

Springer Series in Reliability Engineering

Ajit Kumar Verma
Srividya Ajit
Durga Rao Karanki

Reliability and Safety Engineering

Second Edition

 Springer

Springer Series in Reliability Engineering

Series editor

Hoang Pham, Piscataway, USA

More information about this series at <http://www.springer.com/series/6917>

Ajit Kumar Verma · Srividya Ajit
Durga Rao Karanki

Reliability and Safety Engineering

Second Edition

 Springer

Ajit Kumar Verma
ATØM
Stord/Haugesund University College
Haugesund
Norway

Durga Rao Karanki
Paul Scherrer Institute
Villigen PSI
Switzerland

Srividya Ajit
ATØM
Stord/Haugesund University College
Haugesund
Norway

ISSN 1614-7839 ISSN 2196-999X (electronic)
Springer Series in Reliability Engineering
ISBN 978-1-4471-6268-1 ISBN 978-1-4471-6269-8 (eBook)
DOI 10.1007/978-1-4471-6269-8

Library of Congress Control Number: 2015944434

Springer London Heidelberg New York Dordrecht
© Springer-Verlag London 2010, 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer-Verlag London Ltd. is part of Springer Science+Business Media
(www.springer.com)

To our gurus:

Bhagwan Sri. Sathya Sai Baba

Paramhansa Swami Sathyananda

Pujya Mata Amritanandaji

Smt. Vijaya and Sri. B. Jayaraman

Smt. Kasturi and Sri. C.S. Rao

To our parents:

Late Sri. K.P. Verma and Late Smt. S. Verma

Late Sri. B.C. Khanapuri

and Smt. V.B. Khanapuri

Sri. K. Manikya Rao and Smt. K. Anjali

Foreword

I take immense pleasure in writing the foreword for this very well-written book on “Reliability and Safety Engineering” that connects the bridge between the quintessential first principles of reliability with subsequent theoretical development of conceptual frameworks, and their relevance to practical realization of complex engineering systems. Interspersed with ample demonstrative examples and practical case studies, this is a self-contained exposition, written in a commendably lucid style.

Successful realization of sustainable and dependable products, systems, and services involves an extensive adoption of Reliability, Quality, Safety, and Risk-related procedures for achieving high assurance levels of performance; also pivotal are the management issues related to risk and uncertainty that govern the practical constraints encountered in their deployment. A need for a book that addresses these issues in comprehensive rigor without compromising on the underlying goal of succinct precision and simplicity has been long felt. And, I am sure this book has succeeded in achieving this fine balance.

This book is aimed at giving a conceptually sound introduction to reliability engineering and its allied interdisciplinary applications, especially for students at the graduate level. Building upon the first principles, this gradually evolves into a knowledge bank that can be relied on for gaining insights into the performance analysis of complex systems. With its equally precise explanations both in breadth and scope, researchers and practicing engineers alike will find this a valuable authority as a ready reference and a handbook. After a detailed introduction and models of reliability, risk, and uncertainty analysis, this elaborates on the applications through sufficient exposure to the varied fields of nuclear engineering, electronics engineering, mechanical engineering, software engineering, and power systems engineering.

I strongly recommend this book for its elegant discourse on the fundamentals of reliability and the much needed practical outlook it succeeds in constructing.

Hoang Pham
Distinguished Professor
Department of Industrial
and Systems Engineering
Rutgers, the State University of New Jersey
Piscataway, New Jersey
USA

Preface

Nothing lasts forever and so is the life of engineering systems. The consequence of failures of engineering system ranges from minor inconvenience to significant economic loss and deaths. Designers, manufacturers, and end users strive to minimize the occurrence and recurrence of failures. In order to minimize failures in engineering systems, it is essential to understand ‘why’ and ‘how’ failures occur. It is also important to know how often such failures may occur. If failures occur, inherent safety systems/measures must ensure the consequences of failures are minimal. Reliability deals with the failure concept, whereas safety deals with the consequences of failure. Reliability and Safety Engineering explores failures and consequences of failures to improve the performance of engineering systems. It plays a vital role in sectors such as chemical and process plants, nuclear facilities, and aerospace which can impose potential hazards. The main benefit of its application is to provide insights into design, performance, and environmental impacts, including the identification of dominant risk contributors and the comparison of options for reducing risk. In addition, it provides inputs to decisions on design and back fitting, system operation and maintenance, safety analysis and on regulatory issues.

Reliability and safety are the core issues to be addressed during the design, operation, and maintenance of engineering systems. LCC and sustainability are key to the understanding of risk and environmental impact of operation and maintenance of systems over the designed life leading to what one may call the ‘Green Reliability’. This book aims to present basic concepts and applications along with latest state of art methods in Reliability and Safety engineering. The book is organized as follows:

Chapter 1 introduces reliability and safety concepts and discusses basic terminology, resources, past, present challenges, and future needs. Chapter 2 provides a detailed review of probability and statistics essential for understanding the reliability and safety analysis methods discussed in the remaining chapters.

Chapter 3 discusses various system reliability modeling techniques such as Reliability Block Diagram, Fault Tree Analysis, and Markov modeling. Component (or basic event) reliability values are assumed to be available in analyzing system

level reliability. Repairable systems are also addressed and several practical examples are given. In Chap. 4, methods that focus on reliability analysis of complex systems, Monte Carlo simulation, and dynamic fault tree analysis are explained.

Conventional engineering fields, viz., Electronics Engineering, Software Engineering, Mechanical Engineering, and Structural Engineering, have their own terminology and methodologies in applying the reliability concepts. Though the basic objective is to improve the system effectiveness, approach in adopting reliability concepts is slightly case specific to each area. Chapters 5–8 present reliability terminology in the various above-mentioned conventional engineering fields. The current practices, resources, and areas of research are highlighted with respect to each field.

Chapter 9 focuses on maintenance of large engineering systems. Essentially this chapter covers two areas of maintenance, i.e., prioritizing of equipment and optimization in maintenance decision making.

Methodology for Probabilistic Safety Assessment (PSA) in general is addressed in Chap. 10. Various elements of PSA including common cause failure analysis, human reliability analysis, and importance measures are presented. Chapter 11 introduces dynamic methods in safety analysis with special emphasis on dynamic event tree analysis; the elements involved in the method and comparison among its implementation are also discussed. Practical applications of PSA in operation and maintenance activities of complex systems like nuclear power plants are discussed in Chap. 12.

Uncertainty is present in any reliability and safety calculation due to limitations in exactly assessing the parameters of the model. Creditability and practical usability of reliability and risk analysis results is enhanced by appropriate treatment of uncertainties. Various uncertainty propagation and analyzing methods including Monte Carlo simulation, Fuzzy arithmetic, Probability Bounds, and Dempster-Shafer theory are explained in Chaps. 13 and 14.

This book is useful for advanced undergraduate and postgraduate students in Nuclear Engineering, Aerospace Engineering, Industrial Engineering, Reliability and Safety Engineering, Systems Engineering, Applied Probability and Statistics, and Operations Research. The book is also suitable for one semester graduate course on Reliability and Safety Engineering in all conventional engineering branches like Civil, Mechanical, Chemical, Electrical, Electronics, and Computer Science. It will also be a valuable reference for practicing engineers, managers, and researchers involved in reliability and safety activities of complex engineering systems.

Acknowledgments

We have received excellent support from researchers at other institutes in the development and improvement of some of the chapters of the book. We are grateful for their help. The researchers (which also include our research students) of special mention are:

Mr. C. Hari Prasad (Mechanical Reliability), Lead Engineer, Stanadyne Corp., USA

Mr. P.A. Jadhav (Structural Reliability), Senior Scientist, BARC, India

Dr. R. Anil Nair (Software Reliability), Larsen & Toubro Infotech, Mumbai, India

Prof. Anil Rana (Maintenance of Large Engineering Systems), School of Maritime Studies, Suva, Fiji Islands

We are thankful to the reviewers for their constructive criticism and useful suggestions during the review of the chapters.

We express our sincere thanks to Mr. R.K. Saraf, Dr. V.V.S. Sanyasi Rao, Dr. V. Gopika, Dr. A.K. Ghosh, Mr. H.S. Kushwaha of Bhabha Atomic Research Centre (India), and Dr. Vinh N. Dang of Paul Scherrer Institute (Switzerland) for their valuable suggestions, continuous encouragement, and full moral support throughout our work.

We thank our students Mr. C. Dal Chand (IIT Kharagpur), Mr. M.P. Mangane (SCOE, Navi Mumbai), Mr. Sk. Rafi (SV University, Tirupati), Mr. V. Saklani (NFC, Hyderabad), Mr. A. Chandrakar (IIT Bombay/BARC), and Mr. Mike MacMillan (ETH-EPFL, Switzerland) for their support during the preparation of the manuscript.

Special thanks to Praveena, Harshita, Madhav, K. Prasad, U. Anka Lakshmi, V. Venkataratnam, V. Satyavani, Dr. M. Hari Prasad, T.V. Santosh, Karimulla, Dharma Raju, Dr. Shirish Chodanker, Dr. Mallipudi, and René Gruebe for their love and cooperation.

We are grateful to Prof. Hoang Pham for his suggestions and encouragement. We thank Mr. P. Clarie and P. Udhayakumar for his great support in managing the production of this book.

March 2015

Ajit Kumar Verma
Srividya Ajit
Durga Rao Karanki

Contents

1	Introduction	1
1.1	Need for Reliability and Safety Engineering	1
1.2	Exploring Failures	2
1.3	Improving Reliability and Safety	3
1.4	Definitions and Explanation of Some Relevant Terms	4
1.4.1	Quality	4
1.4.2	Reliability	5
1.4.3	Maintainability	5
1.4.4	Availability	6
1.4.5	Risk and Safety	6
1.4.6	Probabilistic Risk Assessment/Probabilistic Safety Assessment	7
1.5	Resources	7
1.6	History	8
1.7	Present Challenges and Future Needs for the Practice of Reliability and Safety Engineering	12
	References	15
2	Basic Reliability Mathematics	19
2.1	Classical Set Theory and Boolean Algebra	19
2.1.1	Operations on Sets	19
2.1.2	Laws of Set Theory	21
2.1.3	Boolean Algebra	21
2.2	Concepts of Probability Theory	22
2.2.1	Axioms of Probability	24
2.2.2	Calculus of Probability Theory	24
2.2.3	Random Variables and Probability Distributions	28
2.3	Reliability and Hazard Functions	31

2.4	Distributions Used in Reliability and Safety Studies	34
2.4.1	Discrete Probability Distributions	34
2.4.2	Continuous Probability Distributions	40
2.4.3	Summary	59
2.5	Failure Data Analysis	59
2.5.1	Nonparametric Methods	59
2.5.2	Parametric Methods	63
	References	72
3	System Reliability Modeling	75
3.1	Reliability Block Diagram (RBD)	75
3.1.1	Procedure for System Reliability Prediction Using RBD	75
3.1.2	Different Types of Models	78
3.1.3	Solving RBD	87
3.2	Markov Models	92
3.2.1	Elements of Markov Models	92
3.3	Fault Tree Analysis	104
3.3.1	Procedure for Carrying Out Fault Tree Analysis	104
3.3.2	Elements of Fault Tree	107
3.3.3	Evaluations of Fault Tree	109
3.3.4	Case Study	115
	References	122
4	Reliability of Complex Systems	123
4.1	Monte Carlo Simulation	123
4.1.1	Analytical versus Simulation Approaches for System Reliability Modeling	123
4.1.2	Elements of Monte Carlo Simulation	125
4.1.3	Repairable Series and Parallel System	127
4.1.4	Simulation Procedure for Complex Systems	132
4.1.5	Increasing Efficiency of Simulation	139
4.2	Dynamic Fault Tree Analysis	140
4.2.1	Dynamic Fault Tree Gates	141
4.2.2	Modular Solution for Dynamic Fault Trees	143
4.2.3	Numerical Method	144
4.2.4	Monte Carlo Simulation	147
	References	158
5	Electronic System Reliability	161
5.1	Importance of Electronic Industry	161
5.2	Various Components Used and Their Failure Mechanisms	162
5.2.1	Resistors	162
5.2.2	Capacitors	162

- 5.2.3 Inductors 163
- 5.2.4 Relays 163
- 5.2.5 Semiconductor Devices 163
- 5.2.6 Microcircuits (ICs) 164
- 5.3 Reliability Prediction of Electronic Systems 165
 - 5.3.1 Parts Count Method 166
 - 5.3.2 Parts Stress Method 166
- 5.4 PRISM 167
- 5.5 Sneak Circuit Analysis (SCA) 169
 - 5.5.1 Definition of SCA. 169
 - 5.5.2 Network Tree Production 170
 - 5.5.3 Topological Pattern Identification 170
- 5.6 Case Study. 171
 - 5.6.1 Total Failure Rate. 172
- 5.7 Physics of Failure Mechanisms of Electronic Components . . . 174
 - 5.7.1 Physics of Failures 174
 - 5.7.2 Failure Mechanisms for Resistors 174
 - 5.7.3 Failure Mechanisms for Capacitor. 176
 - 5.7.4 MOS Failure Mechanisms 176
 - 5.7.5 Field Programmable Gate Array 180
- References. 182

- 6 Software Reliability 183**
 - 6.1 Introduction to Software Reliability. 183
 - 6.2 Past Incidences of Software Failures in Safety
Critical Systems 184
 - 6.3 The Need for Reliable Software 187
 - 6.4 Difference Between Hardware Reliability
and Software Reliability. 188
 - 6.5 Software Reliability Modeling 189
 - 6.5.1 Software Reliability Growth Models 191
 - 6.5.2 Black Box Software Reliability Models 191
 - 6.5.3 White Box Software Reliability Models. 192
 - 6.6 How to Implement Software Reliability 192
 - 6.7 Emerging Techniques in Software Reliability
Modeling—Soft Computing Technique 199
 - 6.7.1 Need for Soft Computing Methods 201
 - 6.7.2 Environmental Parameters 201
 - 6.7.3 Anil-Verma Model 208
 - 6.8 Future Trends of Software Reliability 215
 - References. 216

7	Mechanical Reliability	219
7.1	Reliability Versus Durability	220
7.2	Failure Modes in Mechanical Systems	221
7.2.1	Failures Due to Operating Load	222
7.2.2	Failure Due to Environment	226
7.3	Reliability Circle.	226
7.3.1	Specify Reliability	228
7.3.2	Design for Reliability	231
7.3.3	Test for Reliability	245
7.3.4	Maintain the Manufacturing Reliability	250
7.3.5	Operational Reliability	252
	References.	255
8	Structural Reliability	257
8.1	Deterministic versus Probabilistic Approach in Structural Engineering	257
8.2	The Basic Reliability Problem	258
8.2.1	First Order Second Moment (FOSM) Method.	259
8.2.2	Advanced First Order Second Moment Method (AFOSM)	263
8.3	First Order Reliability Method (FORM).	264
8.4	Reliability Analysis for Correlated Variables	268
8.4.1	Reliability Analysis for Correlated Normal Variables	269
8.4.2	Reliability Analysis for Correlated Non-normal Variables	270
8.5	Second Order Reliability Methods (SORM)	271
8.6	System Reliability.	282
8.6.1	Classification of Systems	282
8.6.2	Evaluation of System Reliability.	284
	References.	292
9	Maintenance of Large Engineering Systems	293
9.1	Introduction	293
9.2	Peculiarities of a Large Setup of Machinery	294
9.3	Prioritizing the Machinery for Maintenance Requirements	296
9.3.1	Hierarchical Level of Machinery.	299
9.3.2	FMECA (Failure Mode Effect and Criticality Analysis)	301
9.4	Maintenance Scheduling of a Large Setup of Machinery	309
9.4.1	Introduction	309
9.4.2	Example	311