

ENGINEERING SYSTEMS RELIABILITY, SAFETY, AND MAINTENANCE

AN INTEGRATED APPROACH



B.S. DHILLON



CRC Press
Taylor & Francis Group

Engineering Systems Reliability, Safety, and Maintenance An Integrated Approach

B.S. Dhillon



CRC Press

Taylor & Francis Group

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2017 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works

International Standard Book Number-13: 978-1-4987-8163-3 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Names: Dhillon, B.S. (Balbir S.), 1947- author.
Title: Engineering systems reliability, safety, and maintenance : an integrated approach / B.S. Dhillon.
Description: Boca Raton : Taylor & Francis, a CRC title, part of the Taylor & Francis imprint, a member of the Taylor & Francis Group, the academic division of T&F Informa, plc, [2017] | Includes bibliographical references and index.
Identifiers: LCCN 2016040251 | ISBN 9781498781633 (hardback : alk. paper) | ISBN 9781498781640 (ebook)
Subjects: LCSH: Engineering systems. | Reliability (Engineering) | System safety. | Engineering systems--Maintenance and repair.
Classification: LCC TA168 .D52 2017 | DDC 620.001/1--dc23
LC record available at <https://lcn.loc.gov/2016040251>

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the CRC Press Web site at
<http://www.crcpress.com>



Printed and bound in Great Britain by
TJ International Ltd, Padstow, Cornwall

Engineering Systems
Reliability, Safety,
and Maintenance
An Integrated Approach

*This book is affectionately dedicated to the memory
of late family friend Narinder Singh.*

Preface

Today, engineering systems are an important element of the world economy, and each year, billions of dollars are spent to develop, manufacture, operate, and maintain various types of engineering systems around the globe. Many of these systems are highly sophisticated and contain millions of parts. For example, a Boeing jumbo 747 is made up of approximately 4.5 million parts including fasteners. Needless to say, reliability, safety, and maintenance of systems such as this have become more important than ever before. Global competition and other factors are forcing manufacturers to produce highly reliable, safe, and maintainable engineering products.

It means that there is a definite need for reliability, safety, and maintenance professionals to work closely during design and other phases. To achieve this goal, it is essential that they have an understanding of each other's discipline to a certain degree. At present, to the best of the author's knowledge, there is no book that covers the topics of reliability, safety, and maintenance within its framework. It means, at present, to gain knowledge of each other's specialties, these specialists must study various books, reports, or articles on each of the topics in question. This approach is time consuming and rather difficult because of the specialized nature of the material involved.

Thus, the main objective of this book is to combine these three topics into a single volume and to eliminate the need to consult many diverse sources in obtaining basic and up-to-date desired information on the topics. The sources of most of the material presented are given in the reference section at the end of each chapter. This will be useful to readers if they desire to delve more deeply into a specific topic or area. The book contains a chapter on mathematical concepts and another chapter on the basics of reliability, safety, and maintenance considered useful to understand the contents of subsequent chapters. Furthermore, another chapter is devoted to methods considered useful to analyze the reliability, safety, and maintenance of engineering systems.

The topics covered in the book are treated in such a manner that the reader will require no previous knowledge to understand the contents. At appropriate places, the book contains examples along with their solution, and there are numerous problems at the end of each chapter to test the reader's comprehension in the area. An extensive list of publications dating from 1926 to 2013, directly or indirectly on engineering systems reliability, safety, and maintenance, is provided at the end of this book to give readers a view of the intensity of developments in the area.

The book is composed of 11 chapters. Chapter 1 presents the need for and the historical developments in reliability, safety, and maintenance; engineering systems reliability/safety/maintenance-related facts, figures, and

examples; important terms and definitions; and useful sources for obtaining information on reliability, safety, and maintenance. Chapter 2 reviews mathematical concepts considered useful to understand subsequent chapters. Some of the topics covered in the chapter are Boolean algebra laws, probability properties, statistical distributions, and useful mathematical definitions.

Chapter 3 presents various introductory aspects of reliability, safety, and maintenance. Chapter 4 presents a number of methods considered useful to analyze engineering systems reliability, safety, and maintenance. These methods are fault tree analysis, the Markov method, failure modes and effect analysis, probability tree analysis, technique of operations review, hazard and operability analysis, interface safety analysis, maintenance program effectiveness evaluation approach for managers, and indices for maintenance management analysis. Chapter 5 is devoted to computer, Internet, and robot system reliability. Some of the topics covered in the chapter are computer failure sources, computer-related faults classifications and reliability measures, fault masking, Internet failure examples, a method for automating fault detection in Internet services, categories of robot failures, and robot reliability measures and analysis methods.

Chapter 6 is devoted to transportation system failures and human errors in transportation systems and covers topics such as defects in vehicle parts and categories of vehicle failures, rail weld failures and defects, rail tanker failure modes and causes of failures, mechanical failure-related aviation accidents, ship failures, typical human error occurrence areas in railway operation, types of pilot-controller communication-related errors, methods for reducing the manning impact on shipping system reliability, and common driver errors. Chapter 7 presents various important aspects of software, robot, and transportation system safety. Some of the topics covered in the chapter are software safety assurance program; software hazard analysis methods; robot safety-related problems causing weak points in planning, design, and operation; robot safeguard methods; truck and bus safety-related issues; railroad tank safety; analysis of world airline accidents; and marine accidents.

Chapter 8 is devoted to medical and mining systems safety. Some of the topics covered in the chapter are medical system safety-related facts and figures, types of medical device/system safety, safety in medical device/system life cycle, methods for conducting medical device/system safety analysis, mining equipment/systems safety-related facts and figures, causes for mining equipment-related accidents, mining equipment maintenance-related accidents, and methods for performing mining equipment/system safety analysis. Chapter 9 is devoted to software maintenance and reliability-centered maintenance and covers topics such as software maintenance problems and maintenance types, software maintenance methods, software maintenance costing, reliability centered maintenance goals and principles, reliability-centered maintenance process, elements of reliability-centered maintenance,

and reliability-centered maintenance program effectiveness measurement indicators.

Chapter 10 presents various important aspects of maintenance safety and human error in aviation and power plant maintenance. Some of the topics covered in the chapter are maintenance safety-related facts, figures, and examples; factors responsible for dubious safety reputation in performing maintenance tasks and reasons for safety-related problems in maintenance; maintenance personnel safety; guidelines for equipment/system designers for improving safety in maintenance; causes of human error in aviation maintenance; common human errors in aircraft maintenance tasks; methods for performing aircraft maintenance error analysis; human error causes in power plant maintenance and most susceptible maintenance tasks to human error in power generation; and guidelines to reduce and prevent human error in power generation maintenance. Finally, Chapter 11 presents six mathematical models for performing engineering system reliability, safety, and maintenance analysis.

This book will be useful to many individuals, including design engineers; system engineers, reliability and safety professionals; maintenance engineers; engineering administrators; graduate and senior undergraduate students in the area of engineering; researchers and instructors of reliability, safety, and maintenance; and engineers-at-large.

I am deeply indebted to many individuals, including family members, colleagues, friends, and students for their invisible inputs. The invisible contributions of my children are also appreciated. Last, but not least, I thank my wife Rosy, my other half and friend, for typing this entire book and for her timely help in proofreading.

B.S. Dhillon
Ottawa, Ontario

Author

B.S. Dhillon, PhD, is a professor of engineering management in the Department of Mechanical Engineering at the University of Ottawa, Ottawa, Canada. He has served as a chairman/director of the Mechanical Engineering Department/Engineering Management Program for more than 10 years at the same institution. He is the founder of the probability distribution named *Dhillon distribution/law/model* by statistical researchers in their publications around the world. He has published more than 70 single-authored and 160 coauthored journal articles and 152 submissions to conference proceedings on reliability engineering, maintainability, safety, engineering management, and other topics. He is or has been on the editorial boards of 12 international scientific journals. In addition, Dr. Dhillon has written 44 books on various aspects of healthcare, engineering management, design, reliability, safety, and quality published by Wiley (1981), Van Nostrand (1982), Butterworth (1983), Marcel Dekker (1984), and Pergamon (1986). His books are used in over 100 countries, and many of them are translated into languages such as German, Russian, Chinese, and Persian (Iranian).

He has served as the general chairman of two international conferences on reliability and quality control held in Los Angeles and Paris in 1987. Dr. Dhillon has also served as a consultant to various organizations and bodies and has many years of experience in the industrial sector. He has lectured in over 50 countries, including keynote addresses at various international scientific conferences held in North America, Europe, Asia, and Africa. In March 2004, Dr. Dhillon was a distinguished speaker at the Conference/Workshop on Surgical Errors (sponsored by the White House Health and Safety Committee and the Pentagon), held at the Capitol (Washington, DC).

Dr. Dhillon attended the University of Wales, where he earned a BS in electrical and electronic engineering and an MS in mechanical engineering. He earned his PhD in industrial engineering from the University of Windsor.

Contents

Preface.....	xv
Author.....	xix
1. Introduction.....	1
1.1 Background.....	1
1.2 Engineering System Reliability, Safety, and Maintenance Facts, Figures, and Examples.....	2
1.3 Terms and Definitions.....	4
1.4 Useful Sources for Obtaining Information on Reliability, Safety, and Maintenance.....	5
1.4.1 Organizations.....	5
1.4.2 Journals and Magazines.....	6
1.4.3 Data Information Sources.....	6
1.4.4 Standards and Reports.....	7
1.4.5 Books.....	8
1.4.6 Conference Proceedings.....	9
1.5 Scope of the Book.....	9
References.....	10
2. Reliability, Safety, and Maintenance Mathematics.....	13
2.1 Introduction.....	13
2.2 Median, Arithmetic Mean, and Mean Deviation.....	13
2.2.1 Median.....	14
2.2.2 Arithmetic Mean.....	14
2.2.3 Mean Deviation.....	15
2.3 Boolean Algebra Laws.....	15
2.4 Probability Definition and Properties.....	17
2.5 Useful Mathematical Definitions.....	18
2.5.1 Cumulative Distribution Function.....	18
2.5.2 Probability Density Function.....	19
2.5.3 Expected Value.....	20
2.5.4 Laplace Transform.....	21
2.5.5 Final Value Theorem Laplace Transform.....	22
2.6 Solving First-Order Differential Equations with Laplace Transforms.....	23
2.7 Statistical Distributions.....	25
2.7.1 Binomial Distribution.....	25
2.7.2 Exponential Distribution.....	26

2.7.3	Rayleigh Distribution	27
2.7.4	Weibull Distribution.....	27
2.7.5	Bathtub Hazard Rate Curve Distribution	28
	References	29
3.	Reliability, Safety, and Maintenance Basics	33
3.1	Introduction	33
3.2	Bathtub Hazard Rate Curve	33
3.3	General Reliability Formulas	35
3.3.1	Probability (or Failure) Density Function.....	35
3.3.2	Hazard Rate (or Time-Dependent Failure Rate) Function.....	36
3.3.3	General Reliability Function	36
3.3.4	Mean Time to Failure	38
3.4	Reliability Configurations	39
3.4.1	Series Configuration.....	39
3.4.2	Parallel Configuration.....	42
3.4.3	<i>k</i> -out-of- <i>n</i> Configuration	44
3.4.4	Standby System	46
3.4.5	Bridge Configuration.....	47
3.5	The Need for Safety and the Role of Engineers in Regard to Safety	49
3.6	Product Hazard Classifications.....	50
3.7	Safety Management Principles and Product Safety Organization Tasks	52
3.8	Accident Causation Theories.....	53
3.8.1	Human Factors Accident Causation Theory.....	53
3.8.2	Domino Accident Causation Theory	54
3.9	Facts and Figures Related to Engineering Maintenance.....	56
3.10	Maintenance Engineering Objectives	56
3.11	Preventive Maintenance.....	57
3.11.1	Preventive Maintenance Elements and Principle for Selecting Items for Preventive Maintenance	57
3.11.2	Steps for Developing Preventive Maintenance Program ...	58
3.11.3	Preventive Maintenance Measures	59
3.11.4	Preventive Maintenance Benefits and Drawbacks.....	60
3.12	Corrective Maintenance	61
3.12.1	Types of Corrective Maintenance.....	61
3.12.2	Corrective Maintenance Steps, Downtime Components, and Time Reduction Strategies at System Level.....	62
3.12.3	Corrective Maintenance Measures.....	63
	References	65

4. Methods for Performing Reliability, Safety, and Maintenance	
Analysis of Engineering Systems	69
4.1 Introduction	69
4.2 Fault Tree Analysis	69
4.2.1 Probability Evaluation of Fault Trees.....	72
4.2.2 FTA Advantages and Disadvantages.....	74
4.3 Markov Method.....	74
4.4 Failure Modes and Effect Analysis.....	78
4.5 Probability Tree Analysis.....	79
4.6 Technique of Operation Review	82
4.7 Hazard and Operability Analysis	83
4.8 Interface Safety Analysis	84
4.8.1 Classification I: Flow Relationships	85
4.8.2 Classification II: Physical Relationships	85
4.8.3 Classification III: Functional Relationships	85
4.9 Maintenance Program Effectiveness Evaluation Approach for Managers.....	86
4.10 Indices for Maintenance Management Analysis.....	86
4.10.1 Category I: Broad Indices.....	87
4.10.2 Category II: Specific Indices	88
References	92
5. Computer, Internet, and Robot System Reliability	95
5.1 Introduction	95
5.2 Computer System Reliability Issue-Related Factors and Computer Failure Sources.....	96
5.3 Computer-Related Fault Classifications and Reliability Measures	97
5.4 Fault Masking.....	98
5.4.1 Triple Modular Redundancy.....	99
5.4.2 N-Modular Redundancy.....	100
5.5 Internet Failure Examples and Reliability-Related Observations.....	101
5.6 Internet Outage Classifications	102
5.7 A Method for Automating Fault Detection in Internet Services and Models for Conducting Internet Reliability and Availability Analyses.....	103
5.7.1 Mathematical Model I.....	104
5.7.2 Mathematical Model II.....	106
5.8 Robot Reliability-Related Survey Results and Effectiveness Dictating Factors	108
5.9 Categories of Robot Failures and Their Causes and Corrective Measures	109

5.10	Robot Reliability Measures and Analysis Methods.....	111
5.10.1	Robot Reliability Measures	111
5.10.1.1	Mean Time to Robot-Related Problems.....	111
5.10.1.2	Mean Time to Robot Failure	112
5.10.1.3	Robot Reliability	113
5.10.2	Robot Reliability Analysis Methods	114
5.10.2.1	Fault Tree Analysis.....	114
5.10.2.2	Failure Modes and Effect Analysis.....	114
5.10.2.3	Parts Count Method.....	115
5.10.2.4	Markov Method.....	115
	References	116
6.	Transportation System Failures and Human Error in Transportation Systems.....	119
6.1	Introduction	119
6.2	Defects in Vehicle Parts and Categories of Vehicle Failures.....	119
6.3	Rail Weld Failures and Defects.....	121
6.4	Classifications of Road and Rail Tanker Failure Modes and Causes of Failures and Factors Influencing the Nature of Failure Consequences	122
6.5	Mechanical Failure-Related Aviation Accidents and Their Examples	124
6.6	Ship Failures and Their Common Causes.....	125
6.7	Railway System Human Error-Related Facts and Figures and Typical Human Error Occurrence Areas in Railway Operation.....	126
6.8	Aviation System Human Error-Related Facts and Figures and Types of Pilot–Controller Communication-Related Errors ...	128
6.9	Organization-Related Factors in Commercial Aviation Accidents with Respect to Pilot Error and Recommendations for Reducing Pilot–Controller Communication Errors.....	130
6.10	Shipping System Human Error-Related Facts and Figures	131
6.11	Marine Industry-Related Human Factors Issues and Methods for Reducing the Manning Impact on Shipping System Reliability	132
6.12	Road Transportation System Human Error-Related Facts and Figures and Common Driver Errors	133
6.13	Classifications and Ranking of Driver Errors.....	134
	References	136
7.	Software, Robot, and Transportation System Safety.....	139
7.1	Introduction	139
7.2	Software Potential Hazards and Software Risk and Safety Classifications	140