rate matrix  $\underline{A}$  is generated such that

$$a_{ij} = \begin{cases} h_{rg}^v & \text{if } i \neq j \text{ and states } i \text{ and } j \text{ differ only} \\ & \text{in the state of component } v; \\ 0 & \text{if } i \neq j \text{ and states } i \text{ and } j \text{ differ in the} \\ & \text{state of more than one component;} \\ -\sum_{\substack{m=1 \\ m \neq i}}^Z a_{im} & \text{if } i=j \end{cases} \quad (6.29)$$

3. The maximum, in absolute value,  $a_{ij}$  is chosen and the time step is defined such that

$$\Delta t \max\{a_{ij}\} = x \quad (6.29a)$$

where  $x$  is predetermined so that  $e^{-x} \approx 1-x$ .

4. The transition probability matrix  $\underline{P}$  is then generated such that

$$\underline{P} = \underline{I} + \underline{A} \Delta t \quad (6.30)$$

5. Equation (2.4) is solved for the desired time-horizon.  
Since for each trial a different set of transition rates is used, a different time step is determined, and therefore,

the reliability of the system is calculated at different points in time. To get around this problem the following procedure is followed. The time horizon  $T_0$  is divided into  $K$  "large" time steps  $T$  such that

$$T_0 = K T$$

Then along with the "small" time step  $\Delta t$  defined in (6.29a) an auxiliary time step  $\Delta t_1$  is defined such that

$$T = \text{in}[T/\Delta t] \Delta t + \Delta t_1, \quad (6.31)$$

where  $\text{in}[T/\Delta t]$  denotes the integer part of  $T/\Delta t$ . If now every  $\text{in}[T/\Delta t]$  regular time step  $\underline{p}$  is changed into  $\underline{p}_1$  where  $\underline{p}_1$  is defined in (6.30) with  $\Delta t_1$  in the place of  $\Delta t$ , the value of the desired reliability measure would be obtained at the end of each large time step for every trial.

The fact that the transition rates (input variables) are assumed to be random variables unbounded from above (see Section 4.5) presents the Monte Carlo simulation with another problem. From (6.29a) it follows that even if only one of the transition rates has a large value, the time step  $\Delta t$  will be very small, and thus the simulation can be very expensive. Of course, a small time step does not necessarily mean an expensive run, since if all or most of the transition rates take large values, the steady state is reached by the system fairly soon and this means a reasonable number of (small) time steps. If, however, the transition rates are such that one takes values

significantly larger than the others, then the steady state of the system might not be achievable within a reasonable number of time steps. This is due to the fact that the time step is small enough to describe the fast changes of the state of a particular component, while the system changes of state (as far as system-failure or system-repair is concerned) are much slower and they do not require such a small time step. Whenever such differences exist in the values of the transition rates, the Monte Carlo simulation can become inhibitive expensive. One way of getting around this problem is presented in the rest of this section.

Let  $\underline{x}_n = \{x_{in}, \dots, x_{mn}\}$  be the input set for the n-th Monte Carlo trial and let  $\underline{x}_n$  be such that one of the transition rates,  $x_{kn}$  for example, is much larger than the rest. Let  $i \rightarrow j^*$  be a system state transition such that  $h_{ij^*} = x_{kn}$ . Then, if  $\Delta t$  is large enough that

$$e^{-x_{kn} \Delta t} \approx 0, \quad (6.32)$$

it follows from (6.25a) that

$$p_{ij^*} = 1. \quad (6.33)$$

Furthermore, by virtue of (6.32) and (6.25b), it follows that

$$p_{ii} = 0 \quad (6.34)$$

and that

$$p_{ij} = 0 \quad \text{if } j \neq j^* \quad (6.34a)$$

We assume, in other words, that if the system is in state  $i$ , its next transition at the end of a large time step will be to state  $j^*$  (where  $j^*$  is determined by  $x_{kn}$ ) with probability 1.

The definition of  $\underline{p}$  (see steps 2 through 4) is then modified as it follows:

1. Select at random a set of transition rates from their respective pdf's. Examine to find if there is a single transition rate larger than a predetermined value  $x_0$  while all the others are smaller than  $x_0$ . If not, proceed as in steps 2 to 5 mentioned earlier. If yes, let  $x_{kn}$  be this transition rate. Then:
2. For each state  $i$ , examine to see if there is a state  $j^*$  such that

$$h_{ij^*} = x_{kn} .$$

If such a state  $j^*$  does exist, then denote state  $i$  by  $i^*$  and set

$$a_{i^*j} = \begin{cases} 1 & \text{if } j = j^* \\ 0 & \text{otherwise} \end{cases} , \quad (6.35)$$

If a state  $j^*$  does not exist, then  $a_{ij}$  is defined as in (6.29).

3. The maximum, in absolute value,  $a_{ij}$  is chosen and the time step is defined such that [see (6.29a)]

$$\Delta t \max \{a_{ij}\} = x \quad .$$

Note that  $a_{i^*j^*} = 0$  because of (6.35).

4. The transition probability matrix  $\underline{P}$  is then generated such that

$$P_{ij} = \begin{cases} \delta_{ij} + a_{ij} \Delta t & \text{if } i \neq i^* , \\ 1 & \text{if } i = i^* \text{ and } j = j^* , \\ 0 & \text{if } i = i^* \text{ and } j \neq j^* , \end{cases}$$

where  $\delta_{ij}$  is the Kronecker delta. Note that there might be more than one state designated as  $i^*$ . It must be emphasized at this point that this procedure is applied only when one of the transition rates differs significantly from the others. This is due to the special structure of  $\underline{P}$  given in (2.14). Because the transition probability between two system states that differ (for example) in the states of two components, is given by (see 6.23)

$$p_{ij} = (1 - e^{-h_1 \Delta t}) (1 - e^{-h_2 \Delta t}) \quad ,$$



it follows from (6.32) that if both  $h_1$  and  $h_2$  have similar values and  $\Delta t$  is large enough, then

$$P_{ij} \approx 1 \quad .$$

The computer codes used in this work, however, were written under the assumption that transitions involving the change of state of more than two components have negligible probability and that, therefore,  $\underline{P}$  has the structure given in (2.14). One of course could allow such transitions to occur, but then the storage requirements would increase in a way that would negate the gains from the increase of the time step. If, on the other hand, only transitions involving the larger, say  $h_2$ , were artificially put equal to 1, the choice of the time step  $\Delta t$  will be controlled by  $h_1$  and it will be such that  $e^{-h_1 \Delta t} \approx 1 - h_1 \Delta t$ , and therefore, the assumption that  $1 - e^{-h_2 \Delta t} \approx 1$  will not be valid.

A numerical example of this procedure is presented in the following subsection.

#### 6.4.1 A numerical example

To illustrate the approximate method discussed in the previous section, we once more consider the system described in Section 2.5. The transition rates and the dependence coefficients are assumed to be random variables distributed according to gamma pdf's. The parameters of these pdf's are given in Table 7.4 and the random samples obtained in the Monte Carlo simulation in Tables 6.5 through 6.15. Histograms of the negative common logarithms of the transition rates are also given

in Figure 6.2. Examination of these tables reveals that the transition rate that takes the larger values is  $h_6 = k_2 \mu_1$ , i.e., the repair rate of the pumps when only one is failed (see Table 7.3). Furthermore, we notice that only this transition rate takes values larger than 0.08 (see also Figure 6.2). The cutoff value  $x_0$  (see step 1, p. 97) is, therefore, set at this level:  $x_0 = 0.08$ . The Monte Carlo simulation was executed as it was described in Section 6.4, and the results for the expected value of the failure probability with on-line repair are presented numerically in Table 6.3 and graphically in Figure 6.3. While the exact calculation (no cutoff value) required 170 sec, the approximation required only 136 sec. It is noteworthy that even if only 7% of the values of  $h_6$  were above the cutoff value of  $x_0$ , and therefore only 7% of the trials were affected, a reduction of 20% in the necessary computing time was achieved. A higher reduction in the computing time could be achieved if the cutoff value is set at a lower level, say at  $x_0 = 0.04$ . This time 18% of the values of  $h_6$  are larger than  $x_0$  and the Monte Carlo simulation can be executed in only 95 sec, a reduction of 44%. The error in the computed expected values, however, is rather large, on the order of 50%. This is due to the fact that many values of the transition  $h_5$  are very close to 0.04 (see Table 6.8). In fact, 1% of the values of  $h_5$  are above it. Even though the probability that values of  $h_5$  near or above  $x_0$  will occur simultaneously with values of  $h_6$  above  $x_0$  is small, such pairs do occur in the sample and contribute to the error.

To illustrate the importance of the location of the cutoff value  $x_0$  with respect to the transition rate, the expected value of the failure

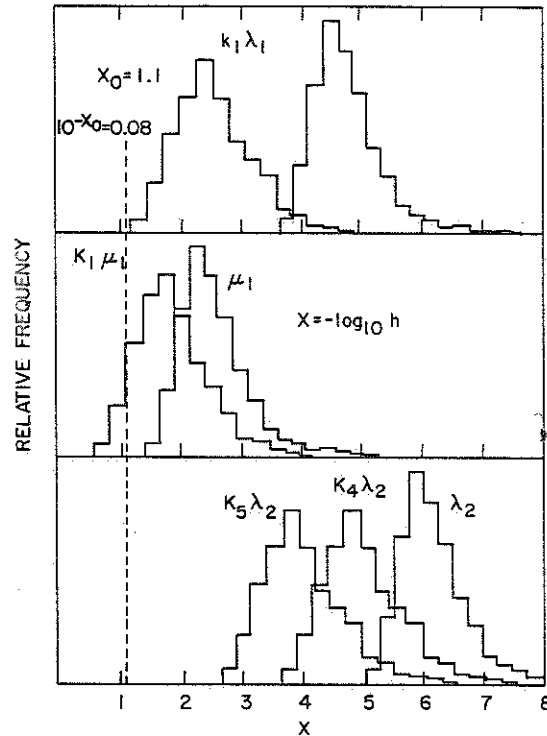


Figure 6.2. Histograms of the negative common logarithm of some transition rates of components of the sample system.

probability without repair was calculated. This time the dependence coefficient  $k_1$  (see Table 7.3) was assumed distributed according to a gamma pdf with mean value equal to 601, while all the other parameters were unchanged. The resulting sample for the transition rate  $h_5 = k_1 \lambda_1$  is presented in Table 6.16. From this table it follows that 50% of the values of  $h_5$  are above 0.01. Furthermore, examination of Tables 6.4, 6.6, and 6.10 to 6.12 reveals that the rest of the failure rates take values far below 0.01. Thus, the cutoff value was set at  $x_0 = 0.01$ , and the results are presented in Table 6.4 and Figure 6.3. A reduction of 70% in the computing time was achieved and the approximate results differ from the exact by only 7%.

TABLE 6.3  
Expected failure probability with repair for  
various cutoff values  $x_0$ .

Cutoff value → Time (Hr) ↓	Failure Probability with Repair		
	Regular Run	$x_0=0.08$	$x_0=0.04$
200	$0.2 \times 10^{-2}$	$0.1 \times 10^{-2}$	$0.1 \times 10^{-2}$
400	$0.4 \times 10^{-2}$	$0.3 \times 10^{-2}$	$0.2 \times 10^{-2}$
600	$0.6 \times 10^{-2}$	$0.5 \times 10^{-2}$	$0.3 \times 10^{-2}$
800	$0.8 \times 10^{-2}$	$0.7 \times 10^{-2}$	$0.4 \times 10^{-2}$
1000	$1.0 \times 10^{-2}$	$0.8 \times 10^{-2}$	$0.5 \times 10^{-2}$
1200	$1.3 \times 10^{-2}$	$1.0 \times 10^{-2}$	$0.6 \times 10^{-2}$
1400	$1.5 \times 10^{-2}$	$1.2 \times 10^{-2}$	$0.8 \times 10^{-2}$
1600	$1.7 \times 10^{-2}$	$1.4 \times 10^{-2}$	$0.9 \times 10^{-2}$
1800	$1.9 \times 10^{-2}$	$1.5 \times 10^{-2}$	$1.0 \times 10^{-2}$
2000	$2.1 \times 10^{-2}$	$1.7 \times 10^{-2}$	$1.1 \times 10^{-2}$
Computing Time (sec)	170	136	95

TABLE 6.4  
Expected failure proba-  
bility without repair:  
regular run ( $x_0=\infty$ ) and  
 $x_0=0.01$ .

F. Prob. without Repair	
Regular Run	$x_0=0.01$
$0.8 \times 10^{-2}$	$0.100 \times 10^{-2}$
$2.0 \times 10^{-2}$	$1.3 \times 10^{-2}$
$3.1 \times 10^{-2}$	$2.5 \times 10^{-2}$
$4.3 \times 10^{-2}$	$3.6 \times 10^{-2}$
$5.4 \times 10^{-2}$	$4.8 \times 10^{-2}$
$6.5 \times 10^{-2}$	$5.9 \times 10^{-2}$
$7.5 \times 10^{-2}$	$7.0 \times 10^{-2}$
$8.6 \times 10^{-2}$	$8.0 \times 10^{-2}$
$10.0 \times 10^{-2}$	$9.1 \times 10^{-2}$
$10.6 \times 10^{-2}$	$10.1 \times 10^{-2}$
70	22

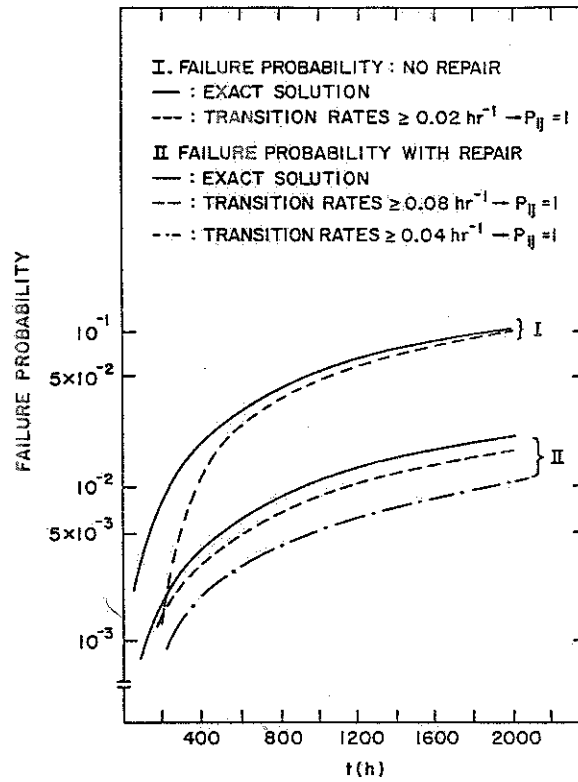


Figure 6.3. Expected value of future probability for various cutoff values  $x_0$ .

TABLE 6.5 Random Sample for  $\lambda_1$ .

CLASS	FROM	TO	FREQUENCY
1	.00000	.00001	362
2	.00001	.00002	274
3	.00002	.00004	173
4	.00004	.00005	146
5	.00005	.00006	73
6	.00006	.00007	48
7	.00007	.00008	43
8	.00008	.00009	19
9	.00009	.00011	19
10	.00011	.00012	16
11	.00012	.00013	7
12	.00013	.00014	8
13	.00014	.00015	4
14	.00015	.00016	5
15	.00016	.00018	1
16	.00018	.00019	0
17	.00019	.00020	0
18	.00020	.00021	1
19	.00021	.00022	0
20	.00022	.00024	0
		TOTAL	= 1200

TABLE 6.6 Random Sample for  $\mu_1$ .

CLASS	FROM	TO	FREQUENCY
1	.00000	.00196	326
2	.00196	.00392	274
3	.00392	.00588	173
4	.00588	.00784	146
5	.00784	.00980	73
6	.00980	.01176	48
7	.01176	.01372	43
8	.01372	.01568	19
9	.01568	.01763	19
10	.01763	.01959	16
11	.01959	.02155	7
12	.02155	.02351	8
13	.02351	.02547	4
14	.02547	.02743	5
15	.02743	.02939	1
16	.02939	.03135	0
17	.03135	.03331	0
18	.03331	.03527	1
19	.03527	.03723	0
20	.03723	.03919	0
		TOTAL	= 1200

TABLE 6.7 Random Sample for  $\lambda_2$ .

CLASS	FROM	TO	FREQUENCY
1	.00000	.00000	362
2	.00000	.00000	274
3	.00000	.00000	173
4	.00000	.00000	146
5	.00000	.00000	73
6	.00000	.00000	48
7	.00000	.00000	43
8	.00000	.00000	19
9	.00000	.00000	19
10	.00000	.00000	16
11	.00000	.00000	7
12	.00000	.00000	8
13	.00000	.00001	4
14	.00001	.00001	5
15	.00001	.00001	1
16	.00001	.00001	0
17	.00001	.00001	0
18	.00001	.00001	1
19	.00001	.00001	0
20	.00001	.00001	0
TOTAL =			1200



TABLE 6.8 Random Sample for  $\mu_2$ .

CLASS	FROM	TO	FREQUENCY
1	.00000	.00004	362
2	.00004	.00008	274
3	.00008	.00012	173
4	.00012	.00016	146
5	.00016	.00020	73
6	.00020	.00024	48
7	.00024	.00027	43
8	.00027	.00031	19
9	.00031	.00035	19
10	.00035	.00039	16
11	.00039	.00043	7
12	.00043	.00047	8
13	.00047	.00051	4
14	.00051	.00055	5
15	.00055	.00059	1
16	.00059	.00063	0
17	.00063	.00067	0
18	.00067	.00071	1
19	.00071	.00074	0
20	.00074	.00078	0
		TOTAL	= 1200

TABLE 6.9 Random Sample for  $h_5 = k_1 \cdot \lambda_1$ .

CLASS	FROM	TO	FREQUENCY
1	.00000	.00319	582
2	.00319	.00636	255
3	.00636	.00958	131
4	.00958	.01277	81
5	.01277	.01597	47
6	.01597	.01916	23
7	.01916	.02235	20
8	.02235	.02555	20
9	.02555	.02874	9
10	.02874	.03193	12
11	.03193	.03513	5
12	.03513	.03832	3
13	.03832	.04151	3
14	.04151	.04471	2
15	.04471	.04790	3
16	.04790	.05109	2
17	.05109	.05429	1
18	.05429	.05748	0
19	.05748	.06067	0
20	.06067	.06387	0
		TOTAL	= 1200

TABLE 6.10 Random Sample for  $h_6 = k_2 \cdot \mu_1$ .

CLASS	FROM	TO	FREQUENCY
1	.00000	.01198	507
2	.01198	.02396	282
3	.02396	.03594	145
4	.03594	.04792	89
5	.04792	.05990	64
6	.05990	.07188	28
7	.07188	.08386	20
8	.08386	.09584	20
9	.09584	.10782	11
10	.10782	.11980	11
11	.11980	.13178	6
12	.13178	.14376	5
13	.14376	.15573	4
14	.15573	.16771	1
15	.16771	.17969	2
16	.17969	.19167	3
17	.19167	.20365	1
18	.20365	.21563	0
19	.21563	.22761	0
20	.22761	.23959	0
		TOTAL	= 1200

TABLE 6.11 Random Sample for  $h_7 = k_3 \cdot \lambda_2$ .

CLASS	FROM	TO	FREQUENCY
1	.00000.	.00001	549
2	.00001	.00001	271
3	.00001	.00002	132
4	.00002	.00002	87
5	.00002	.00003	56
6	.00003	.00003	22
7	.00003	.00004	21
8	.00004	.00004	17
9	.00004	.00005	12
10	.00005	.00006	11
11	.00006	.00006	7
12	.00006	.00007	3
13	.00007	.00007	3
14	.00007	.00008	2
15	.00008	.00008	3
16	.00008	.00009	2
17	.00009	.00009	1
18	.00009	.00010	0
19	.00010	.00011	0
20	.00011	.00011	0
TOTAL			= 1200

TABLE 6.12 Random Sample for  $h_3 = k_4 \cdot \lambda_2$ .

CLASS	FROM	TO	FREQUENCY
1	.00000	.00001	566
2	.00001	.00002	263
3	.00002	.00003	131
4	.00003	.00004	86
5	.00004	.00005	50
6	.00005	.00007	21
7	.00007	.00008	21
8	.00008	.00009	19
9	.00009	.00010	11
10	.00010	.00011	12
11	.00011	.00012	4
12	.00012	.00013	4
13	.00013	.00014	3
14	.00014	.00015	2
15	.00015	.00016	3
16	.00016	.00017	2
17	.00017	.00019	1
18	.00019	.00020	0
19	.00020	.00021	0
20	.00021	.00022	0
		TOTAL	= 1200

TABLE 6.13 Random Sample for  $h_9 = k_5 \cdot \lambda_2$ .

CLASS	FROM	TO	FREQUENCY
1	.00001	.00011	582
2	.00011	.00021	255
3	.00021	.00032	131
4	.00032	.00043	81
5	.00043	.00053	47
6	.00053	.00064	23
7	.00064	.00075	20
8	.00075	.00085	20
9	.00085	.00096	9
10	.00096	.00106	12
11	.00106	.00117	5
12	.00117	.00128	3
13	.00128	.00138	3
14	.00138	.00149	2
15	.00149	.00160	3
16	.00160	.00170	2
17	.00170	.00181	1
18	.00181	.00192	0
19	.00192	.00202	0
20	.00202	.00213	0
		TOTAL	= 1200

TABLE 6.14 Random Sample for  $h_{10} = k_6 \cdot \mu_2$ .

CLASS	FROM	TO	FREQUENCY
1	.00000	.00109	566
2	.00109	.00218	263
3	.00218	.00327	131
4	.00327	.00436	86
5	.00436	.00544	50
6	.00544	.00653	21
7	.00653	.00762	21
8	.00762	.00871	19
9	.00871	.00980	11
10	.00980	.01089	12
11	.01089	.01198	4
12	.01198	.01307	4
13	.01307	.01416	3
14	.01416	.01525	2
15	.01525	.01633	3
16	.01633	.01742	2
17	.01742	.01851	1
18	.01851	.01960	0
19	.01960	.02069	0
20	.02069	.02178	0
TOTAL			= 1200

TABLE 6.15 Random Sample for  $h_5 = k_1 \cdot \lambda_1$ , where  $\bar{k}_1 = 601$ .

CLASS	FROM	TO	FREQUENCY
1	.00000	.00956	584
2	.00956	.01913	255
3	.01913	.02869	130
4	.02869	.03825	80
5	.03825	.04782	48
6	.04782	.05738	22
7	.05738	.06694	20
8	.06694	.07651	20
9	.07651	.08607	9
10	.08607	.09563	12
11	.09563	.10520	5
12	.10520	.11476	3
13	.11476	.12432	3
14	.12432	.13389	2
15	.13389	.14345	3
16	.14345	.15301	2
17	.15301	.16258	1
18	.16258	.17214	0
19	.17214	.18170	0
20	.18170	.19127	0
		TOTAL	= 1200



## CHAPTER SEVEN

### THE TAYLOR SERIES APPROXIMATION

#### 7.1 Introduction

An approximation of the moments of the reliability can be obtained by expanding the function  $R(x_1, \dots, x_m)$  [see (4.1)], into a Taylor series around the mean values of the  $x_i$ 's and retaining only a finite number of terms. This approximate form of the function  $R$  is then used for the calculation of the moments. This method was originally presented by Tukey (a,b,c, 1957) in a series of three reports. It has also been used by Evans (1974) and Hahn and Shapiro (1967) for non-nuclear applications and by Apostolakis and Lee to calculate the moments of the top event of a fault tree. A different version of this technique is found in the literature under the name of response-surface method. This later technique is used to provide an analytical approximation of a function  $R(x_1, \dots, x_m)$  whenever its derivatives cannot be calculated, and the only information about  $R$  is in the form of specific "responses"  $R_v$  to various inputs  $\underline{x}^v$ . The responses are made available via real or numerical experiments. This chapter is organized as follows: Section 7.2 discusses the Taylor series approximation for the calculation of the moments of a function of random variables; Section 7.3 presents the method for the calculation of the derivatives of the  $n$ -th power of the transition probability matrix  $\underline{P}$ ; Section 7.4 presents results of the Taylor method for a two-state system; and Section 7.5 presents results of the Taylor and the moment-matching methods for the sample system described in Chapter Two.

## 7.2 Approximate Evaluation of the System-Moments by Taylor Series Expansion

An approximate closed form of the function  $R(x_1, \dots, x_m)$  [see (4.1)] can be obtained by expanding it in a Taylor series around the expected values  $\bar{x}_i$ 's of  $x_i$ 's and retaining only the first few terms. If terms up to fourth order are retained, this procedure yields

$$\begin{aligned}
 R(x_1, \dots, x_m) = & R(\bar{x}_1, \dots, \bar{x}_m) + \sum_i \frac{\partial R}{\partial x_i} (x_i - \bar{x}_i) \\
 & + \frac{1}{2!} \sum_i \sum_j \frac{\partial^2 R}{\partial x_i \partial x_j} (x_i - \bar{x}_i)(x_j - \bar{x}_j) \\
 & + \frac{1}{3!} \sum_i \sum_j \sum_k \frac{\partial^3 R}{\partial x_i \partial x_j \partial x_k} (x_i - \bar{x}_i)(x_j - \bar{x}_j)(x_k - \bar{x}_k) \\
 & + \frac{1}{4!} \sum_i \sum_j \sum_k \sum_r \frac{\partial^4 R}{\partial x_i \partial x_j \partial x_k \partial x_r} (x_i - \bar{x}_i)(x_j - \bar{x}_j)(x_k - \bar{x}_k)(x_r - \bar{x}_r) ,
 \end{aligned} \tag{7.1}$$

where the partial derivatives are evaluated at the point  $(\bar{x}_1, \dots, \bar{x}_m)$  and all summations extend from 1 to  $m$ .

This expression of  $R$  can now be used to determine any moment of  $R$  about the origin [see (5.4)] or about its mean [see (5.3)]. If  $\mu_k^i$  denotes the  $k$ -th central moment of  $x_i$ , the combination of (5.3), (5.5), and (7.1) yields

$$\begin{aligned}
E[R] &= R(\bar{x}_1, \dots, \bar{x}_m) + \frac{1}{2} \sum_{i=1}^m \frac{\partial^2 R}{\partial x_i^2} \mu_2^i + \frac{1}{6} \sum_{i=1}^m \frac{\partial^3 R}{\partial x_i^3} \mu_3^i \\
&+ \frac{1}{24} \sum_{i=1}^m \frac{\partial^4 R}{\partial x_i^4} \mu_4^i + \frac{1}{24} \sum_{i=1}^{m-1} \sum_{j=i+1}^m \frac{\partial^4 R}{\partial x_i^2 \partial x_j^2} (\mu_2^i)(\mu_2^j) ; \quad (7.2)
\end{aligned}$$

$$\begin{aligned}
\text{var}[R] &= \sum_{i=1}^m \left( \frac{\partial R}{\partial x_i} \right)^2 \mu_2^i + \sum_{i=1}^m \left( \frac{\partial R}{\partial x_i} \right) \left( \frac{\partial^2 R}{\partial x_i^2} \right) \mu_3^i \\
&+ \frac{1}{3} \sum_{i=1}^m \left( \frac{\partial R}{\partial x_i} \right) \left( \frac{\partial^3 R}{\partial x_i^3} \right) \mu_4^i + \frac{1}{4} \sum_{i=1}^m \left( \frac{\partial^2 R}{\partial x_i^2} \right)^2 [\mu_4^i - (\mu_2^i)^2] ; \quad (7.3)
\end{aligned}$$

$$\mu_3(R) = \sum_{i=1}^m \left( \frac{\partial R}{\partial x_i} \right)^3 \mu_3^i + \frac{3}{2} \sum_{i=1}^m \left( \frac{\partial R}{\partial x_i} \right)^2 \left( \frac{\partial^2 R}{\partial x_i^2} \right) [\mu_4^i - (\mu_2^i)^2] ; \quad (7.4)$$

$$\mu_4(R) = \sum_{i=1}^m \left( \frac{\partial R}{\partial x_i} \right)^4 [\mu_4^i - 3(\mu_2^i)^2] + 3(\text{var}[R])^2 ; \quad (7.5)$$

where it has been assumed that the  $x_i$ 's are uncorrelated (see Section 4.5), and therefore cross products of order  $E[(x_i - \bar{x}_i)(x_j - \bar{x}_j)]$  and higher vanish. These results are also presented by Tukey (a,b,c, 1957) and Evans (1974), while results for correlated  $x_i$ 's are presented by Tukey and including up to second-order terms by Hahn and Shapiro (1967).

The problem of estimating the first four moments of the reliability reduces, therefore, into the calculation of the various derivatives of  $R$  that are encountered in (7.2) through (7.5). This problem is examined in detail in Section 7.3.

Some general remarks concerning the accuracy and usefulness of this approach are appropriate at this point. The expression given in (7.1) is not a good approximation of  $R(x_1, \dots, x_m)$  except for small deviations of the  $x_i$ 's from their mean values. Equations (7.2) through (7.5) could, nevertheless, be good approximations of the various moments since they are expectations of (7.1) and since this expectation assigns weights (probabilities) to the various points. The probability that the point  $(x_1, \dots, x_m)$  will take a value "far" from its mean  $(\bar{x}_1, \dots, \bar{x}_m)$  or, equivalently, the probability that all  $x_i$ 's will take values simultaneously "far" from their respective means is usually small. Equations (7.2) through (7.5) provide, therefore, expressions for the moments of  $R$  that consist mainly of contributions from points  $(x_1, \dots, x_m)$  that are "near" the mean, and hence of points for which (7.1) gives a relatively good approximation of  $R$ . It is expected, therefore, that (7.2) through (7.5) will yield good estimations of the central moments of  $R$  in cases that the joint pdf of the  $x_i$ 's is not extremely flat (in an  $m$ -dimensional sense).

Whenever accurate, this method also provides a tool for performing a partial sensitivity analysis. Indeed, once the derivatives and the value of  $R$  at  $(\bar{x}_1, \dots, \bar{x}_m)$  are evaluated, (7.2) through (7.5) provide the central moments of  $R$  for any set of central moments  $\mu_k^i$  of the  $x_i$ 's. Alternatively stated, the coefficient of  $\mu_2^i$ , in (7.2) for example,

provides a measure of the contribution of the variance of  $x_i$  to the expected value of  $R$ . Thus, once the accuracy of (7.2) to (7.5) has been checked (perhaps with a Monte Carlo calculation) at a certain level of the means  $\bar{x}_i$ , the sensitivity of the moments of  $R$  to variations of the central moments of the  $x_i$ 's can be studied. If the mean values  $\bar{x}_i$  are changed, however, the derivatives and the value of  $R$  at the new values of  $\bar{x}_i$ 's must be recalculated. This is not a lengthy calculation per se, but the accuracy of (7.2) to (7.5) at this new level of  $\bar{x}_i$ 's must be checked again (possibly by a new Monte Carlo calculation).

### 7.3 Evaluation of Derivatives

In this section recurrence formulas are developed for the evaluation of the derivatives of  $R$  necessary for the calculation of the moments in (7.2) to (7.5). For this derivation the following definitions are needed.

Definition 7.1 The  $k$ -th derivative of an  $1 \times z$  vector  $\underline{u}$  with respect to a scalar  $x$ , is an  $1 \times z$  vector, denoted by  $\partial^k \underline{u} / \partial x^k$  and defined by

$$\frac{\partial^k \underline{u}}{\partial x^k} \equiv \left[ \frac{\partial^k u_1}{\partial x^k}, \dots, \frac{\partial^k u_z}{\partial x^k} \right] \quad (7.6)$$

Definition 7.2 The  $k$ -th derivative of a matrix  $\underline{Y}$  with respect to a scalar  $x$  is a matrix denoted by  $\partial^k \underline{Y} / \partial x^k$  and defined by

$$\frac{\partial^k \underline{Y}}{\partial x^k} \equiv \left[ \frac{\partial^k y_{ij}}{\partial x^k} \right] \quad (7.7)$$

Furthermore, it can be easily shown that the derivative of a product of two matrices is given by

$$\frac{\partial}{\partial x} \{ \underline{Y} \cdot \underline{G} \} = \frac{\partial \underline{Y}}{\partial x} \cdot \underline{G} + \underline{Y} \cdot \frac{\partial \underline{G}}{\partial x} \quad (7.8a)$$

and that if  $\underline{A}$  is matrix the elements of which are not functions of  $x$

$$\frac{\partial}{\partial x} \{ \underline{A} \cdot \underline{Y} \} = \underline{A} \cdot \frac{\partial \underline{Y}}{\partial x} \quad (7.8b)$$

By virtue of (4.6), it follows that

$$\frac{\partial^k R(n)}{\partial x_i^k} = \sum_{i \in X} \sum_{j=1}^Z \pi_j^{(0)} \frac{\partial^k p_{ji}^{(n)}}{\partial x_i^k} \quad (7.9)$$

We introduce the symbolism

$$\underline{D}_{k;i}^{(n)} \equiv \frac{\partial^k p_{ji}^{(n)}}{\partial x_i^k} \quad , \quad (7.10a)$$

$$\underline{d}_{k;i}^{(n)} \equiv \frac{\partial^k \pi_j^{(n)}}{\partial x_i^k} \quad , \quad (7.10b)$$

and thus (7.9) can be written as

$$\frac{\partial^k R(n)}{\partial x_i^k} = \sum_{i \in X} \pi_j^{(0)} \cdot \underline{D}_{k;i}^{(n)} \quad (7.11)$$

or

$$\frac{\partial^k R(n)}{\partial x_i^k} = \sum_{i \in X} \underline{d}_{k;i}^{(n)} \quad , \quad (7.12)$$

where it has been assumed that  $\underline{\pi}(0)$  is constant (not a function of the  $x_i$ 's). By virtue of (7.8) and of

$$\underline{p}^n = \underline{p}^{n-1} \cdot \underline{p} \quad ,$$

it follows that

$$\frac{\partial \underline{p}^n}{\partial x_i} = \frac{\partial \underline{p}^{n-1}}{\partial x_i} \cdot \underline{p} + \underline{p}^{n-1} \cdot \frac{\partial \underline{p}}{\partial x_i}$$

or that

$$\underline{D}_{1;i}^{(n)} = \underline{D}_{1;i}^{(n-1)} \cdot \underline{D}_{0;i}^{(1)} + \underline{D}_{0;i}^{(n-1)} \cdot \underline{D}_{1;i}^{(1)} \quad . \quad (7.13)$$

Repeated differentiation of (7.13) then yields

$$\underline{D}_{k;i}^{(n)} = \sum_{v=0}^k \binom{k}{v} \cdot \underline{D}_{k-v;i}^{(n-1)} \cdot \underline{D}_{v;i}^{(1)} \quad ; \quad (7.14)$$

or by left multiplying both sides of (7.14) by  $\underline{\pi}(0)$

$$\underline{d}_{k;i}^{(n)} = \sum_{v=0}^k \binom{k}{v} \underline{d}_{k-v;i}^{(n-1)} \cdot \underline{D}_{v;i}^{(1)} \quad . \quad (7.15)$$

Thus,  $\underline{d}_{k;i}^{(n)}$  can be obtained from (7.15) recurrently and then the derivatives of  $R$  are calculated from (7.12). The elements of  $\underline{p}$  are linear functions of the various  $x_i$ 's [see (2.9) and Section 4.5], and therefore it follows that

$$\underline{D}_{v;i}^{(1)} = \begin{cases} \underline{p} & \text{if } v=0 \\ \frac{\partial \underline{p}}{\partial x_i} & \text{if } v=1 \\ 0 & \text{if } v \geq 2 \end{cases}, \quad (7.16)$$

By virtue of (7.15) and (7.16) it follows, therefore, that

$$\underline{d}_{1;i}^{(n)} = \underline{d}_{1;i}^{(n-1)} \cdot \underline{p} + \underline{\pi}^{(n-1)} \cdot \underline{D}_{1;i}^{(1)}, \quad (7.17a)$$

$$\underline{d}_{2;i}^{(n)} = \underline{d}_{2;i}^{(n-1)} \cdot \underline{p} + 2\underline{d}_{1;i}^{(n-1)} \cdot \underline{D}_{1;i}^{(1)}, \quad (7.17b)$$

$$\underline{d}_{3;i}^{(n)} = \underline{d}_{3;i}^{(n-1)} \cdot \underline{p} + 3\underline{d}_{2;i}^{(n-1)} \cdot \underline{D}_{1;i}^{(1)}, \quad (7.17c)$$

$$\underline{d}_{4;i}^{(n)} = \underline{d}_{4;i}^{(n-1)} \cdot \underline{p} + 4\underline{d}_{3;i}^{(n-1)} \cdot \underline{D}_{1;i}^{(1)}, \quad (7.17d)$$

where again because of (7.16)



$$\underline{d}_{v;i}^{(1)} = \underline{\pi}(0) \cdot \underline{D}_{v;i}^{(1)} = \begin{cases} \underline{\pi}(1) & \text{if } v=0 \\ \underline{\pi}(0) \cdot \frac{\partial \underline{P}}{\partial x_i} & \text{if } v=1 \\ 0 & \text{if } v \geq 2 \end{cases} \quad (7.18)$$

Equations (7.17) combined with (7.12) provide the derivatives of  $R(n)$  necessary for the calculations of the moments in (7.2) through (7.5).

It should be noted that the method just cited can be used for the calculation of the moments of any function  $y=u(R)$  of  $R$ . Indeed, the derivatives of  $y$  with respect to the  $x_i$ 's can be calculated with the help of the chain rule. For the first derivative, for example, we have that

$$\frac{\partial y}{\partial x} = \frac{\partial u}{\partial R} \frac{\partial R}{\partial x} \quad (7.19)$$

Since  $u(R)$  is a known function,  $\partial u/\partial R$  can be calculated at  $x=\bar{x}$ .

A computer code has been written that calculates the derivatives of the state probability vector  $\underline{d}_{v;i}^{(n)}$  presented in (7.17a) through (7.17d). Then, the derivatives and moments of  $R(n)$  are evaluated from (7.12) and (7.2) to (7.5), respectively. Numerical examples of this method are presented in the next two sections.

#### 7.4 Numerical Example of a Two-State System

Let us assume that the failure rate  $\lambda$  and the repair rate  $\mu$  of a two-state system are distributed according to gamma pdf's with

parameters  $r_1, y_1$  and  $r_2, y_2$ , respectively [see (4.16)],

$$f_Y(\lambda|r_1, y_1) = \frac{\exp[-y_1 \lambda] (y_1 \lambda)^{r_1-1}}{\Gamma(r_1)} y_1, \quad (7.20a)$$

$$f_Y(\mu|r_2, y_2) = \frac{\exp[-y_2 \mu] (y_2 \mu)^{r_2-1}}{\Gamma(r_2)} y_2. \quad (7.20b)$$

Let us furthermore assume that the values of the parameters are

$$r_1=2, y_1=10^4, r_2=5, \text{ and } y_2=400 \quad (7.21)$$

so that the various moments of  $\lambda$  and  $\mu$  are given in Table 7.1.

#### 7.4.1 Time-dependent unavailability

The time-dependent unavailability of a two-state system is given by [see (4.30) and (4.31)]

$$U(n) = \frac{\lambda}{\mu+\lambda} - \frac{\lambda}{\mu+\lambda} [(\lambda+\mu) \Delta t] \quad (7.22)$$

The various derivatives of  $U(n)$  with respect to  $\lambda$  and  $\mu$  can be derived analytically from (7.21) and then used in (7.2) through (7.5). The resulting moments of  $U(n)$  for the data considered in (7.21) are presented in Table 7.2 where they are also compared with the results of a Monte Carlo simulation.

#### 7.4.2 Steady-state unavailability

By virtue of (7.22) it follows that the steady-state unavailability

TABLE 7.1 Moments of gamma distributed failure and repair rates of a 2-state system.

MOMENTS	$\lambda$ (i=1)	$\mu$ (i=2)
$\mu_1^i$	$2 \times 10^{-4}$	$1.250 \times 10^{-2}$
$\mu_2^i$	$2 \times 10^{-8}$	$3.125 \times 10^{-5}$
$\mu_3^i$	$4 \times 10^{-12}$	$1.563 \times 10^{-7}$
$\mu_4^i$	$2.4 \times 10^{-15}$	$4.102 \times 10^{-9}$

TABLE 7.2 Expected value and variance of dynamic failure probability of a 2-state system. Transition rates distributed according to gamma pdf's.

TIME	E[U(n)]		var[U(n)]	
	TAYLOR	MONTE CARLO	TAYLOR	MONTE CARLO
200	$1.62 \times 10^{-2}$	$1.62 \times 10^{-2}$	$1.40 \times 10^{-4}$	$1.65 \times 10^{-4}$
400	$1.89 \times 10^{-2}$	$1.84 \times 10^{-2}$	$2.13 \times 10^{-4}$	$2.56 \times 10^{-4}$
600	$1.97 \times 10^{-2}$	$1.90 \times 10^{-2}$	$2.31 \times 10^{-4}$	$2.96 \times 10^{-4}$
800	$1.99 \times 10^{-2}$	$1.92 \times 10^{-2}$	$2.34 \times 10^{-4}$	$3.15 \times 10^{-4}$
1000	$2.00 \times 10^{-2}$	$1.93 \times 10^{-2}$	$2.35 \times 10^{-4}$	$3.24 \times 10^{-4}$
1200	$2.00 \times 10^{-2}$	$1.93 \times 10^{-2}$	$2.35 \times 10^{-4}$	$3.29 \times 10^{-4}$
1400	$2.00 \times 10^{-2}$	$1.94 \times 10^{-2}$	$2.35 \times 10^{-4}$	$3.31 \times 10^{-4}$
1600	$2.00 \times 10^{-2}$	$1.94 \times 10^{-2}$	$2.35 \times 10^{-4}$	$3.33 \times 10^{-4}$
1800	$2.00 \times 10^{-2}$	$1.94 \times 10^{-2}$	$2.35 \times 10^{-4}$	$3.34 \times 10^{-4}$
2000	$2.00 \times 10^{-2}$	$1.94 \times 10^{-2}$	$2.35 \times 10^{-4}$	$3.35 \times 10^{-4}$
STEADY-STATE	TAYLOR	ANALYTICAL SOLUTION	TAYLOR	ANALYTICAL SOLUTION
T = $\infty$	$2.00 \times 10^{-2}$	$1.92 \times 10^{-2}$	$2.35 \times 10^{-4}$	$2.03 \times 10^{-4}$

is given by

$$U=U(\infty) = \frac{\lambda}{\mu+\lambda} \quad . \quad (7.23)$$

The desired moments of  $U$  are obtained by calculating the derivatives of  $U$  with respect to  $\lambda$  and  $\mu$  and substituting in (7.2) through (7.5). For this case, analytical results for  $E[U]$  and for  $\text{var}[U]$  can be obtained as follows: In Section 4.6.1 the first two moments of the steady-state availability of a two-state system were calculated for gamma-distributed  $\lambda$  and  $\mu$  [see (4.46) and (4.47)]. From these moments, the moments of  $U$  can be calculated from the following relations

$$E[U] = 1 - E[A] \quad , \quad (7.24a)$$

$$\text{var}[U] = E[U^2] - \{E[U]\}^2 = E\{1-A\}^2 - \{E[A]\}^2 \quad ,$$

or

$$\text{var}[U] = E[A^2] - \{E[A]\}^2 \quad . \quad (7.24b)$$

These results are included in Table 7.2.

## 7.5 An Example of the General Case

As an illustration of the Taylor-series expansion technique, the first four moments of various reliability measures of the sample system considered in Chapters Two and Three were calculated. A description of

the system and of the various interdependences are given in Section 2.5. The failure rates and repair rates of the components of the system are presented in Table 7.3 and they are assumed to be random variables distributed according to gamma pdf's. The values of the parameters of the pdf's as well as of the first four moments of the transition rates are given in Table 7.4. The dependence coefficients  $k_j$  are also assumed to be random variables such that the differences  $(k_j-1)$  are distributed according to gamma pdf's. The values of the parameters of the distribution and their first four moments are also given in Table 7.4.

The expected value and the next three central moments of the failure probability with repair and the failure probability without on-line repair were calculated and are presented in Tables 7.5 and 7.6, respectively. In the same tables the corresponding values of the moments obtained by Monte Carlo simulation are presented for comparison.

To illustrate the use of this kind of results in a "sensitivity" analysis, let us consider the expected value and the variance of the failure probability without repair at  $t=1000$  hr. The values for these two quantities shown in Table 7.6 were obtained by using the formulae [see (7.2) and (7.3) and Table 4.1]

$$D \equiv E[F] - F(\bar{x}_1, \dots, \bar{x}_m) = \sum_{i=1}^{12} \left( a_i + \frac{b_i}{r_i} \right) \frac{1}{r_i} \quad (7.25)$$

and

TABLE 7.3 Conditional transition rates for the components of system in Figure 2.1.

CONDITIONAL FAILURE RATES			CONDITIONAL REPAIR RATES	
PUMPS				
TWO UP	$\lambda_1$		-	
ONE UP	$k_1 \lambda_1$		$k_2 \mu_2$	
NONE UP	-		$\mu_1$	
VALVES	TO THE "OPEN POSITION"	TO THE "CLOSED POSITION"	FROM THE "OPEN POSITION"	FROM THE "CLOSED POSITION"
FOUR UP	$\lambda_2$	$\lambda_2$	-	-
THREE UP	$k_3 \lambda_2$	$k_3 \lambda_2$	$k_6 \mu_2$	$k_6 \mu_2$
TWO UP	$k_4 \lambda_2$	$k_4 \lambda_2$	$k_7 \mu_2$	$k_7 \mu_2$
ONE UP	$k_5 \lambda_2$	$k_5 \lambda_2$	$k_8 \mu_2$	$k_8 \mu_2$
NONE UP	-	-	$\mu_2$	$\mu_2$

$$\text{var}[F] = \sum_{i=1}^{12} \frac{c_i}{r_i}, \quad (7.26)$$

where the values of the coefficients  $a_i$ ,  $b_i$ , and  $c_i$  are given in Table 7.7 and  $r_i$  is the parameter of the corresponding gamma pdf's. From this table it can be seen that the contribution of the uncertainties about the dependence coefficients into the value of  $D$  [see (7.24)] and  $\text{var}[F]$  is negligible. More precisely, if the  $k$ 's were fixed at their respective mean values ( $r_i = \infty$ ,  $i=5,7,8,9$ ), then the value of  $D$  would change by only 9% while the value of  $\text{var}[F]$  by only 1.5%. It must be noted, however, that the above statement is true only for the specific values of  $\bar{x}_i$ 's and  $r_1$  and  $r_3$  given in Table 7.4.

As an illustration of the moment-matching technique, the pdf of the reliability without repair at  $t=1000$  hr was determined as it was described in Section 5.2 and the results were compared with the results of a Monte Carlo simulation. By virtue of (5.1), (5.2), and the values of  $\mu_3$  and  $\mu_4$ , an estimation of the coefficients  $\beta_1$ ,  $\beta_2$  was obtained. The location of the point  $(\beta_1, \beta_2)$  in Figure 5.1 indicates that the pdf in question resembles the most to a log-normal pdf. Once the type of the pdf is chosen, its parameters (here,  $\mu, \sigma$ ; see Table 4.1) are determined from the first moment and the variance. It must be noted at this point that even though the log-normal distribution describes variables unbounded from above, it can be used to approximate the true pdf of  $F$  ( $0 \leq F \leq 1$ ) in the region of interest since the contribution of the tail of  $f_{LN}(x|\mu, \sigma)$  for  $x > 1$  is negligible for the considered values of  $\mu$  and  $\sigma$ . The resulting log-normal pdf is plotted in Figure 7.1

together with a histogram obtained by a Monte Carlo simulation of 1200 trials. Cumulative probabilities from the log-normal pdf and the Monte Carlo simulation are presented in Table 7.8.



TABLE 7.4 Expected values and central moments of transition rates and dependence coefficients.

RANDOM VARIABLE $x_i$	Gamma pdf		$x_i = \frac{r_i}{y_i}$	$\mu_2 = \frac{i(x)^2}{r_i}$	$\mu_3 = \frac{2(x)^3}{r_i^2}$	$\mu_4 = \frac{3(r_i+2)(x_i)^4}{r_i^3}$
	$r_i$	$y_i$				
$x_1 = \lambda_1$	1.1	$3.67 \times 10^4$	$3 \times 10^{-5}$	$8.18 \times 10^{-10}$	$4.46 \times 10^{-14}$	$5.66 \times 10^{-18}$
$x_2 = \mu_1$	1.1	$2.20 \times 10^2$	$5 \times 10^{-3}$	$2.27 \times 10^{-5}$	$2.07 \times 10^{-7}$	$4.37 \times 10^{-9}$
$x_3 = \lambda_2$	1.1	$1.10 \times 10^6$	$1 \times 10^{-6}$	$9.09 \times 10^{-13}$	$1.65 \times 10^{-18}$	$6.99 \times 10^{-24}$
$x_4 = \mu_2$	1.1	$1.10 \times 10^4$	$1 \times 10^{-4}$	$9.09 \times 10^{-9}$	$1.65 \times 10^{-12}$	$6.99 \times 10^{-16}$
$x_5 = \kappa_1$	2	$9.95 \times 10^{-3}$	201	$2.02 \times 10^4$	$4.06 \times 10^6$	$2.45 \times 10^9$
$x_6 = \kappa_2$	2	$4.00 \times 10^{-1}$	5	$1.25 \times 10^1$	$6.25 \times 10^1$	$9.38 \times 10^2$
$x_7 = \kappa_3$	2	$1.81 \times 10^{-1}$	11	$6.05 \times 10^1$	$6.65 \times 10^2$	$2.20 \times 10^4$
$x_8 = \kappa_4$	2	$9.52 \times 10^{-2}$	21	$2.20 \times 10^2$	$4.63 \times 10^3$	$2.92 \times 10^5$
$x_9 = \kappa_5$	2	$9.95 \times 10^{-3}$	201	$2.02 \times 10^4$	$4.06 \times 10^6$	$2.45 \times 10^9$
$x_{10} = \kappa_6$	2	$9.52 \times 10^{-2}$	21	$2.20 \times 10^2$	$4.63 \times 10^3$	$2.92 \times 10^5$
$x_{11} = \kappa_7$	2	$1.81 \times 10^{-1}$	11	$6.05 \times 10^1$	$6.65 \times 10^2$	$2.20 \times 10^4$
$x_{12} = \kappa_8$	2	$2.86 \times 10^{-1}$	7	$2.45 \times 10^1$	$1.71 \times 10^2$	$3.60 \times 10^3$

TABLE 7.5 Expected value and central moments of failure probability with repair.

TIME (hrs)	E[F]		STANDARD DEVIATION		$\mu_3(F)$		$\mu_4(F)$	
	TAYLOR ( $\times 10^{-2}$ )	MONTE CARLO ( $\times 10^{-2}$ )	TAYLOR ( $\times 10^{-2}$ )	MONTE CARLO ( $\times 10^{-2}$ )	TAYLOR ( $\times 10^{-5}$ )	MONTE CARLO ( $\times 10^{-5}$ )	TAYLOR ( $\times 10^{-6}$ )	MONTE CARLO ( $\times 10^{-6}$ )
200	0.287	0.185	0.392	0.219	0.007	0.002	0.0030	0.0002
400	0.543	0.404	0.866	0.441	0.073	0.017	0.0570	0.0030
600	0.794	0.623	1.340	0.650	0.262	0.055	0.3020	0.0150
800	1.040	0.843	1.810	0.878	0.638	0.129	0.9710	0.0470
1000	1.290	1.060	2.280	1.090	1.260	0.247	2.3800	0.1110
1200	1.530	1.280	2.740	1.300	2.190	0.418	4.9200	0.2240
1400	1.770	1.500	3.210	1.510	3.500	0.649	9.0700	0.4020
1600	2.000	1.710	3.670	1.720	5.210	0.933	15.4000	0.6490
1800	2.230	1.920	4.130	1.920	7.410	1.280	24.4000	0.9900
2000	2.460	2.140	4.580	2.110	10.100	1.660	36.8000	1.4000

TABLE 7.6 Expected value and central moments of failure probability without repair.

TIME (hrs)	E[F]		STANDARD DEVIATION		$\mu_3(F)$		$\mu_4(F)$	
	TAYLOR ( $\times 10^{-2}$ )	MONTE CARLO ( $\times 10^{-2}$ )	TAYLOR ( $\times 10^{-2}$ )	MONTE CARLO ( $\times 10^{-2}$ )	TAYLOR ( $\times 10^{-4}$ )	MONTE CARLO ( $\times 10^{-4}$ )	TAYLOR ( $\times 10^{-4}$ )	MONTE CARLO ( $\times 10^{-4}$ )
200	0.690	0.494	0.735	0.905	0.006	0.022	0.0002	0.0009
400	0.968	1.470	2.200	2.050	0.186	0.198	0.0180	0.0170
600	2.070	2.530	3.400	3.170	0.708	0.656	0.1070	0.0840
800	3.440	3.600	4.480	4.250	1.660	1.460	0.3300	0.2400
1000	4.690	4.680	5.510	5.280	3.310	2.650	0.7660	0.5370
1200	5.830	5.740	6.520	6.270	5.210	4.220	1.5100	0.9990
1400	6.910	6.790	7.510	7.220	7.980	6.170	2.6600	1.6500
1600	7.950	7.830	8.470	8.120	11.500	8.460	4.3200	2.5200
1800	8.960	8.840	9.410	8.990	15.800	11.100	6.5900	3.6100
2000	9.960	9.840	10.300	9.820	20.900	13.900	9.560	4.9100

TABLE 7.7 Taylor series expansion coefficients for the expected value and the variance of the failure probability without repair at T=1000 hr.

TABLE 7.8 Cumulative probabilities for the failure probability without repair at T=1000 hr.

i	Variable	$a_i$	$b_i$	$c_i$	$F_0$	$\Pr\{F \leq F_0\}$	
						TAYLOR	MONTE CARLO
1	$\lambda_1 (\times 10^{-3})$	-15.000	-0.7700	3.300			
2	$\mu_1$	0.000	0.0000	0.000	$1.0 \times 10^{-3}$	0.060	0.100
3	$\lambda_2 (\times 10^{-3})$	0.039	0.0009	$9 \times 10^{-6}$	$4.0 \times 10^{-3}$	0.350	0.340
4	$\mu_2$	0.000	0.0000	0.000	$8.0 \times 10^{-3}$	0.580	0.530
5	$k_1 (\times 10^{-3})$	-9.500	18.0000	0.090	$1.2 \times 10^{-2}$	0.700	0.680
6	$k_2$	0.000	0.0000	0.000	$1.6 \times 10^{-2}$	0.780	0.780
7	$k_3 (\times 10^{-5})$	-0.067	-0.0010	$1 \times 10^{-4}$	$2.0 \times 10^{-2}$	0.830	0.850
8	$k_4 (\times 10^{-8})$	-1.600	0.0320	$1 \times 10^{-4}$	$3.2 \times 10^{-2}$	0.910	0.950
9	$k_5 (\times 10^{-10})$	-29.000	2.0000	$4 \times 10^{-5}$	$4.0 \times 10^{-2}$	0.940	0.980
10	$k_6$	0.000	0.0000	0.000	$4.8 \times 10^{-2}$	0.955	0.990
11	$k_7$	0.000	0.0000	0.000	$5.6 \times 10^{-2}$	0.966	0.994
12	$k_8$	0.000	0.0000	0.000	$6.0 \times 10^{-2}$	0.976	0.997

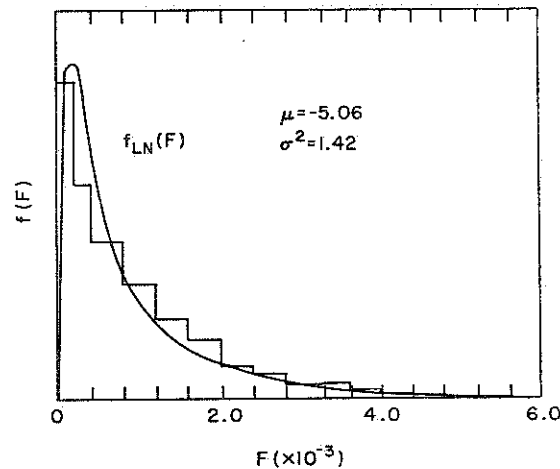


Figure 7.1. Pdf of failure probability without repair at t=1000 hr.

CHAPTER EIGHT

RELIABILITY ASSESSMENT OF THE CLINCH RIVER  
BREEDER REACTOR SHUTDOWN SYSTEM UNDER UNCERTAINTY

8.1 Introduction

The purpose of this chapter is to present the reliability assessment of the Clinch River Breeder Reactor Shutdown System under uncertainty. In particular, the probability of loss of coolable core geometry due to failure to scram on a transient has been evaluated in the presence of uncertainties about the failure data.

A point estimate of the reliability of the Reactor Shutdown System (RSS) of the CRBR has been presented in the Preliminary Safety Analysis Report (PSAR), Appendix C, and in WARD-D-0118. In the present analysis, it has been assumed that there is uncertainty about the failure data which can be accounted for by expressing the various transition rates and probabilities as random variables. Thus, the probability density function of the failure probability of the RSS has been calculated, and a confidence interval or probability band for the failure probability has been derived.

The techniques developed in Chapters 2 through 7 were employed in this analysis. The probabilistic behavior of the RSS was modeled as a Markov Process with all input variables being randomly distributed. The effect of common cause failures was included in the model by allowing interdependences between the failure rates of component and the states of other components in the system. In contrast to other studies, the assumption that the system unavailability is independent

of the challenge rate was relaxed. This is possible because the model allows for system renewal after a successful response to a transient, and because the model does not allow transients and, therefore, failures to occur while the reactor is shut down. The possibility of human errors during inspection of the system was also included. The probability density function of the failure probability has been calculated with both the Monte Carlo and the Taylor-series methods.

The chapter is organized as follows: Section 8.2 presents the description of the system; Section 8.3 describes the mission of the system and gives the reliability duty cycle; Section 8.4 develops the top-model for the system; Section 8.5 develops the detailed models for the subsystems and the system inspection; Section 8.6 gives the data base and the associated uncertainties; finally, Section 8.7 presents the results.

## 8.2 System Description

### 8.2.1 Introduction

The Reactor Shutdown System (RSS) of the Clinch River Breeder Reactor (CRBR) is designed to provide safe shutdown of the reactor, when required in response to normal and off-normal events. The overall RSS consists of two independent shutdown systems, the primary and the secondary. Each shutdown system is designed to independently terminate the effects of the anticipated and unlikely fault events, without exceeding specified core damage limits, and consists of an electrical and a mechanical subsystem. The primary and secondary electrical subsystems are designed to sense the need for a shutdown and signal the

primary and secondary mechanical subsystems, respectively, to insert the control rods into the reactor core.

This section provides a brief description of the RSS. A detailed description of the RSS, its subsystems, and its modes of operation can be found in the PSAR (1975) of the CRBR and its Amendments.

#### 8.2.2 Primary Electrical Subsystem

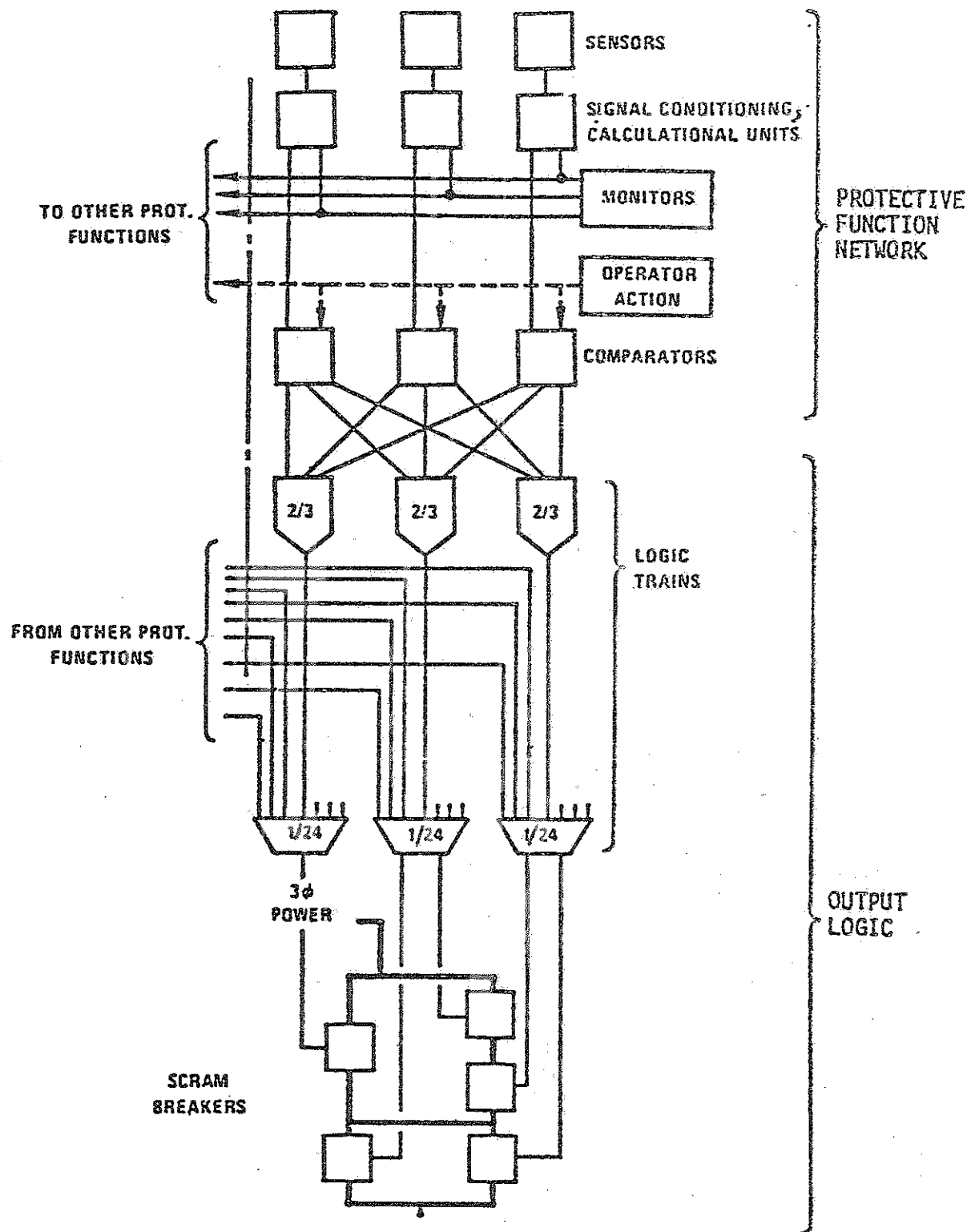
The Primary Electrical Subsystem design has the potential to include up to 24 protective functions arranged in a local coincidence logic configuration. Of these, 16 are intended to provide protection during full power operation, and the remaining 8 will be used to provide protection where required during startup and part load operations. The primary electrical logic diagram is given in Figure 8.1.

Each protective function consists of three redundant channels, each of which feeds into three redundant logic trains, as shown in Figures 8.2 and 8.3. A typical protective function channel is made up of sensors, signal conditioning, a calculation unit, and a comparator. The sensor measures a plant dynamic parameter which provides the safety envelope within which the plant is required to operate and converts this measurement into an electrical signal. The signal conditioning and calculation unit scales and provides signal processing to the measured analog electrical signal prior to transmitting it to the comparator. The comparator compares this analog signal with a setpoint. The setpoint may be generated either internally or externally via other sets of sensors, signal conditioning, and calculation units. When the analog input signal exceeds the setpoint, the output of the









### ELECTRICAL POWER TO PCRD M STATORS

Figure 8.3. Primary electrical shutdown subsystem block diagram.

comparator changes from a reset to a trip state. If more than one of the three comparators in a protective function trip, a trip signal is applied to each of the three logic trains. When more than one of the three logic trains provide a trip signal to their respective scram breakers, the proper combination of scram breakers opens, causing all power to the 15 primary control rods to be removed, thus activating their unlatching mechanisms.

Figure 8.3 also includes a representation of the way automatic monitoring of the protective-function channels is accomplished. Each of the three analog channels is compared with the others. If a discrepancy is detected in a channel, it will be automatically announced to the reactor operator via the Plant Data Handling and Display System. After evaluation, the operator will manually trip the comparator of the failed analog channel until it is repaired by maintenance personnel. Thus, the usual 2-out-of-3 logic configurations of the protective-function channels will have one tripped input (reconfigured to an effective 1-out-of-2 logic configuration) until repair of the failed channel is completed, at which time the channel is returned to service.

### 8.2.3 Secondary Electrical Subsystem

The Secondary Electrical Subsystem design has the potential to include up to 16 protective functions arranged in a general coincidence logic configuration. Of these, 11 provide protection during full power operations, and the remaining 5 are included as spares based on hardware design considerations. The secondary electrical logic diagram is given in Figure 8.4.

Each protective function consists of three redundant channels, each channel separately feeding a logic train as shown in Figures 8.5 and 8.6. Thus, there is separation between redundant protective function channels throughout the Secondary Electrical Subsystems. A typical secondary protective function channel is similar to the primary protective function channel. The coupling between the protective function network and the logic trains is, however, different, being optical in the primary and magnetic in the secondary (see Figures 8.2 and 8.5). Whenever more than one of the three logic trains propagate a trip signal to the four 2-out-of-3 valve configurations, designed to vent argon whenever two or more valves have their power removed, the rods are unlatched and fall to their shutdown position.

The monitoring and the manual tripping of the secondary protective function channels are performed as for the primary channels.

#### 8.2.4 Primary Mechanical Subsystem

The Primary Mechanical Subsystem, which consists of 15 primary control rod systems (PCRS), provides start-up, reactivity (power) control, burn up compensation, and primary shutdown capabilities for the reactor.

The PCRS consists of three major subassemblies: the Primary Control Drive Mechanism (PCRDM), and the Primary Control Assembly (PCA). The control rod drive mechanism is connected to the control rod (movable pin bundle in the PCA) through the control rod driveline as shown in Figure 8.7.

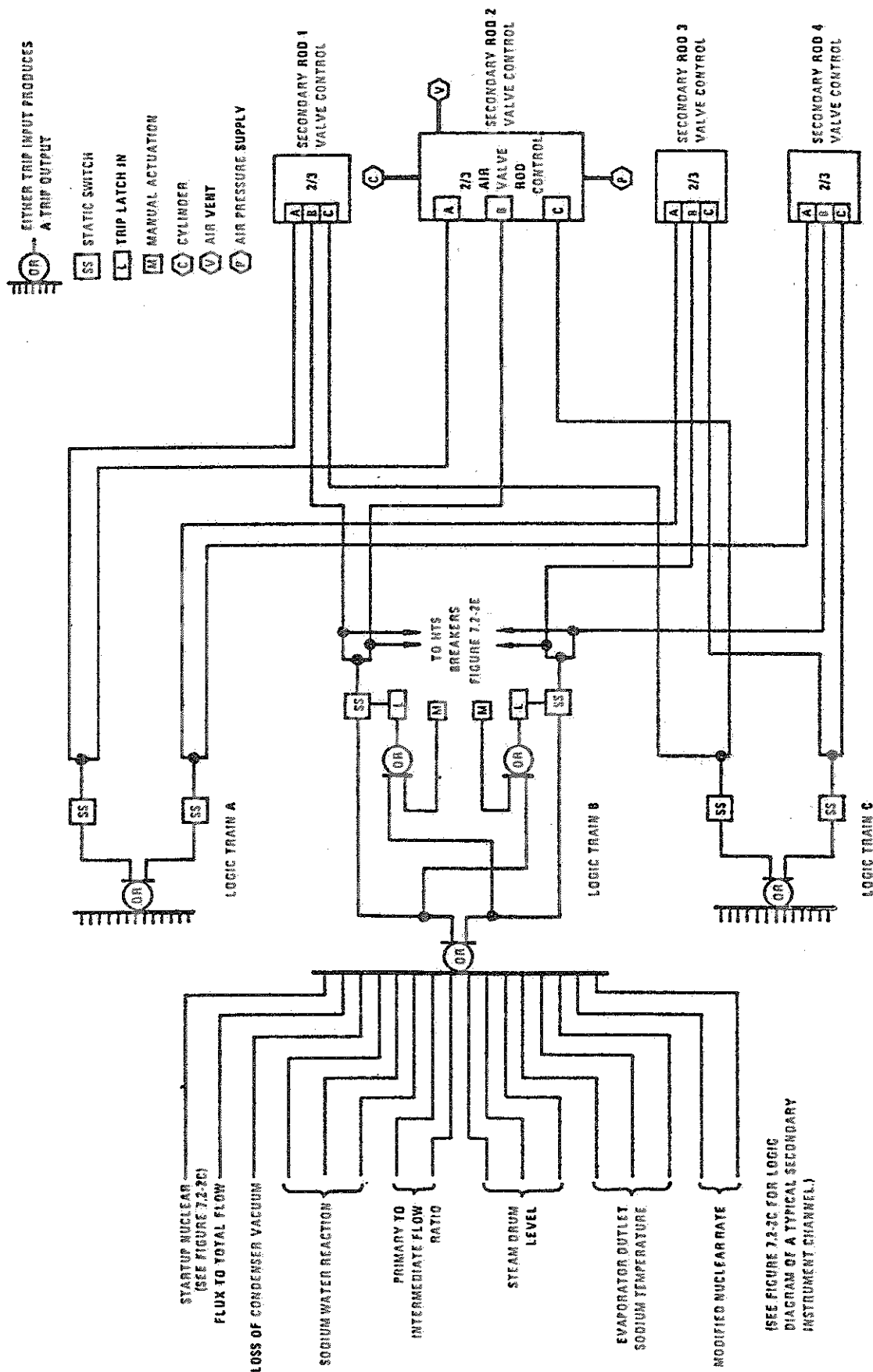


Figure 8.4. Secondary electrical logic diagram.

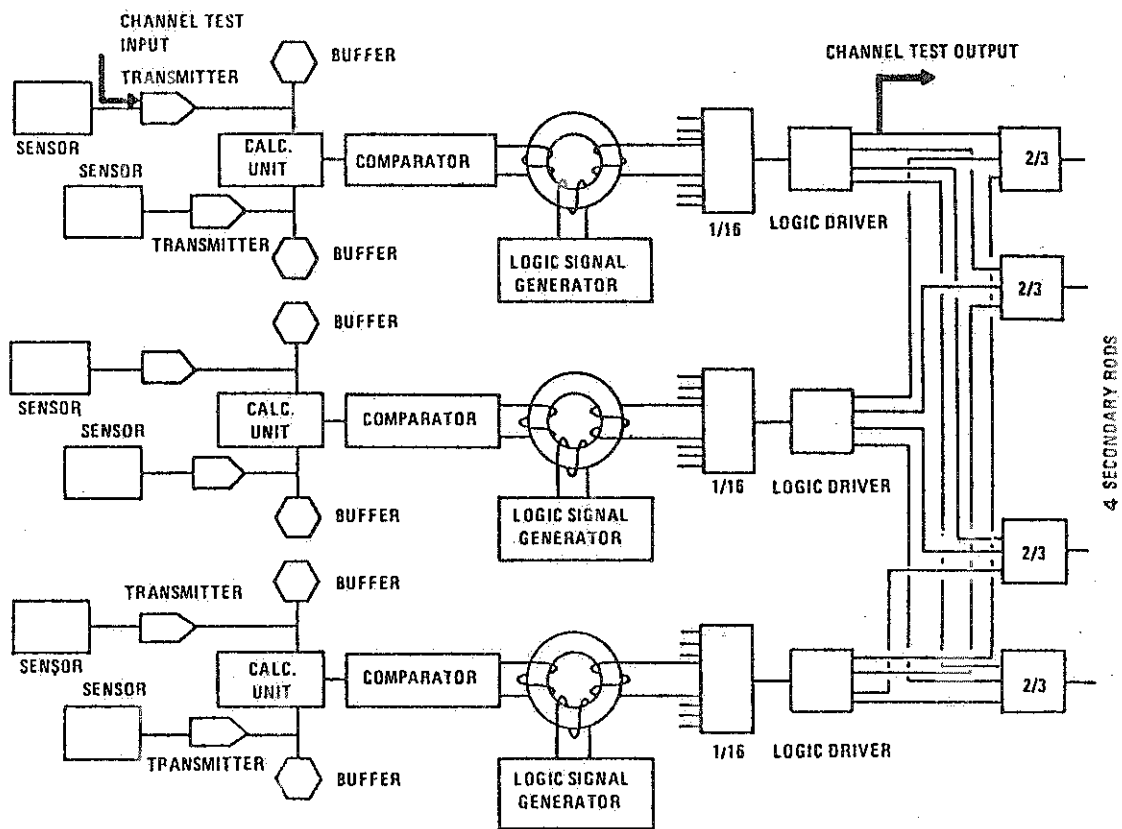


Figure 8.5. Typical primary electrical subsystem.

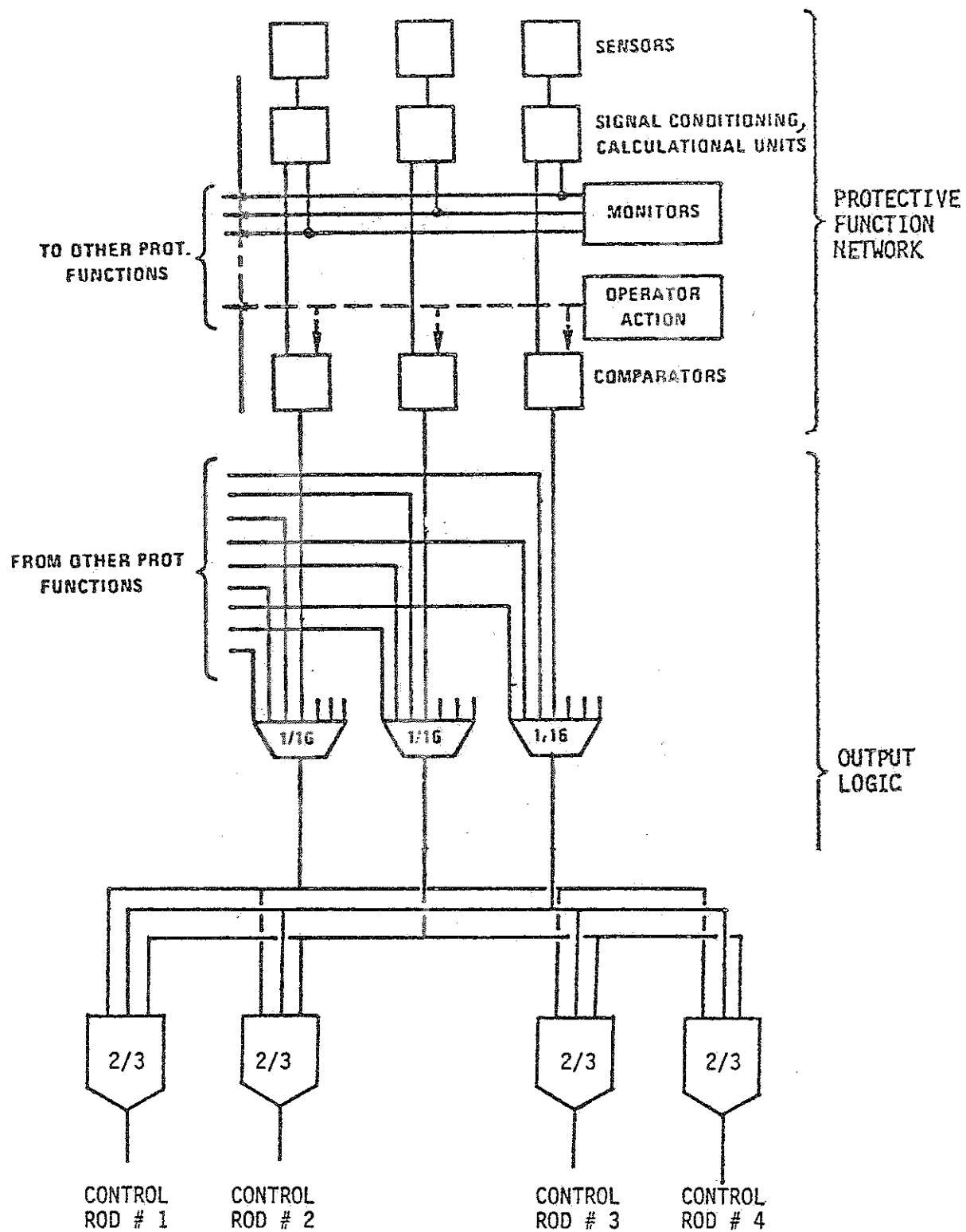


Figure 8.6. Secondary electrical shutdown sub-system block diagram.

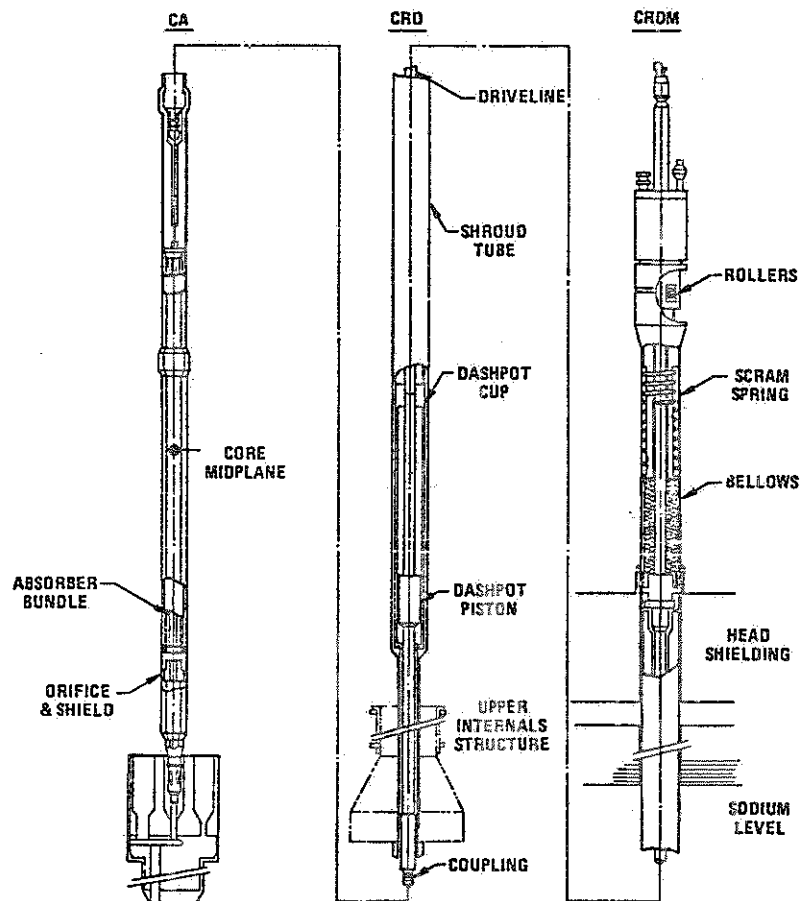


Figure 8.7. Primary control rod system.



The PCRDM consists of a 6-phase, 4-pole dc motor that positions the control rod to desired elevations within the core of the reactor. It utilizes a collapsible rotor roller nut drive which is actuated by signals from the reactor control system. These signals energize the stator and magnetically actuate the rotor assembly segment arms, causing the roller nuts to engage the threaded portion of the lead screw. Rotation of the electrical field of the stator causes rotation of the roller nuts with respect to the lead screw. The control rod can thus be inserted, withdrawn, or held at the desired elevation. Deenergizing the stator allows the roller nut to disengage the lead screw, thereby causing the control rod to drop into the core at a rapid rate of insertion. The operation and screw functions of the rotor and roller nut mechanisms are illustrated in Figure 8.8.

#### 8.2.5 Secondary Mechanical Subsystem

The secondary Mechanical Subsystem, which consists of 4 Secondary Control Rod Systems (SCRS), provides secondary (redundant) shutdown capabilities for the reactor.

The SCRS shown schematically in Figure 8.9 consists of three major subassemblies: The Secondary Control Drive Mechanism (SCRDM); the Secondary Control Rod Driveline (SCRD); and the Secondary Control Assembly (SCA). The SCRS utilizes hydraulic forces to assist scram action. The control rod moves axially within the control assembly guide tube. During normal reactor operation, the rod is supported above the core by the latch that is actuated by a pneumatic cylinder. Appropriate flow paths and orifices within the assembly allow the

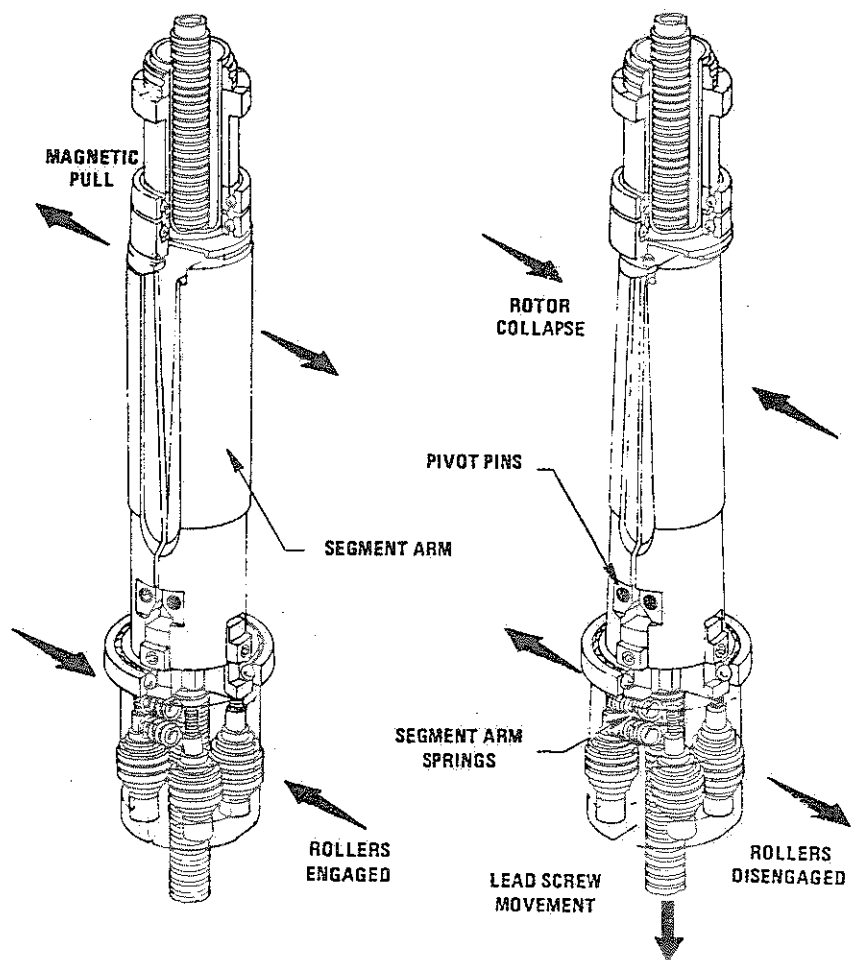


Figure 8.8. Collapsible motor roller nut drive.

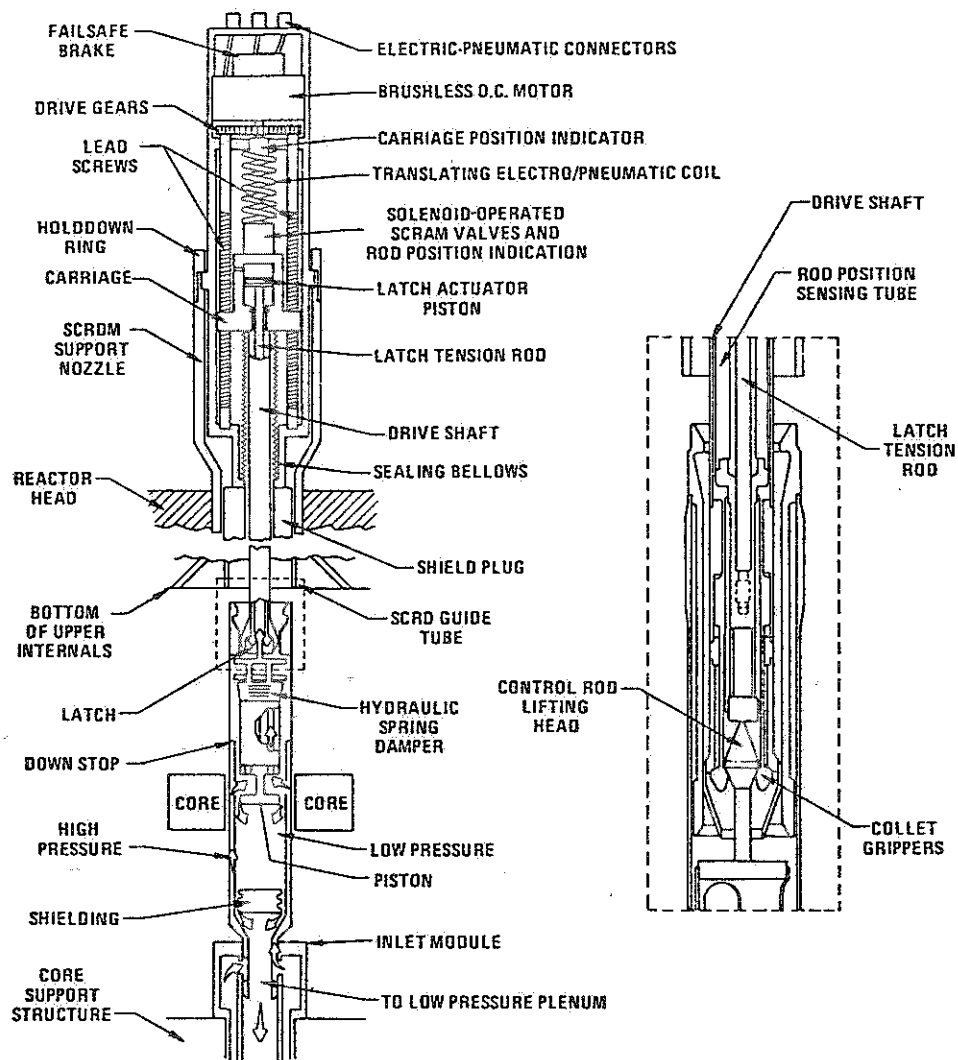


Figure 8.9. Secondary control rod system.

reactor coolant to flow from the high pressure plenum to the region above the piston. Sodium below the piston is ducted to the low pressure plenum. Therefore, a pressure drop in the downward (scram) direction exists across the control rod piston continuously during normal operation. Upon receipt of a scram signal, the control rod is released by depressurization of the latch-actuating cylinder and is forced down by the hydraulic pressure force and gravity into the core region.

### 8.3 System Mission and Reliability Duty Cycle

During the plant operation, the reactor is exposed to a number of normal and off-normal transients. If uncontrolled, some of these transients could cause a loss of core coolable geometry (LCG). Since LCG is an accident that could exceed 10CFR100 guidelines, the function of the Reactor Shutdown System (RSS) is to prevent such an event from happening. We can say, therefore, that "the mission of RSS is to sense and successfully respond to a defined set of transients in such a way that the loss of core coolable geometry is avoided during the lifetime of the plant." In Appendix C of PSAR of the CRBRP, it is assumed that LCG occurs, in the short term, if sodium reaches saturated conditions (boiling) in the hot channel ( $\sim 1700^{\circ}\text{F}$ ), or in the long term, if the in-vessel bulk sodium outlet temperature rises in excess of  $1250^{\circ}\text{F}$ . For a given transient, RSS success or failure depends, therefore, upon inserting the minimum amount of reactivity in an acceptable increment of time so that neither of these two events will happen.

Since RSS success is defined with respect to acceptable response to transients over the lifetime of the plant, the set of the possible transients affecting the RSS during that period should be defined. The set of transients to which the RSS should successfully respond (called also reliability duty cycle of the RSS) is defined if the following questions are answered.

- 1) What are the possible transients that may affect the RSS during plant life?
- 2) Of the transients in 1, which can actually lead to LCG due to RSS failure?
- 3) Of the transients in 2, which can get to LCG conditions in a short period of time?
- 4) Of the transients in 3, which would require more reactivity insertions than is necessary to cover the power defect?

A complete list of the anticipated, unlikely, and extremely unlikely transients that the CRBR may experience during its lifetime is given in the PSAR and in WARD-D-0118. For the purposes of this analysis, however, the transients are classified into three major categories.

1. Reactivity Transients - Those transients occurring as the result of a positive reactivity insertion producing an overpower condition (power flow > 1.0). To successfully shut down the reactor, the RSS must initially insert negative reactivity sufficiently fast to prevent hot channel sodium boiling and in sufficient magnitude to assure an in-vessel bulk sodium outlet temperature below 1250°F. The total negative reactivity inserted must compensate for the reactivity

associated with the initiating event plus the power defect (reactivity changes due to temperature difference between any two operational states of the reactor) associated with going to a stable long-term reactor condition.

2. Major Flow Transients - Those transients associated with a reduction in coolant flow and for which a rapid shutdown is required to prevent LCG. RSS success criteria for these transients are based on the same considerations as reactivity transients except that no compensation is required for reactivity changes associated with the initiating event.

3. Limited Response Transients - Transients in this category do not require electrical protective subsystem response because of the time available between initiation of the event and the time when rod insertions must occur to prevent LCG. In WARD-D-0118, it is shown that transients in this category do not require negative reactivity insertion for at least ten minutes after initiation. Although all of the transients in this category are sensed by the electrical protective subsystem and shutdown by that system is normally initiated, LCG would not result if action did not occur immediately. Redundant visible and audible annunciation will alert the operator of the occurrence of these transients assuring a high probability of manual response should the automatic system fail. Transients in this category are, therefore, only dependent on mechanical subsystem response and, for the purposes of this analysis, it is assumed that the combination of automatic electrical protective subsystem response or manual action by the operator assures actuation of the mechanical subsystems.

Negative reactivity insertion requirements of the RSS for all transients in this category are based on compensating for the power defect between the initial operating power and an acceptable long-term steady-state core condition with pony motor flow.

At the end of each year the reactor is shut down for an extensive period of time ( $\sim 4$  weeks) for refueling. During this period of time, a complete overhaul of the Shutdown System takes place and at the beginning of the next year the RSS is renewed. Since we know that the system is in the as-new condition at the beginning of each year, we need only calculate the probability that the RSS will fail during a typical year of reactor operation.

We want, therefore, to calculate the probability that the RSS will fail to perform its mission (successfully respond to the above cited transients) any time during one year.

#### 8.4 System Model and Assumptions

This section presents the model used for the quantitative evaluation of the probability that the Reactor Shutdown System (RSS) will fail to respond to a set of transients during a typical reactor year, and the assumptions made in the modeling.

The description of the system was given in Section 8.2. A simplified logic block diagram illustrating the logical interconnection of the various subsystems is shown in Figure 8.10. The Primary Shutdown System (PSS) can be divided into three subsystems; the Primary Protective Function (PPF), the Primary Output Logic and the Primary Mechanical Subsystems (PMS). The Secondary Shutdown System (SSS) can

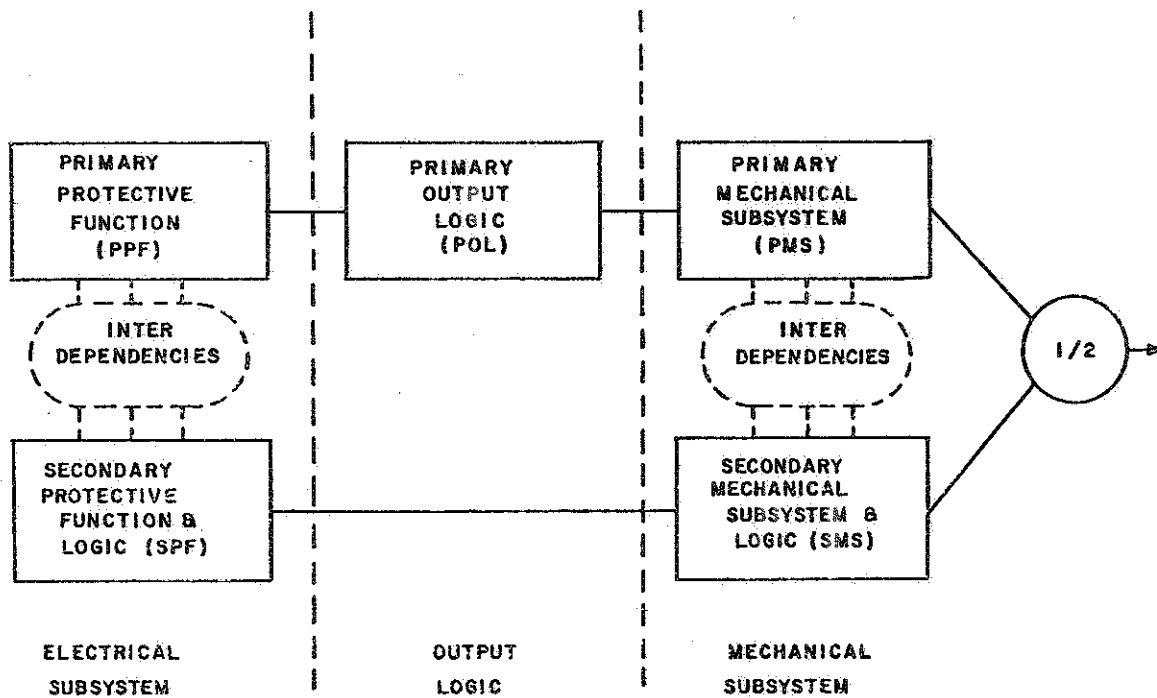


Figure 8.10. Simplified logic block diagram of CRBR reactor shutdown system.



be divided into two subsystems: The Secondary Protective Function (SPF) containing part of the secondary logic and the Secondary Mechanical Subsystem, containing the rest of the secondary output logic. If a transient occurs, either protective function can sense it and signal the corresponding mechanical subsystem to insert the necessary negative reactivity to control the transient. Successful operation of either the PSS or the SSS guarantees successful operation of the RSS.

The three types of transients under consideration are: 1) reactivity transients; 2) major flow transients; 3) limited response transients. The necessary negative reactivity requirements, given in WARD-D-0118, are \$5 for reactivity transients, \$2.5 for major flow transients, and \$2.5 for limited response transients. The set of all possible states of the system can, therefore, be divided into the following six subsets:

- 1) Subset AR - containing all the system-states in which the reactor is online (a transient can occur) and the RSS is able to respond to any type of transient.
- 2) Subset AMF - containing all the system states in which the reactor is online and the RSS is able to respond only to major flow and limited response transients.
- 3) Subset ALR - containing all the system states in which the reactor is online, and the RSS is able to respond only to L.R. transients.
- 4) Subset AF - containing all the system states in which the reactor is online and the RSS is not able to respond to any transient.

5) Subset S - containing all the system states in which the reactor is shut down. No transients may occur if the system is in a state of S.

6) Subset F - containing all the failed states.

The six subsets of states along with the possible transients are shown in Figure 8.11. The system has failed if it enters subset F. The transitions of the system from state to state are random. The probabilistic behavior of the system was simulated by a Markov Process. In the derivation of the Markov model, the following assumptions were made:

- 1) All failures are random and the times-to-failure are exponentially distributed. The failure rates may depend on the state of other components in the following way.
  - 1a) The failure rates of a component of the Primary Protective Function or of the Secondary Protective Function depend on the states of the other components in these two subsystems.
  - 1b) The failure rates of a component of the Primary Output Logic depend on the states of the other components in this subsystem.
  - 1c) The failure rates of a component of the SOL depend on the state of other components in this subsystem.
  - 1d) The failure rates of a component of the Primary Mechanical Subsystem or of the Secondary Mechanical Subsystems depend on the states of the other components in these two subsystems.

These assumptions enable us to consider common cause failures

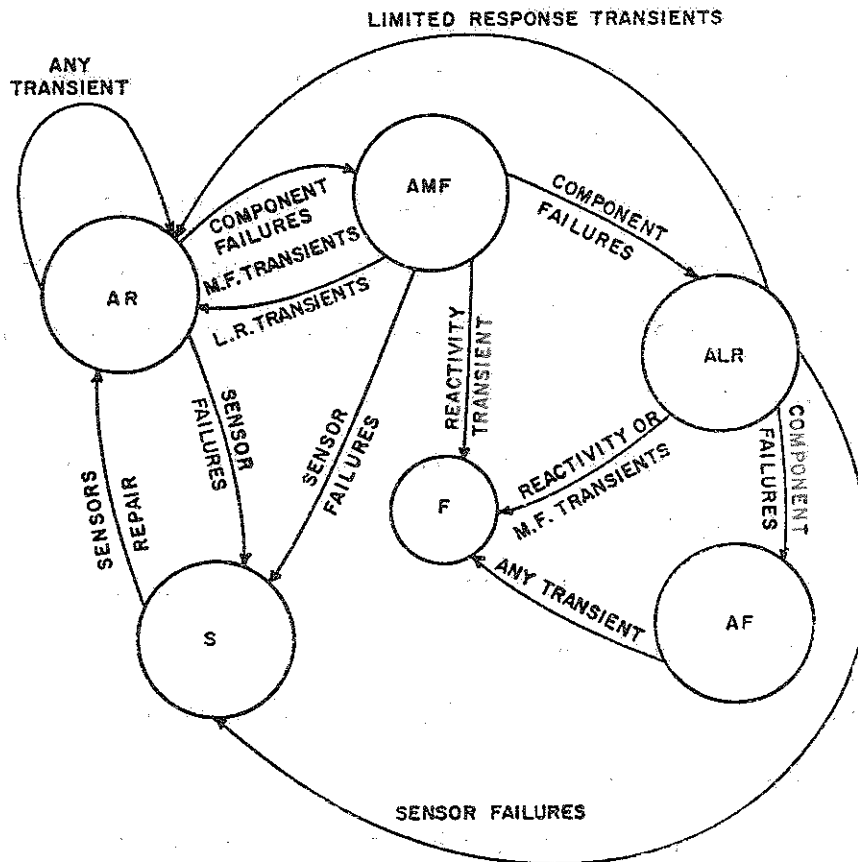


Figure 8.11. State flow chart for CRBR and shutdown system.

in the electrical subsystems, the output logics and the mechanical subsystems.

- 2) Transients occur randomly and they arrive according to a Poisson random process.
- 3) If a transient occurs, the system can either respond successfully or fail.
- 4) Electrical response is required for reactivity and major flow transients only. For limited response transients it is assumed that the plant operator will initiate a manual scram with probability one.
- 5) If the RSS responds successfully to a transient, the system is renewed instantly.
- 6) Subset F of states is absorbing, i.e., the system cannot recover from a failed state.
- 7) While the reactor is shut down no transients occur and, therefore, no failures.
- 8) For a given transient, the Protective Function that monitors the dynamic plant parameters, affected by the transient, constitutes the Protective Function Network for each electrical subsystem.
- 9) Worst case configurations have been assumed for both electrical and mechanical subsystems. This assumption will be further explained at the end of this section and in Section 8.5.
- 10) Inspection of the electrical subsystems at predetermined intervals is possible. The inspection is not perfect. Errors may occur in the sense that a failure might not be detected

or a failure may be caused by the inspection itself.

- 11) The time horizon of the problem is 48 weeks. For the remaining 4 weeks, the reactor is assumed to be shut down for refueling and maintenance.

For model simplification the system has been divided into three subsystems (see Figure 8.10): 1) the Electrical Subsystem, which contains the Primary and Secondary Protective Functions Network as well as part of the secondary logic; 2) the Primary Output Logic; and 3) the Mechanical Subsystem which contains the Primary and Secondary Mechanical Subsystems. Three separate Markov models, one for each subsystem, were constructed. The models for the Mechanical Subsystem and the Primary Output Logic are first solved and the results are used in solving the model of the Electrical Subsystem which represents the whole RSS. The logic of the overall model is presented in Figure 8.12. Further details are given in Section 8.5

In the remainder of this Section the conservatism in the "worst case" assumption is demonstrated. Let  $S(t)$  denote the probability that the reactor is safe at time  $t$  or, equivalently, that no RSS failures have occurred in the interval  $[0,t]$ . Symbolically,

$$S(t) = \Pr\{\text{System safe at time } T\} = \Pr\{\text{No RSS failures in } [0,t]\}. \quad (8.1)$$

Then we have

$$S(t+dt) = \Pr\{\text{No failures in } [0,t] \text{ AND no failures in } dt\} ,$$

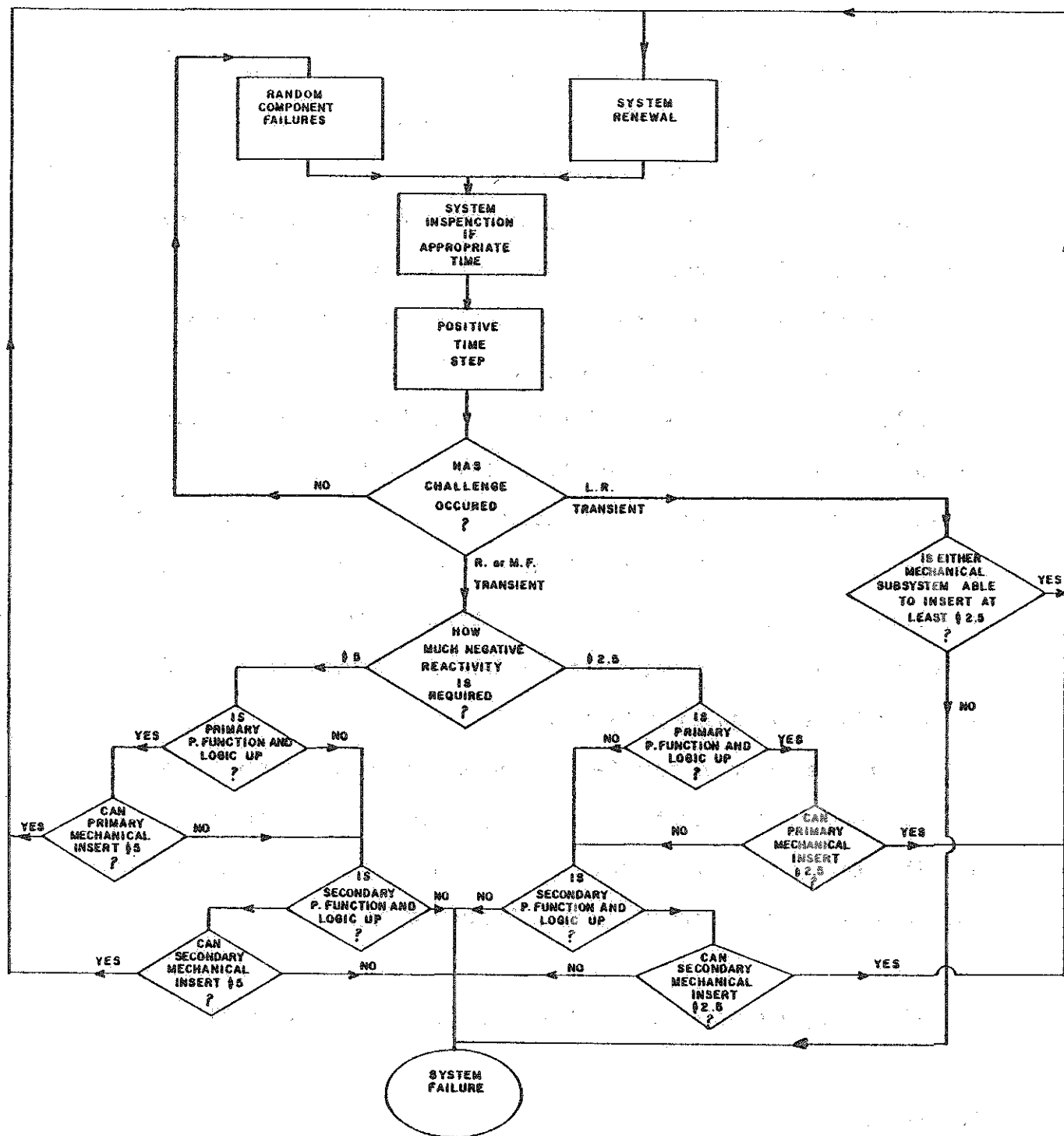


Figure 8.12. Logic flow chart of the reactor shutdown system model.

or

$$S(t+dt) = \Pr\{\text{No failures in } [0, t]\} \Pr\{\text{No failures in } dt | \text{No failures in } [0, t]\},$$

or by virtue of (8.1)

$$S(t+dt) = S(t) \left[ 1 - \Pr\{\text{failure in } dt | \text{No failures in } [0, t]\} \right].$$

The last equation can be written as

$$\frac{S(t+dt) - S(t)}{S(t)} = -\Pr\{\text{failure in } dt | \text{No failures in } [0, t]\}. \quad (8.2)$$

Since a system failure means that a challenge occurs and the RSS is unavailable, (8.2) can be written as

$$\frac{S(t+dt) - S(t)}{S(t)} = -\Pr\{\text{challenge in } dt \text{ AND RSS unavailable} | \text{No failures in } [0, t]\} \quad (8.3)$$

A challenge can be any of the various transients that might occur during the plant lifetime. If we assume that only one transient may happen at any given instant of time, (8.3) can be written as

$$\frac{S(t+dt) - S(t)}{S(t)} = - \sum_i \Pr\{\text{transient } i \text{ occurs in } dt \text{ AND RSS unavailable} | \text{No failures in } [0, t]\}$$

or

$$\frac{S(t+dt) - S(t)}{S(t)} = - \sum_i \frac{\Pr\{\text{transient } i \text{ occurs in } dt | \text{No failures in } [0, t]\} \times \Pr\{\text{RSS unavailable} | \text{Transient } i \text{ AND No failures in } [0, t]\}}{\Pr\{\text{transient } i \text{ occurs in } dt | \text{No failures in } [0, t]\}} \quad (8.4)$$

By virtue of Assumption 2, (8.4) can be written as

$$\frac{dS}{S} = - \sum_i \lambda_i U_i(t) dt, \quad (8.5)$$

where  $\lambda_i dt$  is the probability that transient  $i$  will occur between  $t$  and  $t+dt$  if no system failures have occurred,  $U_i(t)$  is the probability that the RSS will be unavailable to respond to a transient of type  $i$  given a challenge and that no failures have occurred in  $[0, t]$ , and the summation extends over all the transients. Solving (8.5) for the success probability  $S(t)$  yields

$$S(t) = \exp \left[ - \sum_i \lambda_i \int_0^t U_i(\tau) d\tau \right]. \quad (8.6)$$

Then the failure probability  $F(t)$  is

$$F(t) = 1 - S(t) = 1 - \exp \left[ - \sum_i \lambda_i \int_0^t U_i(\tau) d\tau \right]. \quad (8.7)$$

For the purposes of reliability analysis, the composition of the RSS is a function of both the transient that challenges it and of the time  $t$  at which the challenge occurs. The Primary Protective Function and the Secondary Protective Function are those out of the 16 and 11 available, respectively, that can sense the transient, while the negative reactivity available in the Primary Mechanical Shutdown depends on the position of the control rods at the time of the challenge. For this system configuration, the unavailability  $U_i(t)$  can be calculated



as a function  $t$  and for every  $i$ . The failure probability can then be calculated from (8.7). In the present analysis, however, we have assumed that for any transient the RSS consists of those PF's that contain the components with the highest failure rates and that the control rods are at any time at their worst configuration. Thus the unavailability  $U^*(t)$  of the RSS is such that

$$U^*(t) \geq U_i(t) \text{ for all } i \text{ and } t. \quad (8.8)$$

Thus by virtue of (8.7) and (8.8) it follows that

$$F^*(t) = 1 - \exp\left[-\lambda \int_0^t U^*(\tau) d\tau\right] \geq F(t) \quad (8.9)$$

where

$$\lambda = \sum_i \lambda_i.$$

In other words, the assumption that the RSS consists always of those protective functions that have the highest failure rates, and that the mechanical subsystems are in their worst configurations is conservative. If the rate at which challenges occur is very low, then the unavailability of the system at time  $t$  can be assumed to be independent of the occurrence of any challenges in the interval  $[0, t]$ , and it can be calculated by simpler techniques such as combinatorial analysis or fault tree analysis. If, however, the occurrence of challenges affects the availability significantly, a more precise method should be



employed. Such a method is the Markov model used in this analysis. The unavailability of the system  $U^*(t)$  is given by the probability that it will be in any state of the subsets AMF, ALR, AF (see Figure 8.11), while the failure probability is directly calculated as the probability that the system will be in the subset F. The model employed here allows for the renewal effect of successful challenges (via the transitions from the sets AMF and ALR back to AR) and for the fact that a failure cannot occur if the reactor is shut down for a long time for sensor repairs.

## 8.5 Detailed Subsystem Models


### 8.5.1 Mechanical Subsystem

The mechanical subsystem of the RSS consists of the control rods that are inserted in the reactor core to add the necessary negative reactivity for controlling a transient. As already stated the mechanical subsystem consists of two groups of rods, one forming the Primary Mechanical Subsystem, the other forming the Secondary Mechanical Subsystem (see Section 8.2). The Primary Mechanical Subsystem contains 15 control rods which are grouped into 4 basic classes - one center rod, two row-4 startup rods and six row-7 flat rods (see Figure 8.13 and PSAR Chapter 4). The Secondary Mechanical Subsystem contains four row-4 safety rods which are fully withdrawn whenever the reactor is operating. The reactivity worth of each rod is a function of its location in the core and its operational configuration (i.e., amount withdrawn and reactivity interactions with other control rods). The Mechanical Subsystem was modeled for the reactor at the beginning of

**PRIMARY CONTROL ROD SYSTEM**

-  BURNUP & LOAD FOLLOW CONTROL ASSEMBLIES (13)  
CENTRAL, ROW 7 FLAT & ROW 7 CORNER POSITIONS
-  START UP CONTROL ASSEMBLIES (2) ROW 4 POSITIONS

**SECONDARY CONTROL ROD SYSTEM**

-  SECONDARY CONTROL ASSEMBLIES (4)  
ROW 4 POSITIONS

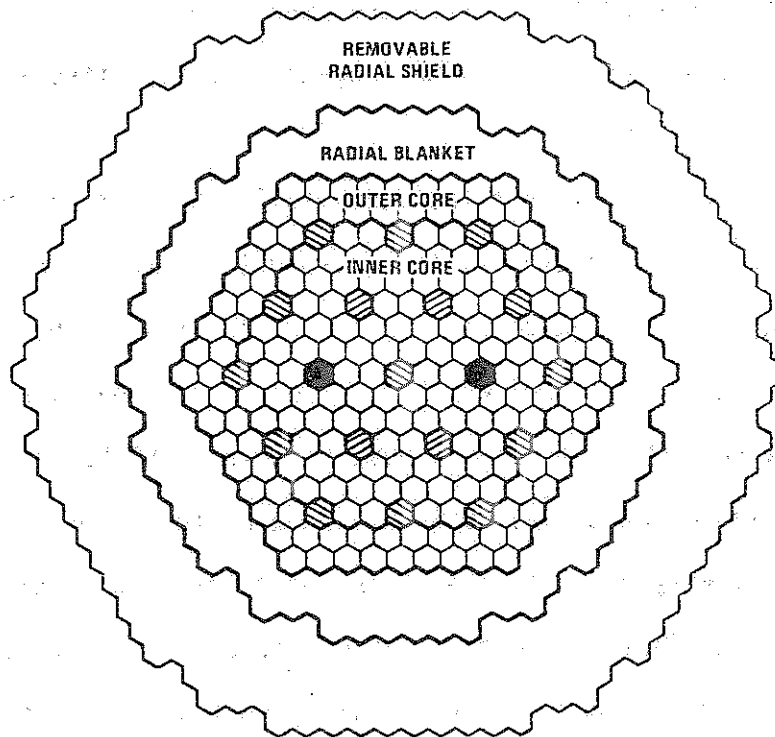


Figure 8.13. Control assembly conditions in core layout.

an equilibrium cycle. The two row-4 startup rods were fully withdrawn along with the six row-7 corner rods. This is the worst configuration for the primary mechanical subsystem because it corresponds to the smallest potential negative reactivity insertion. All other configurations will have more rods withdrawn to compensate for core burnup. The secondary control rods are always fully withdrawn. The changes in the secondary rod worths with time are associated with the overall primary rod configuration and with long-term burnup effects in the core and control rod materials.

In this model we use for the mechanical subsystem's success the same criteria that were derived in WARD-D-0118, namely, that the two row-4 startup rods in the primary have a worth of \$2 each, the six row-7 corner rods in the primary have a worth of \$1 each, and the four row-4 safety rods in the secondary have a worth of \$2.50 each. As it is already stated reactivity accidents require the insertion of \$5 of negative reactivity and all other transients the insertion of \$2.5. For a given transient, therefore, either mechanical subsystem is successful if it has enough rods operating so that their total worth is at least equal to the reactivity requirements of the transient. A Markov model was constructed for the mechanical subsystem based on the following assumptions:

- (1) Each control rod constitutes a component that can be in two states: (a) operating state in which it can insert its reactivity worth into the core in time, and (b) failed state in which it cannot.

- (2) The times-to-failure of the components are exponentially distributed. The failure rate of each component depends on the number of the components that have already failed. Thus, for the operating components the failure rate  $\lambda^*$  is given by

$$\lambda^* = k_i \lambda$$

for  $i=0,1,\dots,11$  and  $k_0=1$ . Numerical values for the  $k_i$ 's are given in Section 8.6.

The system consists of 12 two-state components and, therefore, it has 4,096 states [see (2.1)]. Since there are symmetries in the system, however, the corresponding Markov process is mergeable (see Chapter 3). Indeed, the system consists of two subsystems each with symmetries at the component level. Subsystem I (Primary) consists of 8 components that can be divided into two classes: Class 1 - containing the two row-4 start-up rods worth \$2; and Class 2 - containing the six row-7 corner rods worth \$1. Subsystem II (Secondary) consists of 4 components, the row-4 safety rods worth \$2.5, that form a class (see Definition 3.3.2). Using the code SSTAGEN-I\*, the 4,096 states were merged into 105 superstates. Furthermore, the superstates were grouped according to the reactivity worth of each subsystem into nine groups given in Table 8.1.

The mechanical subsystem can be challenged by Limited Response

---

\* See Appendix B

Transients (LRT). Given a challenge, whether the system will respond successfully or not depends solely upon its state. Thus, since a LRT requires \$2.5 of negative reactivity, the system will fail only if it is in a superstate of group nine (see Table 8.1). In all other instances, it will successfully shut down the reactor and, upon start up, it will be in superstate one (all components operating). To model this behavior an additional superstate, the failed superstate, was added. Then, from each superstate of groups one to eight, the system can transit to superstate one with probability equal to the probability of a LRT arrival, while from each superstate of group nine it transits with the same probability to the failed superstate. The probability that the mechanical subsystems will be in a superstate of group nine is equal to the probability that the RSS will be in a state of subset AF (see Figure 8.11). This is true because in that case the RSS cannot respond to any transient regardless of the state of the electrical subsystem.

The superstate transition probability matrix was generated by the code MMARELA\* and (2.3) was solved for a time period of 48 weeks. As a result, the probabilities that the mechanical subsystem will be in any of the nine groups of superstates as well as the probability that it will be in the failed state were calculated as functions of time. The former probabilities were used as an input in the model for the Primary Output Logic, while the latter is the RSS failure probability due to unsuccessful response to LRT transients.

---

\*See Appendix B

TABLE 8.1 Superstate Groups for Mechanical Subsystem.

Groups of Superstates	Reactivity Worth of Primary	Reactivity Worth of Secondary
1	$W \geq \$5$	$W \geq \$5$
2	$W \geq \$5$	$\$2.5 \leq W < \$5$
3	$W \geq \$5$	$W < \$2.5$
4	$\$2.5 \leq W < \$5$	$W \geq \$5$
5	$\$2.5 \leq W < \$5$	$\$2.5 \leq W < \$5$
6	$\$2.5 \leq W < \$5$	$W < \$2.5$
7	$W < \$2.5$	$W \geq \$5$
8	$W < \$2.5$	$\$2.5 \leq W < \$5$
9	$W < \$2.5$	$W < \$2.5$

### 8.5.2 Primary Output Logic

The Primary Output Logic (POL) subsystem consists of the Logic Trains and the Primary Scram Breakers (see Figures 8.1 to 8.3). If at least two out of the three channels of the Primary Protective Function send a trip signal to the output logic, the three logic trains are energized and if two out of the three together with the right combination of scram breakers function properly, the power in the stators of the Primary Control Drive Mechanisms is interrupted causing the control rods to drop into the core. The logic block diagram for this subsystem is shown in Figure 8.14.

A Markov model was constructed for the POL based on the following assumptions:

(1) Each logic train can be in two states: operating and failed. The time-to-failure is exponentially distributed. The failure rates of the operating logic trains depend on the number of the failed logic trains. Thus, the failure rate,  $\lambda^*$ , is given by

$$\lambda_i^* = k_i \lambda, \quad i = 0, 1, 2,$$

where  $i$  denotes the number of failed logic trains and  $k_0 = 1$ . Further details and numerical values are given in Section 8.6.

(2) Each scram breaker can be in two states: operating and failed. The time-to-failure is exponentially distributed. The failure rates of the operating breakers depend on the number of the failed breakers so that



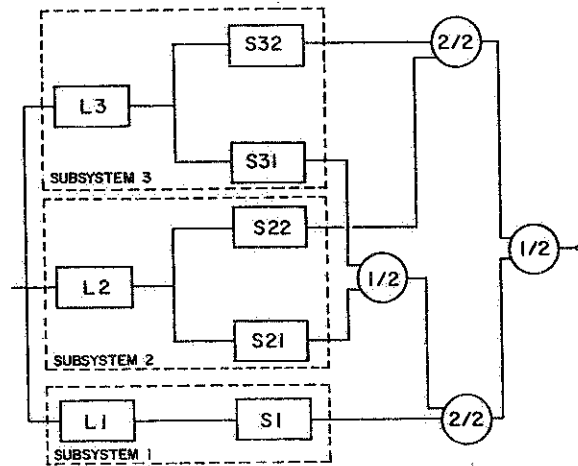


Figure 8.14. Logic block diagram for primary output logic.

$$\lambda_i^* = k_i \lambda, \quad i=0,1,2,3,4 \quad .$$

where  $i$  denotes the number of failed scram breakers and  $k_0 = 1$ .

(3) The system is inspected every four weeks. The inspection is not perfect. Failures may not be discovered or failures may happen during the inspection because of human error. Further details about the inspection and its incorporation in the model are given in subsection 8.5.3.

Since the system consists of 8 two-state components, it has 256 states. Because of system symmetries, however, the corresponding Markov process is mergeable (see Chapter 3). Indeed, as seen in Figure 8.14, the system consists of three subsystems, two of which (subsystems 2 and 3) are symmetrical (see Definition 3.3.7). The process was merged by the code SSTAGEN-I into 20 superstates. The set of these superstates was divided into two groups  $X$  and  $Y$  of operating and failed superstates, respectively. Then, the supertransition probability matrix  $\underline{P}(n)$  was generated by MMARELA. The structure of  $\underline{P}(n)$  is as shown in (2.14) with the following addition: the first column of  $\underline{P}(n)$  consists of non-zero elements. Since the arrival of a Limited Response Transient and the successful response of the Mechanical Subsystem amounts to a system renewal, the elements of the first column of  $\underline{P}(n)$  were set equal to the product of the LRT arrival rate and the probability that the MS will not be in a state of group nine (see Table 8.1).

The availability and the unavailability of the POL were calculated as functions of time. Next, the state-probabilities for the mechanical

subsystem were revised to reflect the availability of the Primary Output Logic. Since the Primary Mechanical Subsystem is connected in series with the POL (see Figure 8.10), the revised superstate probabilities for the mechanical subsystem are given by

$$M_i'(n) = M_i(n) \times A(n), \quad i = 1, 2, \dots, 6,$$

$$M_{j+6}'(n) = M_{j+6}(n) + [(M_j(n) + M_{j+3}(n))] \times [1-A(n)], \quad j = 1, 2, 3,$$

where:

$M_i(n)$  is the probability that the mechanical subsystem will be in a state group  $i$  at time  $n$ ;

$M_i'(n)$  is the revised  $M_i(n)$  to include POL failures;

and

$A(n)$  is the availability of POL at time  $n$ .

The probabilities  $M_i'(n)$  were used as an input to the model of the electrical subsystem described in the next Subsection.

### 8.5.3 Electrical Subsystem

The electrical subsystem consists of the Primary Protective Function Network (PPFN) and the Secondary Protective Function Network (SPFN) which also contains part of the Secondary Output Logic (see also

Section 8.2). The function of the electrical subsystem is to monitor plant conditions and provide the signal processing logic to determine if scram signal is appropriate for these conditions. In the primary electrical subsystem there are five protective functions that provide the main defense against LCG. These are

- (1) High Flux
- (2) Flux -  $\sqrt{\text{Pressure}}$
- (3) HTS Pump Electrics
- (4) Speed Mismatch
- (5) Steam - Feedwater Mismatch .

As discussed in the PSAR and WARD-D-0118 at least one of these functions will trip the plant, given the occurrence of a transient. In the secondary electrical subsystem there are three functions, at least one of which will trip the plant given the occurrence of a transient. These are

- (1) Flux - Total Flow
- (2) Flow Mismatch
- (3) Steam Drum Level .

As stated in Section 8.4, a conservative assumption made here is that the electrical subsystems consist always (for any transient) of the "worst case" protective function, i.e., of the function that has the components with the highest failure rates. These functions are: for the primary the Flux -  $\sqrt{\text{Pressure}}$  and for the secondary the Flux - Total Flow. Functional Block Diagrams of the Flux -  $\sqrt{\text{Pressure}}$  and the Flux - Total Flow functions are given in Figures 8.15 and 8.16,

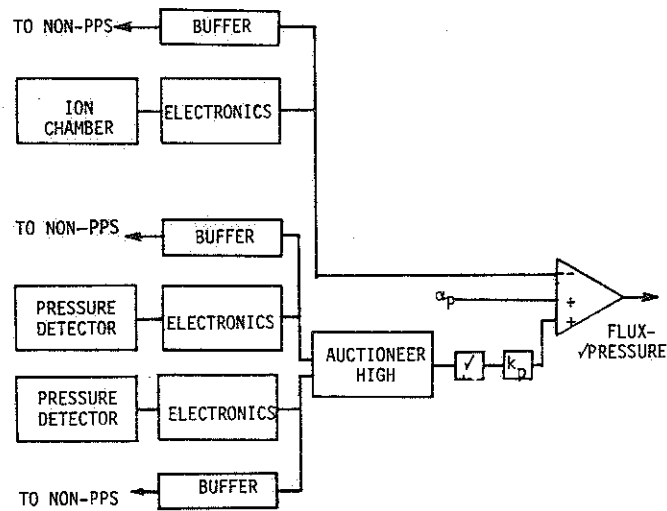


Figure 8.15. Functional block diagram of the flux-square root of pressure subsystem, one channel of three shown.

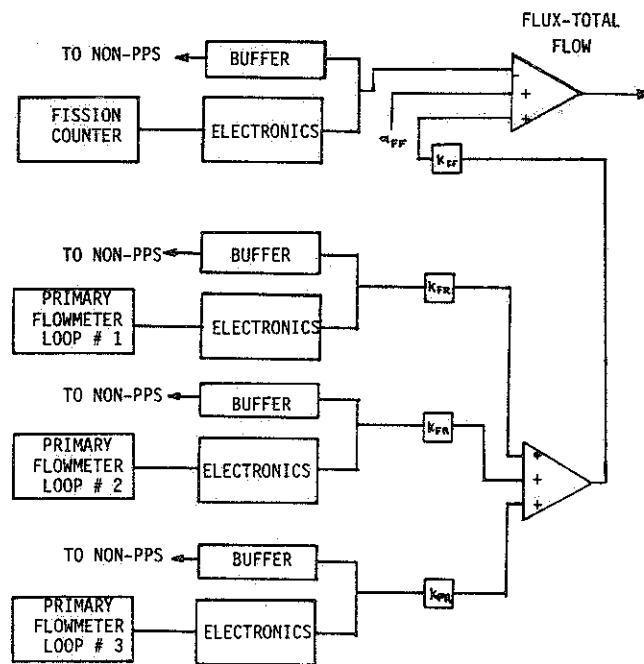


Figure 8.16. Functional block diagram of the flux-total flow protective subsystem, one channel of three shown.

respectively. The PPFN and SPFN are similar in layout. Both consist of three redundant channels operating in a two-out-of-three logic arrangement. A typical channel of the Flux -  $\sqrt{\text{Pressure}}$  Protective Function consists of the following components (see also Figures 8.2, 8.3 and 8.15):

- (1) Primary Flux Sensor
- (2) Primary Flux Electronics
- (3) Primary Pressure Sensors (two)
- (4) Primary Pressure Electronics (two)
- (5) Primary Calculation Unit
- (6) Primary Comparator

A typical channel of the Flux - Total Flow protective function consists of the following components (see also Figures 8.5, 8.6 and 8.16):

- (1) Secondary Flux Sensor
- (2) Secondary Flux Electronics
- (3) Secondary Flow Sensors (three)
- (4) Secondary Flow Electronics (three)
- (5) Secondary Calculation Unit
- (6) Secondary Comparator
- (7) Secondary Logic Train.

The following assumptions were made about the components of the electrical subsystem:

- (1) The components are either operating or failed.
- (2) A component failure can be either detectable (by the plant operator) or undetectable.

- (3) The time-to-detect a detectable failure is exponentially distributed. Its mean value is of the order of one 8-hour shift of operation.
- (4) Once a detectable failure is detected, the channel in which it occurred is put into a trip state by the operator. A trip signal from one out of the two remaining channels will scram the reactor.
- (5) Repair of the detected failures of the sensors cannot be started until the reactor is shut down.
- (6) Repair of the detected failures of the signal conditioning (electronics) and calculation units starts upon detection and is instantaneous.

Since all the components in a channel are logically connected in series, the states of the channel can be merged into the following five states (see Figure 8.17):

- (a) State OP - the operating state.
- (b) State S - containing components with detectable failures but for which repair cannot start before a reactor is shut down.
- (c) State TR - trip state in which the S-failures have been detected.
- (d) State M - containing components with detectable failures for which repairs can start immediately.
- (e) State U - containing components with undetectable failures.

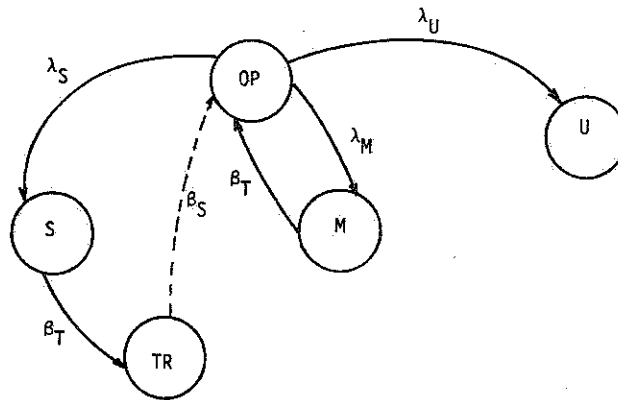


Figure 8.17. State flow chart for typical protective function network.

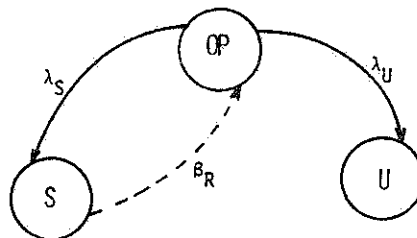


Figure 8.18. Simplified state flow chart for typical primary protective function network.

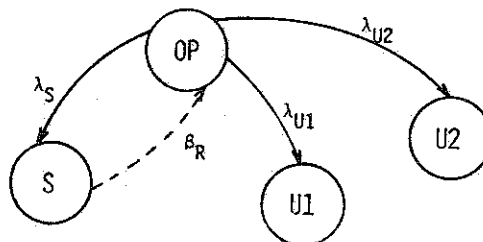


Figure 8.19. Simplified state flow chart for typical secondary protective function network.



The channel can transit from state OP to states S, M, and U with transition rates  $\lambda_S$ ,  $\lambda_M$ , and  $\lambda_U$ , respectively (see Figure 8.17). For the Flux -  $\sqrt{\text{Pressure}}$  function, these rates are given by

$$\lambda_S = p_D (\lambda_{FS} + 2\lambda_{PS})$$

$$\lambda_M = p_D (\lambda_{FE} + 2\lambda_{PE} + \lambda_C)$$

$$\lambda_U = \lambda_{CO} + (1-p_D) \times (\lambda_{FS} + 2\lambda_{PS} + \lambda_{FE} + 2\lambda_{PE} + \lambda_C). \quad (8.12)$$

where

$p_D$  is the probability that a detectable failure will be detected,

$\lambda_{FS}$  is the failure rate of the (Primary) flux-sensor,

$\lambda_{PS}$  is the failure rate of the (Primary) pressure-sensor,

$\lambda_{FE}$  is the failure rate of the (Primary) flux-electronics,

$\lambda_{PE}$  is the failure rate of the (Primary) pressure-electronics,

$\lambda_C$  is the failure rate of the (Primary) calculation unit,

$\lambda_{CO}$  is the failure rate of the (Primary) comparator unit.

For the flux - Total Flow function of the secondary subsystem, the transition rates are given by

$$\lambda_S = p_D \times (\lambda_{FS} + 3 \lambda_{FLS}) \quad (8.13)$$

$$\lambda_M = p_D \times (\lambda_{FE} + 3\lambda_{FLE} + \lambda_C) \quad (8.14)$$

$$\lambda_U = \lambda_{CO} + (1-p_D) \times (\lambda_{FS} + 3\lambda_{FLS} + \lambda_{FE} + 3\lambda_{FLE} + \lambda_C) + \lambda_{U2}, \quad (8.15)$$

where

$\lambda_{FS}$  is the failure rate of the secondary flux-sensor,

$\lambda_{FLS}$  is the failure rate of the secondary flow-sensor,

$\lambda_{FE}$  is the failure rate of the secondary flux-electronics,

$\lambda_{FLE}$  is the failure rate of the secondary flow-electronics,

$\lambda_C$  is the failure rate of the secondary calculation units,

$\lambda_{CO}$  is the failure rate of the secondary comparator unit,

$\lambda_{U2}$  is the failure rate of the secondary logic train.

From state S the channel can transit to state TR with transition rate  $\beta_T$ , where  $1/\beta_T$  is the mean time to detect a sensor failure and trip the channel. If two channels are in state TR, the reactor is shut down and repair of the failed sensor starts. From state M, the channel can transit to state OP with transition rate  $\beta_T$  where now  $1/\beta_T$  is the mean time to detect and repair the failure. Since the mean time to detect and repair a M-failure is much shorter than the mean time-to-failure of the components (8 versus 50,000 hr), it can be assumed that the detection and repair of M-failure is instantaneous. Indeed, calculation of the primary PFN unavailability with and without M-failures ( $\lambda_M = 0$  is equivalent to  $\beta_T = \infty$ ) shows that the two models yield almost identical results. For example, the unavailability of PPFN at  $t = 720$  hr was found to be  $2.9 \times 10^{-5}$  and  $2.4 \times 10^{-5}$  with and without M-failures, respectively (see also Figure 8.20).

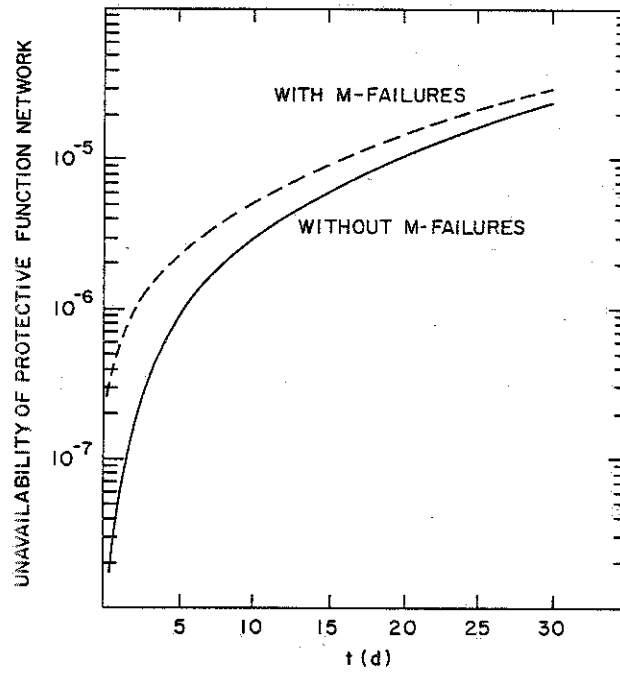


Figure 8.20. Unavailability of primary protective function network.

The Markov model was, therefore, constructed under the following assumptions:

- (1) The system consists of the primary and secondary protective function networks, each comprised of three redundant channels connected in a two-out-of-three logic configuration
- (2) Each primary channel can be in three states: (See Figure 8.18)
  - (a) Operating state OP
  - (b) Tripped state S
  - (c) Failed state U
- (3) Each secondary channel can be in four states: (See Figure 8.19)
  - (a) Operating state OP
  - (b) Tripped state S
  - (c) Failed state U1 - containing failures of the protective function part of the channel
  - (d) Failed state U2 - containing failures of the logic train.

The additional failed state (U2) for the secondary channel was considered for modeling the common cause failures of the secondary output logic, independently of primary protective function failures.

- (4) If two channels of the same subsystem (primary and secondary) are in a trip state the reactor is shut down. While in the shutdown state, the whole system is repaired. The time to repair the electrical subsystem is assumed exponentially distributed, with mean value  $1/\beta_R$ .

(5) The failure rates  $\lambda_S$ ,  $\lambda_U$ , for the primary channels are given in (8.10) to (8.12) and the failure rates  $\lambda_S$ ,  $\lambda_{U1}$ , and  $\lambda_{U2}$  for the secondary channels in (8.13) to (8.15).

(6) The following interdependences are considered:

$$(a) \quad \lambda_S^* = k_{Si} \lambda_S \quad \text{for } i = 0, 1, 2,$$

where  $i$  denotes the tripped channels in both subsystems, and

$$k_{S0} = 1$$

$$(b) \quad \lambda_U^* = k_{Ui} \lambda_U \quad \text{for } i = 0, 1, 2, 3, 4, 5,$$

where  $i$  denotes the number of failed channels in both subsystems

$$\text{and } k_{U0} = 1.$$

$$(c) \quad \lambda_{U2}^* = k_{Li} \lambda_{U2} \quad \text{for } i = 0, 1, 2.$$

where  $i$  denotes the number of failed secondary logic trains

$$\text{and } k_{L0} = 1.$$

The system consists of 3 three-state, and 3 four-state components. It has, therefore, 1728 states [see (2.1)]. The three primary channels and the three secondary channels constitute, respectively, two classes of symmetrical components (see Definitions 3.3.1 and 3.3.2). The corresponding Markov process was merged by the code SSTAGEN-I into 200 superstates. From the superstates, 80 contain states with two tripped channels and, therefore, form the state-subspace  $S$  defined in Section 8.4 (see also Figure 8.11). The other 120 superstates (called online superstates) combined with the nine groups of superstates of the mechanical subsystem (see Section 8.5.1 and Table 8.1) define subspaces AR, AMF, and ALR (see Section 8.4 and Figure 8.11). This is done by labeling the 120 'online' superstates by (a) PF1, if

both primary and secondary protective function networks are available; (b) PF2, if only the primary PFN is available; (c) PF3 if only the secondary PFN is available; (d) PF4 if both PFN's are unavailable. Thus, if the electrical subsystem is in a PF3 superstate, and the mechanical subsystem in a group-2 superstate, the Reactor Shutdown System is in a state of subspace AMF. Indeed, since only the secondary electrical subsystem is available (PF3) and since the mechanical subsystem has available only \$2.5 of negative reactivity (see Table 8.1), the RSS can successfully respond to Major Flow and Limited Response transients, while a Reactivity transient will cause a system failure (see Figure 8.11). The four types of electrical subsystem superstates together with the nine groups of mechanical subsystem superstates form 36 types of RSS-states. The subspaces to which these combinations belong are given in Table 8.2. An additional superstate (201) was added to represent the subspace F of failed system states.

The transition probability matrix of the process was generated by the code MMARELA. This matrix has the form shown in (2.14) where the 120 'online' superstates and the 80 'tripped' superstates constitute the sets X and Y, respectively. A successful response to a challenge corresponds to a system renewal. The first column of  $\underline{P}(n, X, X)$  [see 2.12) and (2.14)] has, therefore, nonzero elements. An unsuccessful response to a challenge corresponds to a system failure. The last column of  $\underline{P}(n, X, Y)$  has, therefore, nonzero elements. The elements of these two columns are determined as follows: Let  $\lambda_R$ ,  $\lambda_{MF}$ ,  $\lambda_{LRT}$  denote the rates of occurrence of reactivity, major flow, and limited response

TABLE 8.2 RSS-State subspaces to which combination of mechanical and electrical subsystem superstates belong.

Mechanical superstate	Worth		Electrical superstate PF1	Electrical superstate PF2	Electrical superstate PF3	Electrical superstate PF4
Group	Primary	Secondary	Both Subsystems UP	Only Primary Up	Only Secondary Up	Both Subsystems Down
	(\$)	(\$)				
1	5	5	AR	AR	AR	ALR
2	5	2.5	AR	AR	AMF	ALR
3	5	0	AR	AR	ALR	ALR
4	2.5	5	AR	AMF	AR	ALR
5	2.5	2.5	AMF	AMF	AMF	ALR
6	2.5	0	AMF	AMF	ALR	ALR
7	0	5	AR	ALR	AR	ALR
8	0	2.5	AMF	ALR	AMF	ALR
9	0	0	AF	AF	AF	AF

transients, respectively. Then, if the electrical subsystem is in a PF1 superstate at time  $n$ , the probability,  $P_{1F}(n)$ , that it will fail at the end of the  $n$ -th time interval is given by

$$p_{1F} = [M'_5(n) + M'_6(n) + M'_8(n) + M'_9(n)] \lambda_R \Delta t + M'_9(n) \lambda_{MF} \Delta t, \quad (8.16)$$

that is, it is equal to the probability that a reactivity transient will occur and the mechanical subsystem will not be able to insert \$5 worth of negative reactivity or that a major flow transient will occur and the mechanical subsystem will not be able to insert at least \$2.5 worth of negative reactivity (see Section 8.5.2 and Table 8.2). Since for every challenge the system will either fail or respond successfully, for a PF1 superstate the success transition probability,  $p_{1S}(n)$ , is given by

$$p_{1S} = (\lambda_R + \lambda_{MF} + \lambda_{LRT}) \Delta t - p_{1F} \quad (8.17)$$

Similarly, for superstates PF2, PF3, and PF4 we have that

$$p_{2F}(n) = [M'_4(n) + M'_5(n) + M'_6(n) + M'_7(n) + M'_8(n) + M'_9(n)] \lambda_R \Delta t + [M'_7(n) + M'_8(n) + M'_9(n)] \lambda_{MF} \Delta t,$$

$$p_{3F}(n) = [M'_2(n) + M'_3(n) + M'_5(n) + M'_6(n) + M'_8(n) + M'_9(n)] \lambda_R \Delta t + [M'_3(n) + M'_6(n) + M'_9(n)] \lambda_{MF} \Delta t,$$

$$p_{4F}(n) = (\lambda_R + \lambda_{MF}) \Delta t,$$

and



$$p_{iS}(n) = (\lambda_R + \lambda_{MF} + \lambda_{LRT})\Delta t - p_{iF} \quad \text{for } i = 2, 3, 4 \quad .$$

Thus, the first element of the  $j$ -th row of  $\underline{P}(n, X, X)$  is equal to  $p_{iS}(n)$ , depending on the type of the  $j$ -th superstate, while the last element of the same row of  $\underline{P}(n, X, Y)$  is equal to  $p_{iF}(n)$ . Finally, since the only transitions out of superstates of subspace  $S$  are those corresponding to complete repairs, the elements of the first column of  $\underline{P}(n, Y, X)$  [see (2.14)] are set equal to  $\beta_R \Delta t$ , where  $\beta_R$  is the repair rate. All the other elements of  $\underline{P}(n, Y, X)$  are equal to zero.

It is noteworthy that a limited response transient cannot cause a system failure in this model since such failures were incorporated in the model for the mechanical subsystem.

The electrical subsystem can be inspected, tested, and maintained at predetermined intervals of time. The detailed modeling of the system inspection is presented in the next subsection.

The code MMARELA performs the multiplication (2.3) for the necessary number of time steps, and the calculated probability that the system will be in state  $F$  at time  $n$ . This probability added to the corresponding probability calculated by the mechanical subsystem model provides the failure probability for the Reactor Shutdown System.

#### 8.5.4 System Inspection

The availability of standby safety-related systems of nuclear reactors can be increased through tests and preventive maintenance. The testing of a system helps to uncover existing failures while

maintenance helps to prevent future ones. The inspection of a system might have, nevertheless, some negative effects on its availability. These effects are:

- (1) The system is not available to perform its safety functions during the duration of the test and maintenance.<sup>(a)</sup>
- (2) Failures in components might be caused by the inspection itself, because of human errors.<sup>(a)</sup>
- (3) Frequent external interruptions might increase the failure rates of the components of a system.<sup>(b)</sup>

Taking into account the positive and negative effects, the optimum inspection frequency is the one that maximizes the availability of the system.

The electrical subsystem of the Reactor Shutdown System of the CRBR is designed so that the components (with the exception of sensors) of the Protective Function Networks and of the Output Logic can be tested online. Inspection was, therefore, included in the models for the primary output logic and the Protective Function networks. The following assumptions were made:

- (1) The inspection is instantaneous. This is a conservative assumption. A channel under inspection is put into a tripped state until the inspection is completed. This results into a one-out-of-two reconfiguration of the two-out-

---

(a) See Reactor Safety Study, Appendix III.

(b) Bourne, private communication.

of-three logic. Thus, even though a reactor shutdown might result from the tripping or a spurious signaling of one of the two remaining channels, an unsafe failure of the system because of the "unavailability" of the channel under inspection cannot happen.

(2) The testing of components belonging to the same subsystem is simultaneous. Testing of different subsystems is, however, staggered, i.e., done at different points in time.

(3) An inspection of a Protective Function Network with one channel in a tripped state means a reactor shutdown. Thus two policies were considered:

Policy I. If at the time of inspection of a PFN one of its channels is in a tripped state, the reactor is shut down.

Policy II. If at the time of inspection of a PFN one of its channels is in a tripped state, the inspection is not performed unless the other PFN has also a tripped channel.

Policy I results, in general, in a lower failure probability for the RSS but in a higher reactor unavailability than Policy II. In choosing between policies I and II, a value trade-off should be established between failure probability and reactor unavailability.

(4) The inspection is not perfect. An inspection error is defined to be a failure that has not been detected or as a failure that has been caused by the inspection.

(5) The failure rates of the components are not affected by the inspection. This assumption was made because of lack of pertinent data.

In Markovian reliability analysis, the modeling of system inspection is done via the inspection probability matrix  $\underline{Q}(n)$ . This matrix is defined as follows:

$$\underline{Q}(n) = \begin{cases} \underline{I} & \text{if } n \neq kn, \\ \underline{Q} & \text{if } n = kn, \end{cases} \quad (8.18)$$

where  $k = 1, 2, \dots, n_0$  is the inspection period, and the element  $q_{ij}$  of  $\underline{Q}$  is equal to the probability that the system will transit from state  $i$  to state  $j$  because of the inspection. The state probability vector  $\underline{\pi}(n)$  is then given by

$$\underline{\pi}(n) = \underline{\pi}(n-1) \cdot \underline{P}(n) \cdot \underline{Q}(n) \quad . \quad (8.19)$$

The use of the inspection probability matrix  $\underline{Q}$  is demonstrated in the following simple example. We consider a system consisting of 2 two-state components connected in parallel. Then the four states of the system are  $(1,1)$ ,  $(1,0)$ ,  $(0,1)$ ,  $(0,0)$ . If now  $q_0$  and  $q_1$  denote the probability of zero and one inspection errors, respectively, the inspection probability matrix  $\underline{Q}^1$  for the first component is

$$\underline{Q}^1 = \begin{bmatrix} q_0 & 0 & q_1 & 0 \\ 0 & q_0 & 0 & q_1 \\ q_0 & 0 & q_1 & 0 \\ 0 & q_0 & 0 & q_1 \end{bmatrix} \quad ,$$

while the inspection probability matrix,  $\underline{Q}^2$ , for inspection of the second component is

$$\underline{Q}^2 = \begin{bmatrix} q_0 & q_1 & 0 & 0 \\ q_0 & q_1 & 0 & 0 \\ 0 & 0 & q_0 & q_1 \\ 0 & 0 & q_0 & q_1 \end{bmatrix} .$$

Two inspection probability matrices were considered so that the two components can be inspected with different frequencies or with the same frequency at different points in time. The state probability vector for this process is given by

$$\underline{\pi}(n) = \underline{\pi}(n-1) \cdot \underline{P}(n) \cdot \underline{Q}^1(n) \cdot \underline{Q}^2(n) .$$

The necessary subroutines have been added into the SSTAGEN-I code, and two inspection probability matrices  $\underline{Q}^P$  and  $\underline{Q}^S$  for the primary and the secondary PFN, respectively, were generated. Then, the state probability vector for the electrical subsystem is given by

$$\underline{\pi}(n) = \underline{\pi}(n-1) \cdot \underline{P}(n) \cdot \underline{Q}^P(n) \cdot \underline{Q}^S(n) , \quad (8.19)$$

where

$$\underline{Q}^P(n) = \begin{cases} \underline{I} & \text{for } n \neq kn_p + n_p^* , \\ \underline{Q}^P & \text{for } n = kn_p + n_p^* , \end{cases} \quad (8.20)$$

and

$$\underline{Q}^S(n) = \begin{cases} \underline{I} & \text{for } n \neq kn_S + n_S^* \\ \underline{Q}^S & \text{for } n = kn_S + n_S^* \end{cases}, \quad (8.21)$$

where  $k = 0, 1, 2, 3, \dots, n_p$ ,  $n_S$  denote the inspection periods and  $n_p^*$ ,  $n_S^*$  the times at which the first inspection takes place. Similar inspection matrices were generated for the two classes of subsystems of the Primary Output Logic.

The necessary input for the generation of the  $\underline{Q}$  matrices consists of the inspection policy (see Assumption (3) above) and of the conditional probabilities of making one error, two given that one has been made, etc.

## 8.6 Data Base

This section presents the failure data used in conjunction with the models in Sections 8.4 and 8.5 to provide the quantitative evaluation of the RSS failure probability given in Section 8.7. Uncertainties about the values of the failure rates and other probabilities are expressed as follows: The failure rates and the transient arrival rates are random variables with range the positive real axis  $[0, \infty)$ , and distributed according to Gamma pdf's (see Section 4.4.1). The dependence coefficients are random variables with range the interval  $[1, \infty)$  and distributed according to Gamma pdf's (see Sections 4.4.1 and 4.5).

In WARD-D-0118, two sets of data are given. One of them called "Objective Set" consists of "failure rates and failure probabilities

which are evaluated using expected test conditions and analyses to produce an objective reliability which will be demonstrated by a combination of tests and analyses" (see also references WR-50670 and WR-50602). Here, it is assumed that these "objective" values are the most probable values of the corresponding random variables. This assumption determines one of the two parameters of the pdf's. The second parameter has been defined such that the upper 90% confidence limit is one order of magnitude higher than the lower 90% confidence limit, the latter being of the same order of magnitude as the most probable value. The numerical values of the parameters of the pdf's as well as the 90% confidence limits are given for the failure rates in Table 8.3.

The parameters of the pdf's and the confidence limits for the dependence coefficients are given in Table 8.4. These parameters are subjectively assessed. The effect of the dependence coefficients on the pdf of some transition rates is shown in Figure 8.21.

The most probable value of the reactor repair rate is assumed to be  $10^{-3} \text{ hr}^{-1}$ . This corresponds to a conditional mean time-to-repair of 1000 hr. The times-to-repair are assumed to be of that order of magnitude, because the repair involves in-vessel components (sensors).

In WARD-D-0118, the "objective" values of the transient arrival rates are assumed to be such that the number of expected transients per year (arriving according to a Poisson random process) is less than that of the design duty cycle with probability 0.95. These "objective" values are assumed to be the most probable values of the corresponding

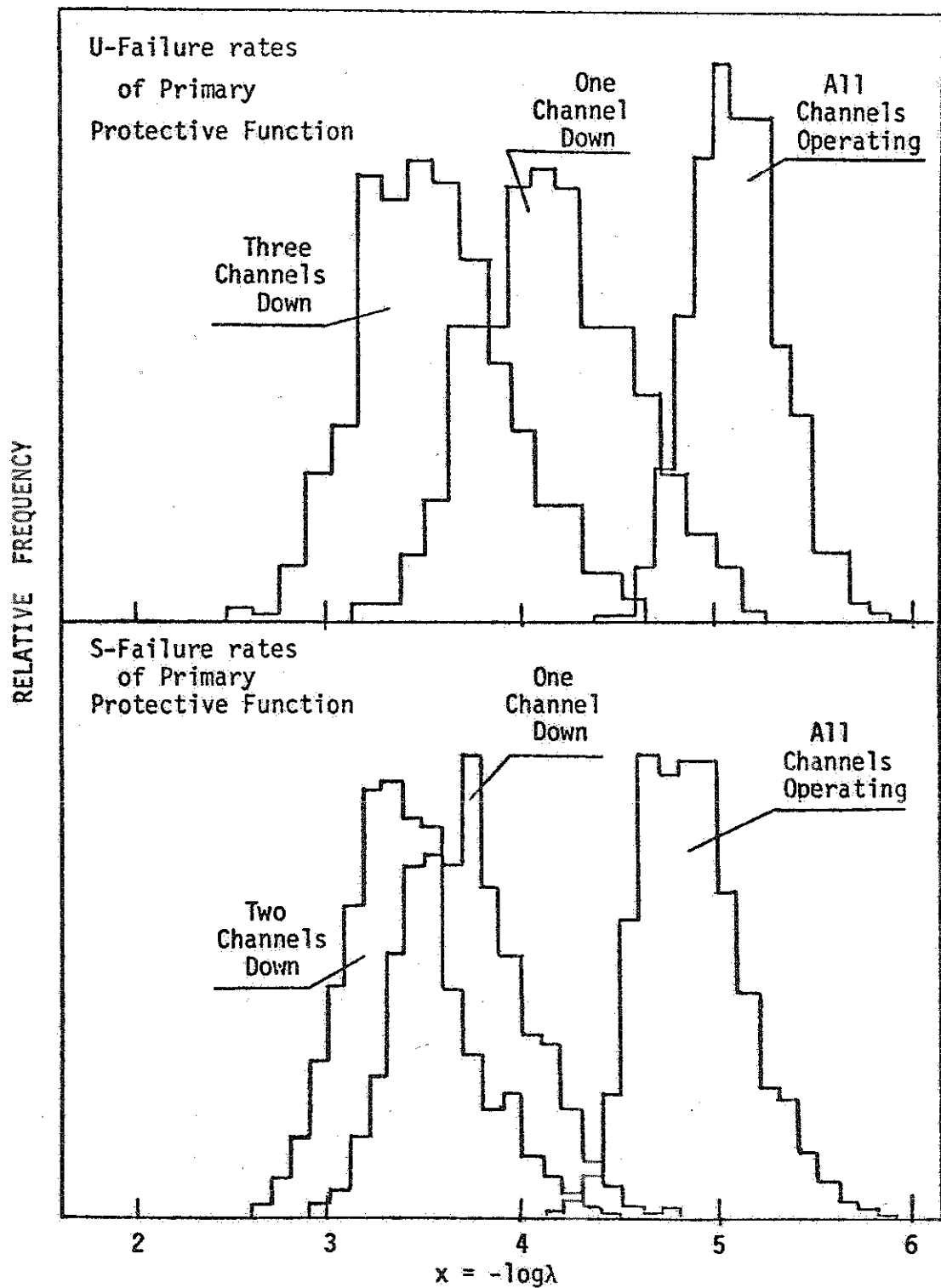


Figure 8.21. Histograms of the negative common logarithm of some transition rates of components of the shutdown system.



Table 8.3 Failure rates and associated uncertainties. Primary and Secondary Protective Function Networks.

Variable No.	Component	Parameter r	Parameter y	Most Probable Value (10 <sup>-6</sup> hr <sup>-1</sup> )	Mean Value (10 <sup>-6</sup> hr <sup>-1</sup> )	Lower 90% Conf. Limit (10 <sup>-6</sup> hr <sup>-1</sup> )	Upper 90% Conf. Limit (10 <sup>-6</sup> hr <sup>-1</sup> )
1	Primary Flux Sensor	2	20,000	5.0	10.0	1.8	23.6
2	Primary Pressure Sensor	2	50,000	2.0	4.0	0.7	9.5
3	Primary Flux Electronics	2	5,000	20.0	40.0	7.0	94.5
4	Primary Pressure Electronics	2	12,500	8.0	16.0	2.8	37.8
5	Primary Calculation Unit	2	34,483	2.9	5.8	1.0	13.7
6	Primary Comparator	2	34,483	2.9	5.8	1.0	13.7
7	Secondary Flux Sensor	2	20,000	5.0	10.0	1.8	23.6
8	Secondary Flow Sensor	2	50,000	2.0	4.0	0.7	9.5
9	Secondary Flux Electronics	2	5,000	20.0	40.0	7.0	94.5
10	Secondary Flow Electronics	2	12,500	8.0	16.0	2.8	37.8
11	Secondary Calculation Unit	2	34,483	2.9	5.8	1.0	13.7
12	Secondary Comparator	2	24,390	4.1	8.2	1.4	19.4
13	Secondary Logic Train	2	25,000	4.0	8.0	1.4	19.9

Table 8.3 (Cont'd)

Variable No.	Component	Parameter r	Parameter y	Most Probable Value (10 <sup>-6</sup> hr <sup>-1</sup> )	Mean Value (10 <sup>-6</sup> hr <sup>-1</sup> )	Lower 90% Conf. Limit (10 <sup>-6</sup> hr <sup>-1</sup> )	Upper 90% Conf. Limit (10 <sup>-6</sup> hr <sup>-1</sup> )
14	Primary Logic Train L1	2	35,714	2.8	5.6	0.98	13.23
15	Primary Logic Train L2 or L3	2	35,714	2.8	5.6	0.98	13.23
16	Primary Breaker S1	2	80,000	1.25	2.5	0.44	5.90
17	Primary Breaker S22 or S32	2	80,000	1.25	2.5	0.44	5.90
18	Primary Breaker S21, S31	2	80,000	1.25	2.5	0.44	5.90
19	Control rod	2	100,000	1.00	2.0	0.35	4.72

Table 8.4. Dependence coefficients and associated uncertainties

Variable No.	Subsystem	Parameter r	Parameter y	Most Probable Value	Mean Value	Lower 90% Conf. Limit	Upper 90% Conf. Limit
20	Electrical Subsystem One Channel Down	2	0.20	6.00	11.00	2.75	24.62
21	Electrical Subsystem Two Channels Down	2	0.10	11.00	21.00	4.50	48.23
22	Three or more channels down	2	21.00	41.00	41.00	8.00	95.46
23	Primary Logic One or more trains or breaker down	2	0.20	6.00	11.00	2.75	24.62
24	One Control Rod down	2	0.50	3.00	5.0	1.70	10.46
25	Two Control Rods down	2	0.25	5.00	9.00	2.40	19.89
26	Three Control Rods down	2	0.17	7.00	13.00	3.10	29.34
27	Four Control Rods down	2	0.13	9.00	17.00	3.80	38.78
28	Five Control Rods down	2	0.10	11.00	21.00	4.50	48.23
29	Six or more Control Rods down	2	0.05	21.00	41.00	8.00	95.46

random variables. The parameters of the pdf's and the 90% confidence limits of the reactor repair rate and the transient arrival rates are given in Table 8.5.

Finally, the parameters and the confidence limits for the probability of failure detection and the probabilities of inspection errors are given in Table 8.6. In "WARD-D-0118" the inspection of the electrical subsystems has been assumed perfect. In this study, we assumed that human errors during an inspection are possible. In the Reactor Safety Study (Appendix III, Human Reliability), it was assumed that the probability of a first error in inspecting the RSS of an LWR is  $10^{-2}$ . A second error, given the first, may happen with probability  $10^{-1}$ . Finally, if two errors have happened the probability of a third was assumed equal to 1. Since the inspections of the primary and secondary subsystems take place at different points in time, each inspection may be compared with the inspection of a LWR Shutdown System (LWRs have only one SS). The CRBR is, however, an experimental demonstration plant, and therefore it is expected that conditions during inspections as well as procedures will be different from those in a typical LWR. The mean value of the probability of making an error in inspecting the first channel of a subsystem is assumed to be  $10^{-3}$ .<sup>\*</sup> The mean value of conditional probability of an error in the second channel, given an error in the first, is set equal to  $3 \times 10^{-1}$ . Finally, the mean value of the conditional probability of a third error, given the first two, is set equal to  $7 \times 10^{-1}$ . The joint probability of three errors, using

---

<sup>\*</sup> See also Apostolakis (1977).

Table 8.5. Transient arrival rates, reactor repair rate and associated uncertainties

Variable No.	Transient	Parameter r	Parameter y	Most Probable Value (10 <sup>-6</sup> xhr <sup>-1</sup> )	Mean Value (10 <sup>-6</sup> xhr <sup>-1</sup> )	Lower 90% Conf. Limit (10 <sup>-6</sup> xhr <sup>-1</sup> )	Upper 90% Conf. Limit (10 <sup>-6</sup> xhr <sup>-1</sup> )
30	Reactor repair	2	1,000	1,000	2,000	350.00	4,723
31	Reactivity transient	2	10,752	93	186	32.55	439.24
32	Major Flow transient	2	24,390	41	82	14.35	193.64
33	Limited Response	2	804	1,244	2,488	435.40	5,875.40

Table 8.6 Failure detection probability, inspection error probability and associated uncertainties

Variable No.	Probability	Parameter p	Parameter q	Most Probable Value	Mean Value	Lower 90% Conf. Limit	Upper 90% Conf. Limit
34	Failure detection	98	2	.99	.98	.95	.99%
35	One inspection error	5	4995	8x10 <sup>-4</sup>	10 <sup>-3</sup>	3.7x10 <sup>-4</sup>	1.85x10 <sup>-3</sup>
36	Two insp. errors given one	3	7	.25	.30	.09	.55
37	Three insp. errors given two	5	2	.80	.70	.42	.94

the above cited mean values as point estimates of the corresponding probabilities, is equal to  $2.1 \times 10^{-4}$ . For an average of 10 inspections per subsystem per year and for 30 years of plant life, the chances of having one triple error during the plant lifetime are approximately one in ten ( $\sim 2.1 \times 10^{-4} \times 2 \times 10 \times 30$ ).

## 8.7 Presentation and Discussion of the Results

This section provides the quantitative assessment of the failure probability of the CRBR Shutdown System and the uncertainties associated with this probability. For this assessment we utilized the models developed in Sections 8.4 and 8.5 and the data in Section 8.6. The probability density function of the RSS failure probability was calculated by the two methods described in Chapters 6 and 7. The median and 90% confidence limits of the failure probability at various times are tabulated in Table 8.7 and plotted in Figure 8.22. These results were obtained as follows.

For the Monte Carlo calculation, 37 random samples (one for each input variable), each containing 1200 values, were generated and the Markov models were solved 1200 times. This resulted in a sample of 1200 values of the failure probability for each point in time. For each sample, estimators of the first four central moments were calculated, and from them the corresponding pdf was estimated as described in Chapter 5. It was found that at each point in time, the failure probability is very closely distributed according to a log-normal distribution (see Section 4.4.2). For example, the coefficients of skewness and kurtosis ( $\beta_1, \beta_2$ ) of the pdf of the negative

Table 8.7 Median and 90% confidence limits of the failure probability as functions of time

TIME (Weeks)	MEDIAN		LOWER 90% CONF. LIMIT		UPPER 90% CONF. LIMIT	
	Monte Carlo	Taylor	Monte Carlo	Taylor	Monte Carlo	Taylor
4	$3.1 \times 10^{-8}$	$1.7 \times 10^{-8}$	$2.0 \times 10^{-9}$	$2.5 \times 10^{-9}$	$6.2 \times 10^{-7}$	$1.5 \times 10^{-7}$
8	$2.7 \times 10^{-7}$	$1.6 \times 10^{-7}$	$2.9 \times 10^{-8}$	$2.1 \times 10^{-8}$	$4.0 \times 10^{-6}$	$1.2 \times 10^{-6}$
12	$5.1 \times 10^{-7}$	$3.2 \times 10^{-7}$	$4.8 \times 10^{-8}$	$4.0 \times 10^{-8}$	$7.4 \times 10^{-6}$	$2.5 \times 10^{-6}$
16	$7.8 \times 10^{-7}$	$4.8 \times 10^{-7}$	$7.1 \times 10^{-8}$	$5.8 \times 10^{-8}$	$1.1 \times 10^{-5}$	$4.0 \times 10^{-6}$
20	$1.0 \times 10^{-6}$	$6.6 \times 10^{-7}$	$9.8 \times 10^{-8}$	$7.6 \times 10^{-8}$	$1.5 \times 10^{-5}$	$5.6 \times 10^{-6}$
24	$1.3 \times 10^{-6}$	$8.3 \times 10^{-7}$	$1.2 \times 10^{-7}$	$9.5 \times 10^{-8}$	$1.9 \times 10^{-5}$	$7.3 \times 10^{-6}$
28	$1.6 \times 10^{-6}$	$1.0 \times 10^{-6}$	$1.5 \times 10^{-7}$	$1.1 \times 10^{-7}$	$2.2 \times 10^{-5}$	$9.1 \times 10^{-6}$
32	$1.9 \times 10^{-6}$	$1.3 \times 10^{-6}$	$1.7 \times 10^{-7}$	$1.3 \times 10^{-7}$	$2.7 \times 10^{-5}$	$1.1 \times 10^{-5}$
36	$2.2 \times 10^{-6}$	$1.4 \times 10^{-6}$	$2.0 \times 10^{-7}$	$1.5 \times 10^{-7}$	$3.3 \times 10^{-5}$	$1.3 \times 10^{-5}$
40	$2.5 \times 10^{-6}$	$1.6 \times 10^{-6}$	$2.2 \times 10^{-7}$	$1.7 \times 10^{-7}$	$3.7 \times 10^{-5}$	$1.4 \times 10^{-5}$
44	$2.8 \times 10^{-6}$	$1.7 \times 10^{-6}$	$2.5 \times 10^{-7}$	$1.9 \times 10^{-7}$	$4.4 \times 10^{-5}$	$1.6 \times 10^{-5}$
48	$3.1 \times 10^{-6}$	$1.9 \times 10^{-6}$	$2.7 \times 10^{-7}$	$2.1 \times 10^{-7}$	$4.5 \times 10^{-5}$	$1.8 \times 10^{-5}$

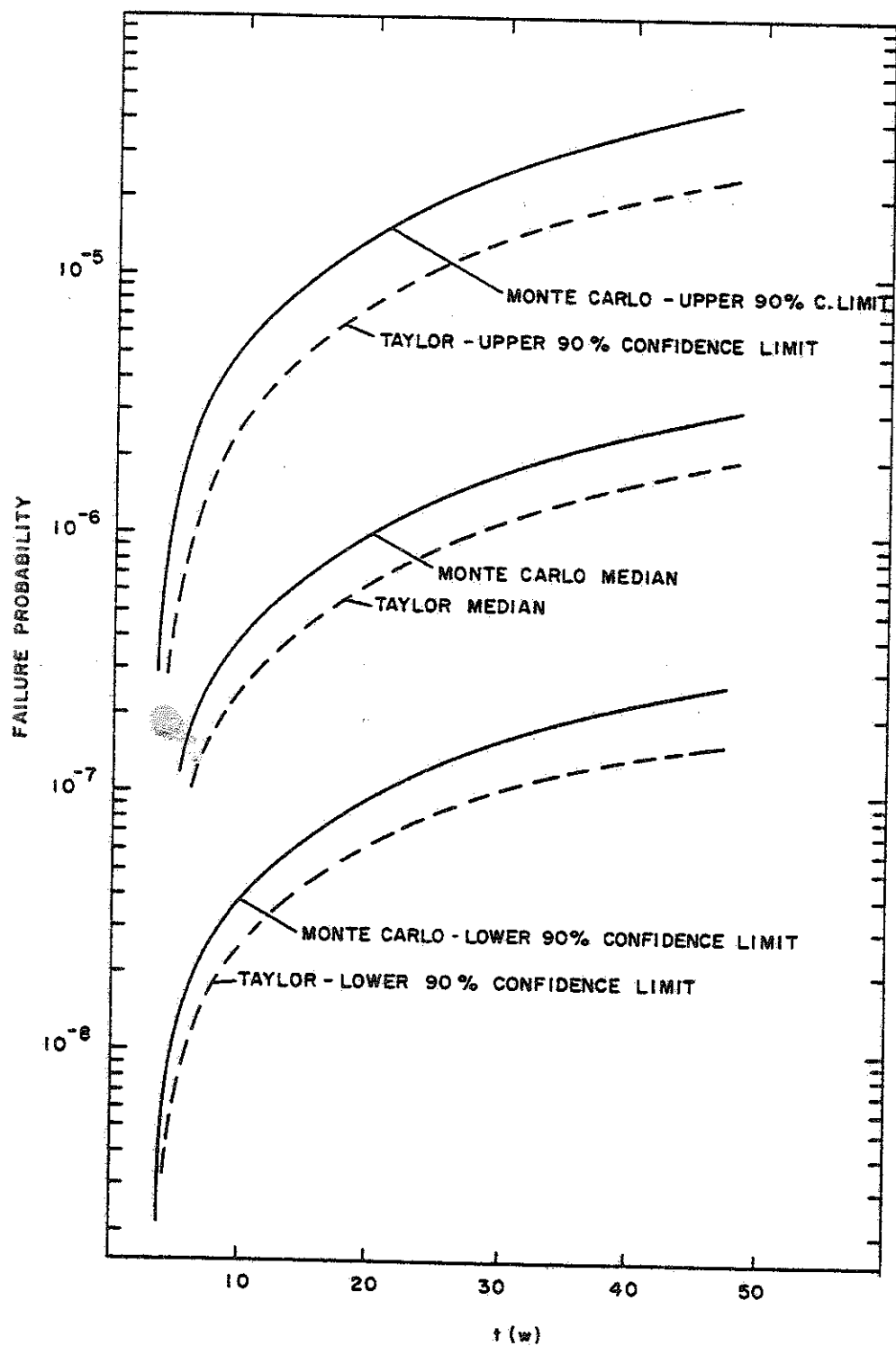


Figure 8.22. Median and 90% confidence limits of the RSS failure probability as a function of time.



common logarithm of the failure probability at the end of the 48th week were estimated to be 0.096 and 3.21, respectively. These values define a point in the  $(\beta_1, \beta_2)$  plane very close to the point (0,3) corresponding to the normal pdf (see Figure 5.1). The mean values, the variance, and the coefficients  $\beta_1, \beta_2$  of the negative common logarithm of the different points in time are given in Table 8.8. Finally the median and the 90% confidence limits of the mean (over a period of 48 weeks) unavailabilities of the system to respond to reactivity, major flow, and limited response transients are given in Table 8.9.

The first four central moments of the negative common logarithm of the failure probability were also estimated via the Taylor-series method developed in Chapter 7. First the derivatives of the failure probability with respect to the 37 input variables were found as shown in (7.17) and (7.12). Then, the derivatives of the negative common logarithm were found by applying the chain rule. For example, the second derivative is given by

$$\frac{\partial^2 Z}{\partial x_i^2} = \frac{\partial^2 Z}{\partial F^2} \left( \frac{\partial F}{\partial x_i} \right)^2 + \frac{\partial Z}{\partial F} \frac{\partial^2 F}{\partial x_i^2} \quad (8.22)$$

where

$$F = 10^{-Z} ,$$

and, therefore,

Table 8.8 Mean, variance and coefficients  $\beta_1$ ,  $\beta_2$  of the negative common logarithm of the failure probability at various times.

TIME (Weeks)	MEAN		VARIANCE		SKEWNESS ( $\beta_1$ )		KURTOSIS ( $\beta_2$ )	
	Monte Carlo	Taylor	Monte Carlo	Taylor	Monte Carlo	Taylor	Monte Carlo	Taylor
4	7.5	7.8	0.53	0.29	0.108	0.075	3.21	3.30
8	6.6	6.8	0.44	0.28	0.114	0.042	3.25	3.26
12	6.3	6.5	0.44	0.30	0.091	0.032	3.22	3.30
16	6.1	6.3	0.44	0.31	0.078	0.020	3.20	3.30
20	6.0	6.2	0.44	0.32	0.071	0.014	3.18	3.30
24	5.9	6.1	0.44	0.33	0.068	0.010	3.16	3.30
28	5.8	6.0	0.45	0.34	0.066	0.009	3.15	3.29
32	5.7	5.9	0.45	0.34	0.068	0.007	3.14	3.29
36	5.6	5.9	0.46	0.35	0.072	0.007	3.14	3.29
40	5.6	5.8	0.46	0.35	0.078	0.006	3.16	3.29
44	5.5	5.8	0.47	0.35	0.086	0.005	3.18	3.28
48	5.5	5.7	0.47	0.35	0.096	0.005	3.22	3.28

Table 8.9 Median and 90% confidence limits of the interval unavailabilities (mean over 48 weeks) of the system to respond to reactivity, major flow and limited response transients

Interval unavailability to respond to	Median	Lower 90% conf. limit	Upper 90% conf. limit
Reactivity trans.	$5.85 \times 10^{-6}$	$5.36 \times 10^{-7}$	$6.38 \times 10^{-5}$
Major flow trans.	$5.62 \times 10^{-6}$	$5.29 \times 10^{-7}$	$5.98 \times 10^{-5}$
Limited response trans.	$6.25 \times 10^{-13}$	$4. \times 10^{-17}$	$9.59 \times 10^{-9}$

$$\frac{\partial Z}{\partial F} = - \frac{1}{\ln 10} \frac{1}{F} ,$$

$$\frac{\partial^2 Z}{\partial F^2} = \frac{1}{\ln 10} \frac{1}{F^2} .$$

The expected value of the negative common logarithm, its variance, and the coefficients  $\beta_1$ ,  $\beta_2$  are tabulated in Table 8.8 for different times. From the same Table it can be seen that the results obtained by the Taylor series method are in good agreement with the results of the Monte Carlo calculations. The median and the 90% confidence limits of the failure probability at various times are given in Table 8.7 and plotted in Figure 8.22. The Taylor approximation of the pdf of the negative common logarithm of the failure probability at the end of the 48-th week and the corresponding histogram obtained from the Monte Carlo calculations are plotted in Figure 8.23.

As already discussed in Section 7.5, the results of the Taylor calculations provide a means for classifying the various input variables according to their contribution to the uncertainties of the failure probability. Such a classification has been done for the RSS failure probability at the end of one year, and the relative importance of the variables is shown in Table 8.10. The variables were classified according to two "Importance Indices". The first index gives, in percent form, the contribution of each variable to the deviation D of the expected value of the negative common logarithm of the failure probability from the value obtained when the input variables are fixed at their means [see (7.2)]. The second index gives, in percent form, the

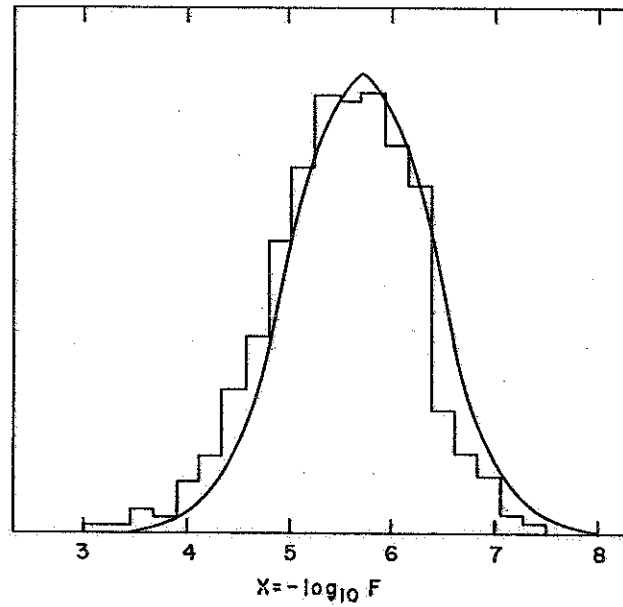


Figure 8.23. Pdf of the negative common logarithm of the RSS failure probability per year. Taylor series approximation and Monte Carlo diagram.

Table 8.10 Classification of input variables according to their contribution to the uncertainties of the failure probability.

Importance Index 1 gives the contribution to the deviation D (see text) and Importance Index 2 gives the contribution to the variance. Negligible contribution is denoted by  $\epsilon$ .

	Variable	Importance Index 1	Variable	Importance Index 2
1	Limited response transients	-69.6	Limited response transient	25.6
2	Reactivity transient	59.7	Reactivity transient	18.0
3	Pr. of one inspection error	36.3	Pr. of one inspection error	15.6
4	Cond. pr. of second insp. error	33.6	Secondary comparator	10.9
5	Dependence coefficient No.22*	22.3	Cond. pr. of second insp. error	9.2
6	Major flow transient	8.6	Dependence coefficient No.22*	7.8
7	Dependence coefficient No.20*	7.8	Failure detection probability	3.2
8	Dependence coefficient No.21*	5.4	Primary comparator	2.2
9	Secondary logic train	- 4.6	Major flow transient	2.0
10	Secondary comparator	3.9	Secondary logic train	1.8
11	Primary comparator	- 3.6	Dependence coefficient No. 21*	1.6
12	Reactor repair rate	3.0	Dependence coefficient No. 20*	1.1
13	Primary logic train L2,L3	- 2.7	Secondary flow electronic	$\epsilon$

Table 8.10 (Cont'd.)

	Variable	Importance Index 1	Variable	Importance Index 2
14	Control rod	- 2.4	Primary logic train L2,L3	ε
15	Failure detection probability	1.3	Secondary flux electronics	ε
16	Secondary flow sensor	ε	Secondary flow sensor	ε
17	Secondary flux sensor	ε	Primary flux electronics	ε
18	Secondary flow electronics	ε	Secondary flux sensor	ε
19	Primary flux electronics	ε	Primary pressure electronics	ε
20	Secondary flux electronics	ε	Dependence coefficient No. 23*	ε
21	Dependence coefficient No. 23*	ε	Reactor repair rate	ε
22	Primary flux sensor	ε	Primary flux sensor	ε
23	Primary pressure electronics	ε	Primary breaker B1	ε
24	Primary pressure sensor	ε	Primary pressure sensor	ε
25	Primary breaker S22,S32	ε	Secondary calculation unit	ε
26	Pr. of three inspection errors	ε	Control rod	ε
27	Primary calculation unit	ε	Primary calculation unit	ε
	Others	ε	Others	ε

\*

See Table 8.4

contribution of each variable to the variance of the negative common logarithm of the failure probability [see (7.3)]. In other words (see Table 8.10), if the arrival rate of the limited response transients were fixed in its mean value, the deviation  $D$  would have increased by 70%, while the variance of the negative logarithm would have increased by 26%. It is noteworthy that the importance of the limited response transient arrival rate is due not to the failures that these transients might cause, but to the renewal effect that successful responses have on the Shutdown System. This means that the limited response transients are equivalent to complete, perfect repairs of the system, occurring randomly in time. Examination of Table 8.10 reveals that the variables that contribute the most to the uncertainty about the failure probability are the arrival rates of the various transients and the probabilities of human error during the inspection of the electrical subsystems.

To assess the contribution of the interdependences and of the human errors in RSS failure probability, four cases were considered: (I) the failure rates of the components are completely independent and the inspection is perfect, i.e., every four weeks the electrical subsystems are completely renewed; (II) interdependences among the failure rates and the state of the components have been assumed and the inspection is perfect; (III) independent failure rates but imperfect inspection, i.e., human errors are possible; (IV) interdependences exist and the inspection is imperfect. The median, the 90% confidence limits, and the point estimates of the RSS failure probability per

year are given in Table 8.11. Point estimate is the value of the failure probability when the input variables are fixed at their mean. The "objective" (see section 8.5) value of the failure probability obtained in WARD-D-0118 is also included in Table 8.11. The difference in the "objective" value of WARD-D-0118 and the point estimate of case I is due to the more detailed modeling of the electrical subsystem that was employed in this study. In particular, successful responses to limited response transients result in the renewal of the electrical subsystem, and the repair of the sensors (with the reactor shut down) is not instantaneous.

We can see from Table 8.11 that: (1) uncertainties in the input variables (case I) result in a 90% confidence interval for the failure probability that spans 3 orders of magnitude ( $4.0 \times 10^{-11}$  to  $2.5 \times 10^{-8}$ ); (2) uncertainties and interdependences (case II) result in a 90% confidence interval for the failure probability of the same size as in case I but shifted to the right by two orders of magnitude ( $2.0 \times 10^{-9}$  to  $6.5 \times 10^{-6}$ ); (3) uncertainties and human errors (case III) result in a 90% confidence interval for the failure probability shifted by two orders of magnitude to the right but narrower than that of case I ( $1.0 \times 10^{-8}$  to  $5.0 \times 10^{-6}$ ); and (4) uncertainties, interdependences and human errors (case IV) result in a 90% confidence interval for the failure probability shifted to the right by three orders of magnitude but narrower than that of case I ( $2.0 \times 10^{-7}$  to  $2.0 \times 10^{-5}$ ). Finally, it is noteworthy that the values of the failure probability obtained with the input variables fixed at their means (point estimates) are very close to the medians for all four cases.



TABLE 8.11 Point estimate median and 90% confidence limits of the RSS failure probability per year under various assumptions. Point estimate is the value of the failure probability obtained when the input variables are assumed fixed at their means.

Case	Description	Point estimate	Median	Lower 90% Conf.Limit	Upper 90% Conf.Limit
0	Ward-D-0118	$1.5 \times 10^{-9}$	-	-	-
I	No dependences, perfect inspection	$8.0 \times 10^{-10}$	$1.0 \times 10^{-9}$	$4.0 \times 10^{-11}$	$2.5 \times 10^{-8}$
II	Dependences, perfect inspection	$2.0 \times 10^{-7}$	$8.0 \times 10^{-8}$	$1.0 \times 10^{-9}$	$6.5 \times 10^{-6}$
III	No dependences, imperfect inspection	$4.0 \times 10^{-7}$	$2.5 \times 10^{-7}$	$1.0 \times 10^{-8}$	$5.0 \times 10^{-6}$
IV	Dependences, imperfect inspection	$2.5 \times 10^{-6}$	$2.0 \times 10^{-6}$	$2.0 \times 10^{-7}$	$2.0 \times 10^{-5}$

## CHAPTER NINE

### SUMMARY AND CONCLUSIONS

The objectives of this study have been: the development of a methodology for the calculation of uncertainties about the reliability of nuclear reactor systems described by Markov models, and the assessment of the uncertainties in the reliability of the Shutdown System of the Clinch River Breeder Reactor.

#### 9.1 Methodology

The uncertainty about the reliability of nuclear reactor systems stems from existing uncertainties about the failure and repair rates of components as well as from uncertainties about other variables that characterize the stochastic behavior of the systems. We quantified these uncertainties by assuming that the various transition rates and the probabilities are random variables distributed according to given probability density functions. We attempted then to answer the following question: "How does one calculate the probability density function of the reliability from the pdf's of the input variables?" For Markovian systems this question reduces into: "How does one calculate the pdf of the state probability vector of a Markov process, given the transition probabilities of the process are random variables distributed according to given pdf's?"

The exact mathematical form of this problem was presented in Chapter 4 where it was stated that, because of the complexity and the size of systems of practical importance, we believe that an analytical solution is not feasible. An approximate method was, therefore,

needed, and the moment-matching technique described in Chapter 5 was employed. According to this technique the first four moments of the reliability are calculated and the pdf of the reliability is approximated by an appropriate distribution with the same first four moments. The moments of reliability were calculated with the help of two methods: 1) the Monte Carlo simulation method, described in Chapter 6; and 2) the Taylor series method, described in Chapter 7.

The Monte Carlo simulation method randomly generates a sample of  $Nm$ -tuples  $x_{ij}$ ,  $i=1,2,\dots,m$   $j=1,2,\dots,N$ , where  $x_{ij}$  denotes the  $j$ -th value of the  $i$ -th input variable, and calculates the reliability  $N$  times, one value of reliability for each  $m$ -tuple  $\{x_{ij}\}$ . A random sample of  $N$  values of the reliability is thus generated and from it the required moments can be estimated. Because the Monte Carlo method is used to estimate moments of, rather than the full, reliability the required sample size is not too large. From the experience gained during this research we feel that about  $10^3$  trials are adequate in most cases.

The Taylor series method consists in: (1) expanding the reliability function in a Taylor series around the means of its variables; (2) truncating the series; and (3) using the resulting simple analytical expression for the direct calculation of the moments. The Taylor series representation of a function is more accurate for small deviations of the independent variables from the point around which the function is expanded. Therefore, the smaller the probability that the variables  $x_{ij}$  will take simultaneously values "far" from their respective means,

the more accurate the estimation of the moments. The Taylor series method also provides a tool for performing sensitivity analyses. Indeed, once the accuracy of the method has been checked at a certain level of the mean values of the  $x_i$ 's (perhaps with a Monte Carlo calculation), the other moments of the  $x_i$ 's can be varied and the changes in the reliability moments can be calculated. The Taylor series method is faster than the Monte Carlo if the number of the independent variables  $x_i$  is smaller than a certain limit. This limit can be calculated as follows. From equations (7.17) it follows that the calculation of the first four partial derivatives of the vector  $\pi(n)$  with respect to a variable  $x_i$  are equivalent to 8 multiplications of the form  $\underline{u} \cdot \underline{M}$ , where  $\underline{u}$  is a  $1 \times z$  row vector and  $\underline{M}$  a  $z \times z$  matrix. This means that the calculation of the partial derivatives with respect to  $m$  independent variables is equivalent to 8 multiplications of the form  $\underline{u} \cdot \underline{M}$  or, equivalently, to a Monte Carlo sample size of  $8m$ . Thus, if  $10^3$  trials are required for a Monte Carlo calculation, the Taylor series method will be faster if the number of independent variables is less than 125. This cutoff value, however, will be lower if terms of higher order than four are included in the Taylor expression, or if the  $x_i$ 's are correlated.

In general, we can say that for a given system at least one Monte Carlo calculation is needed to provide a standard against which the accuracy of the Taylor method is tested. Then, if accurate enough and faster, the Taylor method can be used for sensitivity analysis.

In both methods employed in this study the computational effort consists of the repeated solution of the first-order difference equation

$$\underline{\pi}(n+1) = \underline{\pi}(n) \cdot \underline{P} \quad . \quad (9.1)$$

Thus, this effort can be reduced if the solution of (9.1) is expedited. The computing time necessary for solving (9.1) depends on three factors:

- (1) Structure of  $\underline{P}$
- (2) Dimensions of  $\underline{P}$
- (3) Number of time steps for which (9.1) must be solved.

The first two factors affect also the computer storage requirements.

A technique for simplifying the structure of  $\underline{P}$  by ordering the states of the system was developed and presented in Chapter 2.

A technique for reducing the dimensions of  $\underline{P}$  by merging, whenever possible, the Markov processes was described in Chapter 3. It was shown there that systems exhibiting certain symmetries are described by mergeable Markov processes. Since the nuclear safety systems are highly redundant, they almost always exhibit these symmetries. A systematic way for achieving the merging was also developed.

The choice of the maximum possible time step is discussed in Chapter 6 along with an approximation that permits the use of large time steps in the Monte Carlo calculations.

The calculations necessary for the implementation of the methods described in Chapters 2 through 7 are performed with the help of a computer. The necessary computer codes are briefly described in the Appendices.

## 9.2 Reliability Assessment of the CRRR RSS

As an illustration of the methodology developed in this study, the uncertainties about the failure probability of the Shutdown System of the Clinch River Breeder Reactor were assessed.

The Shutdown System of the CRBR consists of two shutdown systems, the primary and the secondary. Each shutdown system consists of an electrical and a mechanical subsystem. The primary and secondary electrical subsystems are designed to sense the need for a shutdown and signal the primary and secondary mechanical subsystems, respectively, which respond by inserting the control rods into reactor core. The mission of the reactor shutdown system is therefore "to sense and successfully respond to a defined set of transients in such a way that the loss of core coolable geometry is avoided during the lifetime of the plant." It was assumed that the loss of coolable core geometry occurs in the short term if sodium reaches saturation conditions (boiling) in the hot channel ( $\sim 1700^{\circ}\text{F}$ ), or in the long term if the in-vessel bulk sodium outlet temperature rises in excess of  $1250^{\circ}\text{F}$ . Therefore given a transient, the success or failure of shutdown system depends upon inserting the minimum amount of reactivity in an acceptable increment of time, so that neither of the above cited events will happen.

Furthermore, it was assumed that three different types of transients might occur randomly during the plant lifetime: (1) reactivity transients requiring electrical subsystem response and the insertion of \$5 of negative reactivity; (2) major flow accidents that require electrical subsystem response and the insertion of \$2.5 of negative reactivity; and

(3) limited response transients that do not require electrical subsystem response and need the insertion of  $\Delta k$  of negative reactivity.

The probabilistic behavior of the system was modeled by a Markov process. The use of such a model permitted the modeling of:

- (1) Common cause failures by allowing interdependences among the failure rates and the states of the components. Interdependences have been assumed between the components of the two electrical subsystems as well as between the components of the two mechanical subsystems.
- (2) Interdependences between the unavailability of the shutdown system and the occurrence of transients. Given a transient, the system may either respond successfully or fail. Since there are three types of transients, whether the system will succeed or fail depends on the particular state of the system and on the particular transient. Furthermore, a successful response to a transient means a reactor shutdown and system renewal before resuming operations. Thus, the unavailability of the shutdown system depends on the frequency of transient arrivals. Finally, if the reactor is shut down, transients that lead to loss of coolable core geometry cannot occur.
- (3) Inspection and maintenance procedures that depend on the state of the system and include the possibility of human errors. To increase the availability of the shutdown system, tests and maintenance are performed periodically. The policy for such tests may depend on the state of the reactor (online or

shutdown) or on the state of the shutdown subsystems (number of channels tripped, etc.). In addition, there is a possibility of human errors. Such errors may be the failure to reveal and correct an existing fault or the causing of a fault during maintenance.

Uncertainties about the failure rates, the repair rates, the rates at which transients occur, and all other input variables were quantified by assuming that all the variables are random, distributed in such a way that their upper 90% confidence limit is one order of magnitude higher than the lower 90% confidence limit. The latter limit is of the same order of magnitude as the most probable value of the quantity in question. Furthermore, the most probable value of each variable was assumed equal to its "objective value." The "objective values" are the values that the Clinch River Breeder Reactor Project Management Corporation intends to demonstrate by a combination of tests and analyses.

The probability density function of the failure probability was calculated by the moment-matching technique. The moments of failure probability were calculated by both the Monte Carlo and the Taylor series methods. As seen in Tables 8.7 and 8.8, the results of these two methods are in very good agreement.

The failure probability is distributed log-normally with median  $2 \times 10^{-6}$ , and upper and lower 90% confidence limits  $= 2 \times 10^{-5}$  and  $2 \times 10^{-7}$ , respectively. This probability band represents a considerable difference from the  $1 \times 10^{-9}$  point estimate of the failure probability where interdependences are not considered, the inspection is perfect,



and the input variables are fixed at their mean values. The results obtained in this study are in agreement with the analyses and experience for Light Water Reactors, where human errors during test and maintenance activities and common cause failures are major contributors to system unavailability, and therefore to the failure probability. If interdependences and human errors are not considered, the 90% confidence interval of the failure probability extends from  $4.0 \times 10^{-11}$  to  $2.5 \times 10^{-8}$  with a median of  $1.0 \times 10^{-9}$ . The inclusion of interdependences alone (hardware common cause failures) results in a 90% confidence interval from  $1.0 \times 10^{-9}$  to  $6.5 \times 10^{-6}$  with a median of  $8.0 \times 10^{-8}$ . Consideration of human errors (imperfect inspection) has approximately the same effect. The corresponding 90% confidence interval extends from  $1.0 \times 10^{-8}$  up to  $5.0 \times 10^{-6}$  with a median of  $2.5 \times 10^{-7}$ .

Uncertainties of about one order of magnitude for the various input variables resulted in a two orders of magnitude uncertainty for the failure probability. Tests and/or analysis can reduce the uncertainties about the input variables and, hence, the uncertainties about the failure probability of the CRBR due to shutdown system failures. More information about failure rates can be obtained by testing individual components and/or by analysis. However, information about the dependence coefficients (hardware common cause failure), human errors (imperfect inspection), and the transient arrival rates cannot be obtained from tests of individual components. Such information can be obtained only by observing real systems in operation. For this reason we believe that the experience that will be gained from the Fast Flux Test Facility and the

Clinch River Breeder Reactor will be of major importance in assessing the failure probability of large Liquid Metal Breeder Reactors.

## CHAPTER TEN

### RECOMMENDATIONS FOR FURTHER RESEARCH

The reliability of a system is an important factor in evaluating its usefulness and, therefore, explicitly or implicitly decisions are made on the basis of this evaluator. If the value of the reliability is exactly known, then the decision is usually made by comparing this value against a given standard. If the reliability is higher than the standard, the system is considered "reliable enough" and it is accepted. If the reliability is lower, the system is not accepted. In the presence of uncertainties, however, this simple procedure cannot be applied because the value of the reliability is not known exactly. Then we have a problem of decision analysis under uncertainty. A systematic way for making a decision under those circumstances is, therefore, needed.

A systematic way for making decisions under uncertainty is provided by the theory of decision analysis. Decision analysis involves two distinctive features: an uncertainty analysis and a preference analysis. Uncertainty analysis deals with the assessment of the uncertainties about the factors that affect the decision. Preference analysis addresses the problem of classifying all possible outcomes of the uncertain events according to their importance. Usually this is done with the help of the von Neumann-Morgenstern utility theory. In reliability analysis, the application of this theory would mean the definition of a scalar function that describes the relative importance of the various values of the reliability measures. Once such a preference analysis is performed and the uncertainties are assessed, the decision analysis theory can be applied. This dissertation addressed the problem of

uncertainty analysis. The question of preference analysis remains open.

Even when the preference and uncertainty analyses have been completed, an important question is: "Should we base our decision on the available information (on the existing uncertainties) or should we try to obtain more information before we make our decision?" We can obtain more information by testing components and by building and observing prototype systems. Tests of components provide information about the independent failure and repair rates while observation of actual systems provide information about the dependence coefficients and other system-dependent parameters. Then, the previous question becomes: "How many components of each kind should we test and for how long a time? Furthermore, for how long, if at all, should we observe a prototype system?" To answer these questions, preferences or value tradeoffs should be established between reliability and the amount of money and time spent for the experiments. The answers, then, will define the "optimum experiment" or the "optimum reliability demonstration program"; optimum in the light of the performed uncertainty and preference analyses.

Another important question that need be answered in the presence of uncertainties is: "Which is the best test and maintenance policy for the standby safety systems?" This question can be better discussed in terms of a specific example such as a nuclear reactor. As seen in Chapter 8, two possible policies for the testing of the shutdown system of CRBR were: (I) If at the time of a scheduled inspection of

an electrical subsystem a channel is tripped, the reactor is shut down and the system is overhauled; (II) If at the time of a scheduled inspection of an electrical subsystem a channel is tripped, then the reactor is shut down only if a channel of the other subsystem is tripped. Policy I results in a higher reliability, but at the same time in a higher unavailability, of the reactor than policy II. A tradeoff between the reactor unavailability and reliability should be established, and then the best policy can be defined. This analysis will also define the optimum test frequency. Of course, the optimum policy need not be static and may vary with time as more information is obtained about the system. Thus, an adaptive procedure can be established according to which the optimum policy is determined at each point of time, taking into account all the information (in the form of observed failures and repairs) available at this particular time.

Further research could also be done in the area of uncertainty analysis. Since computer time and computer storage requirements for large systems with many states could be severe, research for methods reducing these requirements is advisable. Three such methods are briefly described in the sequel.

Substantial savings in both computing time and computing storage requirements can be achieved if the dimensions of the problem can be reduced. In Chapter 3, the theory of mergeable Markov processes was presented. It was seen that the dimensions of the problem could be reduced by lumping together system states to form superstates. The

resulting process could be exactly solved if the transition probabilities of the original process satisfy a criterion. This criterion guarantees that the superstate transition probabilities are independent of the state probabilities  $\pi_i(n)$ 's of the original process (see Eqs. 3.3 and 3.11). For convenience, we repeat here equation (3.3)

$$p_{IJ}(n) = \sum_{i \in T_I} w_i(n) \sum_{j \in T_J} p_{ij}(n), \quad (10.1)$$

where

$$w_i(n) = \frac{\pi_i(n)}{\sum_{i \in T_I} \pi_i(n)}. \quad (10.2)$$

From (10.1) it follows that if the "weighting coefficients"  $w_i(n)$ 's were known, the supertransition probabilities  $p_{IJ}(n)$ 's could be defined for any grouping of the states of the original process. But knowledge of the  $w_i(n)$ 's means knowledge of the  $\pi_i(n)$ 's which in turn means solving the original problem. If approximations  $\hat{w}_i(n)$  to the weighting coefficients could be obtained, however, an approximate merging of the system states could be possible. Such approximate  $\hat{w}_i(n)$ 's could be obtained by neglecting some of the interdependences between the components and, thus, by decomposing the system into several independent subsystems. The Markov process of each subsystem could be solved separately, and from the resulting subsystem-state probabilities, the state probabilities of the original system can be obtained. A

similar idea could be applied in the Monte Carlo simulation. There, the  $w_i(n)$ 's obtained by solving the exact problem with the transition probabilities fixed at their mean values could be used in all the random trials.

The computer codes for this work were written under the assumption that the time step of the process is sufficiently small that only one component-transition is possible at the end of each time step. This assumption results in a sparse transition probability matrix and, thus, in computer-storage savings. If this assumption is relaxed, larger time steps could be used resulting in shorter running times but requiring more core memory. A study of the memory and running time requirements of the various techniques for solving first-order differential equations could suggest a more effective method.

Finally, in his monograph "Bayesian Decision Problems and Markov Chains," Martin (1967) develops recurrence formulae for the expected value and the variance of the state probability,  $\pi_i(n)$ , of a process with transition probabilities distributed according to a certain family of pdf's. The possible development of similar formulae for the expected value of the utility of a reliability measure should be explored. If such a formula can be developed, a computer code could be written using a compiler that handles efficiently recurrence formulae (PL/1, for example), and the necessary computing time could be compared with the time required by methods developed in this study.

In summary, we recommend: (1) the application of decision theory in establishing "Reliability - demonstration" programs for systems;

(2) the application of decision theory in establishing "test and maintenance" policies for safety systems; (3) the investigation of systematic ways of approximate merging of Markov processes; (4) the investigation of tradeoffs between core memory storage requirements and running time requirements of methods for solving Markov models; and (5) the possible application of a technique developed by Martin (1967) for solving Markov models under uncertainty.



## REFERENCES

- Apostolakis, G.E. and Bansal, P.P. The effect of human error on the availability of periodically inspected redundant systems, IEEE Trans. Reliab., vol R-26, Aug. 1977.
- Apostolakis, G.E. and Lee, Y.T. Methods for the estimation of confidence bounds for the top-event unavailability of fault trees, UCLA-ENG-7650, May 1976.
- Apostolakis, G.E. et al. LMFBR fuel analysis. Task C: Reliability aspects of LMFBRs, Final report, NUREG-0148.
- Bacon, G.C. The decomposition of stochastic automats, Inform. & Contr. vol 7, pp. 320-339, Sept. 1964.
- Barlow, R. and Prochan, F. Mathematical Theory of Reliability, Wiley, 1965.
- Billinton, R., Ringlee, R.J., and Wood, A.J. Power-system Reliability Calculations, MIT Press, 1973.
- Bowers, T.L. and Werner, E.J. Reliability analysis of the Fast Flux Test Facility, Westinghouse Electric Corporation, W-R-750978, July 1975.
- Box, G.E.P. and Tiao, G.C. Bayesian Inference in Statistical Analysis, Addison Wesley, 1973.
- Buzacott, J.A. Markov approach to finding failure times of repairable systems, IEEE Trans. Reliab., vol 19, pp. 128-134, Nov. 1970.
- Carter, L.L. and Cashwell, E.D. Particle-Transport Simulation with the Monte Carlo Method, TID-26607, ERDA, 1975.
- Cox, N.D. and Cermac, J.O. Uncertainty analysis of the performance of complex systems, Energy Sources, Vol. 1, No. 4, pp. 339-359, 1974.

- Cox, N.D. Comparison of two uncertainty analysis methods. Presented at the American Nuclear Society Mathematics and Computation Division Topical Meeting on Improved Methods for Analysis of Nuclear Systems, Tucson, AZ, March 1977.
- Cozzolino, J.M. et al. Markovian decision processes with uncertain transition probabilities, Technical Report No. 11, Operations Research Center, MIT, March 1965.
- Cramer, H. Mathematical Methods of Statistics, Princeton University Press, 1946.
- Dwyer, P.S. and MacPhail, M.S. Symbolic matrix derivatives, Ann. Math. Stat. 19, 517-534 (1948).
- Evans, D.H. Statistical tolerancing: The state of the art. Part I Background, Quality Technology, Vol 6, No. 4, Oct. 1974.
- Evans, D.H. Statistical tolerancing: The state of the art. Part II, Methods for estimating moments, Quality Technol., Vol. 7, No. 1, Jan. 1975.
- Evans, D.H. Applied Multiplex sampling, Technometrics, Vol. 5, No. 3, Aug. 1963.
- Evans, D.H. Multiplex Sampling, Ann. Math. Stat. 34, 1322, (1963).
- Farmer, F.R. Nuclear Reactor Safety, Academic Press, 1977.
- Feller, W. "An Introduction to Probability Theory and its Applications", Vol. I, Vol. II, Wiley, 1950.
- Flenhinger, B. J. A Markovian model for the analysis of the effects of marginal testing on system reliability, Ann. Math. Stat. 33, 754, (1962).

Gangloff, W.G. "Common mode failure analysis", IEEE Trans. PAS., Vol PAS-94, pp. 27-30, Jan/Feb 1975.

Gelbard, (b) "Notes on Monte Carlo simulation", Unpublished lecture notes from lectures given at Bettis Atomic Power Laboratory.

Green, A.E. and Bourne A.J. "Reliability Technology", Wiley-Interscience, 1972.

Hahn, G.J. and Shapiro, S.S. Statistical Models in Engineering, Wiley, 1967.

Haugen, E. Probabilistic Approach to Design, Wiley, 1968.

Henrici, P. Error Propagation for Difference Methods, Wiley, 1964.

Hildebrand, F.B. Finite Difference Equations and Simulations, Prentice-Hall, 1968.

Howard, R. Dynamic Probabilistic Systems, Vol. I - Vol. II, Wiley, 1971.

IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems, IEEE Std. 352-1975, Apr. 1975.

Kahn, H. Applications of Monte Carlo, Rand-Corporation, AECU-3259, Apr. 1954.

Lee, G.T.H. Mean-times of interest in Markovian Systems, IEEE Trans. Reliab., Vol. R-20, pp. 16-21, Feb. 1971.

Kemeny, J.G. and Snell, J.L. "Finite Markov Chains", D. Van Nostrand Co. 1960.

Martin, J.J. Bayesian Decision Problems and Markov Chains, Wiley, 1967.

Mazzumdar et al. Review of the methodology for statistical evaluation of reactor safety analyses, EPRI-NP-194, July 1975.

Morse, P.M. and Feshback. "Methods of Theoretical Physics", McGraw-Hill, 1953.

Neuman, C.P. and Bonhomme, N.M. Evaluation of maintenance policies using Markov Chains and fault tree analysis, IEEE Trans. Reliab., Vol. R-24, pp. 37-44, Apr. 1975.

Papazoglou, I.A. Markovian analysis of reliability of nuclear reactor systems, S.M. thesis MIT Nucl. Eng. Dept., 1974.

Preliminary Safety Analysis Report, Clinch River Breeder Reactor Project.

Raiffa, H. and Schlaifer, R. "Applied Statistical Decision Theory", MIT Press, 1961.

Reactor Safety Study, WASH-1400, Oct. 1975.

Royden, H.L. "Bounds on a distribution function when its first  $n$  moments are given", Ann. Math. Stat. 24, 1953, 361-376 (1953).

Sandler, G.H. "System Reliability Engineering", Prentice-Hall 1963.

Shooman, M.D. Probabilistic Reliability: An Engineering Approach, McGraw-Hill, 1969.

Silver, E.A. Markovian Decision Processes with Uncertain Transition Probabilities and Rewards, Sc.D. Thesis, MIT, Dept. of Civil Eng., Aug. 29, 1963.

Singh, G. and Billinton, R. Frequency and duration concepts in systems reliability evaluation, IEEE Trans. Reliab., Vol. R-24, pp. 31-36, Apr. 1975.

Spanier, J. and Gelbard, E. Monte Carlo Principles and Neutron Transport Problems, Addison-Wesley, 1969.

Tukey, J.W. Propagation of errors, fluctuations and tolerances, No. 1: Basic generalized formulas, Technical Report No. 10, Statistical Techniques Research Group, Princeton University, Princeton, NJ, 1957.

Tukey, J.W. Propagation of errors, fluctuations and tolerances, No. 2: Supplementary formulas, Technical Report No. 11, Ibid.

Tukey, J.W. Propagation of errors, fluctuations, and tolerances, No. 3: Exercise in differentiation, Technical Report No. 12, Ibid.

Vesely, W.E. Estimating common cause failure probabilities in reliability and risk analyses: Marshall-Olkin specializations. Presented to the Int. Conf. Nucl. Systems Reliab. Eng. and Risk Assessment, Gatlinburg, TN, June 1977.

WARD-D-0118 Reliability Assessment of CRBR Reactor Shutdown System, Westinghouse Electric Corporation, Nov. 1975.

WASH-1270 Technical Report on Anticipated Transients without scram for the Water Cooled Power Reactors, Sept. 1970.

Wilks, S.S. "Mathematical Statistics", Wiley, 1962.

WR-50602 "Plant Protection System Test Program Basis", Apr. 1975.

WR-50670 "Reliability Confirmation Test Plan for Primary and Secondary Control Rod System of CRBR", Apr. 1975.

## APPENDIX A

### STAGEN--MARELA

#### A Computer Code for Markovian Reliability Analysis

This Appendix contains a brief description of the computer codes STAGEN and MARELA that evaluate the time-dependent and the average availability (or reliability) of a system described by a Markov process. The methodology upon which the codes are based is presented in Chapter 2.

The code consists of two parts: 1) STAGEN, STATE GENERator, that generates and orders the system states; and 2) MARELA MARKOVian RELia-bility Analysis, that performs the reliability calculations. A flow chart of this code is given in Figure A.1.

Program STAGEN generates the set of  $Z$  of all possible states of the system, partitions  $Z$  into subsets  $X$  and  $Y$  with the help of subroutine STEST, and then classifies  $X$  and  $Y$  into subsets  $X(K)$  and  $Y(K)$  (see Sections 2.2 and 2.4). In addition, this program calculates the number of elements of the ordered transition probability matrix that need be stored and the number of elements of each submatrix  $\underline{P}^{KL}$ , and generates indices that show the starting point of each submatrix within the 1-dimensional  $P$ -array.

Program MARELA generates the transition probability matrix  $\underline{P}$  and performs the multiplication in (2.3) for the necessary number of time steps. The size of the time step is selected internally in such a way that assumption 2.9 (see Section 2.3) is valid.

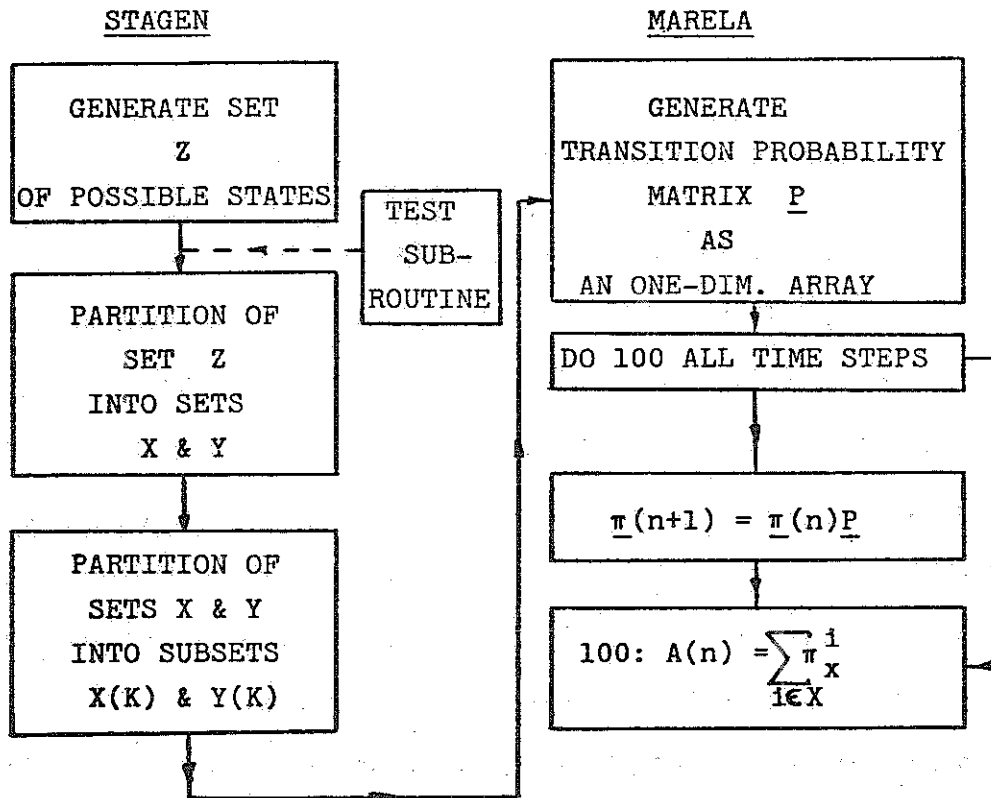


Figure A.1. Flow chart of programs STAGEN and MARELA.

A complete description of the code containing user's instructions is contained in a Brookhaven National Laboratory - NUREG Report, under the title: Computer Codes for Markovian Reliability Analysis.

## APPENDIX B

### SSTAGEN - MMARELA

#### A Computer Code for Mergeable Markovian Reliability Analysis

This Appendix contains a brief description of the computer codes SSTAGEN-I, SSTAGEN-II and MMARELA that evaluate the time dependent and average availability (reliability) of systems described by mergeable Markov processes. The underlying methodology is presented in Chapter 3.

The code consists of two parts: 1) SSTAGEN, SuperState GENerator, that generates and orders the superstates of the system; this part has two versions (I and II); and MMARELA, Mergeable Markovian RELiability Analysis, that performs the reliability calculations.

Programs SSTAGEN-I and SSTAGEN-II generate the superstate of the process. In SSTAGEN-I, the superstates are generated directly from the component states of the original process. Here it is assumed that the symmetries of the system are correctly defined. In SSTAGEN-II the system states of the original process are generated and then merged into superstates on the basis of criterion (3.11).

Program SSTAGEN-I generates the superstates as follows: For each and every subsystem class (see Chapter 3) it generates all the labels characterizing the subsystem-states. Symmetries at a component-level are used at this stage. Then each subsystem is considered as a component that can be in as many states as the subsystem-state labels corresponding to this subsystem. Taking into account symmetries at a subsystem level, the labels of the states of the "equivalent" system are generated. Next, these labels are divided into groups  $X(K)$  and  $Y(K)$



of operating and failed superstates, respectively. In addition, this program calculates the number of elements of the supertransition probability matrix that need be stored, and generates indices that show the starting point of each submatrix within the 1-dimensional array. A flow chart of this code is given in Figure B.1.

Program SSTAGEN-II generates (as in STAGEN) the set of  $Z$  of all possible states of the system and partitions it into subsets  $X(K)$  and  $Y(K)$ . Next, it generates all the possible labels  $L_y$  and lumps all the states of the original process with the same label into superstates. The mergeability of this partition is then checked by criterion (3.11), and if the latter is not satisfied, a new grouping is attempted and so on until a mergeable grouping is achieved. A flow chart of this code is given in Figure B.2.

Program MMARELA, using information generated by either version of SSTAGEN, generates the supertransition probability matrix.

A complete description of these codes, containing user's instructions, is presented in a BNL-NUREG report under the title: Computer Codes for Markovian Reliability Analysis.

# SSTAGEN-I

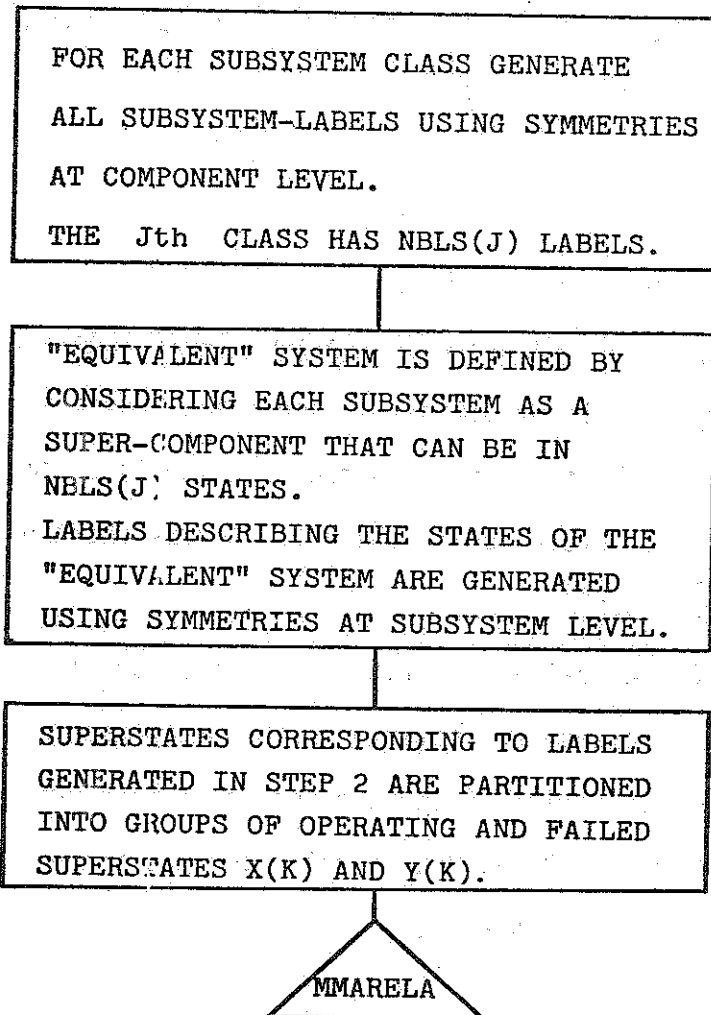


Figure B.1. Flow chart of program SSTAGEN-I.

## SSTAGEN-II

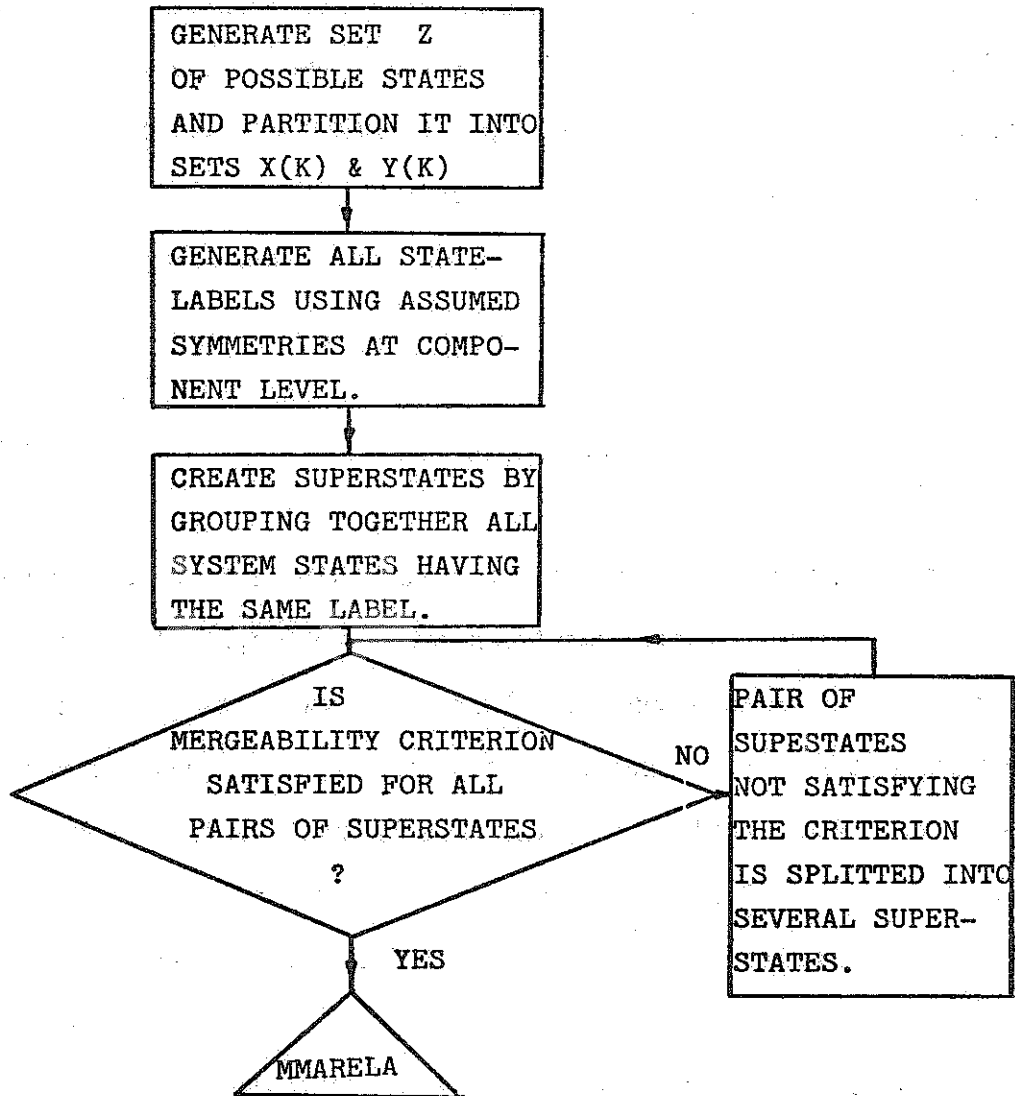


Figure B.2. Flow chart of program SSTAGEN-II.

## APPENDIX C

### Modification of MMARELA for Use in Monte Carlo Simulations

This Appendix contains a brief description of the modified version of MMARELA used in the Monte Carlo simulation. The objective of this modification is to minimize the necessary calculations for the generation of the transition probability matrix of each trial.

The transition probability between two superstates I and J is given by (3.19) or

$$p_{IJ}(n) = a_m^r \cdot h_{mk}^r(n|Iv)\Delta t, \quad (C.1)$$

where  $a_m^r$  is the number of components of class  $r$  that are in the component-state  $m$ , and  $h_{mk}^r(n|Iv)$  is the transition rate from component-state  $m$  to component-state  $k$  for components of class  $r$  at time  $n$ , given the state of the system at time  $n$ . Since the transition rates  $h$ 's have different values for each Monte Carlo trial, the same is true for the transition probabilities  $p_{IJ}$ 's. The values  $r, m, k$ , and  $a_m^r$  are, however, the same for all trials. On the basis of these observations, the following modifications were made in MMARELA.

An one-dimensional array  $TR(.)$  is created, the elements of which correspond to the various  $h_{mk}^r$ 's. Thus, if  $c$  denotes the number of component classes and  $s$  the maximum number of component-states the components of any class can be, index  $I$  defined by

$$I = c(r-1) + s(m-1) + k \quad (C.2)$$

is such that

$$TR(I) = h_{mk}^r \quad . \quad (C.3)$$

Then, instead of defining the transition probability matrix P, two matrices M and L are defined such that

$$m_{IJ} = a_m^r \quad (C.4)$$

and

$$1_{IJ} = I = c(r-1) + s(m-1) + k \quad . \quad (C.5)$$

As seen from (C.4) and (C.5), the elements of matrices M and L are functions of the variables c,s,r,m,k, and  $a_m^r$  only and, thus, need be defined only once. Then, at each trial, the array TR is redefined to contain the new values of h's and the value of  $p_{IJ}$  is given by (see also C.1, through C.5)

$$p_{IJ} = m_{IJ} \cdot TR(1_{IJ}) \quad . \quad (C.6)$$

In this way, only the one-dimensional array TR need be redefined with each trial. Furthermore, this redefinition does not involve comparison of superstates.

For nonmergeable processes, the  $a_m^r$ 's are always equal to unity and, therefore, matrix M is not needed.

REPORT DISTRIBUTION (In Addition to R-7)

Mr. Harry Alter, Chief (1)  
Safety Analysis Branch  
Division of Reactor Development  
and Demonstration  
Department of Energy  
Washington, D. C. 20545

Assistant Director for Reactor (1)  
Safety  
Division of Reactor Development  
and Demonstration  
Department of Energy  
Washington, D. C. 20545

Dr. Raymond Alcouffe (1)  
Los Alamos Scientific Laboratory  
Mail Stop 269  
P. O. Box 1663  
Los Alamos, N. M. 87545

Dr. Robert Avery, Director (2)  
Reactor Analysis & Safety  
Division  
Argonne National Laboratory  
9700 South Cass Ave.  
Argonne, Illinois 60439

Dr. L. W. Caffey, Director (1)  
CRBR Plant Project Office  
Department of Energy  
P. O. Box U  
Oak Ridge, Tennessee 37830

Central Mail & Files (1)  
U.S. NRC  
Public Document Room (LMFBR)  
Washington, D. C. 20555

Dr. R. Curtis, Chief (1)  
Analytical Advanced Reactor  
Safety Research Branch  
Division of Reactor Safety Research  
Nuclear Regulatory Commission  
Washington, D. C. 20555

Dr. William Davey (1)  
Q Division Leader  
Mail Stop 561  
Los Alamos Scientific Laboratory  
P. O. Box 1663  
Los Alamos, N. M. 87545

Dr. Carl A. Erdman (1)  
Department of Nuclear Engineering  
University of Virginia, Thornton Hall  
Charlottesville, Virginia 22901

Dr. R. Ferguson, Director (1)  
Fast Flux Test Facility Project Office  
Department of Energy  
P. O. Box 550  
Richland, Washington 99352

Mr. William P. Gammill, Assistant (1)  
Director for Standardization and  
Advanced Reactors  
Division of Project Management  
Nuclear Regulatory Commission  
Washington, D. C. 20555

Mrs. H. Gearin, Licensing (1)  
Assistant for Special Projects  
Division of Project Management  
Nuclear Regulatory Commission  
Washington, D. C. 20555

Mr. C. R. Hahn, Manager (1)  
Fuels Design and Development  
Pacific Northwest Laboratories  
P. O. Box 999  
Richland, Washington 99352

Dr. Stephen H. Hanauer (1)  
Technical Advisor  
Office of the Executive Director  
for Operations  
Nuclear Regulatory Commission  
Washington, D. C. 20555

Mr. K. Hikido, Manager (1)  
General Electric Company  
Systems Evaluation & Safety  
Engineering  
Fast Breeder Reactor Department  
310 DeGuigne Drive  
Sunnyvale, California 94086

Dr. Harry Hummel Applied Physics Division Argonne National Laboratory Building 208 9700 South Cass Avenue Argonne, Illinois 60439	(1)
Dr. William Kastenberg Department of Chemical Nuclear and Thermal Engineering University of California at Los Angeles Los Angeles, California 90024	(1)
Dr. C. N. Kelber, Assistant Director for Advanced Safety Research Division of Reactor Safety Research Nuclear Regulatory Commission Washington, D. C. 20555	(2)
Mr. Richard Lorenz Air/Ground Explosions Division Naval Surface Weapons Center White Oak Silver Spring, Maryland 20910	(1)
Dr. Roger J. Mattson, Director Division of Systems Safety Office of Nuclear Reactor Regulation Nuclear Regulatory Commission Washington, D. C. 20555	(1)
Dr. James F. Meyer Advanced Reactors Branch Division of Project Management Nuclear Regulatory Commission Washington, D. C. 20555	(15)
Professor F. J. Munno Nuclear Engineering Program Department of Chemical Engineering University of Maryland College Park, Maryland 20745	(1)
Dr. David Okrent Department of Chemical Nuclear and Thermal Engineering University of California at Los Angeles Los Angeles, California 90024	(1)



Mr. Frank E. Panisko, Senior (1)  
Development Engineer  
Fuels Design and Development  
Pacific Northwest Laboratories  
P. O. Box 999  
Richland, Washington 99352

Mr. D. F. Ross, Assistant Director (1)  
for Reactor Safety  
Division of Systems Safety  
Nuclear Regulatory Commission  
Washington, D. C. 20555

Dr. Arkal S. Shenoy, Manager (1)  
Systems & Safety Analysis  
Branch  
Gas Cooled Fast Breeder Reactor  
General Atomic Company  
P. O. Box 81608  
San Diego, California 92138

Mr. M. Silberberg, Chief (1)  
Experimental Fast Reactor  
Safety Research Branch  
Division of Reactor Safety Research  
Nuclear Regulatory Commission  
Washington, D. C. 20555

Mr. Daniel E. Simpson (1)  
Manager, Safety Engineering  
Hanford Engineering Development  
Laboratory  
P. O. Box 1970  
Richland, Washington 99352

Dr. Themis P. Speis, Chief (1)  
Advanced Reactors Branch  
Division of Project Management  
Nuclear Regulatory Commission  
Washington, D. C. 20555

Dr. Michael Stevenson (2)  
Los Alamos Scientific Laboratory  
P. O. Box 1663  
Los Alamos, N. M. 87545

Dr. David Swanson (1)  
Materials Sciences Laboratory  
Aerospace Corporation  
P. O. Box 92957  
Los Angeles, California 90009

Technical Information Center (1)  
Nuclear Regulatory Commission  
P. O. Box 62  
Oak Ridge, Tennessee 37830

Dr. Theo G. Theofanous (1)  
132 Pathway Lane  
Lafayette, Indiana 47906

Dr. J. V. Walker, Dept. Manager (1)  
Reactor Research and Development  
Sandia Laboratories  
P. O. Box 5800  
Albuquerque, New Mexico 87115

Secretary, Advisory Committee on (5)  
Reactor Safeguards  
Nuclear Regulatory Commission  
Washington, D. C. 20555

BNL Distribution

DNE Chairman (1)

RSP Associate Chairman (1)

RSP Division Heads & Group Leaders (18)

SEG/EARS Division (8)

BNL Reactor Safety Library (2)