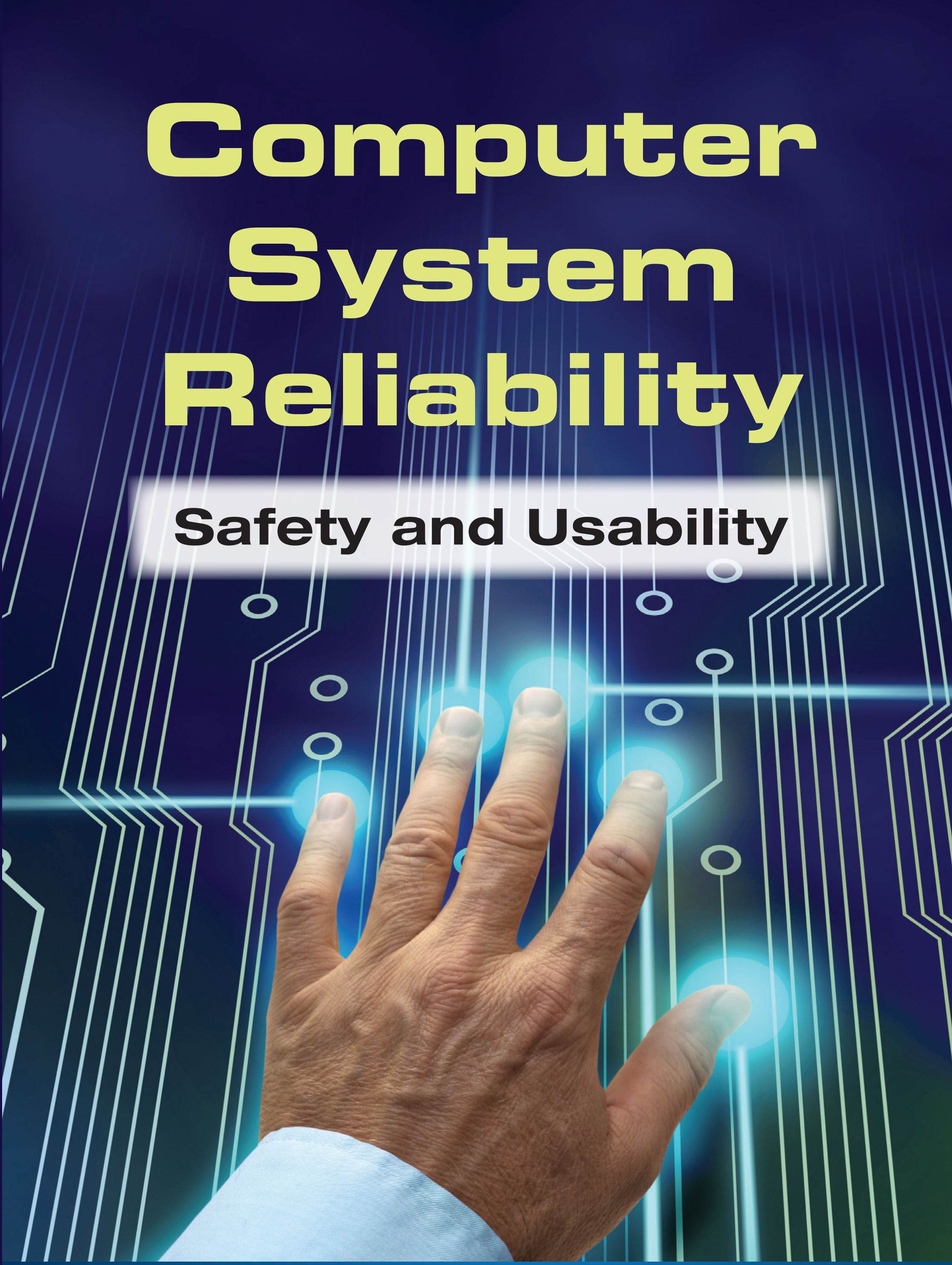
Computer System Reliability

Safety and Usability



B. S. DHILLON

CRC Press
Taylor & Francis Group

Computer System Reliability

Safety and Usability

Computer System Reliability

Safety and Usability

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

Version Date: 20130410

International Standard Book Number-13: 978-1-4665-7313-0 (eBook - PDF)

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.

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

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

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

This book is affectionately dedicated to all my Scythian ancestors

for their firm belief in number 40. (This is my 40th book!)

Contents

Preface

Computer systems are increasingly being used at an alarming rate for various purposes. They have become an important element of the world economy because billions of dollars are spent each year to develop, manufacture, operate, and maintain various types of computer systems around the globe. Their reliability, safety, and usability have become an important concern because of problems such as high cost, wrong decisions and actions, and accidental deaths. For example, a study performed by the National Institute of Standards in 2002 found that software defects alone cost the United States economy about $59 billion annually, i.e., around 0.6% of its gross domestic product (GDP).

Computer system reliability, safety, and usability have become more important than ever before. In response, a large number of journal and conference proceedings' articles on various aspects of computer system reliability, safety, and usability have been published over the years. However, to the best of the author's knowledge, there is no specific book on the topic. This causes a great deal of difficulty for information seekers because they have to consult many different and diverse sources.

Thus, the main objective of this book is to combine computer system reliability, safety, usability, and other related topics into a single volume and to eliminate the need to consult many different and diverse sources to obtain desired information. The book contains a chapter on mathematical concepts considered necessary to understand the material presented in subsequent chapters.

The topics covered in the volume are treated in such a manner that the reader will require no previous specialized knowledge to understand the contents. At appropriate places, the book contains examples along with their solutions, and at the end of each chapter there are numerous problems to test the reader's comprehension. The sources of most of the materials presented are given in the reference section at the end of each chapter. An extensive list of publications dating from 1967 to 2011—directly or indirectly related to computer system reliability, safety, and usability—is provided at the end of this book to give readers a view of the intensity of the developments in this area.

The book is composed of 11 chapters. Chapter 1 presents various introductory aspects of computer system reliability including safety; usability-related facts, figures, terms, and definitions; and sources for obtaining useful information on computer system reliability, safety, and usability. Chapter 2 reviews mathematical concepts considered useful to understanding subsequent chapters. Some of the topics covered in the chapter are arithmetic mean and mean deviation, Boolean algebra laws, probability properties, probability distributions, and useful definitions.

Chapter 3 presents various introductory aspects of reliability, safety, and usability. Chapter 4 presents computer system reliability basics. Some of the topics covered in this chapter are hardware reliability versus software reliability, major sources of computer failures, issues in computer system reliability, fault classifications, fault masking, and computer reliability measures. Chapter 5 is devoted to software reliability assessment and improvement methods. A number of methods grouped under seven categories are presented in this chapter.

Chapters 6 and 7 present various important aspects of software quality and human error and software bugs in computer systems, respectively. Chapter 8 is devoted to software safety and Internet reliability. It covers topics such as software safety classifications; potential software hazards; software safety assurance programs; software hazard analysis methods; Internet facts, figures, and examples; Internet outage classifications; and models for performing Internet reliability and availability analysis.

Chapter 9 covers various important aspects of software usability, including the need to consider usability during the software development phase, the software usability engineering process, software usability inspection methods, software usability test methods, and guidelines for conducting software usability testing. Chapter 10 is devoted to web usability. Some of the topics covered in the chapter are web usability facts and figures, common web design errors, web page design, tools for evaluating web usability, and questions to evaluate the effectiveness of website message communications. Finally, Chapter 11 presents various important aspects of computer system life-cycle costing.

This book will be useful to many individuals, including computer engineers, software engineers, design engineers, system engineers, human factors engineers, and other professionals involved with computers and the Internet—engineering managers and administrators; reliability and other engineers-at-large; researchers and instructors involved with computer systems; and graduate and senior undergraduate students in computer engineering, software engineering, system engineering, computer science, etc.

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

B. S. Dhillon
Ottawa, Ontario

About the Author

Dr. B. S. Dhillon is a professor of engineering management in the Department of Mechanical Engineering at the University of Ottawa. He has served as a chairman/director of the Mechanical Engineering Department/Engineering Management Program for over ten years at the same institution. He is the founder of the probability distribution named the "Dhillon Distribution/Law/Model" by statistical researchers in their publications around the world. He has published over 364 (i.e., 217 [70 single authored and 147 coauthored] journal and 147 conference proceedings) articles on reliability engineering, maintainability, safety, engineering management, etc. He is or has been on the editorial boards of eleven international scientific journals. In addition, Dr. Dhillon has written forty books on various aspects of health care, engineering management, design, reliability, safety, and quality published by Wiley (1981), Van Nostrand (1982), Butterworth (1983), Marcel Dekker (1984), Pergamon (1986), etc. His books are being used in over one hundred countries, and many of them are translated into languages such as German, Russian, Chinese, and Persian (Iranian).

He has served as general chairman of two international conferences on reliability and quality control held in Los Angeles and Paris in 1987. Professor Dhillon has also served as a consultant to various organizations and bodies and has many years of experience in the industrial sector. At the University of Ottawa, he has been teaching reliability, quality, engineering management, design, and related areas for over thirty-three years, and he has also lectured in over fifty 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 White House Health and Safety Committee and Pentagon) held on Capitol Hill (One Constitution Avenue, Washington, DC).

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

1

Introduction

1.1 Background

Nowadays, computer systems have become an important element of the world economy, and each year billions of dollars are spent to develop, manufacture, operate, and maintain various types of computer systems around the globe. Their reliability, safety, and usability have become an important concern because of problems such as high cost, wrong decisions and actions, and accidental deaths. For example, a study conducted by the National Institute of Standards and Technology in 2002 found that software defects alone cost the U.S. economy about $59 billion annually, i.e., around 0.6% of its gross domestic product (GDP) [1].

The history of computer system reliability can be traced back to the late 1940s and 1950s to the works of Shannon [2], Hamming [3], Von Neumann [4], and Moore and Shannon [5]. For example, in 1956 Von Neumann [4] proposed the triple modular redundancy (TMR) scheme (nowadays widely used in computers) to improve system reliability. In 1965, Pierce published a book entitled *Failure Tolerant Design* [6]. This was probably the first book concerned with computer system reliability.

Over the years, a large number of publications related to computer system reliability have appeared. A comprehensive list of useful publications is provided in the appendix to this book.

1.2 Facts, Figures, and Examples

Some facts, figures, and examples concerned with computer system reliability are as follows:

- In 2002, a study commissioned by the National Institute of Standards and Technology (NIST) reported that software errors cost the U.S. economy about $59 billion annually [1].

- As per Kletz [7] and Herrman [8], the number of people killed due to computer system malfunctions worldwide up to the end of 1992 was somewhere between 1,000 and 3,000.
- The Internet has grown from four hosts in 1969 to over 147 million hosts and thirty-eight sites in 2002, and in 2001 there were over 52,000 Internet-related incidents and failures [9, 10].
- In 2000, the Internet economy generated about $830 billion in revenues in the United States [9–11].
- National Aeronautics and Space Administration's (NASA's) Saturn V Launch computer (circa 1964) had a mean time to failure (MTTF) of 25,000 hours [12–14].
- As per Landauer [15], an average software program contains about forty design flaws that impair the ability of workers to use it effectively.
- A pilot set the heading in a plane's computer-controlled inertial navigation system as 270° instead of 027°; the plane ran out of fuel and caused twelve fatalities [16].
- In 1966, European Space Agency's US$1 billion prototype Ariane 5 rocket was destroyed just forty seconds after launch because of a bug in the onboard guidance computer program [17].
- On April 25, 1997, a misconfigured router of a Virginia service provider injected an incorrect map into the global Internet. In turn, this caused network congestion, instability, and overload of Internet router table memory that ultimately shut down the majority of the main Internet backbones for about 2 hours [18].
- In 1963, a software error resulted in the incapacitation of a North American Air Defense Command (NORAD) exercise [19].
- As per Myers and Robson [20], 50% to 80% of all source code development accounts, directly or indirectly, for the user interface.
- A software error in the code controlling the Therac-25 radiation therapy machine caused many deaths in the 1980s [21].
- A computer opened the vent valve on the wrong vessel due to a software error, and fourteen tons of carbon dioxide were vented and lost [16, 22].
- As per Kuhn [23], a number of studies conducted over the years indicate that the reliability of Internet paths falls far short of the 99.999% availability expected in the public-switched telephone network (PSTN).
- In 1981, the launching of the first U.S. space shuttle was postponed for about twenty minutes prior to the scheduled launching time due to a software error [24].
- Some small-scale studies performed in 1994 and 2000 clearly reported that the probability of encountering a major routing pathology along a path (with respect to the Internet) was roughly 1.5% to 3.3% [25, 26].

- In 1991, a software fault caused a MIM-104 Patriot (surface-to-air missile system) to fail to intercept an incoming Iraqi Scud missile that caused twenty-eight American fatalities in Saudi Arabia [27].
- On August 14, 1998, a misconfigured Key Internet Database server mistakenly directed all queries for Internet machines with names ending in ".net" to the wrong secondary database server. This problem resulted in the failure of most connections to ".net" Internet web servers and other end stations for many hours [28].
- A case study performed in regard to Internet outages over a period of one year (November 1997–November 1998) categorized the outages under the following classifications (along with their occurrence percentages in parentheses) [28]:
  - Software problems (1.3%)
  - Malicious attacks (1.5%)
  - Sluggish/congestion (4.6%)
  - Unknown/undetermined/no problem (5.6%)
  - Miscellaneous (5.9%)
  - Routing problem (6.1%)
  - Interface down (6.2%)
  - Hardware problem (6.2%)
  - Unreachable (12.6%)
  - Fiber cut/circuit carrier problem (15.3%)
  - Power outage (16%)
  - Maintenance (16.2%)

1.3 Terms and Definitions

This section presents some useful terms and definitions concerned with various aspects of computer system reliability [14, 29–41].

Accident. An event that involves damage to a certain system/unit that suddenly disrupts the potential or current system/unit output.

Availability. The probability that an item/system is available for use or application when needed.

Debugging. The process of isolating and eradicating errors.

Downtime. The time period during which the item/system is not in a condition to perform its specified mission.

Failure. The inability of an item/system to perform its stated function.

Fault. An attribute that adversely affects the reliability of an item.

Fault-tolerant computing. The ability to execute specified algorithms successfully, irrespective of computer hardware malfunctions and software errors.

Hazard. The source of energy and the physiological and behavioral factors that, when uncontrolled, lead to harmful occurrences.

Human error. The failure to carry out a specified task (or the performance of a prohibited action) that could result in disruption of scheduled operations or damage to property.

Human factors. A body of scientific facts concerning the human characteristics (the term includes all biomedical and psychosocial considerations).

Mission time. The time during which the item/system is carrying out its stated mission.

Redundancy. The existence of more than one means to carry out a specified function.

Reliability. The probability that a system/unit/item will perform its assigned mission satisfactorily for the stated period of time when used according to the specified conditions.

Safety. Conservation of human life and the prevention of damage to systems/units/items as per mission-stated requirements.

Software error. A conceptual clerical or syntactic discrepancy that leads to one or more faults in the software.

Software reliability. The probability of a given software functioning for a specified time interval, without an error, when used according to the designed conditions on the stated machine.

Usability. The quality of an interactive system with respect to factors such as user satisfaction, ease of learning, and ease of use.

Usability evaluation. Any analytical or empirical study directed at assessing or understanding the usability of an interactive system/product.

User-centered design. An early and continuous involvement of potential users in the product design process.

User interface. The physical representations and procedures to view and interact with the product/system functionality.

1.4 Sources To Obtain Information Related to Computer System Reliability, Safety, and Usability

There are many different sources for obtaining information related to computer system reliability, safety, and usability. These include journals and magazines, conference proceedings, industry standards and handbooks, data sources, and books. Some of these sources are listed in the following subsections [14, 29, 30]:

1.4.1 Journals and Magazines

ACM Transactions on Computer-Human Interaction (TOCHI)
Human-Computer Interaction
IEEE Transactions on Reliability
Interacting with Computers
International Journal of Industrial Ergonomics
International Journal of Man-Machine Studies
International Journal of Reliability, Quality, and Safety Engineering
Journal of Safety Research
National Safety News
Professional Safety
Quality and Reliability Engineering
Reliability Engineering and System Safety
Reliability Review
Safety Science
User Modeling and User-Adopted Interaction (UMUAI)

1.4.2 Conference Proceedings

Proceedings of the Annual Conference on Computer Assurance (USA)
Proceedings of the Annual Reliability and Maintainability Symposium (USA)
Proceedings of the Annual Reliability Engineering Conference for the Electric Power Industry (USA)
Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (USA)
Proceedings of the International Conference on Reliability and Exploitation of Computer Systems (Poland)
Proceedings of the Symposium on Reliability in Electronics (Hungary)

1.4.3 Standards and Handbooks

ANSI/AIAA R-103, *Recommended Practice for Software Reliability*, American National Standards Institute (ANSI), New York.