Springer Series in Reliability Engineering

Ajit Kumar Verma
Srividya Ajit
Durga Rao Karanki

Reliability and Safety Engineering

Second Edition

Springer

Springer Series in Reliability Engineering

Series editor

Hoang Pham, Piscataway, USA

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

Ajit Kumar Verma · Srividya Ajit
Durga Rao Karanki

Reliability and Safety Engineering

Second Edition

Springer

Ajit Kumar Verma
ATØM
Stord/Haugesund University College
Haugesund
Norway

Srividya Ajit
ATØM
Stord/Haugesund University College
Haugesund
Norway

Durga Rao Karanki
Paul Scherrer Institute
Villigen PSI
Switzerland

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

Library of Congress Control Number: 2015944434

Springer London Heidelberg New York Dordrecht

Printed on acid-free paper

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

To our gurus:
Bhagwan Sri. Sathya Sai Baba
Paramhamsa Swami Sathyananda
Pujya Mata Amritanandaji
Smt. Vijaya and Sri. B. Jayaraman
Smt. Kasturi and Sri. C.S. Rao

To our parents:
Late Sri. K.P. Verma and Late Smt. S. Verma
Late Sri. B.C. Khanapuri
and Smt. V.B. Khanapuri
Sri. K. Manikya Rao and Smt. K. Anjali

Foreword

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

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

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

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

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

Preface

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

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

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

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

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

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

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

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

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

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

Acknowledgments

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

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

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

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

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

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

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

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

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

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

March 2015

Ajit Kumar Verma
Srividya Ajit
Durga Rao Karanki

Contents

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, environmental impact, and deaths. Examples of major accidents are Fukushima-Daiichi nuclear disaster, Deepwater Horizon oil spill, Chernobyl accident, Bhopal gas tragedy, and space shuttle Columbia disaster. 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 where as the safety deals with the consequences after the failure. Inherent safety systems/measures ensure the consequences of failures are minimal. Reliability and safety engineering provides a quantitative measure of performance, identifies important contributors, gives insights to improve system performance such as how to reduce likelihood of failures and risky consequences, measures for recovery, and safety management.

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

- Increased product complexity
- Accelerated growth of technology
- Competition in the market
- Public awareness or customer requirement
- Modern safety and liability laws
- Past system failures
- Cost of failures, damages and warranty
- Safety considerations with undesirable consequences

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_1

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

- Design evaluation;
- Identification of critical components/events;
- Determination of de-rating/factor of safety;
- Environmental comparisons;
- Redundancy requirements;
- Regulatory requirements;
- Burn-In/Accelerated life tests
- Establishment of preventive maintenance programs;
- Repair and spare part management;
- Replacement and residual life estimations;
- Safety management;
- Emergency management;
- Life cycle cost analysis.

1.2 Exploring Failures

One of the key elements of reliability and safety assessment is exploring failures, which include study, characterize, measure, and analyze the failures. There are many causes for 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.

Failure rate (or hazard rate) of a population of products/items are often represented with a life characteristic curve or bathtub curve. A typical bathtub curve is shown in Fig. 1.1. Failure or Hazard rate is the instantaneous rate of failure for survivals until time t. When the products are put into operation, some of them fail quickly due to manufacturing defects or inherently weak elements. This means that the early hazard rate is very high. But once the weak products are gone the hazard rate falls and becomes fairly constant. Finally the hazard rate rises again due to wear-out. As shown in Fig. 1.1, the hazard function over life time of product can be divided into three distinct regions:

(1) Early failure region or infant mortality (decreasing hazard rate)
(2) Useful life region (constant hazard rate)
(3) Wear-out failure region (increasing hazard rate)

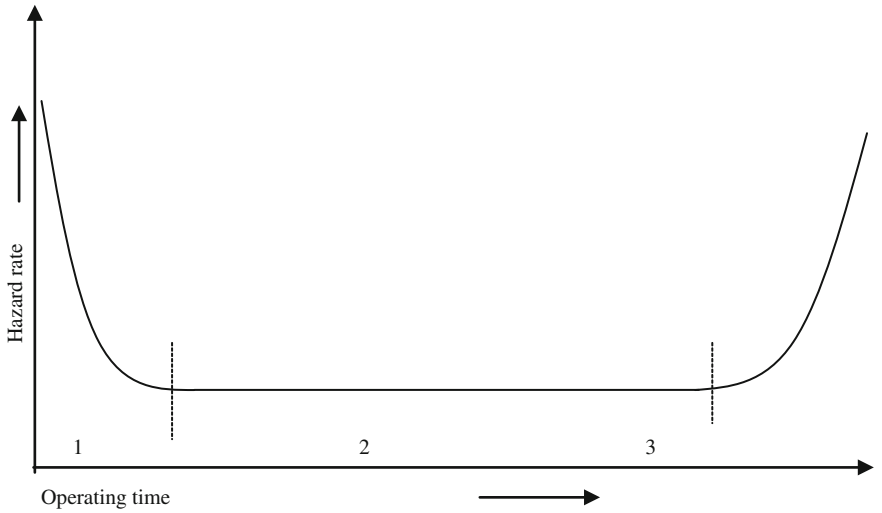

Fig. 1.1 Bath-tub curve

In the region (1), products/items should be monitored carefully before using as hazard rate is high. Some manufactures use burn-in tests to screen out infant mortalities before supplying them to end users. Although highly accelerated life tests or highly accelerated stress tests are useful to identify and eliminate the root causes economically, burn-in tests are still effective for products whose root causes can't be eliminated completely [1]. The region (2) is useful life period where hazard rate is governed by chance/random failure and is fairly constant. The region (3) indicates that the product should be replaced or scrapped as hazard rate starts increasing.

1.3 Improving Reliability and Safety

Reliability is an important issue affecting each stage of life cycle ranging from birth to death of a product or a system. Different stages in life cycle of a system are shown in the Fig. 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 in what stage the system is, for example if the system is in the design stage, only by simplifying the design, using de-rating/factor of safety and redundancy, one can 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.

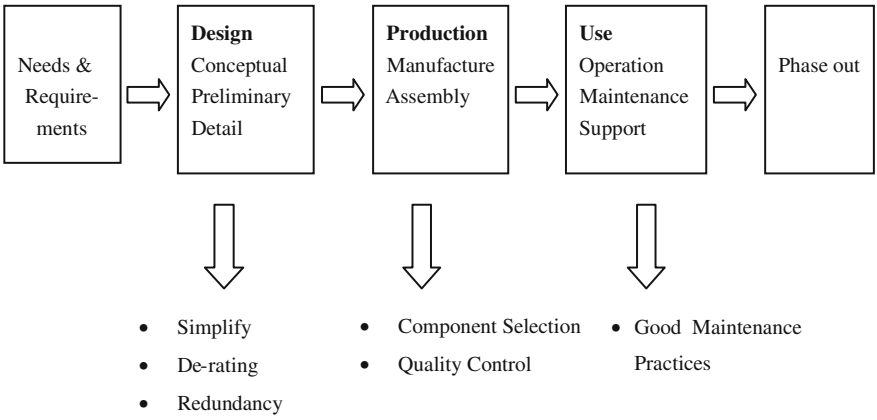

Fig. 1.2 Different stages in life cycle of a system

Safety is 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 anticipates the failures and make sure that consequences are in the acceptable level.

1.4 Definitions and Explanation of Some Relevant Terms

1.4.1 Quality

The International Organization for Standardization (ISO) 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." In other words, quality is conformance to specifications or requirements defined by customer. Quality is not binary rather a continuous structure between good and bad.

Quality management uses quality assurance and control of processes as well as products to achieve more consistent quality. ISO publishes standards that provide guidance on how to ensure consistency and continuous improvement of quality in products or services. For example, ISO 9001:2008 [2] sets out the requirements of a quality management system. Companies or organizations can get certification that a quality management is in place. This ISO standard has been implemented by over one million organizations in over 170 countries [3].

Numerous techniques are available for improving quality. Examples for the methods of quality management and techniques that incorporate and drive quality improvement are ISO 9004:2008, Total Quality Management (TQM), statistical process control, Six Sigma, Quality Function Deployment (QFD), Quality Circle, Taguchi methods, etc.

1.4.2 Reliability

As per IEEE standards [4], reliability is defined as the ability of a system or component to perform its required functions under stated conditions for a specified period of time. The key elements of the definition are ability, required function, conditions, and specified period of time. Ability is expressed quantitatively with probability. Required function relates to expected performance. Stated conditions usually refer to environmental conditions of operation. Specified period of time is also referred as mission time which provides expected duration of operation. Mathematically, reliability is defined as the probability that the random variable time to failure (T) is greater or equal to mission time (t), as shown below.

$$R(t) = P(T \geq t) \tag{1.1}$$

Typical measures of reliability are failure rate/frequency, mean time to failure, mean time between failure, etc. Although reliability provides quantitative measure of performance, one should not look at the absolute values but rather on relative basis. For example, comparison with a target value expected by regulators or comparison among alternative design changes.

It is important to understand the difference between quality and reliability. As mentioned before, quality is conformance to specifications, which is at time t = 0 before we start operation. Reliability can often be termed as projection of quality over time, meeting customer's expectations over its life time.

1.4.3 Maintainability

BS 4778 defines maintainability as "The ability of an item, under stated conditions of use, to be retained in, or restored to, a state in which it can perform its required functions, when maintenance is performed under stated conditions and using prescribed procedures and resources" [5]. 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.

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

Preventive Maintenance
The maintenance 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.

Predictive Maintenance
Form of preventive maintenance performed continuously or at intervals governed by observed condition to monitor, diagnose or trend 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.

Typical measures of maintainability are repair rate, mean time to repair, etc. The technical specifications such as surveillance test interval and inspection interval are often determined using the reliability and maintainability studies.

1.4.4 Availability

As introduced by Barlow and Proschan [6], 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 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 changes.

The simplest representation of availability (A) is:

$$A = \frac{Uptime\ \ of\ system}{Uptime\ \ of\ system + Downtime\ \ of\ system} \tag{1.2}$$

Uptime depends on reliability of the system where as downtime depends on maintainability of the system. Thus availability is function of both reliability and maintainability.

1.4.5 Risk and Safety

Several definitions of risk exist in the literature. The most popular definition of risk is the one proposed by Kaplan and Garrick [7]. They defined risk as function of answers to three questions: "what can go wrong?"; "how likely is it to go wrong?"; "if it does go wrong, what are the consequences?" Quantitatively, risk is defined as a set of triplets as shown in equation:

$$Risk = \langle S_i P_i x_i \rangle \tag{1.3}$$

Where 'i' is a scenario number, i = 1, 2…N and S_i is an accident scenario which has probability of P_i and a consequence of x_i. For example, an accident scenario in a chemical plant has a probability of 1e-2 and its associated consequences results in a financial loss of $10,000. Consequences of different scenarios may have similar or same consequences, which results in probability/frequency of scenario as the vital element. Popular measures of risk for nuclear industry are core damage frequency and large early release frequency.

Aven's definition of risk includes uncertainty as an essential element of risk. As per his definition [8], risk is function of accident scenario (A), consequence (C), and uncertainty (U) about A and C, Risk = (A, C, U).

Risk and safety are related to each other: the higher the risk, the lower the safety. Risk assessment is also referred as safety assessment with practically no difference in engineering applications.

1.4.6 Probabilistic Risk Assessment/Probabilistic Safety Assessment

Probabilistic risk assessment/probabilistic safety assessment (PRA/PSA) is aimed at evaluating the risks of a system using a probabilistic method. IAEA safety standards [9, 10] define PSA as a comprehensive, structured approach to 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 term PRA and PSA are interchangeably used.

PSA/PRAs are performed for practically all nuclear power plants (NPPs), and also applied in aerospace, chemical and process industries. In NPPs, it is performed at three levels: Level-1 PSA to estimate core damage frequency, Level-2 PSA to estimate radioactive release frequency, and Level-3 PSA to estimated public health and societal risk.

1.5 Resources

Tables 1.1, 1.2, 1.3, and 1.4 lists some important journals, international conferences, failure data banks and commercial software in the reliability and safety field.

Table 1.1 International journals

Name of journal	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
Journal of System Safety	The International System Safety Society, USA	1983
Structural Safety	Elsevier, UK	1983
International Journal of Quality and Reliability Management	Emerald Publishers, UK	1984
Quality and Reliability Engineering	John Wiley & Sons, USA	1985
Safety Science	Elsevier, UK	1991
International Journal of Reliability, Quality and Safety Engineering	World Scientific Publishing Co. Pvt. Ltd., Singapore	1994
Process Safety and Environmental Protection	Elsevier, UK	1996
Journal of Risk Research	Taylor & Francis Group	1998
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
Journal of Quality and Reliability Engineering	Hindawi Pub. Co., USA	2008
International Journal of System Assurance Engineering and Management	Springer	2009
Journal of Life Cycle Reliability and Safety Engineering	Society for Reliability and Safety, India	2010

1.6 History

A historical overview of reliability and safety engineering in the form of important milestones is briefly described below.

The concept of reliability and safety started relatively later than other engineering branches. As Dr. W.A. Shewart inspired the rise of statistical quality control at Bell labsin 1920s, W. Weibull conceived the Weibull distribution to represent fatigue of materials. Pierce in 1926 introduced the concept 'the axiom that a chain is no stronger than its weakest link is one with essential mathematical implications'. In the 1930s, aircraft accidents were recorded in the form of statistical reports by collecting failure data of various aircraft components [11]. Designers and manufacturers made use of this feedback for improvement of future designs. The first risk

Table 1.2 International conferences

Name of the conference	Organizer/sponsor	Frequency
Probabilistic Safety Assessment and Management (PSAM)	International Association for Probabilistic Safety Assessment and Management	2 years
Probabilistic Safety Assessment	American Nuclear Society	2 years
Society for Risk Analysis Annual Meeting (SRA)	Society for Risk Analysis	Annual
ESREL Conference	European Safety and Reliability Association	Annual
International System Safety Conference (ISSC)	The International System Safety Society	Annual
The Annual Reliability and Maintainability Symposium (RAMS)	IEEE/ASQ	Annual
The International Applied Reliability Symposium	Reliasoft	Annual
International Conference on Quality, Reliability, and Information Technology (ICQRIT)	IIT Bombay and Delhi Univ., India	3 years
International Conference on Reliability, Safety and Hazard (ICRESH)	Bhabha Atomic Research Centre, India	5 years

Table 1.3 Failure data banks

Name of database	Developed by	Information
IAEA TECDOC-478	International Atomic Energy Agency, Austria	For use in nuclear systems
IAEA TECDOC-1048	International Atomic Energy Agency, Austria	Human reliability data
MIL-HDBK-217F	Department of Defense, USA	Electronic equipment
Telcordia	Telcordia Technologies, USA	For electronic, electrical, electro-mechanical components
IEC 62380	International Electrotechnical Commission, Switzerland	Electronics components, PCBs and equipment
NPRD-95	Reliability Analysis Centre	For use in mechanical systems
PSID	Centre for Chemical Process Safety, USA	For use in process and chemical industry

objective for aircraft safety was defined by Pugsley in 1939. He asked for the accident rate of an aircraft should not exceed 10^{-5}/h.

The first predictive reliability models appeared while Wernher von Braun, one of the most famous rocket scientists, was working on the V1 missile in Germany. The rockets were found to be having 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 remaining components. The team later consulted a mathematician, Eric Pernchka, who came up with a concept

Table 1.4 Commercial software

Software	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	RelconScandpower, Sweden	PSA, Bayesian updating, risk monitor
ITEM	Item Software, UK	Fault trees, event trees, Markov, FMECA, Electronics (MIL-HDBK-217, IEC 62380)
The EPRI HRA calculator	Electric Power Research Institute, USA	Human reliability analysis

which says 'if the survival probability of an element is 1/x, survival probability of system of n such similar components will be $1/x^n$, which forms the basis for the reliability of series system [11]. Subsequently, Wern Von Braun introduced the concept of redundancy to improve the reliability of systems.

The concepts of reliability developed slowly until World War II. During the War, over 50 % of the defense equipment was found to be failed state in storage; it was due to electronic system failure and in particular because of vacuum tube failures. The unreliability of vacuum tube acted as a catalyst to the rise of reliability engineering. Reliability was born as a branch of engineering in USA in 1950s. In 1952 the Department of Defense (DOD) and the American electronic industry created the Advisory Group on Reliability of Electronic Equipment (AGREE). AGREE report suggested modularity in design, reliability growth and demonstration tests to improve reliability and also a classical definition of reliability. This study triggered several applications in electronic industry and also spread to aerospace industry. This period witnessed the first conference on 'quality control and reliability' and the first journal in the area 'IEEE Transaction on Reliability' by the Institute of Electrical and Electronics Engineers.

In 1961 H.A. Watson introduced 'Fault Tree Analysis (FTA)' concept to evaluate control system of Minuteman I Intercontinental Ballistic Missile (ICBM) launching system at Bell telephone laboratories. The FTA is one of the pillars for safety and risk assessment even today, which is extensively used in aerospace and nuclear industries. The failure mode effect analysis (FMEA) method was also introduced in the early 1960s by aerospace industry. FMEA technique also became popular in automotive industry. Following Apollo 1 disaster in 1967, aerospace industry began to use a systematic approach to evaluate risk called 'Probabilistic Risk Assessment (PRA)'. In 1960s, specializations of reliability engineering emerged, for instance structural reliability as a branch was born to investigate structural integrity of buildings, bridges, vessels, pipes, etc. [12]. Distinguished mathematicians Birnbaum, Barlow, Proschan, Esary and Weibull extensively contributed to the development of mathematics of reliability [11].

In the early 1970s, nuclear industry had adapted PRA concepts from aerospace industry, but subsequently PRA methods developed in nuclear industry were adapted by aerospace industry [13]. Undoubtedly the ground breaking study for risk assessment of nuclear power plants is the Reactor Safety Study initiated by US Atomic Energy Commission and led by the pioneer Prof. Rasmuseen. This landmark study resulted in a comprehensive WASH-1400 report [14]. This study investigated a large number of accident scenarios, quantified risk, and identified important risk contributors. Event tree analysis took birth during this study, which is an essential element of today's PRA/PSAs. Although the study had been criticized for underestimating uncertainties, dependencies, and operator actions, three mile island (TMI) accident which took place in USA in 1979 resembled one of the accident scenario identified in WASH-1400. PRA methodology received a major boost after TMI accident. US Nuclear Regulatory Commission made extensive efforts to develop and promote PRA methods. For example, NUREG-1150 [15] study assessed risk of five US nuclear power plants, which demonstrated the potential PRA applications. Today practically nuclear power plants all over the world perform PRA/PSAs and regulators use PRA/PSAs in the risk informed regulation of plants. Risk assessments have also been performed in other industry sectors, for instance, aeronautical, chemical, power, railways for complying with regulations and also for design improvements. In 1970s, another branch of reliability engineering emerged, software reliability which was concerned about software development, testing and improvement [16].

In 1980s, methods to capture dependencies and to model operator actions were extensively developed. For example, common cause failure models proposed by Fleming [17] and Mosleh [18] and human reliability analysis methods introduced by Swann [19]. Techniques such as Bayesian analysis to update failure models with field date and also use of accelerated life testing to investigate failure causes became popular during this time [20].

Traditionally basic event or component failure models were obtained from statistical analysis of field or life tests data, Bayesian updating, or expert elicitation techniques. To overcome the criticism about uncertainties in such models, 1990s witnessed the rise of physics of failure or mechanist models, especially in electronic, electronic, and mechanical components. This approach used knowledge of degradation process and operating stresses/loads to characterize failure mechanisms. The recent trend is the hybrid methods that combine different types of data including failure data banks, expert judgment, physical of failures information, and life test data using Bayesian updating technique [20].

Complexity of systems and technological developments is ever increasing. To cope with these challenges, simulation based safety/reliability analysis methods have been receiving increased attention. The availability of high performance computing infrastructure at unprecedented levels helps in such simulations. Integrating deterministic models with probabilistic models are being explored to improve reliability/risk modeling taking advantage of computational power.