

# DESIGN RELIABILITY

Fundamentals and Applications

**B. S. Dhillon**

Department of Mechanical Engineering  
University of Ottawa  
Ottawa, Ontario, Canada



CRC Press

Boca Raton London New York Washington, D.C.

Acquiring Editor: Cindy Carelli  
Project Editor: Susan Fox  
Cover design: Dawn Boyd

**Library of Congress Cataloging-in-Publication Data**

Dhillon, B. S.

Design reliability : fundamentals and applications / B.S. Dhillon.

p. cm.

Includes bibliographical references (p.

ISBN 0-8493-1465-8 (alk. paper)

1. Engineering design. 2. Reliability (Engineering). I. Title.

TA174.D4929 1999

620'.0042--dc21

99-28211

CIP

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage or retrieval system, without prior permission in writing from the publisher.

The consent of CRC Press LLC does not extend to copying for general distribution, for promotion, for creating new works, or for resale. Specific permission must be obtained in writing from CRC Press LLC for such copying.

Direct all inquiries to CRC Press LLC, 2000 Corporate Blvd., N.W., Boca Raton, Florida 33431.

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

© 1999 by CRC Press LLC

No claim to original U.S. Government works

International Standard Book Number 0-8493-1465-8

Library of Congress Card Number 99-28211

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

Printed on acid-free paper

## *Dedication*

---

*This book is affectionately dedicate to my mother  
**Udham Kaur.***

---

# Preface

Today at the dawn of the twenty-first century, we are designing and building new complex and sophisticated engineering systems for use not only on Earth but to explore other heavenly bodies. Time is not that far off when humankind will permanently reside on other planets and explore stars outside our solar system. Needless to say, the reliability of systems being used for space explorations and for use on Earth is becoming increasingly important because of factors such as cost, competition, public demand, and usage of untried new technology. The only effective way to ensure reliability of engineering systems is to consider the reliability factor seriously during their design.

Over the years as engineering systems have become more complex and sophisticated, the knowledge in reliability engineering has also increased tremendously and it has specialized into areas such as human reliability, software reliability, mechanical reliability, robot reliability, medical device reliability, and reliability and maintainability management.

Even though there are a large number of texts already directly or indirectly related to reliability engineering, there is still a need for an up-to-date book emphasizing design reliability with respect to specialized, application, and related areas. Thus, the main objective of writing this book is to include new findings as well as tailor the text in such a manner so that it effectively satisfies the needs of modern design reliability. Therefore, this book is written to meet this challenge and its emphasis is on the structure of concepts rather than on mathematical rigor and minute details. However, the topics are treated in such a manner that the reader needs no previous knowledge to understand them. Also, the source of most of the material presented in the book is given in references if the reader wishes to delve deeper into particular topics. The book contains a large number of examples along with their solutions, and at the end of each chapter there are numerous problems to test reader comprehension.

The book is composed of 17 chapters. Chapter 1 presents the historical aspect of reliability engineering, the need of reliability in engineering design, reliability in the product design process, and important terms and definitions, and information sources. Chapter 2 reviews mathematics essential to understanding subsequent chapters. Fundamental aspects of engineering design and reliability management are presented in Chapter 3. As the failure data collection and analysis are considered the backbone of reliability engineering, Chapter 4 presents many associated aspects. Chapter 5 presents many basic reliability evaluation and allocation methods. However, the emphasis of the chapter is on the basic reliability evaluation methods. Chapters 6 and 7 describe in detail two most widely used methods (i.e., failure modes and effect analysis and fault tree analysis, respectively) to evaluate engineering design with respect to reliability. Chapter 8 presents two important topics of

reliability engineering: common-cause failures and three state devices. Two specialized areas of reliability, mechanical reliability and human reliability, are discussed in Chapters 9 and 10, respectively.

Chapter 11 presents the topics of reliability testing and growth essential in the design phase of an engineering system. Chapters 12 through 14 present three application areas of reliability, i.e., reliability in computer systems, robot reliability, and medical device reliability, respectively. In particular, the emphasis of Chapter 12 is on computer software reliability. Chapter 15 presents important aspects of design maintainability and reliability centered maintenance. Chapters 16 and 17 describe three topics directly or indirectly related to design reliability: total quality management, risk assessment, and life cycle costing.

The book is intended primarily for senior level undergraduate and graduate students, professional engineers, college and university level teachers, short reliability course instructors and students, researchers, and engineering system design managers.

The author is deeply indebted to many individuals including colleagues, students, friends, and reliability and maintainability professionals for their invisible inputs and encouragement at the moment of need. I thank my children Jasmine and Mark for their patience and intermittent disturbances leading to desirable coffee and other breaks. And last, but not least, I thank my boss, friend, and wife, Rosy, for typing various portions of this book and other related materials, and for her timely help in proofreading.

B.S. Dhillon  
Ottawa, Ontario

---

# The Author

**B.S. Dhillon, Ph.D.**, is a professor of Mechanical Engineering at the University of Ottawa. He has served as a Chairman/Director of Mechanical Engineering Department/Engineering Management Program for 11 years at the same institution. He has published over 260 articles on Reliability and Maintainability Engineering and on related areas. In addition, he has written 20 books on various aspects of system reliability, safety, human factors, design, and engineering management published by Wiley (1981), Van Nostrand (1982), Butterworth (1983), Marcel Dekker (1984), and Pergamon (1986) among others. His books on Reliability have been translated into several languages including Russian, Chinese, and German. He has served as General Chairman of two international conferences on reliability and quality control held in Los Angeles and Paris in 1987. Also, he is or has been on the editorial board of five international journals.

Dr. Dhillon is a recipient of the American Society of Quality Control Austin J. Bonis Reliability Award, the Society of Reliability Engineers' Merit Award, the Gold Medal of Honor (American Biographical Institute), and Faculty of Engineering Glinski Award for excellence in Reliability Engineering Research. He is a registered Professional Engineer in Ontario and is listed in the *American Men and Women of Science*, *Men of Achievements*, *International Dictionary of Biography*, *Who's Who in International Intellectuals*, and *Who's Who in Technology*.

At the University of Ottawa, he has been teaching reliability and maintainability for over 18 years. Dr. Dhillon attended the University of Wales where he received a B.S. in electrical and electronic engineering and an M.S. in mechanical engineering. He received a Ph.D. in industrial engineering from the University of Windsor.

---

# Table of Contents

## **CHAPTER 1: Introduction**

- 1.1 Reliability History
- 1.2 Need of Reliability in Product Design
- 1.3 Reliability in the Product Design Process
- 1.4 Reliability Specialized and Application Areas
- 1.5 Terms and Definitions
- 1.6 Reliability Information Sources
- 1.7 Military and Other Reliability Documents
- 1.8 Problems
- 1.9 References

## **CHAPTER 2: Design Reliability Mathematics**

- 2.1 Introduction
- 2.2 Boolean Algebra Laws
- 2.3 Probability Properties
- 2.4 Useful Definitions
  - 2.4.1 Definition of Probability
  - 2.4.2 Cumulative Distribution Function
  - 2.4.3 Probability Density Function
  - 2.4.4 Reliability Function
  - 2.4.5 Hazard Rate Function
  - 2.4.6 Laplace Transform Definition
  - 2.4.7 Laplace Transform: Final-Value Theorem
  - 2.4.8 Expected Value
- 2.5 Probability Distributions
  - 2.5.1 Binomial Distribution
  - 2.5.2 Poisson Distribution
  - 2.5.3 Exponential Distribution
  - 2.5.4 Rayleigh Distribution
  - 2.5.5 Weibull Distribution
  - 2.5.6 General Distribution
  - 2.5.7 Normal Distribution
- 2.6 Hazard Rate Models
  - 2.6.1 Exponential Distribution
  - 2.6.2 Rayleigh Distribution
  - 2.6.3 Weibull Distribution
  - 2.6.4 General Distribution
  - 2.6.5 Normal Distribution

- 2.7 Partial Fraction Method and Equation Roots
  - 2.7.1 Partial Fraction Method
  - 2.7.2 Equation Roots
- 2.8 Differential Equations
- 2.9 Problems
- 2.10 References

### **CHAPTER 3: Engineering Design and Reliability Management**

- 3.1 Introduction
- 3.2 Engineering Design
  - 3.2.1 Design Failures and Their Common Reasons
  - 3.2.2 The Design Process and Functions
  - 3.2.3 The Design Team and Member Responsibilities
  - 3.2.4 Design Reviews
  - 3.2.5 Design Engineer and Design Review Board Chairman
  - 3.2.6 Designing for Reliability and Design Reliability Check List Items
  - 3.2.7 Design Liability
- 3.3 Reliability Management
  - 3.3.1 General Management Reliability Program Related Responsibilities and Guiding Force Associated Facts for an Effective Reliability Program
  - 3.3.2 Military Specification Guidelines for Developing Reliability Programs and a Procedure to Establish Reliability Goals
  - 3.3.3 Reliability and Maintainability Management Tasks in the Product Life Cycle
  - 3.3.4 Documents and Tools for Reliability Management
  - 3.3.5 Reliability Auditing and Pitfalls in Reliability Program Management
  - 3.3.6 Reliability and Maintainability Engineering Departments and Their Responsibilities
  - 3.3.7 Reliability Manpower
- 3.4 Problems
- 3.5 References

### **CHAPTER 4: Failure Data Collection and Analysis**

- 4.1 Introduction
- 4.2 Failure Data Uses
- 4.3 Failure Data Collection Sources in Equipment Life Cycle and Quality Control Data
- 4.4 Failure Reporting and Documentation System Design Guidelines and Failure Data Collection Forms
- 4.5 External Failure Data Sources
- 4.6 Failure Data For Selective Items and Tasks
- 4.7 Hazard Plotting Method
  - 4.7.1 Hazard Plotting Mathematical Theory

- 4.8 Underlying Distribution Determination Tests
  - 4.8.1 Bartlett Test
  - 4.8.2 General Exponential Test
  - 4.8.3 Kolmogorov-Smirnov Test
- 4.9 Maximum Likelihood Estimation Method
  - 4.9.1 Exponential Distribution
  - 4.9.2 Normal Distribution
  - 4.9.3 Weibull Distribution
- 4.10 Problems
- 4.11 References

## **CHAPTER 5: Basic Reliability Evaluation and Allocation Techniques**

- 5.1 Introduction
- 5.2 Bathtub Hazard Rate Curve
- 5.3 General Reliability Analysis Related Formulas
  - 5.3.1 Failure Density Function
  - 5.3.2 Hazard Rate Function
  - 5.3.3 General Reliability Function
  - 5.3.4 Mean Time to Failure
- 5.4 Reliability Networks
  - 5.4.1 Series Network
  - 5.4.2 Parallel Network
  - 5.4.3 r-out-of-n Network
  - 5.4.4 Standby Redundancy
  - 5.4.5 Bridge Network
- 5.5 Reliability Evaluation Methods
  - 5.5.1 Network Reduction Approach
  - 5.5.2 Decomposition Approach
  - 5.5.3 Delta-Star Method
  - 5.5.4 Parts Count Method
  - 5.5.5 Markov Method
- 5.6 Reliability Allocation
  - 5.6.1 Hybrid Method
  - 5.6.2 Failure Rate Allocation Method
- 5.7 Problems
- 5.8 References

## **CHAPTER 6: Failure Modes and Effect Analysis**

- 6.1 Introduction
- 6.2 Terms and Definitions
- 6.3 Types of FMEA and Their Associated Benefits
  - 6.3.1 Design-Level FMEA
  - 6.3.2 System-Level FMEA
  - 6.3.3 Process-Level FMEA

- 6.4 Steps for Performing FMEA
  - 6.4.1 Define System and Its Associated Requirements
  - 6.4.2 Establish Ground Rules
  - 6.4.3 Describe the System and Its Associated Functional Blocks
  - 6.4.4 Identify Failure Modes and Their Associated Effects
  - 6.4.5 Prepare Critical Items List
  - 6.4.6 Document the Analysis
- 6.5 Criticality Assessment
  - 6.5.1 RPN Technique
  - 6.5.2 Military Standard Technique
- 6.6 FMECA Information Needs, Data Sources, and Users
- 6.7 FMEA Implementation Related Factors and General Guidelines
- 6.8 Advantages of FMEA
- 6.9 Problems
- 6.10 References

## **CHAPTER 7: Fault Tree Analysis**

- 7.1 Introduction
- 7.2 FTA Purposes and Prerequisites
- 7.3 Fault Tree Symbols
- 7.4 Fundamental Approach to FTA
- 7.5 Boolean Algebra Rules
- 7.6 Analytical Developments of Basic Gates, Repeated Fault Events, and Minimal Cut Sets
  - 7.6.1 Repeated Fault Events
  - 7.6.2 Algorithm for Obtaining Minimal Cut Sets
- 7.7 Probability Evaluation of Fault Trees with Repairable and Nonrepairable Components
  - 7.7.1 Probability Evaluation of Fault Trees with Non-Repairable Components
  - 7.7.2 Probability Evaluation of Fault Trees with Repairable Components
- 7.8 Fault Tree Duality and FTA Approach Benefits and Drawbacks
- 7.9 Problems
- 7.10 References

## **CHAPTER 8: Common Cause Failures and Three State Devices**

- 8.1 Introduction
- 8.2 Common Cause Failures
  - 8.2.1 Block Diagram Method
  - 8.2.2 Fault Tree Method
  - 8.2.3 Markov Method
- 8.3 Three State Devices
  - 8.3.1 Reliability Evaluation of a Series Network
  - 8.3.2 Reliability Evaluation of a Parallel Network

- 8.3.3 Reliability Optimization of a Series Network
- 8.3.4 Reliability Optimization of a Parallel Network
- 8.4 Problems
- 8.5 References

## **CHAPTER 9: Mechanical Reliability**

- 9.1 Introduction
- 9.2 Reasons for the Discipline of Mechanical Reliability and Mechanical Failure Modes
- 9.3 General and Gear Failure Causes
- 9.4 Safety Factor and Safety Margin
  - 9.4.1 Safety Factor
  - 9.4.2 Safety Margin
- 9.5 “Design by Reliability” Methodology and Stress-Strength Models
- 9.6 Mellin Transform Method
- 9.7 Failure Rate Models
  - 9.7.1 Break System Failure Rate Model
  - 9.7.2 Clutch System Failure Rate Model
  - 9.7.3 Pump Failure Rate Model
  - 9.7.4 Filter Failure Rate Model
  - 9.7.5 Compressor System Failure Rate Model
  - 9.7.6 Bearing Failure Rate Model
- 9.8 Failure Data Sources for Mechanical Parts
- 9.9 Optimum Models for Mechanical Equipment Replacement or Maintenance
  - 9.9.1 Equipment Replacement Model
  - 9.9.2 Equipment Maintenance Model
- 9.10 Problems
- 9.11 References

## **CHAPTER 10: Human Reliability in Engineering Systems**

- 10.1 Introduction
- 10.2 Terms and Definitions
- 10.3 Human Error Occurrence Examples and Studies
- 10.4 Human Error Occurrence Classification and Its Types and Causes
- 10.5 Human Performance and Stress
  - 10.5.1 Stress Factors and Operator Stress Characteristics
- 10.6 Human Performance Reliability in Continuous Time and Mean Time to Human Error (MTTHE) Measure
- 10.7 Human Reliability Evaluation Methods
  - 10.7.1 Probability Tree Method
  - 10.7.2 Fault Tree Method
  - 10.7.3 Markov Method
- 10.8 Human Reliability Markov Modeling

- 10.8.1 Reliability Analysis of a System with Human Error
- 10.8.2 Reliability Analysis of a Human Performing a Time-Continuous Task Under Fluctuating Environment
- 10.9 Human Error Data
  - 10.9.1 Specific Human Error Data Banks and Sources
  - 10.9.2 Brief Description of Selected Human Error Data Banks
  - 10.9.3 Human Error Data for Selective Tasks
- 10.10 Problems
- 10.11 References

## **CHAPTER 11: Reliability Testing and Growth**

- 11.1 Introduction
- 11.2 Reliability Testing
  - 11.2.1 Reliability Test Classifications
  - 11.2.2 Success Testing
  - 11.2.3 Confidence Interval Estimates for Mean Time Between Failures
  - 11.2.4 Accelerated Life Testing
- 11.3 Reliability Growth
  - 11.3.1 Reliability Growth Program
  - 11.3.2 Reliability Growth Process Evaluation Approaches
- 11.4 Reliability Growth Models
  - 11.4.1 Duane Model
  - 11.4.2 Army Material System Analysis Activity (AMSAA) Model
- 11.5 Problems
- 11.6 References

## **CHAPTER 12: Reliability in Computer Systems**

- 12.1 Introduction
- 12.2 Terms and Definitions
- 12.3 Hardware Reliability Vs. Software Reliability
- 12.4 Computer Failure Causes
- 12.5 Software Life Cycle Phases and Associated Error Sources
- 12.6 Software Reliability Improvement Methods
  - 12.6.1 Reliable Software Design Methods
  - 12.6.2 Fault-Tolerant Software Design Methods
  - 12.6.3 Formal Methods
  - 12.6.4 Testing
- 12.7 Software Reliability Assessment Methods
  - 12.7.1 Analytical Approaches
  - 12.7.2 Software Metrics
  - 12.7.3 Software Reliability Models
- 12.8 Fault Masking
  - 12.8.1 Triple Modular Redundancy (TMR)
  - 12.8.2 N-Modular Redundancy (NMR)

- 12.9 Problems
- 12.10 References

### **CHAPTER 13: Robot Reliability and Safety**

- 13.1 Introduction
- 13.2 Robot Safety
  - 13.2.1 Robot Accidents
  - 13.2.2 Robot Hazards and Safety Problems
  - 13.2.3 Safety Considerations in Robot Life Cycle
  - 13.2.4 Robot Safeguard Approaches
  - 13.2.5 Human Factor Issues in Robotic Safety
- 13.3 Robot Reliability
  - 13.3.1 Causes and Classifications of Robot Failures
  - 13.3.2 Robot Reliability Measures
  - 13.3.3 Robot Reliability Analysis and Prediction Methods
  - 13.3.4 Reliability and Availability Analyses of a Robot System Failing with Human Error
  - 13.3.5 Reliability Analysis of a Repairable/Non-Repairable Robot System
- 13.4 Problems
- 13.5 References

### **CHAPTER 14: Medical Device Reliability**

- 14.1 Introduction
- 14.2 Facts and Figures, Government Control and Liability
- 14.3 Medical Electronic Equipment Classification
- 14.4 Medical Device Recalls
- 14.5 Medical Device Design Quality Assurance
  - 14.5.1 Organizations
  - 14.5.2 Specifications
  - 14.5.3 Design Review
  - 14.5.4 Reliability Assessment
  - 14.5.5 Parts/Materials Quality Control
  - 14.5.6 Software Quality Control
  - 14.5.7 Design Transfer
  - 14.5.8 Labeling
  - 14.5.9 Certification
  - 14.5.10 Test Instrumentation
  - 14.5.11 Manpower
  - 14.5.12 Quality Monitoring Subsequent to the Design Phase
- 14.6 Human Error Occurrence and Related Human Factors
  - 14.6.1 Control/Display Related Human Factors Guidelines
  - 14.6.2 Medical Device Maintainability Related Human Factor Problems

- 14.6.3 Human Factor Pointers for Already Being Used/to be Purchased Medical Devices
- 14.6.4 Issues in Considering the Need for, and Performance of Human Factors Analysis and Testing of Medical Devices
- 14.7 Medical Device Software
  - 14.7.1 Software Testing for Improving Medical Device Safety
  - 14.7.2 Cardioplegia Delivery System Software Reliability Program Core Elements and Software Safety Improvement with Redundancy
- 14.8 Sources for Adverse Medical Device Reportable Events and Failure Investigation Documentation
- 14.9 A small Instrument Manufacturer's Approach to Produce Reliable and Safe Medical Devices
- 14.10 Aerospace and Medical Equipment Reliability and Reliability Approach Comparisons
- 14.11 Guidelines for Reliability and Other Professionals Associated with Health Care
- 14.12 Problems
- 14.13 References

## **CHAPTER 15: Design Maintainability and Reliability Centered Maintenance**

- 15.1 Introduction
- 15.2 Design Maintainability: Maintainability Need and Relationship Between Reliability and Maintainability
  - 15.2.1 Maintainability and Availability Analyses During Design and Development Phase and Maintainability Design Characteristics
  - 15.2.2 Design Reviews
  - 15.2.3 Maintainability Measures
  - 15.2.4 Maintainability Design Guidelines and Common Maintainability Design Errors
- 15.3 Reliability Centered Maintenance
  - 15.3.1 Traditional Maintenance, RCM, and Questions for Selecting Assets for RCM
  - 15.3.2 RCM Process Related Maintenance Task Classification Areas and Steps
  - 15.3.3 RCM Advantages
  - 15.3.4 Reasons for the RCM Methodology Application Failures
- 15.4 Problems
- 15.5 References

## **CHAPTER 16: Total Quality Management and Risk Assessment**

- 16.1 Introduction
- 16.2 TQM

- 16.2.1 Traditional Quality Assurance Vs. TQM
- 16.2.2 TQM Principles and Elements
- 16.2.3 TQM Contributors
- 16.2.4 TQM Methods
- 16.2.5 Designing for Quality and Goals for TQM Process Success
- 16.2.6 Deming's "Deadly Diseases" of American Management and Common Errors During the Starting Quality Initiative Phase
- 16.3 Risk Assessment
  - 16.3.1 Risk Analysis Role and Required Expertise Areas
  - 16.3.2 Risk Analysis Objectives in Hazardous System Life Cycle
  - 16.3.3 Risk Analysis Process Steps
  - 16.3.4 Risk Analysis Techniques for Engineering Systems
  - 16.3.5 Advantages of Risk Analysis
- 16.4 Problems
- 16.5 References

## **CHAPTER 17: Life Cycle Costing**

- 17.1 Introduction
- 17.2 Reasons and Uses of Life Cycle Costing and Required Inputs
- 17.3 Life Cycle Costing Steps and Activities
- 17.4 Skill Requirements Areas of a Life Cycle Costing Analyst and His/Her Associated Professionals
- 17.5 Life Cycle Costing Program Evaluation Areas and Life Cycle Cost Estimate Report
- 17.6 Time Dependent Formulas for Life Cycle Cost Analysis
  - 17.6.1 Single Payment Compound Amount Formula
  - 17.6.2 Single Payment Present Value Formula
  - 17.6.3 Uniform Periodic Payment Present Value Formula
  - 17.6.4 Uniform Periodic Payment Future Amount Formula
- 17.7 Life Cycle Cost Estimation Models
  - 17.7.1 General Life Cycle Cost Estimation Models
  - 17.7.2 Specific Life Cycle Cost Estimation Models
- 17.8 Cost Estimation Models
  - 17.8.1 Cost-Capacity Model
  - 17.8.2 Motor Operation Cost Estimation Model
  - 17.8.3 Corrective Maintenance Labor Cost Estimation Model
- 17.9 Life Cycle Costing Data
  - 17.9.1 Cost Data Sources
- 17.10 Life Cycle Costing Advantages and Disadvantages Resistance Factors and Associated Important Points
- 17.11 Problems
- 17.12 References