Multi-State Reliability Analysis of Nuclear Power Plant Systems

by

Arun Veeramany

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Civil Engineering

Waterloo, Ontario, Canada, 2012

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

The probabilistic safety assessment of engineering systems involving high-consequence low-probability events is stochastic in nature due to uncertainties inherent in time to an event. The event could be a failure, repair, maintenance or degradation associated with system ageing. Accurate reliability prediction accounting for these uncertainties is a precursor to considerably good risk assessment model.

Stochastic Markov reliability models have been constructed to quantify basic events in a static fault tree analysis as part of the safety assessment process. The models assume that a system transits through various states and that the time spent in a state is statistically random. The system failure probability estimates of these models assuming constant transition rate are extensively utilized in the industry to obtain failure frequency of catastrophic events. An example is core damage frequency in a nuclear power plant where the initiating event is loss of cooling system. However, the assumption of constant state transition rates for analysis of safety critical systems is debatable due to the fact that these rates do not properly account for variability in the time to an event. An ill-consequence of such an assumption is conservative reliability prediction leading to addition of unnecessary redundancies in modified versions of prototype designs, excess spare inventory and an expensive maintenance policy with shorter maintenance intervals. The reason for this discrepancy is that a constant transition rate is always associated with an exponential distribution for the time spent in a state.

The subject matter of this thesis is to develop sophisticated mathematical models to improve predictive capabilities that accurately represent reliability of an engineering system. The generalization of the Markov process called the semi-Markov process is a well known stochastic process, yet it is not well explored in the reliability analysis of nuclear power plant systems. The continuous-time, discrete-state semi-Markov process model is a stochastic process model that describes the state transitions through a system of integral equations which can be solved using the trapezoidal rule. The primary objective is to determine the probability of being in each state. This process model ensures that time spent in the states can be represented by a suitable non-exponential distribution thus capturing the variability in the time to event. When exponential distribution is assumed for all the state transitions, the model reduces to the standard Markov model. The exponential distribution is characterized by memoryless property and hence is not able to distinguish between a newly installed system and a system that has already been in service. The primary rationale to move to semi-Markov process model is the ability to address this shortcoming in the Markov process model.

This thesis illustrates the proposed concepts using basic examples and then develops advanced case studies for nuclear cooling systems, piping systems, digital instrumentation and control (I&C) systems, fire modelling and system maintenance. The first case study on nuclear component cooling water system (NCCW) shows that the proposed technique can be used to solve a fault tree involving redundant repairable components to yield initiating event probability quantifying the loss of cooling system. The time-to-failure of the pump train is assumed to be a Weibull distribution and the resulting system failure probability is validated using a Monte Carlo simulation of the corresponding reliability block diagram. The main contribution showcased in this application is the ability to solve a multi-state system composed of repairable and non-repairable binary state components assuming non-exponential failure times. The only other closest tool that can handle this configuration is Monte Carlo simulation which requires intensive iterations and variance reduction techniques.

Nuclear piping systems develop flaws, leaks and ruptures due to various underlying damage mechanisms. This thesis presents a general model for evaluating rupture frequencies of such repairable piping systems. The proposed model is able to incorporate the effect of ageing related degradation of piping systems. Time dependent rupture frequencies are computed and the influence of inspection intervals on the piping rupture probability is investigated. The Markov process model is unable to assume non-exponential profile for flaw growth and probabilistic fracture mechanics (PFM) depend on intensive simulations. Hence, semi-Markov process is shown to be better suitable in the context of modelling piping system failures.

There is an increasing interest worldwide in the installation of digital instrumentation and control systems in nuclear power plants. The main feedwater valve (MFV) controller system is used for regulating the water level in a steam generator. An existing Markov model in the literature is extended to a semi-Markov model to accurately predict the controller system reliability. The proposed model considers variability in the time to output from the computer to the controller with intrinsic software and mechanical failures. Safety critical systems are passive systems in the sense that these are called on demand for a short mission time to mitigate catastrophes. Hence mission unreliability is a prominent reliability index to be determined in order to evaluate the safety effectiveness of these systems. The mission unreliability measure is different from system failure probability in that it takes in to consideration how long the system has already been in service before the system is susceptible to failure with in the mission time. It is proved in this case study that semi-Markov process model is able to effectively differentiate both the indices while Markov process model fails to do so due to memoryless property of exponential distributions.

State-of-the-art time-to-flashover fire models used in the nuclear industry are either based on conservative analytical equations or computationally intensive simulation models. The proposed semi-Markov based case study describes an innovative fire growth model that allows prediction of fire development and containment including time to flashover. The model considers variability in time when transiting from one stage of the fire to the other. The proposed model is a reusable framework that can be of importance to product design engineers and fire safety regulators.

Operational unavailability is at risk of being over-estimated because of assuming a constant degradation rate in a slowly ageing system. In the last case study, it is justified that variability in time to degradation has a remarkable effect on the choice of an effective maintenance policy. The proposed model is able to accurately predict the optimal maintenance interval assuming a non-exponential time to degradation. Further, the model reduces to a binary state Markov model equivalent to a classic probabilistic risk assessment model if the degradation and maintenance states are eliminated.

In summary, variability in time to an event is not properly captured in existing Markov type reliability models though they are stochastic and account for uncertainties. Secondly, the memoryless property of exponential distribution is a hindrance in modelling failure of ageing systems. The proposed semi-Markov process models are easy to implement, faster than intensive simulations and accurately model the reliability of engineering systems.

Acknowledgements

The completion of this thesis has been a significant challenge in itself apart from the research work. I would like to express my sincere gratitude to the following people without whose support, patience and guidance, this task would not be completed successfully.

- Prof. Mahesh Pandey for being my supervisor. His thoroughness of fundamentals and clear insights in to the advanced topics have left me awe-inspiring and motivated for rest of my professional career. I express my special thanks to him for providing me an opportunity to be a graduate student with consistent financial support through out the program.

- Dr. Sriram Narasimhan for the opportunity to work with him on wireless sensor networks. His project helped me provide a swift transition from the abstract mathematical sciences to the more practical engineering arena. Volunteering for seismic data extraction for one of his projects mid-way rejuvenated me to keep going ahead with my research work.

- My committee members. Their suggestions and comments during the comprehensive exam gave me a big boost to choose supporting topics and incorporate those ideas in to my thesis work.

- Madhusudan Chalasani without whose push and constant inspiration I would not even have thought of joining a master's program, let alone completing this Ph.D. dissertation.

- Suresh Verma Datla and Anup Sahoo. They were my special consultants. Discussions with them helped me come out of mental blocks and helped me to keep going ahead without imaginary dead-ends.

- Shoba and Ravi. I am largely indebted for their moral support in helping me choose my best life partner and subsequently helping me lead a smooth and married student life.

- My friends Sunil Kumar Nimmagadda, Srinivas Reddy Gangam, Sumanth Kumar Ananthula, Srikanth Vemradhi, Praveen Mynam, Krishnam Raju Jampani, Satya Prakash Ponnaluri, Murthy Ganti, Feng Ming (Raymond), Dongen Zhou (Sunny) and colleagues Pradeep Ramchandani, Budhaditya Hazra, Ayan Sadhu, Dongliang Lu, Tianjin Cheng, Shun Hao Ni, Xufang Zhang and others whom I would simply give a phone call during ups and downs of graduate life.

- My sister and brother-in-law kept reminding me every now and then how happy they felt having someone in their family doing research work.

- Abderrazzaq Bounagui and Grant Cherkas at the Canadian Nuclear Safety Commission (CNSC), Ottawa for providing me an opportunity to work for the Canadian Nuclear Regulator. The idea of pursuing the fire growth model stemmed from this summer student experience.

- Prof. Beth Weckman at the Department of Mechanical Engineering, University of Waterloo provided the most needed academic thrust to ensure completion of the fire model.

- Srikanth Mangalam, Director, Technical Standards and Safety Authority (TSSA), Toronto for providing me an opportunity to work for TSSA as a Public Safety Risk Advisor. This timely opportunity allowed me to concentrate stress-free on my thesis. Special thanks to my colleagues Lency Mulamootil, Jorge Larez, Dwight Reid, Supraja Sridharan, Cole Lepine and Elvina Chow.

- My wife Sai Gaayathri who accompanied me on long hikes, sky dives, bungee venues, kayaking, wilderness camping and much more. All along, she proved to be my best companion until my Ph.D. and forever.

Dedication

This dissertation is dedicated to my parents, in-laws and my wife.

Contents

List of Tables

List of Figures

List of Abbreviations

LCM	Life Cycle Management
SSC	System, Structure, and Component
NPP	Nuclear Power Plant
CANDU	CANada Deuterium Uranium
EPRI	Electric Power Research Institute
PSA	Probabilistic Safety Assessment
FTA	Fault Tree Analysis
RAM	Reliability, Availability, Maintainability
NCCW	Nuclear Component Cooling Water
HTS	Heat Transport System
SDS1	ShutDown System number one
HMP	Homogeneous Markov Process
SMP	Semi-Markov Process
SMC	Semi-Markov Chain
DTSMP	Discrete-Time Semi-Markov Process
MRE	Markov Renewal Equation
CTMRE	Continuous Time Markov Renewal Equation
UGF	Universal Generating Function
CCF	Common Cause Failure
RBD	Reliability Block Diagram
MTTF	Mean Time To Failure
MTTFF	Mean Time To First Failure
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
GA	Genetic Algorithm
MSS	Multi-State System

pdf	Probability Density Function
pmf	Probability Mass Function
cdf	Cumulative Distribution Function
mgf	Moment Generating Function
pgf	Probability Generating Function
cov	Coefficient of Variation
$r.v.$	Random Variable

List of Symbols

γ_{ij}	Shape parameter of Weibull distribution for the transition from state i to state j
$\hat{Q}$	Statistical estimate of unavailability
λ	Constant failure rate, mean time to failure λ^{-1}
$\lambda(t)$	Hazard rate function of a non-repairable system with possibly repairable subsystem
λ_c	Failure rate due to a common cause failure
λ_{ij}	Failure rate at (i, j) of the Markov transition rate matrix
μ	Constant repair rate, mean time to repair μ^{-1}
$\overline{\tau}_j$	Mean time spent in state j
$\phi(\mathbf{x})$	Structure function of a system represented by a vector $\mathbf{x}$ of component states
$\phi_{ij}(t)$	Probability that process spends time t in state i before jumping to state j
π_j	Steady state probability of being in state j
$\widetilde{p}(s)$	Laplace transform of $p(t)$
$A(t)$	Time dependent availability
$C(t)$	Kernel matrix of the semi-Markov process
$c_{ij}(t)$	$(i, j)th$ entry of the kernel matrix
$diag(W(t))$	Diagonal matrix formed by the entries of the column vector $W(t)$
$E[X]$	Expectation of the random variable X
$f_T(t)$	Density function of the time-to-failure random variable T
$g_T(t)$	Density function of the time-to-repair random variable T

$P\Box H$	Element by element product of elements of matrices P and H
$P(E)$	Probability of event E
$p_i(t)$	Probability of being in state i at time t
p_{ij}	Probability that transition from state i to state j occurs
$Q(t)$	Time dependent Unavailability or unreliability
$R(t)$	Time dependent reliability
S_n	Time until the nth failure
$u(z)$	u-function of a component with random variable z denoting its state or performance
$V[X]$	Variance of the random variable X
$W_i(t)$	Probability that process does not stay beyond t time units in state i
$w_i(t)$	The unconditional probability that process waits for t time units in state i
$X(t)$	State of the process at time t

Chapter 1

Introduction

1.1 Engineering Reliability and Nuclear Power Applications

A key objective of Life Cycle Management (LCM) is the development of a complete life cycle approach for the maintenance and ageing management of systems, structures, and components (SSCs) important to plant operation and safety. To reduce the probability of system failures that can render a safety system unavailable, plant operators often take the approach of periodic inspections and repair if anything is found wrong.

The Canadian nuclear regulator states that though nuclear power plants were highly reliable in the early years, they had to be increasingly taken offline later to counter the effects of degradation and subsequently had to be shut down for refurbishment five to fifteen years earlier than the expected design life (Blahoianu et al., 2011). Calling for frequent inspections that require the system to be taken offline is clearly not an optimal approach from a cost viewpoint, especially if predictions of failure can be improved. As a result, there is an increasing interest in probabilistic methods to model several forms of material degradation such as flow-accelerated corrosion, delayed-hydride cracking and stress-corrosion cracking for optimizing in-service inspection programs (Fleming, 2004; Blahoianu et al., 2011).

The wide acceptance of risk-informed decision making approaches for managing safety critical infrastructure (Kafka, 2008) coupled with the availability of in-service operating experience in the form of databases is resourceful in advancing the sophistication of probabilistic models to accurately predict system reliability.

Many authors have expressed the need to go beyond conservative approaches and develop advanced models to account for dynamic behaviour (account for time dependence) and complex interactions (*e.g.*, hardware-software) among system components (Aldemir et al., 2007; Boudali et al., 2007; Rao et al., 2009; Distefano and Puliafito, 2009; Brissaud et al., 2011). Though there has been introduction of new formalisms to represent dynamic dependence through dynamic fault trees (DFT), dynamic reliability block diagrams (DRBD), binary decision diagrams (BDD), dynamic flowgraph methodology (DFM) and stochastic petri nets, the primary way of quantifying the models has been simulation(Rao et al., 2009; Ibáñez-Llano et al., 2010; Chiacchio et al., 2011; Al-Dabbagh and Lu, 2010; Škňouřilová and Briš, 2008). The key objective of this thesis is to develop advanced stochastic models that bypass the need for simulation and improve time-dependent reliability of engineering systems while taking in to account the susceptible nature of systems to ageing related damage mechanisms. With this motivation, the next section gives an overview of stochastic processes.

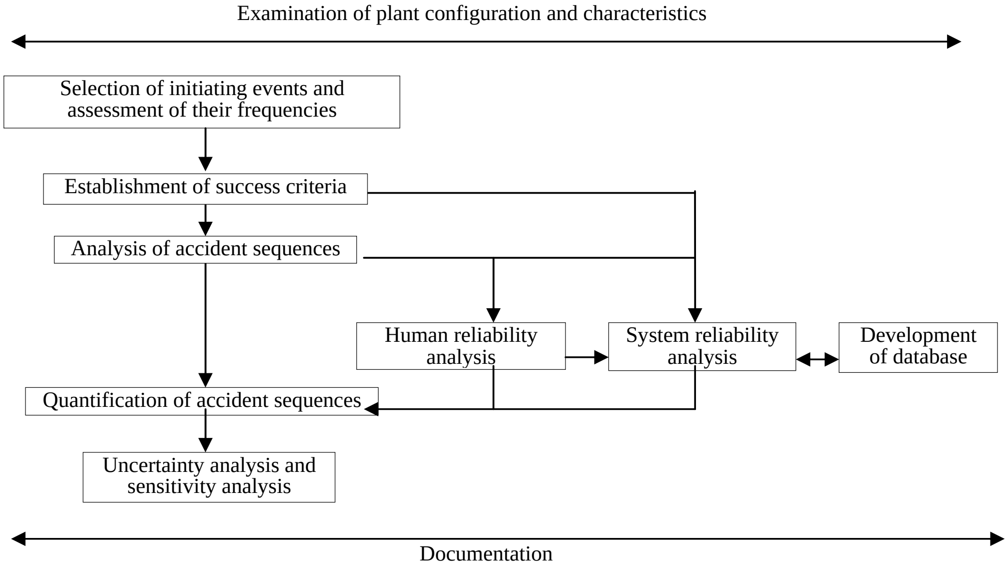

Examination of plant configuration and characteristics
Selection of initiating events and assessment of their frequencies
Establishment of success criteria
Analysis of accident sequences
Human reliability analysis
System reliability analysis
Development of database
Quantification of accident sequences
Uncertainty analysis and sensitivity analysis
Documentation

Figure 1.1: System reliability analysis in PSA Level 1 Workflow(JNES, 2011)

The Probabilistic Safety Assessment (PSA) is a comprehensive methodology to (a) identify event combinations that could potentially lead to severe accidents (b) determine the probability of occurrence of each event combination and (c) assess the consequences. The US Nuclear Regulatory Commission (USNRC) initially coined and continues to use the term Probabilistic Risk Assessment (PRA) whereas the term PSA is used in the international nuclear community. In other fields Quantitative Risk Assessment (QRA) is in widespread use (Garrick and Christie, 2008).

Level 1 PSA analyzes contribution of system reliability to frequency of core damage (Figure 1.1), Level 2 PSA determines the frequency of radioactive release and Level 3 PSA estimates risk to public and the environment. The terms reliability, availability and safety should not be confused. Safety deals with consequences of system failure. A reliable system may not be safe and a safe system may not be reliable (Leveson, 2011). Reliability is used in the context of non-repairable systems or systems whose first failure after installation or repair completion is of importance whereas availability is defined for repairable systems. When there is no repair involved in the system, availability reduces to reliability and the steady-state availability represents the long-run performance of a repairable system.

1.2 Introduction to Stochastic Processes

The states of a system are characterized by a continuous-time stochastic process denoted by $\{X(t), t \geq 0\}$, a sequence of random variables which take a set of values in a set S, called the state space of the stochastic process. For example, $X(t)$ may represent one of the states S={working=3, minor repair=2, major repair=1} of a repairable system at time t. The aim of the study of stochastic processes is to characterize the statistical behaviour of the system and hence to predict the future of the system. A *sample path* is a record of how a process evolved in one particular instance. A typical sample path of a continuous-time, discrete space stochastic process is shown in Figure 1.2. The set of all possible sample paths of a stochastic process is called the *sample space* of the stochastic process. The following are the most common and important stochastic processes:

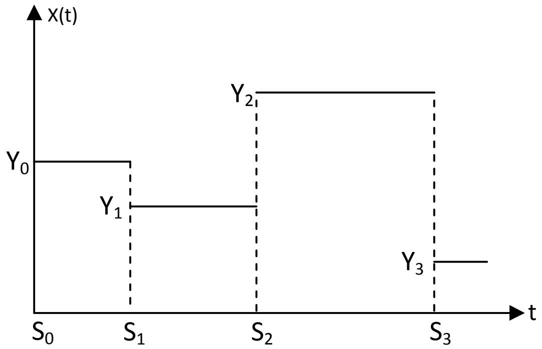


Figure 1.2: A typical sample path of a continuous-time, discrete space stochastic process

1. **Markov Processes** Consider the time points $0 \leq t_0 < t_1 < ... < t_n < t_{n+1}$ and the corresponding states $i_0, i_1, ...i_{n+1}$ the process was in. Then, the Markov property is given by:

$$\begin{aligned} &P(X(t_{n+1}) = i_{n+1}|X(t_n) = i_n, X(t_{n-1}) = i_{n-1}, ..., X(t_0) = i_0) \\ &= P(X(t_{n+1}) = i_{n+1}|X(t_n) = i_n) \end{aligned} \tag{1.1}$$

   i.e. the conditional transition probability distribution of future states of the process, given the present state and all past states, depends only upon the present state and not on any past states. Such a stochastic process $X(t)$ satisfying the Markov property is said to be a Markov process. If these transition probabilities do not change over time, then the process is the time-homogeneous Markov process:

$$Pr\{X(t+s) = j|X(s) = i\} = P\{X(t) = j|X(0) = i\} \tag{1.2}$$

   Markov process model is a stochastic state-space based approach to solving system reliability problems(Dhillon and Yang, March 1997; Xing et al., 1996). This technique takes all possible system dynamics in to consideration and also offers flexibility of evaluating system reliability as well as availability of repairable systems. However, it suffers from state explosion *i.e.*, as the number of system components and their failure modes increase, there is an exponential increase in system states, making the resulting reliability model more difficult to analyze (Pukite and Pukite, 1998). For example, if the system consists of n different components, then the resulting number of system states is 2^n. Thus, even for a relatively simple system, the resulting Markov model may contain an extremely large number of states. Researchers sought approximation methods like state merging and lumping to contain the problem(Xing et al., 1996). The Markov process model assumes that failure and repair time distributions always follow an exponential distribution which is associated with constant state transition rates. The method has found a class of applications that model ageing related degradation phenomena to support risk-informed decision making programs(Fleming, 2004; Vesely, 1993).

2. **Poisson Processes** The stochastic process $N(t) = N(0, t)$ representing the number of events in the interval (0,t) having a Poisson distribution with parameter λ as the mean occurrence rate of the events is called a Poisson

process. Poisson process is a point process given by:

$$P(N(t) = n) = e^{-\lambda t}\frac{(\lambda t)^n}{n!} \tag{1.3}$$

For example, $N(t)$ may represent the number of failed machines at time t.

3. **Renewal Processes** If the interval between the point events (example: two failure events) are independent and identically distributed random variables, the process formed by the sequence of these random variables $X(t) = \{x = t_1, x = t_2 - t_1, ...\}$ is called a renewal process. The name renewal process is motivated by the fact that every time there is an occurrence the process starts all over again. This kind of process can be used to model a sequence of failures of a machine in continuous time.

   An alternating renewal process consists of two types of independent and identically distributed random variables alternating with each other. This process is proved to be amenable to repairable systems, with one distribution for successful operation and the other for periods of repair. Since the process does not restrict itself to one particular distribution, this process is a generalization of the Poisson process.

   A complex engineering system composed of components can be graphically represented as a Reliability Block Diagram (RBD) and quantitatively evaluated based on probability rules. When all the components are repairable, the alternating renewal process (Birolini, 2007) emerged as a powerful tool in dealing with system risk and reliability analysis. Its application to infrastructure asset management was explored by Pandey et al. (2008). In this stochastic method, each component is assumed to alternate between failures and repairs. Time-to-failure and time-to-repair are treated as independent random variables following arbitrary distributions. Availability results of the components based on this theory are integrated at the system level using probability rules. Since each component is individually assessed, this method does not take in to consideration all the collective dynamics that a system undergoes during its life-span. Apart from alternating between failures and repairs, a component may go through gradual degradation. It may not fail only due to sudden random occurrence. In such a case other state-space based process models are preferred.

4. **Semi-Markov Processes** A sequence of bivariate random variables $\{(Y_n, S_n), n \geq$

0} is called a *Markov renewal sequence* (Kulkarni, 1995) if:

(a) $S_0 = 0, S_{n+1} \geq S_n; Y_n \in \{0, 1, 2, ...\}$, and

(b) for all $n \geq 0$,

$$\begin{aligned} &P\{Y_{n+1} = j, S_{n+1} - S_n \leq x | Y_n = i, S_n, Y_{n-1}, S_{n-1}, ..., Y_0, S_0\} \\ &= P\{Y_{n+1} = j, S_{n+1} - S_n \leq x | Y_n = i\} \\ &= P\{Y_1 = j, S_1 \leq x | Y_0 = i\} \end{aligned} \tag{1.4}$$

where the system is being observed at times $S_0 = 0, S_1, S_2, ...$ etc. and Y_n is the observation (state) at time S_n.

In addition to the time-homogeneous Markov property, the Markov renewal sequence also emphasizes on the time spent in the state.

A continuous-time stochastic process {X(t), $t \geq 0$} with countable state-space S is said to be a *semi-Markov process* if

(a) it has piecewise constant, right continuous sample paths, and

(b) $\{(Y_n, S_n), n \geq 0\}$ is a Markov renewal sequence, where $Y_n = X(S_n+)$

A semi-Markov process reduces to an alternating renewal process when the number of states is limited to two and reduces to a renewal process when there is only one state in the semi-Markov model. Semi-Markov process model is based on Markov Renewal theory and brings together the features of renewal theory and Markov chains *i.e.*, this technique derives the possibility of assuming arbitrary distributions for transition time from renewal theory and the ability to think beyond binary states from Markov process model. This method also inherits the penalties of both the parent techniques. Renewal method is based on solving a system of integral equations involving computationally resource intensive convolution operations. From the Markov process model, the semi-Markov approach inherits the state explosion problem.

5. **Markov Renewal Processes** The Markov renewal processes (MRP) are equivalent to semi-Markov process (SMP) (Nakagawa and Osaki, 1976) allowing finitely many states in the model with arbitrary waiting time distributions. While the objective of the latter is to determine the probability of being in a state, the former yields the expected number of visits to a state

(Birolini, 2007):

$$N_i(t) = \text{number of transitions in state } Z_i \text{ during } (0, t] \tag{1.5}$$

An application of this process model is to determine the expected number of visits to the system failure state in a repairable system(Nakagawa and Osaki, 1975a).

1.3 Research objectives

The objectives of the thesis are:

1. Formulate Markov and semi-Markov process models for system reliability analysis

2. Compare the Markov process model with fault tree method for system reliability analysis

3. Develop the idea of modularized semi-Markov models to eliminate state explosion using generating function and simple probability rules.

4. Validate results of the proposed semi-Markov process models using Monte-Carlo reliability block diagram and process simulations whichever appropriate in the context.

5. Apply the previously developed ideas to practical case studies.

1.4 Thesis organization

The thesis is divided in to seven chapters including the present chapter. Chapter 2 reviews the Markov process model to obtain time-dependent and steady state system reliability. Techniques to determine transition rates using event data and Bayesian techniques is discussed. Further, the Markov reward model is reviewed to derive mean number of failures and the mean time to failure. This chapter introduces the Nuclear Component Cooling Water (NCCW) system and models its shutdown initiating event frequency using fault tree analysis. This chapter analyzes the NCCW problem from a Markovian perspective.

In chapter 3, semi-Markov process model is presented as an extension to Markov process model. After literature review specific to this chapter, semi-Markov process is compared to the Markov process. This is followed by model formulation and computation of the reliability indices. Partial closed form solutions are derived when holding time is assumed to be Weibull distributed. While appreciating the idea of non-exponential holding times, practical difficulties in dealing with multiple failures and large systems is discussed. Methods of finding steady state solution and simulation of the process are discussed. For downsizing the models, state reduction technique is introduced. In quest for faster computational techniques, discrete time version of the semi-Markov process model is explored.

Case studies on various systems are dealt in Chapter 4.

Chapter 5 on Monte-Carlo simulation of reliability block diagrams aids as a tool for validating semi-Markov process models. Detailed pseudo-codes are presented to deal with repairable and non-repairable systems. A typical block diagram and the NCCW system reliability models are revisited to validate the models developed in the earlier chapter. Practical difficulties in using simulation techniques for multi-state systems are discussed.

Chapter 6 describes Universal Generating Function (UGF) method. UGF is considered in this thesis as a rescue tool to work around the well known 'state explosion' problem associated with Markov and semi-Markov processes. An example allows the reader to appreciate its flexibility and ease of use. The chapter ends with comments on the use of this technique for general multi-state systems as compared to the network reliability method. The semi-Markov and UGF tool is applied to the Heat Transport System (HTS) in a Nuclear Power Plant (NPP) to highlight the fact that this combination is instrumental in modeling practical reliability problems.

Chapter 7 concludes with a summary of research contributions and recommendations for future studies.

Appendix A covers a trapezoidal rule based algorithm to solve the system of integral equations to compute the interval transition probabilities discussed in chapter 3. Appendix B tabulates the relation between the coefficient of variation and the Weibull shape parameter. The appendix includes a glossary of technical terms used in this thesis.

Chapter 2

Markov Processes

2.1 Introduction

The two main concepts in the Markov process model are system states and state transitions. The state of a system represents a specific combination of system parameters that describe the system at any given instant of time. The state transitions govern the changes of a state that occur within a system. As time passes and failures occur, the system goes from one state to another until one of the absorbing states (usually the system failure states, if any) is reached. The state transitions are characterized by parameters such as failure rates and repair rates. Solving a Markov model consists of solving a set of differential equations, typically using Laplace transform or numerically using a variable step Runge-Kutta method. The solution includes the probability of the system being in each state and the system unreliability can be calculated by adding the probability of being in each failure state.

2.2 Literature Review

The class of Markov chains with a denumerable number of states modelled as an infinite system of stochastic differential equations called the *Kolmogorov differential equations* was first considered by Kolmogoroff (1931) in his fundamental paper on this subject. Feller (1937) formulated the more general integro-differential equations also called the forward and backward equations describing the Markov processes in continuous time and discrete space. The time-homogeneous or stationary properties of the Markov transition probabilities were laid out by Lévy (1951). A comprehensive discussion of the analytical properties of the transition probabilities can be found in Kolmogorov (1951); Austin (1956); Kendall (1955).

Billinton and Bollinger (1968) discussed and illustrated the basic concepts of stationary Markov processes and particularly their application to transmission system reliability evaluation. Transmission components were assumed to operate within a 2-state fluctuating environment described by normal and stormy weather conditions.

A Markov process model for the growth of maximum pit depth in oil and gas pipelines was discussed by Provan and Rodriguez (1989). Xing et al. (1996) made comparison between Markov and fault tree models for determining support system failure initiating event frequency in a nuclear power plant, for both power and shutdown conditions. Further, they developed a correlation to estimate the ratio between initiator frequencies through both approaches for a two parallel component system. Bharucha-Reid (1997) gave a formal nonmeasure-theoretic treatment to Markov processes with main emphasis on applications.

Bloch-Mercier (2001) considered a repairable Markov system such that different completeness degrees are possible for the repair (or corrective maintenance) that go from a minimal up to a complete repair. They observed that the optimal restarting distribution is generally random and does not correspond to a new start in a fixed up-state. Vinod et al. (2003) incorporated the effects of degradation mechanism and maintenance activities by a Markov model as an efficient method for realistic analysis. Ajah et al. (2006) developed a multi-state reliability model of a proton exchange membrane (PEM) fuel cell power plant via Markov process. Cho and Jiang (2008) developed a Markov process model to study the effect of test interval in the shutdown system number one (SDS1) of a CANDU plant. Representing the state transitions in the SDS1 by a time-homogeneous Markov process, their model can be used to quantify the effect of surveillance test durations and interval on the unavailability and the spurious trip probability.

2.3 Formulation of the Markov process

Consider a system whose states i=1,2,...k are observed at times $t \geq 0$. The system stays in state i for a random amount of time that is exponentially distributed with a parameter a_{ij} called the transition intensity and then moves to state j. The time spent in state i and the jump to next state depend only on the state i and not on the history of the system prior to time t. The Markov process is based on this fundamental property called the "'Markov property"' as defined in (1.1)

While (1.1) represents a conditional probability, let $p_i(t)$ be the unconditional probability of the process being in state i. $p_i(t)$ is called the state probability of X(t) at time t:

$$p_i(t) = Pr\{X(t) = i\}, i = 1, ..., k; t \geq 0. \tag{2.1}$$

$$\text{such that } \sum_{i=1}^{k} p_i(t) = 1 \tag{2.2}$$

2.4 Determining state probabilities

The goal of Markov process is to determine the state probabilities of a stochastic process following the Markov property. The rate of change of any state probability of an arbitrary state j is equal to sum of the state probabilities of incoming transitions in to state j multiplied by the corresponding transition intensities minus the state probability of state j multiplied by the sum of transition intensities of all outgoing transitions from state j:

$$\frac{dp_j(t)}{dt} = [\sum_{\substack{i=1 \\ i \neq j}}^{k} p_i(t) a_{ij}] - p_j(t) \sum_{\substack{i=1 \\ i \neq j}}^{k} a_{ji} \tag{2.3}$$

It is assumed that the system starts in the best state k and therefore, the initial conditions are $p_k(0) = 1, p_{k-1}(0) = p_{k-2}(0) = ...p_1(0) = 0$. If the state transitions are caused due to failures and repairs of the system, then the transition intensities are given by the corresponding failure and repair rates.

Compactly, the system of linear differential equations (2.3) can be written in the matrix form as:

$$\frac{d\mathbf{P}(t)}{dt} = \mathbf{P}(t)\mathbf{A} \tag{2.4}$$

where

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1k} \\ a_{21} & a_{22} & ... & a_{2k} \\ & & ... & \\ a_{k1} & a_{k2} & ... & a_{kk} \end{bmatrix} \tag{2.5}$$

$$\text{such that } a_{jj} = -\sum_{\substack{i=1 \\ i \neq j}}^{k} a_{ji} \text{ and}$$

$$\mathbf{P}(t) = [p_1(t), p_2(t), ..., p_k(t)]$$

2.4.1 Solutions of the system of differential equations

The system (2.3) can be solved numerically using an algorithm like variable step Rungekutta method or can be solved analytically using the Laplace-Stieljes transform. An example is given below to illustrate the solution method.

Consider a two state non-repairable system with a constant failure rate λ. Assume that the system initially starts in state 2, the functioning state. Then the transition intensity matrix based on (2.5) is written as:

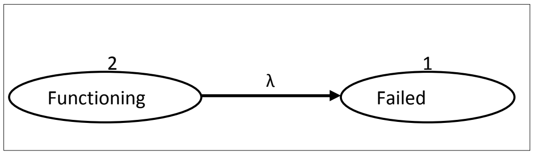


Figure 2.1: 2-state non-repairable system with a constant failure rate λ=0.5

$$\begin{bmatrix} 0 & 0 \\ \lambda & -\lambda \end{bmatrix}$$

The system of differential equations are formulated as per (2.3):

$$\begin{aligned} \frac{dp_1(t)}{dt} &= \lambda p_2(t) \\ \frac{dp_2(t)}{dt} &= -\lambda p_2(t) \\ p_1(t) + p_2(t) = 1 \text{ and} & \\ p_1(0) = 0, p_2(0) = 1 & \end{aligned}$$

The Laplace transform is given as:

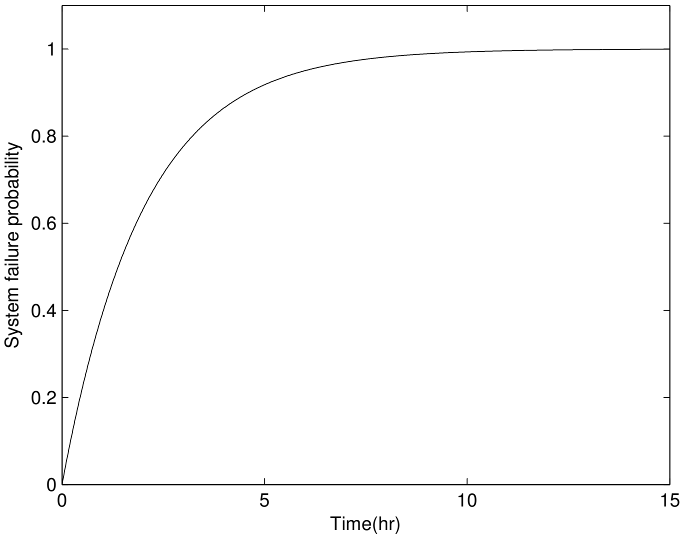


Figure 2.2: System failure probability of 2-state non-repairable system with $\lambda = 0.5$

$$
\begin{aligned}
s\widetilde{p_1}(s) - p_1(0) &= \lambda \widetilde{p_2}(s) \\
s\widetilde{p_2}(s) - p_2(0) &= -\lambda \widetilde{p_2}(s)
\end{aligned}
$$

Solving for $\widetilde{p_1}(s)$:

$$\widetilde{p_1}(s) = \frac{1}{s(\frac{s}{\lambda}+1)} = \frac{1}{s} - \frac{1}{\lambda(\frac{s}{\lambda}+1)}$$

The inverse Laplace transform gives:

$$p_1(t) = 1 - exp(-\lambda t) \tag{2.6}$$

$$p_2(t) = exp(-\lambda t) \tag{2.7}$$

$p_1(t)$ corresponds to system failure probability given that the system initially started in state 2, the functioning state. $p_2(t)$ represents systems reliability.

2.5 Asymptotic solution

Theoretically, the steady-state probabilities are the state probabilities as time approaches infinity. The sum of all steady-state probabilities corresponding to the working states represents steady-state availability or long-run availability. Note that it is inappropriate to term steady state reliability, because a non-repairable system is never reliable in a long run.

A Markov process is said to be *irreducible* if every state of the process can be reached from any other state (Ross, 1992). It is always possible to compute the steady state probabilities for an irreducible Markov process.

i.e., it can be shown that the time-dependent state probabilities approach a definite value:

$$\lim_{t \to \infty} p_j(t) = p_j \tag{2.8}$$

Alternatively, a definite value is reached when the derivative of $p_j(t)$ is zero as $t \to \infty$. This definition can be used to rewrite Equation (2.4):

$$\mathbf{0} = \mathbf{PA} \tag{2.9}$$

where $P = [p_1, p_2, ..., p_k]$ along with the constraint that $\sum\limits_{i=1}^{k} p_i = 1$

Note that there are $k+1$ system of equations along with the constraint and there are k unknowns. Hence, any k of these equations with the constraint included is sufficient to solve this system to obtain all the steady state probabilities.

2.6 Transition rate estimation

Transition rates of a Markov model can be estimated based on failure data available at hand. This section discusses three different ways for this task.

2.6.1 Point estimate

This method is valid when count of failure events is available. The estimate $\widehat{\lambda}$ is based on the number of failures n observed in a sample of size N over a period of time T:

$$\widehat{\lambda} = \frac{n}{NT} \tag{2.10}$$

Table 2.1: Sample data for transition rate estimation

Event Type	Inspected	Event Count
Flaws from normal state	2000	8
Leaks from flaw state	3000	4
Ruptures from leak state	5500	3

For example, consider a piping model with four states - normal, flaw, leak and rupture. Table 2.1 shows sample event count data gathered over 10 years. The first row gives the count of flaws observed in the pipe given that the pipe was in normal state when earlier observed *i.e.*, 2000 normal pipe elements were inspected and 8 of them were found to develop flaws. Therefore, an estimate of flaw occurrence rate is $\widehat{\lambda} = 8/(2000 * 10) = 4e - 3$ per year. Hence in the context of Markov modelling, the analyst needs conditional failure data.

The estimate thus found reflects quality of the sample population only. The sample might be from a particular plant site. Given the rarity of the events and inadequate data collection, these estimates could often be misleading.

2.6.2 Estimation using Bayesian method

In Bayesian inference (Kelly and Smith, 2009), plant specific failure data from the above section is combined with known failure rates from other sources. These external failure rates from world-wide plants could be averaged and used as prior knowledge. The source could also be based on engineering judgment or expert opinion. Advantage of this approach is that uncertainty factor can be introduced by considering the failure rate as a random variable following a valid statistical distribution. This distribution $\pi(\lambda)$ is called "prior distribution" in Bayes' terminology because it reflects prior knowledge of the failure rates. For example, failure rate of a component pooled from other plants could follow a gamma distribution corresponding to a mean failure rate of 10^{-6} and standard deviation of 0.0001.

It can be assumed that the plant specific data are likely to occur from a different distribution having the failure rate as a distribution parameter. This is represented by the 'likelihood function' $f(x|\lambda)$ and it can take in to account complete, interval, left and right censored data. Note that this 'failure rate' is the random variable in the prior distribution.

The normalized product of likelihood function and the prior distribution yields an updated failure rate in the form of a distribution. This is called the "posterior distribution" $\pi_1(\lambda)$ in Bayes's methodology:

$$\pi_{post} \propto likelihood(x|\lambda)\pi_{prior}(\lambda)$$
$$\Longrightarrow \pi_1(\lambda|x) = \frac{f(x|\lambda)\pi(\lambda)}{\int f(x|\lambda)\pi(\lambda)d\lambda} \tag{2.11}$$

The denominator in Equation 2.11 is a normalizing constant and is called the marginal or unconditional distribution of x often denoted by $f(x)$.

For example, let the following failure rates per year be observed from different plants: $3e-3, 6e-4, 5e-5$. Mean and standard deviation of this data are $\mu = 1.22e-3$ per year and $\sigma = 1.57e-3$ respectively. The corresponding gamma distribution parameters are $\alpha = 0.604$ and $\beta = 495$ component years by assuming the following characteristics for the gamma distribution:

$$f_{pdf}(\lambda|\alpha,\beta) = \frac{\beta^{\alpha}}{\Gamma(\alpha)}\lambda^{\alpha-1}e^{-\beta\lambda} \tag{2.12}$$
$$Mean = \frac{\alpha}{\beta} \tag{2.13}$$
$$Variance = \frac{\alpha}{\beta^2} \tag{2.14}$$

If Poisson data is supplied, α represents the number of failure events and β represents the period of time over which these failures were observed.

Let the observed plant data be $x = 8$ failures out of 200 components inspected over 10 years *i.e.*, $t = (200)(10) = 2000$ component-years. The likelihood function for this data assuming a Poisson distribution is:

$$Pr(X = x|\lambda) = \frac{e^{-\lambda t}(\lambda t)^x}{x!} \tag{2.15}$$

In this context, the denominator of Equation 2.11 denotes the probability of observing x failures independent of the failure rate λ.

Then from Equation 2.11,

$$\pi_1(\lambda|x) \propto e^{-\lambda t}(\lambda t)^x \lambda^{\alpha-1}e^{-\beta\lambda}$$
$$\propto \lambda^{(\alpha-1)+x}e^{-\lambda(t+\beta)} \tag{2.16}$$

i.e., the posterior distribution is also a gamma distribution such that

$$\begin{aligned} \alpha_{post} &= x + \alpha_{prior} \\ \beta_{post} &= t + \beta_{prior} \end{aligned} \tag{2.17}$$

In the example considered, $\alpha_{post} = 8 + 0.604 = 8.604$ and $\beta_{post} = 2000 + 495 = 2495$ *i.e.*, based on the plant data, failure rate of the component can be updated as $\Gamma(8.604, 2494)$ which represents a mean failure rate of 3.44e-3 while the prior failure rate was 1.22e-3.

The failure rate thus obtained can be utilized as a transition rate in a Markov model. The failure frequency (hazard rate) obtained from Markov model can be used in a fault tree as part of a Probabilistic Safety Assessment (PSA).

A gamma prior and Poisson likelihood results in a gamma posterior. Hence gamma distribution is called a 'conjugate prior' for the Poisson distribution. If the resultant posterior distribution is not one of the standard known distributions, then the posterior characteristics can be determined through numerical treatment. The difficulty lies in calculating the marginal in the denominator of Equation 2.11. Markov Chain Monte Carlo (MCMC) method is a preferred tool to find the marginal in such circumstances. Metropolis-Hastings (or its special case Gibbs sampling) and Splice sampling are well known MCMC algorithms.

WinBUGS (Lunn et al., 2000) and its open source version OpenBUGS are widely used software tools for Bayesian inference.

2.6.3 Estimation using Time-to-Failure data

A time-to-failure database can be developed by maintaining a list of similar components and their respective failure times. For a multi-state system, the data must be classified as the time-to-event data between given two states. An exponential distribution can be fit to this data by assuming that the time-to-event is a random variable. The mean of this dataset can be considered as the distribution parameter, which is also the transition rate for a Markov transition. However, such a database is exhaustive and requires more effort and maintenance when compared to that of Poisson data. The Offshore REliability DAta (OREDA), for example is a database sponsored by eight international oil and gas organizations. The main purpose of this database is to act as a data bank of reliability and maintenance data. Considerable time and effort has been put to gather time-to-failure data in to the OREDA repository.

2.7 Markov reward model

The Markov reward model was initially developed keeping cost and financial models in mind. Later Volik et al. (1988) proved that this model can be used to obtain reliability indices such as the mean time to failure and mean number of failures. An example in the case of a multi-state repairable component was cited by Lisnianski and Levitin (2003).

The continuous-time Markov chain and the Markov transition rate matrix form the basis for this model. Additionally, each state transition and stay in a state is associated with a reward. This reward can be positive when it fetches profit or negative when it signifies losses. For developing a cost model, reward can be the associated loss due to a failure or the cost incurred on a repair or profit due to a sale. These rewards are arranged in a separate matrix which is similar in dimension to the transition rate matrix. Given these as the input along with the initial conditions, the total expected reward accumulated up to time t can be obtained using the Markov reward model:

$$\frac{dV_i(t)}{dt} = r_{ii} + \sum_{j=1, j\neq i}^{K} a_{ij} r_{ij} + \sum_{j=1}^{K} a_{ij} V_j(t) \tag{2.18}$$

where,

- $V_i(t)$ is the total expected reward accumulated up to time t with i as the initial state of the process at time 0,
- r_{ii} is the reward per unit time for staying in state i,
- r_{ij} is the reward for the transition from state i to state j,
- a_{ij} is the $(i, j)th$ element of the transition rate matrix,
- K is the number of states in the model.

Equation 2.18 can be written in a matrix form as:

$$\frac{d}{dt}\boldsymbol{V(t)} = \boldsymbol{u} + \boldsymbol{aV(t)} \tag{2.19}$$

where,

$$u_i = r_{ii} + \sum_{j=1,j\neq i}^{K} a_{ij} r_{ij} \tag{2.20}$$

2.7.1 Mean number of failures

Consider a repairable system. The mean number of failures in the time interval $(0, t)$ can be obtained by setting the reward r_{ij} to 1 for all transitions from an operating state i to a non-operating state j and solving the system of differential equations in (2.18). This essentially sets up a counter to zero and increments it for every failure encountered. Hence the total expected accumulated reward in this case corresponds to the mean number of failures.

2.7.2 Mean time to failure

Consider a Markov state space with an absorbing state denoting system failure. Then, the mean time to failure can be obtained by setting the reward r_{ii} to 1 for staying in each of the operating states and finding the stationary solution of the system of differential equations in (2.18):

$$0 = r_{ii} + \sum_{j=1}^{K} a_{ij} V_j(t) \tag{2.21}$$

Note that $r_{00} = r_{ij} = 0$ for all $i \neq j$. In this case the total expected accumulated reward corresponds to mean time to failure of the system.

2.8 Multi-state system reliability

Assessment of reliability of a system from its basic elements is one of the most important aspects of reliability analysis. A system is a collection of elements (subsystems, components etc.) whose proper, coordinated operation leads to the proper functioning of the system (Modarres et al., 1999). Consider such a multi-state system composed of n elements, each element j having k_j different states denoted by the set {1,2,...,k_j }. Suppose that Markov processes for each of these elements is independent of one another. Further, assume that there can only be one transition across the entire system i.e., there can only be one failure or one repair in the system at any time instant t (Lisnianski and Levitin, 2003). The first step would be to develop a state-space diagram for the entire system and then subsequently evaluate the reliability or availability of the system. For a large system with many components, each having multiple states, a pictorial state-space representation is not feasible. It would be more convenient to represent the model in terms of the system transition intensity matrix generated by composing the element transitions together.

Let E denote the set of ordered n-tuples representing all possible combinations of the states of the n elements.

$$E = \{1, 2, ...k_1\} \times \{1, 2, ...k_2\} \times ... \times \{1, 2, ...k_n\} \tag{2.22}$$

The exhaustive number of states K of the entire system is the cardinality of the set E. Also,

$$K = \prod_{j=1}^{n} k_j \tag{2.23}$$

Let each element of E be denoted by unique number from the set S={1,2,...,K}. The order of this enumeration has no formal rule. For convenience, let the first combination denote perfect working state of the system and the last one be the total failure.

Consider a system transition. Then, it has to be a change in state of the system from $e_1 \in$ E to $e_2 \in E$. As per the assumption, these two n-tuples are identical except for one position in the n-tuple. The corresponding transition rate of this positional change is filled up in the system matrix. If this assumption is violated, the corresponding transition rate is zero. The diagonal elements of the system matrix satisfy the condition of a transition matrix of a single element as stated in (2.5).

For example, let $e_1 = (1, 2, 3), e_2 = (2, 1, 3)$. Since element 1 has transited from state 1 to state 2 and element 2 has transited from state 2 to state 1, there have been two transitions which is a violation of the assumption. Hence, the entry at the intersection of e_1 and e_2 of the system transition matrix is zero.

Let $e_1 = (1, 1, 3), e_2 = (1, 1, 2)$. Since only element 3 has a state change, the corresponding transition rate of element 3 ($\mu_{3,2}^{(3)}$) is entered in the system transition matrix at the intersection of e_1 and e_2.

2.8.1 Example

Consider a system with two elements in series with constant failure rate of λ_1, λ_2 and repair rates μ_1, μ_2 respectively. The state space diagram for the entire system is given in Figure 2.3. The shaded state is the state of fully functional system while the other states represent system failure due to series connection of the elements.

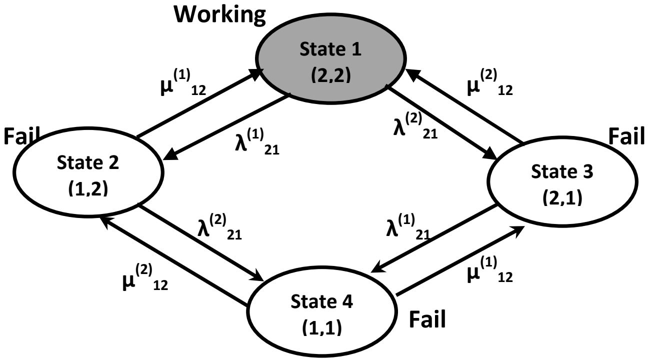


Figure 2.3: Muti-state system with two elements

The transition intensity matrices a_1 and a_2 respectively for each of these elements based on (2.5) is written as:

$$a_1 = \begin{bmatrix} -\mu_1 & \mu_1 \\ \lambda_1 & -\lambda_1 \end{bmatrix} \qquad a_2 = \begin{bmatrix} -\mu_2 & \mu_2 \\ \lambda_2 & -\lambda_2 \end{bmatrix}$$

The system transition intensity matrix a as described in section (2.8) is:

State Combinations $\in E$	State# $\in S$	(2,2) 1	(1,2) 2	(2,1) 3	(1,1) 4
(2,2)	1	$-(\lambda_{2,1}^{(1)} + \lambda_{2,1}^{(2)})$	$\lambda_{2,1}^{(1)}$	$\lambda_{2,1}^{(2)}$	0
(1,2)	2	$\mu_{1,2}^{(1)}$	$-(\mu_{1,2}^{(1)} + \lambda_{2,1}^{(2)})$	0	$\lambda_{2,1}^{(2)}$
(2,1)	3	$\mu_{1,2}^{(2)}$	0	$-(\mu_{1,2}^{(2)} + \lambda_{2,1}^{(1)})$	$\lambda_{2,1}^{(1)}$
(1,1)	4	0	$\mu_{1,2}^{(2)}$	$\mu_{1,2}^{(1)}$	$-(\mu_{1,2}^{(2)} + \mu_{1,2}^{(1)})$

The system of differential equations are formulated as per (2.3):

$$
\begin{aligned}
\frac{d}{dt}p_1(t) &= \mu_{1,2}^{(1)}p_2(t) + \mu_{1,2}^{(2)}p_3(t) - (\lambda_{2,1}^{(1)} + \lambda_{2,1}^{(2)})p_1(t)\\
\frac{d}{dt}p_2(t) &= \lambda_{2,1}^{(1)}p_1(t) + \mu_{1,2}^{(2)}p_4(t) - (\mu_{1,2}^{(1)} + \lambda_{2,1}^{(2)})p_2(t)\\
\frac{d}{dt}p_3(t) &= \lambda_{2,1}^{(2)}p_1(t) + \mu_{1,2}^{(1)}p_4(t) - (\mu_{1,2}^{(2)} + \lambda_{2,1}^{(1)})p_3(t)\\
\frac{d}{dt}p_4(t) &= \lambda_{2,1}^{(2)}p_2(t) + \lambda_{2,1}^{(1)}p_3(t) - (\mu_{1,2}^{(2)} + \mu_{1,2}^{(1)})p_4(t)
\end{aligned}
$$

$$p_1(t) + p_2(t) + p_3(t) + p_4(t) = 1 \qquad \text{and}$$

$$p_1(0) = 1, p_2(0) = p_3(0) = p_4(0) = 0$$

The Laplace transforms for the above system of differential equations are:

$$
\begin{aligned}
s\widetilde{p_1}(s) - p_1(0) &= \mu_{1,2}^{(1)}\widetilde{p_2}(s) + \mu_{1,2}^{(2)}\widetilde{p_3}(s) - (\lambda_{2,1}^{(1)} + \lambda_{2,1}^{(2)})\widetilde{p_1}(s)\\
s\widetilde{p_2}(s) - p_2(0) &= \lambda_{2,1}^{(1)}\widetilde{p_1}(s) + \mu_{1,2}^{(2)}\widetilde{p_4}(s) - (\mu_{1,2}^{(1)} + \lambda_{2,1}^{(2)})\widetilde{p_2}(s)\\
s\widetilde{p_3}(s) - p_3(0) &= \lambda_{2,1}^{(2)}\widetilde{p_1}(s) + \mu_{1,2}^{(1)}\widetilde{p_4}(s) - (\mu_{1,2}^{(2)} + \lambda_{2,1}^{(1)})\widetilde{p_3}(s)\\
s\widetilde{p_4}(s) - p_4(0) &= \lambda_{2,1}^{(2)}\widetilde{p_2}(s) + \lambda_{2,1}^{(1)}\widetilde{p_3}(s) - (\mu_{1,2}^{(2)} + \mu_{1,2}^{(1)})\widetilde{p_4}(s)
\end{aligned}
$$

Substituting $\lambda = 0.5$ and $\mu = 1$, then algebraically solving for $\widetilde{p_1}(s)$:

$$
\begin{aligned}
\widetilde{p_1}(s) =& \frac{2 + 3.5s + s^2}{s(4.5 + 4.5s + s^2)}\\
=& \frac{0.4444}{s} + \frac{0.1111}{s + 1.5} + \frac{0.4444}{s + 3}
\end{aligned}
$$

Applying inverse Laplace transform on $\widetilde{p_1}(s)$, $p_1(t)$ is found:

$$p_1(t) = 0.444 + 0.111e^{-1.5t} + 0.444e^{-3t}$$

Since the system considered is a series system, states 2,3 and 4 lead to system failure. Hence availability of the system is given by $p_1(t)$ whose plot is shown in Figure 2.4. The asymptotic solution is given by:

$$\underset{t\to\infty}{Lt}\, p_1(t) = 0.44444$$

This asymptotic limit represents the fact that failure frequency of both the components have survived their infant mortality phase.

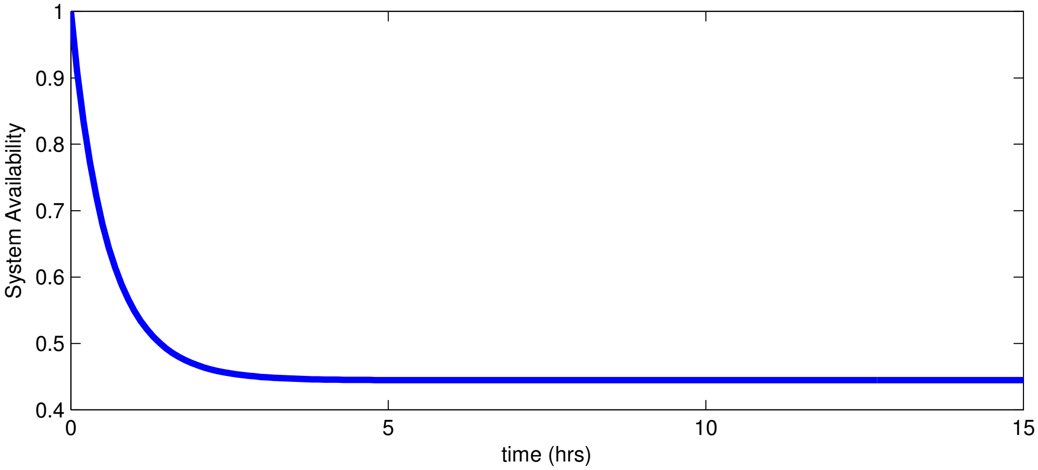


Figure 2.4: System availability of 4-state repairable system with $\lambda_1 = \lambda_2 = 0.5; \mu_1 = \mu_2 = 1$

Alternatively, the definition in Equation 2.9 can be used to find the asymptotic solution:

$$\begin{aligned}
0 &= \mu_{1,2}^{(1)} p_2 + \mu_{1,2}^{(2)} p_3 - (\lambda_{2,1}^{(1)} + \lambda_{2,1}^{(2)}) p_1 \\
0 &= \lambda_{2,1}^{(1)} p_1 + \mu_{1,2}^{(2)} p_4 - (\mu_{1,2}^{(1)} + \lambda_{2,1}^{(2)}) p_2 \\
0 &= \lambda_{2,1}^{(2)} p_1 + \mu_{1,2}^{(1)} p_4 - (\mu_{1,2}^{(2)} + \lambda_{2,1}^{(1)}) p_3 \\
0 &= \lambda_{2,1}^{(2)} p_2 + \lambda_{2,1}^{(1)} p_3 - (\mu_{1,2}^{(2)} + \mu_{1,2}^{(1)}) p_4
\end{aligned}$$

Ignoring the last equation and considering the constraint $p_1 + p_2 + p_3 + p_4 = 1$, the following system is obtained:

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} p_1 & p_2 & p_3 & p_4 \end{bmatrix} \begin{bmatrix} -(\lambda_{2,1}^{(1)} + \lambda_{2,1}^{(2)}) & \lambda_{2,1}^{(1)} & \lambda_{2,1}^{(2)} & 1 \\ \mu_{1,2}^{(1)} & -(\mu_{1,2}^{(1)} + \lambda_{2,1}^{(2)}) & 0 & 1 \\ \mu_{1,2}^{(2)} & 0 & -(\mu_{1,2}^{(2)} + \lambda_{2,1}^{(1)}) & 1 \\ 0 & \mu_{1,2}^{(2)} & \mu_{1,2}^{(1)} & 1 \end{bmatrix}$$

Solving this system the steady state probabilities are obtained as

$$\begin{bmatrix} 0.4444 & 0.2222 & 0.2222 & 0.1111 \end{bmatrix}$$

0.4444 represents availability of the series system in this example and is the same as the result obtained through the Laplace method.

Transitional probabilities $p = \{p_{ij}\}$are given by:

$$
\begin{aligned}
p &= \begin{bmatrix}
0 & \dfrac{\lambda_{2,1}^{(1)}}{(\lambda_{2,1}^{(1)} + \lambda_{2,1}^{(2)})} & \dfrac{\lambda_{2,1}^{(2)}}{(\lambda_{2,1}^{(1)} + \lambda_{2,1}^{(2)})} & 0 \\
\dfrac{\mu_{1,2}^{(1)}}{(\mu_{1,2}^{(1)} + \lambda_{2,1}^{(2)})} & 0 & 0 & \dfrac{\lambda_{2,1}^{(2)}}{(\mu_{1,2}^{(1)} + \lambda_{2,1}^{(2)})} \\
\dfrac{\mu_{1,2}^{(2)}}{(\mu_{1,2}^{(2)} + \lambda_{2,1}^{(1)})} & 0 & 0 & \dfrac{\lambda_{2,1}^{(1)}}{(\mu_{1,2}^{(2)} + \lambda_{2,1}^{(1)})} \\
0 & \dfrac{\mu_{1,2}^{(2)}}{(\mu_{1,2}^{(2)} + \mu_{1,2}^{(1)})} & \dfrac{\mu_{1,2}^{(1)}}{(\mu_{1,2}^{(2)} + \mu_{1,2}^{(1)})} & 0
\end{bmatrix} \\
&= \begin{bmatrix}
0 & 0.5000 & 0.5000 & 0 \\
0.6667 & 0 & 0 & 0.3333 \\
0.6667 & 0 & 0 & 0.3333 \\
0 & 0.5000 & 0.5000 & 0
\end{bmatrix}
\end{aligned}
$$

From Figure 2.4, since $\lambda_{2,1}^1 = \lambda_{2,1}^2$, it is seen that $p_{12} = p_{13}$. It is also observed that $p_{21} > p_{24}$ because repair rate μ_1 of component 1 is greater than the failure rate λ_2 of component 2.

In order to calculate the expected number of failures, the reward matrix elements are set to 1 is written as per the description in Section 2.7.1:

$$
\boldsymbol{r} = \begin{bmatrix}
0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
$$

The system of integral equations (2.18) to be solved to yield the mean number of failures with $\lambda = 0.5$ and $\mu = 1$ are:

$$
\begin{aligned}
\frac{d}{dt}V_1(t) &= 1 - V_1(t) + 0.5V_2(t) + 0.5V_3(t) \\
\frac{d}{dt}V_2(t) &= V_1(t) - (3/2)V_2(t) + 0.5V_4(t) \\
\frac{d}{dt}V_3(t) &= V_1(t) - (3/2)V_3(t) + 0.5V_4(t) \\
\frac{d}{dt}V_4(t) &= V_2(t) + V_3(t) - 2V_4(t)
\end{aligned}
$$

$$V_1(0) = 1, V_2(0) = 0, V_3(0) = 0, V_4(0) = 0$$

In this system, $V_1(0) = 1$ represents the fact that the system starts its operation in state 1 *i.e.*, the perfectly operating state. The mean number of failures varies with the initial state of operation as seen in Figure 2.5. If the system starts from the failure state 4, it takes some time to return to operating state and hence experiences relatively lesser failures. As a result, we see that $V_4(t)$ is lesser for all t than other cases. If system begins with state 2 or state 3, it is more likely to be repaired and hence returns to state 1. Since some time is spent in this process, the system encounters lesser number of failures than the case when system starts from state 1.

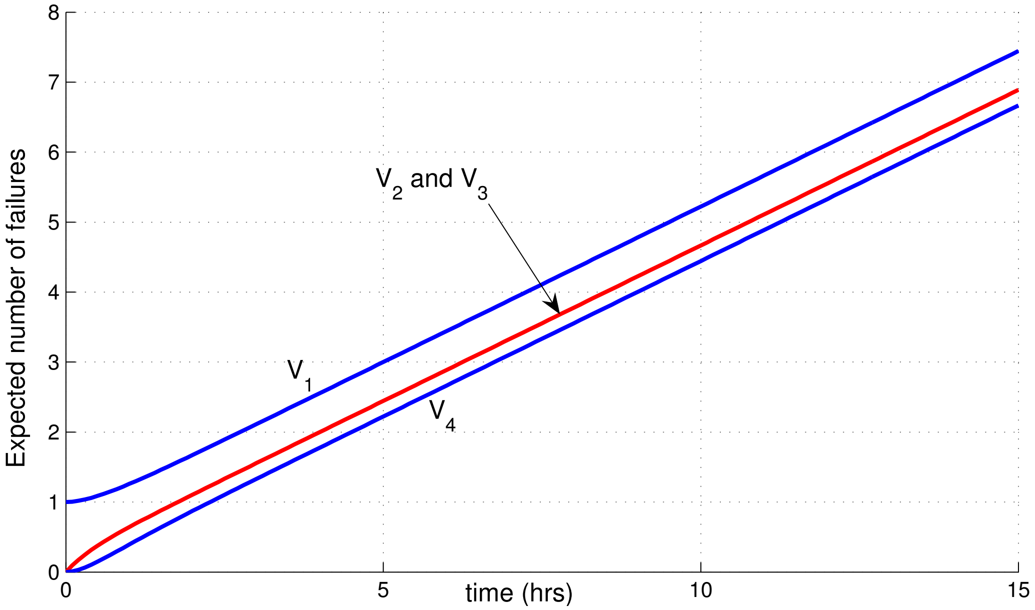


Figure 2.5: Expected number of failures of 4-state repairable series system with $\lambda_1 = \lambda_2 = 0.5; \mu_1 = \mu_2 = 1$

2.9 Case Study: Nuclear Component Cooling Water (NCCW) System

In nuclear power plants, Nuclear Component Cooling Water (NCCW) systems are typically used for removing heat (cooling) systems containing potentially radioactive fluids. These systems are in turn cooled by the ultimate cooling system - river, lake, sea, or ocean water. An event that creates a disturbance in these plants having the potential to lead to core damage, depending on the successful operation of required mitigating systems in the plant is called an initiating event.The number of such events occurring in a unit time is called the initiating event frequency. Xing et al. (1996) compared Markov and fault tree models for determining support system failure initiating event frequency in the Probabilistic Safety Assessment (PSA) of nuclear power plant for both power and shutdown conditions. They studied two-train systems with common failure/repair characteristics. The NCCW system consists of two parallel pump trains connected in series with a heat exchanger train. Both pump trains have 5 components each connected in series - pump, pump suction manual valve, pump suction filter, pump discharge check valve and pump discharge manual valve. The heat exchanger train consists of the following: heat exchanger, heat exchanger inlet check valve, heat exchanger cooling water inlet valve, heat exchanger cooling filter valve and heat exchanger cooling water outlet valve. The task is to evaluate the initiating event frequency during the outage time of approximately $\tau_m = 80$ hours. The success criterion is any one of the two pump trains running and the heat exchanger train operating. The fault tree of the system with the loss of NCCW train as the top event is shown in Figure 2.6.

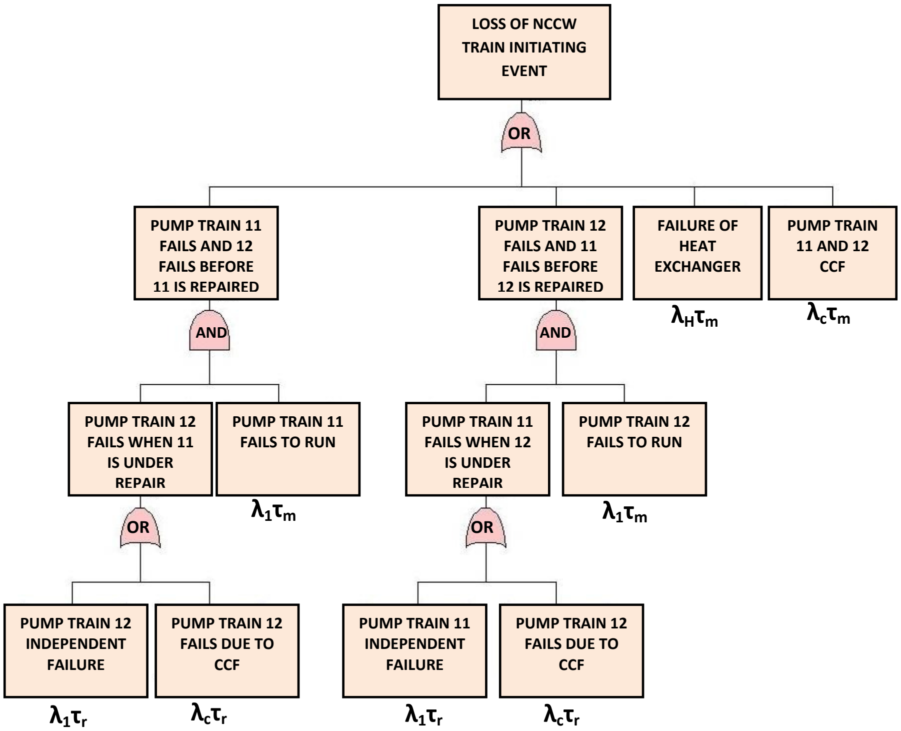

LOSS OF NCCW TRAIN INITIATING EVENT
OR
PUMP TRAIN 11 FAILS AND 12 FAILS BEFORE 11 IS REPAIRED
PUMP TRAIN 12 FAILS AND 11 FAILS BEFORE 12 IS REPAIRED
FAILURE OF HEAT EXCHANGER
λHτm
PUMP TRAIN 11 AND 12 CCF
λcτm
AND
AND
PUMP TRAIN 12 FAILS WHEN 11 IS UNDER REPAIR
PUMP TRAIN 11 FAILS TO RUN
λ1τm
PUMP TRAIN 11 FAILS WHEN 12 IS UNDER REPAIR
PUMP TRAIN 12 FAILS TO RUN
λ1τm
OR
OR
PUMP TRAIN 12 INDEPENDENT FAILURE
λ1τr
PUMP TRAIN 12 FAILS DUE TO CCF
λcτr
PUMP TRAIN 11 INDEPENDENT FAILURE
λ1τr
PUMP TRAIN 12 FAILS DUE TO CCF
λcτr

Figure 2.6: Fault tree for the NCCW train system.

The data for component failure rate and repair time are listed in Table 2.2.

Table 2.2: Reliability data for NCCW System

Pump train		
TDTF1R (hr^{-1})	Pump fails during operation	5.44 x 10^{-6}
TSHOVT (hr^{-1})	Manual valve transfers open/closed	4.20 x 10^{-8}
TNSC2P (hr^{-1})	Filter plugs fail during operation	2.19 x 10^{-6}
TSCOVP (hr^{-1})	Check valve transfers open/closed	1.03 x 10^{-8}
BDTF1R	β-factor for common cause failure	2.70 x 10^{-2}
τ_r (Hours)	Pump train repair time	1.94 x 10^{1}
Heat exchanger		
TBHX1B (hr^{-1})	Heat exchanger rupture/leak rate	1.14 x 10^{-6}

There are two cases considered here: base case and sensitivity case. Base case represents a strong presence of a common cause failure as opposed to the sensitivity case. The failure rate λ_1 of the pump train, λ_H of the heat exchanger and the common cause failure rate λ_c are computed from Table 2.2 and listed in Table 2.3 for the base case as computed by Xing et al. (1996). For the sensitivity case the independent failure rate of the pump $TDTF1R$ is steeply increased to 2.0 x $10^{-3}(hr^{-1})$ and β-factor is decreased to 1.0 x 10^{-3}.

Table 2.3: Failure rates for the pump train and heat exchanger.

λ_1	=	TDTF1R*(1-BDTF1R)+2*TSHOVT+TNSC2P+TSCOVP
λ_c	=	TDTF1R*BDTF1R
λ_H	=	TBHX1B+TSCOVP+2*TSHOVT+TNSC2P

Applying the rules in (C.1) and (C.1), the probability of the loss of NCCW initiating event can be computed as:

$$\begin{aligned} f_{FT} &= (\lambda_1\tau_r + \lambda_c\tau_r)\lambda_1\tau_m + (\lambda_1\tau_r + \lambda_c\tau_r)\lambda_1\tau_m + \lambda_H\tau_m + \lambda_c\tau_m \\ &= 2(\lambda_1\tau_r + \lambda_c\tau_r)\lambda_1\tau_m + (\lambda_H + \lambda_c)\tau_m \\ &\approx 2\lambda_1^2\tau_r\tau_m + (\lambda_H + \lambda_c)\tau_m \end{aligned} \tag{2.24}$$

The evaluated event frequencies for both the base and sensitivity cases are tabulated in Table 2.4. It is seen that the system failure probability is higher in the presence of bigger common cause failure rate since for a parallel system failure of both the pump trains leads to a definite failure of the entire system.

A basic assumption in the fault tree analysis is that all system failures are binary

Table 2.4: NCCW train failure probability evaluated from the fault tree

Case	Failure Probability (f_{FT})
Base	2.8516 x 10^{-4}
Sensitivity	1.2821 x 10^{-2}

in nature, i.e. a system either performs successfully or fails completely. It is also assumed that the system is capable of performing its task if all sub-components or sub-systems are operating. But, in the real world, a system could pass through a number of states before it completely fails i.e. a fault tree does not treat degradation of a system or its components over a period of time. Moreover, fault tree analysis addresses only instantaneous failures.

The NCCW problem can be analyzed in a more rigorous time-dependent manner using the Markov process model. With three components in the system and given that each component could be in one of the two possible states: functioning or failed, the system as a whole can have 2^3=8 possible states. Instead, the state space diagram is reduced to three states: (a) two pumps and the heat exchanger running, (b) one pump and the heat exchanger running and (c) system failure. Since that any one of the pumps can fail in no particular order, the failure rate for the transition from two pumps running to one pump running is taken as twice the failure rate λ_1 of a single pump train. If single pump fails, it can be repaired with a constant repair rate of μ. The system fails if either both the pump trains fail or the heat exchanger train fails. This state of system failure is considered as an absorbing state. There can be common cause failure (CCF) for the system, and

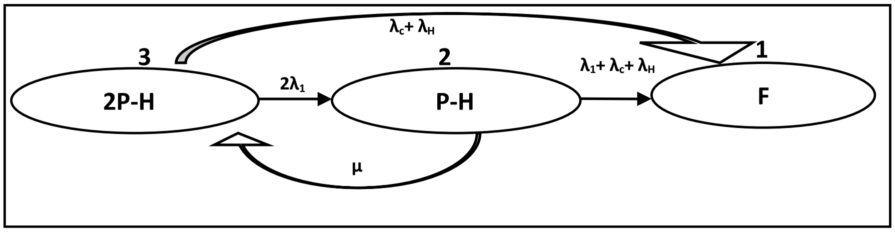


Figure 2.7: Markov state-space diagram for NCCW train 10 System.

such failures can occur when either two components are operating or when only one is operating. Such a failure could cause the entire system to fail with failure rate of λ_c (hr^{-1}). CCF is dealt on a sensitivity basis. The absence of a CCF is represented by setting λ_c to zero and increasing the independent failure rate λ_1 of the pump trains.

The reduced state space diagram in shown in Figure 2.7 and a reliability block diagram corresponding to the same is shown in Figure 2.8 The transition intensity matrix can be written off directly from Figure 2.7 keeping the conditions (2.5) in mind:

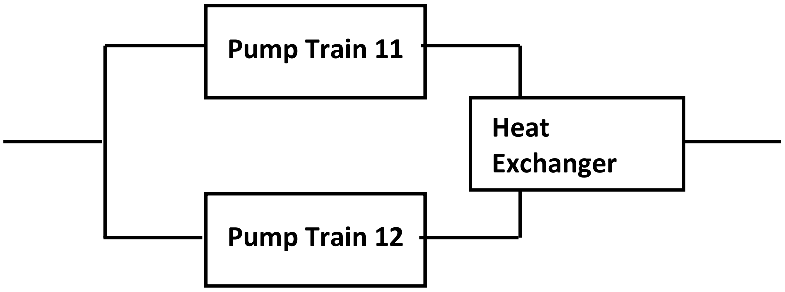


Figure 2.8: Reliability Block Diagram of the NCCW train system.

$$\begin{bmatrix} 0 & 0 & 0 \\ \lambda_1+\lambda_c+\lambda_H & -(\lambda_1+\lambda_c+\lambda_H+\mu) & \mu \\ \lambda_c+\lambda_H & 2\lambda_1 & -(\lambda_c+\lambda_H+2\lambda_1) \end{bmatrix}$$

The system of differential equations follows from the intensity matrix

$$\begin{aligned} \frac{dp_1(t)}{dt} &= (\lambda_1+\lambda_c+\lambda_H)p_2(t)+(\lambda_c+\lambda_H)p_3(t) \\ \frac{dp_2(t)}{dt} &= 2\lambda_1 p_3(t) - (\lambda_1+\lambda_c+\lambda_H+\mu)p_2(t) \\ \frac{dp_3(t)}{dt} &= \mu p_2(t) - (\lambda_c+\lambda_H+2\lambda_1)p_3(t) \\ \text{with the initial conditions} \quad & p_1(0)=p_2(0)=0, p_3(0)=1 \end{aligned}$$

The values for the failure and repair rates are taken from Table 2.3. Solving for $p_1(t)$, gives the time-dependent system failure probability. $p_1(t)$ is plotted in Figure (2.9) for both the base and sensitivity cases.

2.9.1 Comparison of the Markov model and Fault Tree Analysis

Even those systems that are entirely composed of non-ageing elements (with a constant failure rate) will deteriorate (fail more often) with age, if these systems

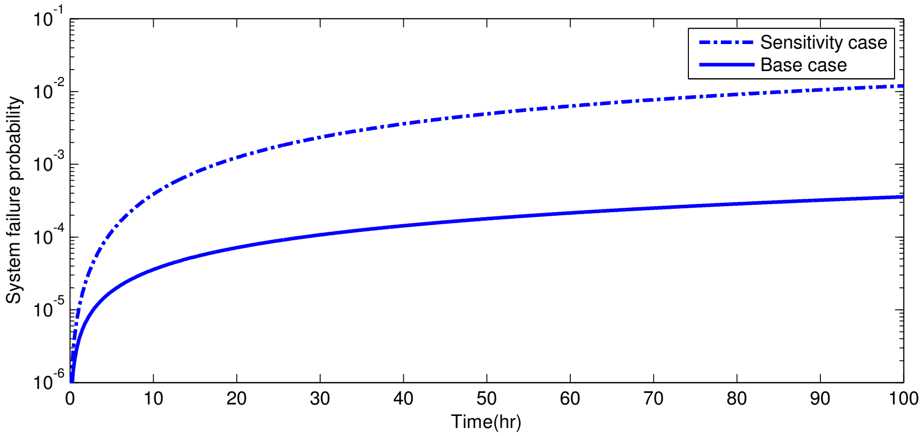


Figure 2.9: System failure probability for the 3-state NCCW Markov System

are redundant in irreplaceable components. Hence ageing is a direct consequence of systems redundancy Gavrilov and Gavrilova (2003).

The system hazard rate of the NCCW system is non-constant and the expected number of failures or the initiator frequency can be computed using:

$$f_{mk} = \int_0^{\tau_m} \lambda(t)dt \tag{2.25}$$

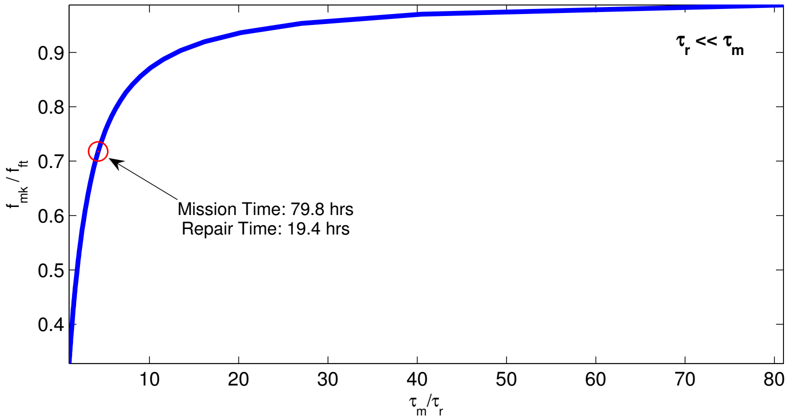


Figure 2.10: Comparison of Markov and fault tree results for NCCW System(Xing et al., 1996).

Figure 2.10 shows a plot of the ratio of the initiator frequencies computed by Markov and fault tree methods. On the x-axis, the ratio of the mission time τ_m to the repair time is considered. When the repair time is comparable (closer to mission time), results of fault tree and Markov model agree with each other. However, when repair time is much smaller than the mission time, fault tree yields conservative results. Xing et al.(1996) argued that for systems configuration in which mission time is short and the independent failure (common-cause failure is negligible) dominates the failure mode, the effect of repair is more important so that fault tree approach yields conservative results.

2.10 Conclusion

In this chapter, Markov model has been shown as a more rigorous time-dependent alternative to the time-independent fault tree model. A system is allowed to transit through multiple states in its lifetime with specified constant failure and repair rates to yield failure probability over its mission time. However, Markov model has the significant disadvantage that its size grows exponentially as the size of the system increases. This rapid growth of the number of states may lead to intractable models. In addition, Markov model assumes exponential time-to-failure distribution. While the reliability and failure probabilities computed using the Markov model are time-dependent, a more generic time-dependent model would have the failure and repair rates also as a function of time. The next chapter on semi-Markov models attempts to improvise on the Markov model by allowing flexibility in choosing non-exponential transition times.

Chapter 3

Semi-Markov Processes

3.1 Introduction

The *hazard rate function* $\lambda_s(t)$ for a system is the probability that the system will fail given that it was reliable until time t. It forms a good measure of the ageing phenomenon for a complex engineering system.

A Markov process model assumes exponential failure or repair times. Asymptotically, this model shows a constant hazard rate and thus does not account for the increasing hazard. A semi-Markov process model, on the other hand, assumes arbitrary distributions for time spent during state transitions and hence, is able to deviate from the conventional ideas of reliability analysis based on exponential distributions.

If various components of the same type were observed and their time-to-failure were tabulated, then these values are unlikely to be the same in all the cases. Assuming a constant failure rate leads to the usage of exponential distribution as the basis of Markov analysis. However, the failure rate function of an ageing system is non-constant and hence a Markov process model is likely to yield not so accurate reliability estimates.

The reliability of many engineering components can be described by a 'bathtub' curve which has one of its zones representing the component's wear out period. The Weibull distribution is capable of describing the lifetime of such components. Its probability density function (*pdf*), cumulative distribution function (*cdf*) and reliability function are respectively given by:

$$f_T(t|\gamma, \lambda) = (\lambda\gamma)(\lambda t)^{\gamma-1} e^{-(\lambda t)^{\gamma}} \tag{3.1}$$

$$F_T(t|\gamma, \lambda) = 1 - e^{-(\lambda t)^{\gamma}} \tag{3.2}$$

$$R_T(t|\gamma, \lambda) = e^{-(\lambda t)^{\gamma}} \tag{3.3}$$

where λ is the scale parameter and γ is the shape parameter. The scale parameter centers around the mean life of the component and the shape factor is a function of variation in the observed mean life. When $\gamma = 1$ the Weibull distribution reduces to the exponential distribution: $f_T(t|\lambda) = \lambda e^{-(\lambda t)}$ where $1/\lambda$ is the mean time to failure and λ is the failure rate. Further, for γ around 3.4, Weibull distribution reduces to normal distribution.

The coefficient of variation (*cov*) is the ratio of the standard deviation of the set of observed time-to-failure life to its mean. The Weibull shape and scale parameters corresponding to this combination of mean life and *cov* can be back calculated from the following formulas for Weibull mean, standard deviation and coefficient of variation:

$$\begin{aligned} \mu_{wbl} &= \lambda\Gamma(1 + \frac{1}{\gamma}) \\ \sigma^2_{wbl} &= \lambda^2\Gamma(1 + \frac{2}{\gamma}) - \mu^2_{wbl} \\ \mathrm{cov}_{wbl} &= \frac{\sigma_{wbl}}{\mu_{wbl}} \end{aligned} \tag{3.4}$$

The semi-Markov process (SMP) like a Markov process also has a set of states and the transitions between them are governed by a transition probability matrix. The fact that the transition time between any two states is distributed exponentially limits the use of Markov processes to many practical problems. However, in a semi-Markov process, the time spent in any state after entering it is a random variable which can be described by a non-exponential distribution as well. This feature would be useful in cases where the lifetime and repair times are not exponential. The distributions for the time spent between various states are represented in a matrix form called the 'kernel matrix' of the process. The kernel matrix and the initial state occupied by the process completely define the stochastic behavior of the semi-Markov process. Given these as the input, the statistical time behavior of the process is described by a system of linear integral equations. The main problem then is to find the solution of this system of equations yielding the probability of being in any state given that the process started in an initial state.

3.2 Literature Review

The idea of semi-Markov process model was proposed almost simultaneously by Lévy (1954) and Smith (1958). The foundations of semi-Markov processes can be found in Ross (1992), Gihman and Skohorod (1974), Cinlar (1975), Silverstov (1980), Korolyuk and Swishchuk (1995). This thesis follows the general formulation of the semi-Markov process as developed in Howard (1964, 1971). For the first passage distribution of general semi-Markov process, Pyke (1961a, 1961b) suggested a Laplace-Stieljes transform approach. Ciardo et al. (1990) proposed a method of computing the distribution of performability in a Markov reward process. For finite mission times Iyer et al. (1986) obtained the double Laplace transform of performability for systems that may be modeled by semi-Markov processes. White and Palumbo (1990) proposed a method called trimming for reducing the number of states in a semi-Markov reliability model, and derived an error bound. The interval reliability for a repairable semi-Markov system which alternates between working and repair periods was studied by Csenki (1995). The author applied the results to a two-unit system with sequential preventive maintenance.A two-point trapezoidal rule was used to numerically solve the resulting system of integral equations. Kovalenko et al. (1997) concentrate on aspects of semi-Markov models as a basis for mathematical theory of reliability of time dependent systems.

Ouhbi and Limnios (2003) presented a modern overall view of semi-Markov processes and its applications in reliability. A bootstrap simulation method using a saddlepoint approximation was proposed by Butler and Bronson (2002). Lisnianski and Levitin (2003) systematically describe the tools for multi-state system reliability assessment and optimization with applications to different fields. Ouhbi and Limnios (2002) derived the estimators of reliability and availability of semi-Markov systems.They studied the asymptotic properties of these estimators and constructed the non-parametric confidence intervals for the point availability. Maximum likelihood and Bayes estimates of the parameters included in a three state semi-Markov reliability model were presented by El-Gohary (2004).

D'Amico et al. (2006) considered the credit risk problem as a semi-Markov reliability problem.They applied their model to compute the default probability of a company going into debt. özekici and Soyer (2006) considered a Poisson process in which arrival rate at any time depends on the state of a semi-Markov process. Tomasevicz and Asgarpoor (2006) presented a continuous-time semi-Markov process to determine the amount of preventive maintenance to be performed on an equipment in order to maximize availability. They assumed that an equipment could fail due to both deterioration and random occurrences of failures. Lisnianski (2007) extended the classical reliability block diagram method to a repairable multi-state system.The suggested method is based on the combined random processes and the universal generating function technique and drastically reduces the number of states in the multi-state model. Koutras and Platis (2008) modelled preventive maintenance technique (software rejuvenation) to prevent failures in continuously running systems that experience software ageing. Rejuvenation is modelled in a redundant computer system via a semi-Markov process in order to counteract software ageing. Gámiz and Román (2008) proposed a smooth estimation of the availability based on semi-Markov kernel estimator of the cumulative distribution functions (CDF) of the failure and repair times, for which the bandwidth parameters were obtained by bootstrap procedures.

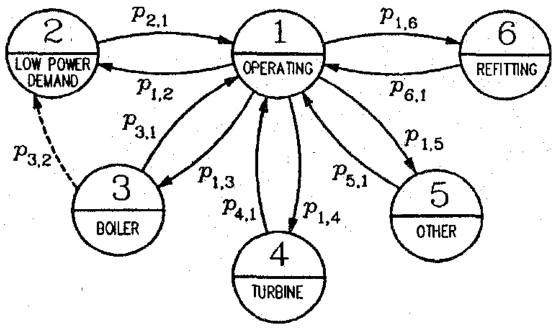


Figure 3.1: Power plant reliability model. *Source*: Perman et al. (1997)

Perman et al. (1997) applied semi-Markov process model to power plant reliability analysis. The model consisted of six states as in Figure 3.1 with failure states dedicated to major components in the plant. These include the boiler and turbine. The failure times were Weibull distributed with parameters estimated from real operating data using maximum likelihood method. It was assumed that the observations of the holding-times in a given state are independent and identically-distributed (*i.i.d*). However, the reliability estimates were a result of direct numerical computations by discretizing the integrals. In this thesis, the use of Weibull distribution is further explored leading to some closed form solutions and techniques to reduce states in a model.

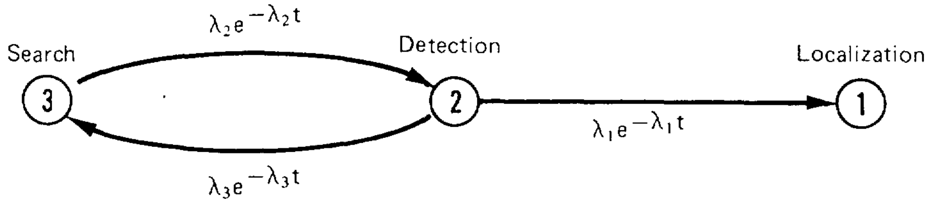

Search
Detection
Localization
3
2
1
$\lambda_2 e^{-\lambda_2 t}$
$\lambda_1 e^{-\lambda_1 t}$
$\lambda_3 e^{-\lambda_3 t}$

Figure 3.2: Search for submerged submarine. *Source*: Nunn and Desiderio (1977)

Figure 3.2 shows a state space model to obtain reliability of a search operation. An aircraft searches for a submerged submarine by dropping sensors in the ocean. When an approximate location is detected, additional sensors are dropped to exactly localize the position. The time taken to detect and localize follow exponential distribution.

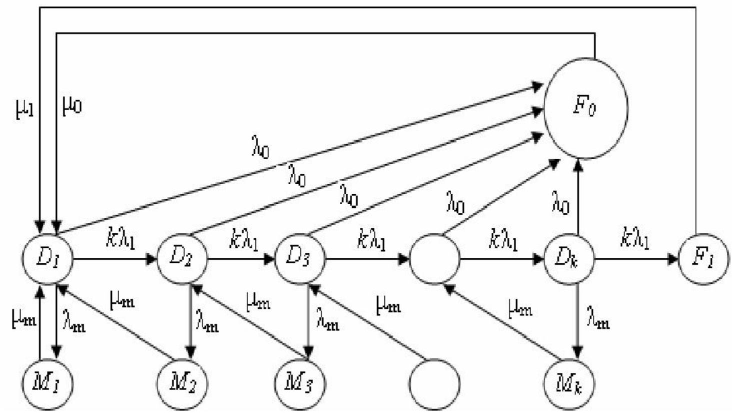


Figure 3.3: General state space diagram for preventive maintenance. *Source*: Tomasevicz and Asgarpoor (2006)

Tomasevicz and Asgarpoor (2006) et al. developed a continuous time semi-Markov process model for equipments that fail due to both deterioration and random occurrences as in Figure 3.3. They modelled the deterioration in k-discrete steps with exclusive states for preventive and corrective maintenance. Their approach uses the time spent in the states in the formulation rather than statistical distribution representing the time spent in the states and the outputs are steady-state state probabilities.

A real time online computer database system is vulnerable to cyber attacks. A cycle of a typical attack could comprise of six states - normal state G, infected state

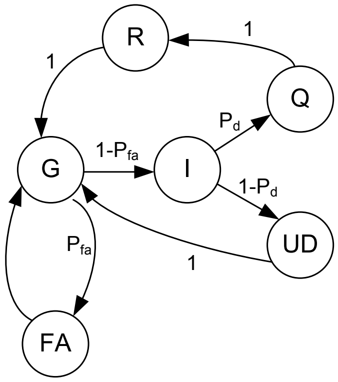


Figure 3.4: Survivability model of an intrusion tolerant database system. *Source*: Wang et al. (2010)

I, quarantined state Q, undetected state UD, and false alarm state FA as seen in Figure 3.4. Wang et al. (2010) et al. developed a semi-Markov based survivability model for this state space. Steady state probabilities for false alarm and detection were obtained.

3.3 The Semi-Markov Process Model

This thesis follows the general formulation of the continuous-time discrete-state semi-Markov process model as developed by Howard (1964, 1971).

Suppose the model has N states. Let $f_{ij}(t)$ and $F_{ij}(t)$ denote the *pdf* and *cdf*, respectively, of the event corresponding to the transition from state i to state j at time t.

Assume that the process is in state i. From this state, there could be k different states to which the process could transit in a single step. These states could be completion of a repair, further degradation of the system or a failure mode with an underlying failure mechanism. Also assumed in this model is that all these k possibilities are independent of the occurrence of each other. At a time instant t, the process chooses only one state from these choices such that the time to be spent in the current state i is the minimum before instantaneously jumping to the chosen state. The probability that the next state is j and not any other state k reachable from i is given by:

$$c_{ij}(t) = f_{ij}(t) \prod_{k \neq j} (1 - F_{ik}(t)) \tag{3.5}$$

For N=2, $c_{ij}(t) = f_{ij}(t)$. The matrix $C(t) = [c_{ij}(t)]$ is called the kernel or core of the semi-Markov process model and

$$w_i(t) = \sum_{j=1}^{N} c_{ij}(t) \tag{3.6}$$

is called the waiting time density function for the state i. It represents the probability that the system waits in state i for t time units before making a transition. Hence it is an unconditional density function. It is assumed that any row i of the kernel $C = [c_{ij}]$ satisfies the condition:

$$\int_{0}^{\infty} \sum_{j} c_{ij}(t) dt \approx 1 \tag{3.7}$$

This assumption assures that there is unit probability that the system will be in one of the N states of the system at time t, given the initial state as i. The probability that the system does not leave state i by time t is given by:

$$W_i(t) = 1 - \int_{0}^{t} w_i(t) dt \tag{3.8}$$

The objective of the model is to determine the probability $\phi_{ij}(t)$ of being in each state j given that the system initially is in a particular state i. $\phi_{ij}(t)$ can be determined by solving a system of integral equations:

$$\phi_{ij}(t) = \delta_{ij} W_i(t) + \sum_{k} \int_{0}^{t} c_{ik}(\tau) \phi_{kj}(t - \tau) d\tau \tag{3.9}$$

Where $i = j = k = 0, 1, 2, ...N - 1$.

The right hand side of Equation 3.9 describes the following probabilities:

1. $i = j$ and second term=0: $W_i(t)$ is the probability that the process does not leave state i by time t.

2. $i = j$ and second term not 0: process leaves state i and returns to i by time t.

3. $i \neq j$ and second term $\neq 0$: process leaves state i and reaches state j by time t.

The system of equations can alternatively be written in a compact form as a matrix:

$$\phi(t) = diag(W(t)) + \int_0^t C(\tau)\phi(t-\tau)d\tau \tag{3.10}$$

Given that the system started its operation in state i and that state j is the only absorbing state, the failure probability of the system is given by $\phi_{ij}(t)$ and reliability $R(t) = 1 - \phi_{ij}(t)$.

Table 3.1: Explanation of terms in the Markov renewal equation

Term	Explanation
$C_{ij}(t)$	Kernel of the semi-Markov process(Howard, 1971): probability density function for the event that the process entering state i at time zero will make its next transition to state j after holding for t time units. A homogeneous model is assumed which means that entry in to state i at time t is the same as entering it at time zero.The transition from i to j is a single step transition. Occurrence of this transition either has a probability p or a probability is assigned according to the competing risk model.The competing risk model states that the process chooses state j as the successor and not any other state reachable from state i in a single step because the time spent in i with j as the successor is the minimum of the times spent in i with any other state as the successor.
ϕ_{ij}(t)	Interval transition probability (Howard, 1971): a conditional probability that the process will occupy state j at time t if it entered state i at time zero. This is a multi-step transition obtained using the Markov renewal equations. If i is completely operational state and j is an absorbing state, $\phi_{ij}(t)$ represents the system failure probability and $1-\phi_{ij}(t)$ gives system reliability (Lisnianski, 2003).
$W_i(t)$	Complementary cumulative waiting time probability (Howard, 1971): an unconditional probability that the process will not leave its starting state i by time t. This is analogous to saying that the process will remain in state i for t time units and the successor state is not yet known

3.3.1 Example

Consider a simple 2-state non-repairable system with state 1 as down state and state 2 as up state. Let $f_{21}(t) = \lambda\ e^{-\lambda t}$.
$c_{21}(t) = f_{21}(t)$ since there is no competing risk in this problem. Then by Equations 3.5 and 3.6:

$$C(t) = \begin{bmatrix} \delta(t-\infty) & 0 \\ \lambda e^{-\lambda t} & 0 \end{bmatrix} \qquad\qquad w(t) = \begin{bmatrix} 0 \\ \lambda e^{-\lambda t} \end{bmatrix}$$

$\delta(t-\infty)$ is just a formal notation stating that once the system enters down state, it is irreparable.

3.3.2 Solution of Markov Renewal Equation

1. Continuous time solution

   (a) Transform techniques: If the process has a few states and the waiting time distributions are simple functions, it is convenient to apply Laplace-Stieljes or Geometric transform on Equation 3.9. This transformed algebraic set of equations is solved for ϕ_{ij} in the transformed space and then a corresponding inverse transform is applied to obtain $\phi_{ij}(t)$. These techniques have been discussed in Howard (1971). Sometimes even for simple systems, application and inversion of transforms is non-trivial and numerically intractable. Most distributions do not possess a closed form Laplace transform. Cole.W.Gulyas (2007) in a thesis dissertation employed a transform approximation method (TAM) to evaluate the Laplace transform of Weibull distribution and then numerically evaluated its Laplace inversion.

   (b) Direct numerical evaluation: Algorithms based on trapezoidal and Simpson's rule were derived by Nunn and Desiderio (1977) and Smith (1958). Smith (1958) derived an algorithm in which Eq.(3.9) is expanded in power series. This is a recursive algorithm, but, needs to be customized to specific distributions.

2. Discrete time solution

   (a) Discretized Markov renewal equation: Nunn and Desiderio (1977) use Eq.(3.9) almost "as is" to produce $\phi_{ij}(t)$ in a recursive manner by taking the values of the distribution on lattice points of the desired time period:

$$\phi(t_n) = W(t_n) + \sum_{\tau=0}^{t_n} C(\tau)\phi(t_n - \tau) \tag{3.11}$$

Starting with $\phi(t_0) = W(t_0)$, the above equation can be solved recursively.

(b) Convolution inverse method: A discrete-time semi-Markov process (DTSMP) generalizes discrete-time Markov chain. A DTSMP does not suffer from state explosion like continuous-time SMP. The Markov renewal equation can be expressed as a finite series of semi-Markov kernel convolution product. Within this framework, the initial state distribution of the system and the discrete semi-Markov kernel completely characterize the system. The reliability and its related measures follow from this formulation. Barbu et al. (2004) defined a discrete time semi-Markov model and proposed a computational procedure for solving the Markov renewal equation. They introduced identity and inverse elements for the discrete case convolution operation.

$$\begin{aligned} &\phi = diag(W) + C * \phi \\ \Rightarrow\ &\phi(n) = (I - C)^{(-1)} * diag(W(n)) \qquad\qquad n \in N \end{aligned}$$

In this proposal trapezoidal rule has been adopted for availability computations since relatively little literature exists regarding the numerical accuracy or running time of the other algorithms.

3.3.3 Solution by direct numerical integration

Equation 3.8 is computationally expensive if the integral has to be evaluated for each t. Instead, it can be computed as a recurrence relation as follows:

$$W_i(t_n) = \begin{cases} 1 - \int_0^{\Delta t} w_i(t_n)dt & n = 1 \\ W_i(t_{n-1}) - \int_{t_{n-1}}^{t_n} w_i(t)dt & n > 1 \end{cases} \tag{3.12}$$

Where, by trapezoidal rule, we have:

$$\int_{t_{n-1}}^{t_n} w_i(t)dt = \frac{\Delta t}{2}\{w_i(t_{n-1}) + w_i(t_n)\} \tag{3.13}$$

To solve the system of Markov renewal equations, Nunn and Desiderio(1977) derived the following recurrence relation based on trapezoidal rule by distributing t on a set of equally spaced points in the interval $[0, t]$:

$$\begin{aligned}\phi(t_n) = [I - \frac{\Delta t}{2}C(0)]^{-1}[diag(W(t_n)) + \Delta t \sum_{k=1}^{n} C(t_k)\phi(t_n - t_k) \\ - \frac{\Delta t}{2}C(t_n)\phi(0)]\end{aligned} \tag{3.14}$$

Where $\Delta t = t_n - t_{n-1}$. The solution is started with $\phi(0) = W(0) = I$. The derivation is discussed in detail in the appendix.

The convolution operation in the above equation involves repeated addition and multiplication of matrices thus slowing down the computations as n grows. With sufficiently large storage space, the following technique for convolution improves the speed:

$$\sum_{k=1}^{n} C(t_k)\phi(t_n - t_k) = \begin{bmatrix} C(t_1) & C(t_2) & ... & C(t_n) \end{bmatrix} \begin{bmatrix} \phi(t_{n-1}) & \phi(t_{n-2}) & ... & \phi(t_0) = I \end{bmatrix}^T$$

3.4 Concepts in reliability analysis

3.4.1 System reliability

Reliability of non-repairable system is expressed in terms of its time-to-failure distribution, which can be represented by respective *cdf*, *pdf*, or hazard (failure) rate function (Modarres et al., 1999) *i.e.*, the lifetime of a nonrepairable component lasts until its first entrance in to the subset of unacceptable states called the "absorbing state". Given that the process started in state i at time zero, the first passage time to the absorbing state j is given by $\phi_{ij}(t)$ and its reliability is computed as Lisnianski and Levitin (2003):

$$R(t) = 1 - \phi_{ij}(t) \tag{3.15}$$

3.4.2 Availability and unavailability

Components of a system can be repaired and such an activity takes time. A repairable system does not have an absorbing state. Rather it has a set of acceptable states B that meet a preset demand and the rest are termed as unacceptable states. The instantaneous availability of the system is computed by summing $\phi_{ij}(t)$ over the set B (Lisnianski and Levitin, 2003):

$$A(t) = \sum_{j \in B} \phi_{ij}(t) \tag{3.16}$$

and instantaneous unavailability is $1 - A(t)$.

3.4.3 Hazard rate

Hazard rate is used to refer to instantaneous rate of failure of a non-repairable system or non-repairable component in a system. It is denoted by $\lambda(t)$ or $h(t)$ and has the units "failures per unit of time". It is a conditional failure rate in the sense that it expresses the likelihood that a component will fail in $(t, t + \Delta t)$ given that it was reliable until time t. Hazard rate can be greater that one, but it is often misinterpreted as a probability.

Some authors refer it to as failure rate function since it is considered as well established in applied reliability Rausand and Høyland (2004). In this thesis, hazard rate is used when dealing with non-repairable system with a repairable subsystem.

Hazard rate can be expressed in multiple ways for the continuous case Rausand and Høyland (2004):

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1 - F(t)} = \frac{-1}{R(t)} \frac{dR(t)}{dt} = -\frac{d\ln R(t)}{dt} \tag{3.17}$$

where $f(t)$, $F(t)$ and $R(t)$ denote the density, cumulative distribution and reliability functions respectively of the time to failure of a component.

3.5 Steady state probabilities

Given the Markov transition rate matrix A with zero diagonal entries, the Markov transition probability matrix $P = [p_{ij}]$ can be found by dividing every row of the matrix by its row sum. For $N = 2$, P is the following matrix:

$$P = [p_{ij}] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{3.18}$$

After a long time of operation, the probability of being in a state j in the Markov sense, regardless of where the system started is given by π_j. This is called the stationary distribution of the imbedded Markov chain of the semi-Markov process model and is found by solving the following set of equations:

$$\pi_j = \sum_{i=0}^{N-1} \pi_i p_{ij} \tag{3.19}$$

$$\sum \pi_j = 1 \tag{3.20}$$

The semi-Markov steady state probability ϕ_j for state j, considering arbitrary distributions for failure/repair time is given by(Howard, 1964, 1971):

$$\phi_{ij} = \frac{\pi_j \overline{\tau}_j}{\sum_{j=1}^{N} \pi_j \overline{\tau}_j} = \phi_j \tag{3.21}$$

Where $\overline{\tau_j}$ is the mean time spent in the state j waiting for the next transition to happen. For $N = 2$, $\overline{\tau_j}$ is simply the mean of failure/repair time distribution of the component. However, for $N > 2$, $\overline{\tau_j}$ is more complicated:

$$\overline{\tau}_j = \int_0^\infty \tau w_j(\tau) d\tau \tag{3.22}$$

This integral can be numerically integrated; however, the resulting steady-state probability may not be accurate due to varying profiles of the statistical distributions considered.

3.6 Process simulation

Barbu and Limnios(2008) presented an algorithm to simulate a trajectory of a given semi-Markov chain (SMC) in the time interval $[0, M]$. The output of their algorithm was the successive visited states and the jump times up to the time M. In this section, simulating a semi-Markov process based on the "Competing risk model" as described by Howard(1971) is presented. Assume that the process is in state i. From this state, there could be k different states to which the process could transit to in a single step. These states could be completion of a repair, further degradation of the system or a failure mode with an underlying failure mechanism. Also assumed in this model is that all these k possibilities are independent of the occurrence of each other. The process chooses only one state from these choices such that the time to be spent in the current state i is the minimum before instantaneously jumping to the chosen state. Hence, in simulation, all possible adjacent states and a sample time to be spent in the current state based on each potential successor are enumerated and the state corresponding to the minimum time is chosen. This procedure is repeated either until the mission time is reached or the process lands in a trapping state.

In a typical availability problem, if the process is in a down state at the end of the mission, then the system is considered to be unavailable and available if not. Since there is no absorbing state in such a problem, the simulation goes on until mission time is reached. This constitutes a single trial of the simulation. A sufficiently large number of such trials gives an estimate of the system availability. On the other hand, for a reliability problem, the process terminates as soon as it encounters the absorbing state flagging the system as unreliable in that trial.

3.6.1 Algorithm for process simulation

1. Variables

   S_c: The current state the process is in (operational initially)

   S_t: Target state (usually the system failure state)

   T_{ci}: Sample time spent in current state c given the successor is state i

   T_{min}: $min\{T_{c1}, T_{c2}, ...\}$

   T: Current time

T_m: Mission time (input)

x_i: Whether process is in target state at end of mission in trial i; 1(true) or 0(false)

p: a uniform random number

$inv(p, c, t)$: inverse transform of probability p based on current state c and target state t

2. Repeat until $T < T_m$

   - Choose p
   - For each state i reachable in one-step from current state S_c
     - $T_{ci} = inv(p, c, i)$
   - $T_{min} = min\{T_{c1}, T_{c2}, . . .\}$
   - If $T + T_{min} > T_m$, then exit loop
   - $S_c =$ state i corresponding to T_{min}
   - If $S_c = S_t$, then exit loop
   - $T = T + T_{min}$

3. $x_i = \begin{cases} 1 & \text{if } S_c = S_t \\ 0 & otherwise \end{cases}$

For sufficiently large number N of trials, the instantaneous unavailability of the system at time t can be calculated from x_i:

$$\widehat{Q} = 1 - \frac{1}{N}\sum_{i=1}^{N} x_i \tag{3.23}$$

If N is small, the denominator in Equation 3.23 is replaced with $N - 1$ in order to obtain an unbiased estimate of unavailability.

3.7 Example: Non-repairable system

Consider a two state non-repairable system with a failure time given by Weibull distribution with a scale parameter λ and shape parameter γ. Assume that the system starts in state 2, the functioning state. Then the kernel matrix and waiting

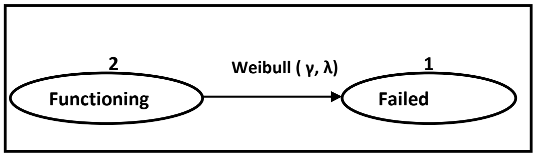


Figure 3.5: 2-state non-repairable system with a Weibull failure time distribution

time probabilities are given by:

$$C(t) = \begin{bmatrix} \delta(t-\infty) & 0 \\ f_{wbl}(t|\gamma,\lambda) & 0 \end{bmatrix} \qquad W(t) = \begin{bmatrix} 1 \\ 1 - F_{wbl}(t|\gamma,\lambda) \end{bmatrix}$$

These matrices are plugged in to the Markov renewal equation (3.9) and solved recursively for the state probabilities $\phi_{ij}(t)$ by trapezoidal rule. Refer to the appendix for the derivation of the algorithm. The time-dependent system failure probabilities are found in $\phi_{21}(t)$ since the system started in state 2 and state 1 is the state of failure. These are plotted in Figure 3.6 for $\lambda = 0.5$ and $\gamma = 1,\ 1.5,\ 2.5$. Note that the plot corresponding to $\gamma = 1$ is the same as the one in Figure 2.2 of the Markov chapter. It can also be seen that larger values of γ attain increased failure probability at an earlier time than the case when $\gamma = 1$. Since the system is not repairable, it is observed that the life time of the system does not go beyond 5 hours given that $\gamma = 1$. But, if the transition times are not exponential in real time, it is observed that the system fails in less than 5 hours.

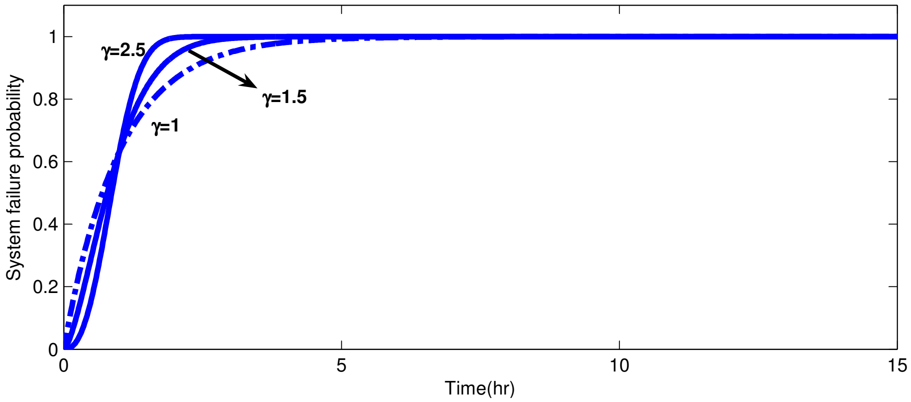


Figure 3.6: System failure probability based on semi-Markov model for Example 3.7.

3.8 Example: Repairable system

Assume that in the example above, the system is repairable (Figure 3.7) with an exponential repair time distribution holding a repair rate μ.

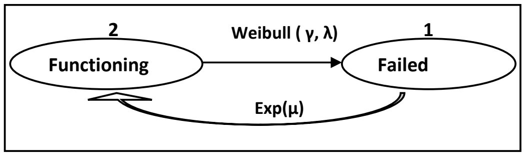


Figure 3.7: 2-state repairable system with a Weibull failure time and exponential repair time.

$$C(t) = \begin{bmatrix} 0 & \mu e^{-\mu t} \\ f_{wbl}(t|\gamma,\lambda) & 0 \end{bmatrix} \quad W(t) = \begin{bmatrix} e^{-\mu t} \\ 1 - F_{wbl}(t|\gamma,\lambda) \end{bmatrix}$$

Since there is no absorbing state for this system, it is always repairable. It is more appropriate to discuss its availability than reliability. The state probabilities are computed using Eq.(3.9). While $\phi_{21}(t)$ in Figure 3.8 represents the system unavailability, $\phi_{22}(t)$ gives the availability (Figure 3.9) of the system. Both state probabilities are conditioned that the system began its operation in state 2. The assumed parameters are $\mu = 1, \lambda = 0.5$ and $\gamma = 1$,5 and 15. Note that the variation in γ produces a substantial difference in the system unavailability. The dips and raises in the plot corresponding to low unavailability and high unavailability is due to the effect of γ along with longer repair times and higher failure rates. Moreover, since that the system is repairable, it is seen that the unavailability never reaches or stays at one. After 5 hours, the availability reaches a steady state as seen in in Figure 3.9.

3.9 Example: Repair and Redundancy

Consider two identical components connected in parallel. Let the random variables X_1 and X_2 denote time to failure of the components. Let state 2 be fully operational state, state 1 be a state with only one component working and state 0 be an absorbing state denoting state of system failure. Let both the components be

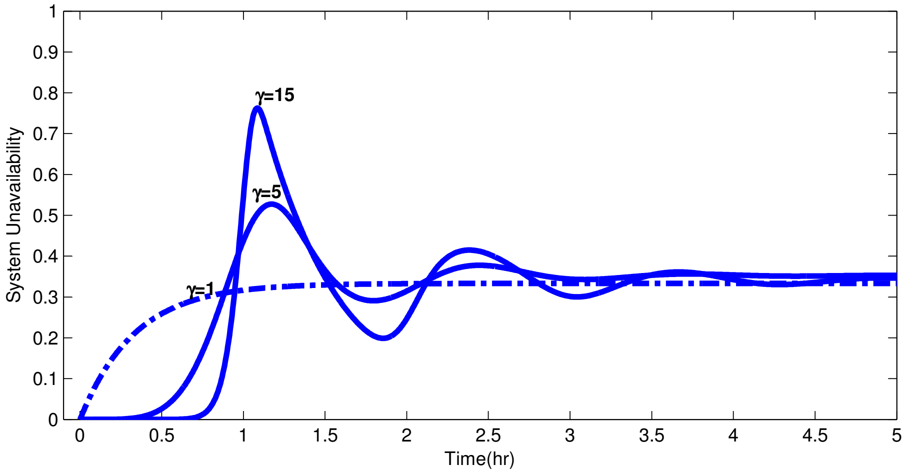


Figure 3.8: System unavailability for Example 3.8.

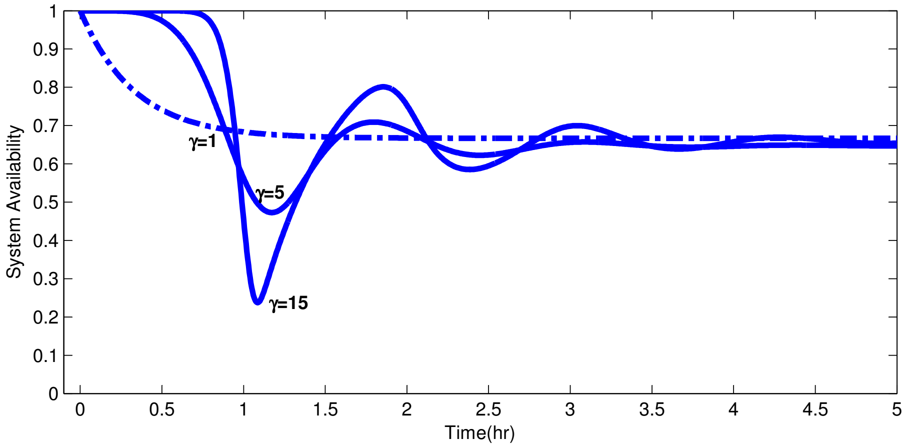


Figure 3.9: System availability for Example 3.8.

repairable. Then the transition 1 to 2 represents repair of a single failed component. Let its time to repair be denoted by Y.

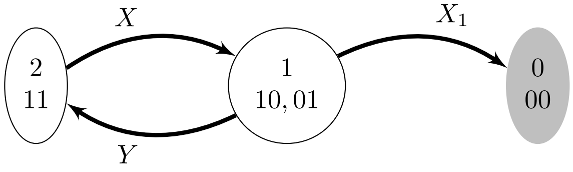


Figure 3.10: State space exemplifying time to failure.

Let X denote the time to transit from state 2 to state 1.Then,

$$X = min\{X_1, X_2\}$$

Since both the components are identical and indistinguishable, let the time to transit from state 1 to state 0 be X_1. The total time Z taken to reach state 0 from state 2 can be one of the following:

$$
\begin{aligned}
&Z = X + X_1 \\
&Z = X + Y + X + X_1 \\
&Z = X + Y + X + Y + X + X_1 \\
&Z = X + Y + X + Y + X + Y + X + X_1 \\
&\quad . \\
&\quad . \\
&Z = X + ... + X_1
\end{aligned}
$$

i.e., transition in to state 0 acts as a stopping rule for the process. Assuming that X and Y follow valid statistical distributions and are statistically independent, the sum of these finite number of random variables represents a convolution operation in continuous time. The state diagram in shown in Figure 3.10. Note that for two random variables X and Y, both not necessarily independent, density of the sum $Z = X + Y$ is given by:

$$F_{X+Y}(z) = \int_{-\infty}^{\infty} \int_{-\infty}^{z-x} F_X(x, y) dy dx \tag{3.24}$$

By assuming independence of X and Y, we arrive at a convolution operation:

$$
\begin{aligned}
F_{X+Y}(z) &= Pr\{X + Y \leq z\} \\
&= \int_{-\infty}^{\infty} Pr\{X + Y \leq z | Y = y\} dF_Y(y) \\
&= \int_{-\infty}^{\infty} Pr\{X \leq z - y\} dF_Y(y) \\
&= \int_{-\infty}^{\infty} F_X(z - y) dF_Y(y) \\
&= \int_{0}^{z} f_Y(y) F_X(z - y) dy
\end{aligned} \tag{3.25}
$$

If all the distributions are exponential, then the distribution of Z follows a gamma distribution, otherwise one has to resort to Laplace transforms, Monte Carlo simulations, saddle point approximation or other numerical techniques to arrive at the distribution of Z.

Let $F(t)$,$G(t)$, and $H(t)$ be the *cdf* of X, Y and $X1$ respectively. Then the kernel of the semi-Markov process model is given by Equation 3.5:

$$C(t) = \begin{bmatrix} 0 & 0 & 0 \\ f(t)(1-G(t)) & 0 & g(t)(1-F(t)) \\ 0 & h(t) & 0 \end{bmatrix}$$

3.10 Kernel with Weibull sojourn times

In this section, the kernel matrix of the semi-Markov process model is based on Weibull family of distributions which means that time spent in each state before a transition is made can be either a Weibull, exponential or a normal distribution. This section is needed only when there is a competing risk situation *i.e.*, a row of the core matrix at any time t has multiple non-zero entries.

A matrix of Weibull *cdf*s (say $Q(t)$) and *pdf*s (say $P(t)$) representing the transition times is constructed such that

$$Q_{ij}(t) = \begin{cases} F_T(t|\gamma_{ij}, \lambda_{ij}) & \text{if } \lambda_{ij} \neq 0 \\ 0 & \text{if } \lambda_{ij} = 0 \end{cases} \tag{3.26}$$

$$P_{ij}(t) = \begin{cases} f_T(t|\gamma_{ij}, \lambda_{ij}) & \text{if } \lambda_{ij} \neq 0 \\ 0 & \text{if } \lambda_{ij} = 0 \end{cases} \tag{3.27}$$

where it is assumed that:

$$\gamma_{ij} = 1 \text{ whenever } \lambda_{ij} = 0. \tag{3.28}$$

The kernel (3.5) of the semi-Markov process is obtained as follows. Let $R(t) = 1 - Q(t)$ and let each column i of $R_1(t)$ be the product of the columns of $R(t)$ excluding the column i. Then an element-wise product of $P(t)$ and $R_1(t)$ yields the kernel or core matrix, C. This is given as $C(t) = P(t)\Box R_1(t)$ in Howard's (1971) notation.

Consider a row i whose entries represent a competing risk situation, then for $1 \leq j, k \leq N$,

$$\int\limits_0^t \sum_j c_{ij}(t)dt \quad = \quad \int\limits_0^t \sum_j [f_{ij}(t|\gamma_{ij}, \lambda_{ij}) \prod_{k \neq j} (1 - F_{ik}(\gamma_{ik}, \lambda_{ik}))]dt$$

$$
\begin{aligned}
&= \int_0^t \sum_j [(\lambda_{ij}\gamma_{ij})(\lambda_{ij}t)^{\gamma_{ij}-1} e^{-\lambda_{ij}t^{\gamma_{ij}}} e^{-\sum\limits_{k\neq j}(\lambda_{ik}t)^{\gamma_{ik}}}]dt \\
&= \int_0^t \sum_j [(\lambda_{ij}\gamma_{ij})(\lambda_{ij}t)^{\gamma_{ij}-1} e^{-\sum\limits_{k}(\lambda_{ik}t)^{\gamma_{ik}}}]dt \\
&= -e^{-\sum\limits_{k}(\lambda_{ik}t)^{\gamma_{ik}}} + 1 \qquad (3.29)
\end{aligned}
$$

Letting t to ∞ in Equation 3.29, it is proved that the process holds the assumption in Equation 3.7.

The $W_i(t)$ in Integral Equation 3.9 based on Equation 3.8 is computed as

$$W_i(t) = 1 - (3.29) = e^{-\sum\limits_{k}(\lambda_{ik}t)^{\gamma_{ik}}} \qquad (3.30)$$

This simplified expression for $W_i(t)$ aids in fast computation of the state probabilities in the presence of numerous competing risk situations. It remains to plug-in both the matrices $C(t)$ and $W(t)$ and evaluate the state probabilities recursively using Equation 3.10 by applying the trapezoidal rule in Equation 3.14.

3.11 A typical system

Given the strengths and weaknesses of the semi-Markov process model, we look at possible approaches to quantitatively evaluate the sample reliability block diagram shown in Figure 3.11.

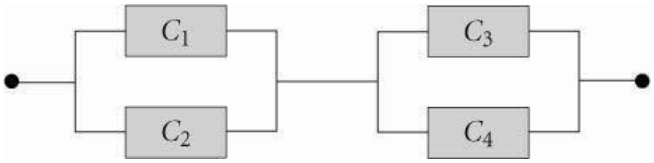


Figure 3.11: A typical parallel-series system.

Failure and repair data of the components are listed in Table 3.2. A coefficient of variation (cov) of 1 is assumed for all the repair times, though this is not a must for the analysis.

The first unsuitable way of solving this problem is to develop a single semi-Markov model with 16 states assuming binary states for each component. Though

Table 3.2: Component data for the four component example system

Component	Mean failure time, *cov* (years)	Mean repair time (years)
C1	40,1	0.5
C2	30,0.3	1
C3	30 , 1	0.5
C4	20, 0.25	1

it comprises of all possible system dynamics, this kind of modelling cannot be considered practically as a final solution to a given arbitrarily large and complex system due to state explosion.

Hence, in this thesis we look at alternative ways of solving this problem with a mixture of semi-Markov process model and probability rules.

3.11.1 Component level analysis

One option is to evaluate the availability of each component and use probability rule to arrive at the system availability. Lisnianski et al. (2003) explored this option by proposing an extended reliability block diagram method in which each block of the diagram embeds a multi-state semi-Markov model for the corresponding component.

For component C1, a state space with two states is considered as seen in Figure 3.12. State 1 is working state and 0 is the failed state. The transition 1→0 represents a component failure. The mean life and *cov* of time to failure of C1 are listed as the label for the edge connecting 1 and 0. Similarly, the label for the transition 0→1 represents the mean repair time along with *cov* of time to repair. The failure and repair distributions are not part of the label. This facilitates the flexibility to assume any arbitrary distribution at a later time.

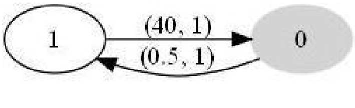


Figure 3.12: State-space diagram for component C1

Let $f_{ij}(t)$ and $g_{ij}(t)$ be the failure and repair *pdf* respectively for the transitions in Figure 3.12 corresponding to the mean and *cov* parameters listed along the edges of the transitions in the figure. Then arranging these in a matrix, we get the kernel matrix:

$$C(\tau) = \begin{bmatrix} 0 & g_{01}(\tau) \\ f_{10}(\tau) & 0 \end{bmatrix} \tag{3.31}$$

Summing up the kernel matrix elements column-wise, we get the waiting time matrix:

$$w(\tau) = \begin{bmatrix} g_{01}(\tau) \\ f_{10}(\tau) \end{bmatrix} \tag{3.32}$$

$W(t)$ is evaluated using the waiting time matrix:

$$W(t) = \begin{bmatrix} 1 \\ 1 \end{bmatrix} - \int_0^t \begin{bmatrix} g_{01}(\tau) \\ f_{10}(\tau) \end{bmatrix} d\tau \tag{3.33}$$

Assuming that the component begins its operation from state 1, the probability of being in state 0 denoted by $\phi_{10}(t)$ gives unavailability of C1. $Q_2(t), Q_3(t), Q_4(t)$ are similarly obtained for rest of the components.

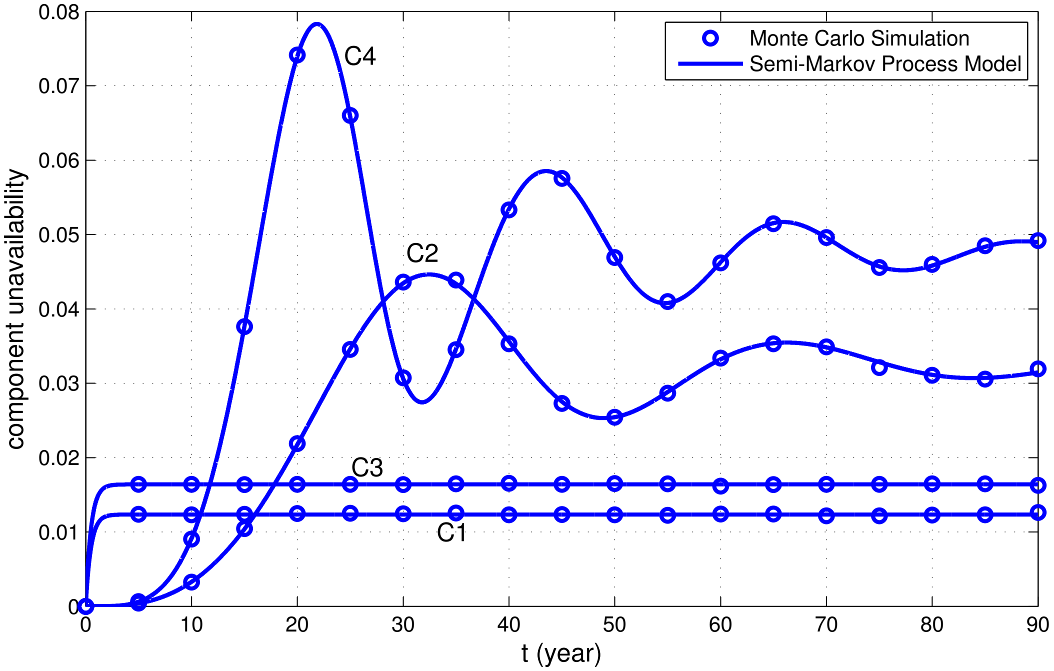


Figure 3.13: Component unavailability of individual components.

In all the cases, Weibull distribution is assumed for time-to-failure and exponential distribution for repair time. Figure 3.13 shows the unavailability of individual components based on solving the integral equations using trapezoidal rule and validated using process simulation. The simulations were performed with 500,000 trials for the hypothetical system. Availability of the entire system can be evaluated using Equation 3.34:

$$A_s(t) = \{1 - \prod_{i=1}^{2} Q_i(t)\}\{1 - \prod_{i=3}^{4} Q_i(t)\} \tag{3.34}$$

Then, system unavailability is $1 - A_s(t)$.

3.11.2 Steady state probabilities for component level analysis

In this section, steady state probabilities are illustrated for component C1. For the analysis at the component level, mean waiting time need not be computed explicitly. It is the mean of the component failure/repair distribution.

For each component Markov model as in Figure 3.12, the transition probabilities are given as 1 for the transitions 0→1 and 1→0:

$$P = [p_{ij}] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{3.35}$$

The imbedded Markov chain stationary distribution is determined by solving the following set of equations:

$$\pi_0 = \pi_0 p_{00} + \pi_1 p_{10} \tag{3.36}$$

$$\pi_1 = \pi_0 p_{01} + \pi_1 p_{11} \tag{3.37}$$

$$\pi_0 + \pi_1 = 1 \tag{3.38}$$

Since the stationary chain depends only on the transition probability matrix, it is the same for all the components:

$$\pi = [\pi_j] = \begin{bmatrix} 0.5000 & 0.5000 \end{bmatrix} \tag{3.39}$$

Finally, the steady state probabilities can be computed using Equation 3.21:

$$\phi = [\phi_j] = \begin{bmatrix} 0.0123 & 0.9877 \end{bmatrix} \tag{3.40}$$

i.e., No matter in which state component C1 starts initially, its steady state unavailability is 0.0123. Component 1 has an availability of 0.9877. Steady state unavailability of all the components is listed in Table 3.3.

Table 3.3: Steady state unavailability of components

Component	Steady State Unavailability
C1	0.0123
C2	0.0323
C3	0.0164
C4	0.0476

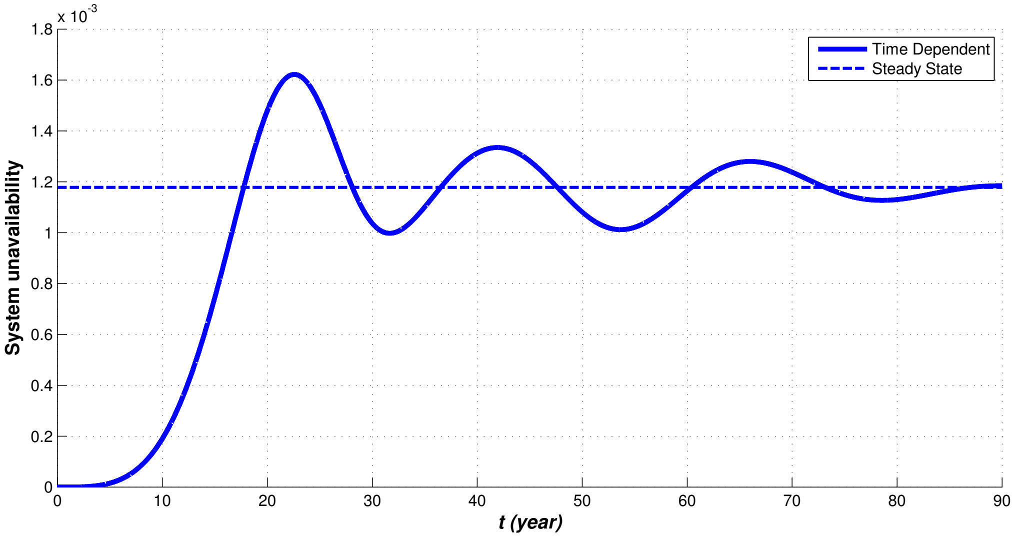


Figure 3.14: System unavailability from components

The steady state system unavailability of the system based on Equation 3.34 without the time dependence can be computed as 0.00118. Plots for time-dependent and steady state system unavailability are plotted in Figure 3.14. A plot of the normalized system unavailability with Weibull, gamma and lognormal failure distributions and exponential repair distribution are shown in Figure 3.15.

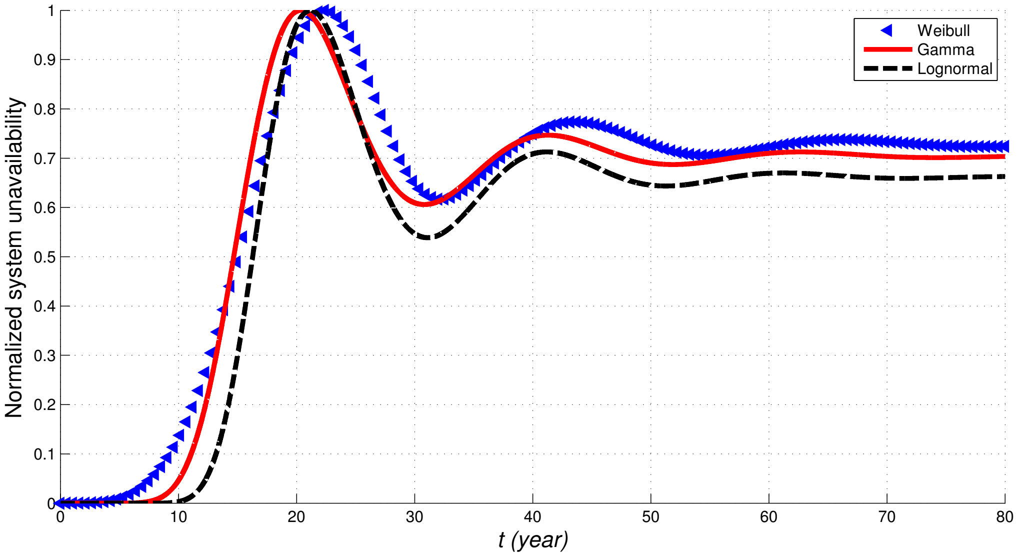


Figure 3.15: Normalized system unavailability with various distributions (Component level analysis)

3.11.3 Subsystem level analysis

An alternative option to preserve the system dynamics to the possible extent is to evaluate availability of each subsystem by semi-Markov technique and then compose the system results using the probability rule. An advantage of this method is that common cause failure can be integrated into the model.

In the example considered, there are two subsystems - {C1, C2} and {C3, C4}. For N=2, the four possible states 0,2,1,3 are 00, 10, 01, 11 representing total system failure (00), only component 1 working (10), only component 2 working (01), and both working normally (11) respectively. A system transition represents a change in the state of a single component. In the example, 3→2 means that component 2 has failed and 1→3 means that component 1 has been repaired. 3→0, if exists represents a

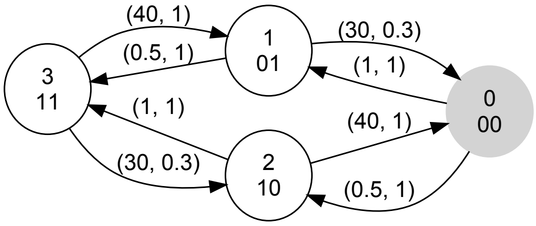


Figure 3.16: State-space diagram for subsystem 1

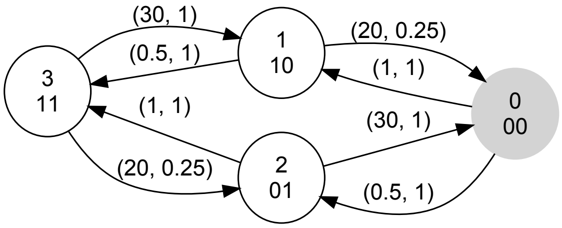


Figure 3.17: State-space diagram for subsystem 2

common cause failure. Figures 3.16 and 3.17 show the state-space models for both the subsystems. Assuming that both the subsystems start operating from state 3, $\phi_{30}(t)$ represents subsystem unavailability. Let these be represented by $Q_1(t)$ and $Q_2(t)$ for subsystem1 and subsystem2 respectively. Then the system unavailability $Q_s(t)$ is given by:

$$Q_s(t) = Q_1(t) + Q_2(t) - Q_1(t)Q_2(t) \tag{3.41}$$

Let $f_{ij}(t)$ and $g_{ij}(t)$ be the failure and repair *pdf* respectively for the transitions corresponding to the state space diagram. These are arranged as shown below:

$$f(\tau) = \begin{bmatrix} 0 & g_{01}(\tau) & g_{02}(\tau) & 0 \\ f_{10}(\tau) & 0 & 0 & g_{13}(\tau) \\ f_{20}(\tau) & 0 & 0 & g_{23}(\tau) \\ 0 & f_{31}(\tau) & f_{32}(\tau) & 0 \end{bmatrix} \tag{3.42}$$

Let $F_{ij}(t)$ and $G_{ij}(t)$ be the corresponding *cdf*. Then the kernel of the semi-Markov process model takes the following form:

$$C(\tau) = \begin{bmatrix} 0 & g_{01}(\tau)(1 - G_{02}(\tau)) & g_{02}(\tau)(1 - G_{01}(\tau)) & 0 \\ f_{10}(\tau)(1 - G_{13}(\tau)) & 0 & 0 & g_{13}(\tau)(1 - F_{10}(\tau)) \\ f_{20}(\tau)(1 - G_{23}(\tau)) & 0 & 0 & g_{23}(\tau)(1 - F_{20}(\tau)) \\ 0 & f_{31}(\tau)(1 - F_{32}(\tau)) & f_{32}(\tau)(1 - F_{31}(\tau)) & 0 \end{bmatrix}$$

The equation for not leaving each state up to time t is written as:

$$W(t) = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} - \int_0^t \begin{bmatrix} g_{01}(\tau)(1 - G_{02}(\tau)) + g_{02}(\tau)(1 - G_{01}(\tau)) \\ f_{10}(\tau)(1 - G_{13}(\tau)) + g_{13}(\tau)(1 - F_{10}(\tau)) \\ f_{20}(\tau)(1 - G_{23}(\tau)) + g_{23}(\tau)(1 - F_{20}(\tau)) \\ f_{31}(\tau)(1 - F_{32}(\tau)) + f_{32}(\tau)(1 - F_{31}(\tau)) \end{bmatrix} d\tau \tag{3.43}$$

The kernel and $W(t)$ are sufficient to calculate the state probabilities using the Markov renewal equations. Assuming that each subsystem begins its operation in working state 3, the probability of being in state 0 denoted by $Q_1(t) = \phi_{30}(t)$ gives subsystem1 unavailability. $Q_2(t)$ is similarly obtained for subsystem 2. Based on Equation 3.41, system unavailability can be determined as $1 - A_s(t)$.

Figure 3.18 shows the unavailability of both the subsystems assuming Weibull distribution for time-to-failure and exponential distribution for repair time. System unavailability is also shown in the same figure.

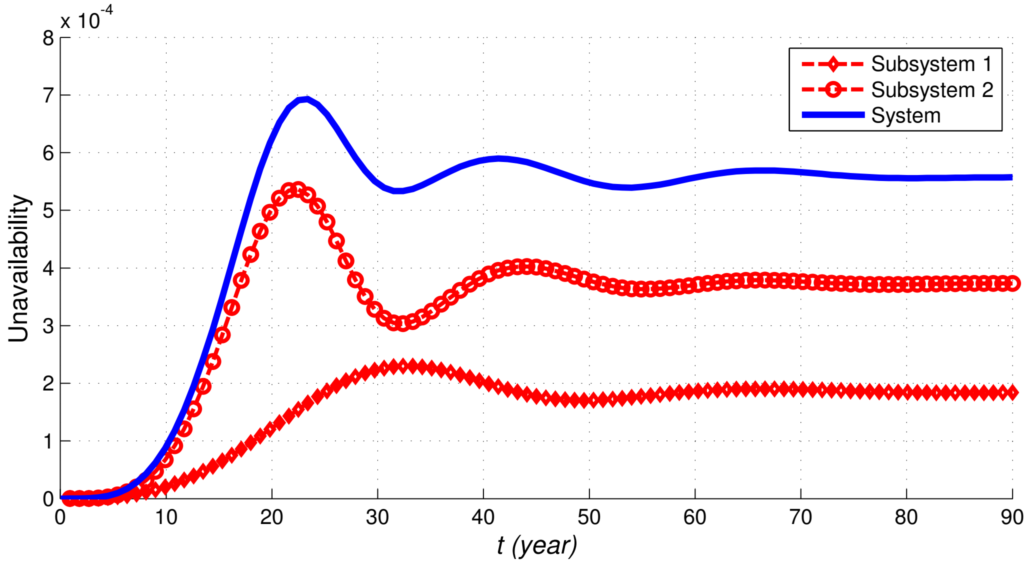


Figure 3.18: Subsystem and system unavailability

The system unavailability plots in Figures 3.14 and 3.18 based on component and subsystem level analysis respectively do not yield the same results. The reason for this discrepancy is the fact that semi-Markov process model is a Markov process model at the time instants of state jumps, yet not a Markov process since the time spent in a state can follow a non-exponential distribution. The selection of successor state is based on the Markov chain property and not on the time spent in the previous state. If repair of component 1 starts in state 1 in Figure 3.16, state 0 does not consider this time spent already in repair, rather, repair of one of the two components begins in state 0. But, ideally repair of component 1 must be continued in state 0 and the system must be brought online following the completion of repair. Hence, in the rest of the thesis system availability analysis in the presence of redundant units is not considered. However, it will be demonstrated through the NCCW system that reliability analysis in the presence of redundant parallel units yields accurate results. The next section delves deeper in to the problems carried forward by semi-Markov process model from the Markov process model.

3.12 Regenerative stochastic processes

Markov and renewal processes come under a general class of processes called regenerative processes. There are random points on the time axis called regeneration points, the behaviour of the system after which is independent of its past operation. The system is said to regenerate or renew itself past this point and the time between any two regeneration points called an 'nth-cycle' is considered as a random variable holding a statistical distribution. These cycles are assumed to be independent, otherwise, behaviour of the system structure could become mathematically complicated. Also note that the moment the system begins its operation initially, which usually is zero, is also a regeneration point.

In an ordinary renewal process, the point when system fails and is instantaneously replaced by a new one is a regeneration point called the 'renewal point'. After a renewal, the system becomes 'as good as new' and follows the same probabilistic law as before the renewal.

In an alternating renewal process, a single regeneration cycle consists of a failure and a repair *i.e*, time until failure and subsequently the time until completion of repair together forms a cycle. The time instant at which repair is completed is a regeneration point. The distribution of sum of the random variables representing the time to failure and time to repair is given by convolution operation. This same distribution is replicated for every regeneration cycle until the desired mission time.

The Markov process model is based on the 'memoryless' property. If current state of the process is known, then the knowledge of the past states does not hold a predictive value. This can be seen from the definition of discrete time Markov chain:

$$P(X(t_{n+1}) = i_{n+1}|X(t_n) = i_n, X(t_{n-1}) = i_{n-1}, ..., X(t_0) = i_0)$$
$$= P(X(t_{n+1}) = i_{n+1}|X(t_n) = i_n) \tag{3.44}$$

i.e., the probability of being in state i_{n+1} at time t_{n+1} is dependent only on the fact that the system is in state i_n at time t_n. Moreover, the time spent in any state follows an exponential distribution which is characterized by the memoryless property:

$$P(T > t + t_2|T > t) = P(T > t_2) \tag{3.45}$$

i.e., the probability that a system will be reliable for t_2 more time units is the same as the conditional probability that it is reliable for t_2 more time units given that it was reliable until time t. Since the system forgets about its past, it does not keep track of its age and starts anew each time it transits to a different state. Hence all states of a Markov process model are regenerative states and the time instant at which the state transition happens is a regeneration point.

To illustrate this point, consider a three state system shown in Figure 3.19 with two identical components A and B. Let A be functioning and B be under repair *i.e.*, let the system be in state 1. Assume that A fails and the process steps in to state 0 where both the components are non-operating. In an ideal case the repair of B must continue and system must be brought online as soon as the repair is completed. However, due to the memoryless property, the process forgets that in the earlier state, B had already undergone a partial repair and begins repairing one of them in state 0. This flaw is a consequence of the Markov property in Equation 3.44 *i.e.*, the time spent in repairing the component B while in state 0 has nothing to do with the partial time spent on repairing it in state 1.

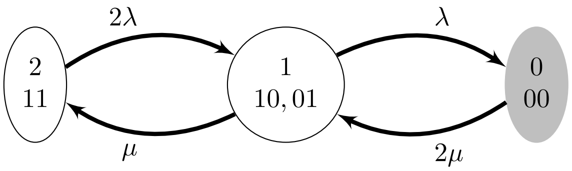


Figure 3.19: A three state Markov model for 2-unit redundant system

As per Gulland(2003), this flaw is rectified by assuming that there are two repair men repairing each component independently. This is achieved by halving the repair time which is equivalent to doubling the repair rate corresponding to the transition from state 0 to state 1. In this sense, the associated transition rate is 2μ instead of μ. An alternative reasoning would be that the time to get the system online is the minimum of the repair times of the two components leading to an exponential distribution with mean as the sum of the repair rates of the individual components.

This anomaly can be seen by comparing the steady state probabilities obtained through the Markov and probability rule approaches. The steady state unavailability of both the components is given by $Q_A = Q_B = \frac{\lambda}{\lambda+\mu}$. Assuming that the repair time is much smaller compared to the failure time *i.e.*, $\mu >> \lambda$, the steady state unavailability Q_m by Markov method and the system unavailability Q_p by probability rule respectively are:

$$Q_m = \frac{2\lambda^2}{2\lambda^2 + 2\lambda\mu + \mu^2} \approx 2\left(\frac{\lambda}{\mu}\right)^2 \tag{3.46}$$

$$Q_p = Q_A Q_B = \left(\frac{\lambda}{\lambda+\mu}\right)^2 \approx \left(\frac{\lambda}{\mu}\right)^2 \tag{3.47}$$

Note that when μ is assumed for the transition $0 \rightarrow 1$, Q_m is twice that of Q_p. However when 2μ is assumed for this transition, the corrected Q_m is:

$$Q_m = \frac{2\lambda^2}{2\lambda^2 + 2\lambda\mu + 2\mu^2} \approx \left(\frac{\lambda}{\mu}\right)^2 \tag{3.48}$$

A detailed account of this flaw including the analysis of k-out-of-n systems is discussed in Gulland(2003).

Semi-Markov process is a generalization of Markov process in the sense that it is based upon the Markov chain in selecting the successor state. It follows the Markov property at the instant of state transition also called the 'epoch' of transition. It departs from the Markov process because the time spent in the state need not be exponentially distributed. Markov renewal process is based on generalized random variables dealing with the count of visits to each state of the process while semi-Markov process assumes each state visited by the process is itself a random variable. However, both the processes are considered equivalent from the viewpoint of probability theory (Birolini, 2007). Hence a semi-Markov process model is a regenerative stochastic process and if at least one of the states is not a regeneration point, then the process ceases to be a semi-Markov process, rather, it is a semi-regenerative process with an embedded semi-Markov process. For a two-state model of a repairable component, both the states are points of regeneration since this model corresponds to an alternating renewal process.

Usually, the system up-states are regeneration states, while the down-states are not. Even for a simple system with more than two states in the model, the assumption of arbitrary failure and repair times leads to a non-regenerative stochastic process (Birolini, 2007). For example, consider the two component redundant system in Figure 3.19. In this model, if failure time is assumed to follow Weibull distribution, then states 1 and 2 are regenerative states, but state 0 is not because the time spent in state 0 is dependent on how long the repair activity went on in state 1. Hence, the following system of integral equations based on the state diagram in Figure 3.19 does not yield the appropriate system unavailability:

$$\begin{aligned}
\phi_{20}(t) =& \int_0^t C_{21}(\tau)\phi_{10}(t-\tau)d\tau \\
\phi_{10}(t) =& \int_0^t C_{10}(\tau)\phi_{00}(t-\tau)d\tau + \int_0^t C_{12}(\tau)\phi_{20}(t-\tau)d\tau \\
\phi_{00}(t) =& W_0(t) + \int_0^t C_{01}(\tau)\phi_{10}(t-\tau)d\tau
\end{aligned} \tag{3.49}$$

To work around the problem of dealing with a non-regenerative point with arbitrary transition distribution, Birolini (2007) suggested modifying the integral equations by considering a loop from state 1 to itself assuming a single repairman. In this case when component A fails while B is under repair, it waits for the completion of repair of B and then jumps back to state 1 and starts repair of component A. There are two problems with this approach, firstly, standard approach in reliability analysis is to assume independent repair crew; secondly, dealing with non-regenerative points varies with each problem.

While it seems lucrative that semi-Markov process model can handle arbitrary sojourn time distributions, there comes an extra clause that all states must be regenerative. Hence this technique does not offer a standard boilerplate solution to any given reliability block diagram assuming independent repair crew and arbitrary transition time distributions.

However, semi-Markov process model has potential in dealing with first failure of small systems which are a mixture of repairable and non-repairable components. It can also deal with degrading systems that eventually fail and are non-repairable.

In rest of the chapter, such systems will be considered as independent case studies.

3.13 State Reduction Techniques for Semi-Markov Process Models

Consider n components connected in series as shown in the Reliability Block Diagram in Figure 3.20. Each component has a reliability R_i. Then, assuming that each of these components fails according to exponential distribution with a failure rate of λ_i, the reliability R_s of this system also follows an exponential distribution:

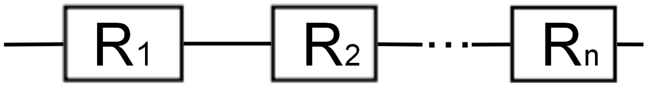


Figure 3.20: Reliability Block Diagram for n Components in series.

$$\begin{aligned} R_s(t) =& R_1(t)R_2(t)...R_n(t) \\ =& e^{-\lambda_1 t}e^{-\lambda_2 t}...e^{-\lambda_n t} \\ =& e^{-\left(\sum_{i=1}^{n}\lambda_i\right)t} \end{aligned} \tag{3.50}$$

In a Markov model, this feature acts as a state reduction technique. If a system has complex network of parallel and series combination of components, an entire subsystem of the form shown in Figure 3.20 can be reduced to a single block with a failure rate of sum of the failure rates of the components connected in series.

However, in an SMP model, when Weibull distribution is assumed for failure/repair time, this elegance is lost. The product of Weibull distributions is not a Weibull distribution, rather another distribution called the *poly-Weibull* distribution:

$$R_s(t) = e^{-\left(\sum_{i=1}^{n}(\lambda_i t)^{\gamma_i}\right)} \tag{3.51}$$

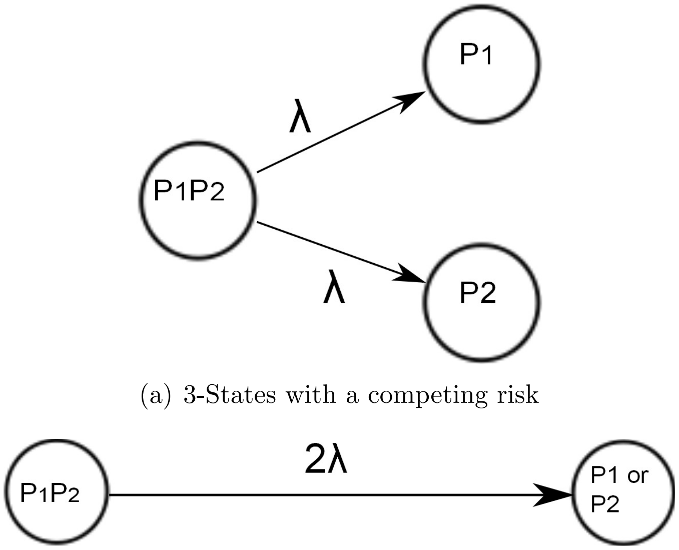
Then, the *cdf* of the poly-Weibull distribution is given by $1 - R_s(t)$:

$$F(t) = 1 - e^{-\sum_{q=1}^{n}(\lambda_q t)^{\gamma_q}} \tag{3.52}$$

pdf is found by differentiating $F(t)$ $w.r.t.$ t:

$$f(t) = \sum_{p=1}^{n}[(\lambda_p \gamma_p)(\lambda_p t)^{\gamma_p - 1}]e^{-\sum_{q=1}^{n}[(\lambda_q t)^{\gamma_q}]} \tag{3.53}$$

Another instance of state reduction is a competing risk situation (Figure 3.21). Consider two identical pipes connected in parallel each of which has a failure rate λ. Let P_1P_2 be the state in which both the pumps are in working condition. When pump 1 fails, the process moves to state P_2 and when pump 2 fails, the process moves to state P_1. Let the process be in state P_1P_2 initially. Let T_1 and T_2 be the random variables representing the random time taken to transit to state P_1 and P_2 respectively. The process chooses the successor state based on the minimum time taken to transit *i.e.* according to the rule $min\{T_1, T_2\}$. In general, if $T_1, T_2, ...T_n$ are n independent exponentially distributed random variables arising out of a competing risk situation, $min\{T_1, T_2, ..., T_n\}$ turns out to be an exponential



(a) 3-States with a competing risk

(b) 3-States reduced to 2-States with no competing risk

Figure 3.21: Dealing with identical parallel components.

distribution with mean $n\lambda$ as can be seen in the following derivation:

$$\begin{aligned} Pr(min\{T_1, T_2, ..., T_n\} > t) =& Pr(T_1 > t \text{ and } T_2 > t \text{ and ... and } T_n > t) \\ =& \prod_{i=1}^{n} Pr(T_i > t) \\ =& \prod_{i=1}^{n} e^{(-\lambda t)} \\ =& e^{-t \sum_{i=1}^{n} \lambda} \\ =& e^{-n\lambda t} \end{aligned} \tag{3.54}$$

Hence, in a competing risk situation involving identical components connected in parallel, state reduction in a Markov model can be achieved by considering a state transition with a transition rate of *failure rate * number of parallel components.* For example, the 3-state model in Figure 3.21(a) can be replaced by a simple model shown in Figure 3.21(b). Similarly, when Weibull failure times are considered, Equation 3.54 turns out to be poly-Weibull distribution:

$$\begin{aligned} Pr(min\{T_1, T_2, ..., T_n\} > t) =& \prod_{i=1}^{n} e^{-(\lambda t)^{\gamma}} \\ =& e^{-\sum_{i=1}^{n} (\lambda t)^{\gamma}} \\ =& e^{-n(\lambda t)^{\gamma}} \end{aligned} \tag{3.55}$$

Such adjustments of transition rates also occur in modeling $k-out-of-n$ systems, load-sharing systems etc.

Now that poly-Weibull distribution is identified as an ideal distribution to achieve state reduction in SMP models, in what follows, it is proved that an SMP model's kernel can be entirely built using poly-Weibull distribution.

Let transition from a state i to a state j follow a poly-Weibull distribution made of a mixture of n Weibull distributions. If $n = 1$, distribution is a regular Weibull distribution.

Consider a row i whose entries represent a competing risk situation, then for $1 \leq j, k \leq N$.

Then $\int\limits_0^t \sum\limits_j c_{ij}(t)dt$

$$
\begin{aligned}
&= \int\limits_0^t \sum_j [f_{ij}(t) \prod_{k \neq j} (1 - F_{ik}(t))]dt \\
&= \int\limits_0^t \sum_j [\sum_{p=1}^{m_{ij}} (\lambda_{ijp}\gamma_{ijp})(\lambda_{ijp}t)^{\gamma_{ijp}-1} e^{-\sum\limits_{q=1}^{m_{ij}} (\lambda_{ijq}t)^{\gamma_{ijq}}} \prod_{k \neq j} e^{-\sum\limits_{q=1}^{m_{ik}} (\lambda_{ikq}t)^{\gamma_{ikq}}}]dt \\
&= \int\limits_0^t \sum_j [\sum_{p=1}^{m_{ij}} (\lambda_{ijp}\gamma_{ijp})(\lambda_{ijp}t)^{\gamma_{ijp}-1} e^{-\sum\limits_{q=1}^{m_{ij}} (\lambda_{ijq}t)^{\gamma_{ijq}}} e^{-\sum\limits_{k \neq j} \sum\limits_{q=1}^{m_{ik}} (\lambda_{ikq}t)^{\gamma_{ikq}}}]dt \\
&= \int\limits_0^t \sum_j [\sum_{p=1}^{m_{ij}} (\lambda_{ijp}\gamma_{ijp})(\lambda_{ijp}t)^{\gamma_{ijp}-1} e^{-\sum\limits_{k} \sum\limits_{q=1}^{m_{ik}} (\lambda_{ikq}t)^{\gamma_{ikq}}}]dt \\
&= \int_0^X e^{-X} dX \\
&= -\, e^{-X} + 1 \qquad (3.56)
\end{aligned}
$$

where

$$
\begin{aligned}
X &= \sum_k \sum_{q=1}^{m_{ik}} (\lambda_{ikq}t)^{\gamma_{ikq}} \text{ so that} \\
dX &= \sum_k \sum_{q=1}^{m_{ik}} (\lambda_{ijq}\gamma_{ijq})(\lambda_{ijq}t)^{\gamma_{ijq}-1} dt
\end{aligned}
$$

Letting t to ∞ in Equation 3.56, it is proved that the process holds the assumption in Equation 3.7.

The $W_i(t)$ in Integral Equation 3.9 based on Equation 3.8 is computed as

$$
W_i(t) = 1 - (3.56) = e^{-X} = e^{-\sum\limits_k \sum\limits_{q=1}^{m_{ik}} (\lambda_{ikq}t)^{\gamma_{ikq}}} \qquad (3.57)
$$

This simplified expression for $W_i(t)$ aids in fast computation of the state probabilities in the presence of numerous competing risk situations. It remains to plug-in both the matrices $C(t)$ and $W(t)$ and evaluate the state probabilities recursively using Equation 3.10 by applying the trapezoidal rule in Equation 3.14.

3.13.1 Example

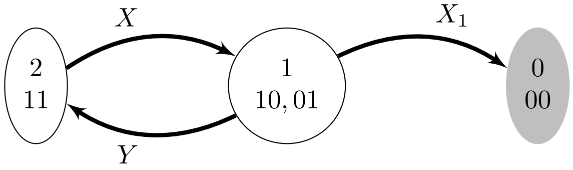


Figure 3.22: State space exemplifying state reduction.

Consider two identical components connected in parallel. Let the random variables X_1 and X_2 denote time to failure of the components. Let state 2 be fully operational state, state 1 be a state with only one component working and state 0 be an absorbing state denoting state of system failure. Let both the components be repairable. Then the transition 1 to 2 represents repair of a single failed component. Let its time to repair be denoted by Y.

Let X denote the time to transit from state 2 to state 1.Then,

$$X = min\{X_1, X_2\}$$

Since both the components are identical and indistinguishable, let the time to transit from state 1 to state 0 be X_1. Let X_1 and X_2 follow Weibull distribution whose *pdf* is denoted by $f(t)$. Then X follows a poly-Weibull distribution with *pdf* $h(t)$:

$$h(t) = 2(\lambda\gamma)(\lambda t)^{\gamma-1}e^{-2(\lambda t)^\gamma}$$

and the reliability function

$$H(t) = e^{-2(\lambda t)^\gamma}$$

Finally, let Y follow an exponential distribution with mean μ and *pdf* denoted by $g(t)$. Then the kernel of the semi-Markov process model is given using Equation

3.5:

$$C(t) = \begin{bmatrix} 0 & 0 & 0 \\ f(t)(1-G(t)) & 0 & g(t)(1-F(t)) \\ 0 & h(t) & 0 \end{bmatrix}$$

The matrix $W(t)$ in Equation 3.8 is given as per Equation 3.57:

$$W(t) = \begin{bmatrix} 1 \\ e^{-\mu t-(\lambda t)^{\gamma}} \\ H(t) \end{bmatrix}$$

3.14 Discrete-time Semi-Markov Process (DTSMP) Model

3.14.1 Introduction

In continuous time semi-Markov process model, continuous statistical distributions are used as kernel entries and the accuracy of the state probabilities depends on how closely the time points are spaced. On the other hand DTSMP model involves discrete holding time distributions. Since discrete distributions are evaluated for discrete time points, the DTSMP method is much faster than its continuous counterpart. Howard (1971) developed a discrete version of SMP model that can include arbitrary discrete distributions for holding times.

The continuous Markov renewal equation 3.9 is discretized as follows:

$$\phi(n) =^{>} W(n) + \sum_{m=0}^{n} [P.H(m)]\phi(n-m) \tag{3.58}$$

where $n = 0, 1, 2, 3, ...$ The period in the above expression represents an element-wise multiplication of the matrices. All the required variables and matrices are listed in Table 3.4.

It is seen that the core matrix is written as a product of one-step transition probabilities and holding time densities. One-step transition probabilities are often found from data as:

$$p_{ij} = \frac{\text{Number of transitions from state } i \text{ to state } j}{\text{Total number of transitions from state } i} \tag{3.59}$$

Table 3.4: Notation used in Howard's (1971) formulation of DTSMP.

Notation	Meaning	Remarks
p_{ij}	Transition probability. Current state i, the probability that next state is j	-
τ_{ij}	Random variable denoting time spent in i before going to j	-
$h_{ij}(n) =$ $P\{\tau_{ij} = n\}$	*Holding time.* Probability that n time units is spent in i before transiting to j.	Any discrete distribution
${}^{\leq}h_{ij}(n) =$ $P\{\tau_{ij} <= n\}$	*cumulative holding time.*Probability that n or fewer time units is spent in i before transiting to j.	$\sum_{m=0}^{n} h_{ij}(m)$
${}^{>}h_{ij}(n) =$ $P\{\tau_{ij} > n\}$	*complementary cumulative holding time.*Probability that more than n time units is spent in i before transiting to j.	$\sum_{m=n+1}^{\infty} h_{ij}(m) =$ $1 -^{\leq} h_{ij}(n)$
$w_i(n) =$ $P\{\tau_i = n\}$	*Waiting time.* Probability that n time units is spent in i before transiting to an unknown state.	$\sum_{j=1}^{N} p_{ij} h_{ij}(n)$
${}^{\leq}w_i(n) =$ $P\{\tau_i <= n\}$	*cumulative waiting time.*Probability that n or fewer time units is spent in i before transiting to unknown state.	$\sum_{m=0}^{n} w_i(m) =$ $\sum_{j=1}^{N} p_{ij} {}^{\leq}h_{ij}(n)$
${}^{>}w_i(n) =$ $P\{\tau_i > n\}$	*complementary cumulative waiting time.*Probability that more than n time units is spent in i before transiting to unknown state.	$\sum_{m=n+1}^{\infty} w_i(m) =$ $\sum_{j=1}^{N} p_{ij} {}^{>}h_{ij}(n)$
$\phi_{ij}(n)$	Interval transition probability. Probability of being in state j at time n given that the state was in state i at time 0	computed from Markov renewal equation
P	Transition probability matrix	$\{p_{ij}\}$
$H(n)$	Holding time matrix	$\{h_{ij}(n)\}$
$P.H(m)$	Holding time weighted by transition probability. Element-wise multiplication	$\{p_{ij} h_{ij}(m)\}$
${}^{>}W(n)$	complementary cumulative waiting time diagonal matrix	$\{\delta_{ij} \; {}^{>}w_i(n)\}$
$\phi(n)$	state probability matrix	$\{\phi_{ij}(n)\}$

Most noted discrete holding time distribution is the discrete Weibull distribution

(Nakagawa and Osaki, 1975b) :

$$W_{q,b}(0) = 0 \tag{3.60}$$

$$W_{q,b}(\gamma) = q^{(\gamma-1)^b} - q^{\gamma^b}, \qquad \gamma \geq 1 \tag{3.61}$$

where q, b are the scale and shape parameters respectively. Khan et al. (1989) presented a method to estimate the parameters for the distribution. Further, they established an equivalence between the parameters of the continuous Weibull and the discrete Weibull distributions.

For $\gamma = 1$, this distribution reduces to geometric distribution:

$$g(0) = 0 \tag{3.62}$$

$$g(\gamma) = q^{(\gamma-1)}(1-q), \qquad \gamma \geq 1 \tag{3.63}$$

$$= p(1-p)^{(\gamma-1)} \qquad \text{where } p + q = 1 \tag{3.64}$$

However, one has to resort to approximation techniques to compute mean and variance of the discrete Weibull distribution. Perman et al. (1997) applied SMP model to power plant reliability analysis. They fit semi-Markov model with discretized Weibull distributed holding-times to actual power-plant operating data.

Due to less or no availability of detailed failure data in terms of state transitions, the DTSMP method, though much faster, is not suitable for highly reliable systems with scanty data. Moreover collection of data at different states requires more inspection and data storage investments.

3.14.2 Example - A three-state system

Barbu et al. (2004) defined DTSMP model and proposed a computational procedure based on convolution inverse method for solving the Markov renewal equation along with methods to compute the reliability and related measures. There has been no mention of why a new convolution inverse method is needed to solve the DTSMP renewal equations or how it is superior to Howard's (1971) original work.

The example considered here is taken from their work and the results are verified against the published results. However, Howard's (1971) method is followed to solve the Markov renewal equation.

Consider the state space shown in Figure 3.23 to be partitioned in to the up-state set $U = \{1, 2\}$ and down-state set $D = \{3\}$.

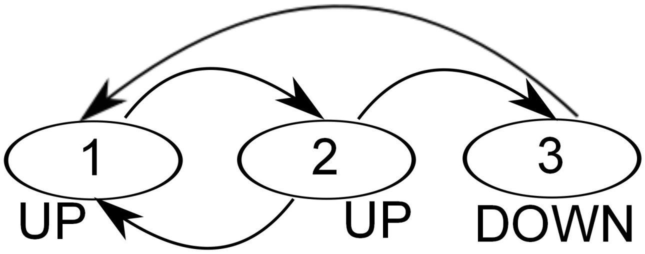


Figure 3.23: System state space.

The system is initially conditioned to be in the up-state 1 with the transition probability matrix P:

$$P = \begin{bmatrix} 0 & 1 & 0 \\ a & 0 & b \\ 1 & 0 & 0 \end{bmatrix}$$

where $a = 0.7$ and $b = 0.3$.

Assume the following discrete conditional holding times in each state before moving to the successor state:

$$H(n) = \begin{bmatrix} 0 & h_{12}(n) & 0 \\ h_{21}(n) & 0 & h_{23}(n) \\ h_{31}(n) & 0 & 0 \end{bmatrix}$$

Then, the kernel $C(n)$ is given by

$$C(n) = P.H(n) = \begin{bmatrix} 0 & h_{12}(n) & 0 \\ ah_{21}(n) & 0 & bh_{23}(n) \\ h_{31}(n) & 0 & 0 \end{bmatrix}$$

The waiting time matrix is given by summing up the column entries of the kernel:

$$W(n) = \begin{bmatrix} h_{12}(n) \\ ah_{21}(n) + bh_{23}(n) \\ h_{31}(n) \end{bmatrix}$$

The complementary cumulative holding time matrix ${}^{>}H(n)$ is given by

$$
{}^{>}H(n) = \begin{bmatrix} 0 & 1 - \sum_{m=1}^{n} h_{12}(m) & 0 \\ 1 - \sum_{m=1}^{n} h_{21}(m) & 0 & 1 - \sum_{m=1}^{n} h_{23}(m) \\ 1 - \sum_{m=1}^{n} h_{31}(m) & 0 & 0 \end{bmatrix}
$$

Then the complementary cumulative diagonal waiting time matrix ${}^{>}W(n)$ follows

$$
{}^{>}W(n) = diag\left(\begin{bmatrix} 1 - \sum_{m=1}^{n} h_{12}(m) \\ a(1 - \sum_{m=1}^{n} h_{21}(m)) + b(1 - \sum_{m=1}^{n} h_{23}(m)) \\ 1 - \sum_{m=1}^{n} h_{31}(m) \end{bmatrix}\right)
$$

Assume the following scale (q) and shape (b) parameters for the holding time entries: 0.4, 1 for $h_{12}(n)$, 0.7,1 for $h_{21}(n)$, 0.6, 0.9 for $h_{23}(n)$ and 0.5,1 for $h_{31}(n)$.

${}^{>}W(n)$ and the kernel $C(n)$ can now be plugged in to the discrete Markov Renewal Equation 3.58. A recursive computation scheme with $\phi(0) = I$ and $n = 1, 2, 3....$ yields the required state probabilities.

Figure 3.24 shows the reliability plot. This was obtained by disregarding the repair from system failure state 3 to up-state 1 before solving the Markov Renewal Equation and computing $R(n) = 1 - \phi_{13}(n)$. In other words, the down state is considered as an absorbing state.

Figure 3.26 is the system hazard rate plot calculated from:

$$
\begin{aligned}
\lambda(0) =& 0 \\
\lambda(n) =& 1 - \frac{R(n)}{R(n-1)}, \qquad n = 1, 2, 3....
\end{aligned}
$$

Figure 3.25 shows the availability plot. Availability was computed using the above procedure for reliability, except that the system repair was not disregarded.

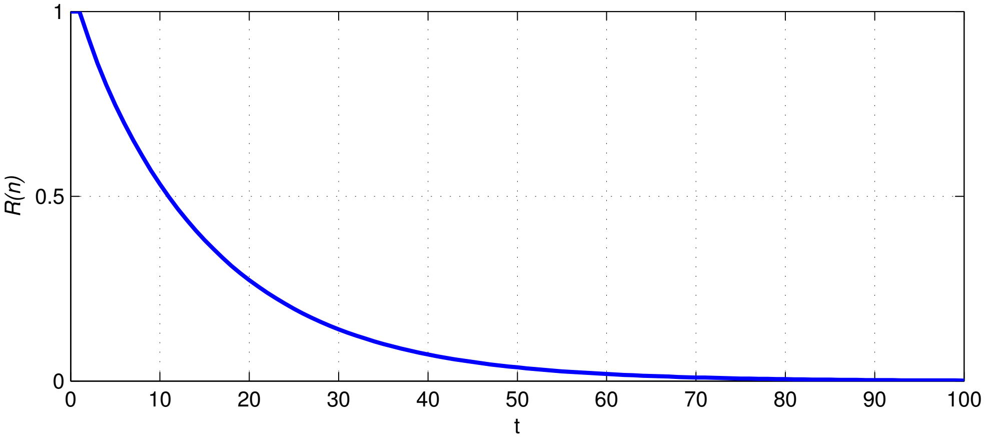


Figure 3.24: System reliability.

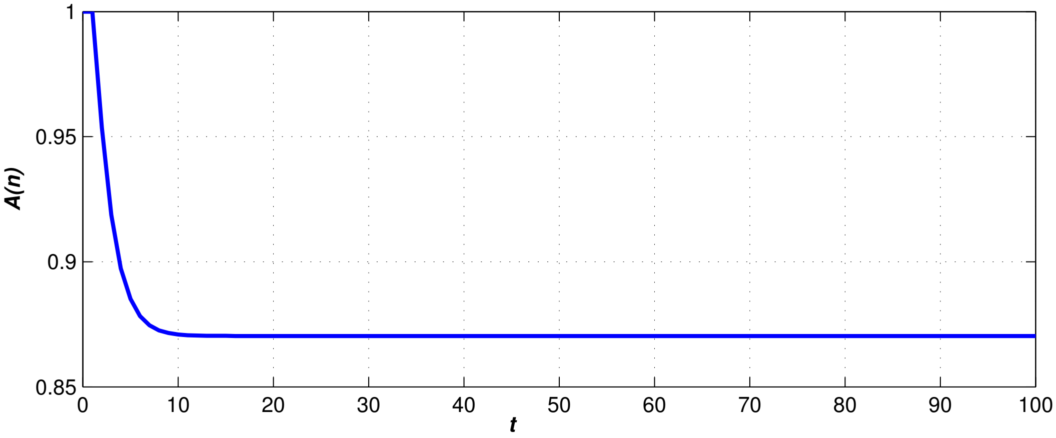


Figure 3.25: System availability.

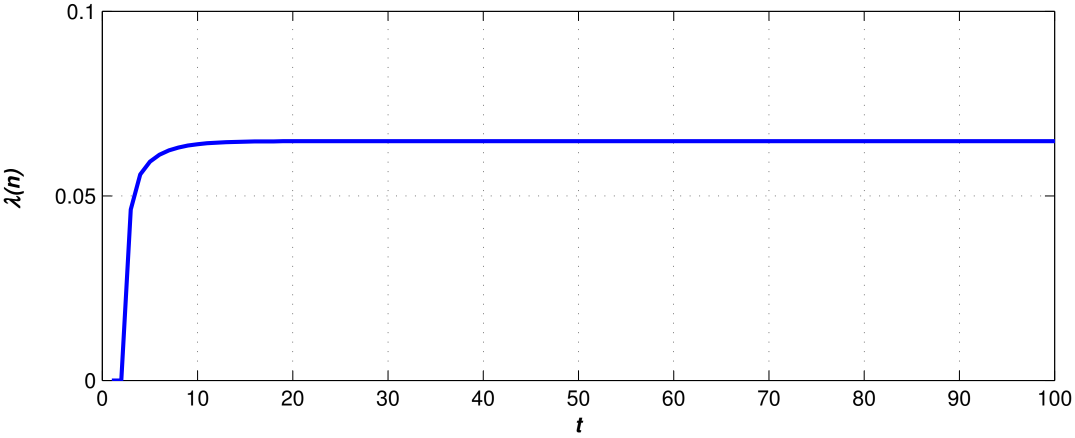


Figure 3.26: System hazard rate.

3.15 Conclusion

This chapter focused on binary and multi-state system reliability analysis based on the semi-Markov process model. Numerical and simulation based methods were reviewed to solve a given model. While fault tree lacks the time dependency in its model, Markov model is unable to handle non-exponential failure/repair times. Though the semi-Markov model works around both the issues, it still suffers from the state explosion problem. Simple techniques to combine two or more states in to a single state were introduced. The next chapter explores different areas of nuclear power plant systems where semi-Markov modelling can be practically applied.

Chapter 4

Case Studies

4.1 Nuclear Component Cooling Water (NCCW) System

A reliability analysis of nuclear component cooling water system (NCCW) is carried out. Semi-Markov process model is used in the analysis because it has potential to solve a reliability block diagram with a mixture of repairable and non-repairable components. With Markov models it is only possible to assume an exponential profile for component failure times. An advantage of the proposed model is the ability to assume Weibull distribution for the failure time of components. In an attempt to reduce the number of states in the model, it is shown that usage of poly-Weibull distribution arises. The objective of this case study is to determine system failure probability under these assumptions. This result can be utilized as an initiating event probability in probabilistic safety assessment projects.

4.1.1 Problem

In nuclear power plants, nuclear component cooling water (NCCW) system is used for removing excess heat from components that may contain potentially radioactive fluids. Xing et al. (1996) compared the Markov and fault tree models for determining system failure initiating event frequency in the Probabilistic Safety Assessment (PSA) of NCCW systems for shutdown conditions. They argued that for systems with short mission time and failure mode dominated by independent failure, the effect of repair is significant.

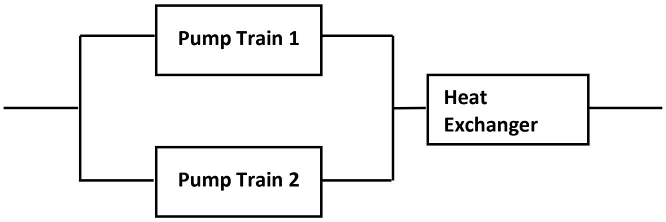


Figure 4.1: Reliability block diagram of the NCCW system(Xing et al., 1996).

The NCCW system constitutes two parallel pump trains connected in series with a heat exchanger train as seen in Figure 4.1. While both the pump trains are repairable, the heat exchanger train is a non-repairable component. This configuration makes semi-Markov model a tool of choice to perform system reliability analysis. In order to solve this system involving parallel redundancy, we first look in to what kind of redundancy problems were tackled using semi-Markov process model in the existing literature.

There were numerous studies in the past on the reliability of multi-unit and in particular two-unit parallel redundant systems using semi-Markov or renewal processes involving regeneration point techniques. These methods were utilized to analyze systems with different configuration settings. To cite a few, Osaki and Nakagawa (1971) derived time to first failure distribution of two-unit standby system allowing simultaneous failure of both the units; Gupta et al. (1982) considered a two-unit cold standby redundant system with exponential failure and general repair distribution; Mokaddis and Tawfek (1995) dealt with semi-Markov analysis of a two-unit warm standby system with dissimilar units. However, in all these models, only a *single repair act* was considered. Even, availability modeling with a single repair act is not a straightforward semi-Markov process model, rather it turns out to be a semi-regenerative process whose modeling and computations range from high to very high difficulty levels (Birolini, 2007). This difficulty arises during availability modeling with general failure or repair distributions because semi-Markov process is a *regenerative* process which means every state must correspond to a renewal or restoration of the system condition. Hence, Birolini (2007) cites a two-unit redundant example with only two system up-states in the model and the system down state is used in the formulation, but it is not part of the state space.

When availability of each unit of the redundant system is evaluated individually using Markov or renewal process models, it means that each unit undergoes an independent, dedicated repair act. Usually, these unit availabilities are combined using probability rules to obtain overall system availability. If a redundancy problem can be solved using a single semi-Markov process model with independent number of repair acts and general failure distribution like Weibull, then the results would be comparable to that of the probability rule method. However, a semi-Markov process model considering *independent repair act* has not been modeled and compared against the probability rule method so far due to inherent modeling complexities. A potential use of solving this open problem is to model parallel subsystems with common cause failures and then integrate the results using fault trees in PSA projects. We do not address this problem in the present study, rather use the semi-Markov process model in a setting where these issues do not hinder the modeling *i.e.*, we use semi-Markov process model as an effective tool to solve a reliability block diagram in which some of the components are repairable and others are not. In this case, once the system fails, the process terminates and we do not require an independent repair act to repair the system. However, the repairable components follow the failure and repair cycle until the system fails.

Relatively recent studies on the application of semi-Markov models for system reliability have concentrated on multi-state systems with varying performance levels (Lisnianski and Levitin, 2003). Perman et al. (1997) applied semi-Markov process model to power plant reliability analysis. The failure times were Weibull distributed with parameters estimated from real operating data.

The objective of this case study is to present a more advanced semi-Markov process (SMP) model for the evaluation of NCCW system failure probability by considering Weibull failure time distribution in the model.

4.1.2 Explosion model

Considering binary states for each component, the state space for the NCCW system consists of $2^3 = 8$ states as seen in Figure 4.2. The transition rate matrix associated with this system is a square matrix with dimension 8. The list of all possible transitions is listed in Table 4.1. In order to reduce the number of states in this model, state reduction techniques must be used.

4.1.3 Reduced model

As per Xing et al. (1996), the Markov state-space shown in Figure 4.3 has three states. In state ‘2P-H’, entire system is operational. When one of the pump trains

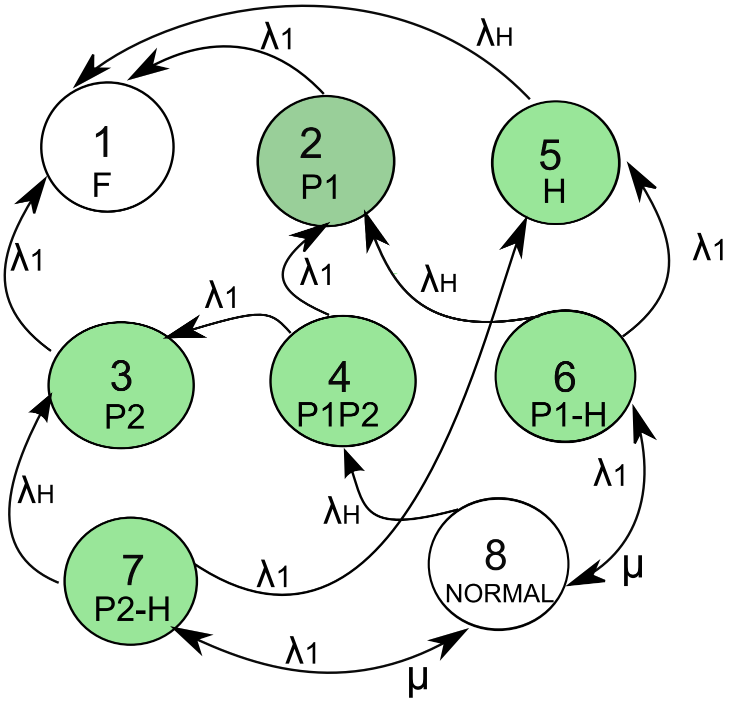


Figure 4.2: NCCW State Space Diagram (repairable pump train).

Table 4.1: Transition rate matrix

Cut set ?		000	100	010	110	001	101	011	111
Yes	0 0 0	0	0	0	0	0	0	0	0
Yes	1 0 0	λ_1	0	0	0	0	0	0	0
Yes	0 1 0	λ_1	0	0	0	0	0	0	0
Yes	1 1 0	0	λ_1	λ_1	0	0	0	0	0
Yes	0 0 1	λ_H	0	0	0	0	0	0	0
	1 0 1	0	λ_H	0	0	λ_1	0	0	μ
	0 1 1	0	0	λ_H	0	λ_1	0	0	μ
	1 1 1	0	0	0	λ_H	0	λ_1	λ_1	0

fail, the system moves to state ‘P-H’. Failure of heat exchanger train leads to system failure represented by the state ‘F’. Both the pump trains are susceptible to common cause failure.

Both the trains are composed of five components each and their effective failure rates are listed in Table 4.2 in the absence of common cause failure.

Let $p_1(t)$, $p_2(t)$, and $p_3(t)$ represent the probability of being in states F, P-H and 2P-H respectively. Based on the state-space diagram, the system of differential equations for the Markov model is written as per the theory described by Lisnianski and Levitin (2003):

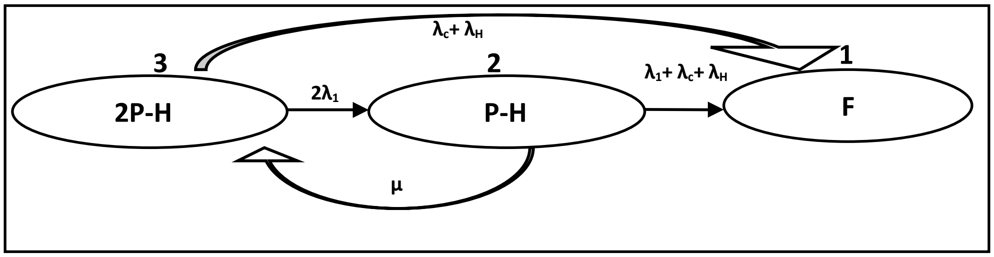


Figure 4.3: Markov state-space for the NCCW system.

Table 4.2: Failure/repair data for the NCCW components(Xing et al., 1996)

λ_1	Pump train failure rate	7.7243 x 10^{-6} hr^{-1}
λ_H	Heat exchanger train failure rate	3.4243 x 10^{-6} hr^{-1}
μ^{-1}	Pump train repair time	19.4 hr
λ_c	Common cause failure	0 (Not in present study)

$$\begin{aligned}\frac{dp_1(t)}{dt} &= (\lambda_1 + \lambda_H)p_2(t) + \lambda_H p_3(t)\\ \frac{dp_2(t)}{dt} &= 2\lambda_1 p_3(t) - \mu p_2(t)\\ \frac{dp_3(t)}{dt} &= \mu p_2(t) - (2\lambda_1 + \lambda_H)p_3(t)\end{aligned} \tag{4.1}$$

In the proposed semi-Markov model, we assume that pump train failure time and repair time follow exponential distribution with mean λ_1 and μ respectively. Let the heat exchanger failure time be governed by a Weibull distribution with mean time to failure λ_H^{-1} hours and a coefficient of variation of c associated with the time to failure. A list of functions required to construct the kernel are shown in Table 4.3.

Table 4.3: Summary of transition functions used in the kernel

$f_1(t), R_1(t)$	failure time *pdf* and rf(pump train)
$g(t), G(t)$	repair time *pdf* and rf(pump train)
$f_H(t), R_H(t)$	failure time *pdf* and rf (heat exchanger train)
$f_{32}(t)$	*pdf* for transition from 2P-H to P-H
$R_{32}(t)$	reliability function corresponding to $f_{32}(t)$
$f_{21}(t)$	*pdf* for transition from P-H to F
$R_{21}(t)$	reliability function corresponding to $f_{21}(t)$

rf - reliability function

Both the pump trains are identical and the *pdf* of the transition from 2P-H to

P-H is the *pdf* of minimum of the random variables denoting time-to-failure of the individual pump trains and the reliability function for this transition is the product of the reliability functions of each pump train as in Equation 3.55:

$$R_{32}(t) = R_1(t)R_1(t) \tag{4.2}$$

Similarly, for the transition from P-H to F, system failure could occur due to pump or heat exchanger train failures acting as two competing causes. Hence, the reliability $R_{21}(t)$ and *pdf* $f_{21}(t)$ of this transition are given by:

$$R_{21}(t) = R_1(t)R_H(t) \tag{4.3}$$

$$f_{21}(t) = f_H(t)R_1(t) + f_1(t)R_H(t) \tag{4.4}$$

$f_{21}(t)$ and similarly $f_{32}(t)$ are poly-Weibull distributions as discussed in Section 3.13.

For convenience, all the density functions corresponding to the transitions can be arranged in a matrix form:

$$f(t) = \begin{bmatrix} 0 & 0 & 0 \\ f_{21}(t) & 0 & g(t) \\ f_H(t) & f_{32}(t) & 0 \end{bmatrix} \tag{4.5}$$

With the distributions for transitions, the kernel of the semi-Markov process model can be written according to Equation 3.5:

$$C(t) = \begin{bmatrix} 0 & 0 & 0 \\ f_{21}(t)G(t) & 0 & g(t)R_{21}(t) \\ f_H(t)R_{32}(t) & f_{32}(t)R_H(t) & 0 \end{bmatrix} \tag{4.6}$$

Since all the failure/repair time distributions in matrix $f(t)$ are poly-Weibull, the elements of matrix $W(t)$ can written in closed form expression using Equation 3.57:

$$W(t) = \begin{bmatrix} 0 \\ R_{21}(t)G(t) \\ R_H(t)R_{32}(t) \end{bmatrix} \tag{4.7}$$

The kernel $C(t)$ and the matrix $W(t)$ are sufficient to describe the time evolution of the system. By substituting these matrices in Equation 3.10 and computing the system of integrals using the trapezoidal rule discussed in the Appendix, time dependent state probabilities of being in each state can be obtained.

Contrary to the preceding discussion, it is possible to assume that the pump train failure time follows Weibull distribution and the heat exchanger train failure time follows an exponential distribution. The analysis follows the same set of Equations from 4.2 to 4.7.

4.1.4 Results and discussion

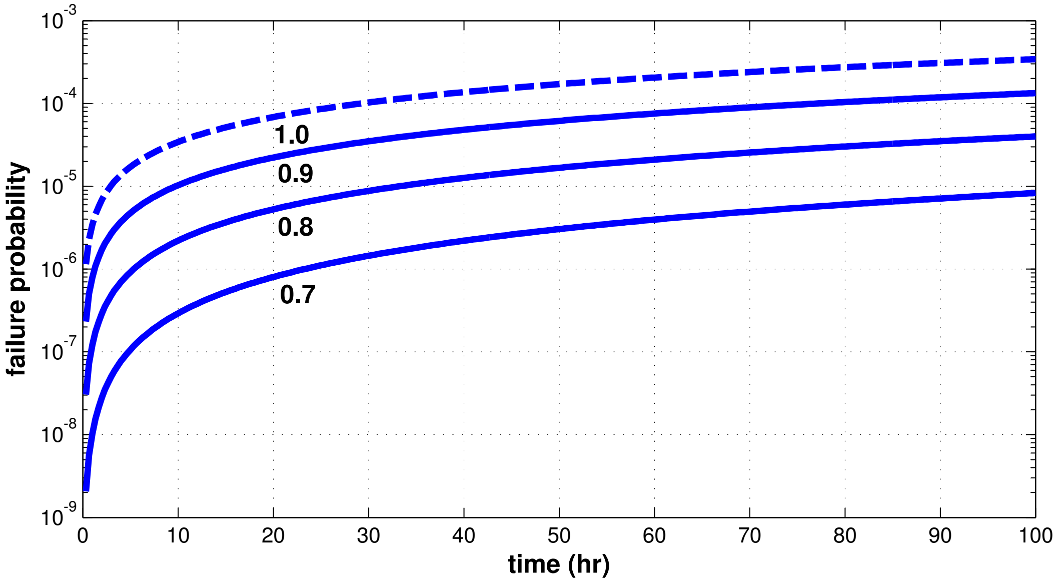


Figure 4.4: System failure probability for cov = 0.7, 0.8, 0.9, 1.0 with heat exchanger train failure time following a Weibull distribution

The time-dependent failure probability of the NCCW system is the probability of the system being in state F with the assumption that the system started its initial operation in state 2P-H. This quantity is given by solving for $\phi_{31}(t)$ in the Equation 3.10. A mission time of 100 hrs assuming various values for the coefficient of variation c are plotted in Figures 4.4 and 4.5. Also super-imposed on both the plots is the system failure probability obtained by solving the differential equations for the Markov case in Equation 4.1. For $c = 1$, the model reduces to a Markov model. The first observation is that the system failure probability using Markov and semi-Markov formulations is the same. For the entire range of c considered

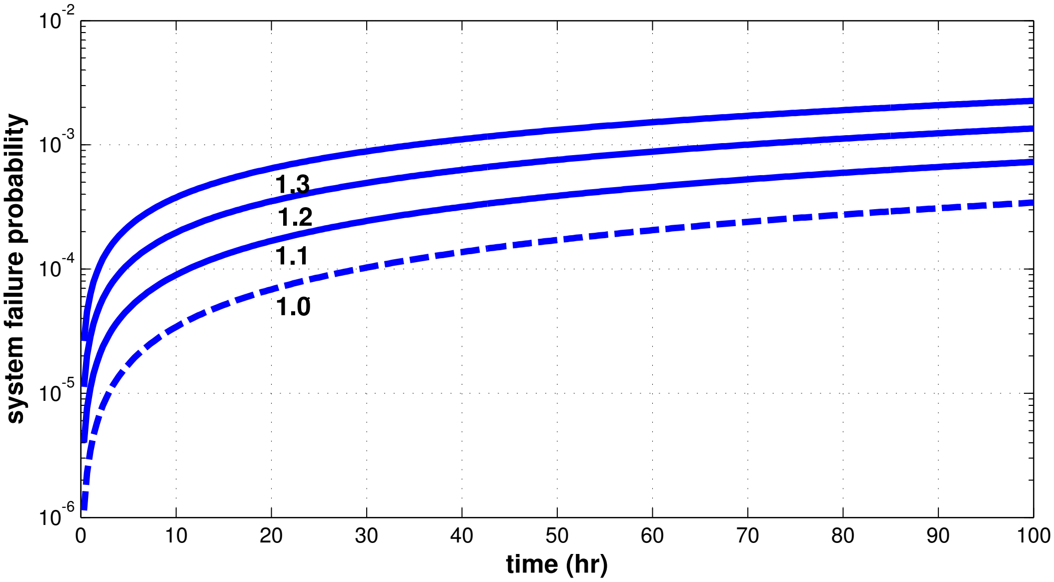


Figure 4.5: System failure probability for cov = 1.0, 1.1, 1.2, 1.3 with heat exchanger train failure time following a Weibull distribution

i.e., $c = 0.7, ..., 1.3$, we see an increasing trend in the failure probability with time for each c. For $c < 1$, the failure probability decreases and increases when $c > 1$ relative to $c = 1$. In simpler words, failure probability is a function of the variability in the failure times. Higher the variability, higher is the system failure probability. Random failures often show up large variation in failure times whereas those of a cohort of ageing systems are likely to show less variability.

For the NCCW system, with low failure rate of the components and perfect repair of the pump trains, system failure probability will reach a certain probability of 1.0 much beyond the mission time. Further, assumption of this model is that the observation starts from the time when the system is newly installed *i.e.*, from age zero. Xing et al. (1996) stated that the transient nature of the hazard rate of their NCCW Markov model with in the mission time is due to the dominant independent component failure mode making the repairs significant as opposed to the common cause failure. Hence, in order to witness any ageing in the system, the Markov and semi-Markov model results must be compared long after the considered mission time where the hazard rate of the Markov model plateaus. An alternative solution is to introduce common cause failure in to the semi-Markov model and consider truncated Weibull distribution to shift the focus to period of time when ageing is clearly observable.

Consider the second case where pump train failure time follows a Weibull distri-

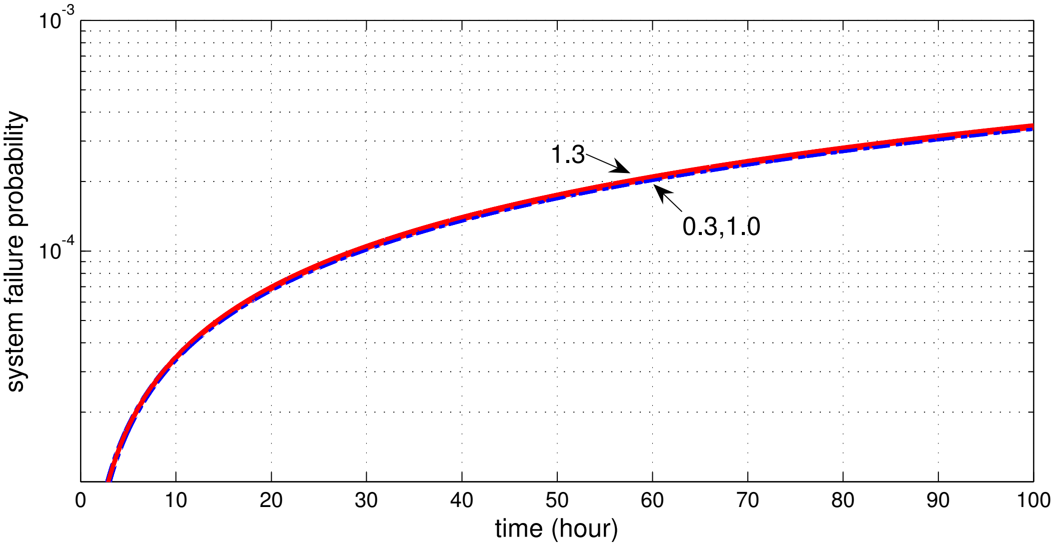


Figure 4.6: System failure probability for cov=0.3,1.0,1.3 with pump train failure time following a Weibull distribution

bution with mean λ_1^{-1} hours and *cov* of c associated with the time to failure, where as heat exchanger train failure time follows exponential distribution. The system failure probability for this case is plotted in Figure 4.6 for $c = 0.3, 1.0$ and 1.3. It is interesting to see that the failure probabilities for $c = 0.3$ and $c = 1.0$ are hardly distinguishable, while for $c = 1.3$, the system failure probability is relatively larger. *i.e.*, an increase in the *cov* until 1.0 has not led to a distinguishable increase in system failure probability. This system behavior is a result of the following reasons with respect to the pump trains: (1) parallel redundancy: two pump train units, (2) small expected repair time of 19.4 hrs against very small failure rate of 7.7243 x 10^{-6} hr^{-1}.

We see Markov model being used widely though it restricts the failure time profile to exponential distribution. However, for engineering systems, often Weibull distribution is a desirable choice due to its additional shape parameter signifying the trend in the component's failure rate. Hence, this case study demonstrated that semi-Markov model for reliability analysis is a choice where better predictability is desired by considering Weibull distribution for failure times in a partially repairable system.

The fault tree is extensively used in the nuclear industry as part of Probabilistic Safety Analysis (PSA). The basic events are often quantified in terms of failure probabilities or frequencies resulting from Markov models. For example, the failure of the NCCW system could be a basic event that initiates a potential Loss of

Coolant Accident (LOCA) leading to a core damage. The present study proposes the use of semi-Markov models in place of Markov models for better accuracy of failure probabilities in such PSA applications.

4.1.5 Conclusion

The component cooling water system failure probability was determined using Semi-Markov process model. This method is found to be effective when a system is composed of two-unit parallel redundant components in combination with at least one non-repairable component. Unlike the Markov model, the proposed method allows the usage of Weibull distribution for the component failure time. The NCCW system failure probability can be used as an initiating event probability in probabilistic safety assessment projects.

4.2 Nuclear Piping System

This section presents a general model for evaluating the rupture frequencies and reliability of the piping system in nuclear power plant based on the theory of semi-Markov process. The proposed model is able to incorporate the effect of ageing related degradation of pipes. Time dependent rupture frequencies are computed and compared against those obtained from the homogeneous Markov process model. The influence of flaw and leak inspection intervals on the piping rupture probability is investigated.

4.2.1 Problem

Piping systems in nuclear power plants are susceptible to ageing mechanisms such as corrosion, cracking and fatigue. Since data regarding pipe ruptures in the nuclear plant are rare, different modelling approaches have been developed in the literature to estimate the rupture frequency, which serves as a useful input of the frequency of an initiating event in probabilistic safety analysis (PSA). A piping reliability model (Simonen and Woo, 1984) was developed based on probabilistic fracture mechanics using Monte Carlo simulation. This method considered initial crack size, flaw (or crack) detection probability, crack growth relation, and the deterministic stress history as the random variables and it was observed that crack detection capability and inspection time had the greatest impact on leak probabilities. The Markov process model also has been applied to analyze reliability of the piping system (Fleming, 2004). This method identifies various states of degradation, and requires input regarding the transition rates and average time taken to recover from one state to another. Based on this input, the Markov model is able to predict the rupture frequency in a future operating interval.

In the context of modelling of pipe failure, the Markov model consists of three main states or events other than the normal state of the pipe. They are flaw initiation, leakage and rupture. The Markov process model assumes constant transition rate, which means that the transition time follows an exponential distribution. In case of an ageing piping system, this assumption is problematic. For example, flaw initiation rate in degrading pipes is likely to change with the age of the pipe. The exponential distribution with constant hazard rate cannot capture this aspect of ageing. Typically, the Weibull distribution with time-dependent hazard rate is used for modelling the ageing effects. In summary, the homogeneous Markov process model is not adequate for modelling the ageing effects contributing to the pipe rupture.

The objective of this paper is to present a more advanced semi-Markov process (SMP) model for the evaluation of rupture frequencies including the effect of ageing related degradation mechanisms.

Section 4.2.2 defines the problem of piping reliability analysis, as described by Fleming (2004). Section 4.2.3 discusses formulation of the piping system reliability using semi-Markov process model.

4.2.2 State Space Model

Formulation

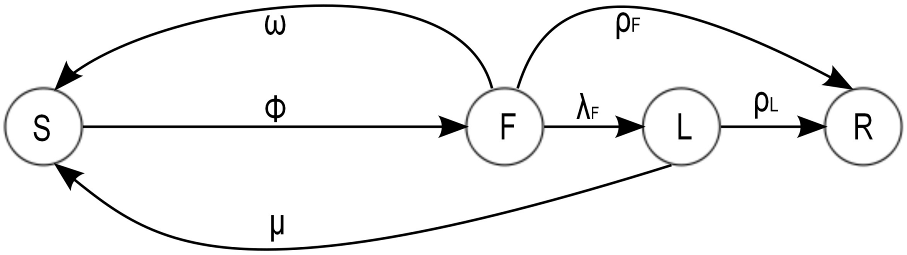


Figure 4.7: Four-state transition model for nuclear piping system degradation.

The Markov process model to predict piping system reliability was proposed by Fleming (2004). The model consists of four states as seen in Figure 4.7. In the first state S, the piping system is assumed to be in a normal operational state. Flaws formed in the system grow gradually until they become detectable. At this time, the system moves to the state F with a transition rate of ϕ per year. A detectable flaw is either detected and repaired with a repair rate of ω, or further degrades until it becomes a detectable leak, or directly leads to rupture of the piping system. If the flaw is detected and repaired, the system moves back to state S, if not, it moves to either state L or R. The rates to transit from state F to L and F to R are λ_F and ρ_F per year respectively. In this model, the transitions $S \to F$, $F \to L$, and $L \to R$ represent gradual degradation processes.

A leak when detected is either repaired with a repair rate of μ or it develops into a rupture with a rate of ρ_L per year. If the leak is repaired, the system moves back to the state S, otherwise it transits to the state R.

The system is assumed to be non-repairable, fail state once a flaw or leak develops in to a rupture *i.e.*, the state R is an absorbing state. This is primarily done to evaluate the reliability of the piping system. It is assumed that all other repairs bring back the system to 'as good as new' condition.

The flaw repair rate ω is determined as in Equation 4.8 (Fleming, 2004)

$$\omega = \frac{P_I P_{FD}}{(T_{FI} + T_R)} \tag{4.8}$$

Where P_I=0.25 is the probability that a piping segment with a flaw will be inspected per inspection interval, $P_{FD} = 0.90$ is the probability that this flaw is detected and T_R =200hrs is the time to repair the flaw once it is detected. The flaw inspection interval T_{FI} is taken as 10 years in the present paper unless stated otherwise.

The leak repair rate is formulated on similar lines in Equation 4.9:

$$\mu = \frac{P_I P_{LD}}{(T_{LI} + T_R)} \tag{4.9}$$

Where P_I =0.90 is the probability that a piping segment with a flaw will be inspected per inspection interval, $P_{LD} = 0.90$ is the probability that this leak is detected and T_R =200hrs is the time to repair the leak once it is detected. The leak inspection interval T_{LI} is taken as 1 year in the present paper unless stated otherwise. (Note that the formula for μ in Fleming (2004) is missing P_I, but considered in the table entitled "Example Markov model transition parameters for a weld in a PWR reactor coolant system").

This four state model is applicable to pipe failure mechanisms which are a combination of crack propagation (e.g. thermal fatigue near welds) and wall thinning (e.g. flow accelerated corrosion in pipe base metal) failure mechanisms. Failures due to severe loading such as overpressure are not accounted as observed from the absence of direct transitions $S \rightarrow R$ and $S \rightarrow L$. In other words, leak or a rupture can only occur from the state of an existing flaw (Fleming, 2004).

Homogeneous Markov Process Model

The system state transition matrix (Lisnianski and Levitin, 2003) for the model in Figure 4.7 is given by:

$$T = \begin{bmatrix} -\phi & \phi & 0 & 0 \\ \omega & -(\omega + \lambda_F + \rho_F) & \lambda_F & \rho_F \\ \mu & 0 & -(\mu + \rho_L) & \rho_L \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{4.10}$$

Let $S(t)$, $F(t)$, $L(t)$,and $R(t)$ represent the time-dependent probabilities of being in the states S,F,L, and R respectively. These state probabilities can be obtained by solving the system of differential Equations 4.11 with the initial condition $S(0) = 1, F(0) = L(0) = R(0) = 0$. The initial condition ensures that the system initially starts operating in state S.

$$\begin{aligned} dS(t)/dt &= \omega F(t) + \mu L(t) - \phi S(t) \\ dF(t)/dt &= \phi S(t) - (\omega + \lambda_F + \rho_F)F(t) \\ dL(t)/dt &= \lambda_F F(t) - (\mu + \rho_L)L(t) \\ dR(t)/dt &= \rho_F F(t) + \rho_L L(t) \end{aligned} \tag{4.11}$$

subject to the condition that $S(t) + F(t) + L(t) + R(t) = 1$

This system of equations is based on the fact that the rate of change of probability of being in any state S is negatively proportional to the rate at which the transitions occur outward from S and positively proportional to the rate at which inward transitions occur from other states (Lisnianski and Levitin, 2003).

For example, from Figure 4.7, it is seen that there are two inward transitions in to state S originating from states F and L with transition rates ω and μ respectively. $\omega F(t)$ and $\mu L(t)$ are weighted transition rates added to $dS(t)/dt$. There is one outward transition to state F with transition rate ϕ and hence negatively influences $dS(t)/dt$ as seen in the system of equations. The numerical solution to this system yields the state probabilities.

4.2.3 Rupture Frequency Analysis

Formulation

The *pdfs* are denoted by general symbol $f(t)$ and subscripts are used to denote the states as shown in Figure 4.7:

$$f(t) = \begin{bmatrix} 0 & f_{SF}(t) & 0 & 0 \\ f_{FS}(t) & 0 & f_{FL}(t) & f_{FR}(t) \\ f_{LS}(t) & 0 & 0 & f_{LR}(t) \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

The elements $c_{ij}(t)$ of the kernel matrix $C(t)$ are found according to Equation 3.5:

$$\begin{aligned} c_{SF}(t) =& f_{SF}(t) \\ c_{FS}(t) =& f_{FS}(t)[1 - F_{FL}(t)][1 - F_{FR}(t)] \\ c_{FL}(t) =& f_{FL}(t)[1 - F_{FS}(t)][1 - F_{FR}(t)] \\ c_{FR}(t) =& f_{FR}(t)[1 - F_{FS}(t)][1 - F_{FL}(t)] \\ c_{LS}(t) =& f_{LS}(t)[1 - F_{LR}(t)] \\ c_{LR}(t) =& f_{LR}(t)[1 - F_{LS}(t)] \end{aligned}$$

The transition probability matrix and its elements are denoted by $\boldsymbol{\phi(t)}$ and $\boldsymbol{\phi_{ij}(t)}$ respectively as per Howard's (1971) notation. These are a function of time and will be written in bold font in this paper. ϕ has been used by Fleming (2004) to denote the rate of flaw growth and is independent of time. This symbol is written in normal font in the present paper. This approach to distinguish the symbols has been done so as to be consistent with the notation of both the authors.

The flaw occurrence rate ϕ is based on the data from results of Non-Destructive Examination (NDE) (Fleming, 2004). In order to obtain parameters of an assumed non-exponential distribution for the time to flaw growth *i.e.*, for the transition $S \rightarrow F$, it is beneficial to additionally consider the variability associated with the time to flaw growth from the test results. Hence, the parameters affecting the coefficient of variation (*cov*) will be the chemical, material, texture and other properties taken in to consideration in the NDE inspections. For example, let the

Table 4.4: Constant transition rates for the piping system model (Fleming, 2004)

Parameter	Value	
ϕ	Flaw detection rate	4.35 x 10^{-4}/yr
ω	Repair rate of a detected flaw	2.1 x 10^{-2}/yr
λ_F	Leak detection rate	1.79 x 10^{-4}/yr
ρ_F	Rupture occurrence rate from flaw state	9.53 x 10^{-6}/yr
μ	Repair rate of a detected leak	7.92 x 10^{-1}/yr
ρ_L	Rupture occurrence rate from leak state	1.97 x 10^{-2}/yr

time to flaw growth until being detectable in the piping system represented by the state transition $S \rightarrow F$ be considered a Weibull distribution with scale λ_ϕ and shape γ_ϕ corresponding to the mean ϕ^{-1} years and *cov* of c. Let the rest of the transition times follow exponential distribution. $W(t)$ is constructed as per Equation 3.8, and the details are presented in Section 3.3.3. Then the Markov Renewal given in Equation 3.10 is formulated as:

$$\boldsymbol{\phi(t)} = \begin{bmatrix} e^{-(\lambda_\phi t)^{\gamma_\phi}} & 0 & 0 & 0 \\ 0 & e^{-(\omega+\lambda_F+\rho_F)t} & 0 & 0 \\ 0 & 0 & e^{-(\mu+\rho_L)t} & 0 \\ 0 & 0 & 0 & S \end{bmatrix} + \int_0^T \begin{bmatrix} 0 & c_{SF}(\tau) & 0 & 0 \\ c_{FS}(\tau) & 0 & c_{FL}(\tau) & c_{FR}(\tau) \\ c_{LS}(\tau) & 0 & 0 & c_{LR}(\tau) \\ 0 & 0 & 0 & 0 \end{bmatrix} \boldsymbol{\phi(t-\tau)} d\tau$$

By solving the above system using the trapezoidal rule, the state probabilities $\boldsymbol{\phi(t)}$ can be found. Given that the system initially started in a perfect operating condition (state S), the probability of a flaw being detectable (state F), a leak being detectable (state L) and that of a rupture (state R) are given by $\boldsymbol{\phi_{SF}(t)} = \boldsymbol{\phi_{12}(t)}$, $\boldsymbol{\phi_{SL}(t)} = \boldsymbol{\phi_{13}(t)}$, and $\boldsymbol{\phi_{SR}(t)} = \boldsymbol{\phi_{14}(t)}$ respectively.

Results

The transition rates for the Markov model are taken from Fleming (2004) and are summarized in Table 4.4.

When the coefficient of variation of the flaw initiation time is c=1.0, the semi-

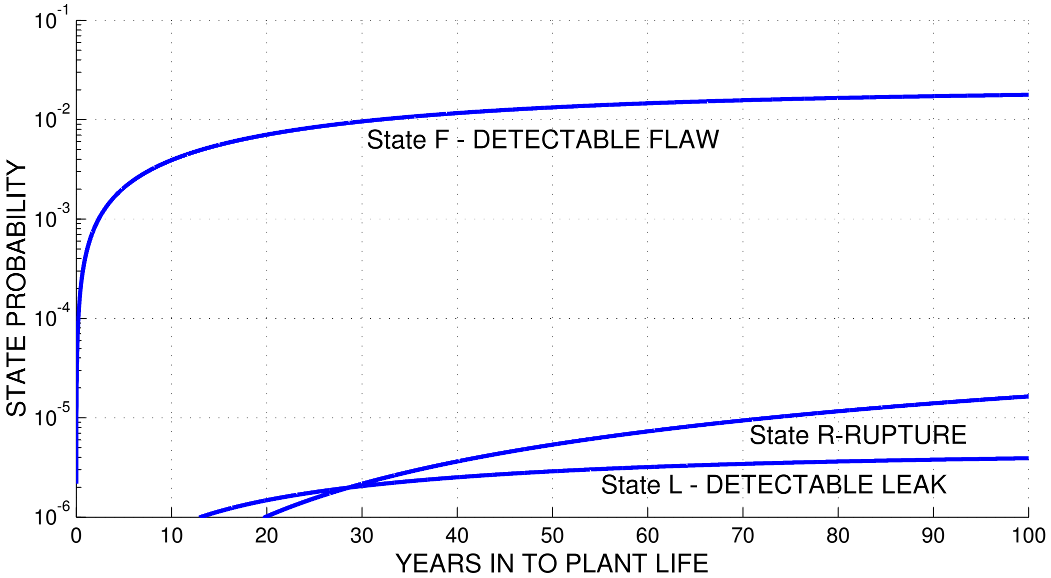


Figure 4.8: State probabilities. Time to flaw growth: mean = ϕ^{-1} years, cov = 1.0

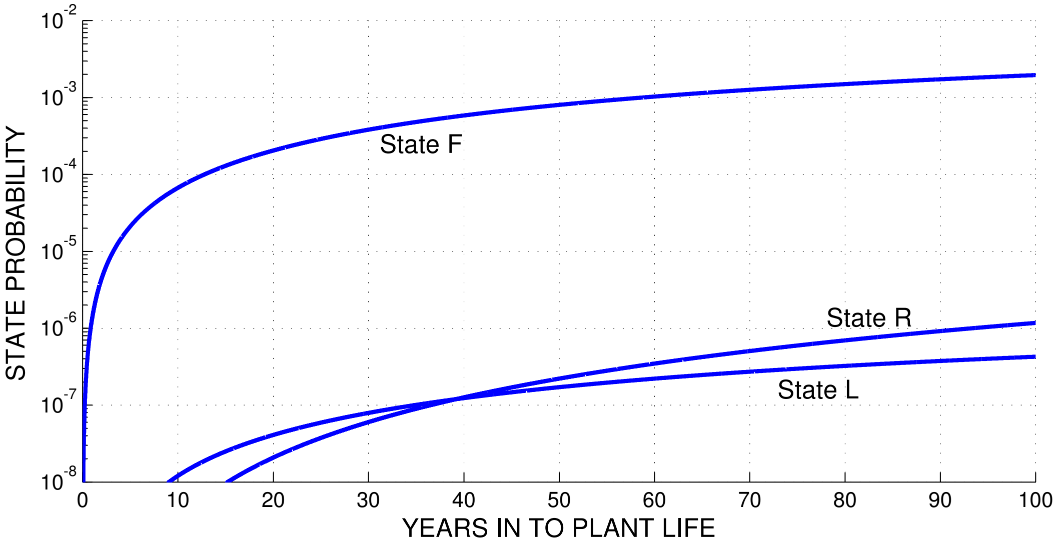


Figure 4.9: State probabilities. Time to flaw growth: mean = ϕ^{-1} years, cov = 0.6

Markov process model yields the same results as reported by Fleming (2004) using homogeneous Markov model (Figure 4.8). It is seen that the state probability of being in state F is higher than being in states L and R. This is due to timely detection and repair of detectable flaws. On repair, the system goes back to state S thus reducing the probability of going to state of rupture.

Now we consider the cases in which flaw initiation time is modeled by the Weibull distribution and proposed SMP model is used for reliability computation. Figure

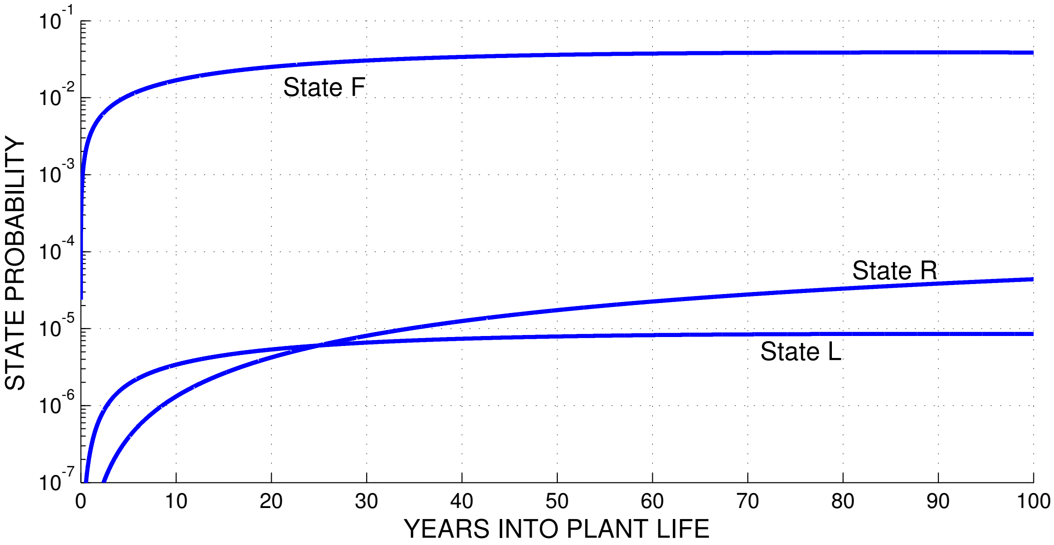


Figure 4.10: State probabilities. Time to flaw growth: mean = ϕ^{-1} years, cov=1.3

4.9 and Figure 4.10 show the state probabilities for c=0.6 and c=1.3 respectively. When $c < 1$, the state probabilities are lesser than that when $c = 1$. A reduced c implies lesser variability in the time-to-flaw initiation, which leads to smaller state probabilities as compared to the case of c= 1. On the other hand, increased c means that there is large variance in the observed data. Therefore, the flaw initiation rate is higher, which in turn increases the probability of leak and rupture events.

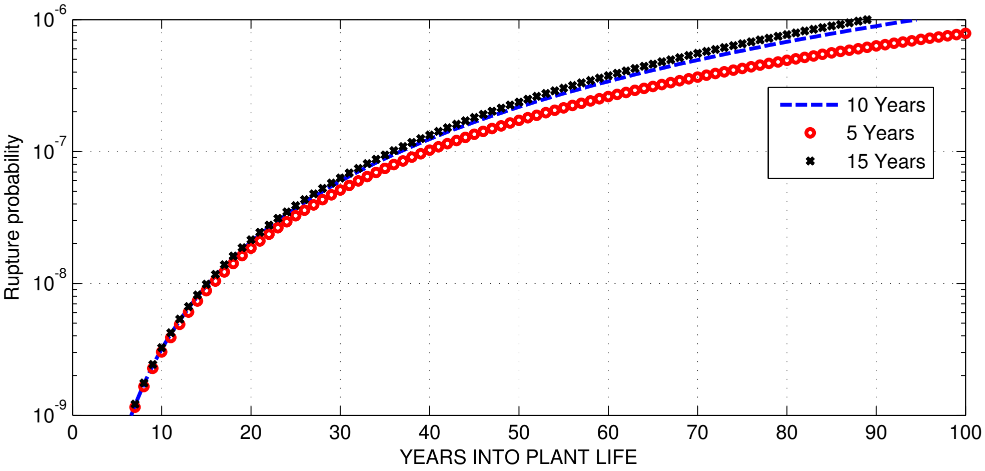


Figure 4.11: Influence of flaw inspection interval on rupture probability, Time to flaw growth: mean ϕ^{-1} years with cov=0.6

The impact on rupture probability with change in the flaw inspection interval T_{FI} is seen in Figure 4.11. Setting T_{FI} in Equation 4.8 to 5, 10, and 15 year intervals, it is observed that rupture probability increases with increase in the flaw inspection interval. However, the difference in the probabilities is hardly distinguishable with in a life span of 60 years for c=0.6.

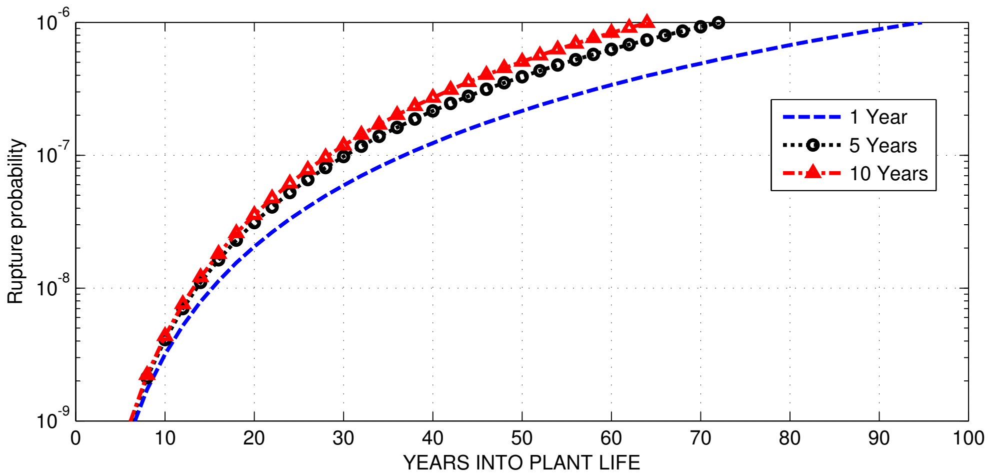


Figure 4.12: Influence of leak inspection interval on rupture probability, Time to flaw growth: mean ϕ^{-1} years with cov=0.6

The change in rupture probability for c=0.6 with change in the leak inspection interval T_{LI} is seen in Figure 4.12. Setting T_{LI} in Equation 4.9 to 1,5, and 10 year intervals, it is observed that rupture probability increases with increase in the leak inspection interval.

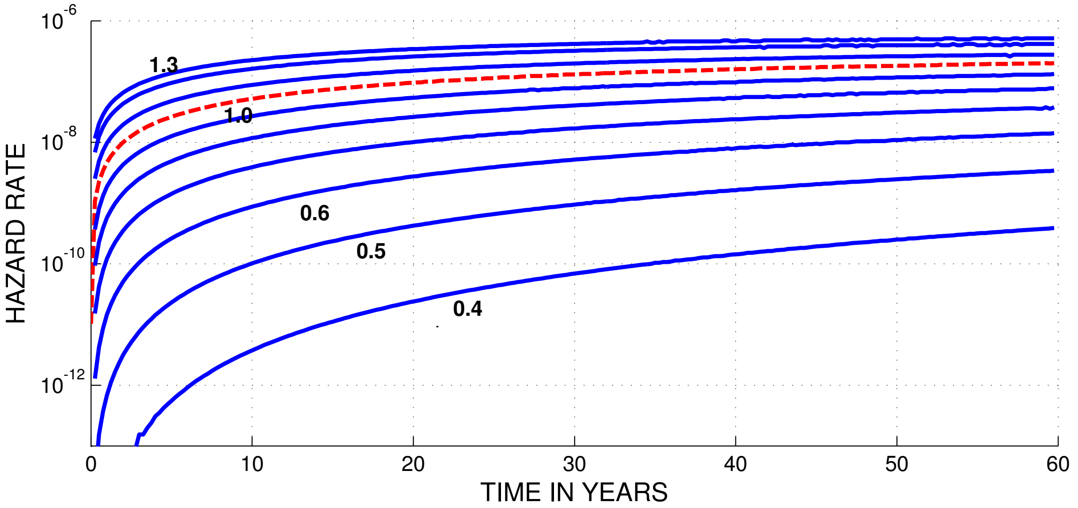


Figure 4.13: Hazard rate of rupture with repair. Time to flaw growth: mean ϕ^{-1} years with cov=0.4, 0.5,..., 1.3

The rupture frequency increases with increase in variability (or cov) associated with the time to flaw initiation distribution, as shown in Figure 5. In early life time, the transient nature of solution is seen by increasing nature of the hazard rate curve. However, a steady state solution is likely to be achieved at in long term, which may be way beyond the intended life time of the nuclear plant.

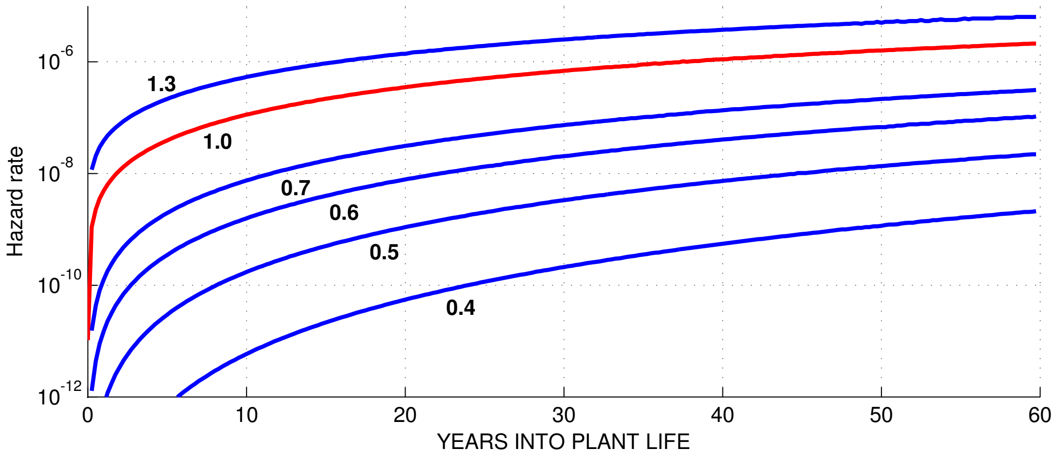


Figure 4.14: Hazard rate of rupture without repair. Time to flaw growth: mean ϕ^{-1} years with *cov*=0.4, ..., 0.6,1.0, 1.3.

The rupture hazard rate in the absence of repair is plotted in Figure 4.14. As expected, in the absence of repair, the rupture rate will increase significantly.

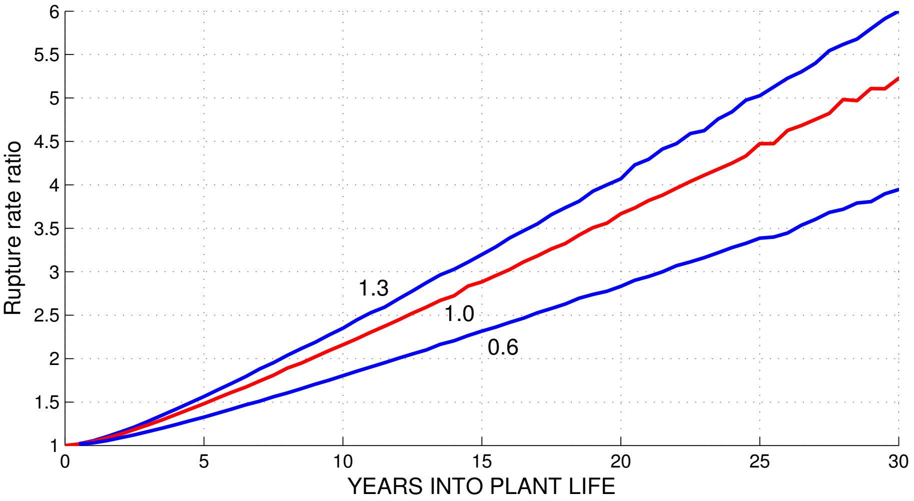


Figure 4.15: Ratio of rupture rate without repair to rupture rate with repair.

The ratio of rupture rate without repair to rupture rate with repair is shown in Figure 4.15 for three cases, c=0.6, 1 and 1.3. The increasing ratio with time shows that in the absence of repair, rupture rate is larger. Moreover, higher the variability in flaw growth, larger is the ratio. At the end of 30 years with a variation of 0.6

in the time to flaw growth, it is seen that the rupture rate without repair is four times larger than that in the presence of repair. This demonstrates the importance of effective in-service inspection (ISI) programs for timely detection and repair of flaws. Further research involves using the knowledge of these rupture rates in risk informed programs to optimize the inspection intervals.

4.2.4 Conclusion

A semi-Markov process model was proposed to analyze reliability of the nuclear piping system. In this model, the flaw initiation is modelled by Weibull distribution, which allows to incorporate the ageing effect, i.e., increase in flaw initiation rate with time. It was observed that the pipe rupture rate increases with increase in the variability of time to flaw initiation distribution. Hence, a maintenance program that removes the flaw from piping systems and repair leaks promptly will improve the reliability against rupture event. The proposed model provides a tool set to optimize the pipe inspection and maintenance program over the life cycle of the plant.

4.3 Availability Analysis of a System

Availability analysis of a general system with multi-state components following arbitrary failure and repair time distributions is described in presence of preventive maintenance. Each component can be in one of the following four states - operational, degraded, repair and corrective maintenance. Analysis at the component level is conducted using semi-Markov process model. Based on a general reliability block diagram, the collection of all possible operational set of components are identified using network reliability techniques. Component availabilities from the semi-Markov model are combined with probability rules to arrive at system unavailability. This general method is illustrated using a seven component system. The influence of inspection interval on the system unavailability is investigated.

4.3.1 Problem

A large reliability block diagram consisting of all repairable components with each component's failure and repair time following a general distribution can be solved for unavailability using Monte Carlo simulation (Billinton and Li, 1994). But simulation requires either large number of repeated trials or effective variance reduction techniques with added complexity. In this section, semi-Markov process model combined with simple probability rules is applied to obtain system unavailability from constituent components.

Time-dependent availability analysis of a large system involves obtaining availability of individual components, finding the minimal path sets of the system and finally using an algorithm to integrate all these results. A reliability block diagram can be represented in the form of a links matrix (Younes and Girgis, 2005). This matrix has all the information required to identify which two of the components in the system are connected directly in series. Using this matrix, all the minimal path sets of the system can also be enumerated.

For example, consider the tail-gas quench and clean-up system (Caceres and Henley, 1976) whose reliability block diagram is shown in Figure 4.16. The links matrix corresponding to this system with only the non-zero entries for easy read-

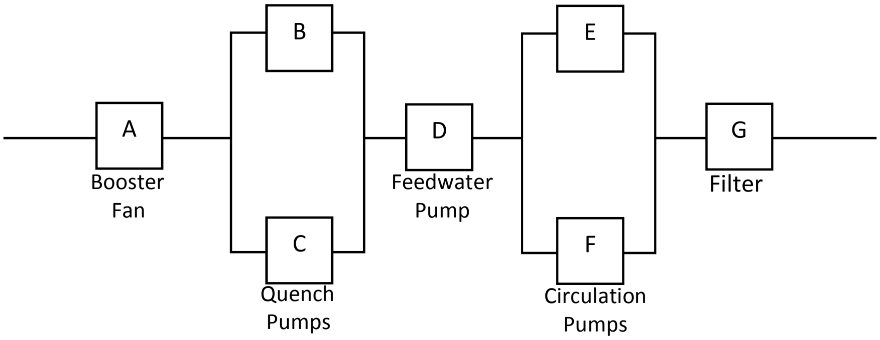


Figure 4.16: Reliability block diagram for tail-gas quench and clean-up system.

ability is:

$$\begin{array}{c}
\begin{array}{ccccccc} A & B & C & D & E & F & G \end{array} \\
\left(\begin{array}{ccccccc}
1 & 1 & & & & & \\
1 & & 1 & & & & \\
 & 1 & & 1 & & & \\
 & & 1 & 1 & & & \\
 & & & 1 & 1 & & \\
 & & & 1 & & 1 & \\
 & & & & 1 & & 1 \\
 & & & & & 1 & 1
\end{array}\right)
\end{array} \tag{4.12}$$

Using this links matrix we can trace all possible paths from A to G. For example, tracing the ones, we find that $A \rightarrow B \rightarrow D \rightarrow E \rightarrow G$ is a valid path which maintains the system in an operational state. The set $\{A, B, D, E, G\}$ is called a minimal path set. If all the components in this set are functional, then the system is guaranteed to be operational *i.e.*, these components are connected in series. This fact can also be represented in the form of an expression using set theoretic symbols. For example $(B \cup C) \cap (E \cup F)$ would mean that either of $\{B, C\}$ and either of $\{E, F\}$ must be operational. Using this notation, we find the following possible ways of the system being in operational state:

$$E_1 = A \cap B \cap D \cap E \cap G$$
$$E_2 = A \cap B \cap D \cap F \cap G$$
$$E_3 = A \cap C \cap D \cap E \cap G$$

$$E_4 = A \cap C \cap D \cap F \cap G \tag{4.13}$$

Similarly, one can define a path matrix. Each row of this matrix corresponds to one path set and the number of rows corresponds to number of minimal path sets in the system. For the tail-gas system, the path matrix is given in Matrix 4.14.

$$\begin{array}{c} \begin{array}{ccccccc} A & B & C & D & E & F & G \end{array} \\ \left(\begin{array}{ccccccc} 1 & 1 & & 1 & 1 & & 1 \\ 1 & 1 & & 1 & & 1 & 1 \\ 1 & & 1 & 1 & 1 & & 1 \\ 1 & & 1 & 1 & & 1 & 1 \end{array}\right) \end{array} \tag{4.14}$$

All these path sets are analogous to four components connected in parallel. Let T represent the fact that the system works through at least one of the paths listed in 4.13:

$$T = E_1 \cup E_2 \cup E_3 \cup E_4 \tag{4.15}$$

T can be arrived at using a step by step procedure:

$$\begin{aligned} E_1 \cup E_2 &= A \cap B \cap D \cap (E \cup F) \cap G \\ E_3 \cup E_4 &= A \cap C \cap D \cap (E \cup F) \cap G \\ T &= A \cap (B \cup C) \cap D \cap (E \cup F) \cap G \end{aligned} \tag{4.16}$$

While for a human eye it is easy to simplify the expressions, for automation and computation of arbitrarily large and complex systems, obtaining T is not straightforward. In this thesis the algorithm developed by Younes and Girgis (2005) is applied in conjunction with semi-Markov process model to carry out system availability analysis.

4.3.2 Expression for system unavailability

Assuming that failure of one component does not affect the other, for a series system with components B and C, let the availability of the components be $B(t)$ and $C(t)$

respectively, then the system availability $A_s(t)$ is given by:

$$A_s(t) = P(B \cap C) = B(t)C(t) \tag{4.17}$$

If any two components B and C are connected in parallel with availabilities $B(t)$ and $C(t)$ respectively, then system availability is given by:

$$A_s(t) = P(B \cup C) = B(t) + C(t) - B(t)C(t) \tag{4.18}$$

Using these notations, availability of the tail-gas system using Equation 4.16 can be evaluated as

$$A_s(t) = P(T) = A(t)[B(t) + C(t) - B(t)C(t)]D(t)[E(t) + F(t) - E(t)F(t)]G(t) \tag{4.19}$$

Using the same notation, Equations 4.13 translate to:

$$\begin{aligned}
E_1(t) &= A(t)B(t)D(t)E(t)G(t)\\
E_2(t) &= A(t)B(t)D(t)F(t)G(t)\\
E_3(t) &= A(t)C(t)D(t)E(t)G(t)\\
E_4(t) &= A(t)C(t)D(t)F(t)G(t)
\end{aligned} \tag{4.20}$$

where each $E_i(t)$ represents the combined availability of all components in its path set. However, union of more than two events as in Equation 4.15 becomes a combinatorial problem:

$$\begin{aligned}
P(E_1 \cup E_2 \cup ... \cup E_n) = {} & P(E_1) + ... + P(E_n)\\
& - \sum_{i<j} P(E_i \cup E_j)\\
& + \sum_{i<j<k} P(E_i \cup E_j \cup E_k)\\
& ...\\
& (-1)^{(p-1)} P(E_1 \cup E_2 \cup ... \cup E_n)
\end{aligned} \tag{4.21}$$

Younes and Girgis (2005) proposed to construct the union matrix in order to avoid repetitions in evaluating the Expression 4.21. The first k rows of the union matrix is nothing but the path matrix. The subsequent rows are the union of the sets listed in the last column of the matrix. Table 4.5 shows the union matrix for the tail gas system. For example, by the union of first two rows corresponding to $E1$ and $E2$, we get the fifth row *i.e.*, $E1 \cup E2$. Further, the probability of the event listed in the last column is the product of the availabilities of the components which are tagged as 1. For example $P(E_1 \cup E_2) = A(t)B(t)D(t)E(t)F(t)G(t)$. Similarly, by evaluating each row of the union matrix and summing them up, we get the system availability at a single time instant t. System unavailability follows by finding 1-(4.21).

Table 4.5: Union Matrix for the tail-gas system

A	B	C	D	E	F	G	
1	1		1	1		1	E1
1	1		1		1	1	E2
1		1	1	1		1	E3
1		1	1		1	1	E4
1	1		1	1	1	1	$E1 \cup E2$
1	1	1	1	1		1	$E1 \cup E3$
1	1	1	1	1	1	1	$E1 \cup E4$
1	1	1	1	1	1	1	$E2 \cup E3$
1	1	1	1		1	1	$E2 \cup E4$
1		1	1	1	1	1	$E3 \cup E4$
1	1	1	1	1	1	1	$E1 \cup E2 \cup E3$
1	1	1	1	1	1	1	$E1 \cup E2 \cup E4$
1	1	1	1	1	1	1	$E1 \cup E3 \cup E4$
1	1	1	1	1	1	1	$E2 \cup E3 \cup E4$
1	1	1	1	1	1	1	$E1 \cup E2 \cup E3 \cup E4$

Equation 4.19 is simple and can be computed swiftly, but arriving at it from Equations 4.13 needs an advanced programming construct which could get time consuming for a complex system. Equation 4.21 is long and computation of possibilities might get time consuming, but, arriving at this equation is a straightforward programming approach from Equations 4.13.

The Universal Generating Function (UGF) technique proposed by Lisnianski and Levitin (2003) greatly helps in managing combinations by assuming that states of a component can be expressed in the form of a polynomial. The polynomials thus obtained can be integrated at the system level to obtain system unavailability. This technique, however, is effective when there are at least three states for each component. In the case of binary states, storing both the failure and operational probabilities in each polynomial is redundant since one probability can be obtained when the other is known.

4.3.3 Results

Consider the hypothetical life and repair data of the tail-gas quench and clean-up system shown in Table 4.6. Availability of each of the components is obtained using the semi-Markov process model described in Section 3.3 with an illustrative example. Let the availability computed by this method for component A be denoted as $A(t) = \phi_{21}(t)$. The same method is followed for rest of the components. In the next step, these quantities are used in Equation 4.21 with the help of Table 4.5 to evaluate the system availability.

Table 4.6: Hypothetical life data for the components of the tail-gas system

Component	Mean life (cov)	Repair time
	(years)	(days)
Booster fan (A)	5 (0.6)	7
Quench pumps (B,C)	10(0.4)	15
Feedwater pump (D)	10(0.3)	15
Circulation pump (E,F)	10(0.6)	15
Filter (G)	5 (0.4)	7

Time dependent unavailability of A, D, and G are plotted in Figure 4.17 and that of B, C, E, and F are plotted in Figure 4.18. It is observed that the peak unavailabilities of these components fall around their respective mean life. Time-dependent system unavailability by both the exact method (4.19) and automated method (4.21) are shown in Figure 4.19.The observed difference between both the results is indistinguishable.

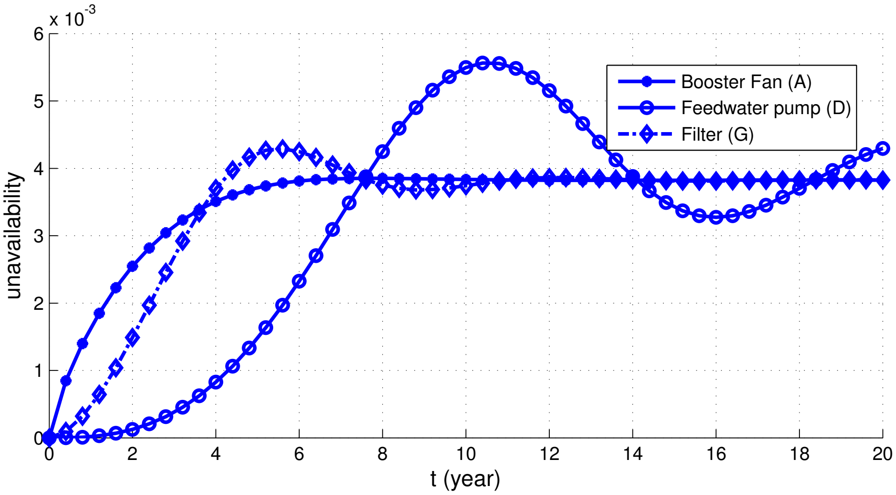


Figure 4.17: Unavailabilities of components A, D and G

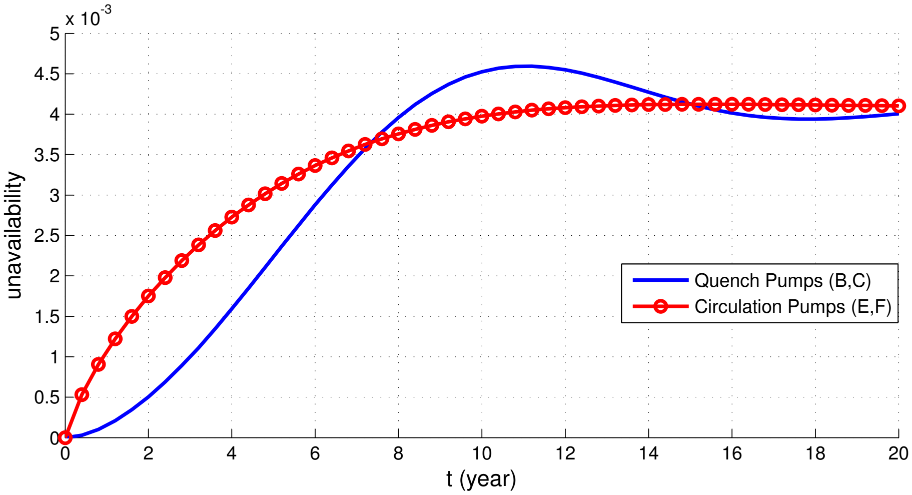


Figure 4.18: Unavailabilities of components B,C, E and F

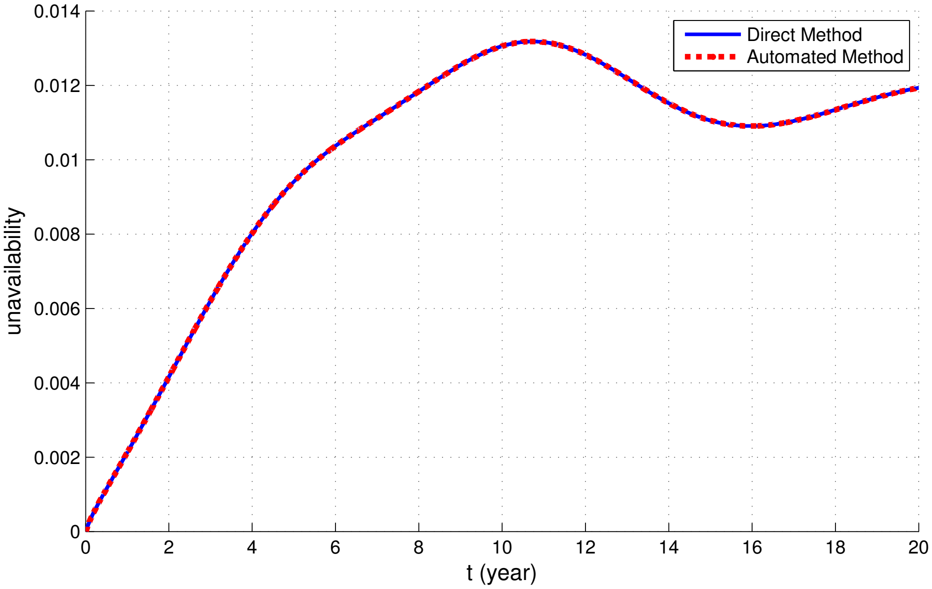


Figure 4.19: Tail-gas quench and clean-up system unavailability by exact and automated methods

For a general series-parallel system the steps to be followed to evaluate system availability are (1) Translate block diagram in to links matrix - this step can be done by updating a matrix as and when a link is made between blocks using a Graphical User Interface (GUI) (2) Determine the path matrix and hence path sets from the links matrix (3) Compute component availabilities using semi-Markov process model (4) Generate a union matrix to quantify individual terms (5) Use probability rule to arrive at expression for system availability.

In conclusion, this section analyzed a general method to automate availability analysis of a given reliability block diagram using semi-Markov process model combined with probability rules was discussed. It was demonstrated with examples how the path set of a general system can be obtained using links matrix form of the block diagram. The advantage of using this combination of semi-Markov process model and probability rules is that the semi-Markov method is faster than Monte Carlo simulations and does not need additional variance reduction methods. The proposed technique has potential in virtually every field of reliability design. However, for modeling aspects such as spares, preventive maintenance etc. in a large and complex system, Monte Carlo simulation method continues to be the tool of choice.

4.3.4 Multi-State Availability Analysis

This section has two objectives - (1) Present a semi-Markov process model for multi-state component availability analysis in the presence of preventive maintenance with Weibull failure time and (2) Apply the results of this model to a general system made of many components. Tomasevicz and Asgarpoor (2006) developed a continuous time semi-Markov process model for equipments that fail due to both deterioration and random occurrences. They modeled the deterioration in k discrete steps with exclusive states for corrective maintenance. For practical purposes, it is desirable to improvise their paper with possibility of considering general statistical distributions like Weibull for failure time. Vesely (1993) presented a comprehensive Markov model with four states - operational, degraded, maintenance and failure for quantifying the effects of maintenance on availability. Marais and Saleh (2009) developed a Markov model based framework for capturing and quantifying the value of maintenance and argued that maintenance optimization techniques in existing literature focus merely on cost minimization and not on the value of maintenance. Markov model has a limitation that the time spent in the states follows an exponential distribution. A semi-Markov process has the flexibility to incorporate non-exponential distributions. Hence this section applies semi-Markov process model combined with simple probability rules to obtain system unavailability from constituent multi-state components.

In the proposed model, it is assumed that the entire system undergoes a preventive maintenance at specified inspection intervals. At these intervals, all the components of the system are assumed to be independently inspected for signs of degradation. A preventive maintenance action involving repair of each component is undertaken. This kind of repair leads to an 'as good as new' state of the component. If the component fails even before a preventive action is taken, it leads to a component failure. In this situation, a corrective action in the form of repair is taken in order to restore the component to its operational state.

Consider again the tail-gas quench and clean-up system (Caceres and Henley, 1976) whose reliability block diagram is shown in Figure 4.16. The link, path and union matrices of this system remain the same as discussed in the earlier section with binary states.

4.3.5 Component State Space Model

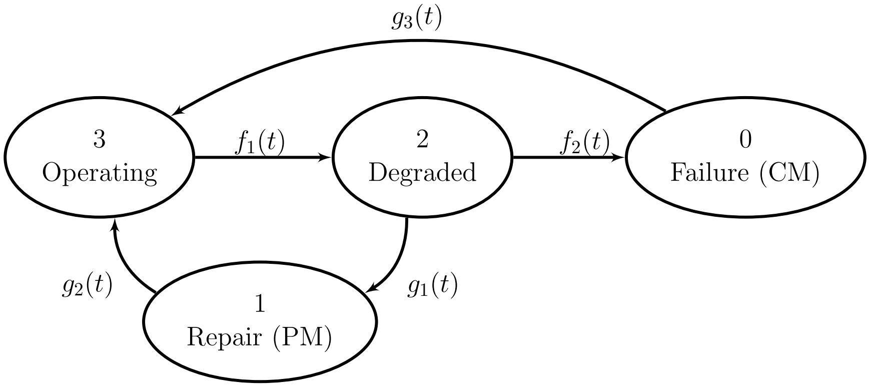


Figure 4.20: State-space of a four-state repairable component with preventive maintenance.

Consider a repairable multi-state component whose state-space diagram is shown in Figure 4.20. The transitions from one state to another are labeled with the corresponding density (*pdf*) functions with the assumption that time to transit is a random variable. The model has four states - operating state (3), degraded state (2), preventive maintenance state (1), and failure state or corrective maintenance state (0). Initially, the component is assumed to be operating in state 3. Let the time taken to proceed to a significant state of degradation ($3 \rightarrow 2$) be a random variable with an observed mean and coefficient of variation (*cov*). From this information, a Weibull distribution can be fit using a mapping between *cov* and Weibull shape parameter. Let the *pdf* of this transition be $f_1(t)$.

In the degraded state, the component either waits until the next inspection ($2 \rightarrow 1$) takes place or fails ($2 \rightarrow 0$) completely. If an inspection takes place, a repair is undertaken and the component is restored to operating state. Let the time to next inspection follow an exponential distribution with mean μ. Let its *pdf* be given by $g_1(t)$. Let the Weibull parameters for the time to failure ($2 \rightarrow 0$) be λ and γ with a *pdf* given by $f_2(t)$.

Upon inspection, the time to repair ($1 \rightarrow 3$) follows *pdf* given by $g_2(t)$. On the other hand, if the component fails completely, let the time to repair ($0 \rightarrow 3$) follow an exponential distribution with *pdf* given by $g_3(t)$. Let the *cdf* of the distributions considered be denoted by capital letter versions of the *pdf*. For example, let the *cdf* of time to failure (*pdf* $f_2(t)$) be $F_2(t)$.

It is assumed that the component failure occurs only after an amount of degradation *i.e.*, this model does not take random failure in to consideration. If it is considered, the transition $3 \rightarrow 0$ must also be taken in to account.

The kernel matrix $C(t)$ for the four-state component consists of the failure and repair time *pdfs*:

$$C(t) = \begin{bmatrix} 0 & 0 & 0 & g_3(t) \\ 0 & 0 & 0 & g_2(t) \\ f_2(t)(1 - G_1(t)) & g_1(t)(1 - F_2(t)) & 0 & 0 \\ 0 & 0 & f_1(t) & 0 \end{bmatrix}$$

and the matrix $W(t)$ consists of the closed form expressions as derived for a general case in the Appendix:

$$W(t) = \begin{bmatrix} 1 - G_3(t) \\ 1 - G_2(t) \\ e^{-\mu t - (\lambda t)^\gamma} \\ 1 - F_1(t) \end{bmatrix}$$

The state probabilities can be computed by substituting the above matrices in Equation 3.10 and solving it using trapezoidal rule as given in the Appendix:

$$\phi(t) = \begin{bmatrix} 1 - G_3(t) \\ 1 - G_2(t) \\ e^{-\mu_m t - (\lambda t)^\gamma} \\ 1 - F_1(t) \end{bmatrix} + \int_0^t C(\tau)\phi(t - \tau) d\tau$$

The element at (4,1) of the matrix $\phi(t)$ yields the component unavailability at time t and the element at (4,4) yields component availability.

Example

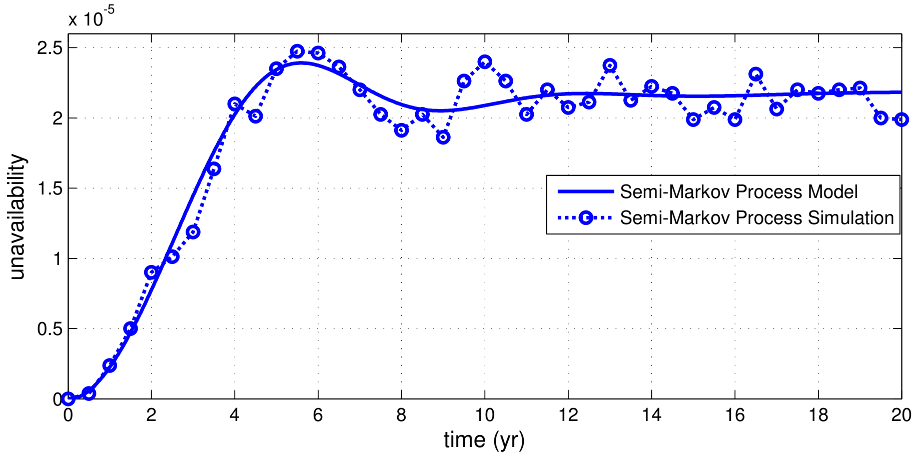


Figure 4.21: Unavailability of 4-state repairable component with a 30 day inspection interval.

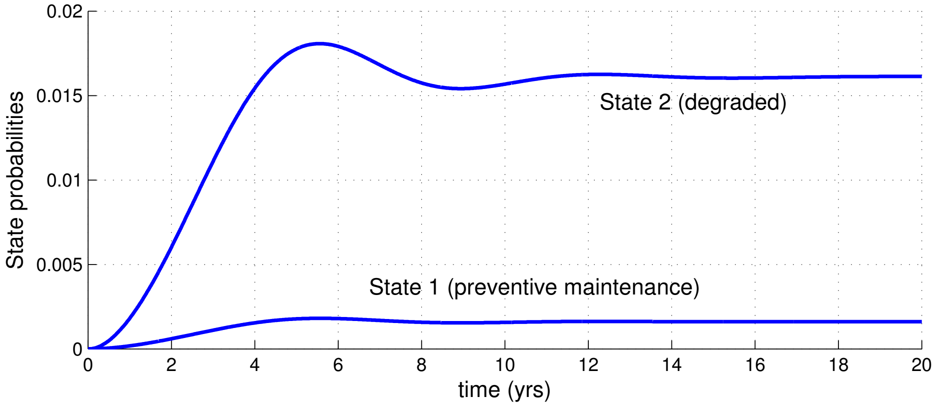


Figure 4.22: Probability of taking a preventive action versus that of being in degraded state.

For illustrative purposes, consider a component which degrades significantly around a mean time of five years with a *cov* of 0.4 associated with the time to degradation. Let the preventive maintenance be carried out every 30 days on average. Let the mean time to repair from the degraded state be 3 days while the mean time for completion of a corrective action be 5 days. Let the mean time to fail completely from a degraded state be 5 years with a *cov* of 0.8 associated with the time to failure. The unavailability of this component obtained using both the analytical and Monte Carlo process simulation methods is plotted in Figure 4.21.

It required 8 x 10^{-6} Monte Carlo iterations to achieve the accuracy shown in the Figure. It is rather time consuming and still needs a reduction in the variance. However, solving Equation 3.10 using trapezoidal rule needed only 8000 points on the interval. It is seen that the component unavailability is peak around the mean time to degradation *i.e* 5 years.

Figure 4.22 shows probabilities of being in a degraded state and undergoing a preventive maintenance action. Since the time spent in preventive repairs is lesser than the time spent in the degraded state waiting for the next inspection, we observe that the probability of being in state 2 is larger than that of being in state 1. Both these probabilities are larger than the unavailability in Figure 4.21 since there is higher probability of detecting degradation and carrying out a minimal repair given an inspection interval smaller than the time to failure.

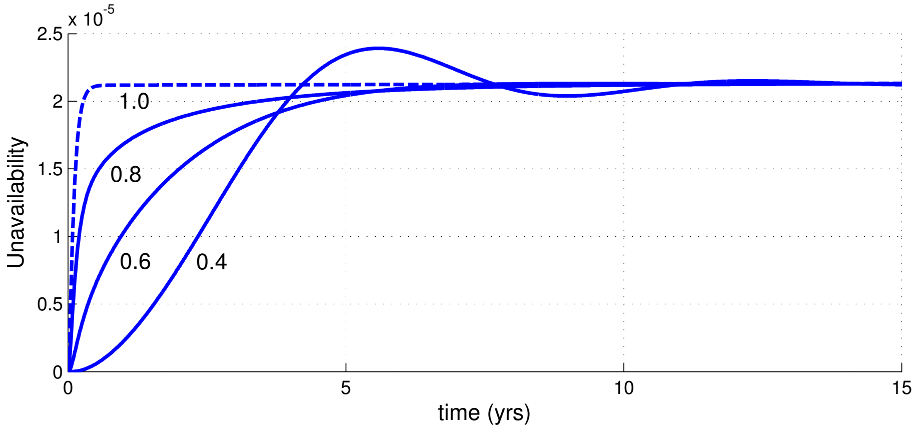


Figure 4.23: Effect of *cov* associated with time to degradation.

The *cov* of the time to degradation represented by the transition 3 → 2 has a profound influence on the component's unavailability. This effect is shown in Figure 4.23. A decrease in the *cov* shows a decrease in the unavailability of the component until around the mean time to degradation. After that a lesser *cov* shows increased unavailability. This behavior can be attributed to aging of the component.

4.3.6 Results

Consider the hypothetical life and repair data of the tail-gas quench and clean-up system shown in Table 4.7. Availability of each of the components is obtained using the semi-Markov process model. Let the availability computed by this method for component A be denoted as $A(t) = \phi_{44}(t)$. The same method is followed for rest of

Table 4.7: Life data for the components of the multi-state system.

Component	degradation time 3→2 (years)	time-to-failure 2→0 (years)	PM time 1→3 (days)	CM time 0→3 (days)
Booster fan (A)	7 (0.4)	8(0.6)	3	5
Quench pumps (B,C)	10(0.5)	10(0.4)	5	7
Feedwater pump (D)	9(0.6)	6(0.4)	5	7
Circulation pump (E,F)	8(0.4)	12(0.5)	5	7
Filter (G)	8(0.4)	7(0.3)	3	5

the components. In the next step, these quantities are used in Equation 4.21 with the help of Table 4.5 to evaluate the system availability.

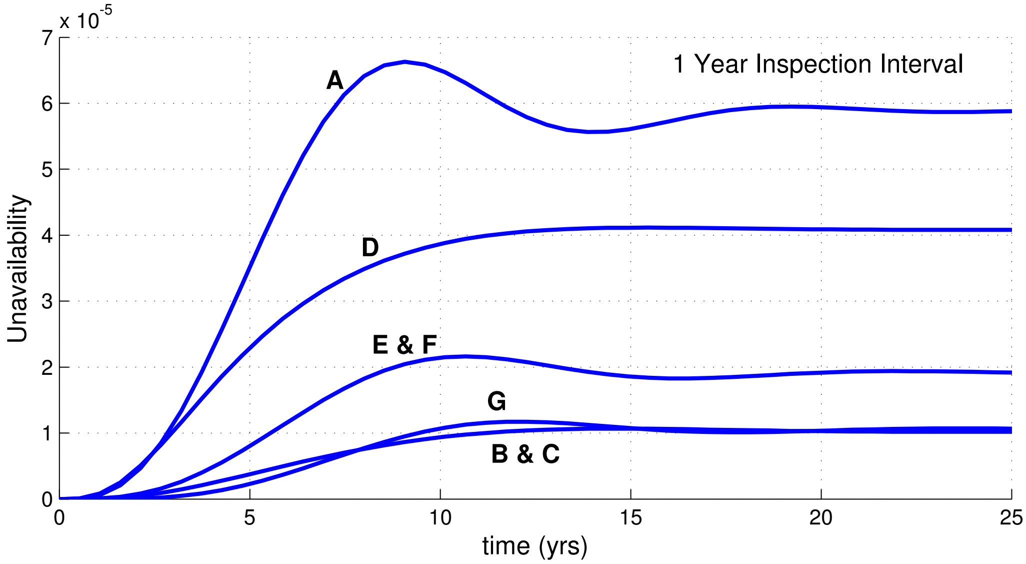


Figure 4.24: Component unavailability with one year inspection program.

Time dependent unavailability of all the components is plotted in Figures 4.24 and 4.25 with an inspection interval of one and five years respectively. It is observed that the peak unavailabilities of these components fall around the mean time to reach the degraded state. The unavailabilities are in the order of 10^{-4} in the five year inspection program whereas they have decreased to the order of 10^{-5} in the one year case *i.e.*, increasing the frequency of inspection shows decreased unavailability. In comparison, it is also seen that there is a general shift in the unavailability of the components. For example, peak unavailability of component A is between 5 and 10 years in the first case whereas peak unavailability is reached between 10 and 15 years for the second case. As a result, steady state is reached relatively quickly with a one year inspection schedule. This pattern of availability improvement as

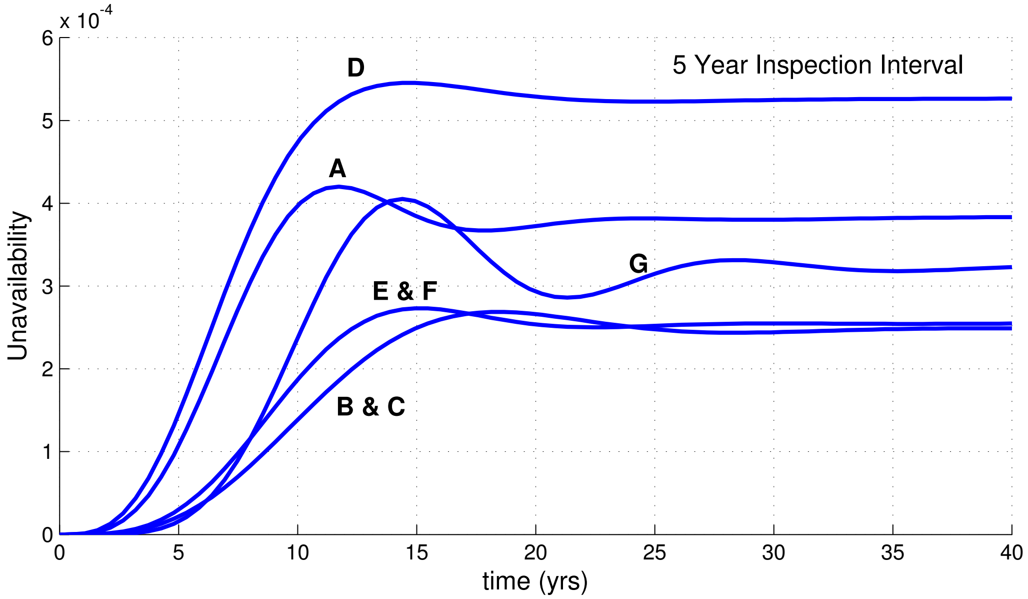


Figure 4.25: Component unavailability with five year inspection program.

a result of in-service inspection was demonstrated in the context of nuclear piping reliability analysis (Simonen and Woo, 1984).

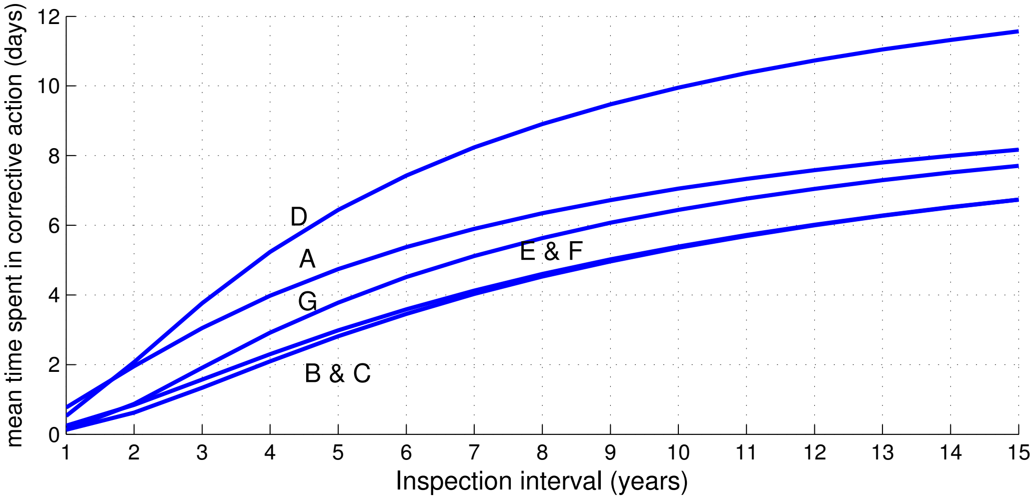


Figure 4.26: Mean time spent in corrective action as a function of inspection interval.

The mean time spent in corrective maintenance action can be evaluated as the time spent in state 0 using Equation 3.22 with $i = 3$, $j = 0$ and $T = 20$. It is a function of the inspection interval and increases with decrease in the frequency of inspections as seen in the Figure 4.26. However, inspections done at too frequent or rare intervals may not be practically effective. This needs further investigation by augmenting the unavailability model to a cost model. Results of such a model have direct impact on inspection programs and policy making.

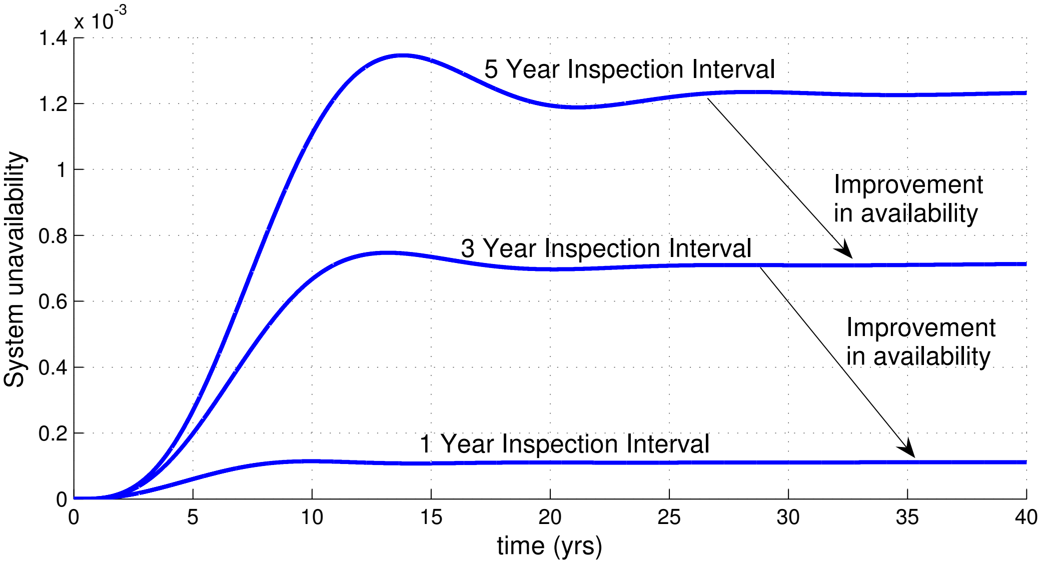


Figure 4.27: Tail-gas quench and clean-up system unavailability.

Time-dependent system unavailability by the proposed method using Equation 4.21 is shown in Figure 4.27 with inspection intervals of 1,3, and 5 years. There is a visible improvement in the system availability with smaller inspection intervals. Also, steady state unavailability is reached quicker with increased inspection frequency. In a general sense, the proposed method has qualitative impact in any field where there is a notion of components and systems or where there is a need for multi-state system modeling - dependability analysis in software testing, fault tolerant control systems in hardware reliability, wireless sensor reliability in ad hoc communication networks, search and destroy/rescue scenario analysis in defense etc.

4.3.7 Conclusion

A general method to conduct availability analysis of a given reliability block diagram using semi-Markov process model combined with probability rules was discussed. A general four state model was proposed for component availability analysis in the presence of preventive maintenance. It was demonstrated with examples how the path set of a general system can be obtained using links matrix form of the block diagram. The advantage of using this combination of semi-Markov process model and probability rules is that the semi-Markov method is faster than

Monte Carlo simulations and does not need additional variance reduction methods. The proposed technique has potential in virtually every field of reliability analysis. However, for modeling aspects such as spares, crew availability etc. in a large and complex system, Monte Carlo simulation method continues to be the tool of choice.

4.4 Substation Reliability and Cost Analysis

A reliability model to study the effect of number of spares on a system comprising of a series of transformers in a substation is developed. The model takes ageing of the transformers in to consideration. This is achieved by developing a semi-Markov model assuming Weibull distribution for failure times. Further, it is assumed that the transformers are repairable. The results for both Markov and semi-Markov models are compared and the advantage of considering variability in failure times as measure of ageing is demonstrated. Further, a substation cost model is developed to determine the ideal number of spares to have in the inventory.

4.4.1 Problem

Redundancies and spares are expensive, yet well established ways of preventing a mission critical system from failing. daSilva et al. (2010) proposed Markov and Monte Carlo simulation methods to determine the optimal number of spares that minimize the total cost. The paper compared the obtained results against a model based on Poisson distribution. Marseguerra et al. (2005) applied a combination of Monte Carlo simulation and genetic algorithms to optimize the number of spare parts required by a multi-component system. The objective was to maximize the system revenues and minimize the total spares volume. While the Markov model assumes constant failure rates irrespective of the variability in the transformer failure times, the Monte Carlo simulation is prone to large variability in reliability estimates and demands specialized variance reduction techniques. Hence, the present paper studies the effect of number of spares on substation reliability based on the semi-Markov framework so that non-exponential distributions like Weibull can be considered in the model implementation. The major advantage of this extension is to study the ageing effects on the system. The paper further focuses on a predictive financial model to determine the ideal number of spares to invest upon in order to avoid economic losses due to unforeseen outages. The proposed model is of interest to technical personnel to have reliability estimates at hand and for station owners to decide how much investment needs to be made on spare transformers.

The case study is organized as follows. Section 4.4.2 discusses a Markov model for substation reliability. A subsection in it shows an example with two spares and develops the required differential equations. The theory for semi-Markov model is covered in Section 3.3. Section 4.4.4 deals with the semi-Markov solution of the transformer problem. Markov and semi-Markov results are shown for a 12 transformer system with different number of spares. The Markov reward (cost) model is reviewed in Section 2.7. Section 4.4.5 develops the cost model for determining losses due to repairs and outages. Results are reported in Section 4.4.6.

4.4.2 Markov model

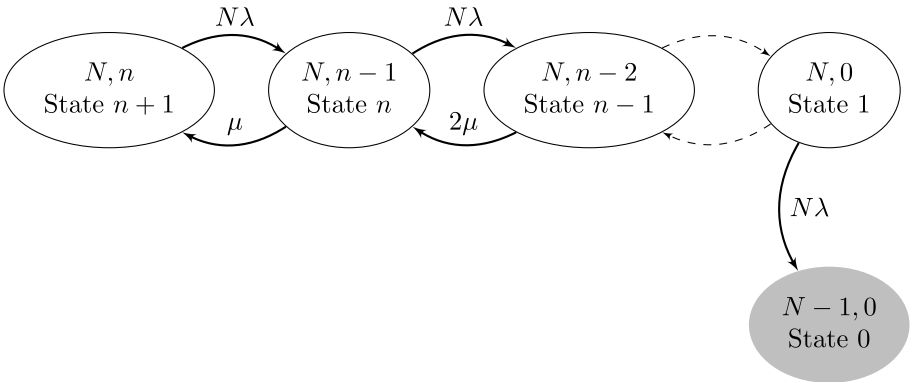


Figure 4.28: State space for N Transformers with n Spares.

Consider N transformers connected in series with n spares available for replacement on failure of any of the operational transformers. It is assumed that when all the spares are used up and at least one of the transformers in use fails, then the system fails. Further, the time taken to replace a failed transformer with a spare is assumed to be negligible. While a single transformer could fail with a failure rate of λ, it can be repaired with a repair rate of μ. The state space diagram for this model is shown in Figure 4.28. For a system with n available spares there are $n+2$ states in the model. Assume that the system starts in state $n+1$ where all the transformers are functional and all the spares are readily available. Then, the probability of landing in state 0 gives the failure probability of the system. The model in daSilva et al. (2010) assumes that two or more transformers are connected in parallel. In the present paper, the same model is considered without redundancies.

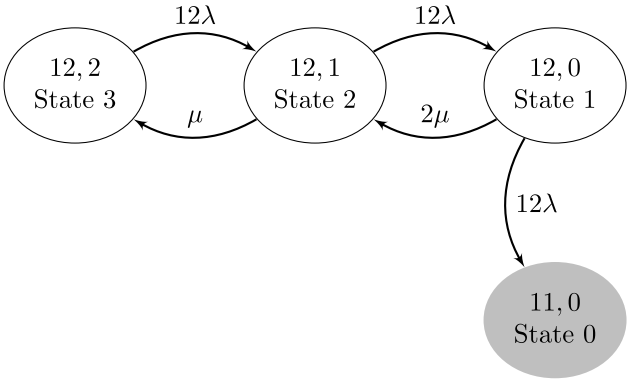


Figure 4.29: State space for $N = 12$ Transformers with $n = 2$ Spares.

4.4.3 Example: 12 Transformers and 2 Spares

In particular, consider an example with $N = 12$ transformers and $n = 2$ spares. The Markov transition rate matrix for this case is given by:

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ N\lambda & -(N\lambda + 2\mu) & 2\mu & 0 \\ 0 & N\lambda & -(N\lambda + \mu) & \mu \\ 0 & 0 & N\lambda & -N\lambda \end{bmatrix} \tag{4.22}$$

Let $\mathbf{P}(t)$ be a row vector of state probabilities to be determined:

$$\mathbf{P}(t) = [p_0(t)\ p_1(t)\ p_2(t)\ p_3(t)] \tag{4.23}$$

Then, the system of differential equations to obtain the state probabilities can be compactly written in matrix form:

$$\frac{d\mathbf{P}(t)}{dt} = \mathbf{P}(t)A \tag{4.24}$$

or elaborately as:

$$\begin{aligned} dp_0(t)/dt &= N\lambda p_1(t) \\ dp_1(t)/dt &= N\lambda p_2(t) - (N\lambda + 2\mu)p_1(t) \\ dp_2(t)/dt &= 2\mu p_1(t) + N\lambda p_3(t) - (N\lambda + \mu)p_2(t) \\ dp_3(t)/dt &= \mu p_2(t) - N\lambda p_3(t) \end{aligned} \tag{4.25}$$

$p_0(t)$ yields the failure probability of the system assuming the initial state vector as [0 0 0 1].

4.4.4 Semi-Markov model for substation reliability

The kernel matrix of the semi-Markov process model consists of statistical distributions respecting the competing risk law of Equation 3.5 instead of constant transition rates. The failure time distributions are modeled as poly-Weibull distributions while the repair times follow an exponential distribution. This section describes how these distributions can be used to construct the kernel matrix.

The *cdf* of the poly-Weibull distribution for the transition time corresponding to the failure rate $N\lambda$ in the Markov model of Figure 4.28 is given by:

$$F_{i,i-1}(t) = 1 - e^{-N(\lambda' t)^{\gamma}} \tag{4.26}$$

where the subscript $i, i-1$ represents the transition from state i to $i-1$ signifying failure of a transformer and replacement by a spare.

The corresponding *pdf* is found by differentiating Equation 4.26:

$$f_{i,i-1}(t) = N(\lambda'\gamma)(\lambda' t)^{\gamma-1} e^{-N(\lambda' t)^{\gamma}} \tag{4.27}$$

Assuming that the repair time follows an exponential distribution, the *cdf* of the time to repair is the minimum of all the times taken to repair the failed k transformers each having a repair rate of μ:

$$G_{i,i+1}(t;k) = 1 - e^{-k\mu t} \qquad\qquad i \neq 0 \tag{4.28}$$

The corresponding *pdf* is:

$$g_{i,i+1}(t;k) = k\mu e^{-k\mu t} \qquad\qquad i \neq 0 \tag{4.29}$$

The kernel matrix $C(\tau) = [c_{ij}(\tau)]$ is given by arranging the distribution functions as per Equation 3.5:

$$\begin{array}{cc} & \begin{array}{cccccc} 0 & 1 & 2 & . & n & n+1 \end{array} \\ \begin{array}{c} 0 \\ 1 \\ . \\ . \\ n+1 \end{array} & \left(\begin{array}{cccccc} 0 & 0 & 0 & . & 0 & 0 \\ f_{10}(\tau)[1-G_{12}(\tau;n)] & 0 & g_{12}(\tau;n)[1-F_{10}(\tau)] & . & 0 & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & 0 & & f_{n+1,n}(\tau) & 0 \end{array}\right) \end{array}$$

The integral equations corresponding to the above kernel matrix can be formulated based on Equation 3.9. The system is then solved using numerical scheme like trapezoidal rule as given in the appendix. Assuming that the system starts functioning in state $n+1$, the probability of being in state 0 denoted by $\phi_{n+1,0}(t)$ gives the system failure probability.

The system of integral equations for $N = 12$ and $n = 2$ is given as an example in the appendix.

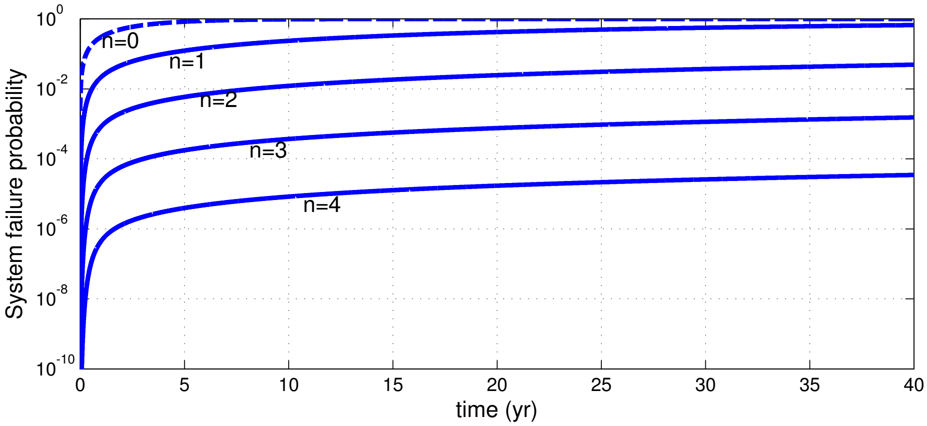


Figure 4.30: System failure probability with exponential failure and repair time; 12 transformers and $n = 0, 1, 2, 3, 4$ spares.

Considering a constant failure rate of $\lambda = 0.03$ per year and a repair rate of 4 per year for a transformer and supposing there are $N = 12$ such transformers connected in series, Figure 4.30 shows the system failure probability by solving the system of differential equations of the Markov model and the system of integral equations of the semi-Markov model proving that the results are identical no matter which method is used by assuming an exponential distribution for both failure and repair times. In both cases, varying number of spares were considered. It is also observed that failure probability is inversely related to the number of spares *i.e.*, system reliability improves with increased number of spares.

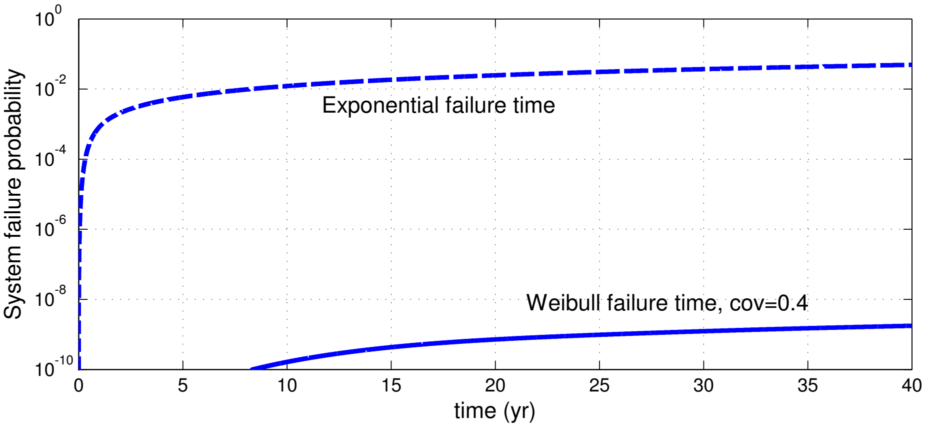


Figure 4.31: System failure probability comparing Webull and exponential failure time; 12 transformers and 2 spares.

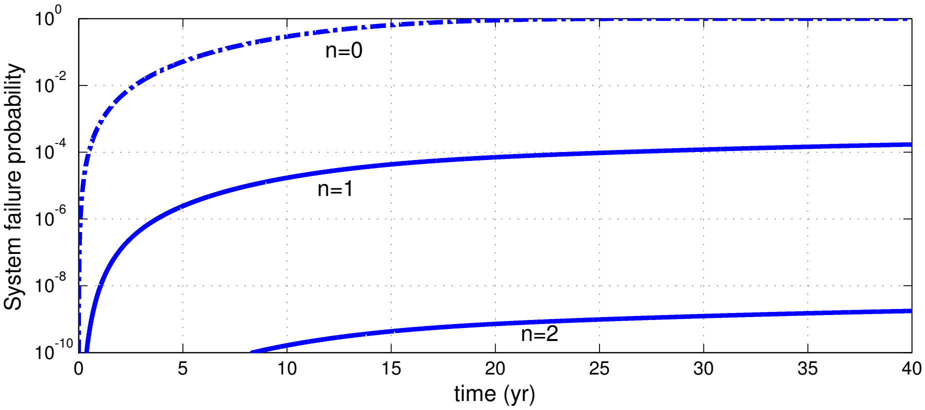


Figure 4.32: System failure probability with Webull failure time and exponential repair time; 12 transformers and $n = 0, 1, 2$ spares.

In the absence of spares, system failure probability reaches 0.9999 at the end of 40 years. In this scenario, there are only two states in the system and either all the transformers are functional or the system fails due to failure of one of the transformers. Addition of a spare lowers the failure probability to 0.667 thus boosting the system reliability by approximately 33%. In this case, there are three states in the system. When one of the spares is used, the failed transformer can undergo repair. After completion of the repair, a spare can be made available again. However, if one of the transformers fails when the spare is being used, then the system fails as the earlier failed transformer is still under repair. Adding further spares increase the reliability, however, beyond a certain number of spares, the system would become too reliable to afford the spares.

Figure 4.31 compares the system failure probability for the case of two spares assuming exponential and Weibull failure times respectively at the end of 40 years. A *cov* of 0.4 is assumed for the Weibull case. While the system failure probability for the exponential case is 4.92 x 10^{-2}, the same for Weibull case is 1.76 x 10^{-9} signifying that lower variability in failure times yields higher reliability. The same trend is observed for varying number of spares in Figure 4.32 assuming Weibull transformer failure times. Random failures often show up large variation in failure times whereas those of a cohort of ageing transformers are likely to show less variability.

Table 4.8: System failure probability as a function of number of spares at $t = 40$ years

	Failure time	
# Spares	Exponential ($cov = 1$)	Weibull ($cov = 0.4$)
0	0.9999	0.9999
1	6.67 x 10^{-1}	1.70 x 10^{-4}
2	4.92 x 10^{-2}	1.76 x 10^{-9}
3	1.53 x 10^{-3}	6.15 x 10^{-15}
4	3.47 x 10^{-5}	9.89 x 10^{-21}

Table 4.8 compares the effect of adding more spares to a system at the end of 40 years by assuming Weibull and exponential transformer failure times respectively. A *cov* of 0.4 was assumed for the Weibull case. In both cases, the repair time is exponentially distributed. Both the results show that the system performs better by having more spares. The failure probability when there are no spares is very high. Since it is assumed that the transformer failure time is less variable in the Weibull case, the system failure probability drops to 1.76 x 10^{-9} by having one spare against no spares. When system reliability is analyzed along with a financial model, these results can have a profound impact on decision making and budget allocation with respect to spare handling. However, one has to invest in more accurate and regular reporting of transformer failure times if variability is also needed as the input. In either case, simultaneous transformer failures due to common cause failures is not considered in the present paper. The next section explores the Markov reward model as an aid in deciding the ideal number of spares to have in the stock.

4.4.5 Cost Model for Substation Spares

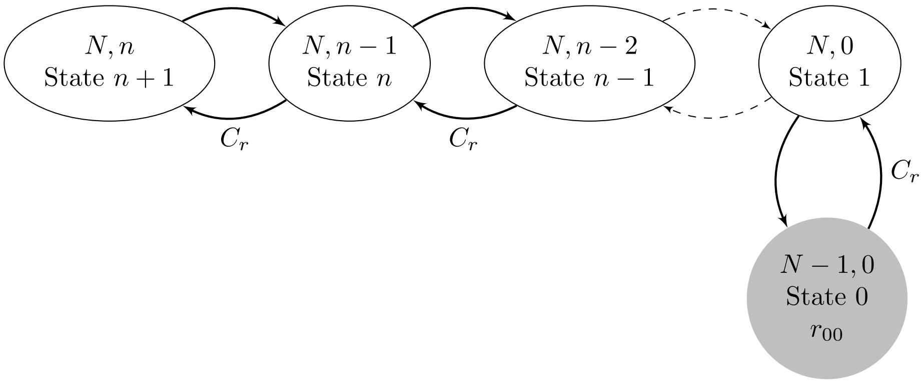


Figure 4.33: Markov Reward Model for N Transformers with n Spares.

The state space for the reward model is similar to the Markov model of Figure 4.28 except that the system is assumed to be repairable from state 0. Each repair is assumed to cost C_r million dollars. A loss of r_{00} million dollars per year is assumed on an outage which is equivalent to the process staying in state 0 and waiting for a system repair to be completed. This loss is based on kilowatts of energy per year not supplied to the consumer until the system goes online again.

The Markov reward model with the specifications described is shown in Figure 4.33. The Markov reward matrix r is a square matrix obtained from the state space:

$$\begin{array}{c|ccccc|} & 0 & 1 & 2 & ... & n+1 \\ 0 & r_{00} & C_r & 0 & ... & 0 \\ 1 & 0 & 0 & C_r & ... & 0 \\ . & . & & & & \\ . & & . & & & \\ . & & & . & & \\ n & 0 & 0 & 0 & ... & C_r \\ n+1 & 0 & 0 & 0 & ... & 0 \end{array} \tag{4.30}$$

4.4.6 Results and discussion

The list of symbols in the model and the assumed values are listed in Table 4.9.

Table 4.9: Parameters for evaluating the cost model

Symbol	Description	Assumed Value
λ	Failure rate of transformer	0.03 yr^{-1}
μ	Repair rate of transformer	4 yr^{-1}
N	Number of transformers connected in series	12
n	Number of required spares	0,1,2,. . .
L	Nominal capacity of one transformer	10^5 kW
C_r	Expected cost of repair of one transformer	C$ 0.05 million
C_j	Expected cost of one spare transformer	C$ 8 million
C_p	Cost of Energy Not Supplied (ENS) per kWh	C$ 1.00
r_{00}	Cost of ENS per year = C_pL x 8760	C$ 876 million
m	Assumed lifespan of a plant	40 years
r	Discount rate	0.07

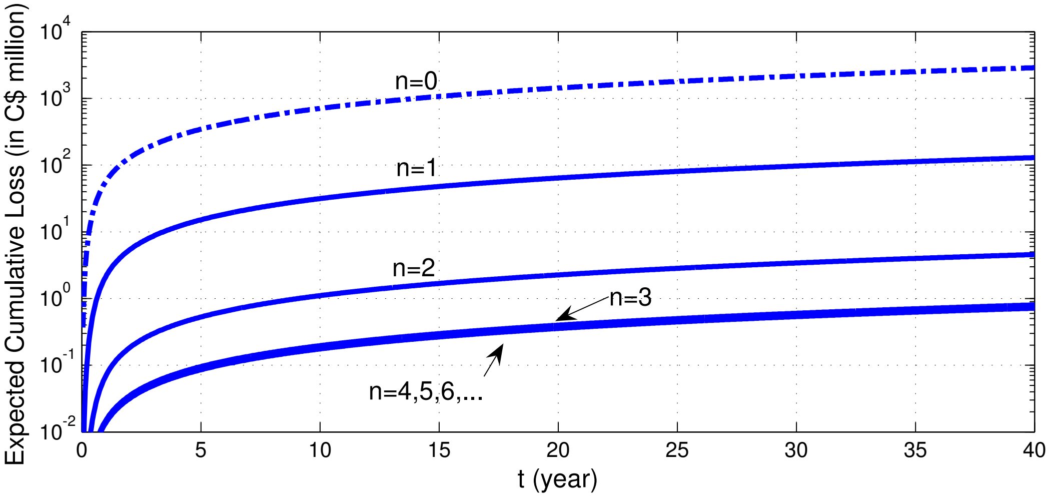


Figure 4.34: Expected Cumulative Losses for 12 Transformers and n Spares.

The accumulated economic loss due to repairs and outages up to m years is shown in Figure 4.34. The reward model does not yet consider the investment on procuring the spares. It is seen that the expected loss is the maximum when there are no spares available in the inventory. For 1,2 or 3 spares, the expected loss decreases and then it is observed that the average loss is the same no matter how many more spares are added.

To get a complete picture, the amount invested on the spares and the net present cost obtained by combining the investment and the net present value of the expected losses is investigated in the next step.

From the cumulative expected losses $V_4(t)$ of the reward model, from hereon referred to as $V(t)$, the annual combined cost of repairs and outages can be calculated as $v_k = V(k+1) - V(k)$ for $k = 1, 2, 3, ..m$ for the m years under consideration. The net present value of the losses is represented as L_j, where j represents the number of spares. The NPV L_j of the annual costs $v_1, v_2, ..v_m$ discounted at a rate r over m years is then calculated as:

$$L_j = \sum_{i=1}^{m} \frac{v_i}{(1+r)^i} \tag{4.31}$$

Let C_j denote the investment made on procuring j spares. The net present cost of losses and investments for j spares is given by $A = L_j + C_j$. The objective then is to determine for what j the value of A is minimum.

Table 4.10: Net present cost of investments and losses

Spares	Investment	NPV of Losses	Net Present Cost
j	C_j	L_j	$C = L_j + C_j$
	C$ million	C$ million	C$ million
0	0	949.01	949.01
1	8	42.37	50.37
2	16	1.49	17.49
3	24	0.26	24.26
4	32	0.24	32.24
5	40	0.24	40.24

Table 4.10 tabulates the net present cost as a function of number of spares. It is seen that the NPV of the losses remains constant beyond three spares. The net present cost is 949 million dollars in the absence of spares highlighting the huge risk involved in running a generating station without spares. With addition of two spares, the net present cost is seen to decrease to nearly 18 million dollars and then increases monotonically if the station decides to invest in more than two spares. This concludes that for the given configuration and assumed costs, it is optimal to have two spares always in the inventory.

Figure 4.35 shows graphically the trend seen in Table 4.10. A simple and final plot as this is of great aid to decision makers for budget allocation and for the smooth and reliable running of the station.

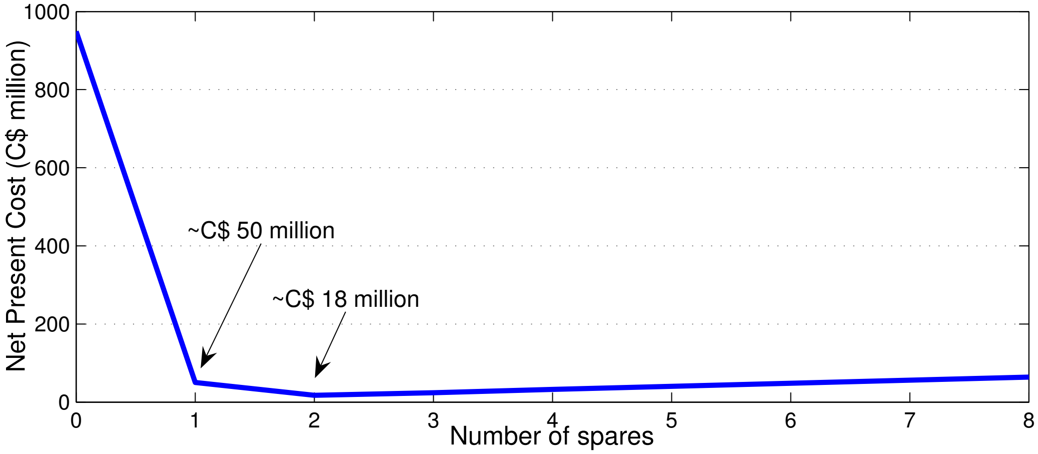


Figure 4.35: Net present cost vs.the number of spares.

4.4.7 Conclusion

A semi-Markov model with Weibull failure times was developed for assessing reliability of ageing transformers. Results were compared against a Markov model and was proved that knowledge of variability in failure times of the transformers helps in obtaining more accurate estimates of system reliability. The Markov model was further extended to a Markov reward model to determine the number of spares to have in the inventory at all times to avoid economic losses due to unforeseen outages.

4.5 A Semi-Markov Fire Growth Model

This paper aims to describe a new fire growth model that allows prediction of fire development, including time to flashover, with inclusion of the unpredictable nature of real fire development and, where available, appropriate fire test data. The model considers potential variability in the times at which the fire will undergo transitions between the various stages of development, using a state transition method called semi-Markov process model. By assuming that the fire goes through five different stages starting from ignition and progressing to flashover, the total time to flashover may also be estimated. Perhaps most importantly, the model is based on a reusable framework which can be modified for use with different sets of fire data and is flexible enough for use in a variety of applications important to both product design engineers and fire safety regulators.

4.5.1 Introduction

Fire is a complex physical phenomenon driven by interactions between chemistry, fluid dynamics and heat transfer within the fire compartment. As such, there is significant variation in fire behavior even in repeated tests of specific fire scenarios. This variation can be attributed not only to the complex physics driving the fire behavior itself, but also to the arrangement and geometry of the fuel, as well as numerous environmental factors. In a real fire, availability of fuel and air, as well as attempts to suppress the fire, due to consecutive fluctuations between fire growth and recession. The many sources of variation inherent if real fire development make probabilistic approaches the favorable choice with which to model the full chronology of a fire.

Probabilistic models have been developed for a wide variety of applications relating to fire safety, including fire detection (Joglar et al., 2005), fire growth (Au et al., 2007; Hasofer and Beck, 1997; Williamson, 1981), fire spread (Rasbash et al., 2004; Colbourn et al., 1994; Platt et al., 1994; Ramachandran, 1991; Morishita, 1985), smoke spread (Hadjisophocleous, 1992; Watts, 1986), and safe egress (Hasofer and Odigie, 2001). Of most interest here are fire growth models which include fire inception and growth up to flashover within a single compartment, and fire spread models which consider the spread of fire from compartment to compartment within a multi-enclosure building.

In these applications, a wide range of modeling techniques have been explored for fire modeling including Bayesian networks (Cheng and Hadjisophocleous, 2009),Monte Carlo simulation (Au et al., 2007; Joglar et al., 2005), stochastic differential equations based on physical laws (Hasofer and Beck, 1997), network reliability techniques(Hasofer and Odigie, 2001; Colbourn et al., 1994), stress-strength models in the context of fire barriers(Platt et al., 1994; Watts, 1986), state transition methods(Berlin, 1985; Williamson, 1981) and other stochastic models(Ramachandran, 1991) including epidemic theory, percolation process and random walk. Graphical(Watts, 1986) means of representing fire resistance and growth include circuit diagrams, fault trees, fire safety trees and logic trees whose quantification can be done using simple probability rules.

Bayesian network models combine graph theory and Bayesian probability theory. For example, in modeling fire spread in an office building fire, the office floor is transformed into a directed acyclic graph (DAG) with the room of origin taken as the root node and assigned an ignition probability (Cheng and Hadjisophocleous, 2009). Fire spread for rest of the nodes is predicted using probabilities conditioned on the root node probability. Computations are performed for two cases: one with fire protection but no suppression and the other for a building with sprinklers. The model produces static fire spread probabilities but no time information is provided on the progress of the fire with time. Though theoretically it could be extended to predict time dependent behaviour, the mathematics would involve multiple integrals and their solution would require Markov Chain Monte Carlo (MCMC) type numerical simulations. Of course, the difficulty in formulating stochastic differential equations based on physical laws depends on the configuration of the compartment and complexity of the fire scenarios under investigation, but even simplified situations result in the need to do Monte Carlo simulations. In general, Monte Carlo simulations are computationally intensive, requiring long calculation times to cover a sufficient range of cases to appropriately model a given scenario. Therefore, hybrid models based on combinations of Monte Carlo and other fire modelling methods have also been developed.

Such hybrid models have gained popularity for modeling fire behaviour in nuclear power plants where the occurrence of a fire is an extremely rare event. In this industry, a fire may progress from ignition of a fuel spill to a larger fire which damages critical electrical cable trays and could lead to reactor core damage. It is clearly of primary interest to determine the core damage frequency (CDF); however, a probabilistic approach must be taken due to uncertainty in fire initiation, in damage to equipment and fire brigade response(Vinod et al., 2008). A combination of fire models such as CFAST(Peacock et al., 1986), FDS(McGrattan, 2004) or COMPBRN(Siu, 1982) are used with Monte Carlo simulation and probabilistic safety assessment (PSA) event/fault tree tools like SAPHIRE(Idaho National Engineering Laboratory, 2010) to determine the estimated frequency of a fire leading to core damage (Valbuena and Modarres, 2009; Siu and Apostolakis, 1982; Lee et al., 2010; Arshi et al., 2010; Hostikka and Keski-Rahkonen, 2003; Frank and Moieni, 1986).

Network reliability methods also take a graph theoretic approach to modeling fire propagation through a multi-enclosure structure. Each node represents a room and is associated with an ignition probability and a fire spread probability. The arcs are used to designate barriers to fire spread and therefore each is given a fire breach probability. The goal is to start from the node of fire origin and recursively traverse through various directed paths until the target room (a leaf) is reached, using probability rules to arrive at the fire spread probability to that target. While such an approach has been developed theoretically in Colbourn et al. (1994) by drawing an analog from communication networks, the fire time dimension is missing in the formulation so important events such as time to flashover cannot be determined.

Other approaches have visualized growing and receding fires as a game between two gamblers and utilized stochastic random walk theory to predict the time to fire extinguishment (Ramachandran, 1991). This method does not, however, account for various stages that a fire under goes from inception to flashover. This method has been extended to examine building to building fire spread via a percolation process (i.e. random walk over a graph) and predict the average number of buildings burnt. In both manifestations, however, there is no consideration made of the various stages of fire growth or development and time dependence is lacking.

Stress-strength models consider two random variables with fire severity modeled as the stress and fire resistance of the barrier modeled as the strength. For fire protection, it is of interest to calculate the probability that the fire resistance is greater than the fire severity. Again, however, no account is taken of the various stages of fire growth and spread, nor of any time dependence of the real fire event(Platt et al., 1994; Watts, 1986).

The spread of fire is dynamic in nature and the variability in real fire scenarios is best modeled as a continuous time dependent process with threshold conditions defining the discrete stages of fire development. Hence, the present paper adopts a state transition approach to fire growth modeling which allows representation and quantification of the key events in the overall fire development. In the next section, existing state transition models for fire analysis are reviewed.

A stochastic state transition model of fire spread has been developed and applied to a hypothetical small house fire to illustrate its effectiveness(Morishita, 1985). Fire spread was analyzed both with and without fire extinguishment. It was assumed that the fire propagates discretely from one space to another and that an arbitrary point in space could ignite due to heat transfer from any other points in the vicinity. While this assumption may be valid and fairly realistic, when incorporated into the model, the number of states in the model grows exponentially with increasing numbers of possible surrounding points of interest. This makes it difficult to determine the rate at which the fire grows between each pair of required points.

In other work, six states were defined in the fire growth model (FGM) of fire development (Williamson, 1981). The states included fire ignition, fire spread to (ignition of) surrounding wall and furniture, fire impingement on the ceiling, flashover, well ventilated fire with steady state burning, and finally, fire burn out. The state transition model was depicted in the form of an event diagram. Deterministic models, supported by experimental data from the U.S. National Bureau of Standards (NBS), were then used to predict the overall fire behavior. For example, within the final model, a set of differential equations was solved to arrive at a distribution to represent the time taken for flames to touch the ceiling. However, the approach does not identify and treat the sources of variability in the prediction.

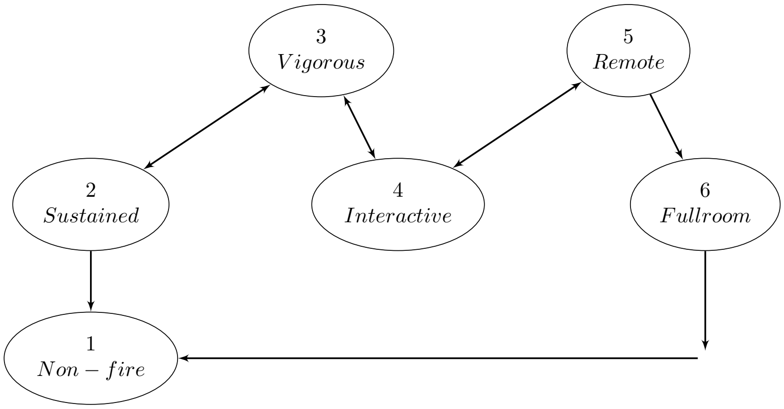


Figure 4.36: State transition model for fire growth.

A more versatile state transition model depicted in Figure 4.36 was based on fire test results and was developed to explain variability in the development of a smoldering fire in a couch with cotton cushions(Berlin, 1985). Statistical distributions were fit to fire test data and the time to transit from one state to another was taken as a random variable. The model was an early attempt to incorporate non-exponential distributions to represent the time to transit from one state to another. Although the exact computations and numerical approximations were not clearly outlined in the paper, the convolution of the random variables led to a probabilistic distribution of the time it would take a given fire to reach flashover. While this model provided a good first step, since its development there have been tremendous advances in state transition models and in computational power, pointing to an opportunity for refinement and/or enhancement of the original concepts. This forms the premise for development of the model outlined here.

Berlin (1985) developed a state transition model (Figure 4.36) based on fire tests to explain the variability of a smoldering fire in a couch with cotton cushions. This paper fitted statistical distributions to fire test data assuming that the time to transit from one state to another is a random variable. The model was an early attempt to incorporate non-exponential distributions to represent the time to transit from one state to another. The result was a probabilistic distribution of a fire ending up in a flashover. Apparently, the results were obtained using convolution of random variables. Further, the paper lacks ideas and thoughts on what computations and numerical approximations were performed. Since then, there have been tremendous advancements in mathematical models and computer programming.

A sophisticated state transition model, which has been successfully applied to model failures in nuclear power plant systems is the semi-Markov process model (Veeramany and Pandey, 2011c,b,a). Using such a model, fire growth can be modeled as a continuous-time, discrete-state process with a wide variety of non-exponential distributions utilized to appropriately describe the time spent in each of the possible fire states. The present paper applies this method to model fire behavior, employing the widely used normal and log-normal distributions to represent the various stages of fire growth. For purposes of illustration and comparison, the new method is initially applied using concepts of fire development and data presented by Berlin (1985); however, it is important to contrast the fundamental bases of the techniques by Berlin (1985) with those applied here. While the method by Berlin (1985) involved the direct convolution of random variables, the semi-Markov process model presented here is based on a structured mathematical approach. Therefore, the background to the present model will first be described and then the method applied to predict average times to flashover based on the maximum probability and the likelihood that an ignited fire does or does not reach flashover conditions for a given fire scenario.

4.5.2 The fire growth model

Table 4.11: Classification of states based on fire characteristics (Berlin, 1985).

	State	Upper Room	Flame	Heat
		Temperature	Height	Release Rate
1	Non-fire	Normal	-	-
2	Sustained/Ignited	Normal	-	-
3	Vigorous	$> 15^oC$	25 cm	> 2 kW
4	Interactive	$> 150^oC$	120 cm	> 50 kW
5	Remote	$> 450^oC$	-	-
6	Full room	$> 800^oC$	-	-

The six transition states chosen for use in the present model mirror those presented by Berlin (1985) as listed in 4.11. These are defined based upon values of upper layer room or ceiling layer temperature, flame height and heat release rate.

The first state is the non-fire state and represents a pre-flaming stage of the fire. While it was used to represent a smouldering phase in the original model (Berlin, 1985), for the present paper, it in itself, does not lead to ignition. Instead it is used as the end, non-fire, state in the case when a growing fire does not continue to full room involvement but instead recedes back, possibly through intermediate stages, to a non-fire state. The second state is the situation in which ignition occurs and the first item ignited begins to burn in a sustained manner. A fire then grows from this state, undergoing transitions to the other states based on it reaching and exceeding the threshold criteria for each state, as listed in Table 4.11. The names of states 4 and 5 are taken directly as those assigned by Berlin (1985); however, it should be noted that no clear explanation was provided for these terms in the original source. Therefore, in this work, the ‘interactive’ stage is defined as the period of time during which surrounding objects might be ignited and contribute to flame spread. The ‘remote’ burning stage is defined as the transition zone to full room involvement (according to Berlin (1985), the external heat flux returning to the fuel surface exceeds 5 kW/m^2 during this period). A given fire need not go through the entire cycle of all states in the model. It can recede from any state to a lower state due to lack of oxygen, lack of fuel or suppression by a fire protection system or even manual suppression by firefighters. In these cases, as in the real situation, the fire can return to the non-fire state without ever reaching flashover. On the other hand, if a fire does grow and reach flashover, in reality the fire physics and dynamics change very rapidly. This is accounted for in the present model, since all fires that have reached flashover (i.e., all post-flashover fires) are forced to remain in the state of 'full-room' involvement and cannot recede back to any previous state.

Table 4.12: Temporal distributions for the state transitions assumedBerlin (1985).

	State Transition	Distribution	Mean (min)	Std. dev. (min)
2 → 1	Sustained to Non-fire	Uniform	2.0	5.0
2 → 3	Sustained to Vigorous	Log-normal	8.45	0.78
3 → 2	Vigorous to Sustained	Uniform	1.0	2.0
3 → 4	Vigorous to Interactive	Normal	5.55	3.22
4 → 3	Interactive to Vigorous	Uniform	1.5	9.0
4 → 5	Interactive to Remote	Uniform	0.5	3.5
5 → 4	Remote to Interactive	Uniform	0.6	6.0
5 → 6	Remote to Full-room	Log-normal	5.18	4.18

Once the transition states have been defined, it is of interest to determine the time it takes a fire to transit from one state to another. Since, this is highly variable and uncertain in any real fire scenario, the transition times from state to state are considered as random variables with associated statistical distributions in the present model. Based on fire test data, a combination of discrete and continuous distributions were used in previous model (Berlin, 1985) as shown in Table 4.12. There is no justification provided for the choice of distribution, for example, as to why a receding fire was assigned a discrete uniform distribution.

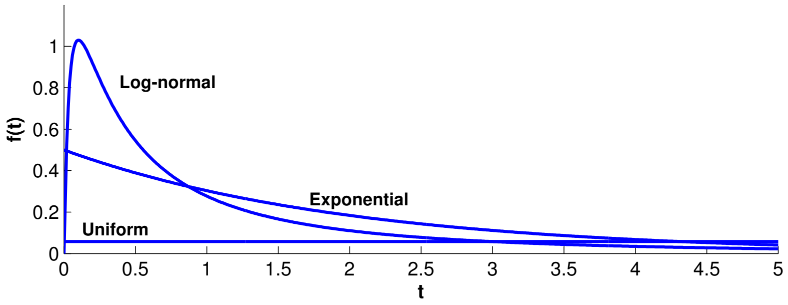


Figure 4.37: Comparison of distributions for 2 → 1 with mean 2.0 min and *s.d.* 5.0 min.

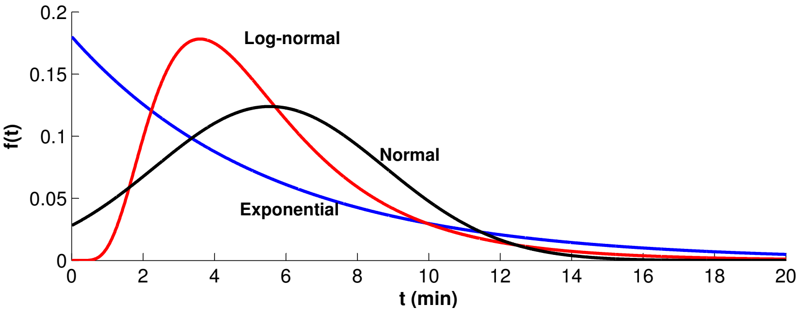


Figure 4.38: Comparison of distributions for 3 → 4 with mean 5.55 min and *s.d.* 3.22 min.

The authors believe that the appropriate choice of distributions is contextual based on the material and/or test data. For example, Figures 4.37 and 4.38 show various distributions fit to a decaying and growing fire for the transitions 2 → 1 and 3 → 4 respectively. Exponential distribution is a good fit for decaying fires, lognormal and normal are good for fires that grow gradually and then exhibit a slowing trend. Exponential distribution for the forward transition is sensible in the context where there is a high probability of an instant transition during a rapid fire growth. Uniform distribution associates with equal chance at all times during a transition.

Table 4.13: Various configurations differing in distributions chosen for state transitions

Case#	Configuration
1	As listed in Table 4.12
2	Backward transitions in Table 4.12 replaced with exponential distribution
3	All transitions in Table 4.12 replaced with log-normal distribution
4	All transitions in Table 4.12 replaced with exponential distribution

The present model explores the possible configurations as listed in Table 4.13. One key difference over the distributions assigned in Berlin (1985) is that all backward transitions in the present work are assumed to follow a continuous distribution, a justifiable assumption since both fire growth and recession occur on a continuous time scale but at times occupy the discrete states defined in the model. Further, it was assumed in Berlin (1985) that all fires that did reach the stage of full room involvement were automatically reset to the non-fire state and no temporal distribution was associated with this state transition. In the present model, the transition from full room involvement to non-fire state is not included as it would necessitate significant additional data to properly describe this transition across real fire scenarios.

Table 4.14: Case 1:Assumed distributions for the state transitions based on Berlin (1985)

Transition	Distribution	Parameters	Mean (min)	Std. Dev. (min)
$2 \rightarrow 1$	Uniform	a= -6.66 b= 10.66	2.00	5.00
$2 \rightarrow 3$	Log-normal	μ=2.13 σ^2=0.01	8.45	0.78
$3 \rightarrow 2$	Uniform	a=-2.46 b=4.46	1.00	2.00
$3 \rightarrow 4$	Normal	μ= 5.55 σ^2=10.37	5.55	3.22
$4 \rightarrow 3$	Uniform	a=-14.09 b=17.09	1.50	9.00
$4 \rightarrow 5$	Uniform	a=-5.56 b=6.56	0.50	3.50
$5 \rightarrow 4$	Uniform	a=-9.79 b=10.99	0.60	6.00
$5 \rightarrow 6$	Log-normal	μ=1.39 σ^2=0.50	5.18	4.18

Table 4.15: Case 2: Backward distributions in Table 4.14 replaced with Exponential distribution

Transition	Distribution	Parameters	Mean (min)	Std. Dev. (min)
$2 \rightarrow 1$	Exponential	λ= 0.5	2.00	2.00
$2 \rightarrow 3$	Log-normal	μ= 2.13 σ^2= 0.01	8.45	0.78
$3 \rightarrow 2$	Exponential	λ= 1	1.00	1.00
$3 \rightarrow 4$	Normal	μ= 5.55 σ^2= 10.37	5.55	3.22
$4 \rightarrow 3$	Exponential	λ= 0.67	1.50	1.50
$4 \rightarrow 5$	Uniform	a= -5.56 b= 6.56	0.50	3.50
$5 \rightarrow 4$	Exponential	λ= 1.67	0.60	0.60
$5 \rightarrow 6$	Log-normal	μ= 1.39 σ^2= 0.50	5.18	4.18

Tables 4.14 - 4.17 list the distributions assumed in the present model for each configuration listed in Table 4.13. These parameters are adapted from Berlin (1985) and therefore reflect the data of the 1970's. They are used here for illustrative

Table 4.16: Case 3: All distributions in Table 4.14 replaced with Log-normal distribution

Transition	Parameters	Mean (min)	Std. Dev. (min)
2 → 1	μ= -0.30 σ^2= 1.98	2.00	5.00
2 → 3	μ= 2.13 σ^2= 0.01	8.45	0.78
3 → 2	μ= -0.80 σ^2= 1.61	1.00	2.00
3 → 4	μ= 1.57 σ^2= 0.29	5.55	3.22
4 → 3	μ= -1.40 σ^2= 3.61	1.50	9.00
4 → 5	μ= -2.65 σ^2= 3.91	0.50	3.50
5 → 4	μ= -2.82 σ^2= 4.62	0.60	6.00
5 → 6	μ= 1.39 σ^2= 0.50	5.18	4.18

Table 4.17: Case 4: All distributions in Table 4.14 replaced with Exponential distribution

Transition	Parameter(λ)	Mean (min)	Std. Dev. (min)
2 → 1	0.50	2.00	2.00
2 → 3	0.12	8.45	8.45
3 → 2	1.00	1.00	1.00
3 → 4	0.18	5.55	5.55
4 → 3	0.67	1.50	1.50
4 → 5	2.00	0.50	0.50
5 → 4	1.67	0.60	0.60
5 → 6	0.19	5.18	5.18

purposes only; the model can be re-run any number of times using different and/or more current datasets with their associated distributions as may be required to model each new set of fire scenarios.

Flashover conditions

Prediction of average times to the onset of flashover is of key importance in defining compartment fire development since this is a time of extremely rapid fire growth

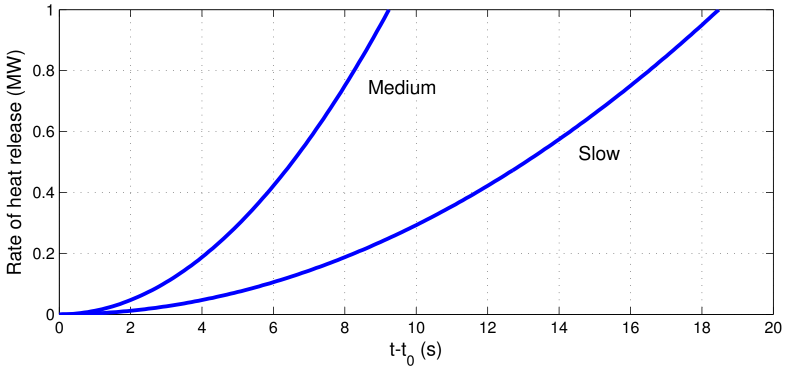


Figure 4.39: Parabolic fire growth for slow to medium fires.

leading to the everything in the room being involved in the fire. Despite this, the scientific definition of flashover is the subject of some debate and times to flashover for similar fire scenarios, even in controlled test situations, can vary greatly. For example, a set of three similar experiments on a furnished bedroom fire yielded flashover times of 17.6 min, 7.2 min and 6.5 min respectively (Croce, 1974) with the large differences attributed to variations in relative humidity. In other experiments, flashover conditions have been reported to occur at ceiling temperature of approximately 600^o C (Hagglund et al., 1974; Fang, 1975; Drysdale, 1998) in 2.7m high compartments or over 450^o C (Heselden and Melinek, 1975; Drysdale, 1998) in a 1m high experimental compartment. Alternative definitions suggest criteria such as heat flux level of 20 kW/m^2 to the compartment floor(Waterman, 1966). The minimum heat release rate (HRR) at which flashover is likely to occur, as per the 600^{o}C criterion, is around 1 MW (Babrauskas et al., 2003). Using these threshold values and a simplified correlation for fire growth, such as the parabolic or t^2 fire, the relation between heat release and time is given by Heskestad (1984):

$$\dot{Q} = \alpha_f (t - t_0)^2 \tag{4.32}$$

where $\dot{Q}$ is the heat release rate (KW), α_f is the fire-growth coefficient (kW/s^2) and t_0 is the initial incubation period (s).

These elements are used, with the fuel specified by Berlin (1985) to make an initial estimate of the fire development as a benchmark for the present work. The cotton cushions in Berlin (1985) can be categorized as resulting in slow to medium growth fires, with growth coefficients ranging between 0.00293 and 0.01172 (Drysdale, 1998). Based on this correlation and the proposed threshold HRR of 1 MW for flashover, it can be seen from Figure 4.39 that the times to flashover for the fires in Berlin (1985) should range from 9.2 to 18.5 min.

Recalling that the probability density function of a transition from state i to state j is represented by $f_{ij}(t)$ and the distribution function by $F_{ij}(t)$, and letting $R_{ij}(t) = 1 - F_{ij}(t)$, the kernel $C(t)$ of the semi-Markov process for the fire growth model can be written in its full matrix form using Equation 3.5:

C(t) =

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ f_{21}(t)R_{23}(t) & 0 & f_{23}(t)R_{21}(t) & 0 & 0 & 0 \\ 0 & f_{32}(t)R_{34}(t) & 0 & f_{34}(t)R_{32}(t) & 0 & 0 \\ 0 & 0 & f_{43}(t)R_{45}(t) & 0 & f_{45}(t)R_{43}(t) & 0 \\ 0 & 0 & 0 & f_{54}(t)R_{56}(t) & 0 & f_{56}(t)R_{54}(t) \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Further, the matrix $W(t)$ in Equation 3.8 can be computed numerically using methods outlined in the Appendix. The kernel matrix and the matrix $W(t)$ are then sufficient to solve for state probabilities. Finally, the probability of being in each of the states is computed by solving the system of integral equations in Equation 3.10 using the trapezoidal rule. The time at which the fires undergoes a transition to that state is taken as the time when the maximum probability of being in that state is reached.

The next step in setting up the model is to define a set of appropriate statistical distributions to use as the state transition descriptors. Appropriate functions can be determined from real fire test data when it is available; however, for the time estimates to be meaningful, the data used must be representative of the fire scenarios of interest. For example, transition descriptors in Berlin's model relied on test data collected between 1959 and 1975 from large scale dwelling and room fires. This data was based on fires initiated in sofas comprising cotton cushions. While this was a representative scenario at that time, new materials and upholstery construction methods will limit its utility for prediction of more modern fire scenarios. Nonetheless, for the purposes of comparison, the data from Berlin is used for the initial test case run with the present model. Then, to demonstrate the flexibility of the model, three combinations of transition state distributions were explored as listed in Table 4.13.

4.5.3 Results

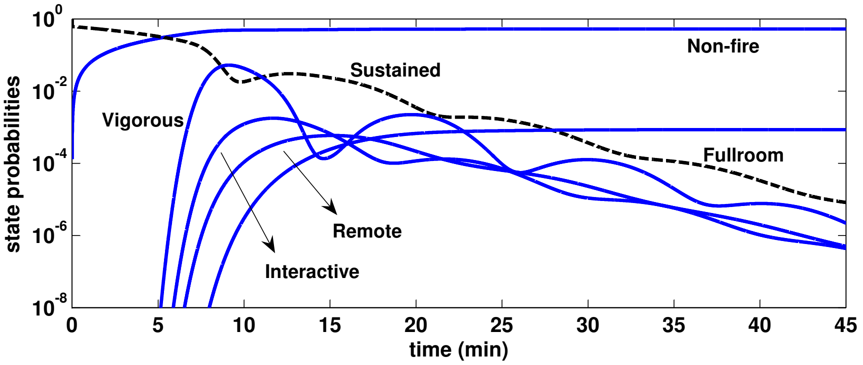


Figure 4.40: Probability of being in each state. Case 1.

Table 4.18: Time at which maximum state probabilities occur. [Case 1]

	State	Maximum probability (1)	Time (min) at which (1) occurs
3	Vigorous	0.05	9.1
4	Interactive	0.0002	11.7
5	Remote	0.0006	15.2

Figure 4.40 shows the calculated probabilities that the fire has reached a certain state at a given time, assuming the distributions for case 1 in Table 4.13. The corresponding times at which values of maximum probability are reached for the various states are summarized in Table 4.18. In these results, the fire is assumed to start in the sustained state (state 2), so the probability of being in each state after fire initiation is given by $\phi_{2j}(t)$. The probability of the fire having grown enough to enter any other state begins to increase after 5 minutes, reaches a maximum value at some time thereafter and then eventually begins to decrease. At the same time, the probability of the fire being in the sustained state (state 2) decreases in time, since the fire is indeed growing. If the fire does not sustain itself, it moves back to the pre-burning stage (state 1). The 5 minute delay could be attributed to the incubation period. For those fires that do grow, the peak probability of the fire growing large enough that the upper layer temperature reaches 450^{o}C, i.e.,

reaching the remote state (state 5), is slightly larger than the probability that the fire remains smaller, i.e., in the interactive state (state 4), but the differences are minimal since they are seen only when three digits of precision are used in the calculations. The difference is physically reasonable, however, because as would be expected in a real fire scenario, it often takes the fire longer to grow from a 450^oC upper layer temperature to full room involvement, than to grow from a 150^oC upper layer temperature to a 450^oC upper layer temperature. The maximum probability of full room involvement is slightly lower than those for either the remote or the interactive stages. This is again as expected since, in general, the probability of full room involvement is expected to be quite low. In reality, there is a lower chance of a fire growing to involve the entire room due to the many paths by which the fire can recede before growing to this point. However, since full room involvement is a high consequence event and is often linked to fire resistance and severity assessments, it can be important to estimate the time taken for the fire to grow to that stage. For this case and all others in the present work, the curve indicating full room involvement will more or less plateau without decay because this state is considered a final state which is not connected back to the non-fire state.

In contrast to the smoothed probability distribution for full room involvement is that for the vigourous state (state 3), where the fire is characterized by low flame heights and heat release rates. This distribution appears multi-modal, which may suggest that describing the transitions to and from this state using a single distribution may not truly represent the real fire data. Again, such an observation is consistent with true fire behavior, since, this stage of fire growth will be highly variable due to frequent fluctuations in development as the fire grows and recedes (Berlin, 1985).

The time-dependent realm frequency plot (Berlin, 1985) do not represent a statistical distribution. In contrast, the state probabilities in Figure 4.40 form a discrete distribution with their sum equal to 1 at all times. Hence not more than one state at any given time can have a probability be equal to 1. In the proposed model, probabilities of states 2 to 5 approach zero beyond 45 min so that the non-fire state probability starts increasing toward certain probability of 1.0. This gives an impression that every fire gets extinguished with in a finite time as per the collected fire test data.

If we retain the criterion that time to flashover corresponds to the time it takes the fire to enter into the remote state, and further that our best estimate of this time can be taken as the time at which we have the maximum probability that the fire is in that state, then the estimated time to flashover for Case 1 in Table 4.13 is 15.2 min. This falls within the range of 9.2min to 18.5min discussed in Section 4.5.2. It is longer, however, than both the comparable empirical estimate of 12.9 min made by the Illinois Institute of Technology Research Institute (IITRI) based on 68 fire tests (Vodvarka and Waterman, 1975) and the estimate of 11.6 min. made based on data from 100 fire tests including the IITRI test data (Berlin, 1985). The increase of more than 31% in time to flashover predicted here as compared to the 11.59 min listed above (Berlin, 1985) can be attributed to the fact that unlike previous estimates, consideration was included here of the fact that, in reality, a fire can recede from its present state to a less well developed state with time.

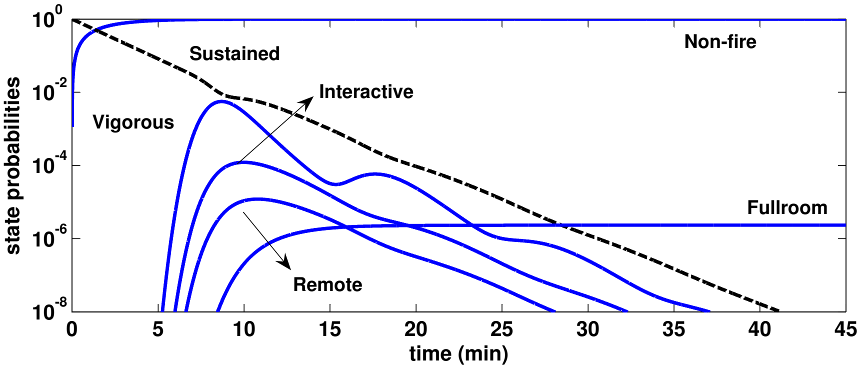


Figure 4.41: Probability of being in each state. Case 2.

Table 4.19: Time at which maximum state probabilities occur. [Case 2]

	State	Maximum probability (1)	Time (min) at which (1) occurs
3	Vigorous	0.005	8.7
4	Interactive	0.0001	10.0
5	Remote	0.00001	10.8

For realistic fire scenarios, it can be difficult to determine the possible variability in time that it might take for a fire to recede from one state back to another. A typical example might be an under-ventilated fire that grows and recedes at different rates across many tests. In these situations, it may only be possible to determine the mean time that it takes the fire to change from being in the remote state (state 4 based on criterion of 150^{o}C upper layer temperature) to being in the interactive state (state 5 based on criterion of a 450^{o}C upper layer temperature). It might then be assumed that the mean time for a transition is the same as the variability, which could be modeled using an exponential distribution with a constant rate of transition. Hence, this case is scenario reflecting that reflects inadequate data collection mechanism, yet incorporating a possible variability information in to model. It is inferred that the resulting time to flashover estimate could be either over or under predicted. This situation is modeled in Case 2 (Table 4.15) where all backward transitions are set to follow exponential distributions. The results are plotted in Figure 4.41. They indicate less fluctuation in the state probabilities than seen for Case 1, with the highest probability that the fire will grow only slightly and less and less probability that ceiling temperatures will reach 150^{o}C (remote), 450^{o}C (interactive) or full room involvement. As indicated in Table 4.19, the maximum probability of the fire reaching each state is lower overall and the fire likely to decay much earlier than in Case 1. Finally, time to reach any given fire growth state, and therefore time to reach flashover, is much shorter, around 10.8min, since the large variability in the fire test data is essentially neglected in the backward distributions used for this case.

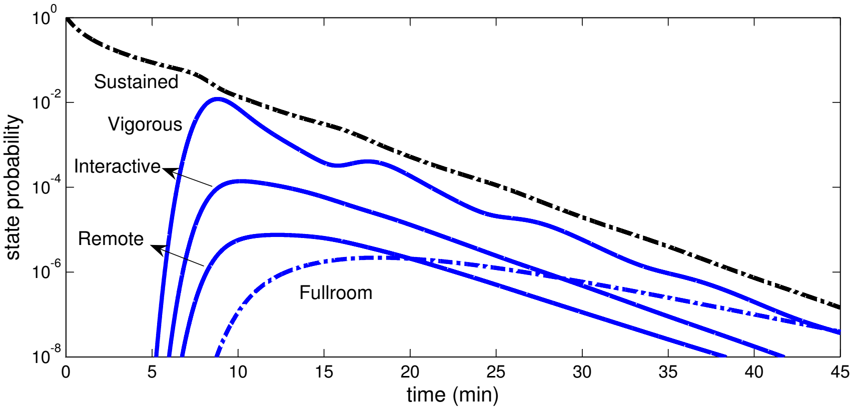


Figure 4.42: Probability of being in each state. Case 3.

Table 4.20: Time at which maximum state probabilities occur. [Case 3]

	State	Maximum probability (1)	Time (min) at which (1) occurs
3	Vigorous	0.0127652	8.8
4	Interactive	0.00013	11.8
5	Remote	0.0002	12.4

Case 3 models the situation for which all the transition times are assumed to follow log-normal distributions which are considered to provide good fits to a wide range of fire test data (Barnett, 2002, 2007). Results are plotted in Figure 4.42 with maximum probability values and times summarized in Table 4.20. For this case, the maximum probability that the fire will reach the remote stage (stage 4) is very close to that estimated for the fire reaching the interactive stage (stage 5), both slightly higher than that for the fire going to full room involvement. Results suggest an earlier time to flashover compared to Case 1, though longer than that for Case 2. Here, the time to flashover, and interestingly for this case also the time to full room involvement, is 12.4 min, comparable to that predicted by IITRI from their fire test data and about 7% higher to that estimated by Berlin.

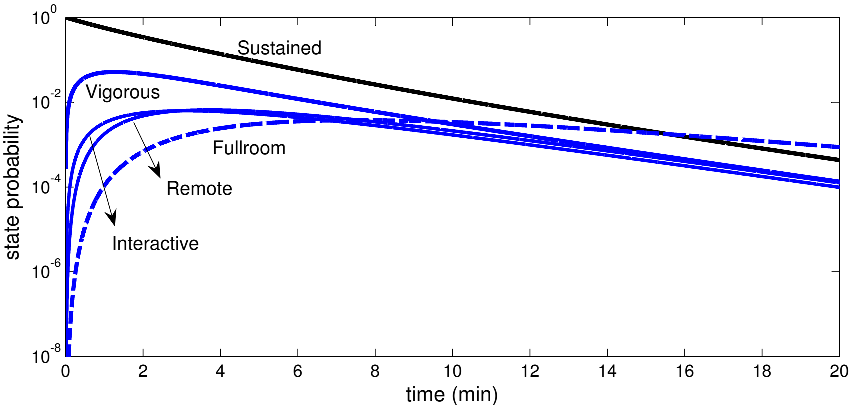


Figure 4.43: Probability of being in each state. Case 4.[Markov method]

Table 4.21: Time at which maximum state probabilities occur. [Markov method]

	State	Maximum probability (1)	Time (min) at which (1) occurs
3	Vigorous	0.0516441	1.27
4	Interactive	0.00627998	3.08
5	Remote	0.00658725	3.71

In Case 4, all of the distributions in Table 2 are assumed to be exponential, leading to a Markov process model. The resulting state probability time curves are shown in Figure 4.43 and times to maximum probability summarized in Table 8. Overall trends, compared to results from the semi-Markov model shown in Figure 5 and Table 4.18, are similar though the time scales of events is marked different, particularly with respect to the times at which maximum probabilities occur. As an example of the differences, the semi-Markov model (Case 3) predicts a time to flashover of 12.4 min, while the Markov model predicts time to flashover of only 3.71 min, i.e., about a third of the semi-Markov model time. This clearly illustrates the importance of the form of the assumed distributions for state to state transitions, since assuming exponential distributions for all the transitions in this study will potentially lead to serious under prediction of critical fire development times and consequent misinterpretation of results.

Table 4.22: Time (min) to flashover

Berlin's model Berlin (1985)	IITRI fire test Vodvarka and Waterman (1975)	Proposed model [Case 3]
11.59	12.9	12.4

Table 4.23: Time to flashover (TTF) for various configurations

Case#	TTF (min)	Comments
1	15.2	31.15% increase compared to Berlin's model (Table 4.22)
2	10.8	Variability information from Table 4.12 is unused
3	12.4	6.99% increase compared to Berlin's model (Table 4.22)
4	3.7	Variability information from Table 4.12 is unused

The time to flashover estimated by each of the cases investigated here is summarized in Table 4.23. The semi-Markov model (Case 3) estimate of 12.4 min falls between the estimate of 11.59 min contained in the original paper (Berlin, 1985) and the IITRI test data estimate of 12.9 min. Cases 2 and 4 do not utilize the variability information from the fire test data and both yield times to flashover of less than 11.59 min. Since there was no justification provided for the distributions chosen in Berlin (1985), it is not clear that their selection is in any way optimal. Similarly with changes in fuels and fuel load distributions in modern enclosures, it is unlikely that the original test data is entirely representative of more 'modern' fires. Through the refinement of methodology and exploration of the effects of varying the distributions, the model described in present paper has been shown to be flexible enough to quantify time to flashover accounting for all the variability of real fire test data, as well as cyclically receding and growing fires or other important fire events by using varying statistical distributions and parameters as the state transition descriptors.

Transition descriptors in Berlin's model relied on large scale dwelling room fire test data collected between 1959 and 1975. The test data was based on combustion of sofas made of cotton cushions which is not the only material marketed today. However, the developed model can still be utilized with appropriate choice of statistical distributions reflecting the test data. Keeping in view the flexibility needed in the model development, Table 4.13 explores four different configurations of distributions possible in applying the model.

4.5.4 Applications

As an early fire growth model, the proposed method has several potential applications. Appropriate transition state distributions, determined from existing fire test data can be acquired and applied to account for specific fire events. Variability in lining or construction materials, potential fuel loads or detector/sprinkler response can also be included through appropriate identification and specification of the transition states. The proposed model could then be used by fire safety regulators for sensitivity analysis or as a "what if" preliminary risk assessment tool to investigate considerations such as required response times or definition of requirements for the kinds of materials allowed in a particular structure.

4.5.5 Conclusions

Existing probabilistic fire behavior models were reviewed. A new model of early fire development based on a mathematically well structured approach called semi-Markov process model was proposed. The model takes into account realistic variability in the timeline for fire growth as well as the possible modes of fire extinguishment. Interpretations were drawn based on the time at which maximum state probabilities occurred with one state transition used as a predictor for time to flashover. The proposed model, with further modification, will be useful to fire safety designers, regulators and practitioners, particularly when they seek to do a sensitivity analysis or wish to incorporate variability into their predictions of overall fire growth.

4.6 Digital Controller System

A semi-Markov process model is developed for the reliability analysis of main feedwater valve (MFV) controller system that is used for regulating the water level in a steam generator. The proposed model is generalization of a Markov process model reported in the literature and allows the use of non-exponential distribution for various state transition times.

4.6.1 Problem

Digital control and protection systems are installed in nuclear power plants (NPP) or as part of upgrades to older plants with analog systems. The primary advantage of a digital system over an analog one in instrumentation and control(I&C) systems is the fault tolerance feature offered through the use of microprocessors instead of relay logic (Hassan and Vesely, 1998). Moreover, digital systems have memory, enabling them to provide diagnostic data at the component level of the control system. While logic in analog systems is driven through the use of relays and transistors, digital systems incorporate logic into software. However, software failures could potentially impact the performance of mitigating systems. Certain failure modes could arise due to software that are not encountered in analog systems (Chu et al., 2010a). This integration of hardware and software in digital I&C systems offers unique challenges in reliability modelling and hence, is an area of important research.

Literature

The technical report by Aldemir et al. (2006) explored various methods available for system reliability evaluation of digital instrumentation and control (I&C) systems. Static fault tree and event tree approaches were considered obsolete due to the inherent inability of these methods to tackle "dynamic interaction" between digital systems and rest of the plant processes. An example of such an interaction is a competition between two tasks to get hold of a digital controller's resources. Deadlock could be a situation when two threads wait for each other to release resources they are in control of. Starvation is a situation where a low priority thread might have to wait indefinitely for the controller's time slice. Hence temporal interactions could lead to dynamic situations and these can be handled well using state transition methods by branching different situations as distinct states. Despite the provisions for specialized dependency gates, the dynamic fault tree (DFT) method (Rao et al., 2009) has the shortcoming that the generated cutsets might change as the system evolves in time.

The dynamic flowgraph methodology, DFM (Al-Dabbagh and Lu, 2010) is another alternative for modelling reliability of digital I&C systems. It takes the directed graph approach with decision tables for state transitions, edges for failure dependencies and nodes for variables (*.e.g.*, Water level, Valve position). Nodes can have discrete states (*e.g.*, High, Stationary, Low). The decision table construction involves all possible mappings of variables and corresponding states (e.g., Water level high and valve open). The mapping must also account for various switching actions for backup solutions. Yau et al. (1995) demonstrated the use of DFM for a digital flight control system where 9 input variables with 5 states each led to 5^9 rows in the decision table. The paper worked around the problem by using equations of motion and control laws thus bypassing the construction and lookup of the decision table. Hence decision table construction could potentially encounter a dimensionality problem and modelling would not adhere to a universal solution though it has the ability to model multiple top events. Stochastic petri nets (Kleyner and Volovoi, 2010) is also a graph theoretic approach whose quantification can be done using simulation. These models can be converted to fault trees, but size of the model and simulation speed could severely prohibit its usage for digital I&C systems.

Another technical report by Aldemir et al. (2007) focused exclusively on reliability modelling of digital I&C systems for nuclear reactor probabilistic risk assessments. Markov models were developed for various controllers and computer systems of the DFWCS. These include the main feedwater regulating valve (MFV) controller, the bypass feedwater regulating valve (BFV) controller, the feedwater pump (FP) controller, the pressure drop indicator (PDI) controller, power source of these controllers and finally the main and its backup computers. This report was at large a proof-of-concept for the use of Markov models for digital systems. The state space for the models were elaborately developed and then reduced according to state reduction principles for practical applications. Aldemir et al. (2010) refined and quantified some of these models by generating Markov transition rates using fault injection techniques. Such techniques in software testing widen the scope of test data by introducing deliberate faults in the system.

Markov models are able to predict future failures while considering failure dependencies and can accommodate both hardware and digital interaction. However, Markov models assume only constant transition rates leading to the assumption that the time spent in any state can follow only the exponential distribution. A system involving complex interactions between hard-wired analog and software controlled digital subsystems could be subjected to human, software, electrical, mechanical and electronic failures. Lognormal, Weibull and Gamma distributions to represent time-to-event have been found to be appropriate in different contexts (Vineyard et al., 1999).

Proposed approach

A water level controller valve could be subject to high failure rates due to surge voltages during startup or shutdown and a fairly constant failure rate at any random running time. With this rationale, the present paper assumes that a Weibull distribution is suitable to model the time to a send a previous valid output to the valve. In order to achieve this ability to consider a non-exponential holding time distribution in the model, the semi-Markov process model is applied for the reliability analysis of digital feedwater regulating valve controller. The idea of applying semi-Markov process model to incorporate the effect of ageing related degradation of pipes in the nuclear industry has earlier been explored by Veeramany and Pandey (2011c).

Markov model requires continuous plant state information to generate the transition rates required as inputs. The semi-Markov process model is also subject to this inhibitive requirement. Further disadvantage is the difficult learning curve for an analyst. This hindrance can be negated to an extent by the use of simple visual interfaces.

4.6.2 The digital feedwater regulating valve controller system

Problem

The present case study is a semi-Markov extension of one of the feedwater controller Markov models from Aldemir et al. (2010). The digital feed water control system (DFWCS) shown in Figure 4.44 is responsible for regulating water level in the steam generator. A water level sensor outputs level to the computer. The computer then

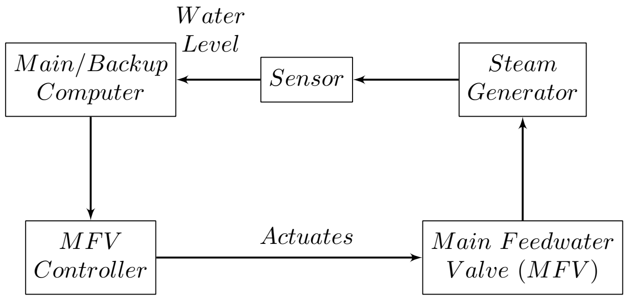


Figure 4.44: Schematic of the digital feed water control system (DFWCS).

determines the amount by which the valves need to be repositioned so as to adjust the water flow speed. This information is sent in the form of a signal to the controller. Accordingly, the controller actuates the main feedwater regulating valve (MFV) to optimize the water flow. Apart from MFV, there are other controllers and actuating devices as part of the DFWCS. The focus of this case study is to analyze the reliability of the MFV controller system based on its output to the valve. There is a finite probability of the valve getting stuck in its maximum or minimum flow position due to an erroneous output from the controller. It is also possible that the controller sends an arbitrary or random output to the valve. These could be due to a processing error or an internal problem in the computer. In these abnormal cases the controller feeds a valid previous output to the valve. This situation is termed as the failure of the controller system.

Markov analysis

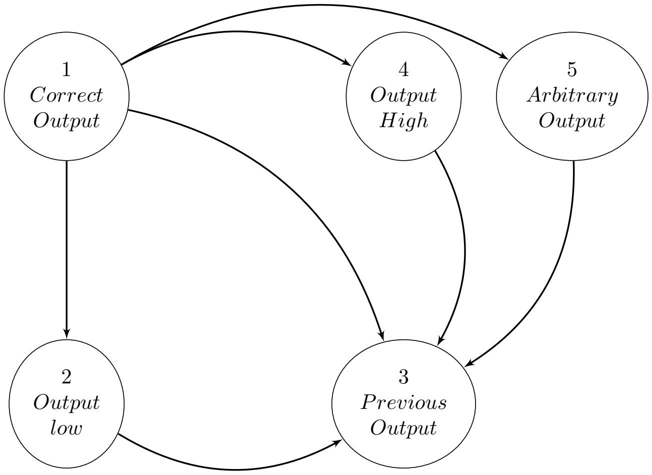


Figure 4.45: State space for Main Feedwater regulating Valve (MFV)(Aldemir et al., 2010).

The model proposed by Aldemir et al. (2010) based on Aldemir et al. (2007) has five states as shown in Figure 4.45. The system initially begins operation in state 1. In this state, the controller receives correct output from the computer and sends it to the valve. The system moves to state 2,4 or 5 when the output is too low, high or arbitrary respectively. It is assumed that these states do not lead back to the correct output, instead move on to state 3 where a valid previous output is sent to the valve. For modelling purposes, state 3 is an absorbing state representing system failure. As per this model, there is a transition from state 1 to state 3 in which case an internal problem with the computer is recognized by the controller and a previous output is sent to the valve. The literature also suggests that there are circumstances when the controller fails to sense the failure of the computer and hence sends arbitrary output to the valve.

Table 4.24: Sample Markov transition rates for the controller system. (Aldemir et al., 2010)

State Transition				Transition Rate (hr^{-1})
λ_{12}	Correct Output	→	Output Low	2.55 x 10^{-7}
λ_{13}	Correct Output	→	Previous Output	4.2 x 10^{-5}
λ_{14}	Correct Output	→	Output High	5.5 x 10^{-8}
λ_{15}	Correct Output	→	Arbitrary Output	5.5 x 10^{-8}
λ_{23}	Output Low	→	Previous Output	4.2 x 10^{-5}
λ_{43}	Output High	→	Previous Output	4.2 x 10^{-5}
λ_{53}	Arbitrary Output	→	Previous Output	4.2 x 10^{-5}

Due to lack of practical data, Aldemir et al. (2010) estimated failure rates based on fault injection experiments. These rates listed in Table 4.24 are useful for demonstrative purposes.

The system of differential equations to solve the Markov model is based on the fact that the rate of change of the probability of being in any state S is negatively proportional to the rate at which the transitions occur outward from S and positively proportional to the rate at which inward transitions occur from other states (Lisnianski and Levitin, 2003).

For example, from Figure 4.45, it is seen that there are four inward transitions in to state 3 originating from states 1,2,4 and 5 while there is only one transition going out from states 2,4 and 5.

$$dp_1(t)/dt = -(\lambda_{12} + \lambda_{13} + \lambda_{14} + \lambda_{15})p_1(t)$$

$$dp_2(t)/dt = \lambda_{12}p_1(t) - \lambda_{23}p_2(t)$$

$$dp_3(t)/dt = \lambda_{13}p_1(t) + \lambda_{23}p_2(t) + \lambda_{43}p_4(t) + \lambda_{53}p_5(t)$$

$$dp_4(t)/dt = \lambda_{14}p_1(t) - \lambda_{43}p_4(t)$$

$$dp_5(t)/dt = \lambda_{15}p_1(t) - \lambda_{53}p_5(t)$$

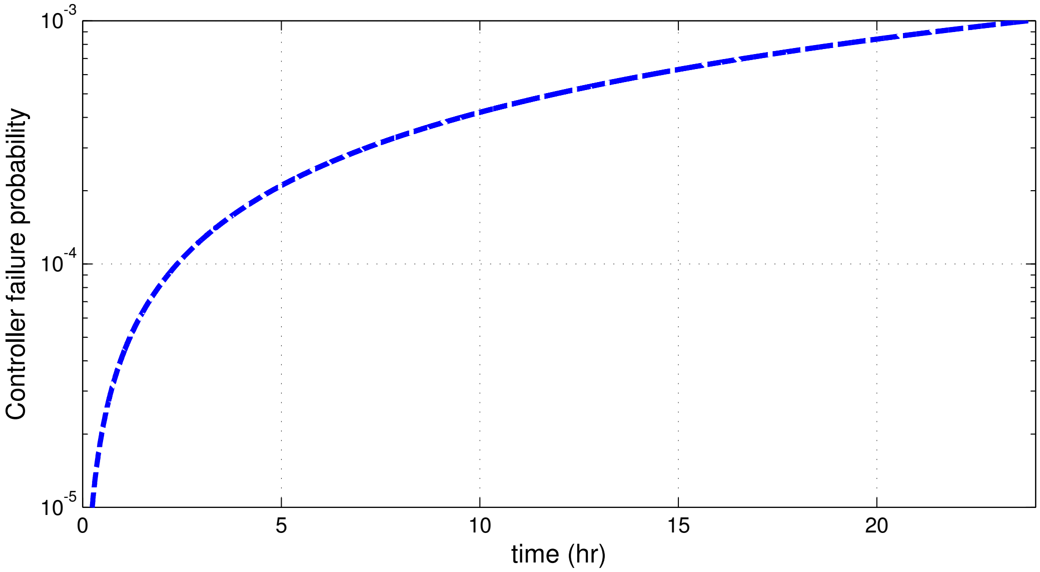


Figure 4.46: Controller failure probability.

Results

Figure 4.46 plots the probability of being in state 3, which is the probability of controller system failure. Note that the system could land in state 3 either directly from state 1 or through the other states. Out of a year, the operational mission time of the DFWCS is assumed to be 11 months allowing for one month of outage time (Aldemir et al., 2007). For PRA purposes, the usual (default) reference time period is 24h (Aldemir et al., 2010). Hence, in this paper, duration for all the plots is 24 hours.

Figure 4.47 plots the probability of being in states 2, 4 and 5. The state probability of a high or an arbitrary output is the same owing to the same failure rate shared by the respective transitions from the state of correct output. The failure rate of a low output from correct output is lower than that of a high or an arbitrary output. Correspondingly, the state probabilities reflect the trend. However, comparing Figure 4.46 and 4.47 the probability of a controller failure is higher than

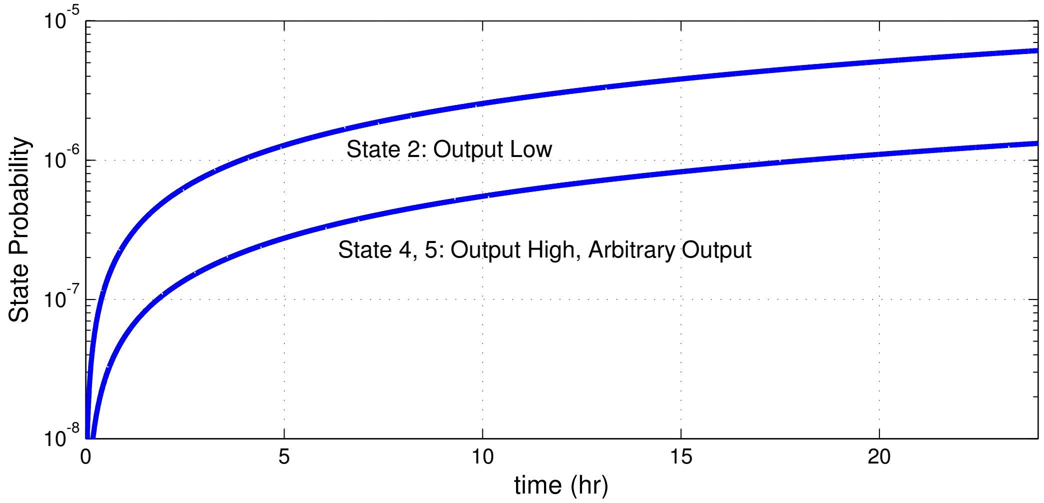


Figure 4.47: Probability of being in states 2,4 and 5.

being in any of the other states. This can be attributed to the fact that state of previous output is an absorbing state and hence all transitions eventually end in this state.

A direct transition from correct to previous output has higher influence over the controller failure probability than that due to transiting through intermediate steps and reaching the previous output. This is due to relatively larger failure rate for the transition from correct to previous output when compared to the combined failure rates of the alternate paths.

4.6.3 Mission Reliability

For the feedwater valve controller system, $\phi_{13}(t)$ denotes the failure probability and $R(t) = 1 - \phi_{13}(t)$. Let the time to failure T of the system be a random variable. Assume that the system is reliable until the time t_b *i.e.*, $T > t_b$. The probability that the system is able to further complete a mission duration of t_m successfully is conditioned on the time already spent in reliable service and is called the mission reliability (Kumar, 2000):

$$MR(t_b, t_m) = \frac{R(t_b + t_m)}{R(t_b)} = \frac{1 - \phi_{13}(t_b + t_m)}{1 - \phi_{13}(t_b)}$$

$MR(t_b, t_m)$ represents the probability that the system stays in one of the states other than the failure state (state 3) given that it has not yet stepped in to state 3 until t_b. Note that if distribution of T is exponential then the mission reliability is independent of t_b, $MR(t_b,t_m) = R(t_m)$. For plotting, the mission unreliability, $1 - MR(t_b,t_m)$, is a convenient choice:

$$1 - MR(t_b,t_m) = \frac{\phi_{13}(t_b + t_m) - \phi_{13}(t_b)}{1 - \phi_{13}(t_b)}$$

This quantity represents the probability that the system enters state 3 during the time interval $(t_b, t_b + t_m)$ given that it has been reliable until time t_b.

4.6.4 Semi-Markov model for digital feedwater valve controller

The holding time in any state is a random variable. Though hard to determine and establish the variability, this information can be of potential use to study its effect on the controller system's failure probability. In this paper, it is assumed that the time-to-previous output from the state of correct output follows a Weibull distribution. The coefficient of variation (cov) is varied between 0.4 and 1.0. The rest of the transition times are assumed to follow exponential distributions with the mean transition rates as listed in Table 4.24. Let $R_{ij}(t) = 1 - F_{ij}(t)$. Then, the kernel $C(t)$ of the semi-Markov process for the controller system can be written using Equation 3.5,

$$\begin{bmatrix} 0 & f_{12}(t)\prod\limits_{i=3,4,5} R_{1i}(t) & f_{13}(t)\prod\limits_{i=2,4,5} R_{1i}(t) & f_{14}(t)\prod\limits_{i=2,3,5} R_{1i}(t) & f_{15}(t)\prod\limits_{i=2,3,4} R_{1i}(t) \\ 0 & 0 & f_{23}(t) & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & f_{43}(t) & 0 & 0 \\ 0 & 0 & f_{53}(t) & 0 & 0 \end{bmatrix}$$

The kernel matrix and the matrix $W(t)$ are sufficient to solve for state probabilities. The probability of being in each of the states is computed by solving the system of integral equations in Equation 3.10 using the trapezoidal rule (Veeramany and Pandey, 2011c,b).

The transition rates for the Markov model (Aldemir et al., 2010) were a result of reducing the total number of states to five from a seven state model. These effective rates are used in the proposed model as a first hand approximation. Alternatively, state reduction techniques can be applied on a semi-Markov process model to determine the effective distribution parameters as explored by Veeramany and Pandey (2011b).

Results of semi-Markov process model

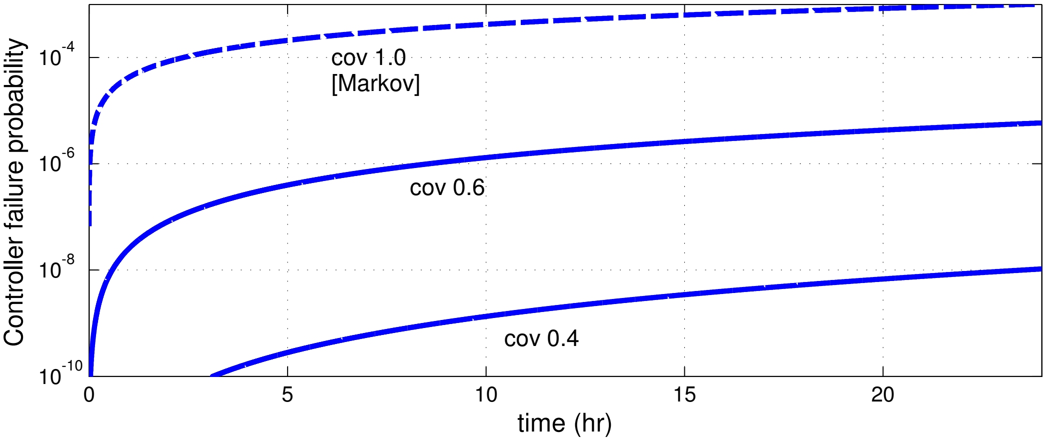


Figure 4.48: Controller system failure probability comparing variability in time to previous-output.

Figure 4.48 shows the controller failure probability for three cases of coefficient of variation: 1.0, 0.6 and 0.4. Recall that this variability corresponds to time to the previous output from the state of correct output. Comparing the Figures 4.46 and 4.48, it can be seen that a cov of 1.0 corresponds to the Markov case. On the other hand, the lower the variability, the lower is the failure probability.

Table 4.25: Controller failure probability at the end of 24 hrs.

cov	Controller failure probability
1.0	1.0075 x 10^{-3}
0.6	5.88034 x 10^{-6}
0.4	1.05061 x 10^{-8}

The controller failure probabilities at the end of 24h are shown in Table 4.25 for each of the covs considered. It is seen that the failure probability increases with an increase in cov and it is the highest for the Markov model.

Consider two MFV controller systems - the first system has been in service for 10 hours and the second system is newly installed after first system has been

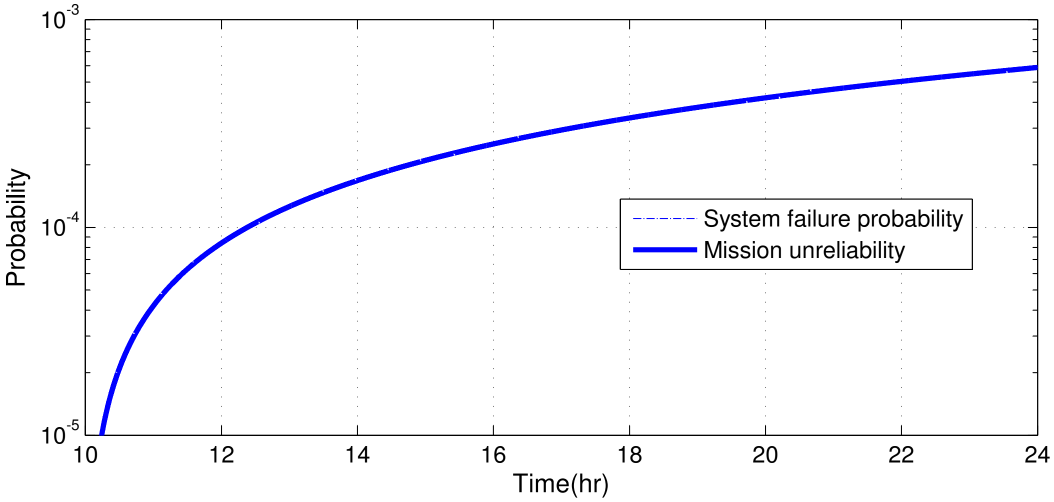


Figure 4.49: Controller system mission unreliability for additional 14 hrs given that the system was reliable for the initial 10 hrs [*cov*=1].

operational for 10 hours. The mission unreliability of the first system given a 10h reliable operating history and the failure probability of the second system are compared in Figure 4.49. The comparison assumes $cov = 1$ for the time to transition from state 1 to state 3. It is observed that both probabilities are the same for the observed 14 hour period. This well known result shows that the Markov model does not differentiate a system already in service and a newly installed one.

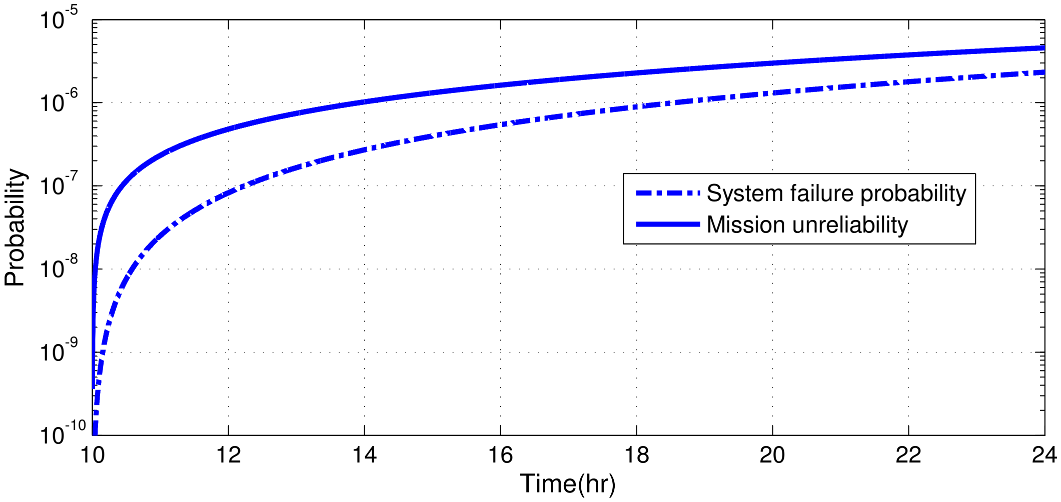


Figure 4.50: Controller system mission unreliability for additional 14 hrs given that the system was reliable for the initial 10 hrs [*cov*=0.6].

Assuming $cov = 0.6$ for the time to transition from state 1 to state 3, Figure 4.50 shows that mission unreliability of the first system is higher than the system failure probability of the newly installed system. This is a result of considering non-exponential distribution in the semi-Markov model formulation.

Since a digital I&C system is a combination of hardware and software systems, it is prone to ageing. Nuclear power plant systems undergo certain maintenance activities that could be carried out even without outages. Under these circumstances, continuous execution of software embedded in hardware (firmware) could exhibit software ageing due to performance degradation, numerical error accumulation and unexpected crashes (Laird and Brennan, 2006). Moreover, mechanical movement of the feedwater valve in response to controller commands could go out of control. In an intuitive sense, the failure probability of an ageing system at the present moment is very low given that the system was reliable until now. Overtime, failure probability of such a system is likely to be higher than that of a newly installed system due to increased risks of wear and tear. However both these quantities remain the same if the failure time of a system is assumed to follow an exponential distribution. This inability to take ageing in to account is a result of the memoryless property of the exponential distribution. A recommendation for future research is to analyze reliability of an ageing digital I&C system over the life span of a typical power plant and not just for a short period of 24h.

Apart from the main feedwater regulating valve (MFV) controller, the digital feedwater controller system (DFWCS) is connected to a feedwater pump (FP) and its controller, a bypass feedwater valve (BFV) and its controller, a main computer and its backup and a pressure drop indicator (PDI) controller. A critical application in the nuclear plant reliability analysis is the probabilistic assessment of the entire digital controller system. NUREG-CR/6942 proposed Markov models for each of MFV, computer and the PDI systems. The MFV, BFV and the FP share the same model used in this paper. Hence, a larger application of semi-Markov process model would be to integrate the reliability models of the above said systems in to a single model for the digital feedwater controller system.

4.6.5 Conclusion

The main feedwater valve controller system used to regulate water level in a nuclear power plant steam generator is a critical digital instrumentation and control system of interest. A Markov model was developed in NUREG-CR/6942. This case study presents a more general semi-Markov model so that non-exponential distributions can be included in the model. An example is presented to analyze this problem in which Weibull distribution is assumed for a state transition time in the model.

4.7 Quantifying Maintenance Effects on Unavailability

This case study presents a general model for evaluating unavailability of engineering systems with maintenance effects based on the theory of semi-Markov process. The proposed model is able to incorporate non-exponential distributions to consider degradation of systems. The effect of degradation intensity, variability in degradation and maintenance interval on the component's unavailability are investigated. The model is able to recommend an optimal maintenance interval for minimizing the operational unavailability.

4.7.1 Problem

Samanta et al. (1991)'s NUREG report was an early attempt to show that degradation can be modeled using state space techniques to identify ageing trends and thus formed the basis for Vesely (1993)'s Markov model. The basic idea was to borrow minimal inputs from standard two-state probabilistic risk assessment (PRA) models and build a Markov model capable of identifying optimal maintenance intervals. However, the Markov process model assumes constant rate of occurrence of degradation implying that the time-to-degradation initiation is a random variable following an exponential distribution. However, if degradation accelerates rapidly due to ageing, Weibull or gamma distribution can be a better choice. For example, Bae et al. (2007) derive insights from comprehensive degradation analyses done by Lu and Meeker (1993); Meeker and Escobar (1998). They explain that the choice of distribution in metal corrosion and degradation of electronic devices such as semiconductors has profound implications on the resulting lifetime model. The paper investigated the characteristics of lifetime distributions when Weibull, Gamma and log-logistical distributions are used in degradation analysis. Vineyard et al. (1999) identified that the Weibull distribution was found to be a strong fit for the time between failures for electronic, human, mechanical, and software failures. Similarly lognormal distribution was found to be a strong fit for the time between failures for electrical failures. Hence, keeping in view the importance of non-exponential distributions in degradation modelling, the objective of this case study is to extend Vesely (1993)'s Markov model in to a more general semi-Markov process (SMP) model that permits the use of non-exponential distributions for time spent in the component states in order to quantify the maintenance effects on unavailability.

Consequences and maintenance management of ageing components have been investigated through renewal theory (Radulovich et al., 1995), physics of ageing damage in passive components(Smith et al., 2001) and linear and Weibull ageing models (Kancev and Čepin, 2011; Vesely, 1978). Veeramany and Pandey (2011c) developed a semi-Markov model to evaluate reliability of a degrading nuclear piping system to support risk-informed in-service inspection programs. The model assumed that the time to flaw growth in a pipe follows non-exponential distribution. The paper extended a Markov model proposed by Fleming (2004) which argues that apart from catastrophic failures like severe loading, there can be a number of piping related degradation issues like flow accelerated erosion-corrosion, thermal fatigue, wall thinning, crack propagation, flaws and leaks. The present case study proposes a more general model that quantifies the effect of maintenance on unavailability of degrading systems. Veeramany and Pandey (2011b) focused on modelling reliability of redundant systems where one or more constituent components could follow non-exponential distribution for time to failure. Ideas for reducing the number of states in the model for specific cases were proposed. Gupta and Dharmaraja (2011) proposed a ten state semi-Markov dependability model yielding time-dependent results. The paper explained the necessity to introduce non-exponential distributions for resource degradation and presented an application that assumed exponential distribution for all sojourn times. Simulation was used to determine probability of a security attack in a telecommunications network. Semi-Markov process model has also been explored (Veeramany and Pandey, 2011a) to model reliability of digital instrumentation and control (I&C) systems where there is a scope for firmware to undergo performance degradation due to software ageing in combination with risks of mechanical wear and tear. Tomasevicz and Asgarpoor (2009) developed a semi-Markov decision process based on an n-state degradation model to solve for optimal maintenance policy of repairable equipment without the use of continuous time statistical distributions.

4.7.2 State Space Model

The original Markov model by Vesely (1993) seen in Figure 4.51 consists of four states - operational, degraded, maintenance and failure. The only input available from a standard probabilistic risk assessment (PRA) is the component's failure rate λ. Vesely derived analytical expressions to connect λ to each of the transition rates in the Markov model by introducing a few intermediary quantities. The proposed

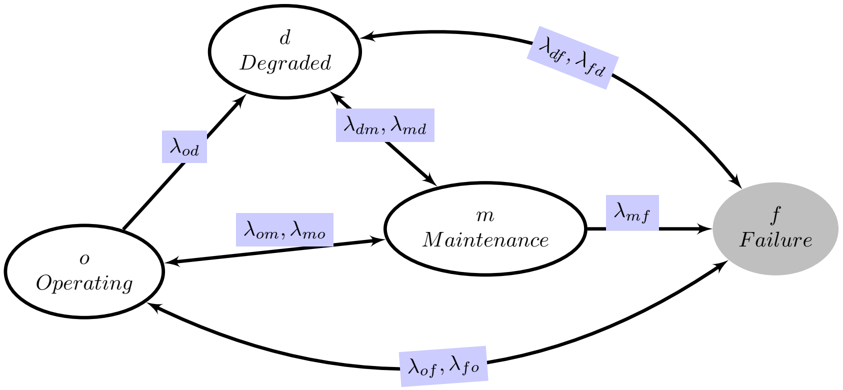

d
Degraded
$\lambda_{df}, \lambda_{fd}$
$\lambda_{dm}, \lambda_{md}$
λ_{od}
m
Maintenance
λ_{mf}
f
Failure
$\lambda_{om}, \lambda_{mo}$
o
Operating
$\lambda_{of}, \lambda_{fo}$

Figure 4.51: Four-state transition model for system degradation (Vesely, 1993).

model additionally introduces coefficient of variation, γ in the time to failure. As a result there is a scope for the time spent in the states o and d towards the transitions $o \rightarrow d$, $o \rightarrow f$ and $d \rightarrow f$ to follow non-exponential distribution. An application is presented assuming that only the time to degradation corresponding to the transition $o \rightarrow d$ follows non-exponential distribution.

The component failure rate λ accounts for both catastrophic failures and also the failures that pass through degradation. However, these are not directly observable. λ is related to the catastrophic failure rate λ_{of} through the catastrophic failure fraction f_{of} (Vesely, 1993):

$$\lambda_{of} = f_{of}\lambda$$

If a non-exponential distribution is to be used for transitions $o \rightarrow d$ and $o \rightarrow f$, it is desirable to have the mean time to failure and the cov of the time to event data so that distribution specific parameters can be fitted for each of the transitions.

Equation 4.7.2 can be alternatively written in terms of the mean time to failures:

$$\mu_{of} = \frac{1}{f_{of}}\mu$$

Let the coefficient of variation (cov) of data that yield μ and μ_{of} be γ and γ_{of} respectively. If the time spent in the operational state is assumed to follow an exponential distribution then, $\gamma_{of} = \gamma = 1$. If not, $\gamma_{of} = \gamma$ assuming that scaling the mean corresponds to a dataset in which each of the data points is scaled accordingly.

Hence, by knowing λ, γ and with an estimate of f_{of}, one could arrive at the mean μ_{of} and cov γ_{of} of catastrophic time to failure corresponding to the transition $o \rightarrow f$. These two quantities are sufficient to set up a desired non-exponential distribution to time to catastrophic failure given that the system is operational. Let the probability density function (*pdf*) and the cumulative distribution function (*cdf*) corresponding to this set of mean and cov be denoted by $g_{of}(t)$ and $G_{of}(t)$ respectively.

On similar lines, it can be argued that the component failure rate λ and the component degradation rate λ_{od} can be related (Vesely, 1993) through degradation ratio r_{od}:

$$\mu_{od} = \frac{1}{r_{od}}\mu$$
$$\gamma_{od} = \gamma$$

The above two quantities are sufficient to set up a desired non-exponential distribution to time to degradation given that the system is operational. Let the *pdf* and the *cdf* corresponding to this set of mean and cov be denoted by $g_{od}(t)$ and $G_{od}(t)$ respectively.

In view of restricting to as less additional variables as possible, the degraded failure rate λ_{df} is related to the total failure rate λ through the ratios r_{od} and f_{of} and the definition that $T_{odf} = T_{od} + T_{df}$ (Vesely, 1993):

$$r_{df} = \frac{r_{od}(1 - f_{of})}{r_{od} - (1 - f_{of})}$$
$$\lambda_{df} = r_{df}\lambda$$

or

$$\mu_{df} = \frac{1}{r_{df}}\mu$$
$$\gamma_{df} = \gamma$$

The above two quantities are sufficient to set up a desired non-exponential distribution to time to failure given that the system is degraded. Let the *pdf* and the *cdf* corresponding to this set of mean and cov be denoted by $g_{df}(t)$ and $G_{df}(t)$ respectively.

The maintenance frequencies λ_{om} and λ_{dm} when in operational and degraded states respectively can be assumed to be constant transition rates owing to the fact that there is less variability in time to maintenance once a maintenance policy is selected. These rates were derived on the assumption that the degradation rate is constant (Vesely, 1993) and continue to be the closest approximate for the proposed semi-Markov model:

$$\lambda_{om} = \frac{exp(-(1-f_{of})\lambda T_m)}{T_m}$$
$$\lambda_{dm} = \frac{exp(-\lambda_{df}\frac{T_m}{2})}{T_m/2}$$

where T_m is the average time between maintenances.

The transition $m \rightarrow f$ representing a component failure while under maintenance and backward transitions $m \rightarrow o$, $m \rightarrow d$, $f \rightarrow o$ and $f \rightarrow d$ representing component state improvements are assumed to follow constant transition rates keeping in view the scarcity of data to fit non-exponential distributions. These transition rates (Vesely, 1993) are listed in Table 4.26.

Table 4.26: Constant transition rates for rest of the transitions (Vesely, 1993)

Transition	Transition rate	Constraints
$m \rightarrow o$	$\lambda_{mo} = p_{mo}/d_m$	$p_{mo} + p_{md} + p_{mf} = 1$
$m \rightarrow d$	$\lambda_{md} = p_{md}/d_m$	d_m: average maintenance duration
$m \rightarrow f$	$\lambda_{mf} = p_{mf}/d_m$	
$f \rightarrow o$	$\lambda_{fo} = p_{fo}/d_f$	$p_{fo} + p_{fd} = 1$
$f \rightarrow d$	$\lambda_{fd} = p_{fd}/d_f$	$d_f = \frac{T}{2}(1 - \frac{1}{3}\frac{T}{T_m}) + r$
		r = average repair time
		T=surveillance test interval

For the Markov model presented in Figure 4.51, the transition rate matrix is given by:

$$\begin{bmatrix} 0 & \lambda_{od} & \lambda_{om} & \lambda_{of} \\ 0 & 0 & \lambda_{dm} & \lambda_{df} \\ \lambda_{mo} & \lambda_{md} & 0 & \lambda_{mf} \\ \lambda_{fo} & \lambda_{fd} & 0 & 0 \end{bmatrix}$$

and the time evolution of states yielding the state probabilities is given by a system of differential equations. In the next section, the semi-Markov process model is described to arrive at a system of integral equations taking in to account the ability to incorporate non-exponential distributions.

4.7.3 Application of SMP to the maintenance model

The proposed model is applied to a hypothetical component assuming that the time to degradation follows Weibull distribution. The mean time to degradation μ_{od} and cov of time to degradation γ_{od} are used to back-calculate the scale λ'_{od} and shape γ'_{od} parameters of Weibull distribution.

The kernel of the semi-Markov process model can be constructed with all the known transition information gathered from Equation 4.7.2 through Table 4.26:

$$C(t) = \begin{array}{c c} & \begin{array}{cccc} o & d & m & f \end{array} \\ \begin{array}{c} o \\ d \\ m \\ f \end{array} & \begin{pmatrix} 0 & c_{od}(t) & c_{om}(t) & c_{of}(t) \\ 0 & 0 & c_{dm}(t) & c_{df}(t) \\ c_{mo}(t) & c_{md}(t) & 0 & c_{mf}(t) \\ c_{fo}(t) & c_{fd}(t) & 0 & 0 \end{pmatrix} \end{array}$$

where

$$\begin{aligned} c_{od}(t) &= g_{od}(t)(1 - G_{om}(t))(1 - G_{of}(t)) \\ c_{om}(t) &= g_{om}(t)(1 - G_{od}(t))(1 - G_{of}(t)) \\ c_{of}(t) &= g_{of}(t)(1 - G_{od}(t))(1 - G_{om}(t)) \\ c_{dm}(t) &= g_{dm}(t)(1 - G_{df}(t)) \\ c_{df}(t) &= g_{df}(t)(1 - G_{dm}(t)) \\ c_{mo}(t) &= g_{mo}(t)(1 - G_{md}(t))(1 - G_{mf}(t)) \\ c_{md}(t) &= g_{md}(t)(1 - G_{mo}(t))(1 - G_{mf}(t)) \\ c_{mf}(t) &= g_{mf}(t)(1 - G_{md}(t))(1 - G_{mo}(t)) \\ c_{fo}(t) &= g_{fo}(t)(1 - G_{fd}(t)) \\ c_{fd}(t) &= g_{fd}(t)(1 - G_{fo}(t)) \end{aligned}$$

$$\phi(t) = \begin{bmatrix} 0 & \phi_{od}(t) & \phi_{om}(t) & \phi_{of}(t) \\ 0 & 0 & \phi_{dm}(t) & \phi_{df}(t) \\ \phi_{mo}(t) & \phi_{md}(t) & 0 & \phi_{mf}(t) \\ \phi_{fo}(t) & \phi_{fd}(t) & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} e^{-((\lambda'_{od}t)^{\gamma'_{od}}+(\lambda_{om}+\lambda_{of})t)} & 0 & 0 & 0 \\ 0 & e^{-(\lambda_{dm}+\lambda_{df})t} & 0 & 0 \\ 0 & 0 & e^{-(\lambda_{mo}+\lambda_{md}+\lambda_{mf})t} & 0 \\ 0 & 0 & 0 & e^{-(\lambda_{fo}+\lambda_{fd})t} \end{bmatrix} +$$

$$\int_0^T C(\tau)\phi(t-\tau)d\tau$$

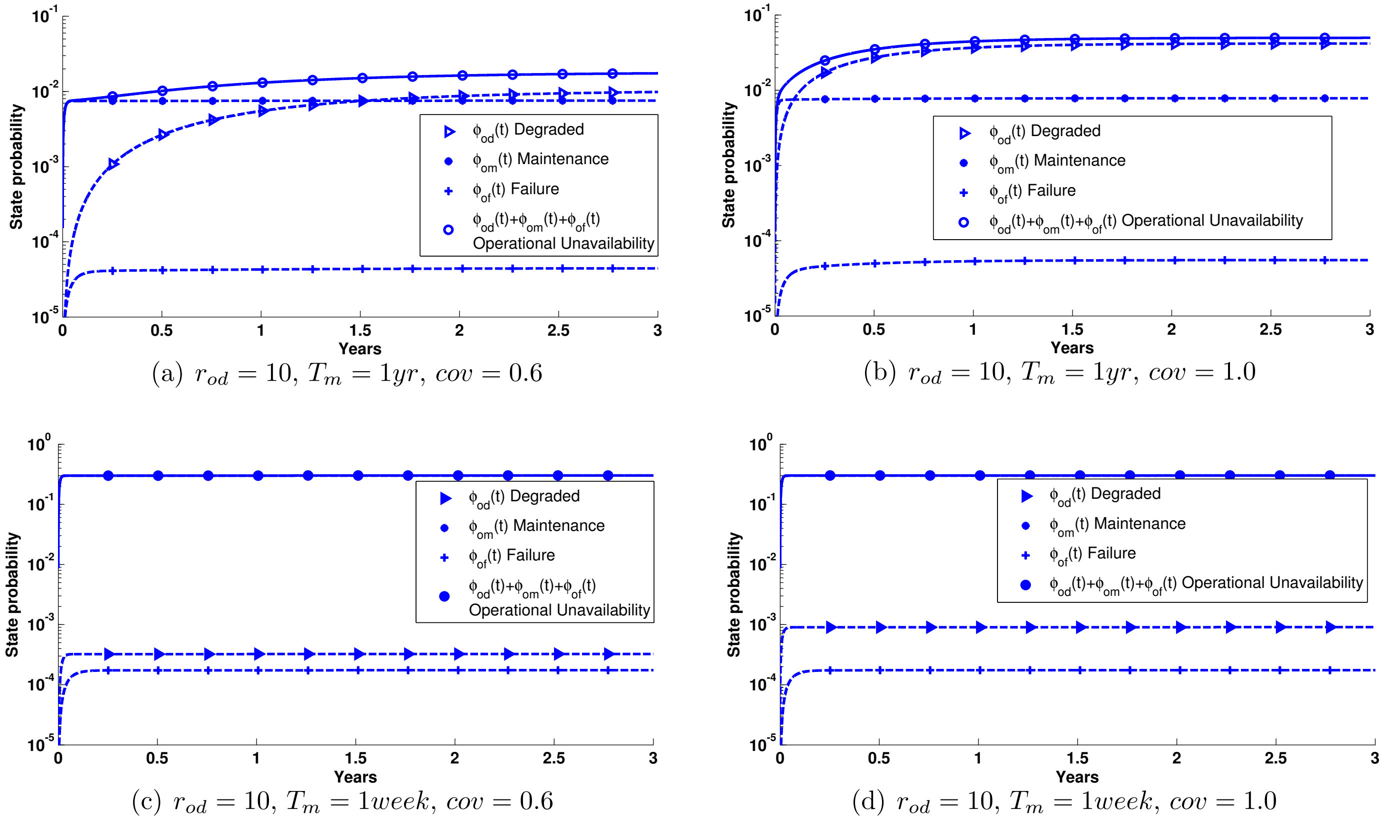
If it is assumed that the component begins in the operating state, the cumulative probability of being in the degraded, maintenance and failure states is given by $\phi_{od}(t), \phi_{om}(t)$ and $\phi_{of}(t)$ respectively. The sum $\phi_{od}(t) + \phi_{om}(t) + \phi_{of}(t)$ yields operational unavailability of the component. The goal then is to determine an optimal maintenance interval that corresponds to minimum operational unavailability.

Table 4.27: Sample input data

Quantity	Value	
λ	1 x $10^{-6}h^{-1}$	Component failure rate
γ	1.0, 0.6, 0.4	variability in time to degradation
f_{of}	0.1	catastrophic failure fraction
r_{od}	3.0, 10.0	degradation ratio
p_{mo}	0.9990	fraction of maintenances resulting in state o
p_{md}	0.0009	fraction of maintenances resulting in state d
p_{mf}	0.0001	fraction of maintenances resulting in state f
p_{fd}	0.01	fraction of failures resulting in state d
p_{fo}	0.09	fraction of failures resulting in state o
r	20h	average repair time
T	730h	surveillance test interval
T_m	various	1 week, 2 weeks, 1 month, 3 months, 6 months, 1 year, 2.5 years, 5 years, 8.33 years

Table 4.27 lists the set of sample inputs used for the present illustrative application. Of these λ, f_{of} and r_{od} have been borrowed from Vesely (1993). γ is specific to the proposed model and rest of the inputs missing from Vesely (1993) have been assumed here based on a hypothetical degrading component.

Results



(a) $r_{od} = 10$, $T_m = 1yr$, $cov = 0.6$

(b) $r_{od} = 10$, $T_m = 1yr$, $cov = 1.0$

(c) $r_{od} = 10$, $T_m = 1week$, $cov = 0.6$

(d) $r_{od} = 10$, $T_m = 1week$, $cov = 1.0$

Figure 4.52: Effect of variability in time to degradation and maintenance interval on state probabilities

Table 4.28: Effect of variability in degradation - steady state probabilities, $r_{od} = 10$

T_m / State	1 week			1 year		
	cov=0.6	1.0	Increase	cov=0.6	1.0	Increase
Degraded	0.0003	0.0009	200%	0.0104	0.0421	304.8%
Maintenance	0.3035	0.3037	0.07%	0.0076	0.0078	2.6%
Operationally Unavailable	0.3040	0.3048	0.26%	0.0180	0.0500	177.8%

Figure 4.52 and Table 4.28 show how variability in degradation affects steady state probabilities. In each of the plots, r_{od} is assumed to be 10. Assuming a constant degradation rate over-estimates the degradation probability by more than 200% when the actual variability in degradation is only 0.6. This proves that exponential distribution for time to degradation is an overly conservative assumption. The conservativeness is significantly reflected in increase in the operational unavailability (177.8%) as the maintenance interval increases. This is because longer maintenance interval adds more to degradation propagation apart from uncertainty in time to degradation.

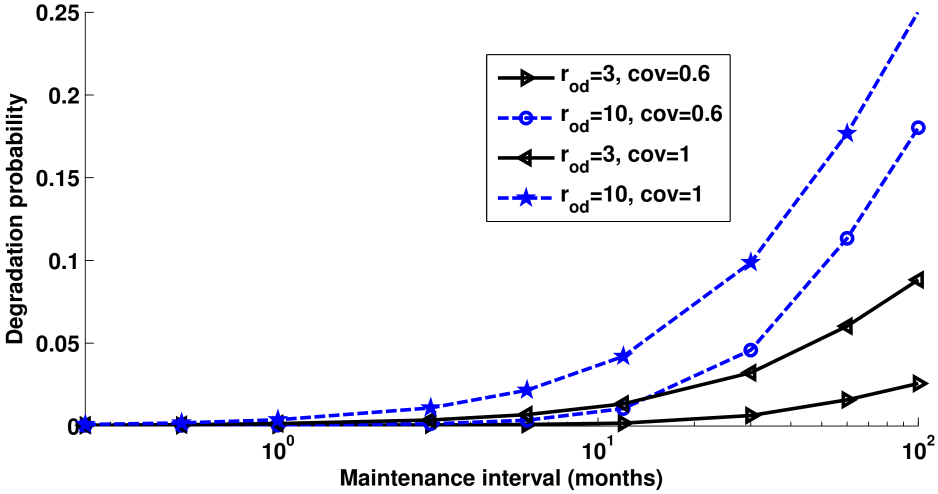
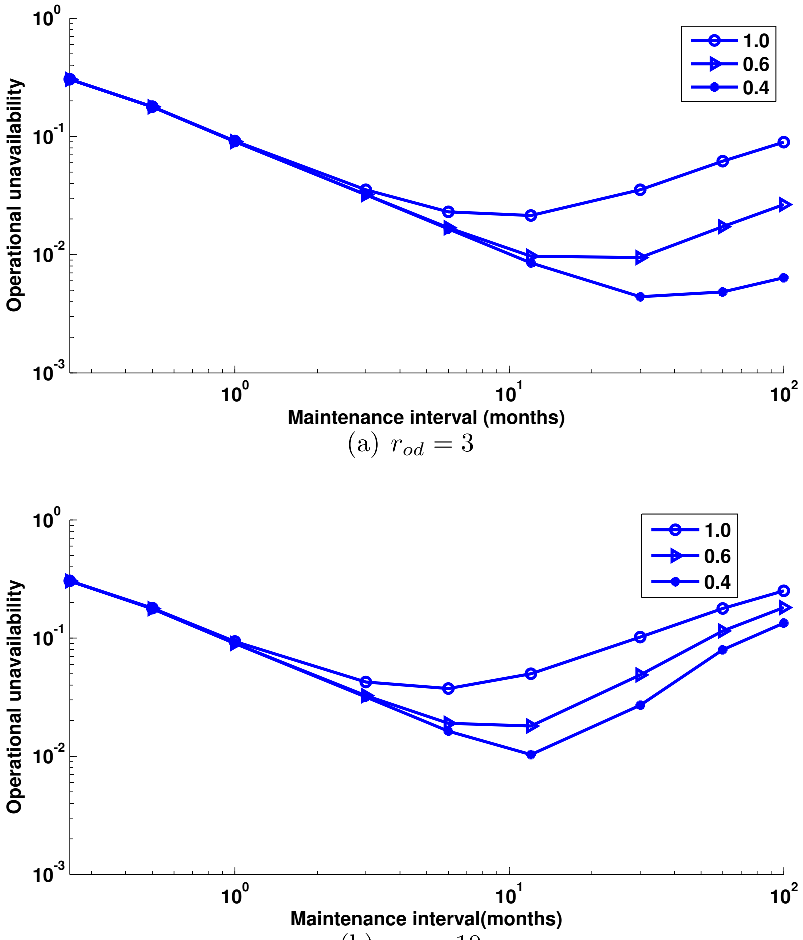


Figure 4.53: Effect of variability in time to degradation and degradation ratio on degradation probability

Figure 4.53 shows that lower degradation probability is associated with lower degradation ratio *i.e.*, if the component failures are driven more by degradation rather than catastrophic failures, it follows that probability of being in the degradation state is higher. Given a degradation ratio and maintenance interval, the degradation probability is proportional to the variability in degradation. However, significant differences in degradation probabilities are not evident for smaller maintenance intervals. If the component undergoes maintenance once in 8.33 years, the degradation probability is the highest (0.2503) when $r_{od} = 10$,cov=1 and lowest(0.0256) when $r_{od} = 3$,cov=0.6.



(a) $r_{od} = 3$

(b) $r_{od} = 10$

Figure 4.54: Operational unavailability $\phi_{od}(t)+\phi_{om}(t)+\phi_{of}(t)$ for degradation ratio $r_{od} = 3, 10$

An important application of the proposed model is to suggest an optimal maintenance interval based on the component's failure rate extracted from a standard PRA model. Such an optimal interval depends additionally on variability in degradation for better accuracy. In Figure 4.54 maintenance interval was varied between one week to 8.33 years and operational unavailability was plotted for degradation ratio of 3.0 and 10.0 separately. It is observed that operational unavailability decreases with decreasing variability in degradation though significant only beyond a two month maintenance interval for $r_{od} = 3.0$ and one month interval for $r_{od} = 10.0$. In all the plots, there is a point at which operational unavailability stops decreas-

Table 4.29: Operational unavailability

Maintenance	$r_{od} = 3$			$r_{od} = 10$		
Interval T_m	cov = 1	0.6	0.4	cov = 1	0.6	0.4
1 week	0.3045	0.3042	0.3042	0.3048	0.3040	0.3040
2 weeks	0.1784	0.1780	0.1780	0.1792	0.1776	0.1776
1 month	0.0915	0.0904	0.0904	0.0936	0.0901	0.0900
3 months	0.0354	0.0323	0.0322	0.0425	0.0326	0.0317
6 months	0.0230	0.0168	0.0165	**0.0374**	0.0190	0.0163
1 year	**0.0214**	0.0097	0.0085	0.0500	**0.0180**	**0.0103**
2.5 years	0.0353	**0.0094**	**0.0044**	0.1018	0.0487	0.0270
5 years	0.0618	0.0173	0.0048	0.1783	0.1148	0.0797
8.33 years	0.0893	0.0265	0.0064	0.2513	0.1811	0.1341

ing and then reverses the trend with increasing maintenance interval. Thus, irrespective of the variability in degradation, too frequent and delayed maintenance schemes increase unavailability due to longer stay in the maintenance state with reduced performance or total unavailability.

The observed point of inflection is a suggested optimal maintenance interval that minimizes unavailability. Table 4.29 shows that for an $r_{od} = 3.0$, it is sufficient to perform maintenance once in 2.5 years when the cov=0.6 as compared to a more frequent 1 year maintenance when the cov=1.0. When cov=0.6, $r_{od} = 10.0$ would require a maintenance interval of 6 months as opposed to an yearly maintenance for $r_{od} = 3.0$. A Markov model would recommend frequent maintenance which could have significant financial implications.

The difference in optimal maintenance intervals between cov=0.6 and cov=1.0 is more dramatic than that between cov=0.6 and cov=0.4. For example, for $r_{od} = 3.0$, the interval could be one year when cov=1.0, but an interval of 2.5 years is sufficient for both cov=0.6 and 0.4 though the operational unavailability is lesser for cov=0.4 when compared to that of cov=0.6. Also observed for a degradation ratio of 10.0 is the relatively steeper increase in operational unavailability if the maintenance interval is more than a year. The application demonstrated could be practically utilized to decide on a maintenance frequency for a class of components prone more to degradation induced failures than catastrophic ones.

4.7.4 Conclusion

An extension of Markov model to evaluate optimum maintenance interval has been proposed based on the theory of semi-Markov process model. This advancement allows non-exponential distributions to be used in the model to describe phenomena underlying state transitions. An example application was demonstrated assuming that component degradation follows Weibull distribution. It was observed that there is significant scope of over-estimating operational unavailability and hence optimum maintenance intervals by assuming a constant degradation rate. The proposed model reduces to a Markov model by assuming constant rate for all the transitions, and further reduces to a standard PRA model if the degradation and maintenance states are eliminated from the model. In other words, the proposed model can be viewed as a direct extension of PRA techniques to account for ageing in a degrading system.

Chapter 5

Monte-Carlo Simulations

5.1 Introduction

Wang and Pham (1997) listed four main difficulties in evaluating availability of complex large scale systems - complex system structure, various failure distributions, arbitrary repair distributions in case of maintainability and insufficient failure data This paper identified Monte Carlo technique combined with Bayes method as a powerful tool to deal with these complexities. This chapter is primarily targeted at promoting Monte Carlo simulation as a validation tool to verify the semi-Markov process model.

5.2 Literature review

Billinton and Li (1994) introduced basic concepts and applications of Monte Carlo simulation with practical applications to electric power generation, transmission, and distribution systems. They summarized Monte Carlo availability simulation procedures and surveyed various reduction techniques. Ramirez-Marquez and Coit (2005) argued that binary state analysis of a system is insufficient and described a Monte Carlo methodology for estimating reliability of a multi-state network based on minimal cutsets. Billinton and Wangdee (2006) utilized sequential Monte Carlo simulation in bulk electric systems to obtain reliability indices. Naess et al. (2009) focused on development of Monte Carlo based method for estimating the reliability of structural systems. Based on the failure probability obtained by Monte Carlo simulation,the paper set up an approximation procedure to reduce the computational cost.

5.3 Reliability indices

Instantaneous or point availability of a system is the probability that it is operational at a time t. A single trial in availability simulation consists of failure and repair times generated until the mission time t. Many such trials are conducted. The status of the system at the end of the mission is noted as:

$$x_i = \begin{cases} 1 & \text{if system operating at end of mission for } i^{th} \text{ trial} \\ 0 & \text{otherwise} \end{cases}$$

Then, for sufficiently large number N of trials, the instantaneous unavailability of the system at time t can be calculated from x_i:

$$\widehat{Q} = 1 - \frac{1}{N}\sum_{i=1}^{N} x_i$$

If N is small, the denominator in Equation 5.3 is replaced with $N - 1$ in order to obtain an unbiased estimate of unavailability.

Further, by keeping track of the mean downtime, an estimate of the steady state unavailability can be determined:

$$Q = \frac{\text{mean downtime}}{\text{mean uptime} + \text{mean downtime}}$$

The mean $E(x)$ and variance $V(x)$ of the simulated observations can be obtained from:

$$E(x) = \overline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$V(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - \overline{x})^2 = \frac{1}{N}\sum_{i=1}^{N} \left(x_i^2\right) - \overline{x}^2$$

Note that x_i in 5.3 can be any reliability index whose mean and variance are of interest. For example, if x_i are the steady state unavailabilities for each trial

i, then $\overline{x}$ and $V(x)$ represent the average and variance estimates of steady state unavailability.

5.4 Simulation algorithm

The algorithm to obtain the reliability estimates consists of two major modules - building a time line of events and then analyzing them to obtain the necessary reliability indices. An abridged pseudo-code comprising both the modules is presented in this section.

5.4.1 Time line construction

A time line consists of all the component events placed in chronological order until the assumed mission time. A time line corresponds to one trial. This section presents a pseudo-code to construct such a time line.

It is assumed that each component of the system follows a general failure and repair distribution. Further each component can either be repairable or non-repairable. Random failure and repair times are based on the "inverse transform" method (Billinton and Li, 1994). In this method, a uniform random number p in [0,1] is generated and the *cdf* of the distribution for the time to event is inverted to obtain a sample time. A pseudo-random generator like Mersenne twister (Matsumoto and Nishimura, 1998) can be used to generate p. It is ideal for Monte Carlo simulations with provision for fast and high quality pseudo-random numbers.

1. Constants
    - DOWN: event denoting component failure
    - UP: event denoting completion of component repair
2. Variables
    - T_{cum}: cumulative time
    - T_m: mission time
    - E: component event - either component DOWN or UP
    - T_e: Time associated with event E

```
    • $C$: Component associated with event $E$
    • $L$: List of events
3. For each component $C$ in the system
    • $T_{cum}$=0, E=DOWN
    • Repeat until $T_{cum} \leq T_m$
        – $T_e$=$\begin{cases} \text{next failure time of } C & \text{if } E\text{=DOWN} \\ \text{time of completion of repair of } C & \text{if } E\text{=UP} \end{cases}$
        – If $T_{cum} + T_e$ has exceeded $T_m$, proceed to next component
        – Add event $E$ to the list $L$
        – If component is not repairable, proceed to next component
        – $T_{cum} = T_{cum} + T_e$
        – Set $E = \begin{cases} DOWN & \text{if E=UP} \\ UP & \text{if E=DOWN} \end{cases}$
4. Sort $L$ according to $T_e$
5. $L$ is the required time line
```

5.4.2 System analysis

Availability analysis

For each time line made up of component events, the time line is analyzed for system failures and down time of the system is tracked accordingly. In order to evaluate availability, the status of the system at the end of the mission is noted. It is assumed that components and hence the system cannot fail until the system is completely recovered from an earlier system failure. The time line consists of all failures and repairs irrespective of whether they have occurred when system is in repair or not. The pseudo code in this section ignores failures during a system failure, however, components that failed earlier to system failure can continue to be repaired. Since components of a cutset are equivalent to a parallel system, failure of all components in the cutset leads to system failure and repair of at least one of its components leads to system repair. To achieve this, a count of the number of components failed in each cutset is stored. When this count reaches length of the cutset, it is considered as a system failure provided system is not already under repair.

1. Variables

   - E: a component event - failure / repair
   - C: component associated with E
   - M: minimal cutset of which C is a member
   - $len(M)$: length of the minimal cutset M
   - $N(M)$: Number of components failed in M
   - T_m : Mission time
   - T_e: $\begin{cases} \text{Failure time} & \text{if } E \text{ is DOWN} \\ \text{Repair time completion} & \text{if } E \text{ is UP} \end{cases}$
   - T_f: Time of last system failure
   - S: minimal cutset due to which system failed
   - DT: total downtime of the system until mission time
   - RDT: remaining down time from the current time
   - B_f: System failed - True or False
   - x_i : $\begin{cases} 1 & \text{if system operating at end of mission for } i^{th} \text{ trial} \\ 0 & \text{otherwise} \end{cases}$
   - N_f: Number of system failures encountered
   - T_{ff}: Time to first system failure

2. Initialize

   - $S = M =$ None
   - T_e= $DT = RDT = T_f = N(M) = N_f = 0$
   - x_i= 1
   - B_f=False

3. Definitions

   - System repair completion
     - System earlier failed due to cutset M

```
        – Component $C$ belongs to $M$
        – $E$ is completion of repair of component $C$
    • System failure
        – $E$ is failure of component $C$
        – $C$ belongs to the cutset $M$
        – $N(M)$ has reached $len(M)$ (all components of cutset $M$ have failed)
        – $B_f$ is false (ensure no failures when system down)
4. For each event $E$ on the time line
    • Set $C$,$T_e$ and $M$ based on $E$
    • If $E$ is a "system repair completion"
        – $DT = DT + (T_e$-$T_f)$          (down time since last system failure)
        – $B_f$= False, RDT=0, $x_i$= 1
    • $N(M) = N(M) + \begin{cases} 1 & \text{if } E \text{ is DOWN} \\ -1 & \text{if } E \text{ is UP} \end{cases}$
    • If $E$ is a "system failure"
        – $B_f$= True, $T_f$= $T_e$,$x_i$=0
        – $N_f = N_f + 1$ (Increment system failures)
        – If $N_f = 1$, then set $T_f$ to $T_e$ (time-to-first-failure)
        – RDT=RDT+($T_m$ - $T_e$)
5. $DT = DT + RDT$          (add up any remaining down time)
6. $UT = T_m$ - $DT$
```

Reliability analysis

In reliability analysis, only the first failure of the system is of interest. However, component repairs can take place as long as the component failure does not lead to a system failure. The time line construction for reliability analysis remains the same as discussed in Section 5.4.1. Hence, in this section the above pseudo-code is modified so that the system repairs are not considered. The algorithm exits when a system failure is encountered.

1. Variables

   - E: a component event - failure / repair
   - C: component associated with E
   - M: minimal cutset of which C is a member
   - $len(M)$: length of the minimal cutset M
   - $N(M)$: Number of components failed in M
   - T_m : Mission time
   - T_e: $\begin{cases} \text{Failure time} & \text{if } E \text{ is DOWN} \\ \text{Repair time completion} & \text{if } E \text{ is UP} \end{cases}$
   - S: minimal cutset due to which system failed
   - i: trial number
   - x_i : $\begin{cases} 1 & \text{system operating at end of mission} \\ 0 & \text{otherwise} \end{cases}$

2. Initialize

   - $S = M =$None, x_i= 1
   - T_e= $N(M) = 0$

3. Definitions

   - System failure
     - E is failure of component C
     - C belongs to the cutset M
     - $N(M)$ has reached $len(M)$ (all components of cutset M have failed)

4. For each event E on the time line

   - Set C,T_e and M based on E
   - $N(M) = N(M) + \begin{cases} 1 & \text{if } E \text{ is DOWN} \\ -1 & \text{if } E \text{ is UP} \end{cases}$
   - If E is a 'system failure'
     - x_i=0, exit

5.5 Example

Consider the reliability block diagram in Figure 5.1. This is the same problem considered in Section 3.11. For convenience, component data is listed again in Table 5.1.

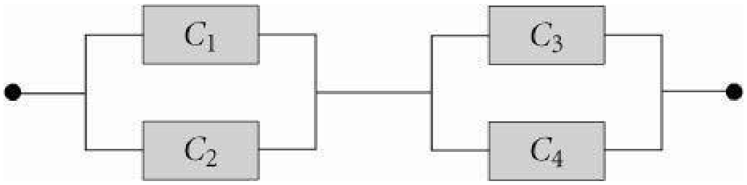


Figure 5.1: Reliability block diagram.

This system has seven cutsets:

$$\{C1, C2\}, \{C3, C4\}$$
$$\{C1, C2, C3\}, \{C1, C2, C4\}$$
$$\{C3, C4, C1\}, \{C3, C4, C2\}$$
$$\{C1, C2, C3, C4\}$$

However only the first two cutsets are minimal cutsets. The others are not since there is at least one component in each of these cutsets such that by removing these components, the set is still a cutset. For example, by removing {C3} from {C1, C2, C3}, the resulting set {C1, C2} is still a cutset. Recall the assumption that components do not fail when the system is down and until completely restored. However, repair of components can continue whether or not they are part of the cutset that failed.

Table 5.1: Component data for the four component example system

Component	Mean failure time, cov (years)	Mean repair time (years)
C1	40,1	0.5
C2	30,0.3	1
C3	30 , 1	0.5
C4	20, 0.25	1

For a single component, the only cutset and minimal cutset is the singleton set with the component itself. In this case, the component and the system mean the same. The system is up when this component is up and it is down when this component is down. This is equivalent to an alternating renewal process with distinct failure and repair distributions. Unavailability of each of the components is shown in Figure 5.2. It is seen that for a single component the Monte Carlo estimates are quite accurate with less variance.

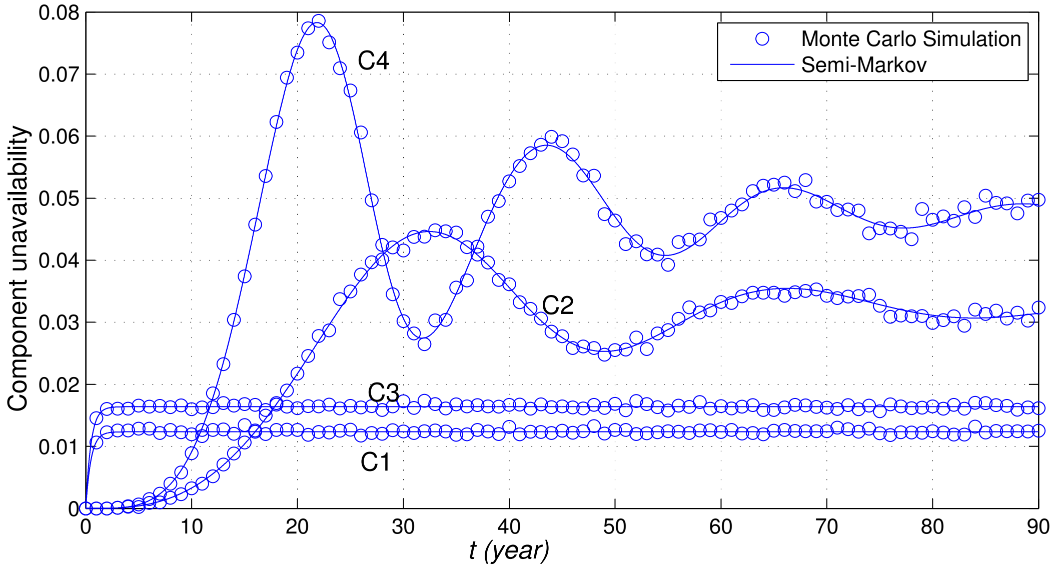
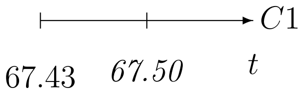
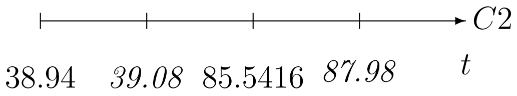
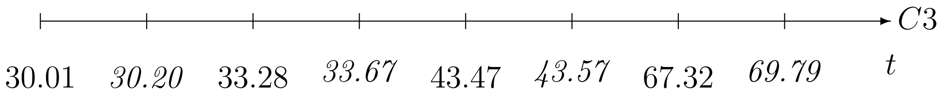


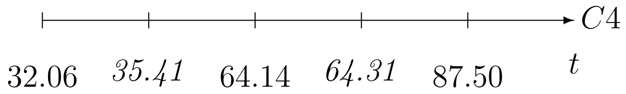
Figure 5.2: Unavailability of individual components.

A sample time line for each component of the 4-component system generated using the pseudo-code presented in Section 5.4.1 is presented here:









By merging all the events and sorting them in the order of occurrence, a single trial representing the time line of events is listed in Table 5.2. This table was generated using the algorithm to generate the times lines. It also shows which of the components were operational at each instant an event occurred.

Table 5.2: A sample trial of events until 90 years

Component	Event Type	Event Time (yrs)	Working Components
C3	Down	30.0195	1,2,4
C3	Up	30.2037	1,2,3,4
C4	**Down**	**32.0616**	**1,2,3**
C3	**Down**	**33.2826**	**1,2**
C3	Up	33.6788	1,2,3
C4	Up	35.4109	1,2,3,4
C2	Down	38.9459	1,3,4
C2	Up	39.0817	1,2,3,4
C3	Down	43.4714	1,2,4
C3	Up	43.5758	1,2,3,4
C4	Down	64.1478	1,2,3
C4	Up	64.3193	1,2,3,4
C3	Down	67.3238	1,2,4
C1	Down	67.4363	2,4
C1	Up	67.5091	1,2,4
C3	Up	69.7963	1,2,3,4
C2	Down	85.5416	1,3,4
C4	Down	87.5023	1,3
C2	Up	87.9878	1,2,3

In the above trial, failure of C3 at 33.28 years led to a system failure and the system is recovered at 33.68 years after C3 is repaired. The downtime is nearly 4.8 months. Despite system failure, the system is operational at the end of the mission. Hence, for this trial the system is available at the end of 90 years.

By repeating such trials large number of times for each time point in the interval [0,90] using the algorithm for analyzing the time line and applying the formula in Equation 5.3, time dependent system unavailability can determined as in Figure 5.3.

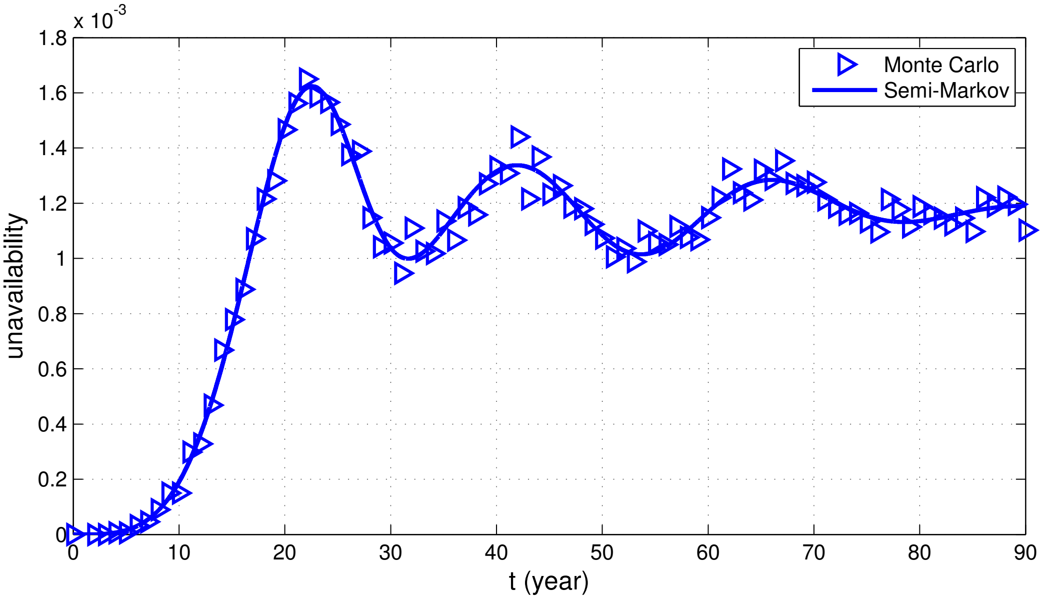


Figure 5.3: System unavailability.

For subsystem 1 and subsystem 2, there is one minimal cutset each. Figure 5.4 and 5.5 respectively illustrate the subsystem level unavailability.

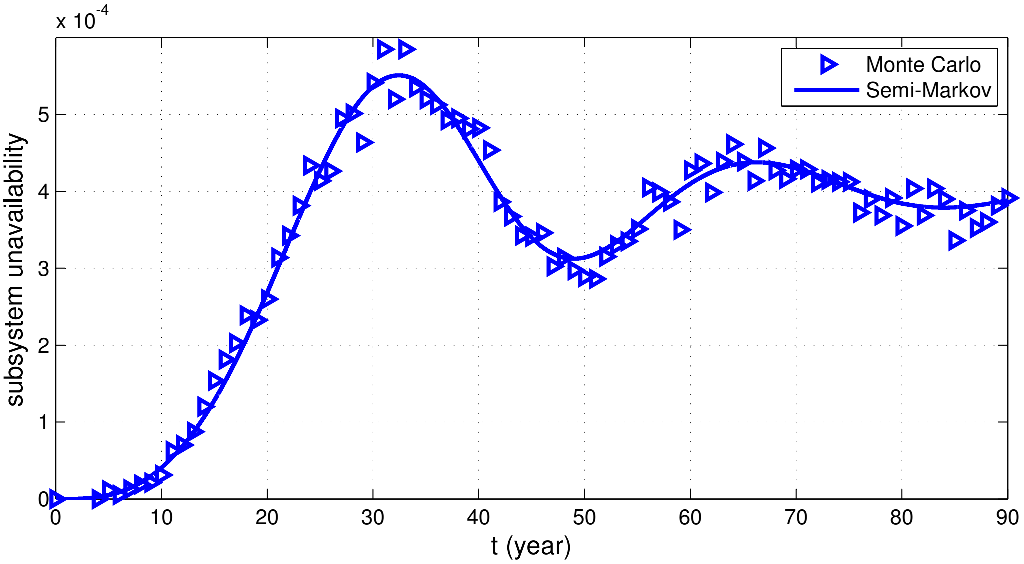


Figure 5.4: Unavailability of subsystem 1.

By averaging all the down times obtained in each trial and applying the formulae in Equation 5.3 and 5.3, an estimate of mean and variance of steady state unavailability of each component and the system can be obtained. However, convergence to steady state unavailability often requires that the trial is carried out beyond the mission time. In cases where failure rates are extremely low and repair

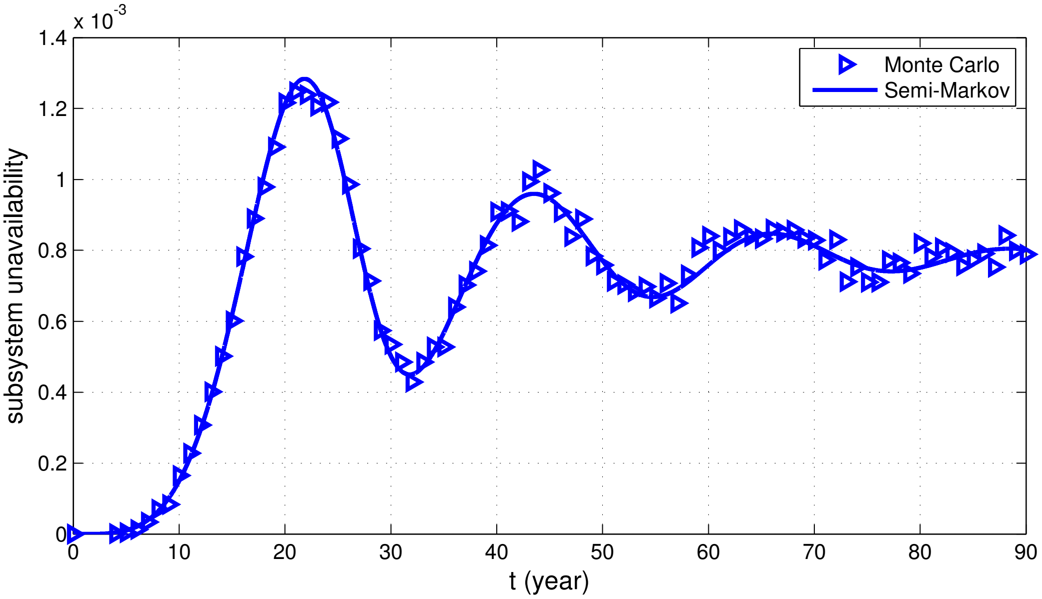


Figure 5.5: Unavailability of subsystem 2.

times are small, steady state unavailability might be reached much beyond the useful life period of the system. Figure 5.6 shows how steady state unavailability is gradually reached with increasing time until 90 years.

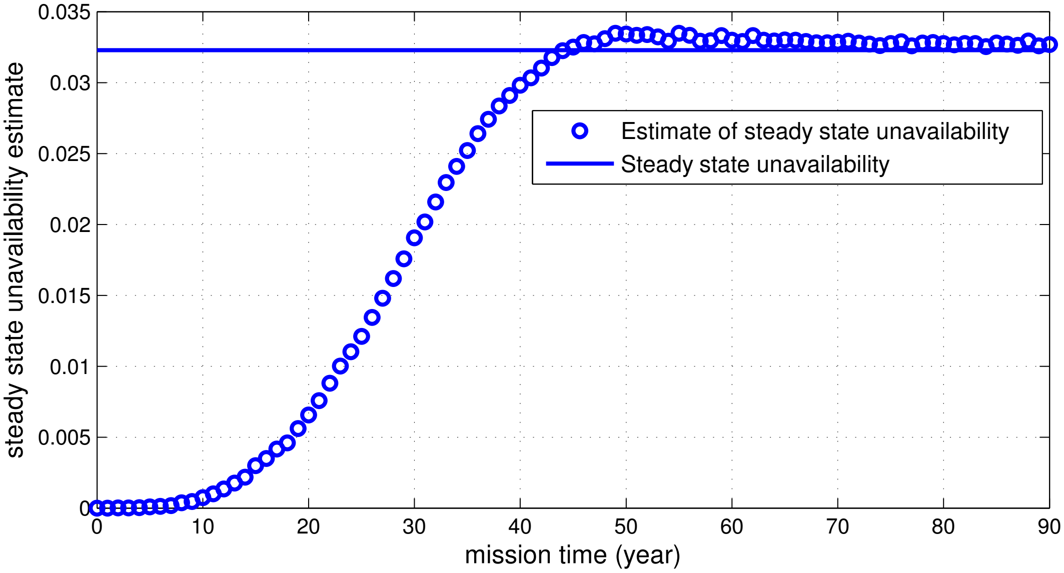


Figure 5.6: Steady state availability of component C2.

Component and system steady state unavailabilities for the 4-component system are listed in Table 5.5. Components trials were replicated 500,000 times while system trials were replicated 1,000,000 times.

Table 5.3: Steady state unavailabilty of 4-component system by Monte Carlo method.

Component	Steady state unavailability (variance)
C1	0.0128121 (0.00012996)
C2	0.0322879 (0.00031301)
C3	0.0168828 (0.00017276)
C4	0.0476043 (0.00045350)
System	0.0010268 (0.00000756)

Table 5.4 lists the other indices such as mean time-to-first failure of the system, average unproductive time spent and the mean number of failures encountered until the mission time of 90 years. Note that all these indices are relatively lesser in the system case. This is due to the rarity of occurrence of minimal cutset failures. The mean number of failures for the components is approximately equal to the ratio of mission time to mean life of the component.

Table 5.4: Time to first failure and other indices of the 4-component example.

Component	mean time-to- first failure(yrs)	mean downtime(yrs)	mean number of failures
C1	26.2975	1.1043	2.22182
C2	29.9824	2.4403	2.47324
C3	24.0351	1.46529	2.94996
C4	20.0027	3.81532	3.86452
System	11.8996	0.09246	0.278077

The simple 4-component example demonstrates the validity of semi-Markov process model and further proves that Monte Carlo has the potential to yield many other reliability estimates of interest to an analyst.

5.6 Case Study: Nuclear Component Cooling Water (NCCW) system

In this section the results of the NCCW system obtained by semi-Markov process model are validated using the Monte Carlo simulation method.

Table 5.5 shows four possible trials leading to a system failure. Since the failure rates of the redundant pump trains and heat exchanger train are of the order of 10^{-6}, it is likely that hardly one pump train failure is experienced in 10^6 trials.

Table 5.5: Sample trials for the NCCW system.

Trial	Component	Event Type	Event Time (hrs)	Remarks
1	Pump Train 12	Down	927.911	
	Pump Train 11	Down	959.527	System down
	Pump Train 12	Up	977.454	for 17.927 hrs
	Pump Train 11	Up	983.887	
2	Pump Train 12	Down	412.041	
	Pump Train 11	Down	439.551	System down
	Pump Train 11	Up	440.034	for 0.483 hrs
	Pump Train 12	Up	452.759	
3	Pump Train 11	Down	378.39	
	Pump Train 12	Down	380.199	System down
	Pump Train 12	Up	382.885	for 2.686 hrs
	Pump Train 11	Up	410.539	
4	Heat Exchanger Train	Down	442.113	System down, not repairable

Hence this table considers a mission time of 1000 hrs to track the failures and repairs. The first three trials exemplify a system failure due to the failure of both the pump trains while the last one shows the possibility of a system failure due to heat exchanger train.

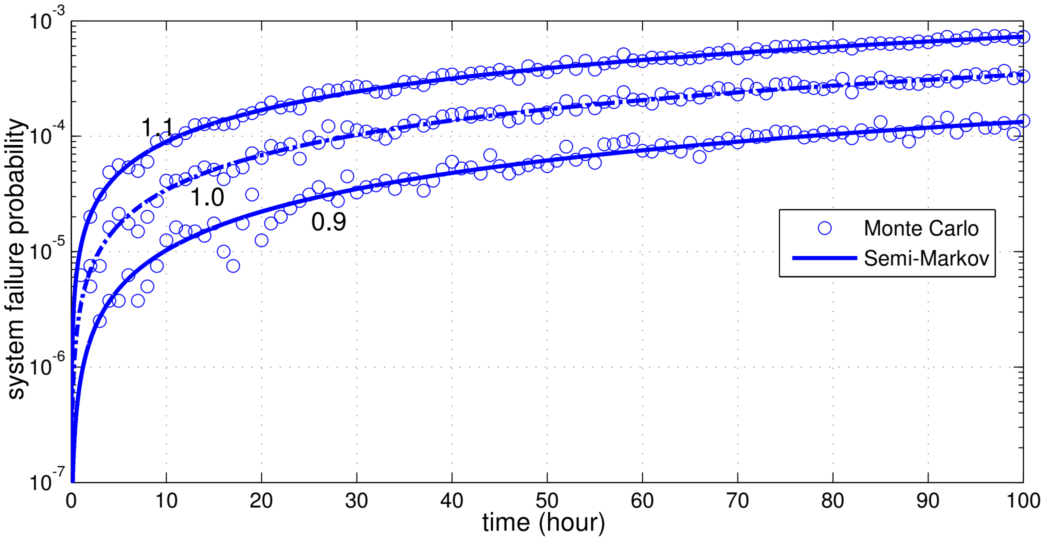


Figure 5.7: System failure probability.

Figure 5.7 compares the system unreliability of the NCCW system with Weibull distribution for heat exchanger train failure obtained by Monte Carlo and semi-Markov methods. It is seen that Monte Carlo traces the stochastic process very

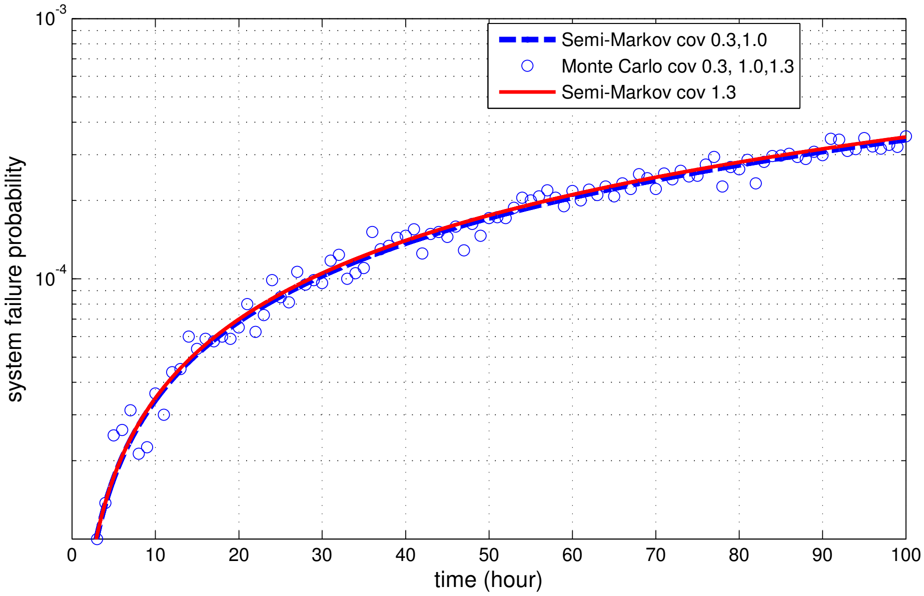


Figure 5.8: System failure probability with cov=0.3,1.0, and 1.3.

well except for relatively higher variance in the first 30 hrs.

Figure 5.8 verifies the results in the case where only the pump train failure follows Weibull distribution. Redundancy, low failure rates and prompt repair prevent the system from rapidly ageing.

5.7 Conclusion

Monte Carlo method has immense flexibility in simulating a large system with a wide array of features and events including degrading components, redundancy, repair, repair crews, spares, inspections, preventive maintenance, cost, logistic delays etc. However, combinatorics and replications consume large amount of time leading us in search of better options. For large systems with multi-state components, system availability computation using Monte Carlo simulation becomes extremely prohibitive. The next chapter deals with a technique that has the ability to mix Markov, Semi-Markov and Monte Carlo methods in a system reliability problem.

Chapter 6

Universal Generating Function (UGF) Method

6.1 Introduction

A typical nuclear power plant system consists of several components (elements) with different hazard and repair rates. The reliability indices of a complex system has been computed traditionally using Fault Tree Analysis (FTA), Reliability Block Diagrams (RBD), stochastic processes like Markov and semi-Markov processes etc. Stochastic processes mentioned are well suited for dealing with multi-state elements, but, they suffer from 'state-explosion' or 'dimension damnation' when applied to a system with many elements. If there are N elements, the number of system states may go up to 2^N. Moreover, state enumeration cannot be elegantly depicted. The number of system states have to be forcibly reduced by different techniques such as lumping series elements in to one component or merging states of similar functionality thus compromising the accuracy of the results. Hence this chapter explores and brings together a set of engineering tools that can deftly compute the availability of a complex system with accuracy, simplicity, less computational burden and without compromising all the possible states of a system and its components.

6.2 Literature Review

The mathematical fundamentals of the Universal Generating Function (UGF) were introduced by Ushakov (1987). Levitin et al. (1998) generalized a redundancy optimization problem to multi-state systems where in UGF is used as a fast procedure to evaluate the multi-state system availability. Levitin and Lisnianski (1999) developed an importance analysis tool for complex series-parallel multi-state systems based on UGF. Ushakov (2000) introduced a composition operator for UGF as a special case of the operator in generalized generating sequences suitable to optimal redundancy problems. Levitin (2001b) adapted the UGF method of multi-state system reliability analysis to incorporate common-cause failures (CCF) using an implicit 2-stage approach. Levitin (2001a) combined the UGF technique with Genetic Algorithm (GA) for solving a family of MSS reliability optimization problems, such as structure optimization, optimal expansion, maintenance optimization and optimal multistage modernization. Lisnianski and Levitin (2003) presented a UGF based method for reliability evaluation of different types of analysis of multi-state system reliability. They also proposed a combination of Markov process with the UGF method by extending the Reliability Block Diagram. Levitin (2004) extended the UGF technique used for the analysis of multi-state systems to the case when the performance distributions of some elements depend on states of another element or group of elements. Levitin (2005) gave a comprehensive description of the UGF technique and its applications in both binary and multi-state system reliability analysis.

6.3 Foundations of Universal Generating Function

6.3.1 Probability mass function (pmf)

For a discrete random variable X, the probability mass function (pmf) is the probability that X assumes the exact value of x; i.e., pmf of X is $\mathrm{P}(X = x)$.

Example

Consider an element A whose set of states are denoted by the r.v. X_1. Let x_1={0,1}, p_1={0.6, 0.4} be the pmf of X_1. *i.e.* $P(X_1 = 0) = 0.6$ and $P(X_1 = 1) = 0.4$ such that $P(X_1 = 0) + P(X_1 = 1) = 1$ Here, element failure is denoted by 0 and its functional state is denoted by 1.

Similarly, let B be another element denoted by the r.v. X_2. Let x_2={0,1}, p_2={0.7, 0.3} be the *pmf* of X_2.

Let A and B undergo failures and repairs independently. Then X_1 and X_2 are statistically independent random variables. This assumption allows the multiplication of probabilities to find the corresponding system level probabilities.

If A and B are connected in series and form a system, then $Y_1 = X_1X_2$ yields all possible states of the system. Similarly, $Y_2 = 1 - (1 - X_1)(1 - X_2)$ yields all possible states of the system for a parallel configuration. Table 6.1 lists the *pmf* of the system states.

From the table, it is possible to obtain availability of a parallel system as

$$\begin{aligned}A &= P(Y_2 = 1)\\ &= P(X_1 = 0)P(X_2 = 1) + P(X_1 = 1)P(X_2 = 0) + P(X_1 = 1)P(X_2 = 1)\\ &= 0.18 + 0.28 + 0.12 = 0.58\end{aligned}$$

Table 6.1: System states for a series and parallel configuration

#	$X_1 = x_1$	$X_2 = x_2$	**Series**	**Parallel**	**Probability**
			Y_1	Y_2	P(X_1=x_1)P(X_2=x_2)
1	0	0	0	0	0.42
2	0	1	0	1	0.18
3	1	0	0	1	0.28
4	1	1	1	1	0.12
				Sum	1.0

It would be elegant if these possibilities can be represented in a compact form and easily computed. With this intent the next section discusses the moment generating function.

6.3.2 Moment generating function (*mgf*)

The *mgf* $m_X(t)$ of the discrete random variable X with *pmf* x, p is defined for all values of t by

$$m_X(t) = E[e^{tX}] = \sum_{i=0}^{k} e^{tx_i}p_i$$

The function $m_X(t)$ is called the moment generating function because all of the moments of r.v. X can be obtained by successively differentiating $m_X(t)$.

6.3.3 Probability generating function (pgf)

The pgf of a r.v. X can be obtained by replacing e^t by the variable z in its mgf (6.3.2):

$$\omega_X(z) = E[z^X] = \sum_{i=0}^{k} z^{x_i} p_i$$

i.e., pmf of a r.v. X can be represented by its pgf in polynomial form.

Example

pgf of X_1 and X_2 in Example 6.3.1 are given by the following functions:

$$u_1(z) = \omega_{X_1}(z) = 0.6z^0 + 0.4z^1$$
$$u_2(z) = \omega_{X_2}(z) = 0.7z^0 + 0.3z^1$$

pmf of the system is given by the product of these polynomials. A formal procedure for multiplication of these functions is discussed in the next section.

6.3.4 Universal Generating Function

Consider a composition operator Ω_ϕ to combine two u-functions $u_1(z)$ and $u_2(z)$:

$$\begin{aligned} U(z) =& \Omega_\phi(u_1(z), u_2(z)) \\ =& \Omega_\phi(\sum_{i_1=1}^{k_1} p_{1i_1} z^{g_{1i_1}}, \sum_{i_2=1}^{k_2} p_{2i_2} z^{g_{2i_2}}) \\ =& \sum_{i_1=1}^{k_1} \sum_{i_2=1}^{k_2} p_{1i_1} p_{2i_2} z^{\phi(g_{1i_1}, g_{2i_2})} \end{aligned}$$

Thus the z-transforms of the random variables along with the composition operator Ω_ϕ to combine them is called the universal z-transform or universal (moment) generating function (UGF).

In particular, Ω_ϕ can be defined for series and parallel connections respectively as follows:

$$\begin{aligned}U(z) =&\Omega_{\phi_s}(\sum_{i_1=1}^{k_1} p_{1i_1} z^{g_{1i_1}}, \sum_{i_2=1}^{k_2} p_{2i_2} z^{g_{2i_2}})\\ =&\sum_{i_1=1}^{k_1}\sum_{i_2=1}^{k_2} p_{1i_1}p_{2i_2} z^{g_{1i_1}*g_{2i_2}}\end{aligned}$$

$$\begin{aligned}U(z) =&\Omega_{\phi_p}(\sum_{i_1=1}^{k_1} p_{1i_1} z^{g_{1i_1}}, \sum_{i_2=1}^{k_2} p_{2i_2} z^{g_{2i_2}})\\ =&\sum_{i_1=1}^{k_1}\sum_{i_2=1}^{k_2} p_{1i_1}p_{2i_2} (z^{1-(1-g_{1i_1})*(1-g_{2i_2})}\end{aligned}$$

Example

It can be seen that the probabilities in Table 6.1 can be obtained by simple polynomial multiplication of $u_1(z)$ and $u_2(z)$ as per Equations 6.3.4 and 6.3.4 for series and parallel configurations respectively.

$$\begin{aligned}\textbf{For series connection, } U(z) &= \Omega_{\phi_s}(0.6z^0 + 0.4z^1, 0.7z^0 + 0.3z^1)\\ &= 0.42z^0 + 0.18z^0 + 0.28z^0 + 0.12z^1\\ \textbf{For parallel connection, } U(z) &= \Omega_{\phi_p}(0.6z^0 + 0.4z^1, 0.7z^0 + 0.3z^1)\\ &= 0.42z^0 + 0.18z^1 + 0.28z^1 + 0.12z^1\end{aligned}$$

6.3.5 Extended Reliability Block Diagram

For multi-state components which have to be connected in a particular order, an extended RBD embeds a Markov or a semi-Markov space diagram with in it. By doing so, each block of the RBD would have multiple states embedded in it. Figure 6.1 illustrates an extended RBD of two elements A and B connected in series with their corresponding Markov space diagrams embedded in their respective blocks. The evaluation of the system structure function $\phi(\boldsymbol{x})$ becomes more tedious because of the book-keeping involved for all possible state and element combinations.

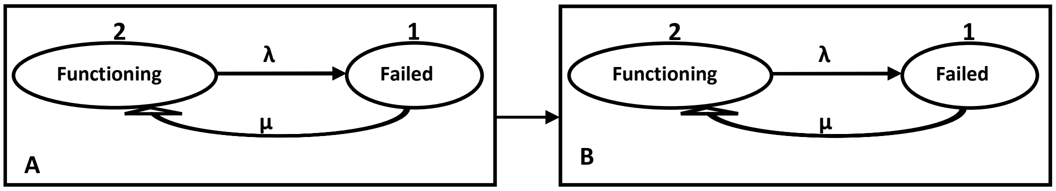


Figure 6.1: An extended RBD with embedded Markov space.

Hence, the next section introduces the idea of u-functions and composition operators attached to an extended RBD in order to simplify the tracking of numerous possibilities.

6.3.6 The u-function

A u-function is essentially a pgf in random variable z and it relates possible values of z with the corresponding probabilities:

$$u_j(z,t) = \sum_{i_j=1}^{k_j} p_{ji_j}(t) z^{g_{ji_j}}$$

Each element j with k_j states is represented as a u-function. The coefficients of z are time-dependent conditional state probabilities of the element j obtained by modelling the element as a semi-Markov process as discussed in Chapter 4. The exponent of z can be any arbitrary mathematical object representing the performance or state in which the element is currently in. It could be as simple as {0,1} corresponding to the failure or functioning state of the system or numbers representing the output of the element like the electricity in megawatts produced by the element. These u-functions are then composed together step-by-step according to the definition of a composition operator Ω_ϕ which is tailored to the series-parallel nature of the connections. ϕ is called the structure function, a terminology borrowed from RBD method and it defines how the performance or status of the elements are combined. Considering the series and parallel connections as AND and OR logical operations respectively, Ω_ϕ is defined as follows:

1. **Series Connection**

$$
\begin{aligned}
u(z,t) =&\Omega_{\phi_s}(u_1(z,t), u_2(z,t))\\
=&\Omega_{\phi_s}(\sum_{i_1=1}^{k_1} p_{1i_1}(t) z^{g_{1i_1}}, \sum_{i_2=1}^{k_2} p_{2i_2}(t) z^{g_{2i_2}})\\
=&\sum_{i_1=1}^{k_1}\sum_{i_2=1}^{k_2} p_{1i_1}(t) p_{2i_2}(t) z^{\phi_s(g_{1i_1}, g_{2i_2})}\\
=&\sum_{i_1=1}^{k_1}\sum_{i_2=1}^{k_2} p_{1i_1}(t) p_{2i_2}(t) z^{g_{1i_1} * g_{2i_2}}
\end{aligned}
$$

2. **Parallel Connection**

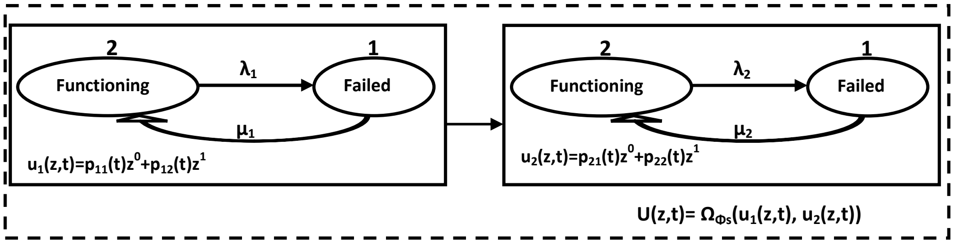
$$
\begin{aligned}
u(z,t) =&\Omega_{\phi_p}(u_1(z,t), u_2(z,t))\\
=&\Omega_{\phi_p}(\sum_{i_1=1}^{k_1} p_{1i_1}(t) z^{g_{1i_1}}, \sum_{i_2=1}^{k_2} p_{2i_2}(t) z^{g_{2i_2}})\\
=&\sum_{i_1=1}^{k_1}\sum_{i_2=1}^{k_2} p_{1i_1}(t) p_{2i_2}(t) z^{\phi_p(g_{1i_1}, g_{2i_2})}\\
=&\sum_{i_1=1}^{k_1}\sum_{i_2=1}^{k_2} p_{1i_1}(t) p_{2i_2}(t) z^{1-(1-g_{1i_1})*(1-g_{2i_2})}
\end{aligned}
$$

It is assumed that the elements of the system are statistically independent. The independence constraint assures that each element can be in one of its set of allowable states irrespective of which state the other elements are. This feature allows the multiplication of the state probabilities as seen in Equations 1 and 2. Since, a single (semi-)Markov system has been modularized in to individual blocks of an extended RBD, the UGF method does not consider the characteristics of system transitions between different states and hence the second assumption of repairability is needed.

The reliability indices like instantaneous availability and unavailability of the system can be derived directly from the final u-function after the composition. Usage of semi-Markov methods has been so far restricted to small systems due to their analytical and computational complexities. This proposed procedure leverages semi-Markov models by modularizing the entire system and composing them one at a time thus bringing a huge impact factor to the field of nuclear reliability engineering.

Example

Consider a system with two elements connected in series. Let each element be repairable with two states having the performance status - 1 (functioning) and 0 (failed). Let the failure/repair be exponentially distributed with a constant failure/repair rate. This system setup can be depicted in an extended RBD as in Figure 6.2. Let $p_{11}(t)$ and $p_{12}(t)$ be the probabilities of the element one being in state 1 and state 2 respectively. Similarly, let $p_{21}(t)$ and $p_{22}(t)$ be defined for element two. Then, the u-functions for element 1 and element 2 are respectively:



2
Functioning
λ_1
1
Failed
μ_1
$u_1(z,t)=p_{11}(t)z^0+p_{12}(t)z^1$
2
Functioning
λ_2
1
Failed
μ_2
$u_2(z,t)=p_{21}(t)z^0+p_{22}(t)z^1$
$U(z,t)= \Omega_{\Phi s}(u_1(z,t), u_2(z,t))$

Figure 6.2: Extended Reliability Diagram for Example 6.3.6.

$$\begin{aligned} u_1(z,t) &= p_{11}(t)z^0 + p_{12}(t)z^1 \\ u_2(z,t) &= p_{21}(t)z^0 + p_{22}(t)z^1 \end{aligned}$$

Since the elements are in series, the above u-functions are composed as per Equation 1:

$$U(z,t) = \{p_{12}(t)p_{21}(t) + p_{11}(t)p_{21}(t) + p_{11}(t)p_{22}(t)\}z^0 + p_{12}(t)p_{22}(t)z^1$$

The state probabilities are either obtained from Markov or semi-Markov models. The coefficient of z^0 gives the unavailability of the system and that of z^1 gives the availability.

$$\begin{aligned} \text{Availability, } A(t) &= p_{12}(t)p_{22}(t) \\ \text{Unavailability } = 1 - A(t) &= p_{12}(t)p_{21}(t) + p_{11}(t)p_{21}(t) + p_{11}(t)p_{22}(t) \end{aligned}$$

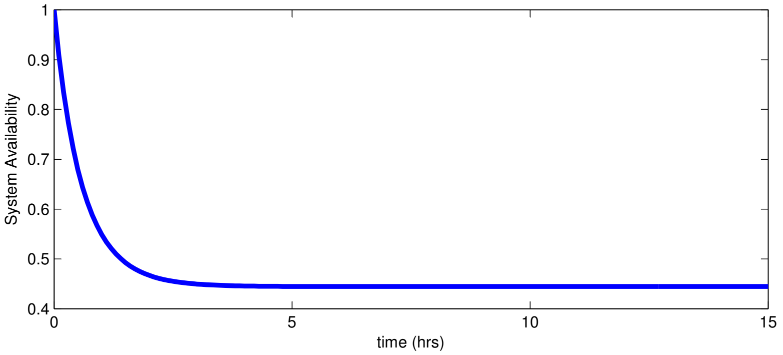


Figure 6.3: System availability of 2-state repairable system.

The availability plot is shown in Figure 6.3 with the parameters $\lambda_1 = \lambda_2 = 0.5$ and $\mu_1 = \mu_2 = 1$. Note that this example is the same as the Example 2.8.1 in the chapter on Markov processes. Over there, a system of four differential equations were solved. Here, two systems of two differential equations are solved at a time, the benefit here being the ability to modularize the system, depict the state transitions pictorially and avoid the problem of state explosion.

6.4 Example: Multi-State System

This section looks at a hypothetical system where each component of the system goes through multiple states. Consider two redundant parallel subsystems connected in series as shown in Figure 6.4.

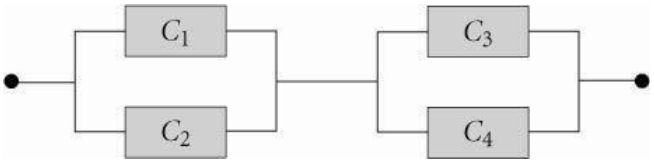


Figure 6.4: Reliability Block Diagram for the four component example problem.

This problem was earlier solved using the semi-Markov process model by solving for each component individually. Assume that each component can exist in three states - operational, degraded and failure.

The probability of being in each state for each individual component can be determined using semi-Markov process model and then the system unavailability can be obtained using the UGF technique. It is assumed that components C1 and

C2 are identical. Similarly, C3 and C4 are identical. The failure and repair data for each of the components is listed in Table 6.2.

Table 6.2: Failure/repair data in (time in hours, cov) format.

Component	time-to degradation $2 \to 1$	time-to failure $1 \to 0$	time-to recover $0 \to 1$	time-to restoration $1 \to 2$
C1, C2	20,0.3	10,0.6	0.8,1	0.5,1
C3, C4	35,0.3	5,0.6	0.8,1	0.5,1

State-space diagram for components C1 and C2 is shown in Figure 6.5. Similarly, the corresponding diagram for components C3 and C4 is shown in Figure 6.6.

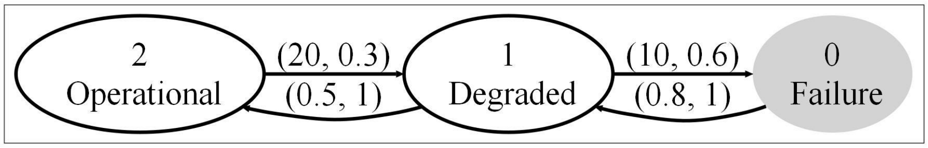


Figure 6.5: State-space for component C1 and C2.

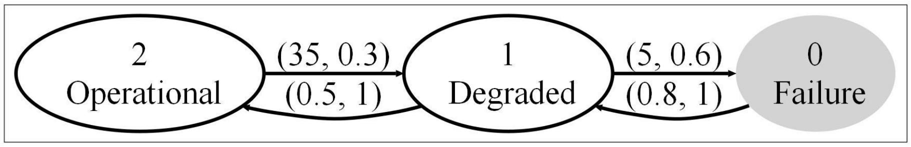


Figure 6.6: State-space for component C3 and C4.

A semi-Markov process model is fitted for each component. The results of the model are then used as the coefficients in the u-functions. For example, $p_{10}(t)$ represents the probability of component 1 being in state 0. It is equivalent to $\phi_{20}(t)$ of the corresponding semi-Markov model which represents that probability of component 1 being in state 0 at time t assuming that the component started its operation in state 2. u-function for each of the components is given below:

$$\begin{aligned}
u_{C1}(z,t) &= p_{10}(t)z^0 + p_{11}(t)z^1 + p_{12}z^2 \\
u_{C2}(z,t) &= p_{20}(t)z^0 + p_{21}(t)z^1 + p_{22}z^2 \\
u_{C3}(z,t) &= p_{30}(t)z^0 + p_{31}(t)z^1 + p_{32}z^2 \\
u_{C4}(z,t) &= p_{40}(t)z^0 + p_{41}(t)z^1 + p_{42}z^2
\end{aligned}$$

The coefficients of z^0 in $u_{Ci}(z,t)$ correspond to the unavailability of the component C_i. These quantities are plotted in Figure 6.7.

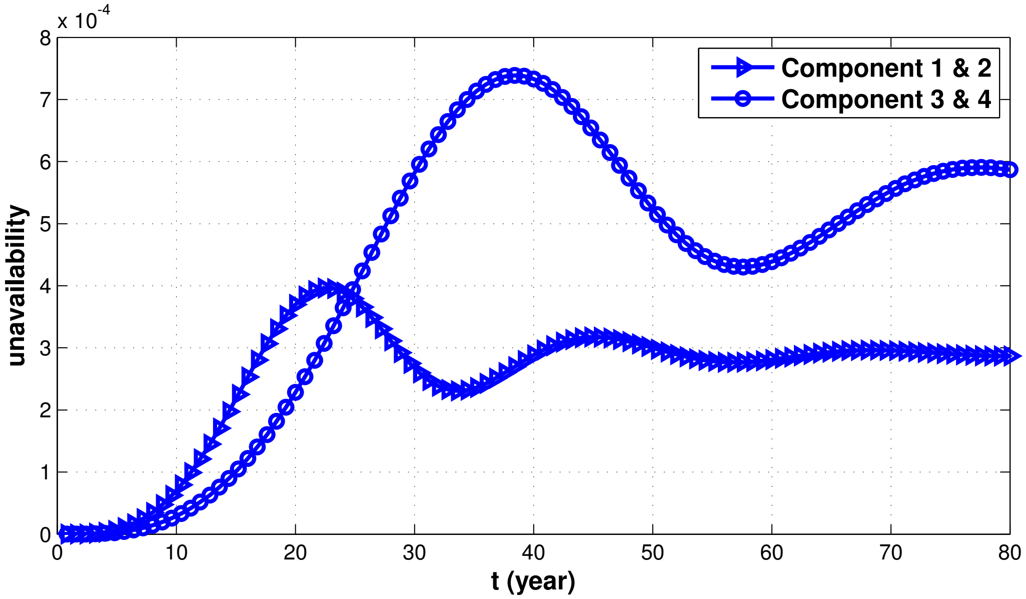


Figure 6.7: Unavailability of individual components.

u-functions can be written for the subsystems as well. Since components C1 and C2 are connected in parallel, the state performance for subsystem 1 is considered as the maximum of the state performances of both the components. These possibilities are listed in Table 6.3.

Table 6.3: Subsystem performance based on component states

	State	
Component 1	Component 2	Subsystem
(s_1)	(s_2)	$max(s_1, s_2)$
Normal (2)	Normal (2)	Normal (2)
Normal (2)	Degraded (1)	Normal (2)
Normal (2)	Failure (0)	Normal (2)
Degraded (1)	Normal (2)	Normal (2)
Degraded (1)	Degraded (1)	Degraded (1)
Degraded (1)	Failure (0)	Degraded (1)
Failure (0)	Normal (2)	Normal (2)
Failure (0)	Degraded (1)	Degraded (1)
Failure (0)	Failure (0)	Failure (0)

Let the u-functions for subsystem 1 and subsystem 2 be denoted as $u_{S1}(z,t)$ and $u_{S2}(z,t)$ respectively:

$$
\begin{aligned}
u_{S1}(z,t) &= u_{C1}(z,t)u_{C2}(t) \\
&= p_{10}(t)p_{20}(t)z^{max(0,0)} + p_{10}(t)p_{21}(t)z^{max(0,1)} + p_{10}(t)p_{22}(t)z^{max(0,2)} + \\
&\quad p_{11}(t)p_{20}(t)z^{max(1,0)} + p_{11}(t)p_{21}(t)z^{max(1,1)} + p_{11}(t)p_{22}(t)z^{max(1,2)} + \\
&\quad p_{12}(t)p_{20}(t)z^{max(2,0)} + p_{12}(t)p_{21}(t)z^{max(2,1)} + p_{12}(t)p_{22}(t)z^{max(2,2)} \\
&= p_{10}(t)p_{20}(t)z^0 + p_{10}(t)p_{21}(t)z^1 + p_{10}(t)p_{22}(t)z^2 + \\
&\quad p_{11}(t)p_{20}(t)z^1 + p_{11}(t)p_{21}(t)z^1 + p_{11}(t)p_{22}(t)z^2 + \\
&\quad p_{12}(t)p_{20}(t)z^2 + p_{12}(t)p_{21}(t)z^2 + p_{12}(t)p_{22}(t)z^2 \\
&= p_{10}(t)p_{20}(t)z^0 + \\
&\quad (p_{10}(t)p_{21}(t) + p_{11}(t)p_{20}(t) + p_{11}(t)p_{21}(t))z^1 + \\
&\quad (p_{11}(t)p_{22}(t) + p_{12}(t)p_{20}(t) + p_{12}(t)p_{21}(t) + p_{12}(t)p_{22}(t) + p_{10}(t)p_{22}(t))z^2 \\
&= v_{10}z^0 + v_{11}z^1 + v_{12}z^2
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
u_{S2}(z,t) &= p_{30}(t)p_{40}(t)z^0 + \\
&\quad (p_{30}(t)p_{41}(t) + p_{31}(t)p_{40}(t) + p_{31}(t)p_{41}(t))z^1 + \\
&\quad (p_{31}(t)p_{42}(t) + p_{32}(t)p_{40}(t) + p_{32}(t)p_{41}(t) + p_{32}(t)p_{42}(t) + p_{30}(t)p_{42}(t))z^2 \\
&= v_{20}z^0 + v_{21}z^1 + v_{22}z^2
\end{aligned}
$$

Since subsystems S1 and S2 are connected in series, the state performance for the system is considered as the minimum of the state performances of both the subsystems. These possibilities are listed in Table 6.4.

Let the u-function for the system be denoted as $u_S(z,t)$:

$$
\begin{aligned}
u_S(z,t) &= u_{S1}(z,t)u_{S2}(z,t) \\
&= v_{10}(t)v_{20}(t)z^{min(0,0)} + v_{10}(t)v_{21}(t)z^{min(0,1)} + v_{10}(t)v_{22}(t)z^{min(0,2)} + \\
&\quad v_{11}(t)v_{20}(t)z^{min(1,0)} + v_{11}(t)v_{21}(t)z^{min(1,1)} + v_{11}(t)v_{22}(t)z^{min(1,2)} + \\
&\quad v_{12}(t)v_{20}(t)z^{min(2,0)} + v_{12}(t)v_{21}(t)z^{min(2,1)} + v_{12}(t)v_{22}(t)z^{min(2,2)} \\
&= (v_{10}(t)v_{20}(t) + v_{10}(t)v_{21}(t) + v_{10}(t)v_{22}(t) + \\
&\quad v_{11}(t)v_{20}(t) + v_{12}(t)v_{20}(t))z^0 + \\
&\quad (v_{11}(t)v_{21}(t) + v_{11}(t)v_{22}(t) + v_{12}(t)v_{21}(t))z^1 +
\end{aligned}
$$

Table 6.4: System performance based on subsystem states

State		
Subsystem 1 (s_1)	Subsystem 2 (s_2)	System $min(s_1, s_2)$
Normal (2)	Normal (2)	Normal (2)
Normal (2)	Degraded (1)	Degraded (1)
Normal (2)	Failure (0)	Failure (0)
Degraded (1)	Normal (2)	Degraded (1)
Degraded (1)	Degraded (1)	Degraded (1)
Degraded (1)	Failure (0)	Failure (0)
Failure (0)	Normal (2)	Failure (0)
Failure (0)	Degraded (1)	Failure (0)
Failure (0)	Failure (0)	Failure (0)

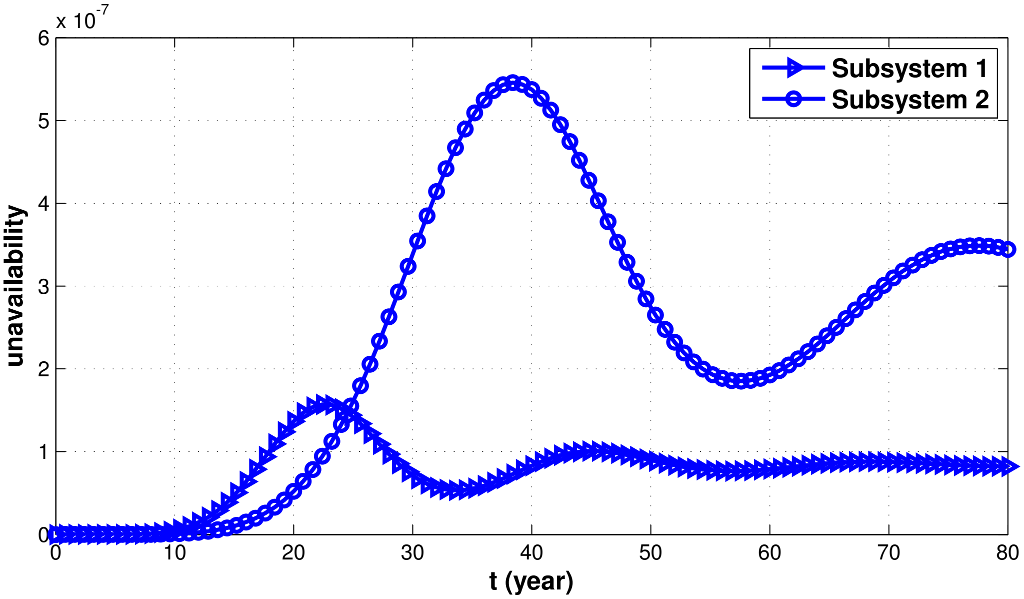


Figure 6.8: Unavailability of individual subsystems.

$$v_{12}(t)v_{22}(t)z^2$$

Collecting the coefficient of z^0 from $u_S(z,t)$, the system unavailability is found. It is plotted in Figure 6.9.

If this problem is solved by a single semi-Markov process model, there would be $3^4 = 81$ states leading to long computational times. Instead, by simplifying the model, there are only 3 states per component and hence 12 states overall. Polynomial multiplication is relatively much faster once the state probabilities are found by any of Markov, semi-Markov or Monte Carlo methods.

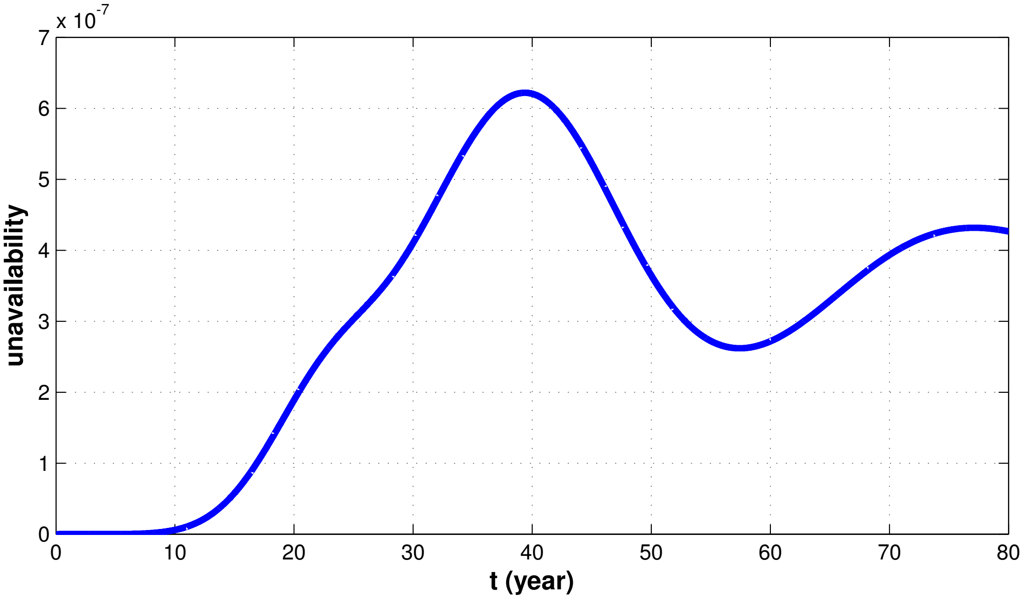


Figure 6.9: Unavailability of the system.

6.5 Case Study: Heat Transport System (HTS)

The proposed method is an improvement over conventional state-space analysis techniques. It needs a reliability block diagram with an embedded state space diagram as the main input. The block diagram helps in identifying the critical components and their series-parallel configuration. The state-space diagram gives an idea of failure and repair times during the life of the components.

Given the above, the objective is to find the availability of individual components and that of the entire system. A semi-Markov model is fitted to each of the components of the system and the respective state probabilities are computed. All these semi-Markov models are combined using the UGF technique. Availability and unavailability of the system follows from the polynomials output by UGF. The following case study on the heat transport system in a nuclear power plant walks through all the above steps.

The heat transport system (HTS) (Figure 6.10) circulates pressurized D_20 coolant through the fuel channels to remove the heat produced by fission in the nuclear fuel. The coolant transports the heat to steam generators, where it is transferred to light water to produce steam to drive the turbine. Two parallel HTS coolant loops are provided in the CANDU system. The heat from half of the several hundred fuel channels in the reactor core (380 in CANDU 6) is removed by each loop. Each loop has one inlet and one outlet header at each end of the reactor core. D_20 is fed

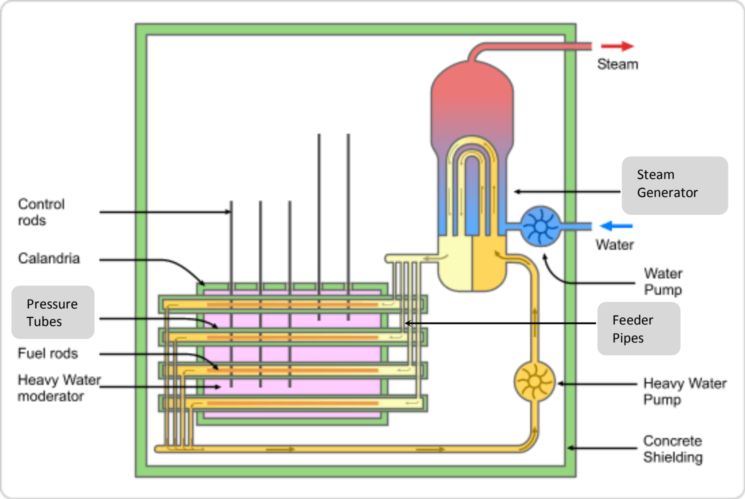


Figure 6.10: Schematic diagram of the CANDU Heat Transport System.

to each of the fuel channels through individual feeder pipes from the inlet headers and is returned from each channel through individual feeder pipes to the outlet headers. Each heat transport system loop is arranged in a ”Figure of 8”, with the coolant making two passes, in opposite directions, through the core during each complete circuit, and the pumps in each loop operating in series. The coolant flow in adjacent fuel channels is in opposite directions. The HTS piping is fabricated from corrosion resistant carbon steel. The pressure in the heat transport system is controlled by a pressurizer connected to the outlet headers at one end of the reactor. Valves provide isolation between the two loops in the event of a loss-of-coolant accident. Thus, the pressure tubes, feeder pipes and the steam generators form the

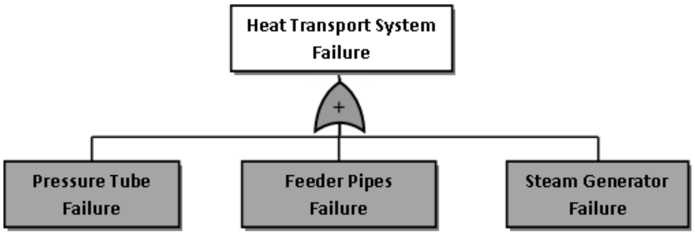


Figure 6.11: Fault tree diagram for the Heat Transport System.

main subsystem connected in series to each other as seen in the fault tree diagram in Figure 6.11. The reliability block diagram for this subsystem is shown in Figure 6.12. Moreover, only one loop of the two parallel coolant loops has been considered here for demonstration.

The mean life of the element gives an idea of the mean time to failure of the

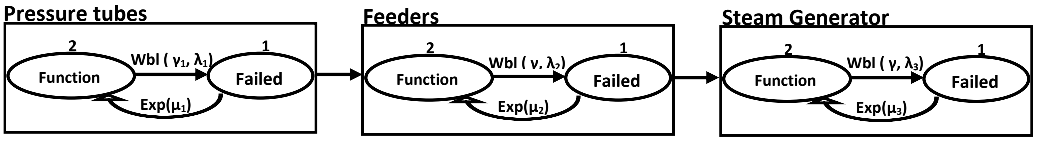


Figure 6.12: Extended Reliability Block Diagram of the Heat Transport System.

element. The coefficient of variation is the ratio of the standard deviation to the mean and for the Weibull distribution, it is a function of the shape parameter. These parameters along with the repair time are listed in Table 6.5.

Table 6.5: Parameters for the elements of heat transport system.

	Feeders	Pressure Tubes	Steam Generator
Mean Life (Yrs) μ_{wbl}	25	30	30
Coeff. of Var. cov_{wbl}	0.2	0.3	0.25
MTTR (Yrs) μ_i	0.1, 0.5, 1	0.1, 0.5, 1	0.1, 0.5, 1

The Weibull shape and scale parameters listed in Table 6.6 are back calculated from the following formulas for Weibull mean, standard deviation and coefficient of variation:

$$\begin{aligned} \mu_{wbl} &= \lambda\Gamma(1+\frac{1}{\gamma}) \\ \sigma^2_{wbl} &= \lambda^2\Gamma(1+\frac{2}{\gamma}) - \mu^2_{wbl} \\ \text{cov}_{wbl} &= \frac{\sigma_{wbl}}{\mu_{wbl}} \end{aligned}$$

Table 6.6: Weibull shape and scale parameters for the elements of the heat transport system.

	Feeder	Pressure Tubes	Steam Generator
Shape (γ_i)	5.797	3.714	4.542
Scale (λ_i)	26.999	44.3146	32.856

With the parameters of the Weibull and exponential distributions in hand, the semi-Markov kernel and waiting time matrices can be set up for i=1,2,3 corresponding to the pressure tubes, feeders and steam generator respectively:

$$H(t) = \begin{bmatrix} \delta(t-\infty) & \mu_i e^{-\mu_i t} \\ f_{wbl}(t|\gamma_i, \lambda_i) & 0 \end{bmatrix} \qquad W(t) = \begin{bmatrix} e^{-\mu_i t} \\ 1 - F_{wbl}(t|\gamma_i, \lambda_i) \end{bmatrix}$$

These matrices are plugged in to the semi-Markov renewal equation 3.10 and solved using the Trapezoidal algorithm to evaluate all the state probabilities $p_{ij}(t)$. Then, the u-functions for the pressure tubes, feeders and the steam generator are respectively:

$$\begin{aligned}
u_1(z,t) &= p_{11}(t)z^0 + p_{12}(t)z^1 \\
u_2(z,t) &= p_{21}(t)z^0 + p_{22}(t)z^1 \\
u_3(z,t) &= p_{31}(t)z^0 + p_{32}(t)z^1
\end{aligned}$$

Since the elements are connected in series, the operator Ω_{ϕ_s} is applied to the above u-functions:

$$\begin{aligned}
U(z,t) = \; & \Omega_{\phi_s}(u_1(z,t), u_2(z,t), u_3(z,t)) \\
& = \{p_{11}(t)p_{21}(t)p_{31}(t) + p_{11}(t)p_{21}(t)p_{32}(t) + p_{11}(t)p_{22}(t)p_{31}(t) + \\
& p_{11}(t)p_{22}(t)p_{32}(t) + p_{12}(t)p_{21}(t)p_{31}(t) + p_{12}(t)p_{21}(t)p_{32}(t) + \\
& p_{12}(t)p_{22}(t)p_{31}(t)\}z^0 + p_{12}(t)p_{22}(t)p_{32}(t)z^1
\end{aligned}$$

While the terms with zero as the exponent of z contribute to the unavailability of the system, the coefficient of the single remaining term gives the availability $A(t)$ of the heat transport system. Let $c > 0$ be the mean life of an element. Then its average availability is given by:

$$A_c = \frac{1}{c}\int_0^c A(t)dt$$

The average availability of each of the elements over the mission time given by their respective mean life for various repair times are shown in Table 6.7. Given the smaller failure rates and repair times, the average availability is very high signifying the heat transport system as a highly reliable subsystem of the nuclear power plant.

Table 6.7: Average availability for the elements and the heat transport system.

MTTR	Feeder	Pressure Tubes	Steam Generator	System
0.1	0.9979	0.9985	0.9985	0.9943
0.5	0.9910	0.9920	0.9923	0.9713
1	0.9837	0.9847	0.9855	0.9464

The observed pattern of unavailability of the elements of heat transport system

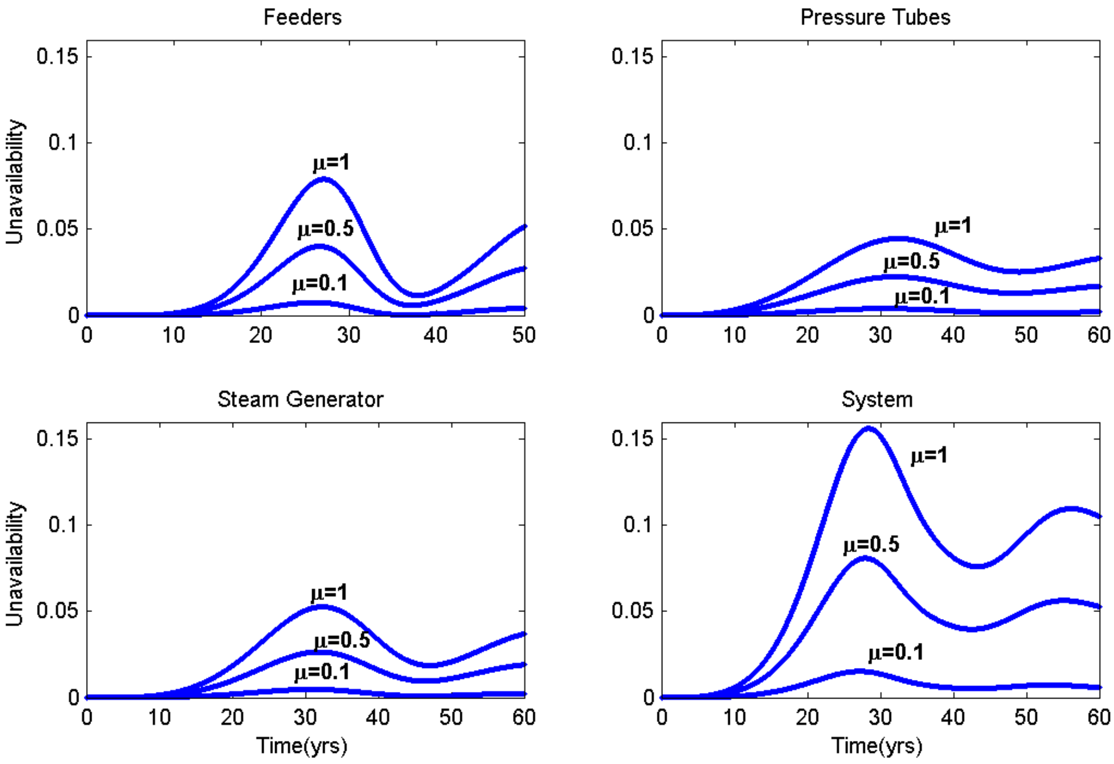


Figure 6.13: Unavailability plot - Effect of repair.

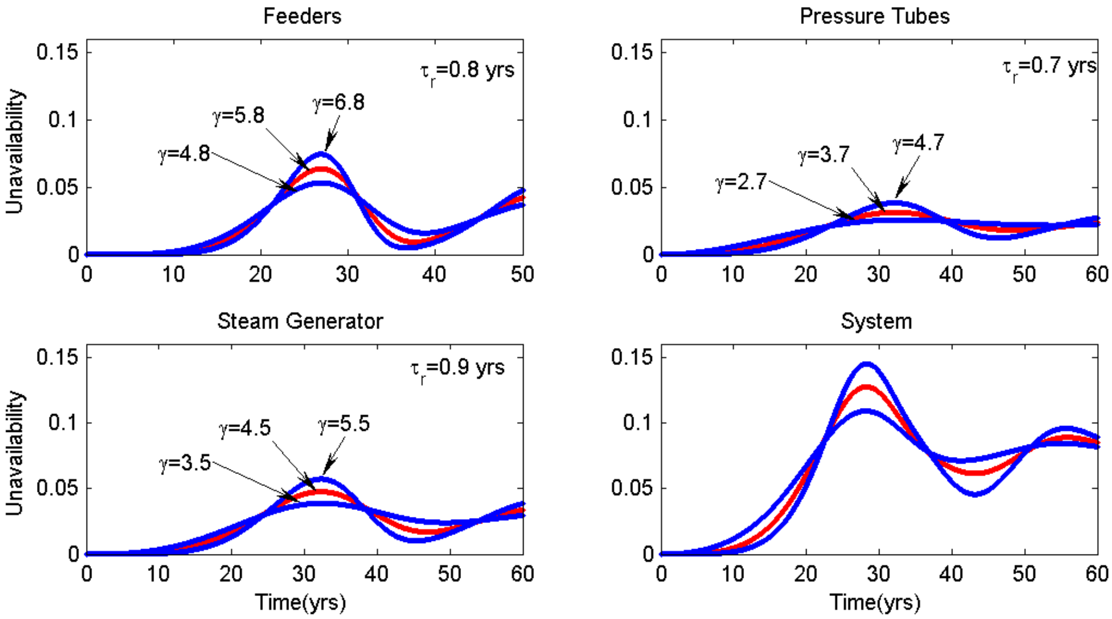


Figure 6.14: Unavailability plot - Effect of ageing.

is plotted in Figure 6.13. The plots show highest unavailability around the mean life time of the respective elements. The unavailability decreases gradually later on due to repair. When the repair time is lesser, the unavailability after the restoration is lesser before the next failure shows its influence. Hence a total availability of one is not witnessed over time after the first failure. The system plot shows multiple dips of high unavailability during a span of 60 years corresponding to the failures of the elements of the system. In all, it can be said that the higher availability is a function of lower failure rates and lesser repair times.

The effect of aging while keeping the mean time to failure and the repair time constant is seen in Figure 6.14. In this plot, only the variability in the time to failure is manipulated. As a result, a decreased coefficient of variation leads to an increased shape parameter of the Weibull failure distribution. As seen in the plots, increasing the shape parameter γ results in increased peak unavailability of the components and of the entire system.

The reader is reminded again the fact that this application considers non-exponential failure distributions for the elements allowing way to more realistic time-dependent availability of the heat transport system while eliminating the state explosion problem faced by the semi-Markov technique.

6.6 Conclusion

This chapter has brought together the versatility of semi-Markov process and the flexibility of UGF technique in eliminating the problem of dimension damnation. The proposed approach is useful in estimating the time-dependent availability of nuclear power plant systems. By eliminating the need for dropping off certain states or merging a few of them for computational ease, the UGF method manages to modularize the entire system in to a set of semi-Markov models. This method requires that subsystems be identified and represented in a polynomial form. However, subsystems are hard to be identified programmatically often requiring expert intervention.

Chapter 7

Conclusions and Recommendations

7.1 Conclusions

Within the framework of multi-state system reliability for nuclear power systems, the current research focused on the following major topics:

1. The applicability of Markov process model for relatively medium scale systems with finite number of states in continuous time.
2. Improving the existing Markov models in the nuclear industry to accommodate non-exponential failure time distribution using semi-Markov models on small scale systems.
3. Application of the developed methodology to nuclear plant systems such as Nuclear Component Cooling Water (NCCW) system, nuclear piping system, tail-gas system, Pressurized Heat Transport System (PHTS) and Digital Instrumentation and Control (I&C) system.

Semi-Markov process model is identified as a potential tool in analyzing small to medium sized reliability block diagrams or system degradation problems. The results of the analysis mainly are the system failure probability and system hazard rate. These results can be incorporated in to a larger fault tree model as part of a probabilistic safety assessment project. Semi-Markov process model is preferable when at least one of the components of a system is non-repairable leading to an analysis of first failure of the system. In case of a degradation problem, the gradual degradation usually leads to an irrecoverable system failure. These two categories were explored in the present study. In the Nuclear Component Cooling Water (NCCW) system, the heat exchanger was a non-repairable component. A Monte Carlo simulation of this system validated the results of the semi-Markov process model. A second case study considered was the degradation of the nuclear piping system. In an attempt, a hypothetical system was considered with two redundant subsystems assuming all the components were repairable. The semi-Markov formulation of this problem with individual model for each subsystem failed to yield known standard results and the reason was found to be a limitation of the model to take in to consideration non-regenerative points in the presence of non-exponential failure time distribution. Moreover, mainstream asset failure analysis professionals in the industry today view semi-Markov process model as either useful, but too complex or as a tool that cannot handle complexities such as spares, inspections, repair crews etc. or as a tool that is too complex for practical requirements. With practical applications and illustrative examples, this thesis hopes to bring the audience at ease with the more sophisticated semi-Markov process model.

7.2 Research Contributions

The key contribution of the thesis is to explore and formulate various applications of the semi-Markov process model for the multi-state reliability analysis of nuclear power plant systems. Most applications are semi-Markov extensions of existing Markov models. A brief technique to reduce the number of states in a semi-Markov model leading to closed form solutions under competing risk conditions avoiding intensive computations was described in Veeramany and Pandey (2011b).

The following practical applications were considered during the course of the research:

1. Reliability analysis of nuclear piping system (Veeramany and Pandey, 2011c).

2. Reliability analysis of nuclear component cooling water system(Veeramany and Pandey, 2011b).

3. Reliability analysis of digital instrumentation and control systems(Veeramany and Pandey, 2011a).

4. Quantifying the effects of maintenance on unavailability of systems (Submitted to Nuclear Engineering and Design on January 25, 2012).
5. Semi-Markov model of fire growth (Submitted to Fire Technology on June 1, 2012).
6. Availability analysis of practical systems (Veeramany and Pandey, 2010a).
7. Availability Analysis of Systems with Multi-State Components (Veeramany and Pandey, 2010b).
8. Substation reliability and cost analysis.
9. Availability analysis of heat transport system.

In summary, the semi-Markov process model provides a framework for analyzing reliability block diagrams and degradation characteristics of multi-state systems. It can be considered as an alternative to Monte Carlo simulations and Markov models for better accuracy in reliability predictions.

7.3 Recommendations for future research

1. Imperfect repair, common cause failure and ageing

   All throughout the thesis, it has been assumed that at the conclusion of a repair, the component is returned to an 'as good as new condition'. This means that the age of the component is returned to time equals zero. However, this may not always be the case. In fact, the age of the component after the repair may be a percentage of its age at the time when the repair took place. This kind of a repair is called an imperfect repair. A provision to incorporate this imperfection in the models is recommended.

   Yet another feature that accelerates system failures is the common cause failure (CCF) and is considered significant in real world situations. There are a few CCF models already available in the literature. One or more of these can be adapted to be included in a semi-Markov model of redundant systems.

   The above two features at large determine how distinctly ageing characteristics are observed in a system that has been put in to service for a long time. For systems with rare events and slow ageing, it is desirable to use truncated statistical distributions to shift the view toward particular period of time in the system's life rather than observing it from the time of installation.

2. Risk analysis
   Reliability analysis is of no use to a decision or policy maker if the risk component is missing in the analysis of a system. Risk analysis for a Markov model can be achieved using the Markov reward model. An extension of this model is the semi-Markov reward model. Hence, future research on risk analysis of nuclear power plant systems could focus on cost models based on the concept of rewards in conjunction with non-exponential failure time distributions as holding times in a semi-Markov analysis.

3. Fault Tree Analysis
   Static fault trees have been extensively used in the industry for over half a century. The recent years have witnessed an increasing interest in dynamic fault tree (DFT) and dynamic reliability block diagram (DRBD). These representations have introduced new symbols to consider interaction between subsystems. Developing semi-Markov models equivalent to these advanced representations is possibly yet another area of exclusive focus.

Appendix A

An algorithm to solve Markov-Renewal Equation

In this appendix, an algorithm derived by Nunn and Desiderio(1977) based on the trapezoidal rule for solving the Markov-renewal Equation 3.9 by numerical integration is listed.

Equation 3.9 is solved by finding $\phi(t)$ on a set of equally spaced points in time. The time points are denoted t_0,t_1 , ..., t_m . The step size, i.e., the interval between the time points, is denoted Δt. The time points can be represented as: $t_n = \Delta t * n$, $0 \leq n \leq m$. With $\phi_{ij}(0) = \delta_{ij}$ the solution for t_n, n > 0, is now desired.

For convenience, Equation 3.9 is rewritten in matrix notation as:

$$\phi(t_n) = W(t_n) + \int_{0}^{t_n} H(\tau)\phi(t_n - \tau)d\tau \tag{A.1}$$

where

$$\phi(t_n) = \{\phi_{ij}(t_n)\}$$
$$H(t_n) = \{h_{ij}(t_n)\}$$

and $W(t_n)$ is the diagonal matrix with elements $W_i(t)$ down the diagonal and zeros elsewhere. It is observed that when $\tau = 0$, the argument of ϕ in the integrand is the same as that of ϕ on the left of the equation. To capitalize on this, Equation

A.1 is rewritten as follows:

$$\phi(t_n) = W(t_n) + \int_0^{t_1} H(\tau)\phi(t_n - \tau)d\tau + \int_{t_1}^{t_n} H(\tau)\phi(t_n - \tau)d\tau \qquad \text{(A.-1)}$$

Equation A.-1 is evaluated using the trapezoidal integration rule, i.e.,

$$\int_{x_1}^{x_2} f(y)dy = \frac{\Delta x}{2}[f(x_1) + f(x_2)] - \frac{(\Delta x)^3}{12} f''(\xi), (x_1 < \xi < x_2) \qquad \text{(A.0)}$$

where x_1 and x_2 are separated by an interval Δx, $f(.)$ is the function to be integrated, and the last term on the right is the error term. Applying equation A.0 without the error term produces:

$$\begin{aligned} \phi(t_n) &= W(t_n) + \frac{\Delta t}{2}[H(0)\phi(t_n) + H(t_1)\phi(t_n - t_1)] \\ &\quad + \Delta t \sum_{k=1}^{n} H(t_k)\phi(t_n - t_k) \\ &\quad - \frac{\Delta t}{2}[H(t_1)\phi(t_n - t_1) + H(t_n)\phi(0)] \qquad \text{(A.-1)} \end{aligned}$$

where $H(0) = H(t_0)$ has been used. Solving for $\phi(t_n)$ produces:

$$\phi(t_n) = [I - \frac{\Delta t}{2}H(0)]^{-1}[W(t_n) + \Delta t \sum_{k=1}^{n} H(t_k)\phi(t_n - t_k) - \frac{\Delta t}{2}H(t_n)\phi(0)] \quad \text{(A.0)}$$

This equation is the basic recursive scheme used numerically to produce the solution of Equation 3.9 on the points t_n , $1 \leq$ n $\leq$ m. The solution is started with $\phi(0) =$ W(0) $= I$, and the solution for $\phi(t)$ is gotten by applying equation (A-5), etc. In this way, the solution of Equation A.0 for any finite t_n is produced. The matrix $[I - \frac{\Delta t}{2}H(0)]$ in Equation A.0 need be inverted only once at the start of the numerical scheme. If the transition matrix $H(t)$ contains only density functions that are zero at time zero, no inversion is required. The transition matrix should contain only density functions that are continuous in the time interval of interest. Discontinuous density functions may cause large numerical inaccuracies in the numerical scheme.

At each step, the solution of Equation A.0 must satisfy the following condition:

$$\sum_{j=1}^{N} \phi_{ij}(t_n) \approx 1 \quad 1 \leq \text{i} \leq \text{N}. \tag{A.1}$$

This condition serves to check on both the numerical accuracy and stability of the solution. The relative numerical accuracy of the iterative scheme is one order of magnitude less than the numerical accuracy of the trapezoidal integration rule. This occurs because of the compounding of numerical errors in the iterative scheme. The relative error for the trapezoidal rule is given by:

$$R = \frac{(\Delta x)^3 f''(\xi)}{12 f(\xi)} \tag{A.2}$$

where $f(.)$ is the function being integrated.

Appendix B

COV vs. Weibull Shape Parameter Mapping

The expression for *cov* of the Weibull distribution can be given solely in terms of its shape parameter γ:

$$cov = \sqrt{\frac{\Gamma(1+\frac{2}{\gamma})}{\Gamma(1+\frac{1}{\gamma})} - 1}$$

By systematically varying γ values, a mapping between *cov* and the shape parameter can be generated as shown in the Table below.

Table B.1: Relation between *cov* and Weibull shape parameter

cov	Shape (γ)	*cov*	Shape (γ)	*cov*	Shape (γ)
0.2	5.797715	0.65	1.57291	1.1	0.910337
0.25	4.542412	0.7	1.451286	1.15	0.872159
0.3	3.713909	0.75	1.34757	1.2	0.837618
0.35	3.128894	0.8	1.258265	1.25	0.806239
0.4	2.695696	0.85	1.18071	1.3	0.777624
0.45	2.363383	0.9	1.11284	1.35	0.751436
0.5	2.101395	0.95	1.053036	1.4	0.727389
0.55	1.8903	1	1	1.45	0.705239
0.6	1.717114	1.05	0.952724		

Appendix C

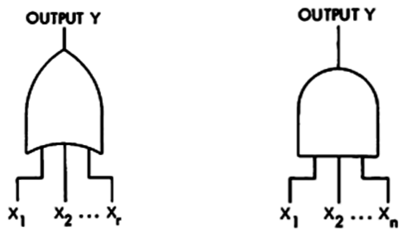
Fault Trees and Reliability Block diagrams

C.1 Introduction

A system is a complex of subsystems (components) and when these subsystems are put together to form an overall system, failure modes may appear that are not at all obvious when viewed from the standpoint of the separate components.

In system reliability analysis, a fault tree is a graphical representation of the logic that relates certain specific events or primary failures to an ultimate undesired event through a deductive failure analysis. This undesired event constitutes the top event in a fault tree diagram, for example, a switch fails to make contact. A fault tree does not model all possible system failures. It is tailored to design the top event and hence includes only those faults that contribute to the top event.

A fault tree analysis is an analytical technique where an undesirable state of the system is specified and then analyzed to find all ways in which the undesired event can occur. The initiating fault events that lead to the top event are called basic events. Logic gates like AND-gate and OR-gate are used to bind these basic events needed for the occurrence of the output events. The basic initiating events are called "failures" and the events resulting from the inter-relationship of the basic events are called "faults". The OR-gate is used to show that the occurrence of one or more of the basic basic events leads to the output event. Inputs to an OR-gate are identical to the output but are more specifically defined to a cause. The AND-gate is used when output fault occurs only if all the input faults occur. Both these



(a) OR Gate (b) AND Gate

Figure C.1: Gates used in a fault tree (a) OR Gate(b) AND Gate

gates can take any number of input faults. There are a few other gates available for fault tree modelling which are basically special cases of these two basic types.

Consider two components A and B in series such that the failure of either of these results in an output fault. Given the probabilities of failures of each of these components, the probability of the fault output is given by the addition rule:

$$P(A \text{ or } B) = P(A) + P(B) - P(A \text{ and } B)$$

Usually, the possibility of the simultaneous occurrence of any two events is ignored. Such a situation is called a 'rare event occurrence'. Hence the addition rule reduces to

$$P(A \text{ or } B) = P(A) + P(B)$$

This union rule can be extended to more than two events and is associated with the OR-gate in a fault tree.

If two components are connected in parallel and isolated from one another, the failure of one does not affect the failure of the other. The failures of these components are assumed to be independent events. For two independent events A and B, the probability that both the events A and B occur is given by the multiplication rule:

$$P(A \text{ and } B \text{ both occur}) = P(A)P(B)$$

C.2 Common Cause Failures (CCF)

Failure of multiple components due to a common cause called the *common cause failure* represents one of the most important issues in evaluation of system reliability or unavailability. The frequency of such events has relatively low expectancy, when compared to random failures, which affect individual components. However, in many cases the consequence is a direct loss of safety system or mitigative safety function. The basic events caused due to a common cause are called *common-mode events* of the cause. For example, lightning could be a common cause and the failure of redundant valves in a cooling system could be common-mode event. Other examples of common cause are impact, stress, vibration, temperature, manufacturer etc. In a fault tree, a common cause failure can be represented by mirroring a basic event for all the components failing due to a common cause. For example, Figure C.2 shows a two component redundant system susceptible to a common cause (Vrbanić et al., 2003).

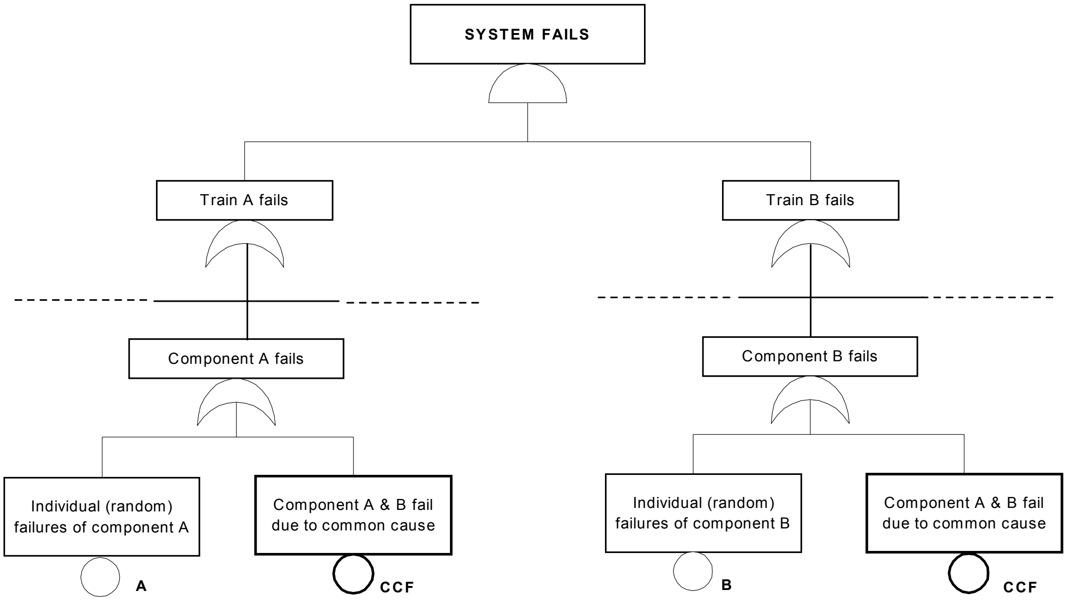

SYSTEM FAILS
Train A fails
Train B fails
Component A fails
Component B fails
Individual (random) failures of component A
Component A & B fail due to common cause
Individual (random) failures of component B
Component A & B fail due to common cause
A
CCF
B
CCF

Figure C.2: Cut set example

A *dependent event* is an event whose probability in a group of events cannot be expressed as simple product of unconditional probability of failure. Recall that if any two events A and B are independent then,

$$P(A|B) = P(A)$$

where as if A is indeed dependent on B, then

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Common cause failures can be categorized under the general class of dependent events and show up in the design of redundant systems. These lead to outage of multiple components caused by a single undesired event, for example, outage of all components due to a common electrical supply failure. *Cascade failures* are another class of dependent events that do not affect redundant components. Failure of one component leads to the failure of another and the chain of failures continues like a cascading waterfall.

C.2.1 $\beta - factor$ model

The $\beta - factor$ model (Fleming, 1974) expresses the correlation between the independent random component failures and common cause failures in a redundant system. Let λ be the failure rate of the component such that

$$\lambda = \lambda_i + \lambda_{CCF}$$

where λ_i is the independent failure rate and λ_{CCF} is the failure rate due to common cause. Define $\beta - factor$ as the ratio of λ_{CCF} to λ:

$$\beta = \frac{\lambda_{CCF}}{\lambda}$$

so that

$$\lambda_{CCF} = \beta\lambda$$

and

$$\begin{aligned}\lambda_i &= \lambda - \lambda_{CCF} \\ &= \lambda(1 - \beta)\end{aligned}$$

i.e., both the independent failure rate and the common cause failure rate are expressed as a function of the component's failure rate. β lies between 0 and 1. In the field of power transmission it is found that the β value averages between 0 and 25% (Borcsok and Holub, 2008).

C.3 Cut sets

A *cut set* of a system is defined as a set of system components, which when failed, causes failure of the system (Billinton and Allan, 1992). In other words, a cut set is collection of basic events; if all these basic events occur, the top event is guaranteed to occur (Henley and Kumamoto, 1980).

A cut set of size n has n basic events in it and is called an $n-$ *event cut set*. Cut sets with a single event significantly contribute to the top-event. The only exception is when this one-event has a very small probability of occurrence.

C.3.1 Example

Consider the fault tree in Figure C.3. The basic events in this example are D, E, F and G. The top event A occurs if both D and E occur and one of F and G occur. Hence the cut sets are

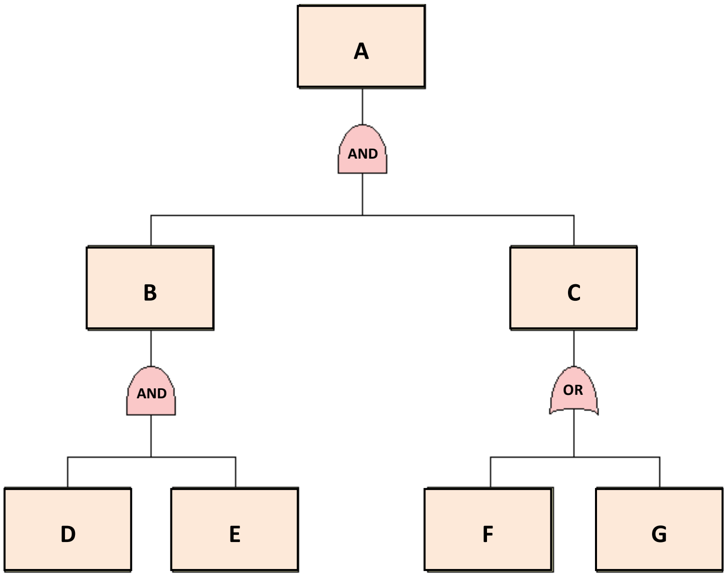


Figure C.3: Cut set example

$$\{D, E, F\}, \{D, E, G\}, \{D, E, F, G\}$$

A *minimal cut* set of a system is also a cut set such that removal of any event from it does not cause the system to fail.

In this example removing either of event F or G from the cut set $\{D, E, F, G\}$still leads to system failure. Hence it is not a minimal one. Also note that this cut set is a superset of the other two cut sets. However, the other two cut sets are minimal since removal of any of F, G does not lead to the top event.

C.3.2 Computer codes

If the occurrence of one event prevents another event from occurring, then these events are called mutually exclusive events. In the absence of such events, a computer program called MOCUS (Fussel et al., 1974) was developed to obtain minimal cut sets from fault trees. It was based on the fact that OR gates increase the number of cut sets and AND gates increase the size of the cut set.

The common cause failure cut sets can be derived from the set of minimal cut sets of a fault tree. Minimal cut sets may contain events from components sharing a common location or a common link. Components share a common location if no barrier insulates any one of them from the common cause. A common link is a dependency among components which cannot be removed by a physical barrier (e.g., a common energy source or common maintenance instructions). Presence of duplicate minimal cut sets identifies a common cause failure. The COMCAN fault tree analysis codes (Burdick et al., 1976) were designed to analyze complex systems, such as nuclear plants for common causes of failure.

The CAFTA software owned by Electric Power Research Institute (EPRI), USA is used widely by US and international nuclear power plants. It is an integrated tool part of the EPRI risk and reliability suite of products providing four main programs - fault tree editor, a reliability database editor, a cutset editor and an event tree editor.

C.4 Reliability Block Diagrams

A reliability block diagram is a success-oriented network describing the function of the system. It is suitable for systems of non-repairable components and where the order in which failures occur does not matter. Each element of the system is represented by a block and a label identifies it. Given a vector $\boldsymbol{x}$ consisting of the state of each of the elements, the state of the system is obtained by evaluating the structure function $\phi(\boldsymbol{x})$:

1. **Series Structure** A system functions if and only if all of its n elements are functional.

$$\phi(\boldsymbol{x}) = x_1.x_2...x_n = \prod_{i=1}^{n} x_i$$

2. **Parallel Structure** A system functions if at least one of its elements is functional.

$$\phi(\boldsymbol{x}) = 1 - (1 - x_1)(1 - x_2)...(1 - x_n) = 1 - \prod_{i=1}^{n}(1 - x_n)$$

The failure rate and mean time to failure of simple series and parallel systems are given by:

$$\begin{aligned}
\lambda_{series} &= \sum_{i=1}^{n} \lambda_i \\
MTTF_{series} &= \frac{1}{\sum_{i=1}^{n} \lambda_i} \\
MTTF_{parallel} &= \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}
\end{aligned}$$

Let $R_A(t)$ and $R_B(t)$ be the reliability of the components A and B respectively. Then the unreliability of a series system $Q_s(t)$ is the unreliability of at least one of the components:

$$Q_s(t) = 1 - R_A(t)R_B(t)$$

Let $Q_A(t)$ and $Q_B(t)$ be the unreliability of the components A and B respectively. Then the unreliability of a parallel system $Q_p(t)$ is the unreliability of both the components:

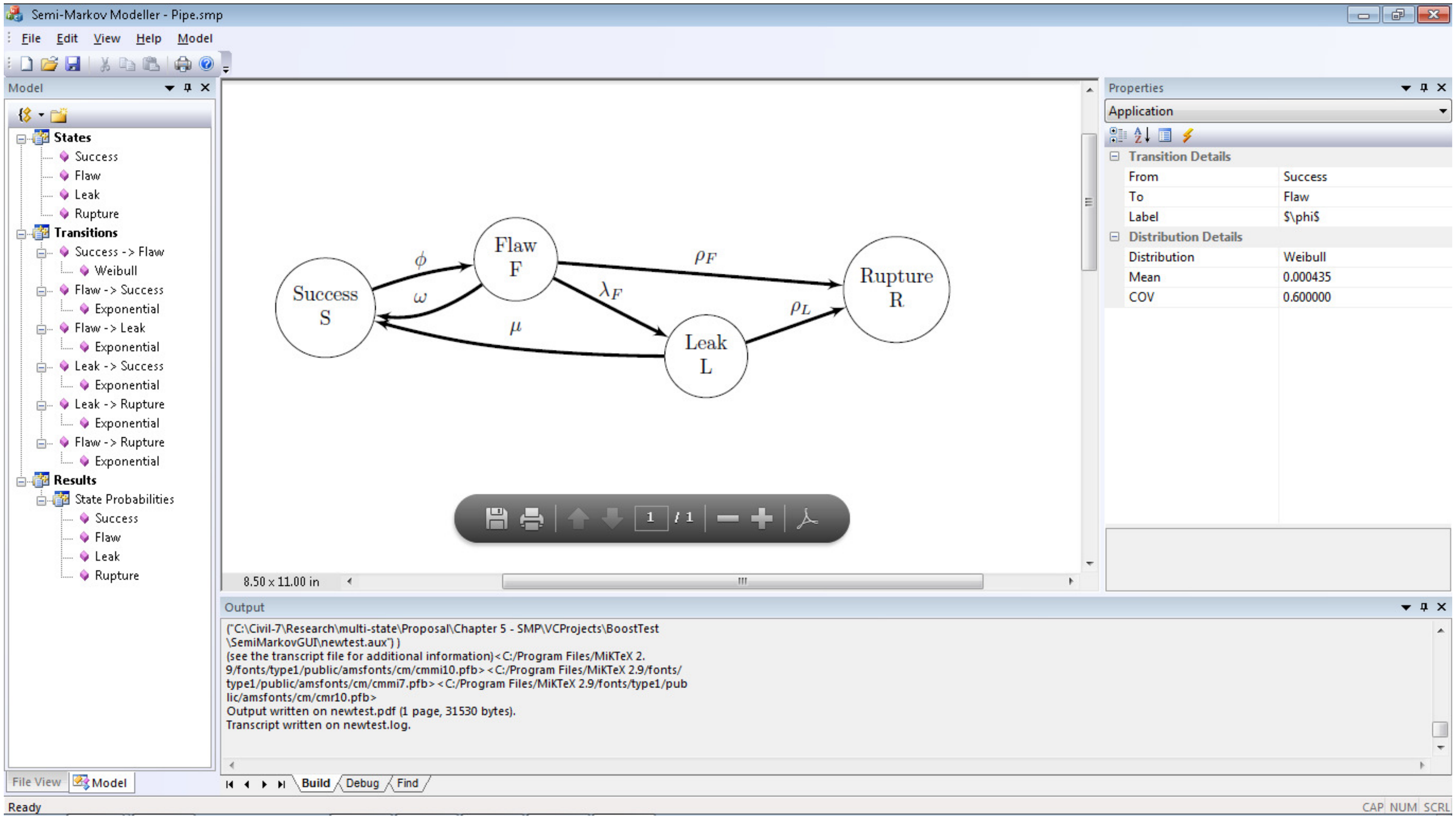
$$Q_p(t) = Q_A(t)Q_B(t)$$

$1 - Q_s(t)$ and $1 - Q_p(t)$ produce the reliability of the series and parallel systems respectively.

Appendix D

Semi-Markov Modeller

The models in this thesis have been developed using the ‘Semi-Markov Modeller’ software. The tool has been developed as an integrated modelling environment (IME) to build, manage, execute and visualize Markov and semi-Markov models. The models are saved with an extension of .smp and displayed as acrobat reader files (pdf) using the GraphViz graph visualization software. State and transition labels can be enclosed in ‘$’ to display mathematical symbols supported by the MiKTeX pdfTeX system. The high quality pdf output can either be embedded as is in a technical report or can be further customized using freely available GraphViz dot language editors. The state probabilities are saved as tab delimited plain text files and can be opened in Matlab for customized plotting though the software itself provides basic plotting of the results. The tool supports a number of commonly used statistical distributions in engineering including exponential, Weibull and lognormal distributions. Figure D.1 shows a snapshot of the software package while the piping system model was under development.



Transition Details

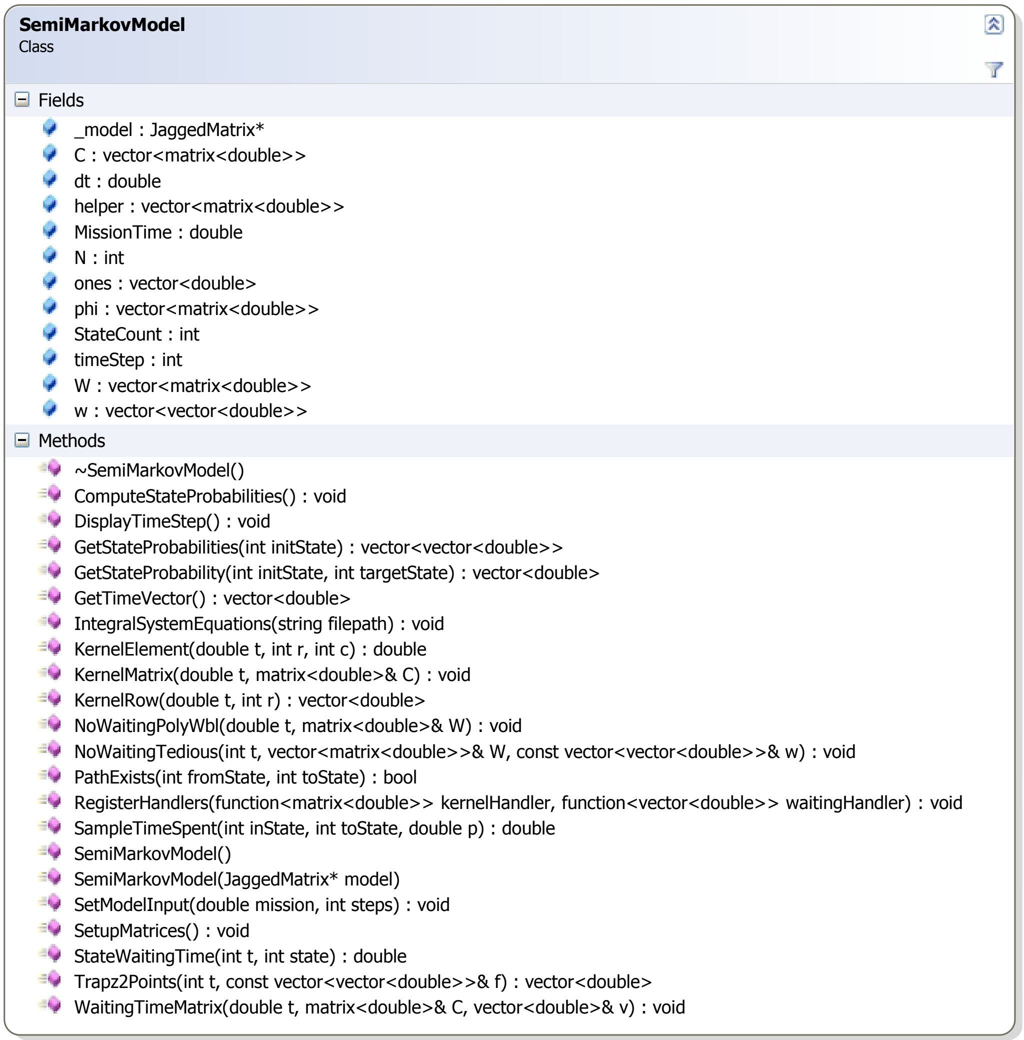
From	Success
To	Flaw
Label	ϕ

Distribution Details

Distribution	Weibull
Mean	0.000435
COV	0.600000

```
("C:\Civil-7\Research\multi-state\Proposal\Chapter 5 - SMP\VCProjects\BoostTest
\SemiMarkovGUI\newtest.aux") )
(see the transcript file for additional information)<C:/Program Files/MiKTeX 2.
9/fonts/type1/public/amsfonts/cm/cmmi10.pfb><C:/Program Files/MiKTeX 2.9/fonts/
type1/public/amsfonts/cm/cmmi7.pfb><C:/Program Files/MiKTeX 2.9/fonts/type1/pub
lic/amsfonts/cm/cmr10.pfb>
Output written on newtest.pdf (1 page, 31530 bytes).
Transcript written on newtest.log.
```

Figure D.1: Semi-Markov Modeller



SemiMarkovModel
Class

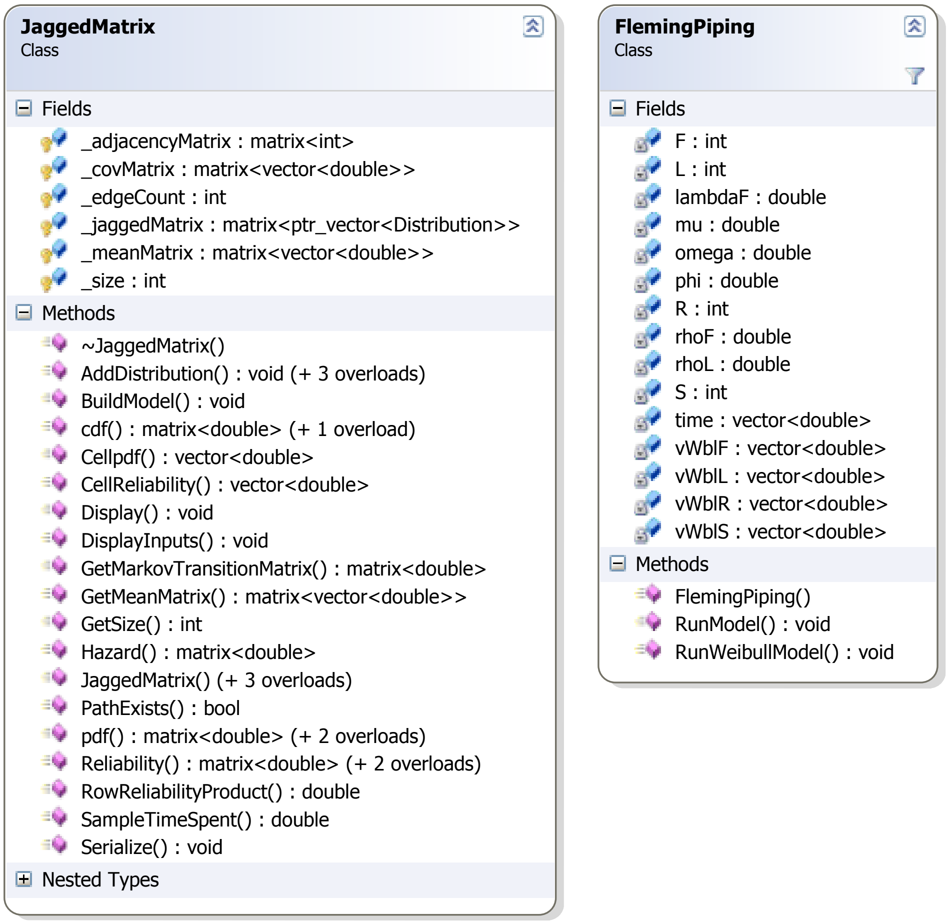
Fields

```
_model : JaggedMatrix*
C : vector<matrix<double>>
dt : double
helper : vector<matrix<double>>
MissionTime : double
N : int
ones : vector<double>
phi : vector<matrix<double>>
StateCount : int
timeStep : int
W : vector<matrix<double>>
w : vector<vector<double>>
```

Methods

```
~SemiMarkovModel()
ComputeStateProbabilities() : void
DisplayTimeStep() : void
GetStateProbabilities(int initState) : vector<vector<double>>
GetStateProbability(int initState, int targetState) : vector<double>
GetTimeVector() : vector<double>
IntegralSystemEquations(string filepath) : void
KernelElement(double t, int r, int c) : double
KernelMatrix(double t, matrix<double>& C) : void
KernelRow(double t, int r) : vector<double>
NoWaitingPolyWbl(double t, matrix<double>& W) : void
NoWaitingTedious(int t, vector<matrix<double>>& W, const vector<vector<double>>& w) : void
PathExists(int fromState, int toState) : bool
RegisterHandlers(function<matrix<double>> kernelHandler, function<vector<double>> waitingHandler) : void
SampleTimeSpent(int inState, int toState, double p) : double
SemiMarkovModel()
SemiMarkovModel(JaggedMatrix* model)
SetModelInput(double mission, int steps) : void
SetupMatrices() : void
StateWaitingTime(int t, int state) : double
Trapz2Points(int t, const vector<vector<double>>& f) : vector<double>
WaitingTimeMatrix(double t, matrix<double>& C, vector<double>& v) : void
```

Figure D.2: Class SemiMarkovModel



JaggedMatrix
Class

Fields
- _adjacencyMatrix : matrix<int>
- _covMatrix : matrix<vector<double>>
- _edgeCount : int
- _jaggedMatrix : matrix<ptr_vector<Distribution>>
- _meanMatrix : matrix<vector<double>>
- _size : int

Methods
- ~JaggedMatrix()
- AddDistribution() : void (+ 3 overloads)
- BuildModel() : void
- cdf() : matrix<double> (+ 1 overload)
- Cellpdf() : vector<double>
- CellReliability() : vector<double>
- Display() : void
- DisplayInputs() : void
- GetMarkovTransitionMatrix() : matrix<double>
- GetMeanMatrix() : matrix<vector<double>>
- GetSize() : int
- Hazard() : matrix<double>
- JaggedMatrix() (+ 3 overloads)
- PathExists() : bool
- pdf() : matrix<double> (+ 2 overloads)
- Reliability() : matrix<double> (+ 2 overloads)
- RowReliabilityProduct() : double
- SampleTimeSpent() : double
- Serialize() : void

Nested Types

FlemingPiping
Class

Fields
- F : int
- L : int
- lambdaF : double
- mu : double
- omega : double
- phi : double
- R : int
- rhoF : double
- rhoL : double
- S : int
- time : vector<double>
- vWblF : vector<double>
- vWblL : vector<double>
- vWblR : vector<double>
- vWblS : vector<double>

Methods
- FlemingPiping()
- RunModel() : void
- RunWeibullModel() : void

Figure D.3: Supporting and Application Classes.

Appendix E

Glossary

Absorbing state An absorbing state is a state from which there is a zero probability of exiting. An absorbing Markov system is a Markov system that contains at least one absorbing state.

Ageing system If the failure rate function $\lambda(t)$ increases with age, we have an ageing system (component) that deteriorates (fails more often) with age. If the failure rate is constant in time, we have a non-ageing system.

Availability Availability represents the probability that the system is capable of conducting its required function when it is called upon given that it is not failed or undergoing a repair action.

Common Cause Failure A common cause failure is a single, shared event that adversely affects two or more components at the same time. When the consequences of the event include the occurrence of an accident sequence initiating event, the event is called a common cause initiating event.

Competing risk Given the current state, if a process has to choose from more than one state for the next transition, then the process is said to be in a competing risk situation.

Cumulative Distribution Function (CDF) The CDF $F_X(x)$ of a random variable X represents the probability that X takes on a value less than or equal to x.

Extended RBD For multi-state components which have to be connected in a particular order, an extended RBD embeds a Markov or a semi-Markov space diagram with in it.

Failure rate function The failure rate of a component is the conditional probability of failure given that it has not already failed. $\lambda(t) = \frac{f(t)}{R(t)}$

Fault tree In reliability and systems analysis, a fault tree is a graphical representation of the logic that relates certain specific events or primary failures to an ultimate undesired event through a deductive failure analysis.

Fault Tree Top Event A fault tree top event is the event at the very top of the fault tree, sometimes referred to as the undesired event, for which the fault tree determines the causes.

Heat Transport System The heat transport system (HTS) circulates pressurized D_20 coolant through the fuel channels to remove the heat produced by fission in the nuclear fuel. The coolant transports the heat to steam generators, where it is transferred to light water to produce steam to drive the turbine.

Holding time (semi-Markov) Let the process be in state i. After the successor state j has been selected and before making a transition from i to j,the process holds for a time t_{ij} in state i. t_{ij} is a random variable called the holding time.

Homogeneous Markov model Given the past state of the process, the probability of entering the present state is the same no matter at what time the arrival in to the present state occurs.
$Pr(X_{n+1} = x|X_n = y) = Pr(X_n = x|X_{n-1} = y)$

Initiating event frequency An event that creates a disturbance in the plant having the potential to lead to core damage, depending on the successful operation of required mitigating systems in the plant is called an initiating event. The number of such events occurring in a unit time is called the initiating event frequency.

Markov process A Markov process or Markov chain is a system that can be in one of several states, and can pass from one state to another each time step according to fixed probabilities satisfying the Markov property.

Markov property Given the present state, the future and past states are independent.
$Pr(X_{n+1} = x|X_n = x_n, ..., X_1 = x_1)$= $Pr(X_{n+1} = x|X_n = x_n)$ The description of the present state fully captures all the information that could influence the future evolution of the process. Future states will be reached through a probabilistic process instead of a deterministic one.

Mission Time The mission time is the time that a system or component is required to operate in order to successfully perform its function.

NCCW system In nuclear power plants, Nuclear Component Cooling Water (NCCW) systems are typically used for removing heat (cooling) systems containing potentially radioactive fluids. These systems are, in turn, then cooled by the ultimate cooling system - river, lake, sea, or ocean water.The NCCW system consists of two parallel pump trains connected in series with a heat exchanger train.

NDE Non-destructive examination is an industrial technique to collect characteristics of a system without subjecting it to permanent damage.

Probability Density Function (PDF) The PDF $f_X(x)$ of a random variable X represents the probability that X takes on a value equal to x.

Probabilistic Safety Assessment (PSA) PSA is a quantitative assessment of the risk associated with plant operation and maintenance. The risk is measured in terms of the frequency of occurrence of different events, including severe core damage.

Reliability Reliability represents the probability of components, parts and systems to perform their required functions for a desired period of time without failure in specified environments with a desired confidence.

Reliability Block Diagram (RBD) A reliability block diagram is a success-oriented network diagram describing the function of the system. It is suitable for systems of non-repairable components and where the order in which failures occur does not matter.

Semi-Markov kernel The matrix $H = \{p_{ij}h_{ij}(t)\}$ is called the kernel or core of the semi-Markov process. Here, p_{ij} are the transition probabilities and h_{ij} are the time spent in state j given that the process initially started in state i. If the transition probabilities are not known, they are replaced by an equivalent competing risk formulation. The kernel totally characterizes the statistical time behavior of the semi-Markov process.

Semi-Markov process Like a Markov process, a semi-Markov process (SMP) also has a set of states and the transitions between them are governed by a transition probability matrix. However, in a semi-Markov process, the time spent in any state after entering it is a random variable which can be described by a non-exponential distribution as well.

State transition diagram A Markov process can be illustrated by means of a state transition diagram, which is a diagram showing all the states and transition rates.

Static and dynamic fault tree A fault tree in which the system failure is insensitive to the order of occurrence of component fault events is called a static fault tree. Dynamic fault trees are a superset of traditional (static) fault trees in that additional gates are used to model sequential behavior.

u-function A u-function is essentially a polynomial in random variable z and it relates possible values of z with the corresponding probabilities. Each element j with k_j states is represented as a u-function.The coefficients of z are time-dependent conditional state probabilities of the element j obtained by modeling the element as a semi-Markov process. The exponent of z can be any arbitrary mathematical object representing the performance or state in which the element is currently in.

Waiting time (semi-Markov) A waiting time t_i in a state i is a holding time where the successor of the state i is not known i.e. an unconditional holding time is called a waiting time.

Bibliography

A. N. Ajah, P. M. Herder, J. Grievink, and M. P. C. Weijnen. Hierarchical markov reliability/availability models for energy and industrial infrastructure systems conceptual design. *Computer aided chemical engineering*, 21(PART B):1753–1758, 2006. 10

A. W. Al-Dabbagh and L. Lu. Reliability modeling of networked control systems using dynamic flowgraph methodology. *Reliability Engineering & System Safety*, 95(11):1202 – 1209, 2010. 2, 144

T. Aldemir, D.W. Miller, M.P. Stovsky, J. Kirschenbaum, P. Bucci, A. W. Fentiman, and L.A. Mangan. NUREG/CR-6901: Current state of reliability modeling methodologies for digital Systems and their acceptance criteria for Nuclear power plant assessments. Technical report, Washington, DC, US Nuclear Regulatory Commission, 2006. 143

T. Aldemir, M.P. Stovsky, J. Kirschenbaum, D. Mandelli, , P. Bucci, L.A. Mangan, D.W. Miller, X. Sun, E. Ekici, S. Guarro, M. Yau, B. Johnson, C. Elks, and S.A. Arndt. NUREG/CR-6942:Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments. Technical report, Washington, DC, US Nuclear Regulatory Commission, 2007. 2, 144, 147, 148

T. Aldemir, S. Guarro, D. Mandelli, J. Kirschenbaum, L.A. Mangan, P. Bucci, M. Yau, E. Ekici, D.W. Miller, X. Sun, and S.A. Arndt. Probabilistic risk assessment modeling of digital instrumentation and control systems using two dynamic methodologies. *Reliability Engineering & System Safety*, 95(10):1011 – 1039, 2010. xv, xix, 144, 145, 146, 147, 148, 150

S. S. Arshi, M. Nematollahi, and K. Sepanloo. Coupling cfast fire modeling and saphire probabilistic assessment software for internal fire safety evaluation of a typical triga research reactor. *Reliability Engineering & System Safety*, 95(3):166 – 172, 2010. ISSN 0951-8320. 126

S. Kui Au, Z. Wang, and S. Lo. Compartment fire risk analysis by advanced monte carlo simulation. *Engineering Structures*, 29(9):2381 – 2390, 2007. 124, 125

D. G. Austin. Some differentiation properties of markoff transition probability functions, 1956. 10

V. Babrauskas, R. D. Peacock, and P. A. Reneke. Defining flashover for fire hazard calculations: Part ii. *Fire Safety Journal*, 38(7):613 – 622, 2003. ISSN 0379-7112. 134

Suk Joo Bae, Way Kuo, and Paul H. Kvam. Degradation models and implied lifetime distributions. *Reliability Engineering and System Safety*, 92(5):601 – 608, 2007. 155

V. Barbu, M. Boussemart, and N. Limnios. Discrete-time semi-markov model for reliability and survival analysis. *Communications in Statistics - Theory and Methods*, 33(11):2833–2868, 2004. 41, 71

C. R. Barnett. Bfd curve: a new empirical model for fire compartment temperatures. *Fire Safety Journal*, 37(5):437 – 463, 2002. ISSN 0379-7112. 140

C. R. Barnett. Replacing international temperature-time curves with bfd curve. *Fire Safety Journal*, 42(4):321 – 327, 2007. ISSN 0379-7112. 140

G. N. Berlin. Managing the variability of fire behavior. *Fire Technology*, 16(4): 287–302, 1985. xiv, 125, 128, 129, 130, 131, 132, 134, 135, 137, 138, 141

Bharucha-Reid. *Elements of the Theory of Markov Processes and Their Applications*. Courier Dover Publications, 1997. ISBN 0-486-69539-5. 10

R. Billinton and R. N. Allan. *Reliability evaluation of engineering systems: concepts and techniques*. Springer, New York, USA, 1992. 213

R. Billinton and K.E. Bollinger. Transmission system reliability evaluation using markov processes. *IEEE Transactions on Power Apparatus and Systems*, PAS-87 (2):538–547, Feb. 1968. 10

R. Billinton and W. Li. *Reliability assessment of electric power systems using Monte Carlo methods*. Plenum Press, New York, USA, 1994. 97, 167, 169

R. Billinton and W. Wangdee. Delivery point reliability indices of a bulk electric system using sequential monte carlo simulation. *Power Delivery, IEEE Transactions on*, 21(1):345–352, Jan. 2006. 167

A. Birolini. *Reliability Engineering: Theory and Practice*. Springer, Berlin, 2007. 5, 7, 77

Andrei Blahoianu, Thomas Viglasky, Colin D. Moses, and Ken Kirkhope. Canadian regulatory approach to ensuring the implementation of effective ageing management programs for nuclear power plants. *Nuclear Engineering and Design*, 241 (3):548 – 554, 2011. 1

S. Bloch-Mercier. Optimal restarting distribution after repair for a markov deteriorating system. *Reliability Engineering and System Safety*, 74(2):181–191, 11 2001. 10

J. Borcsok and P. Holub. Different approaches for probability of common cause failure on demand calculations for safety integrity systems. In *IEEE/ACS International Conference on Computer Systems and Applications*, 2008. 212

H. Boudali, P. Crouzen, and M. Stoelinga. Dynamic fault tree analysis using input/output interactive markov chains. In *Dependable Systems and Networks, 2007. DSN'07. 37th Annual IEEE/IFIP International Conference on*, pages 708–717. IEEE, 2007. 2

F. Brissaud, C. Smidts, A. Barros, and C. Berenguer. Dynamic reliability of digital-based transmitters. *Reliability Engineering & System Safety*, 2011. 2

G. R. Burdick, N. H. Marshall, and J. R. Wilson. Comcan: A computer program for common cause analysis. *ANCR-1314*, 1976. 214

R.W. Butler and D. A. Bronson. Bootstrapping survival times in stochastic systems by using saddlepoint approximations. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 64(1):31–49, 2002. 34

S. Caceres and E.J. Henley. Process failure analysis by block diagrams and fault trees. *Industrial and Engineering Chemistry Fundamentals*, 15(2):128–134, 1976. 97, 105

H. Cheng and G. V. Hadjisophocleous. The modeling of fire spread in buildings by bayesian network. *Fire Safety Journal*, 44(6):901 – 908, 2009. ISSN 0379-7112. 125

F. Chiacchio, L. Compagno, D. D'Urso, G. Manno, and N. Trapani. Dynamic fault trees resolution: A conscious trade-off between analytical and simulative approaches. *Reliability Engineering & System Safety*, 2011. 2

S. Cho and J. Jiang. Analysis of surveillance test interval by markov process for sds1 in candu nuclear power plants. *Reliability Engineering and System Safety*, 93(1):1–13, 1 2008. 10

T. Chu, G. Martinez-Gurdi, A. Kuritzky, and A. Amri. International experience with modeling digital systems in psas. In *Proc. of the 10th International Probabilistic Safety Assessment & Management Conference*, Seattle, Washington, USA, 2010a. 143

G. Ciardo, R.A. Marie, B. Sericola, and K.S. Trivedi. Performability analysis using semi-markov reward processes. *IEEE Transactions on Computers*, 39(10):1251–1264, 1990. 34

E. Cinlar. *Introduction to Stochastic Processes*. Prentice-Hall Inc., Englewood Cliffs, 1975. 34

C. J. Colbourn, L. D. Nel, T. B. Boffey, and D. F. Yates. Network reliability and the probabilistic estimation of damage from fire spread. *Annals of Operations Research*, 50:173–185, 1994. ISSN 0254-5330. 124, 125, 126

Cole.W.Gulyas. Stochastic capability models for degrading satellite constellations. Master's thesis, Air force Institute of Technology, Ohio, USA, 2007. 40

P. A. Croce. A study of room fire development: the second full-scale bedroom fire test of the home fire project. Technical report, Factory Mutual Research Corporation, 1974. 134

A. Csenki. An integral equation approach to the interval reliability of systems modelled by finite semi-markov processes. *Reliability Engineering and System Safety*, 47:37–45(9), 1995. 34

G. D'Amico, J. Janssen, and R. Manca. Homogeneous semi-markov reliability models forcredit risk management. *Decisions in Economics and Finance*, 28(2): 79–93, 2006. 34

A.M.L. daSilva, J.G. Costa, and A.A. Chowdhury. Probabilistic methodologies for determining the optimal number of substation spare transformers. *IEEE Transactions on Power Systems*, 25:68–77, 2010. 113, 114

B.S. Dhillon and N. Yang. Comparisons of block diagram and markov method system reliability and mean time to failure results for constant and non-constant unit failure rates. *Microelectronics and Reliability*, 37:505–509(5), March 1997. 4

S. Distefano and A. Puliafito. Reliability and availability analysis of dependent-dynamic systems with drbds. *Reliability Engineering & System Safety*, 94(9): 1381–1393, 2009. 2

D. Drysdale. The pre-flashover compartment fire. In *An introduction to fire dynamics*. John Wiley & Sons, NY, USA, 2 edition, 1998. 134

A. El-Gohary. Estimations of parameters in a three state reliability semi-markov model. *Applied Mathematics and Computation,*, 154(2):389–403, 2004. 34

J. B. Fang. Measurements of the behavior of incidental fires in a compartment. Technical report, National Bureau of Standards, NBSIR 75-679, 1975. 134

W. Feller. Zur theorie der stochastischen prozesse. *Mathematische Annalen*, 113 (1):113–160, 1937. 9

K. N. Fleming. A reliability model for common mode failures in redundant safety systems. In *General Atomic Report, GA-13284*, Pittsburgh, PA, 1974. 212

K. N. Fleming. Markov models for evaluating risk-informed in-service inspection strategies for nuclear power plant piping systems. *Reliability Engineering and System Safety*, 83(1):27 – 45, 2004. xiv, 1, 4, 86, 87, 88, 90, 91, 92, 156

M. V. Frank and P. Moieni. A probabilistic model for flammable pool fire damage in nuclear power plants. *Reliability Engineering*, 16(2):129 – 152, 1986. ISSN 0143-8174. 126

J. B. Fussel, E. B. Henry, and N. H. Marshall. Mocus - a computer program to obtain minimal cut sets from fault trees. *ANCR-1156*, 1974. 214

L. Gámiz, M and Y. Román. Non-parametric estimation of the availability in a general repairable system. *Reliability Engineering and System Safety*, 93(8): 1188–1196, 8 2008. 35

B.J. Garrick and R.F. Christie. *Quantifying and controlling catastrophic risks.* Academic Press, MA, USA, 2008. 2

L. A. Gavrilov and N. S. Gavrilova. *Early-life factors modulating lifespan. In: Rattan, S.I.S. (Ed.). Modulating Aging and Longevity.* Kluwer Academic Publishers, Dordrecht, The Netherlands, 2003. 30

I. Gihman and A. Skohorod. *The Theory of Stochastic Processes: Vol.: 1, 2 and 3.* Springer Verlag, Berlin, 1974. 34

S.M. Gupta, N.K. Jaiswal, and L.R. Goel. Reliability analysis of a two-unit cold standby redundant system with two operating modes. *Microelectronics Reliability*, 22(4):747 – 758, 1982. 77

V. Gupta and S. Dharmaraja. Semi-markov modeling of dependability of voip network in the presence of resource degradation and security attacks. *Reliability Engineering and System Safety,*, 2011. doi:10.1016/j.ress.2011.08.003. 156

G.V. Hadjisophocleous. A model for calculating the probabilities of smoke hazard from fires in multi-storey buildings. *Journal of Fire Protection Engineering*, 4 (2):67–69, 1992. 124

B. Hagglund, R. Jansson, and B. Onnermark. Fire development in residential rooms after ignition from nuclear explosions, foa report c 20016-d6 (a3). Technical report, Forsvarets Forskningsanstalt, Stockholm, 1974. 134

A. M. Hasofer and V. R. Beck. A stochastic model for compartment fires. *Fire Safety Journal*, 28(3):207 – 225, 1997. ISSN 0379-7112. 124, 125

A. M. Hasofer and D. O. Odigie. Stochastic modelling for occupant safety in a building fire. *Fire Safety Journal*, 36(3):269 – 289, 2001. ISSN 0379-7112. 124, 125

M. Hassan and W. E. Vesely. Digital instrumentation and control systems in nuclear power plants. Technical report, Brookhaven national laboratory, NY, USA, 1998. 143

E. J. Henley and H. Kumamoto. *Reliability engineering and risk assessment.* Prentice-Hall, Englewood Cliffs, N.J., 1980. 213

A. J. M. Heselden and S. J. Melinek. The early stages of fire growth in a compartment: A co-operative research programme of the cib (commission w14). first phase. Technical report, Fire Research Station, 1975. 134

G. Heskestad. Engineering relations for fire plumes. *Fire Safety Journal*, 7(1):25 – 32, 1984. 134

S. Hostikka and O. Keski-Rahkonen. Probabilistic simulation of fire scenarios. *Nuclear Engineering and Design*, 224(3):301 – 311, 2003. ISSN 0029-5493. 126

R. A. Howard. System analysis of semi-markov processes(systems analysis of semi-markov processes, expressing results in form of matrix flow graph). *IEEE transactions on military electronics*, 8:114, 1964. 34, 37, 44

R. A. Howard. *Dynamic Probabilistic Systems, vol. 1: Markov Models*. John Wiley and Sons, Inc., New York, USA, 1971. 34, 37, 40, 44

C. Ibáñez-Llano, A. Rauzy, E. Meléndez, and F. Nieto. A reduction approach to improve the quantification of linked fault trees through binary decision diagrams. *Reliability Engineering & System Safety*, 95(12):1314–1323, 2010. 2

Idaho National Engineering Laboratory. *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE)*. Lockheed Martin Idaho Technologies Company, USA, 2010. 126

B.R. Iyer, L. Donatiello, and P. Heidelberger. Analysis of performability for stochastic models of fault-tolerant systems. *Computers, IEEE Transactions on*, C-35 (10):902–907, Oct. 1986. 34

JNES. Probabilistic safety assessment(PSA). Website, 2011. Japan Nuclear Energy Society, http://www.jnes-elearning.org/contents/tt/JNESeL-TT-003.pdf. xvi, 2

F. Joglar, F. Mowrer, and M. Modarres. A probabilistic model for fire detection with applications. *Fire Technology*, 41:151–172, 2005. 124, 125

Peter Kafka. Probabilistic risk assessment for nuclear power plants. In Krishna B. Misra, editor, *Handbook of Performability Engineering*, pages 1179–1192. Springer London, 2008. 1

D. Kancev and M. Čepin. Evaluation of risk and cost using an age-dependent unavailability modelling of test and maintenance for standby components. *Journal of Loss Prevention in the Process Industries*, 24(2):146 – 155, 2011. ISSN 0950-4230. 156

D. L. Kelly and C. L. Smith. Bayesian inference in probabilistic risk assessment-the current state of the art. *Reliability Engineering & System Safety*, 94(2):628–643, 2009. 15

D. G. Kendall. Some analytical properties of continuous stationary markov transition functions. *Transactions of the American Mathematical Society*, 78(2):529–540, 1955. 10

M.S. Khan, A. Khalique, and A. M. Abouammoh. On estimating parameters in a discrete weibull distribution. *IEEE Transactions on Reliability*, 38:348–350, 1989. 71

A. Kleyner and V. Volovoi. Application of petri nets to reliability prediction of occupant safety systems with partial detection and repair. *Reliability Engineering & System Safety*, 95(6):606 – 613, 2010. 144

A. Kolmogoroff. Über die analytischen methoden in der wahrscheinlichkeitsrechnung. *Mathematische Annalen*, 104(1):415–458, 1931. 9

A. N. Kolmogorov. On some problems concerning the differentiability of the transition-probabilities in a temporally homogeneous markov process having a denumerable set of states. *Vienye Zapiski (Matem.) Moshov. Qos. Univ.*, 148(4): 53–59, 1951. 10

V. Korolyuk and A. Swishchuk. *Semi-Markov random evolutions.* Kluwer Academic, Singapore, 1995. ISBN 0-7923-3150-8. 34

V.P. Koutras and A.N. Platis. Semi-markov availability modeling of a redundant system with partial and full rejuvenation actions. *Dependability of Computer Systems, 2008. DepCos-RELCOMEX '08. Third International Conference on*, pages 127–134, June 2008. 35

I. Kovalenko, N. Kuznetsov, and Ph. Pegg. *Mathematical Theory of Reliability of Time Dependent Systems with Practical Applications.* Wiley, Chchester, England, 1997. 34

V. G. Kulkarni. *Modeling and Analysis of Stochastic Systems.* Chapman and Hall, Madras, India, 1995. 6

D. Kumar. *Reliability maintenance and logistic support: a life cycle approach.* Springer, New York, U.S.A., 2000. 149

L. M. Laird and M. C. Brennan. *Software measurement and estimation: a practical approach.* John Wiley and Sons, NJ, U.S.A., 2006. 153

Y. Lee, J. Kim, and J. Yang. Application of the cfast zone model to the fire psa. *Nuclear Engineering and Design*, 240(10):3571 – 3576, 2010. ISSN 0029-5493. 4th International Topical Meeting on High Temperature Reactor Technology (HTR 2008), with Regular Papers. 126

N.G. Leveson. *Engineering a Safer World: Systems Thinking Applied to Safety.* MIT Press, Massachusetts, USA, 2011. 3

G. Levitin. *A new approach to solving problems of multi-state system reliability optimization.* Wiley, San Francisco, CA, 2001a. 183

G. Levitin. Incorporating common-cause failures into nonrepairable multistate series-parallel system analysis. *Reliability, IEEE Transactions on*, 50(4):380–388, Dec 2001b. 183

G. Levitin. A universal generating function approach for the analysis of multi-state systems with dependent elements. *Reliability Engineering and System Safety*, 84 (3):285–292, 6 2004. 183

G. Levitin. *The Universal Generating Function in Reliability Analysis and Optimization.* Springer, Berlin, 2005. 183

G. Levitin and A. Lisnianski. Importance and sensitivity analysis of multi-state systems using the universal generating function method. *Reliability Engineering and System Safety*, 65:271–282(12), 1999. 183

G. Levitin, A. Lisnianski, H. Ben-Haim, and D. Elmakis. Redundancy optimization for series-parallel multi-state systems. *Reliability, IEEE Transactions on*, 47(2): 165–172, Jun 1998. 182

P. Lévy. Systémes markoviens et stationnaires; cas dénombrable. *Ann. Ec. Norm. Sup.*, 1951. 10

P. Lévy. Systems semi-markoviens ayant au plus une inifinite denombrable d'etats possibles. *Proc. Intern. Congr. Math., Amsterdam, The Netherlands*, 2:294, 1954. 34

A. Lisnianski. Extended block diagram method for a multi-state system reliability assessment. *Reliability Engineering and System Safety,*, 92(12):1601–1607, 12 2007. 35

A. Lisnianski and G. Levitin. *Multi-state System Reliability: Assessment, Optimization and Applications*. World Scientific, Singapore, 2003. 18, 20, 34, 42, 43, 78, 79, 89, 101, 147, 183

C.J. Lu and W.Q. Meeker. Using degradation measures to estimate a time-to-failure distribution. *Technometrics*, pages 161–174, 1993. 155

D. J. Lunn, A. Thomas, N. Best, and D. Spiegelhalter. Winbugs – a bayesian modelling framework: Concepts, structure, and extensibility. *Statistics and Computing*, 10(4):325–337, 2000. 17

K. B. Marais and J. H. Saleh. Beyond its cost, the value of maintenance: An analytical framework for capturing its net present value. *Reliability Engineering and System Safety*, 94(2):644 – 657, 2009. 104

M. Marseguerra, E. Zio, and L. Podofillini. Multiobjective spare part allocation by means of genetic algorithms and monte carlo simulation. *Reliability Engineering & System Safety*, 87(3):325 – 335, 2005. 113

M. Matsumoto and T. Nishimura. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Trans. Model. Comput. Simul.*, 8(1):3–30, 1998. 169

K. McGrattan. *Fire Dynamics Simulator (FDS)*. National Institute of Standards and Technology, Gaithersburg, MD, USA, 2004. 126

William Q. Meeker and Luis A. Escobar. *Statistical Methods for Reliability Data (Wiley Series in Probability and Statistics)*. Wiley-Interscience, 1998. ISBN 0471143286. 155

M. Modarres, M. Kaminskiy, and V. Krivtsov. *Reliability Engineering and Risk Analysis: A Practical Guide*. CRC Press, FL, USA, 1999. 19, 42

G. S. Mokaddis and M. L. Tawfek. Stochastic analysis of a two-dissimilar unit warm standby redundant system with two types of repair facilities. *Microelectronics and Reliability*, 35(12):1467 – 1472, 1995. 77

Y. Morishita. A stochastic model of fire spread. *Fire Science and Technology*, 5(1): 1–10, 1985. 124, 127

A. Naess, B.J. Leira, and O. Batsevych. System reliability analysis by enhanced monte carlo simulation. *Structural Safety*, 31(5):349 – 355, 2009. 167

T. Nakagawa and S. Osaki. Stochastic behaviour of a two-unit priority standby redundant system with repair. *Microelectronics Reliability*, 14(3):309–313, 1975a. 7

T. Nakagawa and S. Osaki. The discrete weibull distribution. *IEEE Transactions on Reliability*, 24:300–301, 1975b. 71

T. Nakagawa and S. Osaki. Markov renewal processes with some non-regeneration points and their applications to reliability theory. *Microelectronics Reliability*, 15 (6):633–636, 1976. 6

W. R. Nunn and A. M. Desiderio. Semi-markov processes: An introduction. *Center for Naval Analyses*, pages 1–30, 1977. xvi, 36, 40

Shunji Osaki and T. Nakagawa. On a two-unit standby redundant system with standby failure. *Operations Research*, 19(2):510–523, 1971. 77

B. Ouhbi and N. Limnios. The rate of occurrence of failures for semi-markov processes and estimation. *Statistics and Probability Letters*, 59(3):245 – 255, 2002. 34

B. Ouhbi and N. Limnios. Nonparametric reliability estimation of semi-markov processes. *Journal of Statistical Planning and Inference,*, 109(1-2):155–165, 1/1 2003. 34

S. özekici and R. Soyer. Semi-markov modulated poisson process: probabilistic and statistical analysis. *Mathematical Methods of Operations Research*, 64(1): 125–144, 2006. 35

M.D. Pandey, T. Cheng, and W.C. Xie. Stochastic renewal process model for infrastructure asset management. *Inaugural International Conference of the Engineering Mechanics Institute*, 2008. 5

R.D. Peacock, G.P. Forney, P. Reneke, R. Portier, and W.W. Jones. *CFAST, the Consolidated Model of Fire Growth and Smoke Transport*. National Institute of Standards and Technology, Gaithersburg, MD, US, 1986. 126

M. Perman, A. Senegacnik, and M. Tuma. Semi-markov models with an application to power-plant reliability analysis. *Reliability, IEEE Transactions on*, 46(4):526–532, Dec 1997. xvi, 35, 71, 78

D. G. Platt, D. G. Elms, and A. H. Buchanan. A probabilistic model of fire spread with time effects. *Fire Safety Journal*, 22(4):367 – 398, 1994. ISSN 0379-7112. 124, 125, 126

J.W. Provan and E. Rodriguez. Development of a markov description of pitting corrosion. i, 1989. 10

J. Pukite and P. Pukite. *Modeling for Reliability Analysis: Markov Modeling for Reliability, Maintainability, Safety, and Supportability Analyses of Complex Computer Systems*. IEEE Press, 1998. 4

R.D. Radulovich, W.E. Vesely, and T. Aldemir. Aging effects on time-dependent nuclear plant component unavailability: an investigation of variations from static calculations. *Nuclear technology*, 112(1):21–41, 1995. 156

G. Ramachandran. Non-deterministic modelling of fire spread. *Journal of Fire Protection Engineering*, 3:37–48, 1991. 124, 125, 126

J. E. Ramirez-Marquez and D. W. Coit. A monte-carlo simulation approach for approximating multi-state two-terminal reliability. *Reliability Engineering and System Safety*, 87(2):253 – 264, 2005. 167

K. D. Rao, V. Gopika, V. V. S. S. Rao, H.S. Kushwaha, A.K. Verma, and A. Srividya. Dynamic fault tree analysis using monte carlo simulation in probabilistic safety assessment. *Reliability Engineering & System Safety*, 94(4):872 – 883, 2009. ISSN 0951-8320. doi: DOI:10.1016/j.ress.2008.09.007. 2, 144

D. Rasbash, G. Ramachandran, B. Kandola, J. Watts, and M. Law. Stochastic fire risk modeling. In *Evaluation of fire safety*, pages 399–420. John Wiley and Sons, 2004. 124

M. Rausand and A. Høyland. *System Reliability Theory.* Wiley-IEEE, San Francisco, CA, 2004. 43

S. M. Ross. *Applied Probability Models with Optimization Applications.* Holden-Day Inc., San Francisco, California, 1992. ISBN 0-486-67314-6. 14, 34

P.K. Samanta, W.E Vesely, F. Hsu, and M. Subudhi. NUREG/CR-5612: Degradation Modeling with Application to Aging and Maintenance Effectiveness Evaluations. Technical report, US Nuclear Regulatory Commission, 1991. 155

D. Silverstov. *Semi-Markov processes with discrete state space.* Sovetskoe Radio, Moscow, 1980. 34

F. A. Simonen and H. H. Woo. Analyses of the impact of in-service inspection using a Piping Reliability Model. Technical report, US Nuclear Regulatory Commission, 1984. 86, 110

N. O. Siu. Physical models for compartment fires. *Reliability Engineering*, 3(3): 77–100, 1982. 126

N. O. Siu and G. E. Apostolakis. Probabilistic models for cable tray fires. *Reliability Engineering*, 3(3):213 – 227, 1982. 126

P. Škňouřilová and R. Briš. Coloured petri nets and a dynamic reliability problem. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 222(4):635, 2008. 2

C. L. Smith, V. N. Shah, T. Kao, and G. Apostolakis. Incorporating aging effects into probabilistic risk assessment: A feasibility study utilizing reliability physics models. Technical report, US Nuclear Regulatory Commission, 2001. 156

W. L. Smith. Renewal theory and its ramifications. *Journal of the Royal Statistical Society*, 20(2):243, 1958. 34, 40

C.L. Tomasevicz and S. Asgarpoor. Preventive maintenance using continuous-time semi-markov processes. In *Proceedings of the 38th North American Power Symposium*, pages 3–8, Carbondale, USA., 2006. xvi, 35, 36, 104

Curtis L. Tomasevicz and Sohrab Asgarpoor. Optimum maintenance policy using semi-markov decision processes. *Electric Power Systems Research*, 79(9):1286 – 1291, 2009. 156

I. Ushakov. Optimal standby problems and a universal generating function. *Soviet Journal of Computer Systems Science*, 25:61–73, 1987. 182

I. Ushakov. The method of generalized generating sequences. *European Journal of Operational Research*, 125(2):316–323, 2000. 183

G. Valbuena and M. Modarres. Development of probabilistic models to estimate fire-induced cable damage at nuclear power plants. *Nuclear Engineering and Design*, 239(6):1113 – 1127, 2009. 126

A. Veeramany and M. D. Pandey. Reliability analysis of digital feedwater regulating valve controller system using a semi-markov process model. *International Journal of Nuclear Energy Science and Technology*, 6(4):298 – 309, 2011a. 128, 156, 202

A. Veeramany and M. D. Pandey. Reliability analysis of nuclear component cooling water system using semi-markov process model. *Nuclear Engineering and Design*, 241(5):1799 – 1806, 2011b. 128, 150, 151, 156, 202

A. Veeramany and M. D. Pandey. Reliability analysis of nuclear piping system using semi-markov process model. *Annals of Nuclear Energy*, 38(5):1133 – 1139, 2011c. ISSN 0306-4549. 128, 145, 150, 156, 202

A. Veeramany and M.D. Pandey. Semi-markov process model for the availability analysis of practical systems. In *Proceedings of the 16th ISSAT International Conference on Reliability and Quality in Design*, Washington D.C., USA, 2010a. 203

A. Veeramany and M.D. Pandey. Availability analysis of systems with multi-state components using semi-markov process model. In *International Conference on Reliability, Safety and Security Engineering*, Singapore, 2010b. 203

W. E. Vesely. Quantifying maintenance effects on unavailability and risk using markov modeling. *Reliability Engineering and System Safety*, 41:177–187, 1993. xv, xix, 4, 104, 155, 156, 157, 158, 159, 161

W.E. Vesely. Risk evaluations of ageing phenomena: the linear ageing reliability and its extensions. Technical report, US Nuclear Regulatory Commission, 1978. 156

M. Vineyard, K. Amoako-Gyampah, and J. R. Meredith. Failure rate distributions for flexible manufacturing systems: An empirical study. *European Journal of Operational Research*, 116(1):139 – 155, 1999. 145, 155

G. Vinod, S. K. Bidhar, H. S. Kushwaha, A. K. Verma, and A. Srividya. A comprehensive framework for evaluation of piping reliability due to erosioncorrosion for risk-informed inservice inspection. *Reliability Engineering and System Safety*, 82(2):187–193, 11 2003. 10

G. Vinod, R.K. Saraf, A.K. Ghosh, H.S. Kushwaha, and P.K. Sharma. Insights from fire psa for enhancing npp safety. *Nuclear Engineering and Design*, 238(9): 2359 – 2368, 2008. ISSN 0029-5493. 126

F. J. Vodvarka and T. E. Waterman. Fire behavior, ignition to flashover. Technical report, IIT Research Institute, Chicago, IL, 1975. 138, 141

B Volik, B.B. Buyanov, N.V. Lubkov, V.I. Maximov, and A.S. Stepanyants. Methods of analysis and synthesis of control systems structures. In *Energoatomizdat (Russian)*, 1988. 18

I. Vrbanić, I. Košutić, I. Vuković, and Z. Šimić. Presentation of common cause failures in fault tree structure of krško psa: An historical overview. *International Conference Nuclear Energy for New Europe 2003*, 2003. 211

A. H. Wang, S. Yan, and P. Liu. A semi-markov survivability evaluation model for intrusion tolerant database systems. In *International Conference on Availability, Reliability and Security*, Krakow, Poland, 2010. xvi, 37

H. Wang and H. Pham. Survey of reliability and availability evaluation of complex networks using monte carlo techniques. *Microelectronics and Reliability*, 37(2): 187 – 209, 1997. 167

T.E. Waterman. Determination of fire conditions supporting room flashover. Technical report, Defense Technical Information Center (DTIC), 1966. 134

J. M. Watts. Dealing with uncertainty: Some applications in fire protection engineering. *Fire Safety Journal*, 11(1-2):127 – 134, 1986. 124, 125, 126

A.L. White and D.L. Palumbo. State reduction for semi-markov reliability models. *Reliability and Maintainability Symposium, 1990. Proceedings., Annual*, pages 280–285, Jan 1990. 34

R. B. Williamson. Coupling deterministic and stochastic modeling to unwanted fire. *Fire Safety*, 3(4):243–259, 1981. 124, 125, 127

L. Xing, K. N. Fleming, and T. L. Wee. Comparison of markov model and fault tree approach in determining initiating event frequency for systems with two train configurations. *Reliability Engineering and System Safety*, 53:17–29(13), 1996. xiv, xvi, xvii, 4, 10, 26, 27, 30, 76, 77, 78, 80, 83

M. Yau, S. Guarro, and G. Apostolakis. Demonstration of the dynamic flowgraph methodology using the titan ii space launch vehicle digital flight control system. *Reliability Engineering & System Safety*, 49(3):335–353, 1995. 144

A. Younes and M. R. Girgis. A tool for computing computer network reliability. *International Journal of Computer Mathematics*, 82:1455–1465, 2005. 97, 99, 100