Risk, Reliability and Safety Engineering

Durga Rao Karanki *Editor*

Frontiers of Performability Engineering

In Honor of Prof. K.B. Misra

Springer

Risk, Reliability and Safety Engineering

In this era of globalization and competitive scenario there is a conscious effort to ensure that while meeting the reliability targets the potential risk to society is minimal and meet the acceptability criteria towards achieving long term targets, including sustainability of a given technology. The objective of reliability is not only limited to customer satisfaction but also important for design, operating systems, products, and services, while complying risk metrics. Particularly when it comes to complex systems, such as, power generation systems, process systems, transport systems, space systems, large banking and financial systems, pharmaceutical systems, the risk metrics becomes an overriding factor while designing and operating engineering systems to ensure reliability not only for mission phase but also for complete life cycle of the entity to satisfy the criteria of sustainable systems.

This book series in Risk, Reliability and Safety Engineering covers topics that deal with reliability and risk in traditional sense, that is based on probabilistic notion, the science-based approaches like physics-of-failure (PoF), fracture mechanics, prognostics and health management (PHM), dynamic probabilistic risk assessment, risk-informed, risk-based, special considerations for human factor and uncertainty, common cause failure, AI based methods for design and operations, data driven or data mining approaches to the complex systems. Within the scope of the series are monographs, professional books or graduate textbooks and edited volumes on the following topics:

- Physics of Failure approach to Reliability for Electronics
- Mechanics of Failure approach to Mechanical Systems
- Fracture Risk Assessment
- Condition Monitoring
- Risk Based-In-service Inspection
- Common Cause Failure
- Risk-based audit
- Risk-informed operations management
- Reliability Cantered Maintenance
- Human and Institutional Factors in Operations
- Human Reliability
- Reliability Data Analysis
- Prognostics and Health Management
- Risk-informed approach
- Risk-based approach
- Digital System Reliability
- Power Electronics Reliability
- Artificial Intelligence in Operations and Maintenance
- Dynamic Probabilistic Risk Assessment
- Uncertainty
- Aging Assessment & Management
- Risk and Reliability standards and Codes
- Industrial Safety

Potential authors who wish to submit a book proposal should contact:
Priya Vyas, Senior Editor, e-mail: Priya.vyas@springer.com

Durga Rao Karanki
Editor

Frontiers of Performability Engineering

In Honor of Prof. K.B. Misra

Springer

Editor
Durga Rao Karanki
Swiss Federal Railways (SBB CFF FFS)
Bern, Switzerland

ISSN 2731-7811 ISSN 2731-782X (electronic)
Risk, Reliability and Safety Engineering
ISBN 978-981-99-8257-8 ISBN 978-981-99-8258-5 (eBook)
https://doi.org/10.1007/978-981-99-8258-5

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Foreword

It is a great pleasure and honour to write a Foreword for this book, as a part of the celebration of Prof. Misra's 80th birthday. His, academic, scientific and professional achievements, publications, awards and global recognition are well-known and readily available through all media of communications.

Hence, I wish to focus on his greatest achievement, from my point of view, which is his vision, carriage and creation of the concept of **performability**. As the father of the modern science, Galileo Galilei (1564–1642) said, "*All truths are easy to understand once they are discovered. The point is to discover them.*" For me, that is the case of performability that integrated all related engineering disciplines with impacting management disciplines, as the best life cycle decisions can be made only by integrating these two ends of the spectrum. The concept of Performability Engineering was Prof. Misra's discovery, whose publication enabled everybody to understand it easily and clearly. The impact of this discovery is everlasting, as the depth and the breath of the topics covered by this book clearly demonstrate. I am confident that the future generations of students and practitioners will greatly benefit from it.

I am delighted to use this opportunity, on behalf of the global community, to thank Prof. Misra for his lifelong contribution to the development of the foundation of Performability Engineering and his contribution to its dissemination through the "army" of students, collaborators and consultants, on the global scale.

I also wish to commend Dr. Ing. Durga Rao Karanki, ex-student of Prof. Misra, for editing this book that is an ever-lasting contribution to the further enhancement and applications of Performability Engineering.

Prof., Dr. Jezdimir Knezevic
Founder and President of MIRCE
Akademy
Exeter, UK

Preface

Performability Engineering aims to address both the dependability and sustainability aspects for engineering systems. Dependability encompasses quality, reliability, availability, maintainability, safety, and security while sustainability covers environment and economic aspects. In the light of shrinking world resources and changing policies, environmental and economic aspects need to be considered while engineering dependability into systems. Dependability analysis has become an essential activity in system life cycle of complex engineering systems such as transportation systems (railways, aviation, and road), nuclear reactors, chemical plants, defence systems, etc. Efforts should be done to integrate sustainability aspects in dependability analysis.

To trade off sustainability, dependability and cost-effectiveness of product or system, performability engineering provides an efficient framework for decision-making. This book presents the latest advances in performability analysis including artificial intelligence-based approaches and digitalization. The latest methods are further extended with several practical applications from the various industrial case studies including software, manufacturing, power systems, electronic systems, nuclear reactors, chemical plants, etc.

The book is organised into three parts. The first part covers the latest developments of the methods in the area of "Reliability, Availability, Maintainability, Quality." For example, reliability and availability modelling for standby systems, dynamic wireless networks, cyber-physical systems and Internet of Things are addressed. Latest methodological advances such as Decision Diagrams for complex system reliability, accelerated life testing analysis, and resilience analysis are also included in this part.

To achieve the goal of sustainable industrial development, instead of replacing assets based on a certain time interval, it is necessary to also consider economy, environmental impact and safety. The Chap. 8 provides a state-of-the-art review of the management of ageing assets and discusses the challenges and opportunities. It discusses knowledge development in the context of RAMS (reliability, availability, maintainability, safety) and PHM (prognostics and health management) and proposes a new general framework for the management of ageing assets.

The influence of maintenance on profitability is too high to ignore in management of complex engineering assets. The Chap. 9 proposes an integrated Key Performance Indicators (KPIs) framework to measure the maintenance performance. The KPI framework is defined as a system that combines all facets of maintenance actions into a set of measures focusing on aspects of maintenance performance that are most critical for the current and future success of the organisation, thus providing a means to quantify the efficiency and effectiveness of its maintenance actions.

The second part focuses on "Safety, Risk, Uncertainty." The lessons learnt from the Fukushima Daiichi accident (2011) and the latest advances in severe accident management guidelines and risk-taking behaviour are presented (in first three chapters) in the context of probabilistic safety assessment and management for nuclear power plants. Risk ranking of critical failure modes, which is a typical goal of failure mode effect and criticality analysis, is explored in the light of uncertainty with multi-criteria decision-making approaches. To overcome some of the limitations of event tree analysis, which is widely used in safety assessments, Petri Nets-based approach is presented and illustrated with examples. Further, trading off computational efforts of accidental simulations and accuracy in risk estimates is a challenge in integrated safety analysis. Alternative approaches are investigated with a case study on chemical reactor problem in the Chap. 17.

The third part presents a few Applications of Performability Engineering. The Chap. 18 provides a holistic view of key enablers of smart manufacturing that drive performablity and maximize manufacturing efficiencies. This chapter discusses advancements in the technologies (Artificial intelligence (AI), Machine learning (ML), cloud computing, advanced robotics, automated decision support, Digital Twin, Internet of things) and various aspects of performability for next-generation manufacturing systems.

The chapter entitled "Cyber-Physical Power System (CPPS): A review on metrics and modelling methods of system resilience" presents recent advances in resilience modelling methods for cascading failures within the CPPS as well as challenges and future research directions for resilience enhancement and modeling of the CPPS are discussed. The Chap. 20 discusses a variety of concepts, models and approaches for assessing performance models at the prototype level of big data including Artificial Intelligence (AI) techniques.

To honour Prof. K. B. Misra on the occasion of his 80th birthday, some of his former Ph.D. students and collaborators who are internationally recognized in academia and industry have contributed to this edited book. Chapter 25 gives a brief account of Prof. Misra's journey of more than four decades to become an internationally acclaimed academician.

This book is designed to assist students and researchers in the area of Performability Engineering. It provides a quick reference to the latest advances of methods and several practical applications.

Bern, Switzerland Dr.-Ing. Durga Rao Karanki

Prologue

It gives me great pleasure to write a Prologue to this edited volume on "Advances in Performability Engineering" in honour of Prof. K. B. Misra, being brought out by one of his ex-students, Dr. Durga Rao Karanki to commemorate Prof. Misra's 80th birthday. Professor Misra pioneered "Reliability Engineering" in India and established "Reliability Engineering Center" at IIT Kharagpur in 1983, which later on was renamed in 2016 as "Subir Chaudhary School of Quality and Reliability Engineering," is probably the only graduate teaching and research centre in India. Some of the first students who graduated out of the Reliability Engineering Center now lead teaching/research in leading industries and top universities across various geographies. Professor Misra, subsequently, in 2005 went on to start an *International Journal of Performability Engineering* to provide a platform for leading researchers to publish their work. He also brought out the first of the volumes that appeared on "Performability Engineering" in 2008 and 2021 published by Springer. I was fortunate to be the Guest Editor (jointly with Prof. Kapur and Prof. Osaki) of the first special issue of this journal. I also had the privilege of being a Guest Editor jointly with Prof. Misra of a special section on Reliability and Risk Assessment of Complex Systems comprising 15 papers in IEEE Transactions on Reliability, vol. 60 II, 2011. His contributions to the field of Reliability Engineering and Performability Engineering are immense and far too many to mention. As an educator and a researcher, he stands tall amongst the various luminaries in the field and he has been decorated with several awards to say the least. It is only apt that this edited volume is being brought out timely by Dr. Durga Rao Karanki of Swiss Federal Railways as a contribution in his honour by his ex-students and collaborators. I take this occasion to wish Prof. Misra a very long and a healthy life full of happiness.

Ajit Kumar Verma
Series Editor and Professor (Technical Safety)
Western Norway University of Applied Sciences
Bergen, Norway

(Ex-)Professor, Department of Electrical Engineering
Indian Institute of Technology Bombay
Mumbai, India

Acknowledgements

It is a great privilege to honor the Guru of Performability Engineering, Prof. K.B. Misra, who immensely contributed to its advancement. He also molded careers of several students, research scholars and colleagues. I am sincerely grateful to him for allowing me to bestow a tribute to him.

I express my sincere thanks to Prof. S.K. Chaturvedi (IIT Kharagpur) for his constant encouragement and full moral support. I am grateful to Prof. A.K. Verma, Prof. P.V. Varde, and Prof. Uday Kumar for their useful suggestions and motivation.

Excellent support has been received from the authors of the chapters in timely preparations as well as revisions. I am grateful for their commitment and dedication. Reviewers are herewith acknowledged for their constructive criticism and useful suggestions during the reviews of the chapters.

Special thanks to Anjamma, Manikya Rao, Praveena, Harshita, Madhav, Prasad, Ankalakshmi, Harsha, and Dharma for their love and cooperation.

Sincere thanks to Ms. Priya Vyas, Mr. Gowrishankar Ayyasamy, and Mr. Gowtham Chakravarthy for their great support and patience in managing the production of this book.

Contents

Part I Reliability, Availability, Maintainability, Quality

Part II Safety, Risk, Uncertainty

Part III Applications of Performability Engineering

About the Editor

Dr. Durga Rao Karanki is currently working as a Senior RAMS Engineer at Swiss Federal Railways (SBB CFF FFS). Earlier he worked as a RAMS Manager at Siemens Mobility AG (2017–2022), responsible for RAMS Management of European Train Control System projects. Prior to switching to the railway industry, he worked as a Scientist at two premier national labs, Paul Scherrer Institute (PSI, ETH Board Switzerland) (2009–2017) and Bhabha Atomic Research Centre (India) (2002–2009). Primarily his research focused on dynamic safety assessment, uncertainty management, and risk informed decision making of nuclear power plants. He is also a visiting faculty at several technical institutes.

He has actively been involved in research and development of Reliability and Safety methods and their applications for the last 21 years. His research resulted in more than 70 publications including four books, several journal articles and conference papers, with more than 1500 citations.

He received two awards for research Excellency from Society for Reliability Engineering, Quality and Operations Management. He is on the editorial board of three international journals in the area of reliability and risk analysis. He holds bachelor's degree (2000) in electrical and electronics engineering from the Nagarjuna University (India), masters (2002) in Reliability Engineering from Reliability Engineering Centre of Indian Institute of Technology (IIT) Kharagpur and Ph.D. (2008) from the IIT Bombay.

Part I
Reliability, Availability, Maintainability, Quality

Chapter 1
Reliability Evaluation of Standby Systems

Suprasad V. Amari

Abstract Redundancy is a basic and fundamental concept used in reliability engineering. However, the methods for analyzing the reliability of redundant systems, particularly for systems with standby redundancy, are limited. In this paper, using the concepts of counting processes, a simple, accurate, and computationally efficient method to evaluate the reliability of standby systems is presented. The method efficiently analyzes the systems with non-identical components, cold/warm/hot standby components, shared standby components among different subsystems operating at different conditions, switching failures, and general failure time distributions. The proposed method is demonstrated using several examples. The results include CPU times for solving the examples as well as the complete listing of the MATLAB script used. The examples demonstrate that the proposed method provides a practical and accurate way of evaluating the reliability of complex standby configurations that arise in a wide range of applications.

Keywords Standby systems · Shared standby components · k-out-of-n systems · Switch failures · System reliability · Warm standby redundancy

Acronyms and Abbreviations

AFTM	Accelerated Failure Time Model
CE	Cumulative Exposure (Model)
DFT	Dynamic Fault Tree
PHM	Proportional Hazards Model
TFR	Tampered Failure Rate (Model)

S. V. Amari (✉)
BAE Systems, Nashua, NH 03062, USA
e-mail: suprasad.amari@gmail.com; suprasad.amari@baesystems.com

D. R. Karanki (ed.), *Frontiers of Performability Engineering*, Risk, Reliability and Safety Engineering, https://doi.org/10.1007/978-981-99-8258-5_1

1.1 Introduction

Redundancy is an important concept in improving the reliability of systems [1, 2]. It is universally accepted that fault tolerant and safety critical systems cannot achieve intended reliability without employing redundancy [3]. There are two basic redundancy types: (1) active redundancy and (2) standby redundancy. According to the failure characteristics of the components in the standby mode, standby redundancy is further classified as cold, warm, and hot standby. When there are no switching delays and failures, the mathematical models for hot standby and active redundancy arrangements are equivalent [2, 4]. Further, several efficient methods are available for analyzing the systems with active redundancy [5]. Therefore, in this chapter, we concentrate only on standby systems.

Standby redundancy has several important applications. The applications and guidelines of standby systems in the electrical power industry are well established [6, 7]. Standby systems also play an important role in aeronautical and space applications. For example, the electronic multiplexing system for the B-1 bomber uses a standby redundant design [8]. Sinaki [9] described the importance of standby redundancy in space exploration and satellite systems. The application of standby systems in emergency telecommunications systems used in nuclear power plants is described in Pham et al. [10]. Similarly, many other systems use standby redundancy as an effective strategy to achieve high reliability including textile manufacturing systems [11], carbon recovery systems used in fertilizer plants [12], and fault tolerant systems used in computer applications [13]. Due to the wide range of practical applications of the standby systems, the reliability analysis of these systems has been a topic of research interest [14–20].

An accurate reliability analysis of standby systems (i.e., systems with standby redundant components) is important for two primary reasons: (1) to assess whether the system meets safety and reliability requirements; and (2) to determine the optimal redundancy configurations and other design alternatives. The accurate reliability analysis is particularly important in situations where repair of a failed component is either not possible (for example, in unmanned spacecraft) or would result in an unacceptable interruption of service (i.e., in air traffic control). After the Challenger disaster in 1986 [21, 22], for example, the Space Station External Maintenance Solutions team recommended replacing NASA's traditional qualitative approach to redundancy with a quantitative approach based on the overall probability of a given failure and its impact on the entire station. Subsequently, NASA sponsored several software tools and methodologies for accurate quantification of risk and reliability of complex systems including the standby configurations. For example, the new fault tree handbook published by NASA [23] includes the dynamic fault trees and the methods for analyzing the standby systems. Similarly, NASA sponsored the development of the Galileo/ASSAP software tool for dynamic fault tree analysis [24].

Although the accurate analysis of non-repairable systems is important in several critical applications, there has been relatively less research directed toward the study of non-repairable standby redundancy as compared to other redundant systems, such as active redundancy systems and/or repairable standby systems. Yearout et al. [25] reviewed and categorized 156 references specifically describing research in standby redundancy. They identified only four references on non-repairable systems with standby redundancy and all of them considered the exponential distributions for component failure times. Further, as mentioned in She and Pecht [26] the methods for analyzing the warm standby redundancy are very limited. Reference [13] emphasized the importance and efficiency of global spares in fault-tolerant systems that contain some identical modules. Despite the widespread use of systems with global spares, the amount of research that has analyzed these systems is relatively small. No analytical study of systems with global spares that assumes arbitrary module failure distribution is known to the authors. Recently, Amari et al. [27], Boudali and Dugan [28] proposed new solution methods for analyzing standby systems under the dynamic fault tree paradigm. However, due to the generic nature of the DFT paradigm, the methods proposed in Amari et al. [27], Boudali and Dugan [28] for analyzing the standby systems are computationally intensive.

Similarly, the methods available for finding the optimal designs of systems with standby redundancy are very limited [29]. For example, Kuo et al. [2] reviewed 337 references describing reliability optimization research. Of those 337, only 13 pertained to standby redundancy. We, the authors of this chapter, believe that the main reason for such a low number of research papers on optimal standby redundancy is due to the difficulty in evaluating the reliability of standby systems. Once we develop the methods for evaluating the reliability of standby systems, it is straightforward to apply the existing optimization methods, particularly heuristic and meta-heuristic optimization methods [2, 14, 30–32], for determining the optimal system designs. Therefore, it is important to develop efficient methods for analyzing the standby systems.

1.2 Motivation and Related Works

Even though the standby redundancy is a very basic and fundamental concept used in reliability engineering, surprisingly, the methods for accurately analyzing the reliability of standby systems are limited [25].

- This is particularly true for k-out-of-n standby systems when the failure times of components are not limited to exponential distributions but can follow any general time-to-failure distribution such as Weibull, Gamma, and lognormal. This is because the underlying stochastic process does not follow any standard model such as semi-Markov or non-homogeneous Poisson processes [33]. Hence, we need to use complex multiple integrals even for the identical component case with cold or warm standby redundancy [34, 35]. The complexity associated with this problem can be identified easily, for example, when we try to find the reliability of a 5-out-of-10 warm standby system with Weibull failure time distributions (with or without identical components).

- The problem becomes more complex when the standby components (spares) are shared by several subsystems where the subsystems have different operating conditions [36].
- The complexity increases further when there are switch-over failures, non-identical components, and mixed cold–warm–hot standby components [31, 34].

The above conclusions are drawn after making an extensive literature survey of the published research articles and textbooks using Scopus, IEEE Xplore, Google Scholar, Google Book Search, and Google Web. In addition, we noticed that some of the important contributions related to standby systems made in the past are almost unnoticed by the current reliability researchers. Special mention is due for Barlow and Proschan [37, p. 175] for their work on counting process in analyzing the reliability of cold standby systems with identical components published in 1965. Similarly, a special mention is due for the Gnedenko et al. [38] research on the 1-out-of-*n* warm standby systems with identical components using the concept of equivalent age (cumulative exposure model) published in 1969.

Although the concepts used in Barlow and Proschan [37], Gnedenko et al. [38] are useful in analyzing standby systems, they are restricted to very simple cases. Further, there is no information about how to generalize these concepts for analyzing the systems with warm standby components and imperfect switches. Therefore, in the current, state-of-the-art literature of reliability and statistical analysis methods, Monte Carlo simulation is the only available method for analyzing standby systems. However, simulation generally takes a great deal of computational time, particularly for analyzing systems with high-reliability requirements, such as safety-critical systems used in space applications. Both computational time and accuracy become a real concern when system reliability must be evaluated several times to find optimal system configurations and redundancy levels.

In this chapter, we present a simple, accurate, and computationally efficient method to find the reliability of *k*-out-of-*n* standby systems and their generalizations. The method can be applied to any combination of the following scenarios:

- Non-identical components.
- Failures of switching mechanisms.
- Cold, warm, and hot standby components.
- Subsystems with mixed standby configurations.
- General failure time distributions for the components.
- Shared standby components among different subsystems.

Premises of the proposed method follow:

- At any logical location/position of initially operating components (primary component locations), only a finite number of standby components are used. The number is limited by the maximum number of failures that can occur at that location prior to overall system failure.
- When the dependencies with other locations (components) are ignored, it is easy to compute the probability of a given number of failures at a specific location. This computation is equivalent to finding the reliability of a 1-out-of-n standby system.

- Each location can be modeled as a multi-state component (a multi-valued discrete random variable) with the above probabilities.
- The total number of standby components used by different locations must be less than the total number of standby components. Using this condition, the overall reliability of the system (or subsystem) can be computed easily (convolution of discrete random variables). Understanding the role of this step is critical to apply the proposed method. It plays a key role in evaluating the system reliability, particularly for systems with shared standby components, warm standby components, and switch failures.

We demonstrate the proposed method using several examples. We also provide the CPU times and a complete listing of the MATLAB scripts used. The examples demonstrate that the proposed method provides a practical and accurate way of evaluating the reliability of complex standby configurations that arise in a wide range of applications. The speed and accuracy of the proposed method prove that it is also suitable for integrating with optimization algorithms to find the cost-effective system configurations and redundancy levels.

1.3 Cold Standby Systems

In this section, we describe the reliability evaluation of cold standby systems.

1.3.1 1-out-of-n Cold Standby Systems

Consider a 1-out-of-n cold standby system, possibly with non-identical components and general failure distributions. Let X_i be the operating (failure) time of component i and F_i be the cumulative distribution function (CDF) of X_i. Hence, the system failure time, T, can be expressed as

$$T = X_1 + X_2 + \cdots + X_n \tag{1.1}$$

Therefore, the system reliability is

$$R(t) = \Pr\{T \geq t\} \tag{1.2}$$

Amari and Misra [39] provided the closed-form solutions for $R(t)$ when component failure distributions are exponential or Erlang. Similarly, closed-form expressions can be found for some other distributions such as normal and uniform. However, for the general case, the distribution of T can be obtained using convolution integrals [37, 38]. Define

$$Y_i = X_1 + \cdots + X_i \tag{1.3}$$

Let $G_i(t)$ be the CDF of the Y_i. Hence,

$$R(t) = 1 - G_n(t) \tag{1.4}$$

where

$$G_i(t) = G_{i-1} * F_i(t); \quad \text{and} \quad G_1(t) = F_1(t) \tag{1.5}$$

By definition, we have $G_0(t) = 1$. Further, the convolution of the two distributions F and G is defined as

$$F * G(t) = \int\limits_0^t dF(x)G(t-x) = \int\limits_0^t F(t-x)dG(x) \tag{1.6}$$

There are several standard methods for computing the convolution integrals [40]. In this chapter, we used a simple method based on the trapezoidal rule for computing the convolution integrals to demonstrate the underlying concepts. The following MATLAB script can be used to compute the convolution of two time-to-failure distributions (F1 and F2).

```
function F = convolution(F1, F2)
   m = max(size(F1)); F = zeros(m,1);
   for i=2:m
    for j=2:i
      F(i) = F(i) + 0.5 * [F1(j) - F1(j-1)]
            * [F2(i-j+1) + F2(i-j+2)];
     end
    end
 end
```

In this script, the mission time (t) is divided into m intervals. Not only the accuracy of the computation increases with m but also the computational time. To extend these calculations for other cases of standby systems, we need to find the state distribution of the underlying stochastic process. Let $P_i \equiv P_i(t)$ be the probability that there are exactly i failures in the system. The P_i values can be calculated as:

$$P_i = G_i(t) - G_{i-1}(t); \quad \text{and} \quad P_0 = 1 - G_1(t) \tag{1.7}$$

The 1-out-of-n system is functioning if there are at most $(n-1)$ failures. Hence, the system reliability can be represented as

$$R(t) = \sum_{i=0}^{n-1} P_i = 1 - G_n(t) \tag{1.8}$$

1.3.2 k-out-of-n Cold Standby Systems

In the k-out-of-n cold standby system, there are a total of n components in the system. Initially, k components are operating and the remaining $(n - k)$ components are in cold standby. Immediately upon the failure of an operating component, the component is replaced by one of the standby components (in the queue). The system functions as long as the number of failed components in the system is less than $(n - k + 1)$. Assume that the operating components are kept at k logical locations or positions. It is important to note that, when the number of failed components is less than $(n - k + 1)$, there is no shortage of spares. Hence, the failure process at each position is independent provided that all spares are identical. This is because the probability of the number of failures at a particular position is independent of the specific sequence of spares used. Therefore, to make the failure process at each position independent, we assume that all standby components are identical. However, the primary components can be non-identical. Similarly, the operating failure distribution of the standby components may vary based on the primary position they used.

Assume that the operating failure distribution of the primary and the standby components at position i are $F_i(t)$ and $H_i(t)$, respectively. Let $G_{ij}(t)$ be the probability that there are at least j failures at the primary position i. Hence, we have

$$G_{ij}(t) = G_{i,j-1} * H_i(t); \quad \text{and} \quad G_{i,1}(t) = F_i(t) \tag{1.9}$$

Let $P_{ij} \equiv P_{ij}(t)$ be the probability that there are exactly j failures at the primary position i. Hence,

$$P_{ij} = G_{ij}(t) - G_{i,j-1}(t); \quad \text{and} \quad P_{i0} = 1 - G_{i,1}(t) \tag{1.10}$$

The overall system reliability of the k-out-of-n cold standby system can be calculated as the probability that the sum of the failures at all positions is less than $(n - k + 1)$. The sum can be calculated using discrete convolutions performed on P_{ij} values. We use the MATLAB built-in function (*conv*) for computing the discrete convolutions. Let $\boldsymbol{P}$ be the resulting vector. The ith element of $\boldsymbol{P}$, P_i for $i < (n - k + 1)$, represents the probability that there are exactly i failures in the system. It should be noted that for $i \geq (n - k + 1)$, the vector $\boldsymbol{P}$ contains meaningless values. Finally, the system reliability is

$$R(t) = \sum_{i=0}^{n-k} P_i \tag{1.11}$$

Example 1 4-out-of-10 cold standby system with identical components. The failure distribution of the components is Weibull with η = 1000 and β = 2.0. Mission time is t = 1000 units of time (say hours).

Solution: The system reliability: $R(t) = 0.99306$. The CPU time is 0.0031 s seconds. The state probability vector: $\boldsymbol{P} = \{0.0183, 0.1033, 0.2396, 0.2958, 0.2130, 0.0949, 0.0281\}$. The following MATLAB script can be used for solving this example.

```
function example1()
  sTime = cputime; nloops = 100; %for CPU time
  for loop = 1:nloops %for CPU time

    %%%% inputs
    eta = 1000; beta = 2.0; %Weibull specific
    mission_time = 1000;
    k = 4; n = 10;

    %%%% integration parameters
    m = 100; m1 = m+1; dt = mission_time/m;
    x = 0:dt:mission_time;

    %%%% Convolution of continuous r.v.
    F1 = 1 - exp(-(x/eta).^(beta)); %Weibull
    F2 = F1; F(1) = F2(m1);
    for i = 2:(n-k+1)
      F2 = convolution(F1, F2);
      F(i) = F2(m1);
    end

    %%%% Convolution of discrete r.v.
    P1 = [1 F] - [F 0]; P = P1;
    for i = 2:k
      P2 = conv(P1, P);
      P = P2(1:n-k+1);
    end
  end

  %%%% Results and CPU time
  CPU = (cputime - sTime)/ nloops
  P, Rel = sum(P)
end
```

The MATLAB script can be optimized further. However, to improve readability and comprehension, we avoided such optimizations. It should be noted that all indexes used in the MATLAB script start from 1. Hence, the index 0 is shifted to 1. Similarly, the variables used in this script may not match with the variables used in the main body of this chapter. However, we believe that anyone with a basic MATLAB programming experience will have no difficulty in understanding the script. The script can be executed by typing example 1 in the MATLAB command window.

Example 2 Same as Example 1 except the failure distribution of a component depends on the primary location (position) that is used. This is because the operating conditions at each location are different. The failure distribution of the components at primary location i is Weibull with $\eta_i = 1000 + 100i$ and $\beta_i = 1 + 0.25i$.

Solution: The system reliability: $R(t) = 0.99487$. The CPU time is 0.0127 s seconds. The state probability vector: $\boldsymbol{P} = \{0.0614, 0.1986, 0.2848, 0.2412, 0.1364, 0.0554, 0.0171\}$. The following MATLAB script can be used for solving this example. Note that, in this script, we computed both the continuous and discrete convolutions in a single *for* loop.

```
function example2()
  sTime = cputime; nloops = 100; % for CPU time
  for loop = 1:nloops
    %%%% inputs: Weibull specific
    k = 4; n = 10; mission_time = 1000;
    eta = 1000 + 100 * [1:k];
    beta = 1 + 0.25 * [1:k];

    %%%% integration parameters
    m = 100; m1 = m+1; dt = mission_time / m;
    x = 0:dt:mission_time; P = 1;

    %%%% Convolutions
    for j = 1:k % primary component type
      %%% F1 calculation is Weibull specific
      F1 = 1 - exp(-(x/eta(j)).^(beta(j)));
      F2 = F1; F(1) = F2(m1);
      for i = 2:(n-k+1)
        F2 = convolution(F1, F2);
        F(i) = F2(m1);
      end
    P1 = [1 F] - [F 0];
    P2 = conv(P1, P); P = P2(1:n-k+1);
    end
  end

  %%%% Results and CPU time
  CPU = (cputime - sTime)/ nloops
  P, Rel = sum(P)
end
```

Example 3 Same as Example 2 except the failure distribution of the standby components is independent of the locations at which they are used. The operating failure distribution of the standby components is Weibull with $\eta = 1000$ and $\beta = 2$.

Solution: The system reliability: $R(t) = 0.99582$. The CPU time is 0.0123 s seconds. The state probability vector: $\boldsymbol{P} = \{0.0614, 0.1979, 0.2850, 0.2432, 0.1376, 0.0548, 0.0160\}$. The MATLAB script is similar to that of Example 2.

1.4 Shared Standby Components

In this section, we describe the method to compute the reliability of systems where a common pool of standby components is shared by multiple subsystems. To minimize introducing new concepts, in this chapter, we describe this method only for systems with subsystems in series. Hence, all subsystems are required to function for the successful operation of the system. Consider the subsystem i requires k_i operating components. Assume that there are n_S cold standby spares. The system is in operation as long as the number of failed components in the system is less than or equal to n_S. Therefore, we can find the reliability of this system using the counting process arguments that are used to analyze k-out-of-n cold standby systems. It should be noted that the number of locations where the standby components are used is the sum of all primaries of all subsystems.

Example 4 The system consists of 10 subsystems in series: $k_i = i$ for $1 \leq i \leq 10$. The failure distribution of an operating component in subsystem i is Weibull with $\eta_i = 1000i$ and $\beta_i = 1 + 0.25i$. There are a total of $n_S = 5$ cold standby components that are shared by all subsystems. The operating failure distribution of the standby component is independent of the subsystem and it follows Weibull with $\eta = 5000$ and $\beta = 2$. Mission time is $t = 1000$ units of time (say hours).

Solution: The system reliability: $R(t) = 0.9921$. The CPU time is 0.137 s. The state probability vector: $\boldsymbol{P} = \{0.0702, 0.2471, 0.3213, 0.2247, 0.0989, 0.0299\}$. The MATLAB script is similar to that of Examples 2 and 3.

1.5 Warm Standby Systems

In this section, we present a method based on counting processes for computing the reliability of warm standby systems with general failure distributions. This method is applicable to all types of systems considered for the case of cold standby systems. Because the basic concept is the same for all cases, we describe the proposed method only for the k-out-of-n warm standby systems with identical components.

1.5.1 Basics of Warm Standby Models

For modeling standby systems, it is important to know how the failure distributions in standby and operational modes are related. Accelerated life testing models play an important role in describing these relationships [41, 42]. Let the failure distributions of a component in standby and operational modes be $F_{sb}(t)$ and $F_{op}(t)$, respectively. The corresponding reliability functions are $R_{sb}(t) = 1 - F_{sb}(t)$ and $R_{op}(t) = 1 - F_{op}(t)$.

- Accelerated Failure Time Model (AFTM): According to this model, we have $R_{sb}(t) = R_{op}(t.\phi_s)$, where ϕ_s is the acceleration (deceleration) factor in the standby mode.
- Proportional Hazards Model (PHM): According to this model, we have $R_{sb}(t) = [R_{op}(t)]^{\psi_s}$, where ψ_s is the failure rate multiplicative factor in the standby mode. Hence, the failure rate relationship is: $h_{sb}(t) = \psi_s.h_{op}(t)$.

A standby component kept in operation experiences both standby and operational environments. Therefore, it is important to consider the effects of the time spent in the standby mode on the operational failure characteristics of the components. Let $R(t|t_{sb} = x)$ be the conditional reliability of a component given that the component is kept in operation at time x. The following models are used to calculate this conditional reliability.

- Cumulative Exposure (CE) Model [41, 42]: According to this model, the effective operational age (x_{op}) of the component at the time of switch-over (x) is calculated using the following relationship: $R_{sb}(x) = R_{op}(x_{op})$.
- Tampered Failure Rate (TFR) Model [43]: According to this model the failure rate of the component at $y \in [x, t]$ is equal to the operational failure rate at y, i.e., $h_{op}(y)$. Hence, $R(t|t_{sb} = x) = R_{op}(t|x) = \Pr\{\text{component is operational at } t \mid \text{component is operational at } x\}$.

To make a consistent notation, for the TFR model, it can be assumed that $x_{op} = x$.

1.5.2 Reliability Analysis of k-out-of-n Warm Standby Systems

Consider a k-out-of-n warm standby system. Initially, k primary components are in operation and the remaining $(n - k)$ components are in warm standby. When there is a failure in one of the primary locations, the system will try to use the next unused standby in that primary location. If the standby component is already failed, then we count the standby failure to the corresponding primary location and mark the standby component as already used (or failed). Now the system looks for the next unused standby component. The process continues until the next non-failed standby component is found or the supply of spares is exhausted, which results in system failure.

Let $G_i(t)$ be the cumulative distribution of the ith failure in a particular primary location. The ith failure occurs before time t when: (1) the $(i-1)$th failure occurs at $x < t$ (2) and the next failure occurs before t. The next failure occurs before time t when the standby component fails: (a) during $[0, x]$ in the standby mode, or (b) during $[x, t]$ in the operation. Hence,

$$G_i(t) = \int_0^t dG_{i-1}(x)\left[F_{sb}(x) + R_{sb}(x)\cdot\left\{1 - R_{op}(t|x_{op})\right\}\right] \tag{1.12}$$

Further, we have

$$G_1(t) = F_{op}(t); \quad \text{and} \quad G_0(t) = 1 \tag{1.13}$$

All other calculations are similar to those for cold standby systems. It should be noted that Eq. (1.12) is not a standard convolution integral. Hence, we need to use a modified convolution function. The following MATLAB script can be used for solving TFR models when the underlying failure distribution is in the form of PHM. Here, *F*, *F1*, and *F2* represent $G_i(t)$, $G_{i-1}(t)$, and $F_{op}(t)$, respectively.

```
function F = TFRconvolution(F1, F2, psi)
  m = max(size(F1)); F = zeros(m,1);
  for i=2:m
    for j=2:i
      T1 = (1-F2(j))^(psi-1) * [F2(i)-F2(j)];
      T2 = (1-F2(j-1))^(psi-1) * [F2(i)-F2(j-1)];
      F(i) = F(i) + 0.5*[F1(j)-F1(j-1)]*(T1+T2);
    end
  end
end
```

Example 5 Same as Example 1 except the spares are in warm standby. The failure rate changes according to PHM and TFR models: $\psi_s = 0.25$.

Solution: The system reliability: $R(t) = 0.91067$. The CPU time is 0.036 s. The MATLAB script used for solving this example is same as the script used for Example 1 except the value of ψ_s (*psi*) is specified in the inputs. Further, the *convolution* function is replaced with the *TFRconvolution*.

Similarly, the following MATLAB script can be used for CE models when the distribution is in the form of AFTM.

```
function F = CEconvolution(F1, F2, phi)
  m = max(size(F1)); F = zeros(m,1);
  for i=2:m
    for j=2:i
     jeff = floor(phi * j);
     F(i) = F(i) + 0.5 * [F1(j) - F1(j-1)]
            * [F2(i-j+jeff+1) + F2(i-j+jeff+2)];
     end
  end
end
```

Example 6 Same as Example 5 except the failure rate changes according to AFTM and CE models: $\phi_s = 0.25$.

Solution: The system reliability: $R(t) = 0.96878$. The CPU time is 0.013 s. The MATLAB script used for solving this example is same as the script used for Example 5 (Example 1) except we used the *CEconvolution* in place of *TFRconvolution.* To produce results up to 5 decimal places in accuracy, we increased the value of m to 200.

1.6 Switch Failures

It is well known that systems or subsystems utilizing cold or warm standby redundancy require additional equipment or resources (hardware and software) to detect a failed component and to activate or switch on the redundant standby component. In this section, we show how to add the effects of switch-over failures to the reliability analysis. There are two basic scenarios for modeling switch failures:

- Switch Failure on Request (demand): At any time the switch is required, there is a constant probability, p_{sw}, that the switch will be successful, i.e., the switch failure probability is $(1 - p_{sw})$.
- Age-dependent switch failure: As any other standby component, the switch can fail when it is not used. In addition, in some applications, the switch-over mechanism may monitor the system performance continuously to detect a failure and to activate the standby components. In such cases, it is appropriate to model switch failures using continuous distributions such as Weibull.

1.6.1 Switch Failure on Request

In the proposed method, we calculate system reliability as the sum P_i values, where P_i is the probability of exactly i failures in the system. If there are exactly i failures in the system, the switch needs to perform its operation successfully for all i requests. This probability is equal to $(p_{sw})^i$. Hence, the system reliability is

$$R(t) = \sum_{i=0}^{n-k} (p_{sw})^i \; P_i \tag{1.14}$$

Example 7 Same as Example 1 except the switch success probability at each request is 0.95.

Solution: The system reliability: $R(t) = 0.85392$. The CPU time is 0.0037 s seconds. The MATLAB script used for solving this example is same as the script used for Example 1. However, the last line is replaced with

```
PSW = 0.95;
RSW = PSW.^[0:n-k];
Rel = sum(RSW .* P)
```

1.6.2 Age-Dependent Switch Failure

In this case, when switch is failed, the failure can occur at any time during the mission. Let $R_{sw}(t)$ be the time-dependent reliability function of the switch. To make a successful switch-over, the switch needs to be operational only up to the last switch-over time (say x), which is less than or equal to the mission time, t. Hence, the lower bound on the system reliability can easily be found by multiplying the switch reliability with the system reliability calculated assuming the perfect switch [29].

Example 8 Same as Example 1, except the switch failure distribution is Weibull with $\eta = 10000$ and $\beta = 2$.

Solution: The switch reliability for the entire mission time is 0.99005. Hence, the lower bound on the system reliability: $R(t) = 0.85392 \times 0.99005 = 0.98318$. The CPU time is 0.0032 s seconds. The required MATLAB script changes are minor and omitted.

The approximation used in Example 8 is valid when switch reliability is very high as compared to the reliability of the components. Now, we present an exact method to compute the system reliability considering the switch failure. Although the method is applicable for all types of systems considered in this chapter, we demonstrate the calculations using a k-out-of-n cold standby system with identical components.

Say the last failure in the system happened at time x in the primary location i, $i = 1, \cdots, k$. Hence, there are no failures during $[x, t]$ in any primary location. Therefore, the switch needs to be functional only up to time x. Let F be the failure distribution of the components (identical components). Define

$$G_i(t) = G_{i-1} * F(t); \quad \text{and} \quad G_1(t) = F(t) \tag{1.15}$$

Further, define