Springer Series in Reliability Engineering

Series Editor

Professor Hoang Pham
Department of Industrial and Systems Engineering
Rutgers, The State University of New Jersey
96 Frelinghuysen Road
Piscataway, NJ 08854-8018
USA

Other titles in this series

The Universal Generating Function in Reliability Analysis and Optimization
Gregory Levitin

Warranty Management and Product Manufacture
D.N.P. Murthy and Wallace R. Blischke

Maintenance Theory of Reliability
Toshio Nakagawa

System Software Reliability
Hoang Pham

Reliability and Optimal Maintenance
Hongzhou Wang and Hoang Pham

Applied Reliability and Quality
B.S. Dhillon

Shock and Damage Models in Reliability Theory
Toshio Nakagawa

Risk Management
Terje Aven and Jan Erik Vinnem

Satisfying Safety Goals by Probabilistic Risk Assessment
Hiromitsu Kumamoto

Offshore Risk Assessment (2nd Edition)
Jan Erik Vinnem

The Maintenance Management Framework
Adolfo Crespo Márquez

Human Reliability and Error in Transportation Systems
B.S. Dhillon

Complex System Maintenance Handbook
D.N.P. Murthy and Khairy A.H. Kobbacy

Recent Advances in Reliability and Quality in Design
Hoang Pham

Product Reliability
D.N.P. Murthy, Marvin Rausand and Trond Østerås

Mining Equipment Reliability, Maintainability, and Safety
B.S. Dhillon

Advanced Reliability Models and Maintenance Policies
Toshio Nakagawa

Justifying the Dependability of Computer-based Systems
Pierre-Jacques Courtois

Reliability and Risk Issues in Large Scale Safety-critical Digital Control Systems
Poong Hyun Seong

Failure Rate Modeling for Reliability and Risk
Maxim Finkelstein

The Complexity of Proceduralized Tasks
Jinkyun Park

Risks in Technological Systems
Göran Grimvall, Åke J. Holmgren, Per Jacobsson and Torbjörn Thedéen

Maintenance for Industrial Systems
Riccardo Manzini, Alberto Regattieri, Hoang Pham and Emilio Ferrari

Mine Safety
B.S. Dhillon

The Complexity of Proceduralized Tasks
Jinkyun Park

Ajit Kumar Verma · Srividya Ajit
Durga Rao Karanki

Reliability and Safety Engineering

Springer

Ajit Kumar Verma, PhD
Indian Institute of Technology
Department of Electrical Engineering
Powai
400076 Mumbai
India
akvmanas@gmail.com

Srividya Ajit, PhD
Indian Institute of Technology
Department of Civil Engineering
Powai
400076 Mumbai
India
asvidya@civil.iitb.ac.in

Durga Rao Karanki, PhD
Paul Scherrer Institute
Nuclear Energy and Safety Research
Department
5232 Villigen PSI
Switzerland
durga_k_rao@yahoo.com

ISSN 1614-7839
ISBN 978-1-84996-231-5
e-ISBN 978-1-84996-232-2
DOI 10.1007/978-1-84996-232-2

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2010932022

Cover design: deblik, Berlin, Germany

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To our parents:
Sri. K.P. Verma and Smt. S. Verma
Sri. B.C. Khanapuri and Smt. V.B. Khanapuri
Sri. K. Manikya Rao and Smt. K. Anjali
and
To our gurus:
Bhagwan Sri. Satya Sai Baba
Paramhamsa Swami Satyananda Saraswati
Mata Amritananda

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. The need for a book that addresses these issues in comprehensive rigor without compromising on the underlining goal of succinct precision and simplicity has long been 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, Professor and Chairman
Department of Industrial and Systems Engineering
Rutgers, the State University of New Jersey
Piscataway, New Jersey, USA

Preface

Nothing lasts forever, and so it is with engineering systems. The consequence of failures of engineering systems 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 regulatory issues.

Reliability and safety are the core issues to be addressed during the design, operation, and maintenance of engineering systems. Life-cycle costs 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 "green reliability." This book aims to present basic concepts and applications along with the latest state-of-the-art methods in reliability and safety engineering. The book is organized as follows.

Chapter 1 introduces reliability and safety concepts and discusses basic terminology, evolution, applications, limitations, and resources. Chapter 2 provides a detailed review of probability and statistics essential in understanding the reliability and safety analysis methods discussed in the remaining chapters.

Chapter 3 discusses various system reliability modeling techniques such as reliability block diagrams, fault tree analysis, Markov modeling, and Monte Carlo simulation. 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.

Conventional engineering fields, *viz.*, electronics engineering, software engineering, mechanical engineering, structural engineering, and power systems engineering, have their own terminology and methodologies in applying reliability concepts. Though the basic objective is to improve the system effectiveness, the approach in adopting reliability concepts is slightly case-specific to each area. Chapters 4 to 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.

Methodology for probabilistic safety assessment (PSA) in general is addressed in Chapter 9. Various elements of PSA including common-cause failure analysis, human reliability analysis and importance measures are presented. Practical applications of PSA in operation and maintenance activities of complex systems like nuclear power plants are discussed in Chapter 10.

Uncertainty is present in any reliability and safety calculations due to limitations in exactly assessing the parameters of the model. The problem of acknowledging and treating uncertainty is vital for practical usability of these results. Various uncertainty propagation and analysis methods including Monte Carlo simulation, fuzzy arithmetic, probability bounds, and Dempster–Shafer theory are explained in Chapter 11.

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 courses on reliability and safety engineering in all conventional engineering branches like civil, mechanical, chemical, electrical, and electronics, as well as 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.

Mumbai
December 2009

Ajit K. Verma
A Srividya
Durga R. Karanki

Acknowledgments

We have received excellent support from researchers at other institutes in the development and improvement of some 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, Engineer (Mechanical Reliability), Stanadyne Corp., USA;
Mr. P.A. Jadhav, Scientist (Structural Reliability), BARC, Mumbai;
Mr. V. Vijay Venu, Researcher (Power Systems Reliability), IIT Bombay;
Dr. R. Anil Nair, Software Engineer, Larsen & Toubro Infotech, Mumbai.

We are thankful to 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, and Mr. H.S. Kushwaha of Bhabha Atomic Research Centre, Mumbai 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), and Mr. A. Chandrakar (IIT Bombay) for their support during the preparation of the manuscript.

Special thanks to Mrs. V.L. Praveena, Ms. K. Harshita, Mr. K. Prasad, Mrs. U. Lakshmi, Mr. V. Venkataratnam, Mrs. V. Satyavani, Mr. M. Hari Prasad, Mr. T.V. Santosh, Mr. Sk. Karimulla, and Mr. N. Dharma Raju for their assistance and cooperation.

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

Mumbai
December 2009

Ajit K. Verma
A. Srividya
Durga R. Karanki

Contents

Chapter 1
Introduction

1.1 Need for Reliability and Safety Engineering

Failure is inevitable for everything in the real world, and engineering systems are no exception. The impact of failures varies from minor inconvenience and costs to personal injury, significant economic loss, and death. Examples of major accidents are those at the Three Mile Island and Chernobyl nuclear plants, the gas leak at the Bhopal pesticide plant, and the Challenger space shuttle explosion. Causes of failure include bad engineering design, faulty manufacturing, inadequate testing, human error, poor maintenance, improper use, and lack of protection against excessive stress. 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. Reliability deals with the failure concept, whereas safety deals with the consequences after the failure. Inherent safety systems/measures ensure the consequences of failures are minimal. Reliability and safety engineering attempts to study, characterize, measure, and analyze the failure, repair, and consequences of failure of systems in order to improve their operational use by increasing their design life, eliminating or reducing the likelihood of failures and risky consequences, and reducing downtime, thereby increasing available operating time at the lowest possible life cycle costs.

The need for higher reliability and safety is further emphasized by the following factors:

- increased product complexity;
- accelerated growth of technology;
- public awareness or customer requirement;
- modern safety and liability laws;
- competition in the market;
- past system failures;

- cost of failure, damage, and warranty;
- safety considerations with undesirable consequences.

Reliability and safety engineering has a wide number of applications in all conventional engineering fields, and the following are worth mentioning:

- design evaluation;
- identification of critical components;
- determination of derating/factor of safety;
- environmental comparisons;
- redundancy requirements;
- regulatory requirements;
- establishment of preventive maintenance programs;
- repair and spare-part management;
- replacement and residual life estimations;
- safety management;
- life cycle cost analysis.

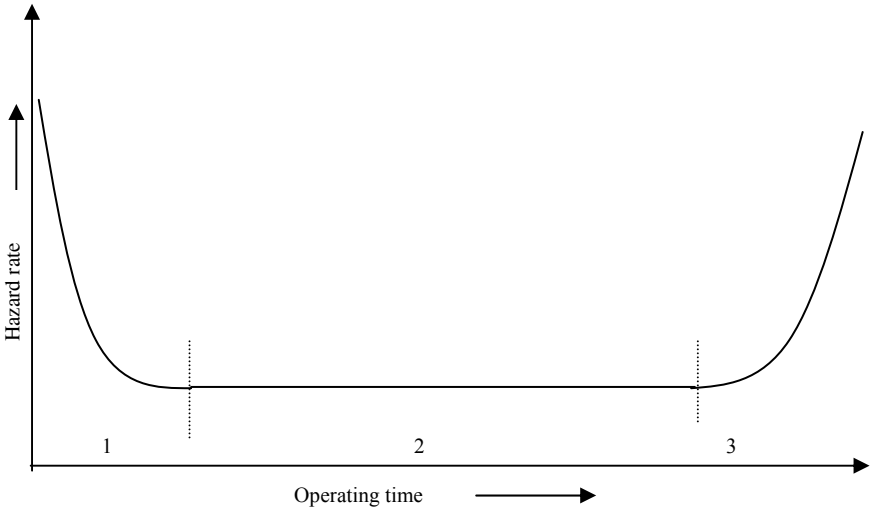

Figure 1.1 Bath-tub curve

1.2 Failures Inevitable

Nothing can last forever, so, in long mission times, the repair and replacement of failed parts can be of critical importance. There are many causes of failures of engineering systems; a few examples are:

- design errors;
- poor manufacturing techniques and lack of quality control;
- substandard components;
- lack of protection against over stresses;
- poor maintenance;
- aging/wear-out;
- human errors.

There are three stages of failures in the life of a product: early stage, operating stage, and wear-out stage as shown in Figure 1.1, which is called the life characteristic curve, or bath-tub curve because of its shape:

1. early failure region (infant mortality);
2. useful life region (hazard rate constant);
3. wear-out failure region.

When the equipment is put into use for the first time any inherently weak parts normally fail soon. Thus early hazard rate is very high. But once the weak parts are replaced the hazard rate falls and is fairly constant, and finally the hazard rate rises again as parts start to wear out.

Region 1 suggests that no item be used unless it has survived this period. Some reputable manufacturers sell only those components which have survived this period. Region 2 is the useful life period where hazard rate is governed by chance failure and is fairly constant. Region 3 indicates that the component should be replaced or scrapped.

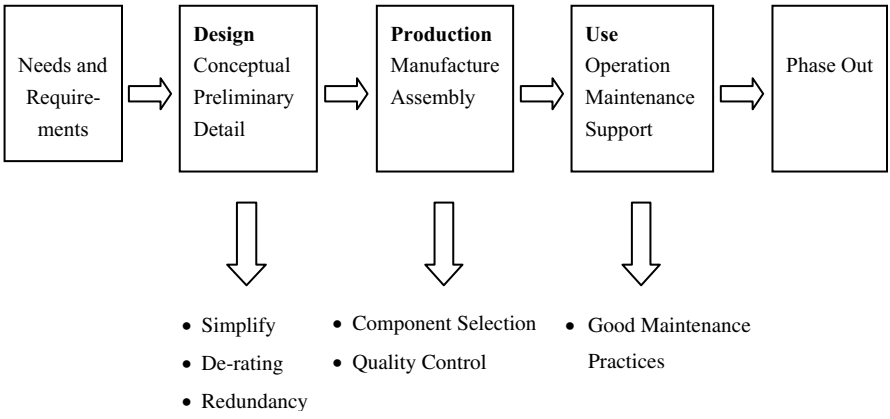

Figure 1.2 Different stages in life cycle of a system

1.3 Improving Reliability and Safety

Reliability is an important issue affecting each stage of the life cycle ranging from birth to death of a product or a system. Different stages in the life cycle of a system are shown in Figure 1.2. The first step in the improvement of reliability is to measure and assess the present level of reliability. One has to identify the important contributors/reasons for improving the reliability with given resources. It also depends upon at what stage the system is, for example if the system is at the design stage, only by simplifying the design, using derating and redundancy, can one improve the reliability. By using good components and quality control practices, reliability can be improved at the production stage. Good maintenance practices are the only resort during the stage of usage of the system.

Safety is a combination of reliability and consequences. Apart from increasing the level of reliability for improving safety, consequences must be reduced by providing protection/safety systems which anticipate the failures and make sure that consequences are at an acceptable level.

1.4 Definitions and Explanation of Some Relevant Terms

1.4.1 Quality

The International Standards Organization (ISO 3534) defines quality as "The totality of features and characteristics of a product or service that bear on its ability to satisfy stated and implied needs." The definition is based on the following:

- Quality is not absolute but refers to given requirements or specifications.
- Quality is not a physical quantity which can be measured. It is not a single feature of the product, but a complex set of characteristics.
- Quality is not a two-condition term in the sense that there is quality/no quality, but has a continuous structure between very good and very bad.

Quality management uses quality assurance and control of processes as well as products to achieve more consistent quality. There are many methods for quality improvement. These cover product improvement, process improvement, and people-based improvement. Examples of the methods of quality management and techniques that incorporate and drive quality improvement are ISO 9001, total quality management, six sigma, quality function deployment, quality circle, and Taguchi methods.

1.4.2 Reliability

The Institute of Electrical and Electronics Engineers (IEEE) defines reliability as the ability of a system or component to perform its required functions under stated conditions for a specified period of time.

There are four elements to the definition.

- *Ability* – expressed quantitatively with probability, refers to the chance or likelihood that the system or component will work properly. This is measured as a decimal ratio between 0 and 1 and is usually expressed as a percentage.
- *Required function* – generally, this is taken to mean operation without failure. The system requirements specification is the criterion against which reliability is measured. For this, a standard is needed, which should contain effective measurement criteria for comparing actual performance to the standard. If the actual performance falls within the tolerance limits of the standards, the intended function of the system is treated as successful.
- *Specified period of time* – nothing lasts for ever and nothing can perform adequately forever. Therefore for an intended function a time frame is needed, usually called a mission time.
- *Stated conditions* – the product may perform its intended function adequately in one set of conditions and quite poorly in another. A part designated for ambient temperature for instance may be totally inadequate for higher and lower temperatures. Stated conditions include air pressure, temperature, humidity, shock, vibration, *etc.*

An example of a reliability statement utilizing all four of the definition elements might be: the system or component has a 99% probability of operating at greater than 80% of rated capacity for 500 h without failure, at ambient temperature 25–50°C, with no more than 55% humidity in a dust-free atmosphere.

1.4.3 Maintainability

Maintainability is the ability of an entity, under given conditions of use, to be restored using stated procedures and resources. The measure of maintainability is the probability that the maintenance action can be carried out within a stated interval. Corrective maintenance is done after the occurrence of failure. However, in order to reduce the chance of failures and associated inconvenience, maintenance can also be preventive or predictive.

1.4.3.1 Corrective Maintenance

The maintenance is carried out after fault recognition to put an entity into a state in which it can perform a required function.

1.4.3.2 Preventive Maintenance

The maintenance is carried out at predetermined intervals or according to prescribed criteria and intended to reduce the probability of failure or the degradation of the functioning of an entity.

1.4.3.3 Predictive Maintenance

This is a form of preventive maintenance that is performed continuously or at intervals governed by observed condition to monitor, diagnose, or identify trends in a structure, system, or components' condition indicators; results indicate current and future functional ability or the nature of and schedule for planned maintenance. It is also known as condition-based maintenance.

1.4.4 Availability

Availability is the probability that a product or system is in operation at a specified time. This definition can be termed as instantaneous availability. There are several forms of availability. For example, average availability is defined on an interval of the real line, and steady-state availability is the limit of instantaneous availability function as time approaches infinity.

Availability is the same as reliability for a non-repairable system. For a repairable system, it can be returned to service with repair when failure occurs, thus the effect of failure can be minimized. By allowing repair, reliability does not change but availability does.

The simplest representation of availability is

$$A = \frac{Uptime\ \ of\ system}{Uptime\ \ of\ system + Downtime\ \ of\ system}.$$

Uptime depends on reliability of the system, whereas downtime depends on maintainability of the system. Thus availability is a function of both reliability and maintainability.

1.4.5 Safety/Risk

Safety is defined as capacity of a unit not to cause or let occur an endangering of persons for specified time and conditions.

A system is safe, if simultaneously:

- Faulty operation does not occur or has no endangering consequence.
- By using the equipment no endangering exists or results.

Risk is a multi-attribute quantity expressing hazard, danger, or chance of harmful or injurious consequences associated with an actual or potential event under consideration. It relates to quantities such as the probability that the specific event may occur and the magnitude and character of the consequences.

1.4.6 Probabilistic Risk Assessment/Probabilistic Safety Assessment

Probabilistic risk assessment/probabilistic safety assessment (PSA/PRA) is aimed at evaluating the risks of a system using a probabilistic method: a comprehensive structured approach for identifying failure scenarios, constituting a conceptual and a mathematical tool for deriving numerical estimates of risk. PSA/PRA essentially aims at identifying the events and their combination(s) that can lead to severe accidents, assessing the probability of occurrence of each combination and evaluating the consequences. The terms PRA and PSA are interchangeably used.

1.5 Resources

Tables 1.1–1.4 list some important journals, failure data banks and commercial software in the reliability and safety field.

Table 1.1 Journals

Title	Publisher	Published since
IEEE Transactions on Reliability	IEEE Reliability Society, USA	1952
Microelectronics Reliability	Elsevier, UK	1962
Reliability Engineering and System Safety	Elsevier, UK	1980
Risk Analysis	Society for Risk Analysis, USA	1981
International Journal of Quality and Reliability Management	Emerald Publishers, UK	1984
Quality and Reliability Engineering	John Wiley & Sons, USA	1985

Table 1.1 (continued)

Title	Publisher	Published since
International Journal of Reliability, Quality and Safety Engineering	World Scientific Publishing Co. Pvt. Ltd., Singapore	1994
Communications in Dependability and Quality Management	DQM Research Centre, Serbia	1998
International Journal of Performability Engineering	RAMS Consultants, Jaipur, India	2005
International Journal of Reliability and Safety	Inderscience Publishers, Switzerland	2006
Journal of Risk and Reliability	Professional Engineering, UK	2006
International Journal of System Assurance Engineering and Management	Springer, India	2009

Table 1.2 Failure data banks

Title	Developed by	Information
IAEA TECDOC-478	International Atomic Energy Agency, Austria	For use in nuclear systems
MIL-HDBK-217F	Department of Defense, USA	For use in electronic systems
NPRD-95	Reliability Analysis Center	For use in mechanical systems
PSID	Centre for Chemical Process Safety, USA	For use in process and chemical industry

Table 1.3 Commercial software

Title	Developed by	Available important tools
RELEX	Relex Software Corporation, USA	RBD, fault tree, event tree, life cycle cost, optimization, Markov
ISOGRAPH	Isograph Ltd, UK	Fault trees, event trees, Markov
RELIASOFT	ReliaSoft Corporation, USA	Accelerated life testing, reliability prediction, Weibull analysis
RISKSPECTRUM	Relcon Scandpower, Sweden	PSA, Bayesian updating, risk monitor

Table 1.4 International conferences

Title	Organizer/sponsor	Frequency
Probabilistic Safety Assessment and Management	International Association for Probabilistic Safety Assessment and Management	Two years
ESREL	European Safety and Reliability Association	Annual
The Annual Reliability and Maintainability Symposium	IEEE/ASQ	Annual
The International Applied Reliability Symposium	Reliasoft	Annual
International Conference on Quality, Reliability and Information Technology	IIT Bombay and Delhi University	Three years

1.6 History

The concept of reliability and safety started relatively later than other conventional engineering branches. Competition, cost effectiveness and safety have asked for better reliability. The history of reliability in the form of important milestones is described briefly below. Detailed explanation on the evolution of reliability engineering can be found in Elsayed [1] and Misra [2]. Table 1.5 summarizes the evolution of reliability tools.

Pierce in 1926 introduced the concept "the axiom that a chain is no stronger than its weakest link is one with essential mathematical implications." Reliability and safety were incorporated by focusing more attention on the critical element. These methods of guaranteeing reliability and safety were more the product of an art than of a scientific technique.

In the 1930s, aircraft accidents were recorded in the form of statistical reports by collecting failure data of various aircraft components. Designers and manufacturers made use of this feedback for improvement of future designs. The first risk objective for aircraft safety was defined by Pugsley in 1939. He asked that the accident rate of an aircraft should not exceed 10^{-5}/h.

Formal reliability techniques were first developed during the Second World War. Most of the defense equipment was found in a failed state at the time of demand. It was due to electronic system failure and in particular because of vacuum tube failures. Efforts to improve reliability were done in the USA in the 1940s by emphasizing two measures. One was that the life of products could be extended by better and improved designs and the second was increasing reliability through quality improvement and quality control.

The first predictive reliability models appeared in Germany where Van Braun was working on the V1 missile. The rockets were found to have poor reliability. The team worked based on the principle that a chain is no stronger than its weakest link. But failures were observed with not only the weakest part but also with the remaining components. The team later consulted a mathematician, Eric Pernchka. He came up with a concept which says if the survival probability of an element is $1/x$, the survival probability of system of n such similar components will be $1/x^n$. In fact, the famous Lusser's formula for reliability of series systems (series system reliability is product of reliability of constituting component) is derived from Pernchka's answer only.

Reliability as a branch of engineering was born in the USA in the 1950s. The availability of military equipment was low and costs were increasing due to high failure rates of electronic systems due to their complexity. In 1952, the Department of Defense (DOD) and all electronic industries created the Advisory Group on Reliability of Electronic Equipment (AGREE). The AGREE report recommended reliability growth tests and demonstration tests and advised that reliability should become an integral part of the development cycle. The recommendations of AGREE were adopted by NASA and DOD.

Watson of Bell Telephone Laboratories introduced the "fault tree analysis" concept for the assessment of system safety designed to control Minuteman missile launching in 1961. This has been used extensively in all engineering fields for safety and risk assessment, for instance, Boeing in the aeronautical field and WASH-1400 studies in the nuclear sector. The failure mode and effects analysis (FMEA) method was also devised in the early 1960s in aeronautics. During the 1960s, probabilistic approaches were increasingly integrated into the design. Initially regulations governing aeronautical safety were deterministic in nature; slowly, probabilistic criteria were introduced into the design of aircraft. This period also saw the birth of the *IEEE Transactions on Reliability*. Distinguished mathematicians like Birnbaum, Barlow, Proschan, Esary, and Weibull contributed to the development of mathematics of reliability.

In 1975, Ramuseen, with a team of 50 engineers, carried out studies on risk assessment of nuclear power plants and published the WASH-1400 report [3]; as a part of these studies, many new methods were developed, including event tree methods to evaluate accident scenarios. The studies considered a very large number of accident scenarios and quantified risk in terms of annual chances of fatalities to the public in the vicinity of a nuclear power plant. The risk thus calculated was lower than the risk from meteorite impacts. However, the Ramussen report was heavily criticized by the evaluation made by Lewis's report in 1977 for underestimating the uncertainty in data, human behavior, common-cause failures and consequences.

The Three Mile Island accident took place in the USA in 1979, and was considered the first major nuclear accident. The safety authority realized that the Ramussen report had identified an accident with a scenario similar to this accident. The commission set up after the accident recommended that PRA methods be increasingly used. Attitudes toward probabilistic methods changed and the number of risk assessment studies of nuclear power plants increased all over the world.

Table 1.5 Evolution of reliability tools

Tool	**Developed by**
Fault tree	Watson of Bell Telephone Laboratories in 1961
Event tree	WASH-1400 in 1975
FMEA	Aeronautics industry in 1960s
Markov models	Andrei A. Markov in 1909

Risk assessments were also performed in other industry sectors, for instance, a risk analysis of Canvey Island petro-chemical plants in the UK. These techniques were widely adopted in various fields such as aeronautical, chemical, power, and railways for complying with regulations and also for design improvements.

Subsequently, in the last 20–25 years, the scientific and practicing community has witnessed an impressive increase of developments and applications of reliability and safety engineering, aimed at rationally coping with the challenges brought

by the growing complexity of the systems and practically taking advantage of the computational power becoming available at reasonable cost [4].

1.7 Present Challenges and Future Needs for the Practice of Reliability and Safety Engineering

Reliability/safety assessment (RSA) is an efficient tool for the management of risk and decision making for the safe, economical, and efficient design and operation of complex engineering systems like nuclear power plants, chemical and process plants, aeronautical systems, and defense equipment. Specific applications of RSA include design evaluations for comparison with standards, identification of critical parts for reliability and safety management, evaluation of inspection and maintenance intervals and residual life estimation; it is also used as a regulatory requirement. Chapter 10 gives some of the practical applications of RSA.

In spite of several potential applications of reliability studies, they have their own limitations. Accuracy of RSA is greatly influenced by methodology, uncertainties in data and models, unjustified assumptions, and incompleteness in the analysis. Since the RSA model attempts to simulate reality, it is inevitable that there will be simplifying assumptions and idealizations of rather complex processes and phenomena. These simplifications and idealizations will generate uncertainties, the impact of which must be appropriately addressed if RSA is to serve as a tool in the decision-making process [5, 6]. Dynamic reliability modeling in complex scenarios is explained in Chapter 3.

The end use of any reliability study is to assist in decision making such as design evaluation, identification of critical components, and operation and maintenance activities. When reliability evaluation of design is carried out for comparison with the standards or required targets (set by the regulatory bodies), the decision maker's dilemma involves whether comparison of the standard should be done with the mean value or the bounds. The issue becomes significant if bounds are of the same order or of lower orders. The standard value (probability of failure) ought to be higher than the upper bound specified in the uncertainty bounds of the design. Similarly, while evaluating operation and maintenance intervals, uncertainty in data and models can make the final decision different. Proper treatment of uncertainty is essential for such practical usability of reliability analysis results. Ignoring uncertainties in reliability analysis may mislead decision making. Consideration of uncertainty in the analysis gives insights into decision making by giving optimistic and pessimistic sets of solutions. An acceptable degree of confidence in the results can only be achieved by proper management of uncertainty.

Many researchers, academicians, and practicing engineers in various fields worked extensively to develop methods for carrying out uncertainty analysis and applied them in their respective fields [7–11]. In particular, distinguishing different types of parameter uncertainty, characterizing the elementary uncertainty,

treatment of model uncertainty, uncertainty in dependency modeling, and considering uncertainty in decision making are still under active research. Some of these issues have been addressed in Chapter 11 of this book.

The presence of regulatory frameworks can have a determining influence on the use of risk and reliability methods in practice. This is clearly visible in high industries such as nuclear and aerospace where reliability and safety studies are enforced by regulators. Indeed, in those industries in which safety requirements are of a prescriptive nature (*e.g.*, automobiles, railways, communication networks, and the building sector), there is little incentive to invest in expensive reliability/risk studies. A cultural breakthrough is needed for plant owners and system managers to be shown and to grasp the benefits obtained from the incurred costs and the time spent in reliability/risk analyses [4].

To this aim, the availability of codes, standards, and good guidance documents is essential for the wider application of risk and reliability methods by practicing engineers. For example, at present there is still a paucity of standards in structural reliability and power system reliability analysis and techniques, and this reduces their practical application. Besides, the actual implementation of reliability methods must be supported by reasonably user-friendly software. Several tools are available for standard applications, whereas those complex issues such as humans, software, and dynamic event trees/fault trees need further development of integrated simulation software [4, 12].

Most of the present reliability and risk studies focus on assessing the level of safety and compare it with explicit or implicit standards. In addition, reliability and risk studies shall be increasingly used in operation and maintenance activities of engineering systems. For example in nuclear power plant, determination of surveillance test interval during operation and determination of in-service inspection interval during maintenance, are some of the practical applications of reliability and risk studies during the phase of use. Finally, the gap between theory and practice can be reduced by developing and implementing practically feasible solutions to industrial scale problems.

References

1. Elsayed EA (1996) Reliability engineering. Prentice Hall
2. Misra KB (1992) Reliability analysis and prediction. Elsevier
3. USNRC (1975) Reactor safety study – an assessment of accident risk in US commercial power plants (WASH-1400). USNRC
4. Zio E (2009) Reliability engineering: old problems and new challenges. Reliability Engineering and System Safety 94:125–141
5. IAEA (1992) Procedure for conducting probabilistic safety assessment of nuclear power plants (level 1). International Atomic Energy Agency, Vienna, Safety Series no. 50-P-4
6. NASA (2002) Probabilistic risk assessment procedures guide for NASA managers and practitioners. Version 1.1, NASA report

7. Modarres M (1985) Statistical uncertainty analysis in reactor risk estimation. Nuclear Engineering and Design 85:385–399
8. Wu JS, Apostolakis GE, Okrent D (1990) Uncertainties in system analysis: probabilistic vs non probabilistic theories. Reliability Engineering and System Safety 30:163–181
9. Helton JC (1993) Uncertainty and sensitivity analysis techniques for use in performance assessment for radioactive waste disposal. Reliability Engineering and System Safety 42:327–367
10. Ferson S, Hajago JG (2004) Arithmetic with uncertain numbers: rigorous and often best possible answers, Reliability Engineering and System Safety 85:135–152
11. Karanki DR, Kushwaha HS, Verma AK, Srividya A (2007) Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies. Reliability Engineering and System Safety 92(7):947–956
12. SAFERELNET (2006) Safety and reliability of industrial products, systems and structures – current position and future research needs, <http://www.mar.ist.utl.pt/saferelnet/>

Chapter 2
Basic Reliability Mathematics

The basics of mathematical theory that are relevant to the study of reliability and safety engineering are discussed in this chapter. The basic concepts of set theory and probability theory are explained first. Then the elements of component reliability are presented. Different distributions used in reliability and safety studies with suitable examples are explained. The treatment of failure data is given in the last section of the chapter.

2.1 Classical Set Theory and Boolean Algebra

A set is a collection of elements having certain specific characteristics. A set that contains all elements of interest is known as a universal set, denoted by U. A subset refers to a collection of elements that belong to a universal set. For example, if universal set U represents employees in a company, then "female employees" is a subset A of U. For graphical representation of sets within the frame of reference of universal set, Venn diagrams are widely used. They can be very conveniently used to describe various set operations.

The Venn diagram in Figure 2.1 shows the universal set with a rectangle and subset A with a circle. The complement of a set A (denoted by $\bar{A}$) is a set which consists of the elements of U that do not belong to A.

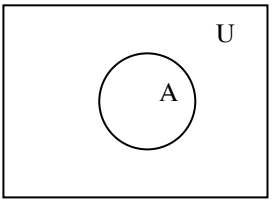

Figure 2.1 Venn diagram for subset A