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

Durga Rao Karanki
Paul Scherrer Institute
Villigen PSI
Switzerland

Srividya Ajit
ATØM
Stord/Haugesund University College
Haugesund
Norway

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)

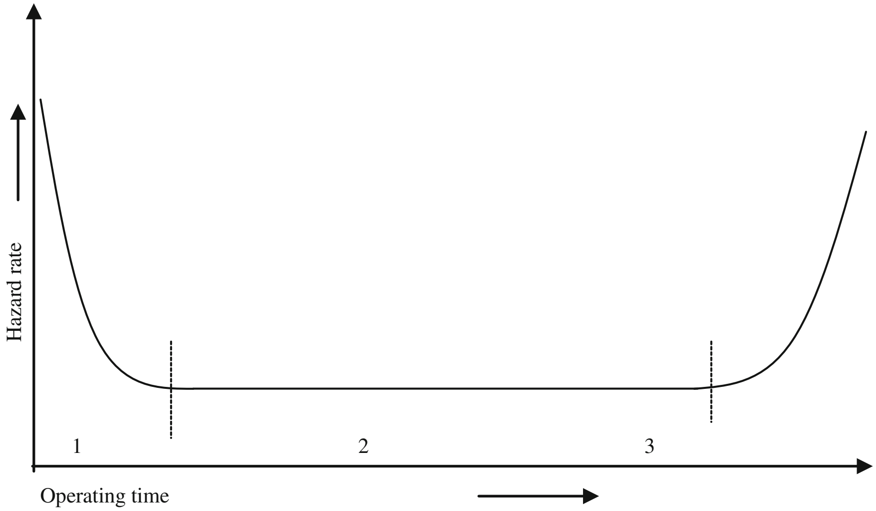


Fig. 1.1 Bath-tub curve

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.

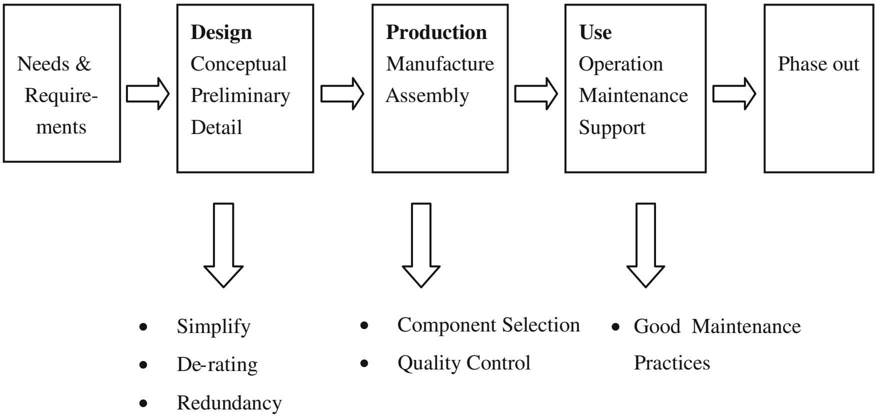


Fig. 1.2 Different stages in life cycle of a system

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.

Table 1.5 Evolution of reliability and risk assessment methods

Method/Milestone	Developed/Inspired by
Reliability predictive models	Eric Pernchka in 1940s
Birth of reliability engineering as a branch	AGREE study in 1950s
Fault tree analysis	Watson at Bell telephone laboratories in 1961
Markov models in reliability/risk studies	Andrei A. Markov invented the method
FMEA	Aeronautics industry in 1960s
Probabilistic risk/safety assessment-Event tree analysis	Rasmussen's Reactor safety study (WASH-1400) in 1975
Bayesian approach in reliability/risk studies	Nuclear/Electronics industry
Importance measures	W.E. Vesely in 1983
Dependency models	A. Mosleh in 1980s
Human reliability	A.D. Swain in 1980s
Physical of failure models	Electronic industry in 1990s
Simulation based safety/reliability methods	Nuclear industry in 2000s

Table 1.5 summarizes important milestones discussed earlier. Detailed explanation on evolution of reliability and safety engineering can be found in Villemeur [11], Elsayed [21], Misra [22], Modarres [13, 20].

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

Reliability/Safety Assessments are very useful to manage reliability/risk and support decision making for 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 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.

In spite of several potential applications of reliability/safety studies, there are a few limitations. Accuracy of these studies is greatly influenced by models, uncertainties in data and models, unjustified assumptions and incompleteness in the analysis. In representing complex behavior of system swith the mathematical models, there could be simplifying assumptions and idealizations of rather complex processes and phenomena. These simplifications and idealizations lead to inappropriate reliability/risk estimates, the impact of which must be appropriately addressed if the assessment is to serve as a tool in the decision making process [9, 23].

The end use of any reliability/risk studies is to assist in decision making such as design/plant evaluation, identification of critical components, and operation and maintenance activities. When reliability/risk evaluation of design/plant 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. 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 [24–28]. 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 Chaps. 13 and 14 of this book.

The regulators play a vital role in the application of reliability and risk studies. This is clearly visible in industries such as nuclear, chemical and aerospace where reliability and safety studies are enforced by regulators. For example, US NRC has been instrumental in developing PSA technology and promoting its applications. Industries which are not enforced by regulators to meet quantitative risk requirements are relatively less inclined to perform rather expensive reliability and risk studies; for example, automobile, railways, communication networks and building sector. Zio [29] advocates the need for a cultural breakthrough convincing plant/system managers about benefits obtained from resource intensive reliability and risk studies. This can be realized by standardization of methods and providing resources guiding the practitioners. For instance, there is scope for improvement in standards for structural reliability and power system reliability analysis. Availability of advanced software tools and comprehensive data banks will rapidly improve applications in various industries [30].

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 studies shall be increasingly used in operation and maintenance activities of engineering systems. For example in nuclear power plants, 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.

Table 1.6 Potential improvements in PSA methodology

S. no.	Potential area	Specific tasks
1.	Increasing the search space and the scope of the analysis	a. Impact of screening criteria
		b. External events and their correlations
		c. Dependencies among multi units
		d. Emergency preparedness
2.	Improving the accident modeling	a. Examine assumptions, approximations, time dependent complex interactions, and associated conservatism
		b. Modeling external events, passive systems, digital systems, and severe accidents
		c. Simulation based risk analysis
3.	Uncertainty analysis	a. Risk estimate: mean versus its uncertainties
		b. Physical phenomena and uncertainties from its simulation codes

Potential Improvements in Risk Assessment as Revealed by Fukushima

PSA standards provide detailed methodology and guidelines to carry out risk/safety assessment; for example, IAEA [31] and ASME/ANS standards [32, 33] for nuclear installations. Practically all nuclear power plants perform level-1 PSA studies, while most of which perform level-2 PSA to severe accident progression. Full scope PSA that includes level-3 PSA should be performed to assess the off-site consequences. Although the full scope PSA is resource intensive, it provides vital safety insights in safety management.

The Fukushima accident (caused by a tsunami triggered by an earthquake) at three units in 2011 revealed some of the potential areas for improving PSA methodology. Siu et al. [34] and Lyubarskiy et al. [35] highlighted a number of issues and lessons learnt from the accident. Some of the important issues are organized into the following three groups. Table 1.6 summarizes three potential areas and their specific tasks to improve PSA methodology.

1. *Increasing the search space and the scope of the analysis*
   The quantitative screening criteria to focus analysis on most risk-significant hazards would likely lead to the screening of events such as Fukushima, which poses a question as to what we might do to avoid such a situation. The events such as earthquake, tsunami, fire, and floods and the correlation between such hazards should be considered. Also, dependencies among multi units on the same site should be appropriately treated in PSAs. The emergency response centers and its associated effect on the consequences should be included in the analysis.
2. *Improving accident modeling*
   It is worthwhile to highlight a point mentioned by Siu et al. [34]: "well-intentioned conservatism in different PSA technical elements can sufficiently skew the analysis results that truly risk-significant scenarios may be

masked". A MLOCA study in [36, 37], where PSA results were compared with Dynamic PSA results including the risk contributors, reported inappropriate importance measures besides conservative results from PSA. The conservative bounding assumptions, approximations, and treating time dependent complex interactions should be appropriately examined before introducing them into PSA studies; simulation based risk analysis methods such as dynamic event trees (DET) can support PSA studies in such conditions. For example, Karanki et al. [38, 39], reported DET informed approach to study the impact of dynamics on success criteria definitions used in PSA. Chapter 11 focuses on the dynamic PSA.

One of the most challenging elements in PSA is accounting human errors and human failure events. In particular the errors of commission, for example the intentional isolation of a safety system at Fukushima unit-1 [34], there are human reliability analysis methods capable of treating such events [40–42]. The methods and applications should be extended to full scope PSA and also address new complexities arising from the severe accident scenarios.

Modeling external events such as seismic, tsunami, flood, fire, etc. pose another important challenge, especially their combinations. Treatment of passive systems and digital systems should be appropriately done in PSA studies.

3. *Understanding the uncertainties*
   It is essential to treat uncertainties in models and model parameters. In current PSA practice, the uncertainties in stochastic PSA model parameters such as basic event probabilities are only propagated to risk. Plant simulations are usually performed to simulate accident scenarios with thermal hydraulic codes. Although physical process is deterministic in nature, the mathematical models representing the physics is subjected to uncertainty, which arises from modeling the phenomena accurately and their associated model parameters. Uncertainty in model parameters of physical phenomena should also be considered to determine sequence outcomes, to define success criteria in building accident sequence models, and should be propagated to risk.

References

1. Wilkins DJ (2002) The bathtub curve and product failure behavior. Reliab Hot Wire 21 & 22
2. ISO 9001:2008 (2012) Quality Management Systems—Requirements
3. http://www.iso.org
4. Institute of Electrical and Electronics Engineers (1990) IEEE standard computer dictionary: a compilation of IEEE standard computer glossaries, New York. ISBN 1-55937-079-3
5. BS 4778 Glossary of terms used in quality assurance, including reliability and maintainability terms. British Standards Institution, London
6. Barlow RE, Proschan F (1973) Availability theory for multicomponent system, multivariate analysis III. Academic Press Inc., New York, pp 319–335 (Reliability and life testing: probability models)
7. Kaplan S, Garrick BJ (1981) On the quantitative definition of risk. Risk Anal 1:11–27

8. Aven T (2010) On how to define, understand and describe risk. Reliab Eng Syst Saf 95:623–631
9. 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
10. IAEA (2002) Review of probabilistic safety assessments by regulatory bodies. Safety Reports Series, No. 25, International Atomic Energy Agency, Vienna
11. Villemeur A (1992) Reliability, maintainability, and safety assessment, vol 1. Methods and techniques. Wiley, New York
12. Saleh JH, Marais K (2006) Highlights from the early (and pre-) history of reliability engineering. Reliab Eng Syst Saf 91:249–256
13. Keller W, Modarres M (2005) A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late professor Norman Carl Rasmussesn. Reliab Eng Syst Saf 89:271–285
14. USNRC (1975) Reactor safety study: an assessment of accident risk in US commercial power plants (WASH-1400). USNRC
15. USNRC (1990) Severe accident risks: an assessment for five US nuclear power plants, NUREG-1150
16. Moranda PB (1975) Prediction of software reliability during debugging. In: Proceedings of the annual reliability maintenance symposium, pp 327–32
17. Fleming KN, Kalinowski AM (1983) An extension of the beta factor method to systems with high level of redundancy. Pickard, Lowe and Garric Inc. PLG-0289
18. Mosleh A et al (1988) Procedures for treating common cause failures in safety and reliability studies. U.S. Nuclear Regulatory Commission and Electric Power Research Institute, NUREG/CR-4780, and EPRI NP-5613, vols 1 and 2
19. Swain AD, Guttmann HE (1983) Handbook of human reliability analysis with emphasis on nuclear power plant applications, NUREG/CR-1278, USNRC
20. Azarkhail M, Modarres M (2012) The evolution and history of reliability engineering: rise of mechanical reliability modeling. Int J Perform Eng 8(1):35–47
21. Elasayed EA (1996) Reliability engineering. Prentice Hall, New Jersey
22. Misra KB (1992) Reliability analysis and prediction. Elsevier Publishers, New York
23. NASA (2002) Probabilistic risk assessment procedures guide for NASA managers and practitioners. Version 1.1, NASA Report
24. Modarres M (1985) Statistical uncertainty analysis in reactor risk estimation. Nucl Eng Des 85:385–399
25. Wu JS, Apostolakis GE, Okrent D (1990) Uncertainties in system analysis: probabilistic Vs non probabilistic theories. Reliab Eng Syst Saf 30:163–181
26. Helton JC (1993) Uncertainty and sensitivity analysis techniques for use in performance assessment for radioactive waste disposal. Reliab Eng Syst Saf 42:327–367
27. Ferson S, Hajago JG (2004) Arithmetic with uncertain numbers: rigorous and often best possible answers. Reliab Eng Syst Saf 85:135–152
28. Karanki DR, Kushwaha HS, Verma AK, Srividya A (2007) Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies. Reliab Eng Syst Saf 92 (7):947–956
29. Zio E (2009) Reliability engineering: old problems and new challenges. Reliab Eng Syst Saf 94:125–141
30. SAFERELNET (2006) Safety and reliability of industrial products, systems and structures: current position and future research needs. http://www.mar.ist.utl.pt/saferelnet/
31. IAEA (2010) Development and application of level 1 probabilistic safety assessment for nuclear power plants. International Atomic Energy Agency, Vienna, IAEA SAFETY STANDARDS SERIES No. SSG-3
32. ASME (2002) Probabilistic risk assessment for nuclear power plant applications, RA-S-2002. American Society of Mechanical Engineers, New York
33. ASME (2013) Probabilistic risk assessment standard for advanced non-LWR nuclear power plants, ASME/ANS RA-S-1.4-2013. American Society of Mechanical Engineers, New York

34. Siu N et al (2013) PSA technology challenges revealed by the great east Japan earthquake. In: PSAM topical conference in light of the Fukushima Daiichi accident, Tokyo, Japan, 15–17 April 2013
35. Lyubarskiy A, Kuzmina I, El-Shanawany M (2011) Notes on potential areas for enhancement of the PSA methodology based on lessons learned from the Fukushima accident. In: Proceedings of the 2nd probabilistic safety analysis/human factors assessment forum, Warrington, UK, 8–9 Sept 2011
36. Karanki DR, Dang VN (2013) Quantified dynamic event trees vs PSA: a comparison for MLOCA risk. In: ANS PSA 2013 international topical meeting on probabilistic safety assessment and analysis, Columbia, SC, USA, 22–26 Sept 2013, American Nuclear Society, CD-ROM
37. Karanki DR, Dang VN Quantification of dynamic event trees: a comparison with event trees for MLOCA scenario. In: Communication with reliability engineering and system safety
38. Karanki DR, Dang VN, Kim TW (2012) The impact of dynamics on the MLOCA accident model: an application of dynamic event trees. In: Proceedings 11th probabilistic safety assessment and management/European safety and reliability 2012 (PSAM11/ESREL2012), Helsinki, Finland, 25–29 June 2012, CD-ROM
39. Karanki DR, Kim T-W, Dang VN (2015) A dynamic event tree informed approach to probabilistic accident sequence modeling: dynamics and variabilities in medium LOCA. Reliab Eng Syst Saf (ISSN: 0951-8320) 142:78–91
40. U.S. Nuclear Regulatory Commission (2000) Technical basis and implementation guidelines for a technique for human event analysis (ATHEANA). NUREG-1624, Rev. 1, Washington, DC
41. Julius JA, Jorgenson EJ, Parry GW, Mosleh AM (1995) A procedure for the analysis of errors of commission in a probabilistic safety assessment of a nuclear power plant at full power. Reliab Eng Syst Saf 50:189–201
42. Podofillini L, Dang VN, Nusbaumer O, Dress D (2013) A pilot study for errors of commission for a boiling water reactor using the CESA method. Reliab Eng Syst Saf 109:86–98

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 universal set, denoted by 'U'. A sub set 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 sub set 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 Fig. 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.

2.1.1 Operations on Sets

Let A and B be any sub-sets of the universal set U, the union of two sets A and B is a set of all the elements that belong to at least one of the two sets A and B. The union is denoted by '$\cup$' and read as 'OR'. Thus $A \cup B$ is a set that contains all the elements that are in A, B or both A and B. The Venn diagram of $A \cup B$ is shown in Fig. 2.2.

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_2

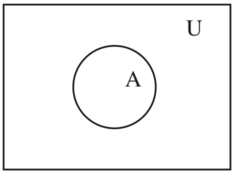


Fig. 2.1 Venn diagram for subset A

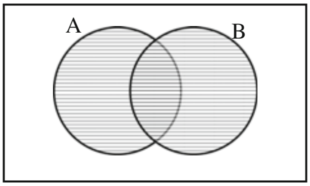


Fig. 2.2 Venn diagram for A ∪ B

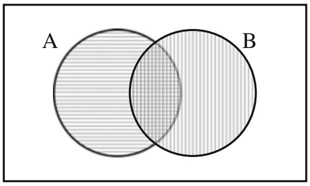


Fig. 2.3 Venn diagram for A ∩ B

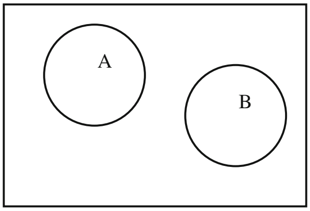


Fig. 2.4 Venn diagram for mutually exclusive events

The intersection of A and B is the set of elements which belong to both sets. The intersection is denoted by '∩' and read as 'AND'. The Venn diagram of A ∩ B is shown in Fig. 2.3.

Two sets of A and B are termed mutually exclusive or disjoint sets when A and B have no elements in common i.e., A ∩ B = ∅. This can be represented by Venn diagram as shown in Fig. 2.4.

Table 2.1 Laws of set theory

Name of the law	Description
Identity law	A ∪ ∅ = A; A ∪ U = U
	A ∩ ∅ = ∅; A ∩ U = A
Idempotency law	A ∪ A = A
	A ∩ A = A
Commutative law	A ∪ B = B ∪ A
	A ∩ B = B ∩ A
Associative law	A ∪ (B ∪ C) = (A ∪ B) ∪ C
	A ∩ (B ∩ C) = (A ∩ B) ∩ C
Distributive law	A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C)
	A ∪ (B ∩ C) = (A ∪ B) ∩ (A ∪ C)
Complementation law	$A \cup \overline{A} = U$ $A \cap \bar{A} = \Phi$ $\bar{\bar{A}} = A$
De Morgan's laws	$(\overline{A \cup B}) = \bar{A} \cap \bar{B}$ $(\overline{A \cap B}) = \bar{A} \cup \bar{B}$

2.1.2 *Laws of Set Theory*

Some important laws of set theory are enumerated in the Table 2.1.

2.1.3 *Boolean Algebra*

Boolean algebra finds its extensive use in evaluation of reliability and safety procedures due to consideration that components and system can present in either success or failure state. Consider a variable 'X' denotes the state of a component and assuming 1 represents success and 0 represents failure state. Then, probability that X is equal to 1 P(X = 1) is called reliability of that particular component. Depending upon the configuration of the system, it will also have success or failure state. Based on this binary state assumption, Boolean algebra can be conveniently used.

In Boolean algebra all the variables must have one of two values, either 1 or 0. There are three Boolean operations, namely, OR, AND and NOT. These operations are denoted by +, . (dot) and $\overline{\quad}$ (super bar over the variable) respectively. A set of postulates and useful theorems are listed in Table 2.2. X denotes a set and $x_{1,}$ $x_{2,}$ x_3 denote variables of X.

Consider a function of f(x_1, x_2, $x_{3,}$ …, x_n) of n variables, which are combined by Boolean operations. Depending upon the values of constituent variables x_1, x_2, …, x_n, function f will be 1 or 0. As these are n variables and each can have two possible values 1 or 0, 2^n combinations of variables will have to be considered for determination of the value of function f. Truth tables are used represent the value of f for

Table 2.2 Boolean algebra theorems

Postulate/Theorem	Remarks
$x + 0 = x$ $x \cdot 1 = x$	Identity
$x + x = x$ $x \cdot x = x$	Idempotence
$\bar{0} = 1$ *and* $\bar{1} = 0$	
$\bar{\bar{x}} = x$	Involution
$x_1 + x_1x_2 = x_1$ $x_1(x_1 + x_2) = x_1$	Absorption
$x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$ $x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$	Associative
$\overline{(x_1 + x_2)} = \bar{x}_1 \cdot \bar{x}_2$ $\overline{(x_1 \cdot x_2)} = \bar{x}_1 + \bar{x}_2$	De Morgan's theorem

Table 2.3 Truth table

x_1	x_2	x_3	F
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

all these combinations. A truth table is given for a Boolean expression $f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_1x_3$ in the following Table 2.3.

In reliability calculations, it is necessary to minimize the Boolean expression in order to eliminate repetition of the same elements. The premise of all minimization techniques is the set of Boolean algebra theorems mentioned in the Table 2.2. The amount of labor involved in minimization increases as the number of variable increase. Geometric methods and famous Karnaugh's map is applicable only up to six number of variables. Nowadays, sophisticated computerized algorithms are available for calculation with large number of variables.

2.2 Concepts of Probability Theory

The word 'experiment' is used in probability and statistics to describe any process of observation that generates raw data. An experiment becomes 'random experiment' if it satisfies the following conditions: it can be repeatable, outcome is random (though it is possible to describe all the possible outcomes) and pattern of occurrence is definite if the experiment is repeated large number of times. Examples of random experiment are tossing of coin, rolling die, and failure times of engineering equipment from its life testing. The set of all possible outcomes of a random experiment is known as 'sample space' and is denoted by 'S'. The sample space for random experiment of rolling a die is {1, 2, 3, 4, 5, and 6}. In case of life testing of engineering equipment, sample space is from 0 to ∞. Any subset of sample space is known as an event 'E'. If the outcome of the random experiment is contained in E then once can say that E has occurred. Probability is used to quantify the likelihood, or chance, that an outcome of a random experiment will occur. Probability is associated with any event E of a sample space S depending upon its chance of occurrence which is obtained from available data or information.

The concept of the probability of a particular event is subject to various meanings or interpretations. There are mainly three interpretations of probability: classical, frequency, and subjective interpretations.

The classical interpretation of probability is based on the notion of equally likely outcomes and was originally developed in the context of games of chance in the early days of probability theory. Here the probability of an event E is equal to the number of outcomes comprising that event (n) divided by the total number of possible outcomes (N). This interpretation is simple, intuitively appealing, and easy to implement, but its applicability is, of course, limited by its restriction to equally likely outcomes. Mathematically, it is expressed as follows:

$$P(E) = \frac{n}{N} \tag{2.1}$$

The relative-frequency interpretation of probability defines the probability of an event in terms of the proportion of times the event occurs in a long series of identical trials. In principle, this interpretation seems quite sensible. In practice, its use requires extensive data, which in many cases are simply not available and in other cases may be questionable in terms of what can be viewed as 'identical trials. Mathematically, it is expressed as follows;

$$P(E) = Lim_{N\to\infty} \frac{n}{N} \tag{2.2}$$

The subjective interpretation of probability views probability as a degree of belief, and this notion can be defined operationally by having an individual make certain comparisons among lotteries. By its very nature, a subjective probability is the probability of a particular person. This implies, of course, that different people can have different probabilities for the same event. The fact that subjective probabilities can be manipulated according to the usual mathematical rules of probability is not transparent but can be shown to follow from an underlying axiomatic framework.

Regardless of which interpretation one gives to probability, there is general consensus that the mathematics of probability is the same in all cases.

2.2.1 Axioms of Probability

Probability is a number that is assigned to each member of a collection of events from a random experiment that satisfies the following properties:

If *S* is the sample space and *E* is any event in a random experiment,

1. P(S) = 1
2. $0 \leq P(E) \leq 1$
3. For two events E_1 and E_2 with $E_1 \cap E_2 = \varnothing$, $P(E_1 \cup E_2) = P(E_1) + P(E_2)$

The property that $0 \leq P(E) \leq 1$ is equivalent to the requirement that a relative frequency must be between 0 and 1. The property that $P(S) = 1$ is a consequence of the fact that an outcome from the sample space occurs on every trial of an experiment. Consequently, the relative frequency of *S* is 1. Property 3 implies that if the events *E*1 and *E*2 have no outcomes in common, the relative frequency of outcomes in is the sum of the relative frequencies of the outcomes in *E*1 and *E*2.

2.2.2 Calculus of Probability Theory

Independent Events and Mutually Exclusive Events

Two events are said to be 'independent' if the occurrence of one does not affect the probability of occurrence of other event. Let us say A and B are two events, if the occurrence of A does not provide any information about occurrence of B then A and B are statistically independent. For example in a process plant, the failure of a pump does not affect the failure of a valve.

Two events are said to be 'mutually exclusive' if the occurrence of one event makes the non-occurrence of other event. If the occurrence of A ensures that B will not happen then A and B are mutually exclusive. If two events are mutually exclusive then they are dependent events. Success and failure events of any component are mutually exclusive. In a given time, if pump is successfully operating implies failure has not taken place.

Conditional Probability

The concept of conditional probability is the most important in all of probability theory. It is often interest to calculate probabilities when some partial information concerning the result of the experiment is available, or in recalculating them in the light of additional information. Let there be two event A and B, the probability of A given that B has occurred is referred as conditional probability and is denoted by $P(A|B) = P(A \cap B)/P(B)$.

If the event B occurs then in order for A to occur it is necessary that the actual occurrence be a point in both A and B, i.e. it must be in $A \cap B$ (Fig. 2.5). Now, since we know that B has occurred, it follows that B becomes our new sample space and hence the probability that the event $A \cap B$ occurs will equal the probability of $A \cap B$ relative to the probability of B. It is mathematical expressed as,

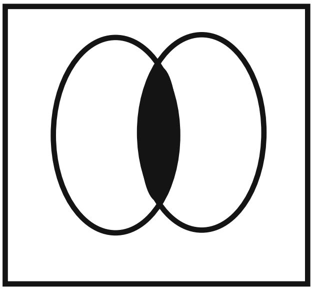


Fig. 2.5 Venn diagram for A ∩ B

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \tag{2.3}$$

Similarly one can write

$$P(B|A) = \frac{P(A \cap B)}{P(A)} \tag{2.4}$$

Probability for Intersection of Events

From Eq. 2.4, one can write

$$P(A \cap B) = P(A) \times P(B|A) \tag{2.5}$$

If A and B are independent events then the conditional probability P(B|A) is equal to P(B) only. Now Eq. 2.5 becomes, simply the product of probability of A and probability of B.

$$P(A \cap B) = P(A) \times P(B) \tag{2.6}$$

Thus when A and B are independent, the probability that A and B occur together is simply the product of the probabilities that A and B occur individually.

In general the probability of occurrence of n dependent events E_1, E_2, …, E_n is calculated by the following expression,

$$\begin{aligned} P(E_1 \cap E_2 \cap \cdots \cap E_n) = {} & P(E_1) \times P(E_2|E_1) \\ & \times P(E_3|E_1 \cap E_2) \ldots P(E_n|E_1 \cap E_2 \cap \cdots \cap E_{n-1}) \end{aligned}$$

If all the events are independent then probability of joint occurrence is simply the product of individual probabilities of events.

$$P(E_1 \cap E_2 \cap \cdots \cap E_n) = P(E_1) \times P(E_2) \times P(E_3) \times \cdots \times P(E_n) \tag{2.7}$$

Probability for Union of Events

Let A and B are two events. From the Venn diagram (Fig. 2.6), as the three regions 1, 2 and 3 are mutually exclusive, it follows that

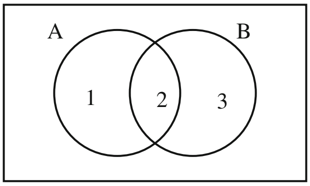


Fig. 2.6 Venn diagram for A and B

$$\begin{aligned}
&P(A \cup B) = P(1) + P(2) + P(3) \\
&P(A) = P(1) + P(2) \\
&P(B) = P(2) + P(3) \\
&\mathit{which\,shows\,that} \\
&P(A \cup B) = P(A) + P(B) - P(2) \\
&As\,P(2) = P(A \cap B), \\
&P(A \cup B) = P(A) + P(B) - P(A \cap B)
\end{aligned} \tag{2.8}$$

The above expression can be extended to n events E_1, E_2, …, E_n by the following equation

$$\begin{aligned}
P(E_1 \cup E_2 \cup \cdots \cup E_n) &= P(E_1) + P(E_2) + \cdots + P(E_n) \\
&- [P(E_1 \cap E_2) + P(E_2 \cap E_3) + \cdots + P(E_{n-1} \cap E_n)] + \\
&+ [P(E_1 \cap E_2 \cap E_3) + P(E_2 \cap E_3 \cap E_4) + \cdots + P(E_{n-2} \cap E_{n-1} \cap E_n)] - \\
&\vdots \\
&(-1)^{n+1} P(E_1 \cap E_2 \cap \cdots \cap E_n)
\end{aligned} \tag{2.9}$$

Total Probability Theorem

Let A_1, A_2 … A_n be n mutually exclusive events forming a sample space S and P (A_i) > 0, i = 1, 2 … n (Fig. 2.7). For an arbitrary event B one has

$$\begin{aligned}
B = B \cap S = B \cap (A_1 \cup A_2 \cup \cdots \cup A_n) \\
= (B \cap A_1) \cup (B \cap A_2) \cup \cdots \cup (B \cap A_n)
\end{aligned}$$

where the events B ∩ A_1, B ∩ A_2,…, B ∩ A_n are mutually exclusive.

$$P(B) = \sum_i P(B \cap A_i) = \sum_i P(A_i) P(B|A_i) \tag{2.10}$$

This is called total probability theorem.

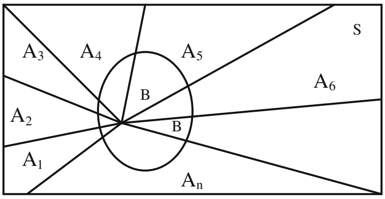


Fig. 2.7 Sample space containing n mutually exclusive events

Bayes Theorem

From the definitions of conditional probability,

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

$$P(A \cap B) = P(B) \times P(A|B) - (a)$$

$$P(B|A) = \frac{P(A \cap B)}{P(A)}$$

$$P(A \cap B) = P(A) \times P(B|A) - (b)$$

Equating both (a) and (b) we have: $P(B) \times P(A|B) = P(A) \times P(B|A)$.

We can obtain P(A|B) as follows

$$P(A|B) = \frac{P(A) \times P(B|A)}{P(B)} \tag{2.11}$$

This is a useful result that enables us to solve for P(A|B) in terms of P(B|A).

In general, if *P*(*B*) is written using the Total Probability theorem, we obtain the following general result, which is known as *Bayes' Theorem.*

$$P(A_i|B) = \frac{P(A_i)P(B|A_i)}{\sum_i P(A_i)P(B|A_i)} \tag{2.12}$$

Bayes' theorem presents a way to evaluate posterior probabilities $P(A_i|B)$ in terms of prior probabilities $P(A_i)$ and conditional probabilities $P(B|A_i)$. This is very useful in updating failure data as more evidence is available from operating experience.

The basic concepts of probability and statistics are explained in detail in the Refs. [1, 2].

2.2.3 Random Variables and Probability Distributions

It is important to represent the outcome from a random experiment by a simple number. In some cases, descriptions of outcomes are sufficient, but in other cases, it is useful to associate a number with each outcome in the sample space. Because the particular outcome of the experiment is not known in advance, the resulting value of our variable is not known in advance. For this reason, random variables are used to associate a number with the outcome of a random experiment. A random variable is defined as a function that assigns a real number to each outcome in the sample space of a random experiment. A random variable is denoted by a capital letter and numerical value that it can take is represented by a small letter. For example, if X is a random variable representing number of power outages in a plant, then x shows the actual number of outages it can take say 0, 1, 2…n.

Random variable can be classified into two categories, namely, discrete and continuous random variables. A random variable is said to be discrete if its sample space is countable. The number of power outages in a plant in a specified time is discrete random variable. If the elements of the sample space are infinite in number and sample space is continuous, the random variable defined over such a sample space is known as continuous random variable. If the data is countable then it is represented with discrete random variable and if the data is measurable quantity then it is represented with continuous random variable.

Discrete Probability Distribution

The probability distribution of a random variable *X* is a description of the probabilities associated with the possible values of *X*. For a discrete random variable, the distribution is often specified by just a list of the possible values along with the probability of each. In some cases, it is convenient to express the probability in terms of a formula.

Let X be a discrete random variable defined over a sample space $S = \{x_1, x_2 \ldots x_n\}$. Probability can be assigned to each value of sample space S. It is usually denoted by f(x). For a discrete random variable *X*, a probability distribution is a function such that

(a) $f(x_i) \geq 0$

(b) $\sum_{i=1}^{n} f(x_i) = 1$

(c) $f(x_i) = P(X = x_i)$

Probability distribution is also known as probability mass function. Some examples are Binomial, Poisson, Geometric distributions. The graph of a discrete probability distribution looks like a bar chart or histogram. For example, in five flips of a coin, where X represents the number of heads obtained, the probability mass function is shown in Fig. 2.8.

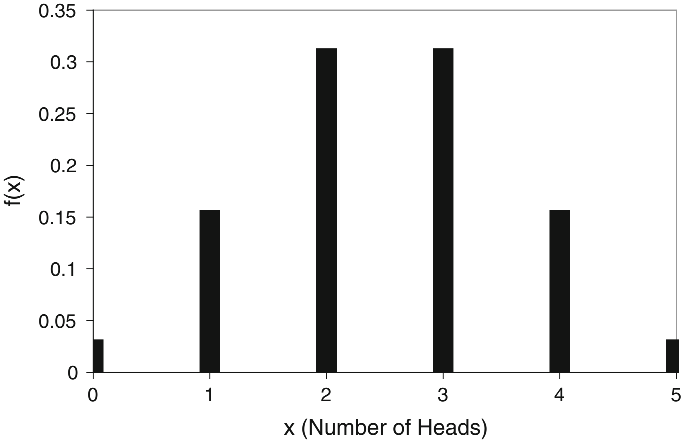


Fig. 2.8 A discrete probability mass function

The cumulative distribution function of a discrete random variable X, denoted as F(x), is

$$F(x) = P(X \leq x) = \sum_{x_i \leq x} f(x_i)$$

F(x) satisfies the following properties for a discrete random variable X.

(a) $F(x) = P(X \leq x) = \sum_{x_i \leq x} f(x_i)$
(b) $0 \leq F(x) \leq 1$
(c) $if\ x \leq y\ then\ F(x) \leq F(y)$

The cumulative distribution for the coin flipping example is given in Fig. 2.9.

Continuous Probability Distributions
As the elements of sample space for a continuous random variable X are infinite in number, probability of assuming exactly any of its possible values is zero. Density functions are commonly used in engineering to describe physical systems. Similarly, a probability density function *f*(*x*) can be used to describe the probability distribution of a continuous random variable *X*. If an interval is likely to contain a value for *X*, its probability is large and it corresponds to large values for *f*(*x*). The probability that *X* is between *a* and *b* is determined as the integral of *f*(*x*) from *a* to *b*. For a continuous random variable *X*, a probability density function is a function such that

(a) $f(x) \geq 0$
(b) $\int\limits_{-\infty}^{+\infty} f(x) = 1$
(c) $P(a \leq X \leq b) = \int\limits_{a}^{b} f(x)dx$

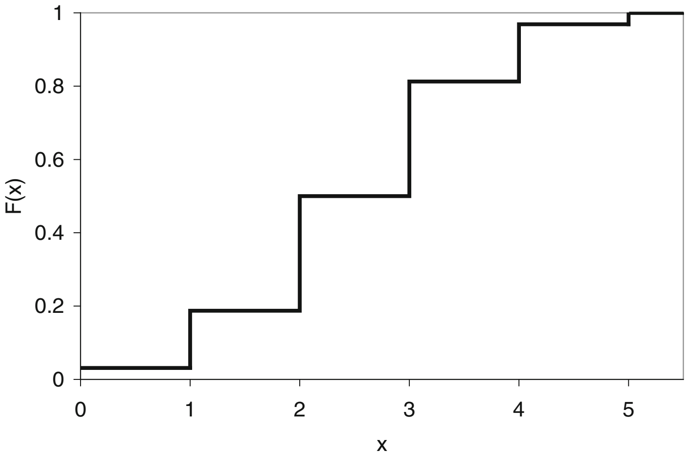


Fig. 2.9 A discrete cumulative distribution function

The cumulative distribution function of a continuous random variable X is

$$F(x) = P(X \leq x) = \int_{-\infty}^{x} f(\theta) d\theta \tag{2.13}$$

The probability density function of a continuous random variable can be determined from the cumulative distribution function by differentiating. Recall that the fundamental theorem of calculus states that

$$\frac{d}{dx} \int_{-\infty}^{x} f(\theta) d\theta = f(x)$$

Now differentiating F(x) with respect to x and rearranging for f(x)

$$f(x) = \frac{dF(x)}{dx} \tag{2.14}$$

Characteristics of Random Variables

In order to represent probability distribution function of a random variable, some characteristic values such as expectation (mean) and variance are widely used. Expectation or mean value represents the central tendency of a distribution function. It is mathematically expressed as

$$
\begin{aligned}
Mean = E(x) &= \sum_i x_i f(x_i) \quad \text{for discrete} \\
&= \int_{-\infty}^{+\infty} x f(x) dx \quad \text{for continuous}
\end{aligned}
$$

A measure of dispersion or variation of probability distribution is represented by variance. It is also known as central moment or second moment about the mean. It is mathematically expressed as

$$
\begin{aligned}
Variance = E((x - mean)^2) &= \sum_x (x - mean)^2 f(x) \quad \text{for discrete} \\
&= \int_{-\infty}^{+\infty} (x - mean)^2 f(x) dx \quad \text{for continuous}
\end{aligned}
$$

2.3 Reliability and Hazard Functions

Let ‘T’ be a random variable representing time to failure of a component or system. Reliability is probability that the system will perform it expected job under specified conditions of environment over a specified period of time. Mathematically, reliability can be expressed as the probability that time to failure of the component or system is greater than or equal to a specified period of time (t).

$$R(t) = P(T \geq t) \tag{2.15}$$

As reliability denotes failure free operation, it can be termed as success probability. Conversely, probability that failure occurs before the time t is called failure probability or unreliability. Failure probability can be mathematically expressed as the probability that time to failure occurs before a specified period of time t.

$$\bar{R}(t) = P(T < t) \tag{2.16}$$

As per the probability terminology, $\bar{R}(t)$ is same as the cumulative distributive function of the random variable T.

$$F(t) = \bar{R}(t) = P(T < t) \tag{2.17}$$

Going by the first axiom of probability, probability of sample space is unity. The sample space for the continuous random variable T is from 0 to ∞. Mathematically, it is expressed as

$$\begin{aligned} P(S) &= 1 \\ P(0 < T < \infty) &= 1 \end{aligned}$$

The sample space can be made two mutually exclusive intervals: one is T < t and the second is $T \geq t$. Using third axiom of probability, we can write

$$\begin{aligned} P(0 < T < \infty) &= 1 \\ P(T < t \cup T \geq t) &= 1 \\ P(T < t) + P(T \geq t) &= 1 \end{aligned}$$

Substituting Eqs. 2.15 and 2.17, we have

$$F(t) + R(t) = 1 \tag{2.18}$$

As the time to failure is a continuous random variable, the probability of T having exactly a precise t will be approximately zero. In this situation, it is appropriate to introduce the probability associated with a small range of values that the random variable can take on.

$$P(t < T < t + \Delta t) = F(t + \Delta t) - F(t)$$

Probability density function f(t) for continuous random variables is defined as

$$\begin{aligned} f(t) &= \underset{\Delta t \to 0}{Lt} \left[\frac{P(t < T < t + \Delta t)}{\Delta t} \right] \\ &= \underset{\Delta t \to 0}{Lt} \left[\frac{F(t + \Delta t) - F(t)}{\Delta t} \right] \\ &= \frac{dF(t)}{dt} \\ &= -\frac{dR(t)}{dt} \ (\textit{from Eq.}\ 2.18) \end{aligned}$$

From the above derivation we have an important relation between R(t), F(t) and f(t):

$$f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt} \tag{2.19}$$

Given the Probability Density Function (PDF), f(t) (Fig. 2.10), then

$$
\begin{aligned}
F(t) &= \int_0^t f(t)dt \\
R(t) &= \int_t^\infty f(t)dt
\end{aligned}
\tag{2.20}
$$

The conditional probability of a failure in the time interval from t to (t + Δt) given that the system has survived to time t is

$$P(t \le T \le t + \Delta t | T \ge t) = \frac{R(t) - R(t + \Delta t)}{R(t)}$$

Then $\frac{R(t)-R(t+\Delta t)}{R(t)\Delta t}$ is the conditional probability of failure per unit of time (failure rate).

$$
\begin{aligned}
\lambda(t) &= \lim_{\Delta t \to 0} \frac{R(t) - R(t + \Delta t)}{R(t)\Delta t} = \lim_{\Delta t \to 0} \frac{-[R(t + \Delta t) - R(t)]}{\Delta t} \frac{1}{R(t)} \\
&= \frac{-dR(t)}{dt} \frac{1}{R(t)} = \frac{f(t)}{R(t)}
\end{aligned}
\tag{2.21}
$$

λ(t) is known as the instantaneous hazard rate or failure rate function.

Reliability as a function of hazard rate function can be derived as follows:We have the following relation from the above expression

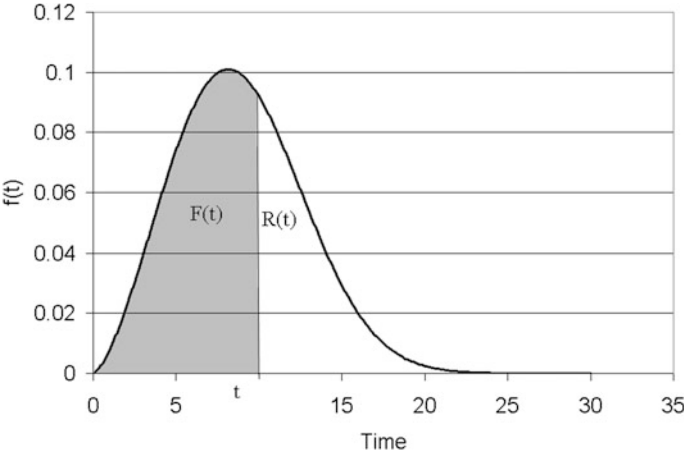


Fig. 2.10 Probability distribution function

$$\lambda(t) = \frac{-dR(t)}{dt}\frac{1}{R(t)}$$
$$\lambda(t)dt = \frac{-dR(t)}{R(t)}$$

Integrating and simplifying, we have

$$R(t) = \exp\left[-\int_0^t \lambda(\theta)d\theta\right] \tag{2.22}$$

2.4 Distributions Used in Reliability and Safety Studies

This section provides the most important probability distributions used in reliability and safety studies. They are grouped into two categories, namely, discrete probability distributions and continuous probability distributions.

2.4.1 Discrete Probability Distributions

2.4.1.1 Binomial Distribution

Consider a trial in which the only outcome is either success or failure. A random variable X with this trail can have success (X = 1) or failure (X = 0). The random variable X is said to be Bernoulli random variable if the probability mass function of X is given by

$$P(X = 1) = p$$
$$P(X = 0) = 1 - p$$

where p is the probability that the trial is success. Suppose now that n independent trials, each of which results in a ‘success’ with probability ‘p’ and in a ‘failure’ with probability 1 − p, are to be performed. If X represents the number of success that occur in the n trials, then X is said to be a binomial random variable with parameters n, p. The probability mass function of binomial random variable is given by

$$P(X = i) = {}^{n}c_{i}p^{i}(1 - p)^{n-i} \quad i = 0,\ 1,\ 2,\ldots,n \tag{2.23}$$

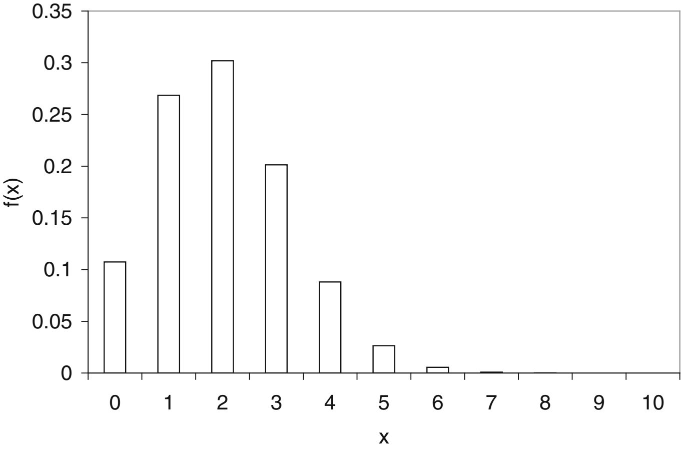


Fig. 2.11 Binomial probability mass function

The probability mass function of a binomial random variable with parameter (10, 0.2) is presented in Fig. 2.11.

The cumulative distributive function is given by

$$P(X \le i) = \sum_{j=0}^{i} {}^{n}c_j p^j (1-p)^{n-j} \tag{2.24}$$

Mean of the binomial distribution is calculated as follows

$$\begin{aligned} E(x) &= \sum xf(x) \\ &= \sum_{i=0}^{n} i \times {}^{n}c_i p^i (1-p)^{n-i} \\ &= np \sum_{i=1}^{n} {}^{n-1}c_{i-1} p^{i-1} (1-p)^{n-i} \\ &= np \sum_{j=0}^{m} {}^{m}c_j p^{j-1} (1-p)^{m-j} \\ &= np \end{aligned}$$

Similarly variance can also be derived as

$$Variance = npq$$

Example 1 It has been known from the experience that 4 % of hard disks produced by a computer manufacture are defective. Find the probability that out of 50 disks tested, what is the probability of having (i) Zero Defects and (ii) All are defective.

Solution: q = 4 % of hard disks produced by a computer manufacture are defective.

We know,

$$\begin{aligned} \mathrm{p} + \mathrm{q} &= 1 \\ \mathrm{p} &= 1 - \mathrm{q} \\ &= 1 - 0.04 \\ \mathrm{p} &= 0.96 \end{aligned}$$

According to Binomial Distribution,

$$P(X = x) = n\boldsymbol{C}_x \cdot p^x \cdot q^{n-x}$$

Now,

(i) *In case of 'zero defects', i.e. p(X = 0)*

$$P(X = 0) = n\boldsymbol{C}_x \cdot\ p^x \cdot q^{n-x} = {}^{50}C_0 \cdot (0.04)^0 \cdot (0.96)^{(50-0)} = 0.1299$$

(ii) *In case of 'all are defective', i.e. p(X = 50)*

$$P(X = 50) = n\boldsymbol{C}_x \cdot p^x \cdot q^{n-x} = ^{50} C_{50}(0.04)^{50}(0.96)^{(50-50)} = 0.8701$$

Or in other way,

$$\mathrm{P(X = 50) = 1 - P(X = 0) = 1 - 0.1299 = 0.8701}$$

Example 2 To ensure high reliability, triple modular[1] redundancy is adopted in instrumentation systems of Nuclear Power Plant (NPP). It is known that failure probability of each instrumentation channel from operating experience is 0.01. What is the probability of success of the whole instrumentation system?

Solution: q = failure probability from operation experience is 0.01.

We know, p = 1 − q = 1 − 0.01 = 0.99

According to Binomial Distribution,

[1] Triple modular redundancy denotes at least 2 instruments should be success out of 3 instruments.

Table 2.4 Calculations

	Formula	Numerical solutions	Value
(i)	$P(X = 0) = nC_x \cdot p^x \cdot q^{n-x}$	$P(0) = 3_{C_0}(0.99)^0 \cdot (0.01)^{(3-0)}$	P(0) = 1e-6
(ii)	$P(X = 1) = nC_x \cdot p^x \cdot q^{n-x}$	$P(0) = 3_{C_1}(0.99)^1 \cdot (0.01)^{(3-1)}$	P(1) = 2.9e-4
(iii)	$P(X = 2) = nC_x \cdot p^x \cdot q^{n-x}$	$P(0) = 3_{C_2}(0.99)^2 \cdot (0.01)^{(3-2)}$	P(2) = 2.9e-2
(iv)	$P(X = 3) = nC_x \cdot p^x \cdot q^{n-x}$	$P(0) = 3_{C_3}(0.99)^3 \ \cdot \ (0.01)^{(3-3)}$	P(3) = 0.97

$$P(X = x) = n\boldsymbol{C}_x \cdot p^x \cdot q^{n-x}$$

The sample space is then developed as in Table 2.4.

Now the failure probability is sum of (i) and (ii), which is obtained as 2.98e-4 and the success probability is sum of (iii) and (iv), which is obtained as 0.999702.

2.4.1.2 Poisson Distribution

Poisson distribution is useful to model when the event occurrences are discrete and the interval is continuous. For a trial to be a Poisson process, it has to satisfy the following conditions:

1. The probability of occurrence of one event in time Δt is λΔt where λ is constant
2. The probability of more than one occurrence is negligible in interval Δt
3. Each occurrence is independent of all other occurrences

A random variable X is said to have Poisson distribution if the probability distribution is given by

$$f(x) = \frac{e^{-\lambda t}(\lambda t)^x}{x!} \quad x = 0,\, 1,\, 2, \ldots \tag{2.25}$$

λ is known as average occurrence rate and x is number of occurrences of Poisson events.

The cumulative distribution function is given by

$$F(x) = \sum_{i=0}^{x} f(X = i) \tag{2.26}$$

The probability mass function and CDF for λ = 1.5/year and t = 1 year are shown in Fig. 2.12. Both the mean and variance of Poisson distribution is λt.

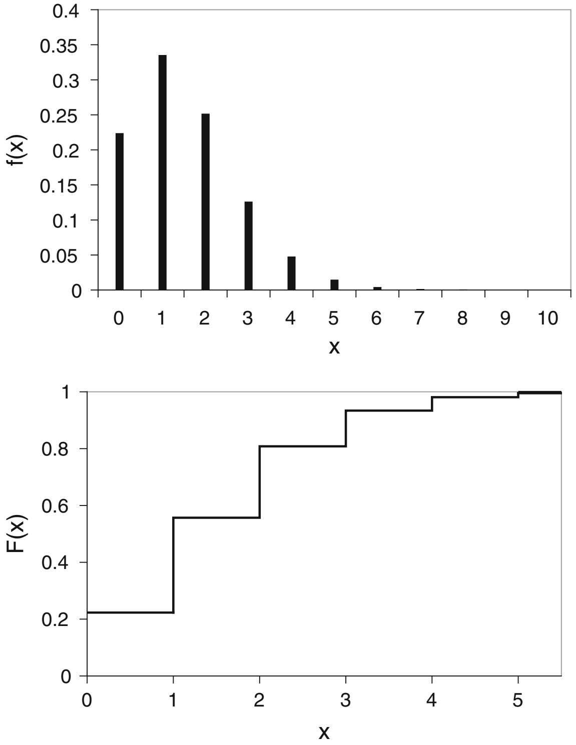


Fig. 2.12 Probability functions for Poisson distribution

If the probability of occurrence is near zero and sample size very large, the Poisson distribution may be used to approximate Binomial distribution.

Example 3 If the rate of failure for an item is twice a year, what is the probability that no failure will happen over a period of 2 years?

Solution: Rate of failure, denoted as λ = 2/year

$$\text{Time t} = 2\text{ years}$$

The Poisson probability mass function is expressed as

$$f(x) = \frac{e^{-\lambda t}(\lambda t)^x}{x!}$$

In a case of no failures, x = 0, which leads to

$$f(X=0)=\frac{e^{-2\times2}(2\times2)^0}{0!}=0.0183$$

2.4.1.3 Hyper Geometric Distribution

The hyper geometric distribution is closely related with binomial distribution .In hyper geometric distribution, a random sample of ‘n’ items is chosen from a finite population of N items. If N is very large with respect to n, the binomial distribution is good approximation of the hyper geometric distribution. The random variable ‘X’ denote x number of successes in the random sample of size ‘n’ from population N containing k number of items labeled success. The hyper geometric distribution probability mass function is

$$f(x)=p(x,N,n,k)={}^{K}c_{x}\cdot{}^{N-k}C_{n-x}/{}^{N}C_{n},\quad \mathrm{x}=0,1,2,3,4,\ldots,\mathrm{n}. \tag{2.27}$$

The mean of hyper geometric distribution is

$$E(x)=\frac{n{\cdot}K}{N} \tag{2.28}$$

The variance of hyper geometric distribution is

$$V(x)=\left(\frac{n{\cdot}K}{N}\right)\left(1-\frac{K}{N}\right)\left(\frac{N-n}{N-1}\right) \tag{2.29}$$

2.4.1.4 Geometric Distribution

In case of binomial and hyper geometric distribution, the number of trails ‘n’ is fixed and number of successes is random variable. Geometric distribution is used if one is interested in number of trails required to obtain the first success. The random variable in geometric distribution is number of trails required to get the first success.

The geometric distribution probability mass function is

$$\mathrm{f(x)=P(x;p)=p(1-p)}^{x-1},\quad \mathrm{x}=1,2,3,\ldots\ldots,\mathrm{n}. \tag{2.30}$$

where ‘p’ is the probability of success on a style trails.

The mean of geometric distribution is

$$E(x)=\frac{1}{p}$$

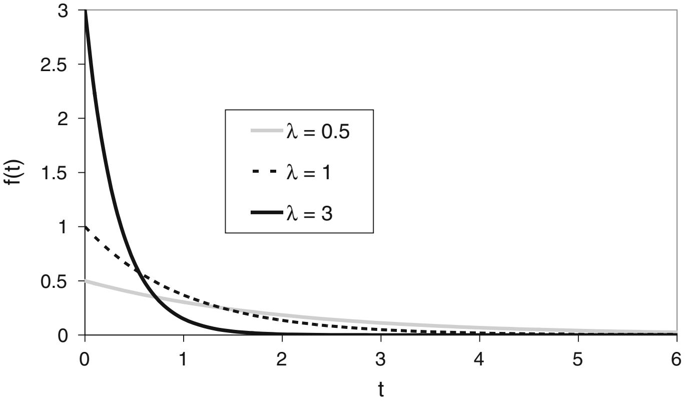


Fig. 2.13 Exponential probability density functions

The variable of geometric distribution is

$$V(x) = \frac{1-p}{p^2}$$

The geometric distribution is the only discrete distribution which exhibits the memory less property, as does the exponential distribution is the continuous case.

2.4.2 *Continuous Probability Distributions*

2.4.2.1 Exponential Distribution

The exponential distribution is most widely used distribution in reliability and risk assessment. It is the only distribution having constant hazard rate and is used to model 'useful life' of many engineering systems. The exponential distribution is closely related with the Poisson distribution which is discrete. If the number of failure per unit time is Poisson distribution then the time between failures follows exponential distribution. The probability density function (PDF) of exponential distribution is

$$\begin{aligned} f(t) &= \lambda e^{-\lambda t} \quad \mathit{for}\; 0 \le t \le \infty \\ &= 0 \qquad\quad \mathit{for}\; t < 0 \end{aligned} \tag{2.31}$$

The exponential probability density functions are shown in Fig. 2.13 for different values of λ.

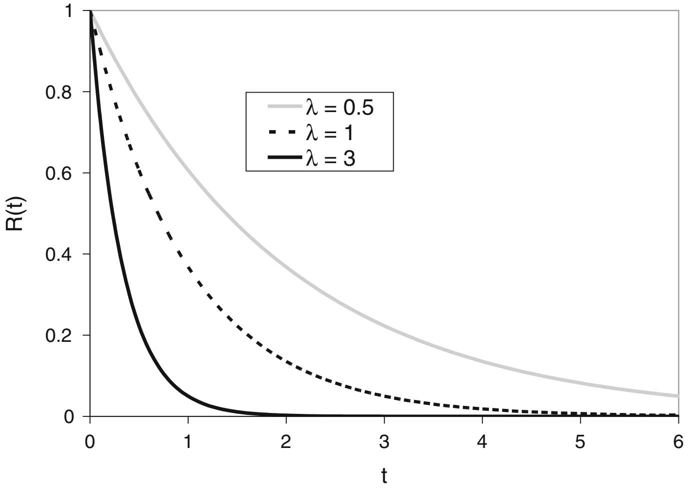


Fig. 2.14 Exponential reliability functions

The exponential cumulative distribution function can be derived from its PDF as follows,

$$F(t) = \int_0^t f(t)dt = \int_0^t \lambda e^{-\lambda t} dt = \lambda \left[\frac{e^{-\lambda t}}{-\lambda} \right]_0^t = \lambda \left[\frac{e^{-\lambda t}}{-\lambda} - \frac{1}{-\lambda} \right] = 1 - e^{-\lambda t} \quad (2.32)$$

Reliability function is complement of cumulative distribution function

$$R(t) = 1 - F(t) = e^{-\lambda t} \quad (2.33)$$

The exponential reliability functions are shown in Fig. 2.14 for different values of λ.

Hazard function is ratio of PDF and its reliability function, for exponential distribution it is

$$h(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda \quad (2.34)$$

The exponential hazard function is constant λ. This is reason for memory less property for exponential distribution. Memory less property means the probability of failure in a specific time interval is the same regardless of the starting point of that time interval.

Mean and Variance of Exponential Distribution

$$
\begin{aligned}
E(t) &= \int\limits_0^\infty tf(t) \\
&= \int\limits_0^\infty t\lambda e^{-\lambda t}dt
\end{aligned}
$$

Using integration by parts formula ($\int udv = uv - \int vdu$)

$$
\begin{aligned}
E(t) &= \lambda\left[t\cdot\frac{e^{-\lambda t}}{-\lambda}\bigg|_0^\infty - \int\limits_0^\infty \frac{e^{-\lambda t}}{-\lambda}dt\right] \\
&= \lambda\left[0+\frac{1}{\lambda}\left(\frac{e^{-\lambda t}}{-\lambda}\bigg|_0^\infty\right)\right] = \lambda\left[\frac{1}{\lambda}\left(\frac{1}{\lambda}\right)\right] = \frac{1}{\lambda}
\end{aligned}
$$

Thus mean time to failure of exponential distribution is reciprocal of failure rate.
Variance(t) = E(T^2) − (mean)^2

$$
E(T^2) = \int\limits_0^\infty t^2 f(t)dt = \int\limits_0^\infty t^2\lambda e^{-\lambda t}dt
$$

Using integration by parts formula

$$
\begin{aligned}
E(T^2) &= \lambda\left[t^2\cdot\frac{e^{-\lambda t}}{-\lambda}\bigg|_0^\infty - \int\limits_0^\infty \frac{e^{-\lambda t}}{-\lambda}(2t)dt\right] \\
&= \lambda\left[0+\frac{2}{\lambda^2}\int\limits_0^\infty t\lambda e^{-\lambda t}dt\right]
\end{aligned}
$$

But the integral term in the above expression is E(T) which is equal to 1/λ, substituting the same,

$$
E(T^2) = \lambda\left[0+\frac{2}{\lambda^2}\times\frac{1}{\lambda}\right] = \frac{2}{\lambda^2}
$$

Now variance is

$$
Variance = \frac{2}{\lambda^2} - \left(\frac{1}{\lambda}\right)^2 = \frac{1}{\lambda^2} \tag{2.35}
$$

Example 4 The failure time (T) of an electronic circuit board follows exponentially distribution with failure rate $\lambda = 10^{-4}$/h. What is the probability that (i) it will fail before 1000 h (ii) it will survive at least 10,000 h (iii) it will fail between 1000 and 10,000 h. Determine the (iv) mean time to failure and (v) median time failure also.

Solution:

(i) $\mathrm{P(T < 1000) = F(T = 1000)}$
For exponential distribution $F(T) = 1 - e^{-\lambda t}$ and substituting $\lambda = 10^{-4}$/h

$$\mathrm{P(T < 1000) = 1 - e^{-\lambda t} = 0.09516}$$

(ii) $P(T > 10{,}000) = R(T = 10{,}000)$
For exponential distribution $R(T) = e^{-\lambda t}$ and substituting $\lambda = 10^{-4}$/h

$$P(T > 10{,}000) = e^{-\lambda t} = 0.3678$$

(iii) $\mathrm{P(1000 < T < 10{,}000) = F(10{,}000) - F(1000) = [1 - R(10{,}000)] - F(1000)}$
From (i), we have F(1000) = 0.09516 and from (ii) we have R (10,000) = 0.3678,

$$\mathrm{P(1000 < T < 10{,}000) = [1 - 0.3678] - 0.09516 = 0.537}$$

(iv) Mean time to failure = $1/\lambda = 1/10^{-4}$ = 10,000 h
(v) *Median time to failure* denote the point where 50 % failures have already occurred, mathematically it is

$$R(T) = 0.5$$
$$e^{-\lambda t} = 0.5$$

Applying logarithm on both sides and solving for t,

$$t = \frac{-1}{\lambda}\ln(0.5) = 6931.47 \text{ h.}$$

2.4.2.2 Normal Distribution

The normal distribution is the most important and widely used distribution in the entire field of statistics and probability. It is also known as Gaussian distribution and it is the very first distribution introduced in 1733. The normal distribution often occurs in practical applications because the sum of large number of statistically

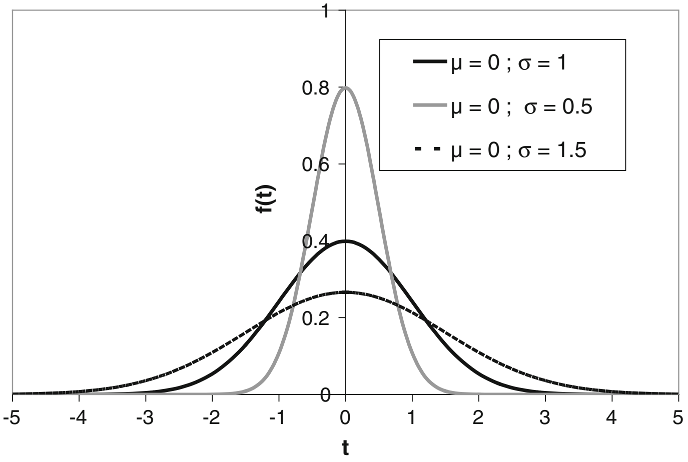


Fig. 2.15 Normal probability density functions

independent random variables converges to a normal distribution (known as central limit theorem). Normal distribution can be used to represent wear-out region of bath-tub curve where fatigue and aging can be modeled. It is also used in stress-strength interference models in reliability studies. The PDF of normal distributions is

$$f(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2}, \quad -\infty \leq t \leq \infty \tag{2.36}$$

where μ and σ are parameter of the distribution. The distribution is bell shaped and symmetrical about its mean with the spread of distribution determined by σ. It is shown in Fig. 2.15.

The normal distribution is not a true reliability distribution since the random variable ranges from −∞ to +∞. But if the mean μ is positive and is larger than σ by several folds, the probability that random variable T takes negative values can be negligible and the normal can therefore be a reasonable approximation to a failure process.

The normal reliability function and CDF are

$$R(t) = \int_{t}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt, \tag{2.37}$$

$$F(t) = \int_{-\infty}^{t} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt \tag{2.38}$$

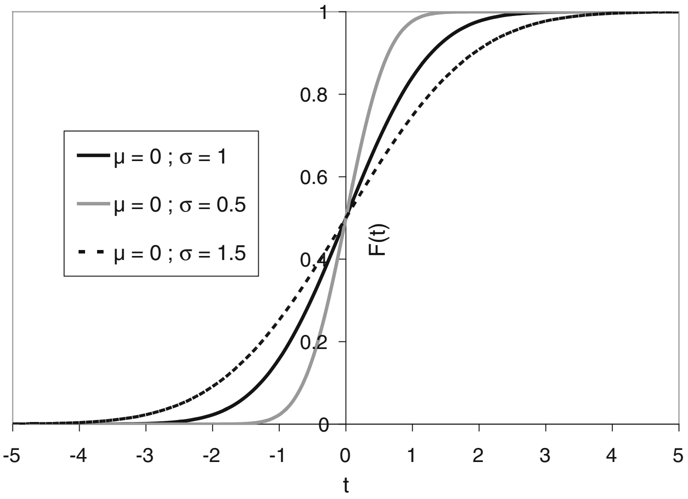


Fig. 2.16 Normal cumulative distribution functions

As there is no closed form solution to these integrals, the reliability and CDF are often expressed as a function of standard normal distribution (μ = 0 and σ = 1) (Fig. 2.16). Transformation to the standard normal distribution is achieved with the expression

$$z = \frac{t - \mu}{\sigma},$$

The CDF of z is given by

$$\phi(z) = \int_{-\infty}^{z} \frac{1}{\sqrt{2\pi}} e^{-\frac{z^2}{2}} dz \tag{2.39}$$

Table A.1 (see appendix) provides cumulative probability of the standard normal distribution. This can be used to find cumulative probability of any normal distribution. However, these tables are becoming unnecessary, as electronic spread sheets for example Microsoft Excel, have built in statistic functions.

The hazard function can expressed as

$$h(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1 - \Phi(z)} \tag{2.40}$$

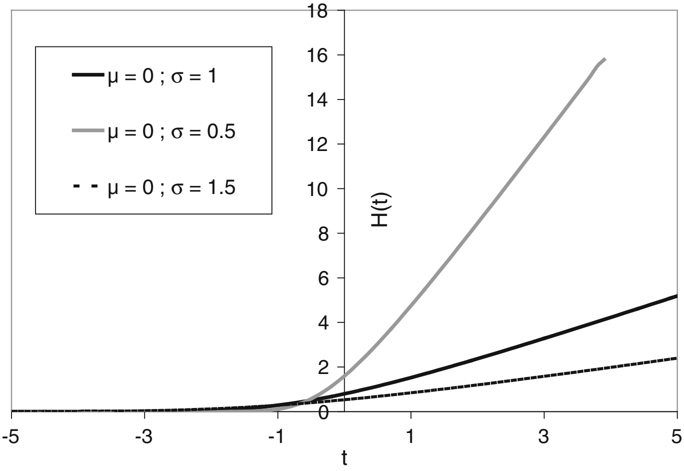


Fig. 2.17 Normal hazard rate functions

Hazard function is an increasing function as shown in Fig. 2.17. This feature makes it suitable to model aging components.

Example 5 Failure times are recorded from the life testing of an engineering component as 850, 890, 921, 955, 980, 1025, 1036, 1047, 1065, and 1120. Assuming a normal distribution, calculate the instantaneous failure rate at 1000 h?

Solution: Given data, n = 10, N = 1000; using the calculations from Table 2.5,

$$\text{Mean} = \bar{x} = \frac{\sum xi}{n} = \frac{9889}{10} = 988.9$$

Now, the sample S.D. is (σ)

$$\sigma = \sqrt{\frac{n\sum_{i=1}^{n} xi^2 - \left(\sum_{i=1}^{n} xi\right)^2}{n(n-1)}} = 84.8455$$

The instantaneous failure rate is given by the hazard function, and is established by

$$h(t) = \frac{f(t)}{R(t)} = \frac{f(1000)}{R(1000)} = \frac{\phi(z)}{1 - \Phi(z)} = \frac{0.0046619}{1 - 0.552} = 0.0104$$

Table 2.5 Calculations

xi	xi^2
850	722,500
890	792,100
921	848,241
955	912,025
980	960,400
1025	1,050,625
1036	1,073,296
1047	1,096,209
1065	1,134,225
1120	1,254,400
$\sum xi = 9889$	$\sum xi^2 = 9,844,021$

2.4.2.3 Lognormal Distribution

A continuous positive random variable T is lognormal distribution if its natural logarithm is normally distributed. The lognormal distribution can be used to model the cycles to failure for metals, the life of transistors and bearings and modeling repair times. It appears often in accelerated life testing as well as when a large number of statistically independent random variables are multiplied. The lognormal PDF is

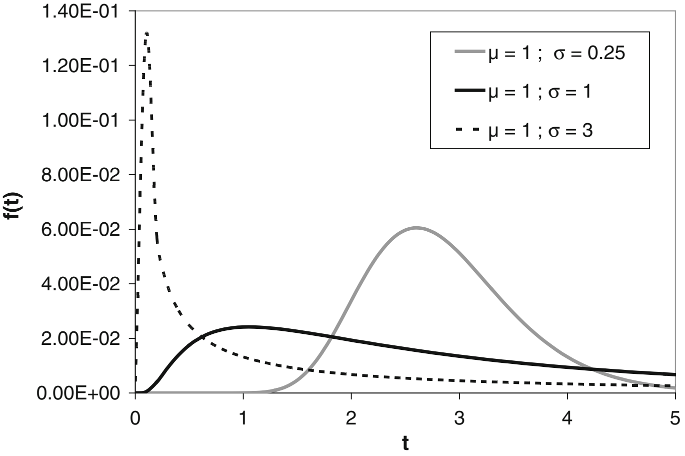


Fig. 2.18 Lognormal probability density functions

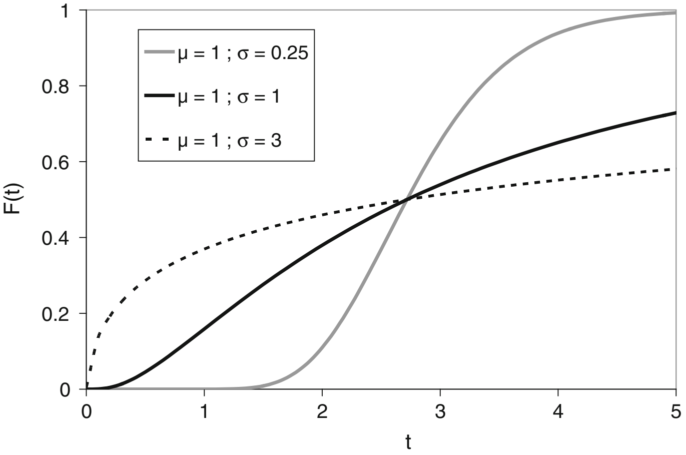


Fig. 2.19 Lognormal cumulative distribution functions

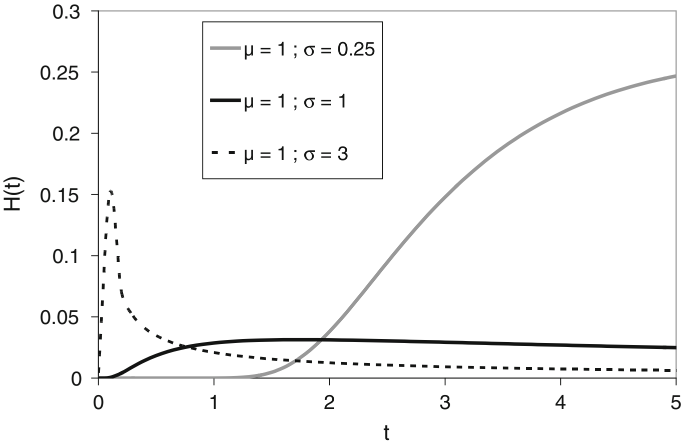


Fig. 2.20 Lognormal hazard functions

$$f(t) = \frac{1}{\sigma t\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{\ln t - \mu}{\sigma}\right)^2}, \quad t > 0 \tag{2.41}$$

where μ and σ are known as the location parameter and shape parameters respectively. The shape of distribution changes with different values of σ as shown in Fig. 2.18.

The lognormal reliability function and CDF are

$$R(t) = 1 - \Phi\left[\frac{\ln t - \mu}{\sigma}\right] \tag{2.42}$$

$$F(t) = \Phi\left[\frac{\ln t - \mu}{\sigma}\right] \tag{2.43}$$

Lognormal failure distribution functions and lognormal hazard functions are shown in Figs. 2.19 and 2.20.

The mean of lognormal distribution is

$$E(t) = e^{\mu + \frac{\sigma^2}{2}} \tag{2.44}$$

The variance of lognormal distribution is

$$V(t) = e^{(2\mu + \sigma^2)}(e^{\sigma^2} - 1) \tag{2.45}$$

Example 6 Determine the mean and variance of time to failure for a system having lognormally distributed failure time with μ = 5 years. And $\sigma = 0.8$.

Solution: The mean of lognormal distribution is,

$$E(t) = e^{\left(\mu + \frac{\sigma^2}{2}\right)}$$
$$E(t) = e^{\left(5 + \frac{0.8^2}{2}\right)} = 204.3839$$

The variance of lognormal distribution is,

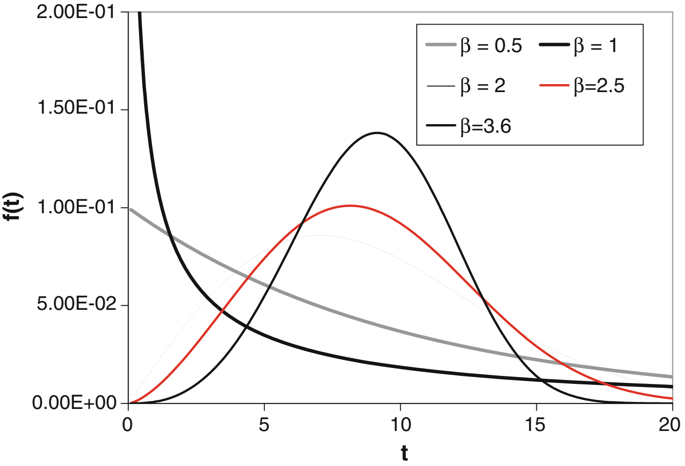


Fig. 2.21 Weibull PDF

Table 2.6 Distributions with different values of β

β	Remarks
1	Identical to exponential
2	Identical to Rayleigh
2.5	Approximates lognormal
3.6	Approximates normal

$$V(t) = e^{(2\mu+\sigma^2)} \times (e^{\sigma^2} - 1)$$
$$V(t) = e^{(10+(0.8)^2)} \times (e^{0.8^2} - 1)$$
$$V(t) = 37{,}448.49$$

2.4.2.4 Weibull Distribution

Weibull distribution was introduced in 1933 by Rosin and Rammler [3]. Weibull distribution has wide range of applications in reliability calculation due to its flexibility in modeling different distribution shapes. It can be used to model time to failure of lamps, relays, capacitors, germanium transistors, ball bearings, automobile tyres and certain motors. In addition to being the most useful distribution function in reliability analysis, it is also useful in classifying failure types, trouble shooting, scheduling preventive maintenance and inspection activities. The Weibull PDF is

$$f(t) = \frac{\beta}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1} e^{-\left(\frac{t}{\alpha}\right)^{\beta}}, \qquad \mathrm{t} > 0 \tag{2.46}$$

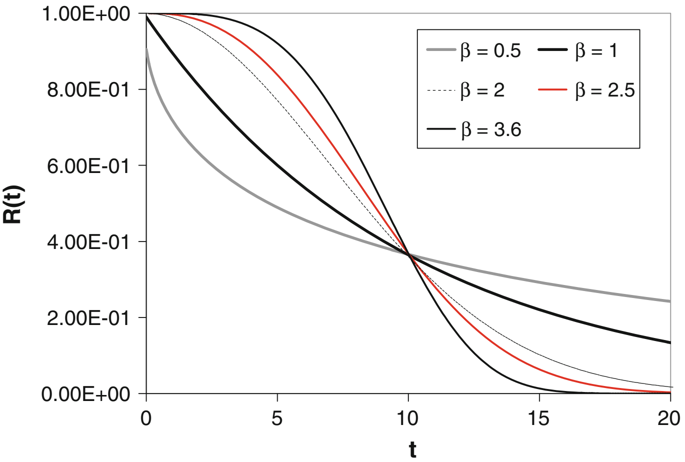


Fig. 2.22 Weibull reliability functions

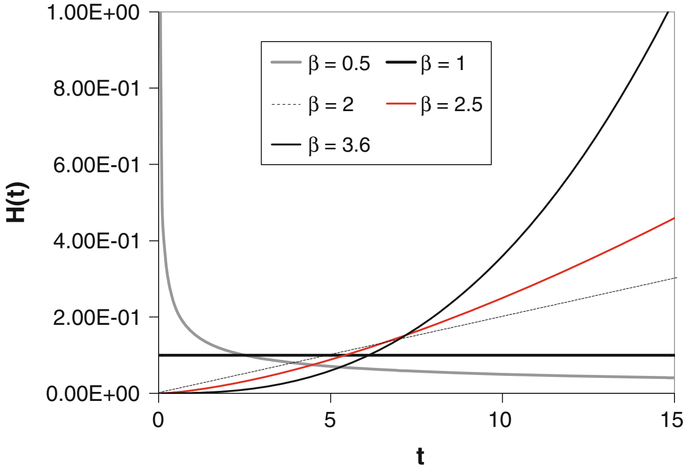


Fig. 2.23 Weibull hazard functions

where α and β are known as scale parameter (or characteristic life) and shape parameter respectively. An important property of Weibull distribution is as β increases, mean of the distribution approaches α and variance approaches zero. Its effect on the shape of distribution can be seen in Fig. 2.21 with different values of β (α = 10 is assumed in all the cases).

It is interesting to see from Fig. 2.21, all are equal to or approximately matching with several other distributions. Due to this flexibility, Weibull distribution provides a good model for much of the failure data found in practice. Table 2.6 summarizes this behavior.

Weibull reliability and CDF functions are

$$R(t) = e^{-\left(\frac{t}{\alpha}\right)^{\beta}} \tag{2.47}$$

$$F(t) = 1.0 - e^{-\left(\frac{t}{\alpha}\right)^{\beta}} \tag{2.48}$$

Reliability functions with different values of β are shown in Fig. 2.22.

The Weibull hazard function is

$$H(t) = \frac{\beta t^{\beta-1}}{\alpha^{\beta}} \tag{2.49}$$

The effects of β on the hazard function are demonstrated in Fig. 2.23. All three regions of bath-tub curve can be represented by varying β value.

β < 1 results in decreasing failure rate (burn-in period)
β = 1 results in constant failure rate (useful life period)
β > 1 results in increasing failure rate (Wear-out period)

The mean value of Weibull distribution can be derived as follows:

$$Mean = \int_0^\infty tf(t)dt = \int_0^\infty t\cdot\left(\frac{\beta}{\alpha}\right)\left(\frac{t}{\alpha}\right)^{\beta-1} e^{-\left(\frac{t}{\alpha}\right)^\beta} dt$$

$$\text{Let } x = \left(\frac{t}{\alpha}\right)^\beta,$$

$$dx = \left(\frac{\beta}{\alpha}\right)\left(\frac{t}{\alpha}\right)^{\beta-1} dt$$

Now mean = $\int_0^\infty t\, e^{-y}\, dy$

Since $t = \alpha\, x^{\frac{1}{\beta}}$

$$Mean = \alpha \int_0^\infty (x)^{\frac{1}{\beta}} e^{-x}\, dx = \alpha\, \Gamma\left(1 + \frac{1}{\beta}\right). \tag{2.50}$$

where $\Gamma(x)$ is known as gamma function.

$$\Gamma(x) = \int_0^\infty y^{x-1}\cdot e^{-y} dy$$

Similarly variance can be derived as

$$\sigma^2 = \alpha^2\left[\Gamma\left(1 + \frac{2}{\beta}\right) - \Gamma^2\left(1 + \frac{1}{\beta}\right)\right] \tag{2.51}$$

Example 7 The failure time of a component follows Weibull distribution with shape parameter β = 1.5 and scale parameter = 10,000 h. When should the component be replaced if the minimum recurred reliability for the component is 0.95?

Solution: Substituting into the Weibull reliability function gives,

$$R(t) = e^{-\left(\frac{t}{\alpha}\right)^\beta}$$

$$0.95 = e^{-\left(\frac{t}{10{,}000}\right)^{1.5}} \Rightarrow \frac{1}{0.95} = e^{\left(\frac{t}{10{,}000}\right)^{1.5}}$$

Taking natural logarithm on both sides

$$\ln\frac{1}{0.95} = \left(\frac{t}{10,000}\right)^{1.5}$$

Taking log on both sides,

$$\log 0.051293 = 1.5\log\frac{t}{10,000} \Rightarrow \frac{-1.2899}{1.5} = \log\frac{t}{10,000}$$

$$\Rightarrow -0.85996 = \log t - \log 10{,}000 \Rightarrow \log 10{,}000 - 0.85996 = \log t$$

$$\Rightarrow t = 1380.38 \text{ h}$$

2.4.2.5 Gamma Distribution

As the name suggests, gamma distribution derives its name from the well known gamma function. It is similar to Weibull distribution where by varying the parameter of the distribution wide range of other distribution can be derived. The gamma distribution is often used to model life time of systems. If an event takes place after ‘n’ exponentially distributed events take place sequentially, the resulting random variable follows a gamma distribution. Examples of its application include the time to failure for a system consisting of n independent components, with n − 1 components being stand by comp; time between maintenance actions for a system that requires maintenance after a fixed number of uses; time to failure of system which fails after n shocks. The gamma PDF is

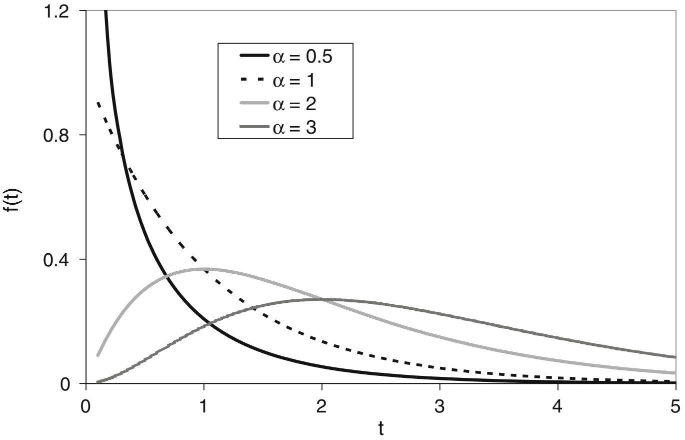


Fig. 2.24 Gamma probability density functions

Table 2.7 Distribution with different values of α

α	Distribution
$\alpha = 1$	Exponential distribution
$\alpha =$ integer	Erlangian distribution
$\alpha = 2$	Chi square distribution
$\alpha > 2$	Normal distribution

$$f(t) = \Gamma(t;\alpha,\beta) = \frac{\beta^{\alpha}}{\Gamma(\alpha)}\,t^{\alpha-1}e^{-\beta t},\ t \geq 0$$
$$where\ \Gamma(\alpha) = \int_{0}^{\infty} x^{\alpha-1}\,e^{-x}\,dx. \tag{2.52}$$

where α *and* β are parameters of distribution. The PDF with parameter $\beta = 1$ known as standardized gamma density function. By changing the parameter α, different well known distributions can be generated as shown in Fig. 2.24 and Table 2.7.

The CDF of random variable T having gamma distribution with parameter α *and* β is given by,

$$F(t) = P(T < t) = \int_{0}^{t} \frac{\beta^{\alpha}}{\Gamma(\alpha)} t^{\alpha-1}e^{-\beta t}dt \tag{2.53}$$

The gamma CDF in general does not have closed form solution. However, tables are available given the values of CDF having standard gamma distribution function.

The mean of gamma distribution is

$$E(T) = \frac{\alpha}{\beta} \tag{2.54}$$

The variable of gamma distribution is

$$V(T) = \frac{\alpha}{\beta^2} \tag{2.55}$$

For integer values of α, the gamma PDF is known as Erlangian probability density function.

2.4.2.6 Erlangian Distribution

Erlangian distribution is special case of gamma distribution where α is an integer. In this case PDF is express as,

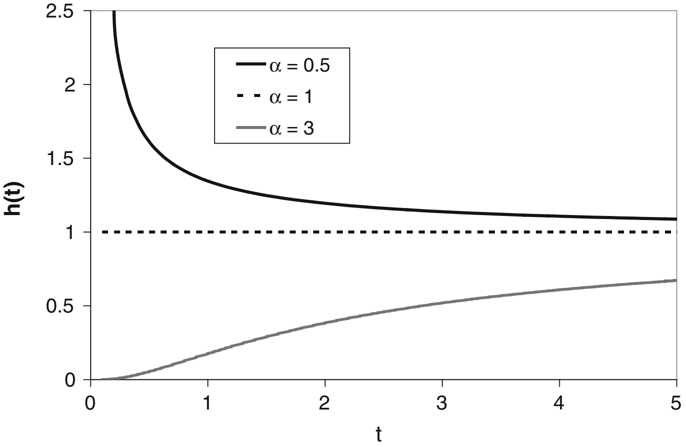


Fig. 2.25 Erlangian hazard functions

$$f(t) = \frac{t^{\alpha-1}}{\beta^{\alpha}(\alpha-1)!} \quad e^{\left(-\frac{t}{\beta}\right)} \tag{2.56}$$

The Erlangian reliability function is

$$R(t) = \sum_{k=0}^{\alpha-1} \frac{\left(\frac{t}{\beta}\right)^{k} e^{-\left(\frac{t}{\beta}\right)}}{k!} \tag{2.57}$$

The hazard function is

$$h(t) = \frac{t^{\alpha-1}}{\beta^{\alpha}\Gamma(\alpha)\sum_{k=0}^{\alpha-1}\frac{\left({}^{t}\!/_{\beta}\right)^{k}}{k!}} \tag{2.58}$$

By changing the value of α, all three phases of bath-tub curves can be selected (Fig. 2.25). If $\alpha < 1$, failure rate is decreasing, $\alpha = 1$, failure rate is constant and $\alpha > 1$, failure rate is increasing.

2.4.2.7 Chi-Square Distribution

A special case of the gamma distribution with $\alpha = 2$ and $\beta = 2/\nu$, a chi-square (χ^2) distribution is used to determinant of goodness of fit and confidence limits.

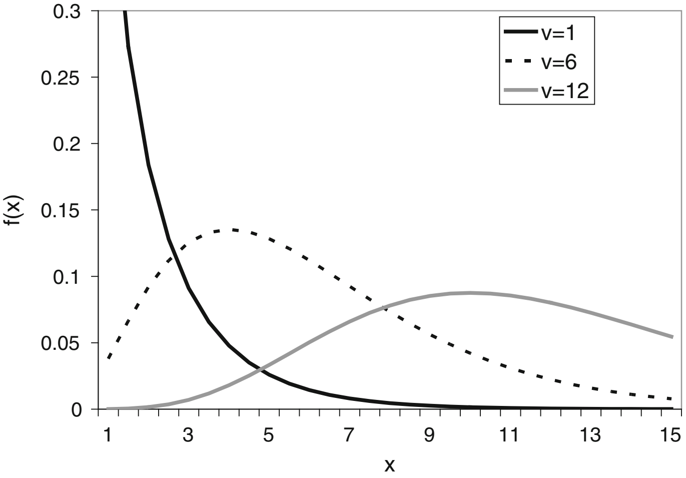


Fig. 2.26 PDF of Chi-Square

The chi-square probability density function is

$$\chi^2(x, v) = f(x) = \frac{1}{2^{v/2}\Gamma(v/2)} \mathrm{x}^{(v/2-1)} e^{-x/2}, \ \mathrm{x} > 0 \tag{2.59}$$

The shape of chi-square distribution is shown in Fig. 2.26.

The mean of chi-square distribution is $E(x) = v$.

The variance of chi-square distribution is $V(x) = 2v$.

If x_1, x_2,..., x_n are independent, standard normally distributed variables, then the sum of squares of random variable, i.e., $(\mathrm{X}_1^2 + \mathrm{X}_2^2 + \cdots + \mathrm{X}_v^2)$ is chi-square distribution with v degree of freedom.

It is interesting to note that the sum of two or more independent chi-square variables is also a chi-square variable with degree-of-freedom equal to the sum of degree-of-freedom for the individual variable. As v become large, the chi-square distribution approaches normal with mean v and variance $2v$.

2.4.2.8 F-Distribution

If χ_1^2 and χ_2^2 are independent chi-square random variable with v_1 and v_2 degrees of freedom, then the random variable F defined by

$$F = \frac{\chi_1^2/v_1}{\chi_2^2/v_2} \tag{2.60}$$

is said to have an F-distribution with v_1 and v_2 degrees of freedom.

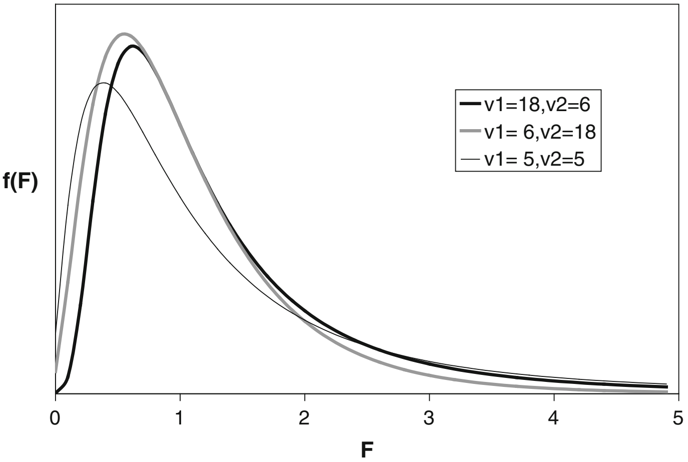


Fig. 2.27 F PDFs with different v_1 and v_2

The PDF of random variable F is given by

$$\mathrm{f(F)} = \left[\frac{\Gamma\left[\left(\frac{v_1+v_2}{2}\right)\right]\left(\frac{v_1}{v_2}\right)^{\frac{v_1}{2}}}{\Gamma\left(\frac{v_1}{2}\right)\Gamma\left(\frac{v_2}{2}\right)}\right]\left[\frac{F^{\frac{v_1}{2}-1}}{\left(1+v_1\frac{F}{v_2}\right)^{\left(\frac{v_1+v_2}{2}\right)}}\right], \quad \mathrm{F} > 0 \tag{2.61}$$

Figure 2.27 shows F PDF with different v_1 and v_2.

The values of F-distribution are available from tables. If $f_\alpha(v_1,v_2)$ represent area under the F pdf, with degree of freedom v_1 and v_2, to the right of α, then

$$F_{1-\alpha}(v_1, v_2) = \frac{1}{F_\alpha(v_2, v_1)} \tag{2.62}$$

It is interesting to observe that if s_1^2 and s_2^2 are the variance of independent random samples of size n_1 and n_2 drawn from normal population with variance of σ_1^2 and σ_2^2 respectively then the statistic

$$\mathrm{F} = \frac{\mathrm{s}_1/\sigma_1^2}{\mathrm{s}_2/\sigma_2^2} = \frac{\sigma_2^2 \cdot s_1^2}{\sigma_1^2 \cdot s_2^2} \tag{2.63}$$

has an F distribution with $v_1 = n_1 - 1$ and $v_2 = n_2 - 1$ degree of freedom.

2.4.2.9 t-Distribution

If Z is normally distributed random variable and the independent random variable χ^2 follows a chi square distribution with v degree of freedom then the random variable t defined by

$$t = \frac{z}{\sqrt{\chi^2/v}} \tag{2.64}$$

is said to be have t-distribution with v degree of freedom.

PDF of t is given by

$$f(t) \; = \frac{\Gamma\left(\frac{v+1}{2}\right)}{\Gamma(v/2)\sqrt{\Pi v}} \left[1 + \frac{t^2}{v}\right]^{\frac{-(v+1)}{2}}, \quad \infty \prec t \prec \infty. \tag{2.65}$$

Table 2.8 Summary of application areas

Distribution	Areas of application in reliability studies
Poisson distribution	To model occurrence rates such as failures per hour or defects per item (defects per computer chip or defects per automobile)
Binomial distribution	To model K out of M or voting redundancy such as triple modular redundancies in control and instrumentation
Exponential distribution	To model useful life of many items
	Life distribution of complex non-repairable systems
Weibull distribution	β > 1 often occurs in applications as failure time of components subjected to wear out and/or fatigue (lamps, relays, mechanical components)
	Scheduling inspection and preventive maintenance activities
Lognormal distribution	To model the cycles to failure for metals, the life of transistors, the life of bearings. Size distribution of pipe breaks
	To model repair time
	Prior parameter distribution in Bayesian analysis
Normal distribution	Modeling buildup of tolerances
	Load-resistance analysis (stress-strength interference)
	Life distribution of high stress components
Gamma distribution	To model time to failure of system with standby units
	To model time between maintenance actions
	Prior parameter distribution in Bayesian analysis
Chi-square distribution	Count the number of failures in an interval
	Applications involving goodness of fit and confidence limits
F distribution	To make inferences about variances and to construct confidence limits
t distribution	To draw inferences concerning means and to construct confidence intervals for means when the variances is unknown

Like the standard normal density, the t-density is symmetrical about zero. In addition, as v become larger, it becomes more and more like standard normal density.

Further,

$$\begin{aligned} & \mathrm{E}(\mathrm{t}) = 0 \\ \text{and} \quad & \mathrm{v}(\mathrm{t}) = \mathrm{v}/(\mathrm{v}-2) \quad \text{for } \mathrm{v} > 2. \end{aligned}$$

2.4.3 Summary

The summary of applications of the various distributions is described in the Table 2.8.

2.5 Failure Data Analysis

The credibility of any reliability/safety studies depend upon the quality of the data used. This section deals with the treatment of failure data and subsequent usage in reliability/safety studies. The derivation of system reliability models and various reliability measures is an application of probability theory, where as the analysis of failure data is primarily an application of statistics.

The objective of failure data analysis is to obtain reliability and hazard rate functions. This is achieved by two general approaches. The first is deriving empirical reliability and hazard functions directly from failure data. These methods are known as non parametric methods or empirical methods. The second approach is to identify an approximate theoretical distribution, estimate the parameter(s) of distribution, and perform a goodness of fit test. This approach is known as parametric method. Both the methods are explained in this section.

2.5.1 Nonparametric Methods

In this method empirical reliability distributions are directly derived from the failure data. The sources of failure data are generally from (1) Operational or field experience and/or (2) Failures generated from reliability testing. Nonparametric method is useful for preliminary data analysis to select appropriate theoretical distribution. This method is also finds application when no parametric distribution adequately fits the failure data.

Consider life tests on a certain unit under exactly same environment conditions with N number of units ensuring that failures of the individual units are independent and do not affect each other. At some predetermined intervals of time, the number of failed units is observed. It is assumed that test is carried out till all the units have failed. Now let us analyze the information collected through this test.

From the classical definition of probability, the probability of occurrence of an event A can be expressed as follows

$$P(A) = \frac{n_s}{N} = \frac{n_s}{n_s + n_f} \tag{2.66}$$

where

n_s is the number of favorable outcomes
n_f is number of unfavorable outcomes
N is total number of trials = $n_s + n_f$

When N number of units are tested, let us assume that $n_s(t)$ units survive the life test after time t and that $n_f(t)$ units have failed over the time t. Using the above equation, the reliability of such a unit can be expressed as:

$$R(t) = \frac{n_s(t)}{N} = \frac{n_s(t)}{n_s(t) + n_f(t)} \tag{2.67}$$

This definition of reliability assumes that the test is conducted over a large number of identical units.

The unreliability Q(t) of unit is the probability of failure over time t, equivalent to Cumulative Distribution Function (CDF) and is given by F(t),

$$Q(t) \equiv F(t) = \frac{n_f(t)}{N} \tag{2.68}$$

We know that the derivative of the CDF of a continuous random variable gives the PDF. In reliability studies, failure density function f(t) associated with failure time of a unit can be defined as follows:

$$f(t) \equiv \frac{dF(t)}{dt} = \frac{dQ(t)}{dt} = \frac{1}{N}\frac{dn_f}{dt} = \frac{1}{N}\underset{\Delta t \to 0}{Lim}\left\{\frac{n_f(t+\Delta t) - n_f(t)}{\Delta t}\right\} \tag{2.69}$$

Hazard rate can be derived from Eq. 2.21 by substituting f(t) and R(t) as expressed below

$$h(t) = \frac{1}{n_s(t)} \underset{\Delta t \to 0}{Lim} \left\{ \frac{n_f(t + \Delta t) - n_f(t)}{\Delta t} \right\} \tag{2.70}$$

Equations 2.67, 2.69 and 2.70 can be used for computing reliability, failure density and hazard functions from the given failure data.

The preliminary information on the underlying failure model can be obtained if we plot the failure density, hazard rate and reliability functions against time. We can define piece wise continuous functions for these three characteristics by selecting some small time interval Δt. This discretization eventually in the limiting conditions i.e., Δt → 0 or when the data is large would approach to the continuous function analysis. The number of interval can be decided based on the range of data and accuracy desired. But higher is the number of intervals, better would be the accuracy of results. However the computational effort increases considerably if we choose a large number of intervals. However, there exist an optimum number of intervals given by Sturges [4], which can be used to analyze the data. If n is the optimum number of intervals and N is the total number of failures, then

$$n = 1 + 3.3\,\mathrm{Log}_{10}(N) \tag{2.71}$$

Example 8 To ensure proper illumination in control rooms, higher reliability of electric-lamps is necessary. Let us consider that the failure times (in hours) of a population of 30 electric-lamps from a control room are given in the following Table 2.9. Calculate failure density, reliability and hazard functions?

Solution:

The optimum number of intervals as per Sturge's formula (Eq. 2.71) with N = 30 is

$$\mathrm{n} = 1 + 3.3\log(30) = 5.87$$

Table 2.9 Failure data

Lamp	Failure time	Lamp	Failure time	Lamp	Failure time
1	5495.05	11	3511.42	21	4037.11
2	8817.71	12	6893.81	22	933.79
3	539.66	13	1853.83	23	1485.66
4	2253.02	14	3458.4	24	4158.11
5	18,887	15	7710.78	25	6513.43
6	2435.62	16	324.61	26	8367.92
7	99.33	17	866.69	27	1912.24
8	3716.24	18	6311.47	28	13,576.97
9	12,155.56	19	3095.62	29	1843.38
10	552.75	20	927.41	30	4653.99

Table 2.10 Data in ascending order

Bulb	Failure time	Bulb	Failure time	Bulb	Failure time
1	99.33	11	1912.24	21	5495.05
2	324.61	12	2253.02	22	6311.47
3	539.66	13	2435.62	23	6513.43
4	552.75	14	3095.62	24	6893.81
5	866.69	15	3458.4	25	7710.78
6	927.41	16	3511.42	26	8367.92
7	933.79	17	3716.24	27	8817.71
8	1485.66	18	4037.11	28	12,155.56
9	1843.38	19	4158.11	29	13,576.97
10	1853.83	20	4653.99	30	18,887

In order to group the failure times under various intervals, the data is arranged in increasing order. Table 2.10 is the data with ascending order of failure times. The minimum and maximum of failure time is 99.33 and 18,887 respectively.

$$Interval\ size = \Delta t_i = \frac{18,887 - 99.33}{6} = 3131.27 \approx 3150$$

We can now develop a table showing the intervals and corresponding values of R(t), F(t), f(t) and h(t) respectively. The following notation is used. The summary of calculations is shown in Table 2.11.

$n_s(t_i)$ number of survivors at the beginning of the interval
$n_f(t_i)$ number of failures during ith interval

The plots of f(t) and h(t) are shown in Figs. 2.28 and 2.29 where as the plots of R (t) and F(t) are given in Fig. 2.30.

Table 2.11 Calculations

Interval	$n_s(t_i)$	$n_f(t_i)$	$R(t_i)$	$F(t_i)$	$f(t_i) = \frac{n_f(t_i)}{N\Delta t_i}$	$h(t_i) = \frac{n_f(t_i)}{n_s(t_i)\Delta t_i}$
0–3150	30	14	1	0	1.48e-4	1.48e-4
3151–6300	16	7	0.53	0.47	7.4e-5	1.38e-4
6301–9450	9	6	0.3	0.7	6.35e-5	2.11e-4
9451–12,600	3	1	0.1	0.9	1.06e-5	1.05e-4
12,601–15,750	2	1	0.066	0.934	1.06e-5	1.58e-4
15,751–18,900	1	1	0.033	0.967	1.06e-5	3.17e-4

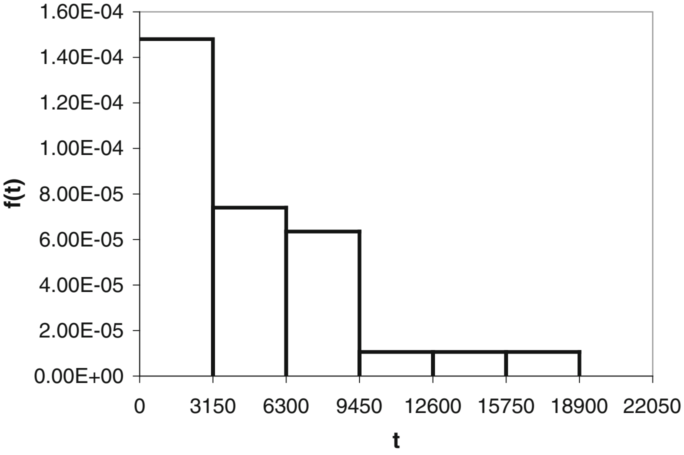


Fig. 2.28 Failure density function

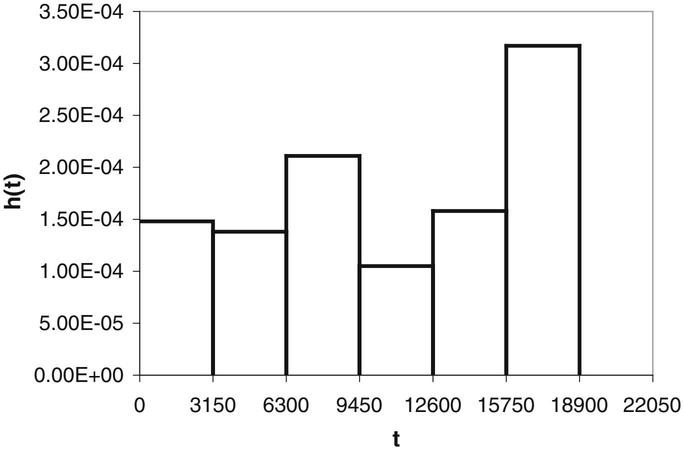


Fig. 2.29 Hazard rate function

2.5.2 Parametric Methods

Preceding section discussed methods for deriving empirical distributions directly from failure data. The second, and usually preferred, method is to fit a theoretical distribution, such as the exponential, Weibull, or normal distributions. As theoretical distributions are characterized with parameters, these methods are known as parametric method. Nonparametric methods have certain practical limitations compared with parametric methods.

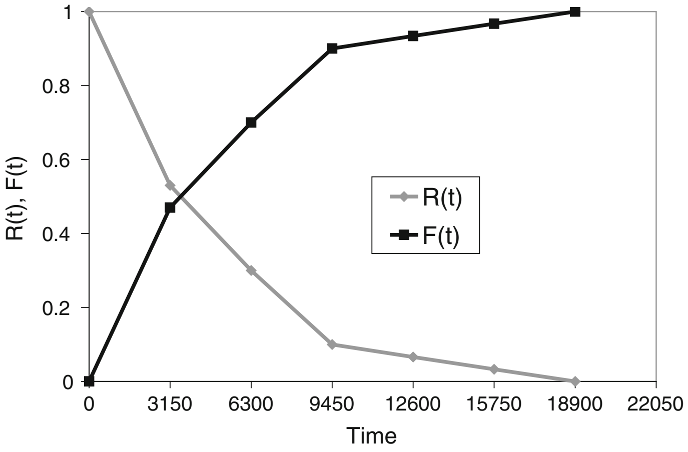


Fig. 2.30 Reliability function/CDF

1. As nonparametric methods are based on sample data, information beyond the range of data cannot be provided. Extrapolation beyond the censored data is possible with a theoretical distribution. This is significant in reliability/safety studies as the tails of the distribution attract more attention.
2. The main concern is determining the probabilistic nature of the underlying failure process. The available failure data may be simple a subset of the population of failure times. Establishing the distribution the sample came from and not sample itself is the focus.
3. The failure process is often a result of some physical phenomena that can be associated with a particular distribution.
4. Handling a theoretical model is easy in performing complex analysis.

In parametric approach, fitting of a theoretical distribution, consists of the following three steps:

1. Identifying candidate distribution
2. Estimating the parameters of distributions
3. Performing goodness-of-fit test

All these steps are explained in the following sections.

2.5.2.1 Identifying Candidate Distributions

In the earlier section on nonparametric methods, we have seen how one can obtain empirical distributions or histograms from the basic failure data. This exercise helps one to guess a failure distribution that can be possibly employed to model the failure data. But nothing has been said about an appropriate choice of the distribution. Probability plots provide a method of evaluating the fit of a set of data to a distribution.

A probability plot is a graph in which the scales have been changed in such a manner that the CDF associated with a given family of distributions, when represented graphically on that plot, becomes a straight line. Since straight lines are easily identifiable, a probability plot provided a better visual test of a distribution than comparison of a histogram with a PDF. Probability plots provide a quick method to analyze, interpret and estimate the parameters associated with a model. Probability plots may also be used when the sample size is too small to construct histograms and may be used with incomplete data.

The approach to probability plots is to fit a linear regression line of the form mentioned below to a set of transformed data:

$$y = mx + c \tag{2.72}$$

The nature of transform will depend on the distribution under consideration. If the data of failure times fit the assumed distribution, the transformed data will graph as a straight line.

Consider exponential distribution whose CDF is $F(t) = 1 - e^{-\lambda t}$, rearranging $1 - F(t) = e^{-\lambda t}$, taking the natural logarithm of both sides,

$$\begin{aligned} \ln(1 - F(t)) &= \ln(e^{-\lambda t}) \\ -\ln(1 - F(t)) &= \lambda t \\ \ln(\frac{1}{1 - F(t)}) &= \lambda t \end{aligned}$$

Comparing it with Eq. 2.72: $y = mx + c$, we have

$$\begin{aligned} y &= \ln(\frac{1}{1 - F(t)}) \\ m &= \lambda; x = t; c = 0; \end{aligned}$$

Now if y is plotted on the ordinate, the plot would be a straight line with a slope of λ.

The failure data is generally available in terms of the failure times of n items that have failed during a test conducted on the original population of N items. Since F(t) is not available, we can make use of $E[F(t_i)]$

$$E[F(t_i)] = \sum_{i=1}^{n} \frac{i}{N + 1} \tag{2.73}$$

Example 9 Table 2.12 gives chronological sequence of the grid supply outages at a process plant. Using probability plotting method, identify the possible distributions.

Table 2.12 Class IV power failure occurrence time since 01.01.1998

Failure number	Date/time	Time to failure (in days)	Time between failure (in days)
1	11.04.1998/14:35	101	101
2	17.06.1998/12:30	168	67
3	24.07.1998/09:19	205	37
4	13.08.1999/10:30	590	385
5	27.08.1999	604	14
6	21.11.1999	721	117
7	02.01.2000	763	42
8	01.05.2000/15:38	882	119
9	27.10.2000/05:56	1061	179
10	14.05.2001	1251	190
11	03.07.2001/09:45	1301	50
12	12.07.2002/18:50	1674	374
13	09.05.2003/08:43	1976	301
14	28.12.2005	2940	964
15	02.05.2006/11:02	3065	125
16	17.05.2007/11:10	3445	380
17	02.06.2007/16:30	3461	16

Table 2.13 Time between failure (TBF) values for outage of Class IV (for Weibull plotting)

I	Failure number	TBF (in days) (t)	F(t) = (i − 0.3)/(n + 0.4)	y = ln(ln(1/R(t))	x = ln(t)
1	5	14	0.04023	−3.19268	2.639057
2	17	16	0.097701	−2.27488	2.772589
3	3	37	0.155172	−1.78009	3.610918
4	7	42	0.212644	−1.43098	3.73767
5	11	50	0.270115	−1.1556	3.912023
6	2	67	0.327586	−0.92412	4.204693
7	1	101	0.385057	−0.72108	4.615121
8	6	117	0.442529	−0.53726	4.762174
9	8	119	0.5	−0.36651	4.779123
10	15	125	0.557471	−0.20426	4.828314
11	9	179	0.614943	−0.04671	5.187386
12	10	190	0.672414	0.109754	5.247024
13	13	301	0.729885	0.269193	5.70711
14	12	374	0.787356	0.437053	5.924256
15	16	380	0.844828	0.622305	5.940171
16	4	385	0.902299	0.844082	5.953243
17	14	964	0.95977	1.16725	6.871091

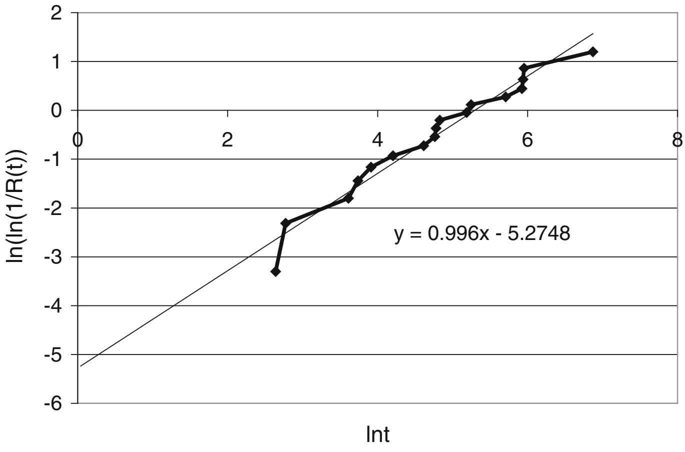


Fig. 2.31 Weibull plotting for the data

Table 2.14 Coordinates of distributions for probability plotting

Distribution	(x, y)	$y = mx + c$

Exponential $F(t) = 1 - e^{-\lambda t}$	$\left(t,\ \ln\left[\frac{1}{1-\hat{F}(t)}\right]\right)$	m = λ
		c = 0

Weibull $F(t) = 1 - e^{-(\frac{t}{\alpha})^{\beta}}$	$\left(\ln t,\ \ln\ln\left[\frac{1}{1-\hat{F}(t)}\right]\right)$	$m = \alpha$ $c = \ln(1/\beta)$
Normal $F(t) = \Phi\left[\frac{t-\mu}{\sigma}\right]$	$\left(t,\ \Phi^{-1}[F(t)]\right)$	$m = \dfrac{1}{\sigma}$ $c = \dfrac{-\mu}{\sigma}$

Solution:

Table 2.13 gives the summary of calculations for x and y coordinates. The same are plotted in Fig. 2.31.

The plot is approximated to a straight line as mentioned below

$$y = 0.996x - 5.2748$$

The shape parameter α = 0.996

Scale parameter, β = $e^{5.2748}$ = 194.4 days

As shape parameter is close to unity, the data fits exponential distribution.

Table 2.14 summarizes (x, y) coordinates of various distributions used in probability plotting.

2.5.2.2 Estimating the Parameters of Distribution

The preceding section on probability plotting focused on the identification of distribution for a set of data. Specification of parameters for the identified distribution is the next step. The estimation of parameters of the distribution by probability plotting is not considered to be best estimates. This is especially true in certain goodness of fit tests that are based on Maximum Likelihood Estimator (MLE) for the distribution parameters. There are many criteria based on which an estimator can be computed, viz., least square estimation and MLE. MLE provides maximum flexibility and is widely used.

Maximum Likelihood Estimates

Let the failure times, t_1, t_2,..., t_n represent observed data from a population distribution, whose PDF is $f(t|\theta_1,\ldots,\theta_k)$ where θ_i is the parameter of the distribution. Then the problem is to find likelihood function given by

$$L(\theta_1\ldots\theta_k) = \prod_{i=1}^{n} f(t_i|\theta_1\ldots\theta_k) \tag{2.74}$$

The objective is to find the values of the estimators of θ_1, ..., θ_k that render the likelihood function as large as possible for given values of t_1, t_2, ..., t_n. As the likelihood function is in the multiplicative form, it is to maximize log(L) instead of L but these two identical since maximizing L is equivalent to maximizing log(L).

By taking partial derivates of the equation with respect to θ_1,..., θ_k and setting these partial equal to zero, the necessary conditions for finding MLEs can be obtained.

$$\frac{\partial \ln L(\theta_1\ldots\theta_k)}{\partial\theta_i} = 0 \quad \mathrm{i} = 1, 2, \ldots, \mathrm{k} \tag{2.75}$$

Exponential MLE

The likelihood function for a single parameter exponential distribution whose PDF is $f(t) = \lambda e^{-\lambda t}$ is given by

$$L(t_1\ldots t_n|\lambda) = (\lambda e^{-\lambda t_1})(\lambda e^{-\lambda t_2})\ldots(\lambda e^{-\lambda t_n}) = \lambda^n e^{-\lambda\sum\limits_{j=1}^{n} t_j} \tag{2.76}$$

Taking logarithm, we have

$$\ln L(t_1, t_2, \ldots, t_n|\lambda) = n \ln\lambda - \lambda\sum\nolimits_{j=1}^{n} t_j \tag{2.77}$$

Partially differentiating the Eq. 2.77 with respect to λ and equating to zero, we have

$$\hat{\lambda} = \frac{n}{\sum_{j=1}^{n} t_j} \tag{2.78}$$

where $\hat{\lambda}$ is the MLE of λ.

Interval Estimation
The point estimates would provide the best estimate of the parameter where as the interval estimation would offer the bounds with in which the parameter would lie. In other words, it provides the confidence interval for the parameter. A confidence interval gives a range of values among which we have a high degree of confidence that the distribution parameter is included.

Since there is always an uncertainty associated in this parameter estimation, it is essential to find upper confidence and lower confidence limit of these two parameters.

Upper and Lower Confidence of the Failure Rate
The Chi square distribution is used to find out upper and lower confidence limits of Mean Time To Failure. The Chi square equation is given as follow

$$\theta_{LC} \equiv \frac{2T}{\chi^2_{2r,\alpha/2}} \tag{2.79}$$

$$\theta_{UC} \equiv \frac{2T}{\chi^2_{2r,1-\alpha/2}} \tag{2.80}$$

where

θ_{LC} and θ_{UC}	Lower and Upper Confidence limits of mean time to failure
r	Observed number of failures
T	Operating Time
α	Level of significance

The mean time represents the Mean Time Between Failure (MTBF) or Mean Time To Failure (MTTF). When failure model follows an exponential distribution, the failure rate can be expressed as

$$\lambda = \frac{1}{\theta}$$

Thus, the inverse of θ_{LC} and θ_{UC} will be the maximum and minimum possible value of the failure rate, i.e. the upper and lower confidence limit of the failure rate.

Upper and Lower Confidence Limit of the Demand Failure Probability:

In case of demand failure probability, F-Distribution is used to derive the upper and the lower confidence limit.

$$P_{LC} = \frac{r}{r + (D - r + 1)F_{0.95}(2D - 2r + 2, 2r)} \tag{2.81}$$

$$P_{UC} = \frac{(r + 1)F_{0.95}(2r + 2, 2D - 2r)}{D - r + (r + 1)F_{0.95}(2r + 2, 2D2r)} \tag{2.82}$$

where,

P_{LC} and P_{UC}	Lower and Upper Confidence limits for demand failure probabilities
r	number of failures
D	number of demands
$F_{0.95}$	95 % confidence limit for variables from F-distribution Table A.4.

Example 10 Estimate the point and 90 % confidence interval for the data given in the previous example on grid outage in a process plant.

Solution: Total Number of Outages: 17

Total Period: 10 year.
Mean failure rate = 17/10 = 1.7/year = 1.94×10^{-4}/h.

The representation of Lower (5 %) and Upper (95 %) limits of (Chi-square) χ^2 distribution is as follows for failure terminated tests is as follows;

$$\frac{\chi^2_{\alpha/2;2\gamma}}{2T} \leq \lambda \leq \frac{\chi^2_{1-\alpha/2;2\gamma}}{2T} \tag{2.83}$$

For the case under consideration

α	100 − 90 = 10 %;
n	17;
Degree of freedom	γ = n = 17;
T	10 year.

$$\frac{\chi^2_{0.05;2\cdot 17}}{2 \cdot 10} \leq \lambda \leq \frac{\chi^2_{0.95;+2\cdot 17}}{2 \cdot 10}$$

Obtaining the respective values from the χ^2 Table A.3, 1.077 ≤ λ ≤ 2.55.

The mean value of grid outage frequency is 1.7/year (1.94×10^{-4}/h) with lower and upper limit of 1.077/year (1.23×10^{-4}/h) and 2.55/year (2.91×10^{-4}/h) respectively.

2.5.2.3 Goodness-of-Fit Tests

The last step in the selection of a parametric distribution is to perform a statistical test for goodness of fit. Goodness-of-fit tests have the purpose to verify agreement of observed data with a postulated model. A typical example is as follows:

Given $t_1, t_2, \ldots, t_n$ as n independent observations of a random variable (failure time) t, a rule is asked to test the null hypothesis

H_0 The distribution function of t is the specified distribution

H_1 The distribution function of t is not the specified distribution

The test consists of calculating a statistic based on the sample of failure times. This statistic is then compared with a critical value obtained from a table of such values. Generally, if the test statistic is less than the critical value, the null hypothesis (H_0) is accepted, otherwise the alternative hypothesis (H_1) is accepted. The critical value depends on the level of significance of the test and the sample size. The level of significance is the probability of erroneously rejecting the null hypothesis in favor of the alternative hypothesis.

A number of methods are available to test how closely a set of data fits an assumed distribution. For some distribution functions used in reliability theory, particular procedures have been developed, often with different alternative hypotheses H_1 and investigation of the corresponding test power. Among the distribution free procedures, chi-square (χ^2) is frequently used in practical applications to solve the goodness-of-fit problems.

The chi-square (χ^2) goodness-of-fit test

The χ^2 test is applicable to any assumed distribution provided that a reasonably large number of data points are available. The assumption for the χ^2 goodness-of-fit tests is that, if a sample is divided into n cells (i.e. we have ν degrees of freedom where ν = n−1), then the values within each cell would be normally distributed about the expected value, if the assumed distribution is correct, i.e., if x_i and E_i are the observed and expected values for cell i:

$$\chi^2 = \sum_{i=1}^{n} \frac{(x_i - E_i)^2}{E_i} \tag{2.84}$$

If we obtain a very low χ^2 (e.g. less than the 10th percentile), it suggests that the data corresponds more closely to the proposed distribution. Higher values of χ^2 cast doubt on the null hypothesis. The null hypothesis is usually rejected when the value of

χ^2 falls outside the 90th percentile. If χ^2 is below this value, there is insufficient information to reject the hypothesis that the data come from the supposed distribution.

For further reading on treatment of statistical data for reliability analysis, interested readers may refer Ebeling [5] and Misra [6].

Exercise Problems

1. A continuous random variable T is said to have an exponential distribution with parameter λ, if PDF is given by $f(t) = \lambda e^{-\lambda t}$, calculate the mean and variance of T?
2. Given the following PDF for the random variable time to failure of a circuit breaker, what is the reliability for a 1500 h operating life?

$$f(t) = \frac{\beta}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1} e^{\left(\frac{t}{\alpha}\right)^{\beta}} \text{ with } \alpha = 1200\,\text{h and } \beta = 1.5.$$

3. Given the hazard rate function $\lambda(t) = 2 \times 10^{-5} t$, determine R(t) and f(t) at t = 500 h?
4. The diameter of bearing manufactured by a company under the specified supply conditions has a normal distribution with a mean of 10 mm and standard deviation of 0.2 mm

   (i) Find the probability that a bearing has a diameter between 10.2 and 9.8 mm?
   (ii) Find the diameters, such that 10 % of the bearings have diameters below the value?

5. While testing ICs manufactured by a company, it was found that 5 % are defective. (i) What is the probability that out of 50 ICs tested more than 10 are defective? (ii) what is the probability that exactly 10 are defective?
6. If the rate of failure for a power supply occurs at a rate of once a year, what is the probability that 5 failures will happen over a period of 1 year?
7. Given the following 20 failure times, estimate R(t), F(t), f(t), and λ(t): 100.84, 580.24, 1210.14, 1630.24, 2410.89, 6310.56, 3832.12, 3340.34, 1420.76, 830.24, 680.35, 195.68, 130.72, 298.76, 756.86, 270.39, 130.0, 30.12, 270.38, 720.12.
8. Using the data given in problem 7, identify possible distribution with the help of probability plotting method?

References

1. Ross SM (1987) Introduction to probability and statistics for engineers and scientists. Wiley, New York
2. Montgomery DC, Runger GC (1999) Applied statistics and probability for engineers. Wiley, New York
3. Weibull W (1951) A statistical distribution of wide applicability. J Appl Mech 18:293–297

4. Sturges HA (1976) The choice of class interval. J Am Stat Assoc 21:65–66
5. Ebeling CE (1997) An introduction to reliability and maintainability engineering. Tata McGraw-Hill Publishing Company Ltd, New Delhi
6. Misra KB (1992) Reliability analysis and prediction. Elsevier, Amsterdam

Chapter 3
System Reliability Modeling

This chapter presents basic system reliability modeling techniques such as reliability block diagram, Markov models, and fault tree analysis. System reliability is evaluated as a function of constituting components' reliabilities.

3.1 Reliability Block Diagram (RBD)

Reliability Block Diagram is a graphical representation of system's success logic using modular or block structures. It is easy to understand and system success paths can be visually verified. RBD approach integrates various components using sub-models/blocks. RBD can be evaluated using analytical methods to obtain system reliability.

Reliability modeling by RBD is primarily intended for non-repairable systems only, for example Space Systems (Space Shuttle etc.) adopt RBD techniques for reliability prediction. In most of electronic systems, though repair is possible replacement is the practical resort, hence RBD is widely used.

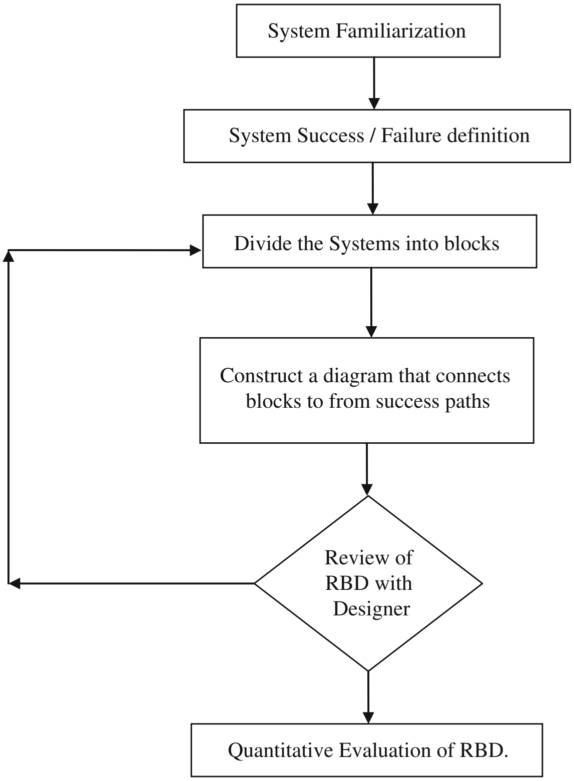
Nevertheless, RBD approach has limitations in considering different failure modes, external events (like human error) and priority of events. In such scenarios fault tree analysis and Markov models are recommended for modeling.

3.1.1 Procedure for System Reliability Prediction Using RBD

The procedure for constructing RBD is shown in Fig. 3.1 [1]. System familiarization is the prerequisite for doing reliability modeling. After system familiarization, one has to select a system success definition. If more than one definition is possible a separate reliability block diagram may be required for each. The next step is to divide the system into blocks of equipment to reflect its logical behaviors of the system so that each block is statistically independent and as large as possible. At

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_3

Fig. 3.1 Procedure for constructing RBD


System Familiarization
System Success / Failure definition
Divide the Systems into blocks
Construct a diagram that connects blocks to from success paths
Review of RBD with Designer
Quantitative Evaluation of RBD.

the same time each block should contain (where possible) no redundancy. For some of numerical evaluation, each block should contain only those items which follow the same statistical distributions for times to failure.

In practice it may be necessary to make repeated attempts at constructing the block diagram (each time bearing in mind the steps referred to above) before a suitable block diagram is finalized.

The next step is to refer to the system fault definition and construct a diagram that connects the blocks to form a 'success path'. As indicated in the diagrams that follow, various paths, between the input and output ports of blocks which must function in order that the system functions. If all the blocks are required to function for the system to function then the corresponding block diagram will be one to which all the blocks are joined in series as illustrated in Fig. 3.2.

In this diagram "I" is the input port, "O" the output port and R1, R2, R3…Rn are the blocks which together constitute the system. Diagram of the type are known as 'series reliability block diagrams'.

A different type of block diagram is needed when failure of one component or 'block' does not affect system performance as far as the system fault definition is concerned. If in the above instances the entire link is duplicated (made redundant),

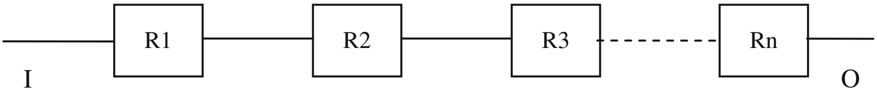


Fig. 3.2 Series model

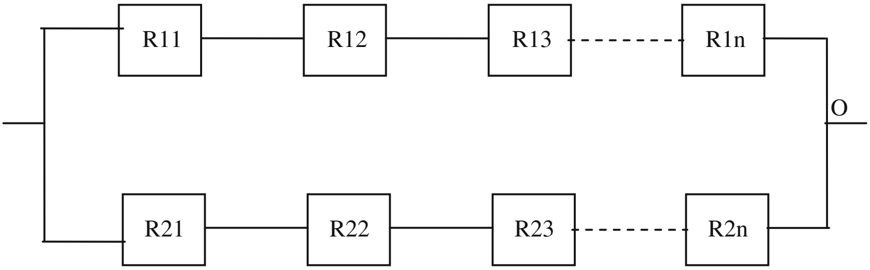


Fig. 3.3 Series—parallel model

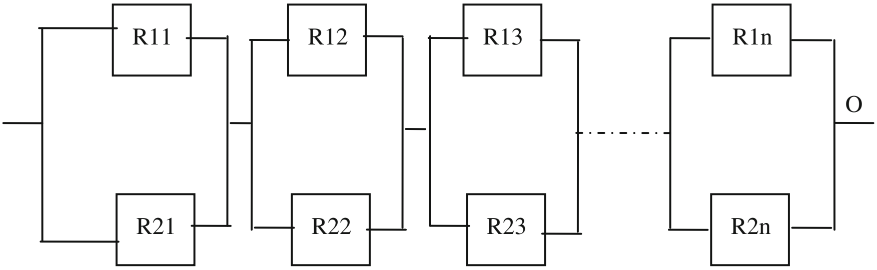


Fig. 3.4 Parallel—series model

then the block diagram is as illustrated by Fig. 3.3. If, however, each block within the link is duplicated the block diagram is as illustrated by Fig. 3.4.

Diagrams of this type are known as parallel reliability block diagrams. Block diagrams used for modeling system reliability are often mixtures of series and parallel diagrams.

Important Points to be Considered while Constructing RBDs

- Sound understanding of the system to be modeled is prerequisite for developing RBD.
- Failure criteria shall be explicitly defined.
- Environmental and operating considerations

The description of the environment conditions under which the system is designed to operate should be obtained. This may include a description of all the conditions to which the system will be subjected during transport, storage and use. A same component of a system is often used in more than one environment, for example, in a space satellite system, on ground, during the flight, in the orbit. In such scenario, reliability evaluation should be carried out using same RBD each time but using the appropriate failure rates for each environment.

- It should be noted RBD may not be synonymous with the physical interconnections of various constitute elements with in a system.
- The relationship between calendar time, operating time and ON/OFF cycles should be established.
- Apart from operational failure rates, the process of switching ON and OFF may also be considered depending upon instances.

3.1.2 Different Types of Models

The reliability of a system, $R_s(t)$, is the probability that a system can perform a required function under given conditions for a given time interval (0, t), in general it is defined by the relationship (Eq. 2.22):

$$R_S(t) = \exp[-\int_0^t \lambda(u) \cdot du] \tag{3.1}$$

where $\lambda(u)$ denotes the system failure rate at t = u, u being a dummy variable. In what follows Rs(t) will be written for simplicity as Rs. The unreliability of a system (probability of failure), Fs, is given by:

$$\mathrm{Fs(t)} = 1 - \mathrm{Rs(t)} \tag{3.2}$$

Series Model

For systems as illustrated by Fig. 3.2, all the elements have to function for the success of the system. The system reliability R_s is the probability of success of all the elements, given by:

$$R_s = P(A \cap B \cap C \cap \cdots \cap Z)$$

Assuming the events to be independent,

$$R_s = R_A R_B R_C \ldots R_z \tag{3.3}$$

That is by multiplying together the reliabilities of all the blocks constituting the system.

Example 1 A personal computer consists of four basic sub systems: motherboard (MB), hard disk (HD), power supply (PS) and processor (CPU). The reliabilities of four subsystems are 0.98, 0.95, 0.91 and 0.99 respectively. What is the system reliability for a mission of 1000 h?

Solution: As all the sub-systems need to be functioning for the overall system success, the RBD is series *configuration* as shown in Fig. 3.5.

The reliability of system is

$$R_{sys} = R_{MB} \times R_{HD} \times R_{PS} \times R_{CPU}$$
$$R_{sys} = 0.98 \times 0.95 \times 0.91 \times 0.99$$
$$R_{sys} = 0.8387$$

Parallel Model

For systems of the type illustrated by Fig. 3.6, all the elements have to fail for the system failure. The system unreliability $\mathrm{F_s}$ is the probability of failure of all the elements, is given by (Fig. 3.7):

$$F_s = P(\bar{A} \cap \bar{B})$$

Assuming the events to be independent,

$$F_s = F_A F_B \tag{3.4}$$

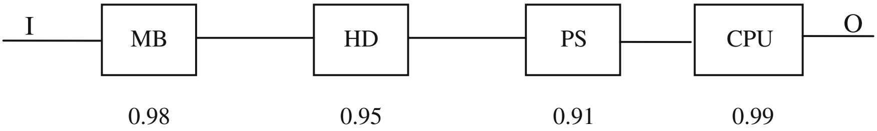


Fig. 3.5 RBD of typical computer

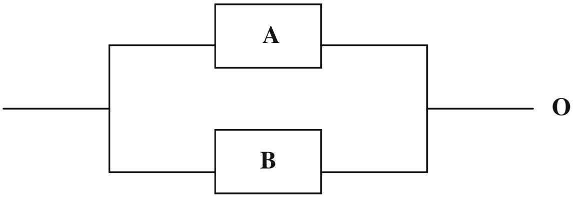


Fig. 3.6 Two unit parallel model

Hence system reliability (R_s) is given by

$$R_s = R_A + R_B - R_A R_B \tag{3.5}$$

Formulae (3.3) and (3.5) can be combined. Thus if we have a system as depicted by Fig. 3.3, but with only three items in each branch, the system reliability is:

$$R_s = R_{A1}R_{B1}R_{c1} + R_{A2}R_{B2}R_{c2} - R_{A1}R_{B1}R_{c1}R_{A2}R_{B2}R_{c2} \tag{3.6}$$

Similarly, For Fig. 3.4 we have:

$$R_s = (R_{A1} + R_{A2} - R_{A1}R_{A2})(R_{B1} + R_{B2} - R_{B1}R_{B2})(R_{C1} + R_{C2} - R_{C1}R_{C2}). \tag{3.7}$$

Example 2 To ensure safe shutdown of nuclear power plants (NPP) during normal or accidental conditions. There is a primary shutdown system and as a redundancy secondary shutdown system (SDS) is present. The failure probability of primarily SDS is 0.01 and secondary SDS is 0.035. Calculate the reliability of overall shutdown system of NPP?

Solution: As any SDS operation is sufficient for the success of overall shutdown system of NPP, the RBD is *Parallel configuration* as shown in Fig. 3.7.

The System reliability is given by,

$$\begin{aligned} R_{SYS} &= Rp + Rs - RpRs \\ Rp &= 1 - Fp = 1 - 0.01 = 0.99 \\ Rs &= 1 - Fs = 1 - 0.035 = 0.965 \\ Now&, \\ R_{SYS} &= Rp + Rs - RpRs \\ R_{SYS} &= 0.99 + 0.965 - (0.99 \times 0.965) \\ Rsys &= 0.9997 \end{aligned}$$

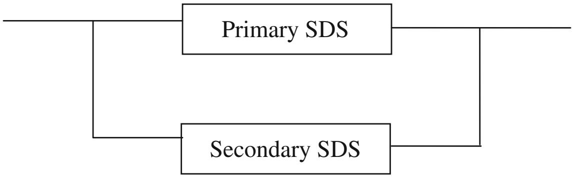


Fig. 3.7 Shutdown system

Example 3 In designing a computer based control system, two computers are being considered for having higher reliability. Designer-A is suggesting for redundancy at the system level, where as, designer-B is suggesting for redundancy at the sub-system level. Use the failure data from the Example 1 and recommend the better design.

Solution: *Designer A—Reliability evaluation*

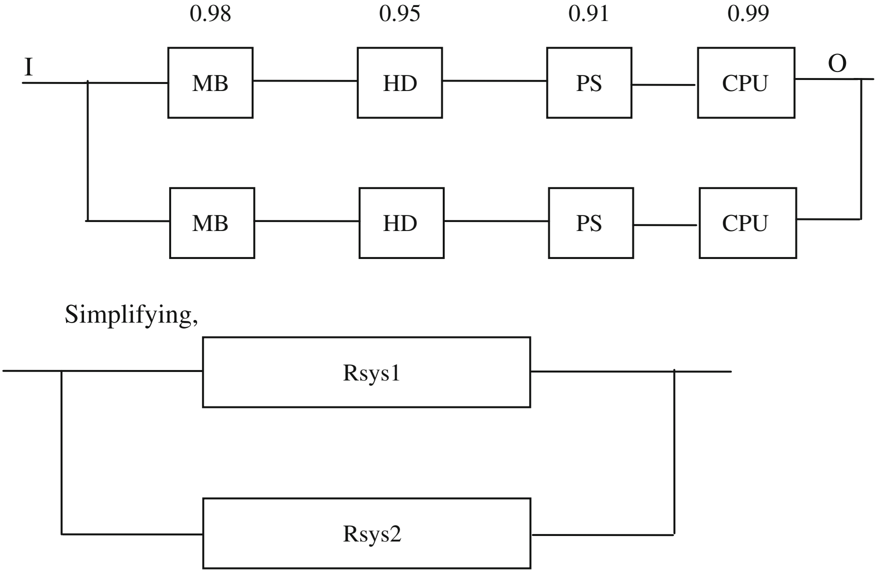
Consider redundancy at the system level will lead to the RBD shown in Fig. 3.8. Where,

$$\begin{aligned} Rsys1 &= R_{MB1} \times R_{HD1} \times R_{PS1} \times R_{cpu1} = 0.8387 \\ Rsys2 &= R_{MB2} \times R_{HD2} \times R_{PS2} \times R_{cpu2} = 0.8387 \\ R_{SYS} &= R_{SYS1} + R_{SYS2} - R_{SYS1} \times R_{SYS2} = 0.9740 \end{aligned}$$

Designer B Reliability evalution (Fig. 3.9)

$$\begin{aligned} R_{MB} &= R_{MB} + R_{MB} - R_{MB} \times R_{MB} = 0.9996 \\ R_{HD} &= R_{HD} + R_{HD} - R_{HD} \times R_{HD} = 0.9975 \\ R_{PS} &= R_{PS} + R_{PS} - R_{PS} \times R_{PS} = 0.9919 \\ R_{CPU} &= R_{CPU} + R_{CPU} - R_{CPU} \times R_{CPU} = 0.9999 \\ &Now, \\ R_{SYS} &= R_{MB} \times R_{HD} \times R_{PS} \times R_{CPU} = 0.9889 \end{aligned}$$

The proposed design of B is better than design of A.



Simplifying,

Fig. 3.8 Designer A RBD

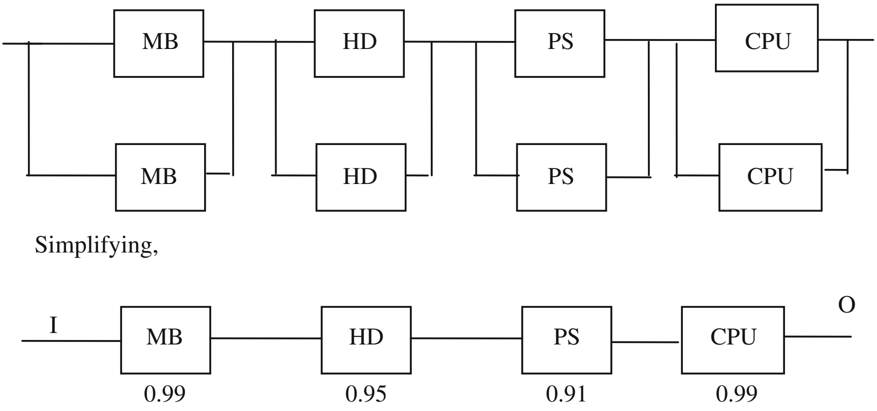
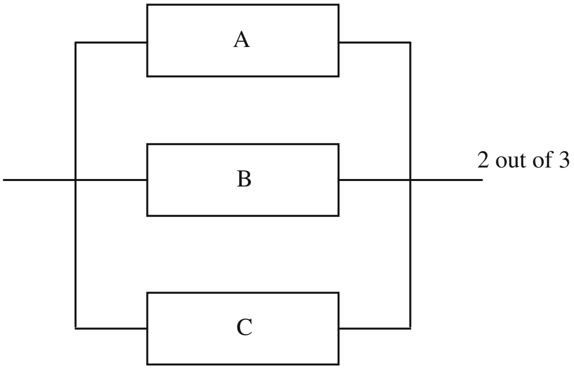


Fig. 3.9 Designer B RBD

Fig. 3.10 2 out of 3 model



M out of N Models (Identical Items)

System having three subsystems A, B and C fails only when more than one item has failed, as shown in Fig. 3.10.

$$\begin{aligned}
R_{Sys} &= 1 - Q_A \cdot Q_B - Q_A \cdot Q_C - Q_B \cdot Q_C + 2Q_A \cdot Q_B \cdot Q_C \\
&= 1 - (1 - R_A) \cdot (1 - R_B) - (1 - R_A) \cdot (1 - R_C) - (1 - R_B) \cdot (1 - R_C) + 2(1 - R_A) \\
&\quad \cdot (1 - R_B) \cdot (1 - R_C) \\
&= 1 - 1 + R_A + R_B - R_A \cdot R_B - 1 + R_A + R_C - R_A \cdot R_C - 1 + R_B + R_C - R_B \cdot R_C \\
&\quad + 2 - 2R_A - 2R_B - 2R_C + 2R_A \cdot R_B + 2R_A \cdot R_C + 2R_B \cdot R_C - 2R_A \cdot R_B \cdot R_C \\
&= R_A \cdot R_B + R_A \cdot R_C + R_B \cdot R_C - 2R_A \cdot R_B \cdot R_C
\end{aligned}$$

In general, if the reliability of a system can be represented by n identical items in parallel where m out of n are required for system success, then the system reliability Rs is given by

$$R_s = \sum_{r=0}^{n-m} ({}^nC_r)R^{n-r}(1-R)^r \tag{3.8}$$

Thus the reliability of the system illustrated by Fig. 3.10 is given by:

$$R_s = R^3 + 3R^2(1-R) = 3R^2 - 2R^3 \tag{3.9}$$

where R is the reliability of the individual items.

Example 4 Control and Instrumentation system is very important in the NPP as it monitors critical process parameters. Failure criteria is two ways

(i) Failure of the C & I equipment when there is actual variation in parameters.
(ii) Failure due to spurious signals.

Compare 1 out of 2: success and 2 out of 3: success designs under both criteria. Assume failure probability (q) for each subsystem.

Solution: 1 out of 2

In scenario (i) where there is actual variation in the process parameters, successful operations of 1 subsystem out of 2 subsystems lead to system success.

The Reliability is given by,

$$\begin{aligned}
R_1^1 &= \sum_{r=0}^{1} {}^2C_r(1-q)^{2-r}q^r \\
R_1^1 &= {}^2C_0(1-q)^{2-0}q^0 + {}^2C_1(1-q)^1q^1 \\
R_1^1 &= (1-q)^2 + 2(1-q)q \\
R_1^1 &= 1 + q^2 - 2q + 2q - 2q^2 \\
R_1^1 &= (1-q^2)
\end{aligned}$$

In scenario (ii), where there is spurious signal, any subsystem failure will lead to system failure for two unit system making it 2 out of 2: successes system or simple series system.

The reliability is given by,

$$\begin{aligned}
R_1^2 &= (1-q)(1-q) \\
R_1^2 &= (1-q)^2
\end{aligned}$$

2 out of 3

In both the scenarios, 2 out of 3 system will have same reliability, Given by

$$
\begin{aligned}
R_2 &= \sum_{r=0}^{1} {}^3C_r(1-q)^{3-r}q^r \\
R_2 &= {}^3C_0(1-q)^3q^0 + {}^3C_1(1-q)^2q^1 \\
R_2 &= (1-q)^3 + 3(1-q)^2q \\
R_2 &= (1-q)^2[1-q+3q] \\
R_2 &= (1-q)^2[1+2q] \\
R_2 &= (1-q^2-2q)(1+2q) \\
R_2 &= 1+2q+q^2+2q^3-2q-4q^2 \\
R_2 &= (1-3q^2+2q^3)
\end{aligned}
$$

for very less q values (high reliability systems) for failure criterion (i)

$$
\begin{aligned}
&(1-q^2) > (1-3q^2+2q^3) \\
&R_1^1 > R_2
\end{aligned}
$$

And in case of failure criteria (ii)

$$R_1^2 \ll R_2$$

Thus the reliability differences is marginal in non spurious case and is significantly different for spurious signal.

Hence 2 out of 3 is better than 1 out of 2 system.

Standby Redundancy Models

Another frequently used form of redundancy is what is known as standby redundancy. In its most elementary form, the physical arrangement of items is represented in Fig. 3.11

In Fig. 3.11, item A is the on-line active item, and item B is standing by waiting to be switched on to replace A when the latter fails. The RBD formulae already established are not applicable for the reliability analysis of standby redundant systems.

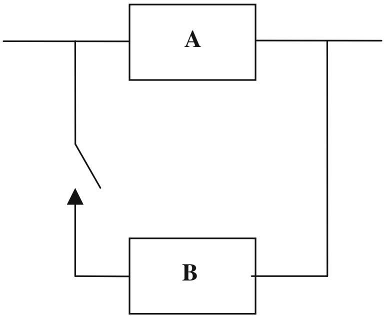
The expression for system reliability is:

$$R_s(t) = e^{-\lambda t}(1+\lambda t)$$

With the following assumptions

(a) when operating, both items have a constant failure rate λ and have zero failure rate in standby mode;
(b) the switch is perfect;
(c) switching-over time is negligible; and
(d) stand by unit does not fail while in standby mode.

Fig. 3.11 Standby model



If there are n items in standby, this expression becomes:

$$R_s(t) = e^{-\lambda t}[1 + \lambda t + \frac{(\lambda t)^2}{2!}! + \frac{(\lambda t)^3}{3!} + \cdots + \frac{(\lambda t)^n}{n!}] \tag{3.10}$$

It is to be noted that a practical block diagram should include blocks to represent the reliability of the switch plus sensing mechanism, which is often the ‘weak link’ in standby systems. Further, unlike this example, the probability of survival of one item (item B) is dependent upon the time when the other item (item A) fails. In other words items A and B can not be regarded as failing independently. As a consequence, other procedures, such as Markov analysis, should be used to analyze standby system.

Example 5 A typical UPS (Uninterrupted Power Supply) circuit is shown in Fig. 3.12. Given the unavailability of components (as shown in Table 3.1), calculate the UPS unavailability?.

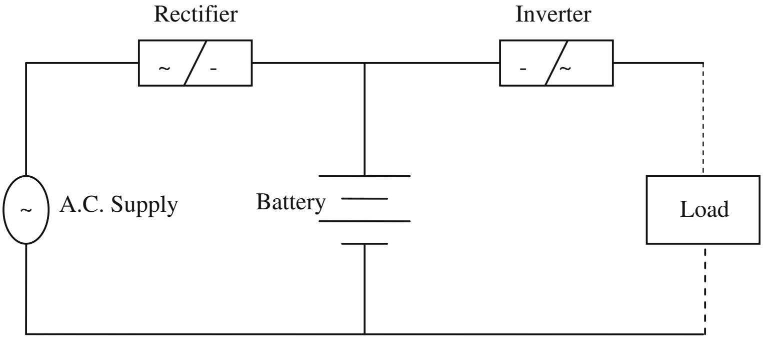


Fig. 3.12 UPS

Table 3.1 Component failure and repair rates

Component	λ (failure rate)	μ (repair rate)
A.C. supply	2.28×10^{-4}	2
Rectifier	1×10^{-4}	0.25
Battery	1×10^{-6}	0.125
Inverter	1×10^{-4}	0.25

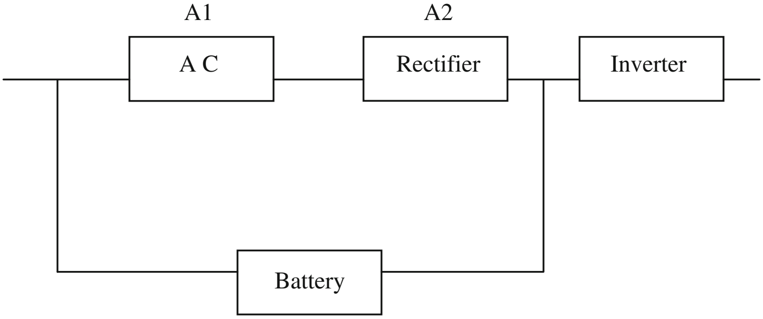


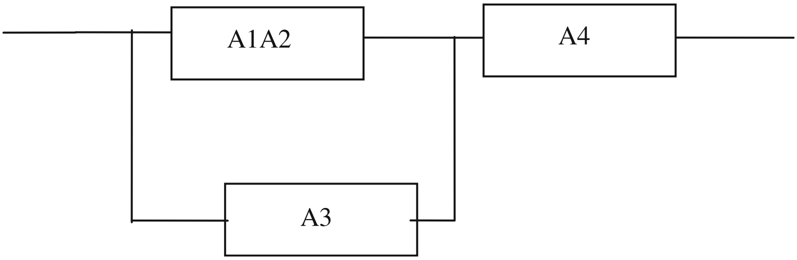
Fig. 3.13 RBD of UPS

Solution: In the normal conditions when AC power supply is present, load draws current from AC supply. When AC supply is not there, load draws current from battery. However, inverter is required in both the scenarios. The RBD for the UPS can be represented as shown in Fig. 3.13.

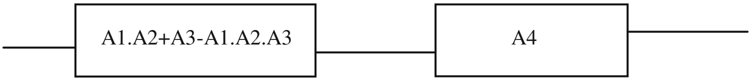
The RBD can be successively simplified as follows:

As A1 and A2 are in series, they can be replaced by their equivalent availability,

A=A1.A2.



Now there is simple parallel structure, represented it with its equivalent expression, A1.A2+A3-A1.A2.A3.



The final availability expression is given as,

A4[A1.A2+A3-A1.A2.A3]

Availability is calculated with the parameters given in the table:

$$A = \frac{\mu}{\mu - \lambda}$$
$$\mathrm{A1} = 0.9999$$
$$\mathrm{A2} = 2.28 \times 10^{-4}$$
$$\mathrm{A3} = 0.9999$$
$$\mathrm{A4} = 0.9996$$

Substitute the values in

$$\mathrm{A_{ups}} = \mathrm{A4}[\mathrm{A1} \cdot \mathrm{A2} + \mathrm{A3} - \mathrm{A1} \cdot \mathrm{A2} \cdot \mathrm{A3}]$$
$$\mathrm{A_{ups}} = 0.9998$$

3.1.3 Solving RBD

Apart from the standard models discussed in the previous section, there can be non-series parallel or complex configurations. There are general solution approaches to solve such RBD such as truth table method, path set/cut set method and bounds method.

3.1.3.1 Truth Table Method

This method is also known as event enumeration method. In this approach, all the combinations of events are enumerated and system state for the given combination is identified. For example, if there are n components in the system considering success and failure for every component, there would be 2^n combinations. All such combinations will be explored for system success. This method is computationally intensive. It is illustrated with simple example here.

Example 6 One portion of a fluid system physically consists of a pump and two check valves in series. The series check valves provides redundancy against flow in the reverse direction when the pump is not operating and the down stream pressure exceeds the upstream pressure.

Solution: The system diagram is as in Fig. 3.14

And the functional diagram is as in Fig. 3.15.

Considering the functional diagram the Boolean expression for this system is given by

$$S = C \cdot (A + B)$$

Or one can make a truth table (Table 3.2) by assigning a ‘0’ and ‘1’ value to failure and success respectively.

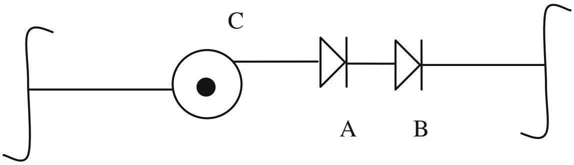


Fig. 3.14 A simple fluid system

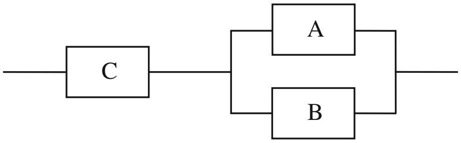


Fig. 3.15 RBD of fluid system

Table 3.2 Truth table

S. no.	A	B	C	S	P(Event probability)
1	0	0	0	0	–
2	0	0	1	0	–
3	0	1	0	0	–
4	0	1	1	1	$(1 - P_A) \cdot P_B \cdot P_C$
5	1	0	0	0	–
6	1	0	1	1	$P_A(1 - P_B) \cdot P_C$
7	1	1	0	0	–
8	1	1	1	1	$P_A P_B \cdot P_C$

Pump Not Working = 1
Pump working = 0
Check valve reverse blocking = 1
Check valve not reverse blocking = 0
System success pump not working and valve reverse blocking = 1
System failure pump working = 0

From this truth table add all the entries under P corresponding to 1 under S. The reliability is obtained as

$$R = (1 - P_A)P_B P_C + P_A(1 - P_B)P_C + P_A P_B P_C$$
$$R = P_C(P_A + P_B - P_A P_B)$$

If it is possible to write Boolean expression of the system it is not necessary to make the truth table. What is required that the Boolean expression should be reduced to its minimal form and then one directly do the probability operation on it.

3.1.3.2 Cut-Set and Tie-Set Method

This is an efficient method to compute reliability of a given system. Computer programmes are also available.

Cut-Set It is the group of those elements or units, which will make the system to fail, if their failure occurs. The minimum number of such units forms the minimal cut set.

Tie-Set The set of those elements, whose working will make the system to work. A minimal tie set is the minimum number of such elements which would assure the system success.

For reliability computation either the minimal cut-set or the minimal tie-set should be found.

Suppose in the system T1, T2,…Tn are the minimal tie-sets then the system reliability is given by

$$P(T1 \cup T2 \cup T3 \ldots \cup Tn)$$

And if the minimal cut-sets are known to be C1, C2,…,Ck then the system reliability is

$$1 - P(C1 \cup C2 \cup C3 \ldots \cup Ck)$$

where PT1, PT2,…PTn denote the success probability attached with the tie-sets T1, T2…Tn and PC1, PC2…PCk are the failure probabilities attached with the cut sets C1, C2…Ck.

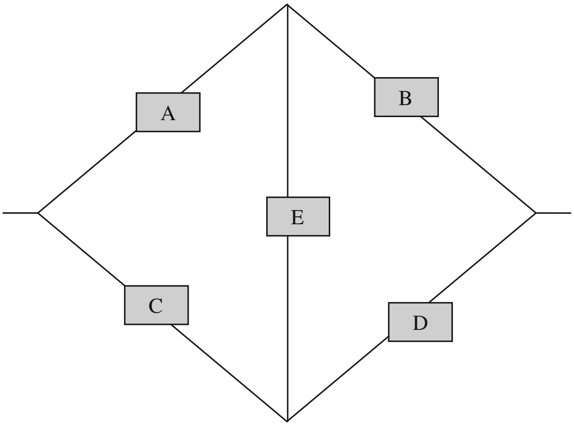


Fig. 3.16 Bridge network

Example 7 Considering a Bridge network shown in Fig. 3.16, calculate reliability of the system as a function of tie sets?

The minimal tie-sets are

$$T_1 = (A, B); T_2 = (C, D); T_3 = (A, E, D); T_4 = (C, E, B);$$

The minimal cut-sets are

$$C_1 = (A, C);\; C_2 = (B, D);\; C_3 = (A, E, D);\; C_4 = (C, E, B);$$

If success probabilities of tie sets are

$$P(T_1) = P_A \cdot P_B;\; P(T_2) = P_C \cdot P_D;\; P(T_3) = P_A P_E P_D;\; P(T_4) = P_C P_E P_B$$

Reliability

$$\begin{aligned}
R &= P(T_1 \cup T_2 \cup T_3 \cup T_4) \\
R &= P(T_1) + P(T_2) + P(T_3) + P(T_4) - [P(T_1)P(T_2) + P(T_2) + P(T_3) + P(T_3) + P(T_4) \\
&\quad + P(T_1) + P(T_4) + P(T_1) + P(T_3) + P(T_2) + P(T_4)] + [P(T_1)P(T_2)P(T_3) + P(T_2)P(T_3)P(T_4) \\
&\quad + P(T_3)P(T_4)P(T_1) + P(T_1)P(T_2)P(T_4)] - P(T_1)P(T_2)P(T_3)P(T_4)
\end{aligned}$$

Similarly cut-set method can be used for Reliability prediction.

Example 8 A simplified emergency power supply system is shown in Fig. 3.17. Availability of power supply at any of the Bus(Bus A or Bus B) ensures the supply to loads. There is transfer switch to connect DG1 to Bus B or to connect DG2 to Bus A. Develop the RBD and identify the combinations of failures leading to failures of power supply.

Solution: The RBD can be represented as shown in Fig. 3.18.

The following combinations of failure lead to system failure.

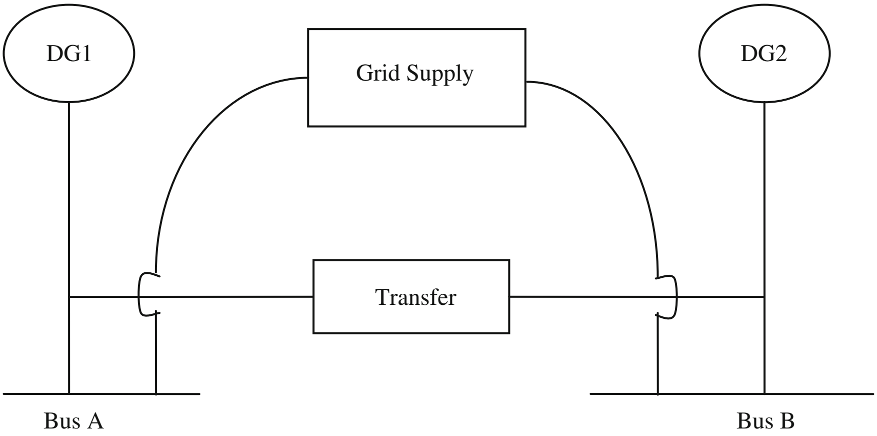


Fig. 3.17 Simplified emergency power supply system

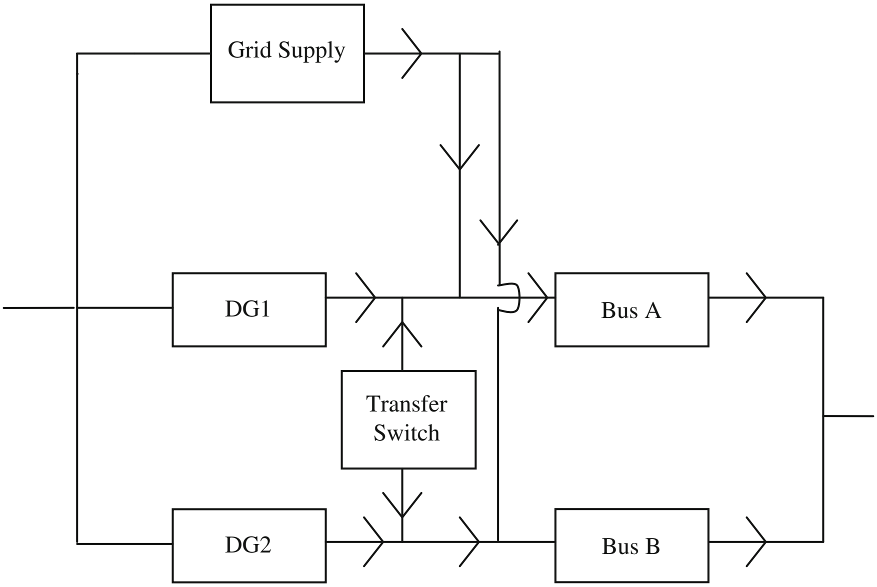


Fig. 3.18 RBD of simplified emergency power supply system

Bus A · Bus B
Grid · DG1 · DG2
Grid · DG1 · TS · Bus.B
Grid · DG2 · TS · Bus.A.

3.1.3.3 Bounds Method

When system is large Boolean Techniques and cut-set, tie set method become tedious. But if we use computer programme with cut-sets and tie-sets then one can adopt Bounds method which is a variation of cut-set and tie-set method.

If T1, T2...Tn are minimal tie-sets then the upper bound for system reliability is

$$\mathrm{R_u} < \mathrm{P(T_1)} + \mathrm{P(T_2)} + \cdots + \mathrm{P(T_n)}$$

This becomes good approximation in low reliability region.

If C1, C2...Ck are minimal cut-sets the lower bound of system reliability can be found as

$$\mathrm{R_l} > 1 - [\mathrm{P(C_1)} + \mathrm{P(C_2)} + \cdots + \mathrm{P(C_n)}]$$

This becomes good approximation in high reliability region.

Reliability of the system approximately will be

$$R = 1 - \sqrt{(1 - R_u)(1 - R_l)} \tag{3.11}$$

3.2 Markov Models

Markov models provide improved modeling of systems where one or more conditions such as strong dependencies between components, repairable components, coverage factors (failures detected or not detected), multiple states, etc. are present. On the flip side, the size of the Markov model explodes for large systems, hence it is practical to combine this technique with fault tree analysis [2]. This section briefly covers Markov technique along with a few examples.

3.2.1 Elements of Markov Models

Markov process originated from the theory of stochastic processes. The basic assumption of Markov process is that the behavior of a system in each state is memory-less, the future depends on the present but independent of the past. Another important assumption is constant transition rate (exponential distribution) between the system states.

A flow chart that shows steps involved in Markov modeling is presented in Fig. 3.19. System state is a function of states of components that constitute the system. Components states are usually discrete such as success or failure states. In first step, all possible system states are identified as a function of components' states, and the resulting system state is labeled as a success or a failure. The possible

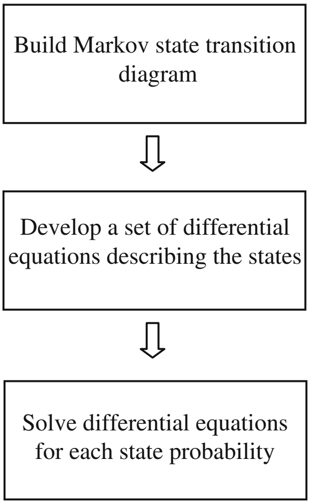

Build Markov state transition diagram
Develop a set of differential equations describing the states
Solve differential equations for each state probability

Fig. 3.19 Steps in Markov modeling

transitions between the different states are shown, identifying the causes of all transitions. In general, the causes of the transitions are either failure of one or several subsystem components or a repair made to a component. This representation is done by constructing a state transition diagram wherein each node (shown as a circle) represents a state of the system; and each arc symbolizes a transition between the two nodes it links. A transition rate between two states is assigned to each arc. In second step, a set of first-order differential equations are developed by describing the probability of being in each state in terms of the transitional probabilities from and to each state. Finally, the probabilities of being in the different states during a certain period in the life of the system or the reliability characteristics (mean time to failure, mean time between failure, mean time to repair) are calculated by solving the system of differential equations.

A simple one component system (repairable system Fig. 3.20) is taken for illustrative purposes and a detailed Markov analysis for the reliability evaluation is presented. In state 1, the system functions (Up state) as the component is available. The failure of the component leads to system state 2, which is labeled as down state.

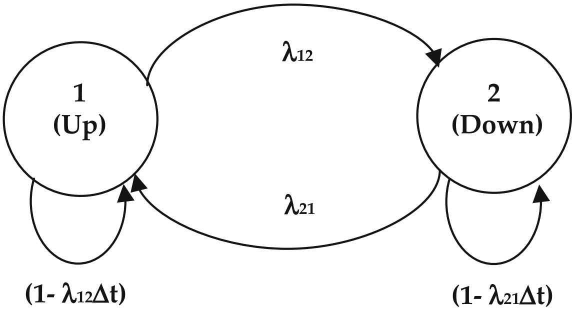


Fig. 3.20 Markov model for a repairable system having one component

The failure rate of component is transition rate (λ_{12}) from state 1 to state 2. Repair of components restores the system taking it back to state 1 from state 2, so the repair rate of the component is the transition rate (λ_{21}). Let $P_1(t)$ be the probability of the system being in state 1 at time t and $P_2(t)$ be the probability of the system being in state 2 at time t. $P_1(t + \Delta t)$ is the probability of the system being in state 1 at time $(t + \Delta t)$ which is expressed as the sum of two event probabilities; first event considers the system is in state 2 at time t and then transfers to state 1 and second event considers the system in state 1 at time t and then continue to stay in the same state. As λ_{21} is the transition rate from state 2 to state 1, $\lambda_{21} \times \Delta t$ is the probability of transition in the interval Δt. Similarly, $(1 - \lambda_{12} \times \Delta t)$ is the probability of continuing in state 1 in the interval Δt.

$P_1(t + \Delta t)$ is the sum of probability of transfer to state 1 given system is in state 2 at time t and probability of non-transfer given system is in state 1 at time t, which is expressed in Eq. 3.12.

$$P_1(t+\Delta t) = \lambda_{21}\Delta t P_2(t) + (1-\lambda_{12}\Delta t)P_1(t) \tag{3.12}$$

Similarly, $P_2(t + \Delta t)$ can be derived as expressed in Eq. 3.13.

$$P_2(t+\Delta t) = \lambda_{21}\Delta t P_1(t) + (1-\lambda_{12}\Delta t)P_2(t) \tag{3.13}$$

The above equations can be rearranged as follows:

$$\Rightarrow \frac{P_1(t+\Delta t) - P_1(t)}{\Delta t} = \lambda_{21}P_2(t) - \lambda_{12}P_1(t)$$

and

$$\frac{P_2(t+\Delta t) - P_2(t)}{\Delta t} = \lambda_{12}P_1(t) - \lambda_{21}P_2(t)$$

As $\Delta t \to 0$,

$$\frac{dP_1(t)}{dt} = \lambda_{21}P_2(t) - \lambda_{12}P_1(t), \text{ and } \frac{dP_2(t)}{dt} = \lambda_{12}P_1(t) - \lambda_{21}P_2(t)$$

Let us say $\lambda_{12} = \lambda$; $\lambda_{21} = \mu$ and substituting in the above equations,

$$\Rightarrow \frac{dP_1}{dt} = \mu P_2(t) - \lambda P_1(t) \tag{3.14}$$

$$\frac{dP_2}{dt} = \lambda P_1(t) - \mu P_2(t) \tag{3.15}$$

Expressing the above equations in matrix form:

$$\begin{bmatrix} \frac{dP_1(t)}{dt} & \frac{dP_2(t)}{dt} \end{bmatrix} = [\,P_1(t) \quad P_2(t)\,] \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix}$$
$$\text{i.e } \left[\overline{P'(t)}\right] = \left[\overline{P(t)}\right][A]$$

where [A] is known as “Stochastic Transition Matrix”.

When the initial distribution, $P_i(0)$ is known, i.e. $P_1(0)$ and $P_2(0)$ are known, true solutions to the Markov differential equations as shown in Eqs. (3.14) and (3.15) can be found, in particular, using Laplace Transforms, Discretization, or the Eigen values of matrix A. For all computational purposes, it can be assumed that the system is initially in the UP state, i.e. all components are working. In the example considered, this renders $P_1(0)$ probability of system being in state 1 at time t = 0 as 1 and $P_2(0)$ as 0.

For the convenience of the reader, the solution of first order differential equations is explained below in detail. This approach needs basics of Laplace transforms and partial fractions.

Refresher of Laplace Transforms

$$L(1) = \frac{1}{S}$$

$$L(t^n) = \frac{\angle n}{S^{n+1}}$$

$$L(e^{at}) = \frac{1}{S-a}$$

Transform of derivatives
If $L(f(t)) = F(s)$, then $L(f'(t)) = SF(S) - f(0)$
Transform of integrals
If $L(f(t)) = F(s)$, then $L(\int_0^t f(t)) = \frac{F(S)}{S}$

Taking Laplace Transforms of Eqs. (3.14) and (3.15):

$$\begin{aligned} SP_1(S) - P_1(0) &= -\lambda P_1(S) + \mu P_2(S) \\ \text{i.e.} SP_1(S) - 1 &= -\lambda P_1(S) + \mu P_2(S) \end{aligned} \tag{3.16}$$

and

$$\begin{aligned} SP_2(S) - P_2(0) &= \lambda P_1(S) - \mu P_2(S) \\ \text{i.e.} SP_2(S) - 0 &= \lambda P_1(S) - \mu P_2(S) \end{aligned} \tag{3.17}$$

Rearranging Eq. (3.17)

$$\Rightarrow SP_2(S) = \lambda P_1(S) - \mu P_2(S)$$

$$\Rightarrow P_2(S)[S+\mu] = \lambda P_1(S)$$

$$\Rightarrow P_2(S) = \frac{\lambda}{S+\mu} P_1(S) \tag{3.18}$$

Substitute Eq. (3.18) in Eq. (3.16)

$$\begin{gathered} SP_1(S) - 1 = -\lambda P_1(S) + \frac{\mu\lambda}{S+\mu} P_1(S) \Rightarrow P_1(S)\left[S + \lambda - \frac{\mu\lambda}{S+\mu}\right] = 1 \\ P1(S) = \frac{1}{S+\lambda - \left[\frac{\mu\lambda}{S+\mu}\right]} \Rightarrow P_1(S) = \frac{S+\mu}{S[S+(\mu+\lambda)]} \end{gathered} \tag{3.19}$$

RHS is resolved into partial fractions:

$$\frac{S+\mu}{S[S+(\mu+\lambda)]} = \frac{A}{S} + \frac{B}{S+(\mu+\lambda)}$$

$$\Rightarrow S+\mu = A[S+(\mu+\lambda)] + BS$$

Comparing the like coefficients on both the sides:

$$\mathrm{A} + \mathrm{B} = 1;\ A(\mu+\lambda) = \mu \Rightarrow A = \frac{\mu}{(\mu+\lambda)}$$

and

$$B = 1 - \frac{\mu}{(\mu+\lambda)}$$

Using partial fractions, Eq. 3.19 can be expressed as

$$\therefore P_1(S) = \frac{\mu}{\mu+\lambda}\left[\frac{1}{S}\right] + \frac{\lambda}{\mu+\lambda}\left[\frac{1}{S+(\mu+\lambda)}\right] \tag{3.20}$$

Inverse Laplace Transformation on Eq. (3.20) yields:

$$P_1(t) = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda} e^{-(\mu+\lambda)t} \tag{3.21}$$

Substituting Eq. (3.19) in Eq. (3.18) to get a simplified $P_2(S)$,

$$P_2(S) = \frac{\lambda}{S[S + (\mu + \lambda)]}$$

RHS is solved into partial Fractions as:

$$\frac{\lambda}{\mu + \lambda}\left[\frac{1}{S}\right] - \frac{\lambda}{\mu + \lambda}\left[\frac{1}{S + (\mu + \lambda)}\right]$$

Inverse Laplace Transformation Yields:

$$P_2(t) = \frac{\lambda}{\mu + \lambda} + \frac{\lambda}{\mu + \lambda} e^{-(\mu+\lambda)t} \tag{3.22}$$

Equations (3.21) and (3.22) give time dependent probabilities of system states 1 and 2 respectively.

Steady state probabilities can be obtained by substituting in these equations the value of t as time t tends to infinity:

Thus,

$$\mathrm{P}_1(\infty) = \frac{\mu}{\mu + \lambda} \tag{3.19}$$

$$\mathrm{P}_2(\infty) = \frac{\lambda}{\mu + \lambda} \tag{3.20}$$

These steady state probabilities can also be obtained directly without the solution of the system of Markov differential equations.

As Probabilities tend to be constant w.r.t time as time tends to infinity, the vector of differential probabilities becomes a Null Vector.

$$[\overline{\mathrm{P}'(\mathrm{t})}] = [0]$$

In general:

$$[\overline{\mathrm{P}'(\mathrm{t})}] = [\overline{\mathrm{P}(\mathrm{t})}][A]$$

For steady state probabilities:

$$[0] = [\overline{\mathrm{P}(\mathrm{t})}][A]$$

For the single component with repair considered, the steady state equations could be written down as follows:

$$0 = -\lambda P_1(\infty) + \mu P_2(\infty)$$
$$\text{and } 0 = \lambda P_1(\infty) - \mu P_2(\infty)$$

Also, the summation of probabilities of all states amounts to 1. Thus,

$$P_1(\infty) + P_2(\infty) = 1$$

For an ‘n’ state Markov model, any (n − 1) steady state Markov linear equations along with the equation of summation of state probabilities are solved simultaneously.

$$P_1(\infty) = \frac{\mu}{\mu + \lambda}$$

$$P_2(\infty) = \frac{\lambda}{\mu + \lambda}$$

Two Component System with Repair

A system consists of two components ‘A’ and ‘B’. State 0 is the UP state where both the components are working. When component ‘A’ fails, transition to state 1 takes place. If repaired in this state, it goes back to state 0. Failure of component ‘B’ in state 1 leads the system to state 3, where both the components are down. The transitions from states 0–2–3 can be explained on similar lines. The Markov model is as shown below. λ_1 and λ_2 are failure rates while μ_1 and μ_2 are repair rates of A and B respectively.

Figure 3.21 shows state transition diagram for two component system. Following the process explained earlier, the differential equations for describing states can be derived as follows:

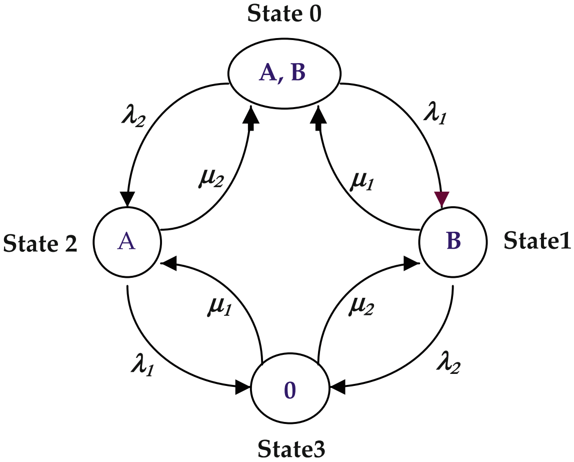


Fig. 3.21 Markov model for two component system

$$\frac{dP_0}{dt} = -(\lambda_1 + \lambda_2)P_0(t) + \mu_1 P_1(t) + \mu_2 P_2(t) \tag{3.21}$$

$$\frac{dP_1}{dt} = -(\mu_1 + \lambda_2)P_1(t) + \lambda_1 P_0(t) + \mu_2 P_3(t) \tag{3.22}$$

$$\frac{dP_2}{dt} = -(\lambda_1 + \mu_2)P_2(t) + \lambda_2 P_0(t) + \mu_1 P_3(t) \tag{3.23}$$

$$\frac{dP_3}{dt} = -(\mu_1 + \mu_2)P_3(t) + \lambda_2 P_1(t) + \lambda_1 P_2(t) \tag{3.24}$$

While writing Markov differential equation for a state 'i' the thumb rule is negative of sum of transition rates going away from the state 'i' multiplied by its probability at time t and other positive terms are sum of product of transition rates coming into the state 'i' and the state probability that come into state 'i'. This rule can be used to write down the system of differential equations quickly.

Solving the Eqs. (3.21–3.24) as explained with Laplace transforms before, steady state probabilities are given by the following expressions:

$$P_0 = \frac{\mu_1 \mu_2}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)}$$

$$P_1 = \frac{\lambda_1 \mu_2}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)}$$

$$P_2 = \frac{\lambda_2 \mu_1}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)}$$

$$P_3 = \frac{\lambda_1 \lambda_2}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)}$$

Having known the probability of each system states, reliability is sum of probabilities of the states where system is successful. In case the two components are in series in a system, the reliability of the system is the probability of that state where both the components are in up state. i.e. State 0. For a parallel system, reliability is given by the summation of probabilities of all those states which have at least one working component, sum of probabilities of states 0, 1, and 2.

Example 9 Three safety injection pumps (A, B, and C) are installed in a plant. Assuming repair is not possible in emergency injection conditions and different failure rates for each pump, construct a Markov model and develop governing differential equations?

As the injection has 3 components, 2^3 are possible states for system. Figure 3.22 shows the state transition diagram for the injection system with transition rates among the states. The differential equations for each state are written based on the thumb rule mentioned earlier:

$$\frac{dP_1}{dt} = -(\lambda_A + \lambda_B + \lambda_C)P_1(t)$$

$$\frac{dP_2}{dt} = -(\lambda_B + \lambda_C)P_2(t) + \lambda_A P_1(t)$$

$$\frac{dP_3}{dt} = -(\lambda_A + \lambda_C)P_3(t) + \lambda_B P_1(t)$$

$$\frac{dP_4}{dt} = -(\lambda_A + \lambda_B)P_4(t) + \lambda_C P_1(t)$$

$$\frac{dP_5}{dt} = -(\lambda_C)P_5(t) + (\lambda_B)P_2(t) + (\lambda_A)P_3(t)$$

$$\frac{dP_6}{dt} = -(\lambda_A)P_6(t) + (\lambda_C)P_3(t) + (\lambda_B)P_4(t)$$

$$\frac{dP_7}{dt} = -(\lambda_B)P_7(t) + (\lambda_C)P_2(t) + (\lambda_A)P_4(t)$$

$$\frac{dP_8}{dt} = (\lambda_C)P_5(t) + (\lambda_A)P_6(t) + (\lambda_B)P_7(t)$$

The differential equations mentioned above can be solved to obtain probabilities of each state.

If two identical states, say x and y are to be merged together, the following relationships are to be employed to obtain the equivalent transition rates between the merged state and other states (say state i) of the state space.

$$\begin{aligned} P_z &= P_x + P_y \\ \lambda_{iz} &= \lambda_{ix} + \lambda_{iy} \\ \lambda_{zi} &= \frac{\lambda_{xi} \cdot P_x + \lambda_{yi} \cdot P_y}{P_x + P_y} \end{aligned}$$

The transitions between two merged states can be obtained from the following relations:

$$\begin{aligned} \lambda_{IJ} &= \frac{\sum_{i \in I} P_i \sum_{j \in J} \lambda_{ij}}{\sum_{i \in I} P_i} \\ \lambda_{JI} &= \frac{\sum_{j \in J} P_j \sum_{i \in I} \lambda_{ji}}{\sum_{j \in J} P_j} \end{aligned} \tag{3.25}$$

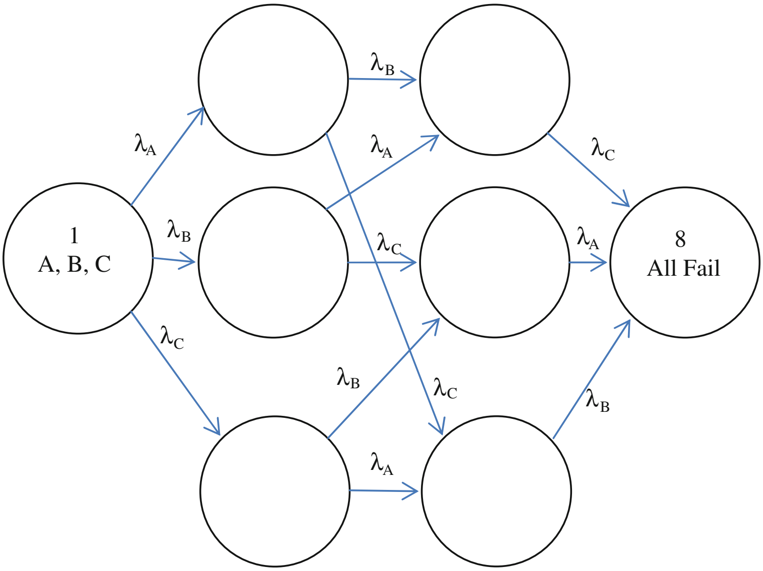


Fig. 3.22 Markov model for 3 pump injection system

This could be illustrated by considering the problem illustrated in Example 10 (Fig. 3.22).

In Markov model of 3 pump system as shown in Fig. 3.22, system states 2, 3, and 4 are identical because only one pump is down while other two are up. Similarly, states 5, 6, and 7 are identical as one pump is up while other two pumps are down. Using the concept of merging as expressed in Eq. 3.25, we can alter the definitions of states accordingly and arrive at a simplified Markov model. The states could now be interpreted as:

Step 1: Three pumps are up
Step 2′: Only one pump is down
Step 3′: Only one pump is up
Step 8: All pumps are down

Using Eq. 3.25 for merging states 2, 3, and 4 to yield state 2′:

$$\lambda_{12\prime} = \lambda_A + \lambda_B + \lambda_c$$

$$\lambda_{2'3\prime} = \frac{P2(\lambda_B + \lambda_c) + P3(\lambda_A + \lambda_c) + P4(\lambda_B + \lambda_c)}{P2 + P3 + P4}$$

$$\lambda_{3'4'} = \frac{P5(\lambda_A) + P6(\lambda_B) + P7(\lambda_c)}{P5 + P6 + P7}$$

If all failure rates are identical, then:

$$\lambda_{12'} = 3\lambda$$

$$\lambda_{2'3'} = 2\lambda$$

$$\lambda_{3'4'} = \lambda$$

Example 10 Considering Markov model shown in Fig. 3.23, Determine the reliability for the following success criterion (a) Two pumps necessary for success of the injection (b) one pump meets injection requirements?

2′, 3′, and 4′ are denoted as 2, 3, and 4 in this example for convenience. The reliability for success criteria (a) is sum of probabilities of system states 1 and 2. The reliability for success criteria (b) is sum of all state probabilities except 4. The differential equations for each system state can be written based on the approach discussed earlier,

$$\frac{dP_1}{dt} = -3\lambda P_1(t) \tag{3.26}$$

$$\frac{dP_2}{dt} = -2\lambda P_2(t) + 3\lambda P_1(t) \tag{3.27}$$

$$\frac{dP_3}{dt} = -\lambda P_3(t) + 2\lambda P_2(t) \tag{3.28}$$

$$\frac{dP_4}{dt} = \lambda P_3(t) \tag{3.29}$$

Applying Laplace transforms and rearranging the equations, we have

$$\begin{aligned} P_1(s) &= \frac{1}{(s+3\lambda)} \\ P_2(s) &= \frac{3\lambda}{(s+2\lambda)(s+3\lambda)} \\ P_3(s) &= \frac{6\lambda^2}{(s+\lambda)(s+2\lambda)(s+3\lambda)} \\ P_4(s) &= \frac{6\lambda^3}{s(s+\lambda)(s+2\lambda)(s+3\lambda)} \end{aligned} \tag{3.30}$$

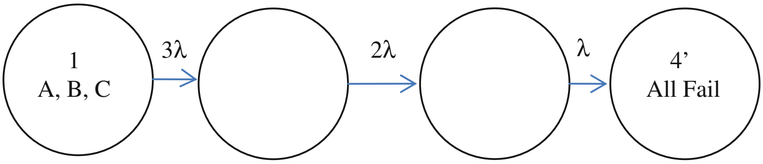


Fig. 3.23 Markov model with identical failure rates

Before applying inverse Laplace transforms, partial fraction expansion to split up a complicated fraction into standard forms are used. A quick method is 'cover-up' method as shown below on $P_2(s)$:

$$\begin{aligned} P_2(s) &= \frac{3\lambda}{(s+2\lambda)(s+3\lambda)} = \frac{A}{(s+2\lambda)} + \frac{B}{(s+3\lambda)} \\ A &= \left.\frac{3\lambda}{(s+2\lambda)(s+3\lambda)}\right|_{s=-2\lambda} = 3 \\ B &= \left.\frac{3\lambda}{(s+2\lambda)(s+3\lambda)}\right|_{s=-3\lambda} = -3 \end{aligned} \tag{3.31}$$

Similarly, applying partial fraction cover up method on $P_3(s)$ and $P_4(s)$:

$$P_3(s) = \frac{3}{(s+\lambda)} - \frac{6}{(s+2\lambda)} + \frac{3}{(s+3\lambda)} \tag{3.32}$$

$$P_4(s) = \frac{1}{s} - \frac{3}{(s+\lambda)} + \frac{3}{(s+2\lambda)} - \frac{1}{(s+3\lambda)} \tag{3.33}$$

Applying inverse Laplace transforms on Eqs. (3.30–3.33) to obtain probability of state as a function of time:

$$\begin{aligned} P_1(t) &= e^{-3\lambda t} \\ P_2(t) &= 3e^{-2\lambda t} - 3e^{-3\lambda t} \\ P_3(t) &= 3e^{-\lambda t} - 6e^{-2\lambda t} + 3e^{-3\lambda t} \\ P_4(t) &= 1 - 3e^{-\lambda t} + 3e^{-2\lambda t} - e^{-3\lambda t} \end{aligned}$$

Reliability of the system as a function of time can be obtained for both success criterion,

Case (a): $R(t) = P_1(t) + P_2(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t}$
Case (b): $R(t) = P_1(t) + P_2(t) + P_3(t) = 3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}$

Markov models are particularly useful in solving fault tolerant systems which would be very difficult to model with classical techniques [3]. Later in the book, application of Markov models in dynamic fault trees [4] and pipe reliability problems [5] are presented.

3.3 Fault Tree Analysis

Fault tree analysis is a failure oriented, deductive and top-down approach, which considers an undesirable event associated with the system as the top event, the various possible combinations of fault events leading to the top event are represented with logic gates.

Fault tree is a qualitative model which provides useful information on the various causes of undesired top events. However, quantification of fault tree provides top event occurrence probability and critical contribution of the basic causes and events. Fault tree approach is widely used in probability safety assessment.

The faults can be events that are associated with component hardware failure, software error, human errors, or any other relevant events which can lead to top events. The gates show the relationships of faults (or events) needed for the occurrence of a higher event. The gates those serve to permit or inhibit the fault logic up the tree. The gate symbol denotes the type of relationship of the input (lower) events required for the output (higher) event.

3.3.1 Procedure for Carrying Out Fault Tree Analysis

The procedure for carrying out fault tree analysis is shown as a flow chart in Fig. 3.24 [6, 7].

(a) *System Awareness and Details*

Thorough understanding of the system is the prerequisite for doing FTA. System awareness through discussion with designers, operating and maintenance engineers is very important, plant or system visits will also enhance it further. Input information such as the following mentioned should be collected and studied:

(i) Design basis reports.
(ii) Safety analysis reports (deterministic).
(iii) Technical specification report (for test and maintenance information).
(iv) History cards, maintenance cards and safety related unusual occurrence reports for obtaining failure or repair data

(b) *Defining Objectives, Top Event and Scope of Fault Tree Analysis*

Objectives are defined in consultation with decision makers or managers who commissioned fault tree analysis (FTA). Though general objective may be evaluation of current design or comparisons of alternative designs, particular objectives should be explicitly defined in terms of system failure.

The Top event of fault tree is the event which is analyzed to find all credible ways in which it could be brought about. The failure probability is determined for the defined top event. The top event of FT is defined based on the objectives of the analysis.

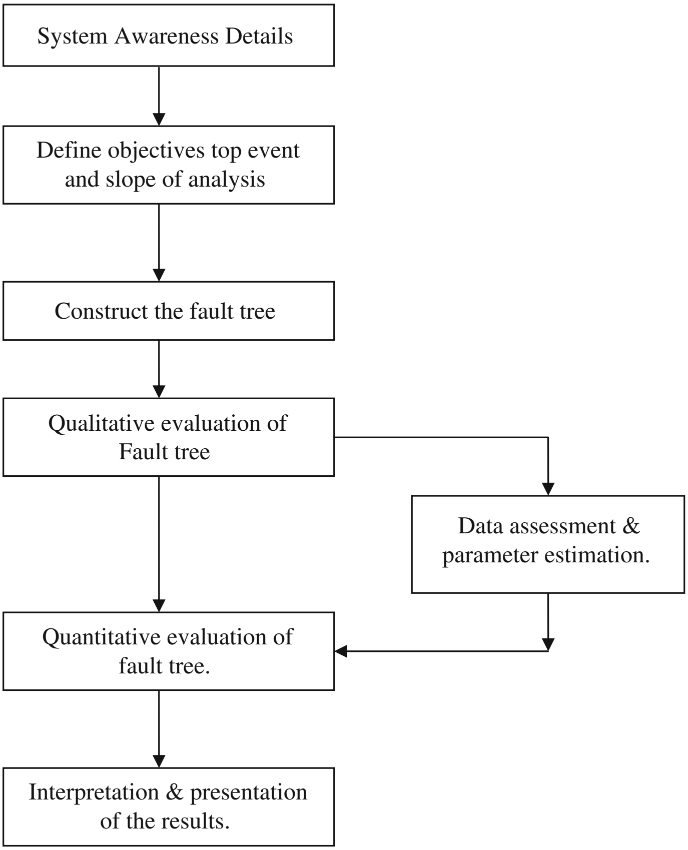

System Awareness Details
Define objectives top event and slope of analysis
Construct the fault tree
Qualitative evaluation of Fault tree
Data assessment & parameter estimation.
Quantitative evaluation of fault tree.
Interpretation & presentation of the results.

Fig. 3.24 Procedure for carrying out fault tree analysis

There can be more than one top event required for successfully meeting objectives. In such cases separate top events are then defined.

Lack of proper understanding of objectives may lead incorrect definition of top event, which will result in wrong decisions being made. Hence it is extremely important to define and understand the objectives of the analysis. After identifying top event from the objectives, scope of the analysis is defined. The scope of the FTA specifies which of the failures and contributors to be included in the analysis. It mainly includes the boundary conditions for the analysis. The boundary conditions comprise the initial states of the sub systems and the assumed inputs to the system. Interfaces to the system such as power source or water supplies are typically included in the analysis their states need to be identified and mentioned in the assumptions.

(c) *Construction of the Fault Tree*

The basic principle in constructing a fault tree is “consider short sightedly”. The immediate events or causes are identified for the event that is analyzed. The analysis does not jump to the basic causes of the event. Instead, a small step is taken and the necessary and sufficient immediate events are identified. This talking of small steps backwards assures that all of the relationships and primary consequences will be revealed. This backward stepping ends with the basic consequence identified that constitutes the resolution of the analysis. Fault trees are developed to a level of detail where the best failure probability data are available. The terminology and basic building blocks of fault tree are explained in the next section.

(d) *Qualitative Evaluation of the Fault Tree*

The qualitative evaluations basically transform the fault tree into logically equivalence forms that provide more focused information. The qualitative evaluation provides information on the minimal cut sets of the top event. Minimal cut set is the smallest combination of basic events that result in the occurrence of top event. The basic events are the bottom events of the fault tree. Hence, the minimal cut set relates the top event is represented by the set of minimal cut set. Success sets may also be identified that guarantee prevention of the top event.

Methods of obtaining minimal cut set are explained in the subsequent sections.

(e) *Data Assessment and Parameter Estimation*

This step aims at acquiring and generating all information necessary for the quantitative evaluation of the fault tree.

The tasks of this step include the following considerations:

- Identification of the various models that describe the stochastic nature of contain phenomena related to the events of interest and the corresponding parameters that need to be estimated.
- Determination of the nature and sources of relevant data.
- Compilation and evaluation of the data to produce the necessary parameter estimations and associated uncertainties

(f) *Quantitative Evaluation of the Fault Tree*

Fault trees are quantified by the first calculating the probability of each minimal cut set and then by summing all the cut set probabilities. The quantitative evaluation produces the probability of the top event. This determines dominant cut sets and also identifies important basic events that contribute to the top event.

Sensitivity studies and uncertainty propagation provide further key information.

Identification of important basic events is very useful for decision making in resource allocation and trade off studies. Better, surveillance, maintenance and replacement can be focused on the critical events for cost effective management of reliability or risk.

(g) *Interpretation and Presentation of the Results*

It is very important to interpret the results of the analysis and present it to the decision makers in an effective manner. FTA should not be limited to documentation and set of numerical values. The FTA results must be interpreted to provide tangible implications, especially concerning the potential impact upon the objectives.

Important Points to be Considered while Constructing Fault Trees
The following issues should be considered carefully while carrying out fault tree analysis:

- To maintained consistency and traceability all the assumptions and simplifications made during the analysis should be well documented.
- To ensure quality, consistency, oppressiveness and efficiency, standard computer codes should be used.
- To ensure the clarity and ease of identification of events, a standardized format need to be adopted while giving the names in the fault tree for intermediate and basic events. The format should include specific component type and identification, specific system in which the component is located, and component failure mode. However, the formatting should be compatible with the computer code adopted.
- To avoid double counting and/or complete omission of systems/interfaces/support systems, it is strongly recommended that explicit definitions of boundary conditions should be established and documented.
- It is important to see whether protective systems or testing practices may induce failures. If such failure causes are possible, they need to be considered in the analysis.
- The following aspects should also be considered:
  - Human reliability issues
  - Operator recovery actions
  - Dependent and common causes failures
  - External environment impact (fire, flood, seismic and missile attack)

3.3.2 Elements of Fault Tree

A typical fault tree is shown in Fig. 3.25. It depicts various combinations of events leading person X late to office.

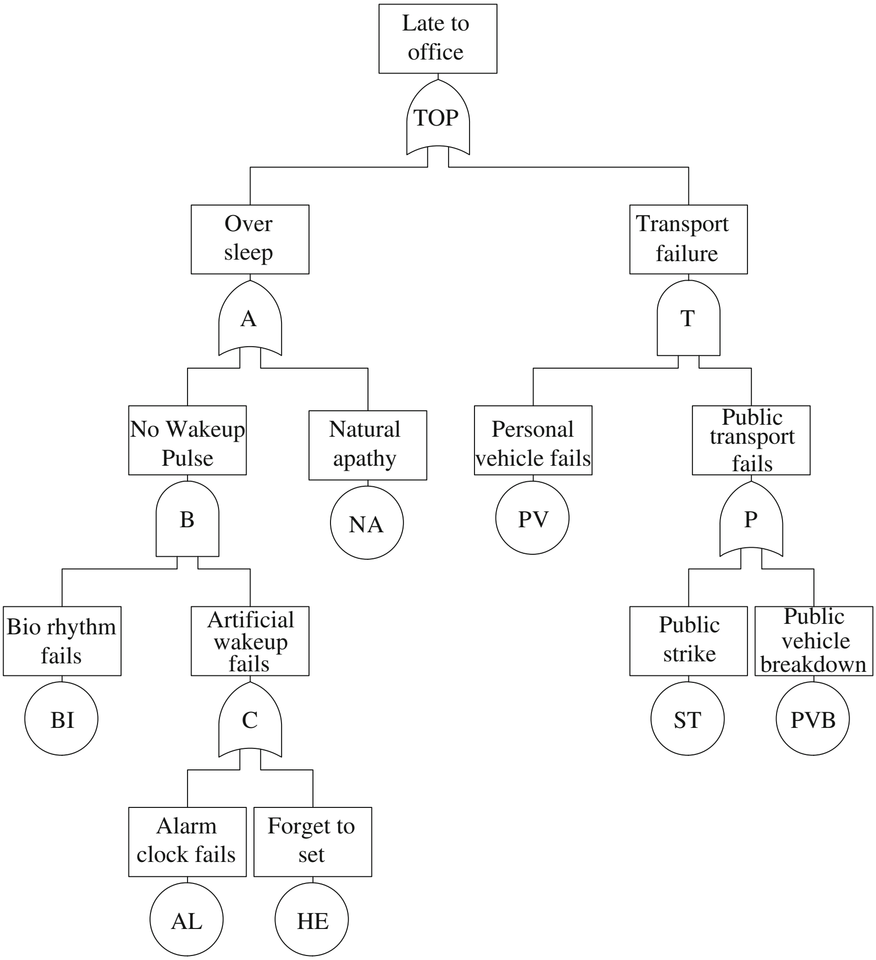


Fig. 3.25 Fault tree for the top event 'late to office'

It is essential to understand some of the terms that are used in fault tree analysis (Figs. 3.26 and 3.27).

Basic Event It is the initiating fault event that requires no further development.

Intermediate Event An intermediate event is a failure resulting from the logical interaction of primary failures.

Top Event It is an undesired event for the system under consideration and occurs as a result of occurrence of several intermediate events. Several combinations of primary failures lead to the event.

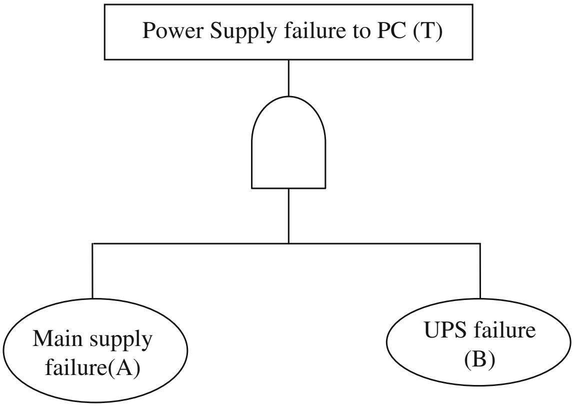


Fig. 3.26 Example forAND gate

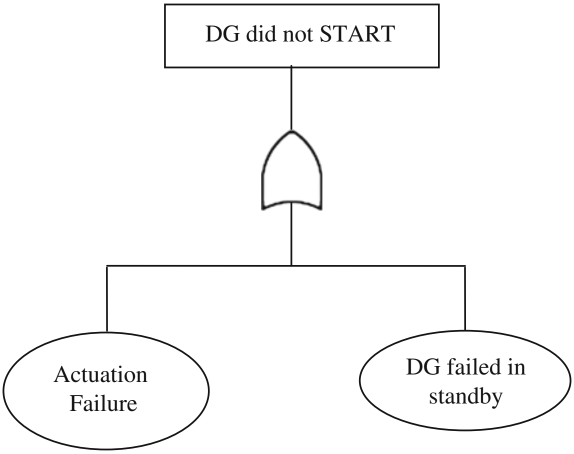


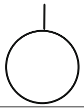
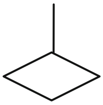
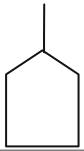
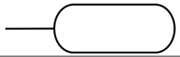
Fig. 3.27 Example for OR gate

The symbols used in fault trees for representing events and their relations have been more or less standardized. The symbols can be classified into three types, viz., event symbols (Table 3.3), gate symbols (Table 3.4) and transfer symbols (Table 3.5).

3.3.3 Evaluations of Fault Tree

The evaluations of fault tree include both qualitative evaluation and quantitative evaluation. The top events as a function of minimal cut set are determined with the help of Boolean algebra. Later, by applying probability over the Boolean expression and substitute the respective basic event probability values, the quantification is carried out. There is one to one correspondence between the fault tree gates representation and Boolean operations. Boolean algebra is explained in Chap. 2.

Table 3.3 Event symbols

Name of event	Symbol	Description
Basic event		A basic initiating fault requiring no further development
Undeveloped event		An Event which is not further developed either because it is of insufficient consequence or because information is unavailable
House event		An event which is normally expected to occur
Conditional event		Specific conditions or restrictions that apply to any logic gate

In the development of any fault tree, OR-gate and the AND-gate are often present. Both are explained here to obtain basic probability expressions.

AND Gate

This gate allows the output event to occur only if the all input events occur, representing the intersection of the input events. The AND gate is equivalent to the Boolean symbol "·".

For example, an AND gate with two input events A and B and output event T can be represented by its equivalent Boolean expression, T = A · B.

A realistic example is power supply failure to personal computer due to occurrence of both the events, failure of main supply and uninterrupted power supply (UPS) failure.

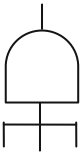
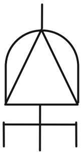
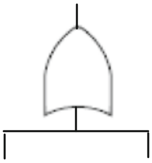
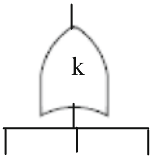
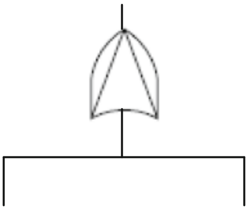
The probability formula for the top event T is given by

$$\begin{aligned} \mathrm{P(T)} &= \mathrm{P(A \cdot B)} \\ &= \mathrm{P(A) \cdot P(B)} \\ \text{or}\quad & \\ &= \mathrm{P(B) \cdot P(A/B)} \end{aligned}$$

if A and B are independent events, then

$$P(T) = P(A) \cdot P(B)$$
$$(\text{as})\quad P\left(\frac{A}{B}\right) = P(A)$$

Table 3.4 Gate symbols

<table>
<tr><th>Name of gate</th><th>Symbol</th><th>Description</th><th>Truth table</th></tr>
<tr><td>AND gate</td><td></td><td>Output fault occurs if all of the input faults occur</td><td><table><tr><td>A</td><td>B</td><td>o/p</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table></td></tr>
<tr><td>Priority gate</td><td></td><td>Output fault occurs if all the input faults occur in a specific sequence</td><td><table><tr><td>A</td><td>B</td><td>o/p</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1
(first)</td><td>1
(second)</td><td>1</td></tr><tr><td>1
(sec.)</td><td>1
(first)</td><td>0</td></tr></table></td></tr>
<tr><td>OR gate</td><td></td><td>Output fault occur if a least one of the input faults occur</td><td><table><tr><td>A</td><td>B</td><td>o/p</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table></td></tr>
<tr><td>Voting gate</td><td> </td><td>Output fault occur if a least k out of m input faults occur</td><td><table><tr><td>A</td><td>B</td><td>C</td><td>o/p</td></tr><tr><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>0</td><td>1</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>0</td><td>0</td></tr><tr><td>1</td><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td><td>1</td></tr></table></td></tr>
<tr><td>EXOR gate</td><td></td><td>Output fault occurs if exactly one of the input faults occur</td><td><table><tr><td>A</td><td>B</td><td>o/p</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table></td></tr>
</table>

(continued)

Table 3.4 (continued)

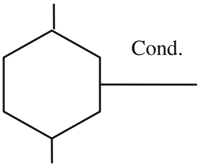
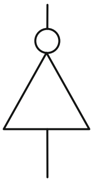
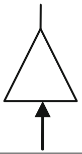
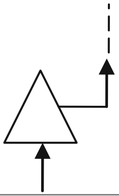
<table>
<tr><th>Name of gate</th><th>Symbol</th><th>Description</th><th>Truth table</th></tr>
<tr><td>INHIB IT gate</td><td>
</td><td>Output fault occurs if (single) the input faults occur in the presence of an enabling condition</td><td><table><tr><th>A</th><th>B</th><th>o/p</th></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td></td></tr><tr><td>1</td><td>0</td><td></td></tr><tr><td>1</td><td>1</td><td></td></tr></table></td></tr>
<tr><td>INV gate</td><td></td><td>Output event is true if and only if input event is false</td><td><table><tr><th>A</th><th>o/p</th></tr><tr><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td></tr></table></td></tr>
</table>

Table 3.5 Transfer symbols

Name of transfer symbol	Symbol	Description
Transfer—in		Indicates that the tree is developed further at the occurrence of the corresponding TRANSFER OUT. (e.g. on another page)
Transfer—out		Indicate that this portion of the tree must be attached at the corresponding TRANSFER IN

and

$$P\left(\frac{B}{A}\right) = P(B)$$

When A and B are completely dependent (if event A occurs, B will also occur)

$$P(T) = P(A)$$

In case of any partial dependency, one can give the bounds for P(T) as

$$P(A) \cdot P(B) < P(T) < P(A) \text{ or } \cdot P(B) \tag{3.34}$$

Generalizing for n input events,

For independent case,

$$P(T) = P(E_1) \cdot P(E_2)\ldots P(E_n) \tag{3.35}$$

where Ei, i = 1, 2,…n are input events.

As when Ei's are not independent

$$P(T) > P(E_1) \cdot P(E_2)\ldots P(E_n)$$

OR Gate

This gate allows the output event to occur if any one or more input event occur, representing the union of input events. The OR gate is equivalent to the Boolean symbol "+".

For example, an OR gate with two input events A and B and the output event T can be represented by its equivalent Boolean expression, T = A + B.

A practical example for OR gate is a diesel generator did not start on demand due to actuation failure or DG already in failed condition prior to demand on both.

The probability formula for the top event T is given by

$$P(T) = P(A + B)$$
$$P(T) = P(A) + P(B) - P(A \cap B)$$

where $P(A \cap B)$ is equivalent to output from an AND gate.

This can be rearranged as $P(T) = 1 - P(\bar{A} \cap \bar{B})$ where $\bar{A}$ and $\bar{B}$ denote the non-occurrence of events A and B respectively.

If the input events are mutually exclusive, then

$$\mathrm{P(T) = P(A) + P(B)}$$

If the event B is completely dependent event A then

$$\mathrm{P(T) = P(B)}$$

In case of any partial dependency, are can give bounds on P(T) as

$$P(A) + P(B) - P(A) \cdot P(B) < P(T) < P(B) \not\subset P(A) \tag{3.36}$$

Generating for n input events,

$$P(T) = 1 - P[\bar{E}_1 \cap \bar{E}_2 \cap \bar{E}_3 \cap \cdots \cap \bar{E}_n]$$

$$P(T) = \sum_{i=1}^{n} P(Ei) - \sum_{i<j} P(Ei \cap Ej) + \cdots + (-1)^{k-1} P(E_1 \cap E_2 \cap E_3 \cap \cdots \cap E_n \cap) \tag{3.37}$$

If the probability of events are low values (say P(Ei) < 0.1) and are independent then P(T) can be approximated to $P(T) = \sum_{i=1}^{n} P(Ei)$.

It is famously known as rare event approximation.

When Ei's are not independent

$$P(T) = 1 - \left\{ P(\bar{E}_1) \cdot P\left(\frac{\bar{E}_2}{\bar{E}_1}\right) \cdots P\left(\frac{\bar{E}_n}{\bar{E}_1 \cap \bar{E}_2 \cdots \cap \bar{E}_{n-1}}\right) \right\} \tag{3.38}$$

$$P(T) > \sum_{i=1}^{n} P(Ei)$$

Prior to obtaining the quantitative reliability parameter results for the fault tree, repetition of basic events and redundancies must be eliminated.

If the calculations are carried out directly on the fault tree without simplifying, the quantitative values will be incorrect.

This is achieved by obtaining minimal cut sets using Boolean algebra rules algorithms developed for the same.

There are many methods available in the literature, for example Vesely, Fussell, Kumamoto, Rasmuson. However, methods based on top-down or bottom-up successive substitution method and Monte Carlo simulation are most often used. The later is numerical computer based approach. The top-down successive substitution method can be done by simple hand calculations also. In this method, the equivalent Boolean representation of each gate in the fault tree is obtained such that only basic events remain. Various Boolean algebra rules are used to reduce the Boolean expression to its most compact form. The substitution process can proceed from the top of the tree to the bottom or vice versa. The distribution law, laws of Idempotence and the law of absorption are extensively used in there calculations. The final expression thus obtained is having minimal cut sets which is in the form of run of products, can be written in general form,

$$T = \sum_{i=1}^{n} \prod_{j=1}^{mi} E(i,j) \tag{3.39}$$

where

n no. of minimal cut sets.

m_i no. of basic events in *i*th minimal cut set.

Any fault tree will consist of finite number of minimal cut sets that are unique for that top event. If there are single order cut sets, then those single failures will lead to the occurrence of the top event.

3.3.4 Case Study

The basic aspects of fault tree analysis can be explained through an example of containment spray system which is used to scrub and cool the atmosphere around a nuclear reactor during an accident. It is shown in Fig. 3.28.

Any one of the pump and one of two discharges valves (V1 and V2) is sufficient for its successful operation. To improve the reliability, an interconnecting valve (V3) is there which is normally closed. The system is simplified and the actual system will contain more number of valves.

Step 1: The undesired top event is defined as 'No water for cooling containment'.

Step 2: The fault tree is developed deductively to identify possible events leading to the top event. These may be

- No water from 'V1 branch and V2 branch'.
- No supply to V1 or V1 itself failed. Since V1 failure is basic event, it doesn't need further analysis.
- The lack of supply to V1 is due to simultaneous failure of P1 branch and V3 branch.
- Supply from V3 branch is due to either failure of V3 or P2.
- Similarly V2 branch is also developed.

The resulting fault tree is shown in Fig. 3.29.

Step 3: Qualitative evaluation of fault tree.

The qualitative evaluation of fault tree determines minimal cut sets of fault tree. One can write the logical relationship between various events of fault tree as follows: T = A · B

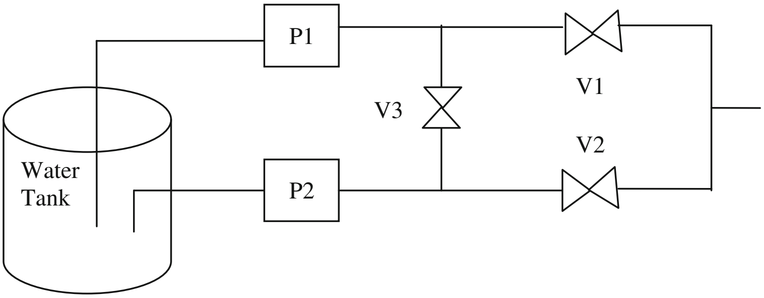


Fig. 3.28 Contain spray system of NPP

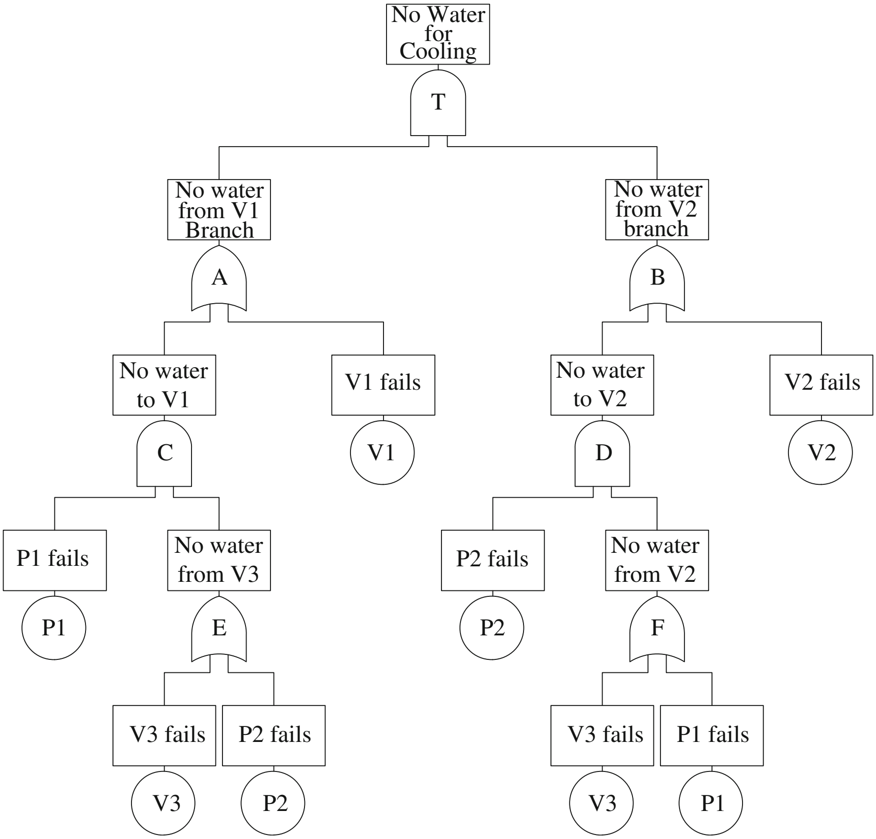


Fig. 3.29 Fault tree for containment spray system

$$A = C + V1$$
$$C = E \cdot P1$$
$$E = V3 + P2$$
$$B = D + V2$$
$$D = F \cdot P2$$
$$F = V3 + P1$$

where,

T is the top event
A, B, C, D, E, F is intermediate events
P1, P2, V1, V2, V3 are basic events.

First the top-down substitution will be performed, starting with the top event equation and substituting and expanding until the minimal cut set expression for the top event is obtained.

Substituting for A and B and expanding produces.

$$\begin{aligned} T &= (C + V_1) \cdot (D + V_2) \\ T &= C \cdot D + C \cdot V_2 + V_1 \cdot D + V_1 V_2 \end{aligned}$$

Substituting for C,

$$\begin{aligned} T &= (E \cdot P_1) \cdot D + (E \cdot P_1) \cdot V_2 + V_1 \cdot D + V_1 \cdot V_2 \\ T &= E \cdot P_1 \cdot D + E \cdot P_1 \cdot V_2 + V_1 \cdot D + V_1 \cdot V_2 \end{aligned}$$

Substituting for D,

$$\begin{aligned} T &= E \cdot P_1 \cdot (F \cdot P_2) + E \cdot P_1 \cdot V_2 + V_1(F \cdot P_2) + V_1 V_2 \\ T &= P_1 P_2 EF + EP_1 V_2 + V_1 P_2 F + V_1 V_2 \end{aligned}$$

Substituting for E,

$$T = P_1 P_2 (V_3 + P_2) \cdot F + (V_3 + P_2) P_1 V_2 + V_1 P_2 F + V_1 V_2$$

By using Distributive law,

$$\mathrm{X(Y + Z) = XY + XZ}$$

and by using Idempotent law,

$$\begin{aligned} &\mathrm{X \cdot X = X.} \\ &\quad T = P_1 P_2 V_3 F + P_1 P_2 F + P_1 V_2 V_3 + P_1 P_2 V_2 + V_1 P_2 F + V_1 V_2 \end{aligned}$$

Substituting for F and By using Distributive law,

$$\mathrm{X(Y + Z) = XY + XZ}$$

and by using Idempotent law,

$$\begin{aligned} &\mathrm{X \cdot X = X.} \\ &\quad T = P_1 P_2 V_3 (V_3 + P_1) + P_1 P_2 (V_3 + P_1) + P_1 V_2 V_3 + P_1 P_2 V_3 + V_1 P_2 (V_3 + P_1) + V_1 V_2 \\ &\quad T = P_1 P_2 V_3 + P_1 P_2 V_3 + P_1 P_2 V_3 + P_1 P_2 P_1 + P_1 V_2 V_3 + P_1 P_2 V_3 \\ &\qquad + V_1 P_2 V_3 + V_1 P_2 P_1 + V_1 V_2 \end{aligned}$$

By using Idempotent law,

$$
\begin{aligned}
&(\mathrm{X} + \mathrm{X} = \mathrm{X})\\
&T = P_1P_2V_3 + P_1P_2 + P_1V_2V_3 + P_1P_2V_2 + P_1V_2V_3 + P_1P_2V_1 + V_1V_2\\
&T = P_1P_2[V_3 + 1 + V_1 + V_2] + P_1V_2V_3 + P_2V_1V_3 + V_1V_2
\end{aligned}
$$

By using Absorption law

$$
\begin{aligned}
&(\mathrm{A} + \mathrm{AB} = \mathrm{A})\\
&T = P_1P_2 + P_1V_2V_3 + P_2V_1V_3 + V_1V_2
\end{aligned}
$$

Rearranging the terms, $T = P_1P_2 + V_1V_2 + P_1V_2V_3 + P_2V_1V_3$ which is the final Boolean expression.

There are four minimal cut sets; two double component minimal cut sets and two triple component minimal cutsets.

Step 4: The quantitative evaluation of fault determines probability of top event. The basic event probability information and list of minimal cutset required for final quantification. The probability of top event is probability over union of the minimal cut sets, it is mathematically expressed as

$$P(T) = P(P_1P_2 \cup V_1V_2 \cup P_1V_2V_3 \cup P_2V_1V_3)$$

using example For OR gate evaluation P(T) can be derived as

$$
\begin{aligned}
P(T) &= P(P_1P_2) + P(V_1V_2) + P(P_1V_2V_3) + P(P_2V_1V_3)\\
&\quad - \begin{bmatrix} P(P_1P_2V_1V_2) + P(P_1P_2V_2V_3) + P(P_1P_2V_1V_3) + P(P_1V_1V_2V_3) + P(P_1V_1V_2V_3)\\ + P(P_2V_1V_2V_3) + P(P_1P_2V_1V_2V_3) \end{bmatrix}\\
&\quad + [P(P_1P_2V_1V_2V_3) + P(P_1P_2V_1V_2V_3) + P(P_1P_2V_1V_2V_3) + P(P_1P_2V_1V_2V_3)] - [P(P_1P_2V_1V_2V_3)]\\
&= P(P_1P_2) + P(V_1V_2) + P(P_2V_1V_3) + P(P_1V_2V_3) - P(P_1P_2V_1V_2) - P(P_1V_1V_2V_3) - P(P_1P_2V_2V_3)\\
&\quad - P(P_2V_1V_2V_3) - P(P_1P_2V_1V_3) + 2P(P_1P_2V_1V_2V_3)
\end{aligned}
$$

Example 11 Main Control Power Supply (MCPS) is a very important support system in Nuclear Power Plant which provides uninterrupted A.C. power supply to safety related loads such as reactor regulation systems and safety system loads such as shut down systems. The schematic diagram of this system is shown in Fig. 3.30. There are four (Uninterrupted Power Supply) UPSs namely, UPS-1, UPS-2, UPS-3 and UPS-4; Input supply to UPS-1 and UPS-3, and UPS-2 and UPS-4 is taken from division I and division II of Class III respectively. Failure criterion is unavailability of power supply at 2 out of 3 buses. The circuit breaker can be assumed to be part of respective division supply and unavailability data can be assumed to be available for the UPS. Develop the fault tree with these assumptions and calculate the minimal cut sets of MCPS.

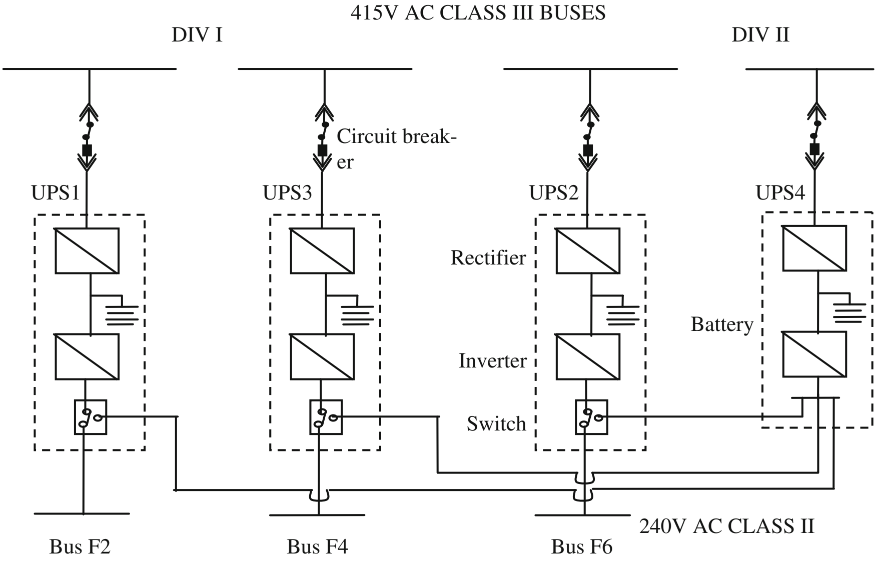


Fig. 3.30 Schematic diagram of MCPS

Solution: As the failure criterion is failure of power supply at more than 2 Buses, the top event is a voting gate with 2 out of 3: failure logic as shown in Fig. 3.31. From the fault tree we have the following Boolean expression for various gates.

$$
\begin{aligned}
T &= F2F4 + F4F6 + F2F6 \\
U1BR &= U1 \cdot DIV1 \\
U2BR &= U2 \cdot DIV2 \\
U3BR &= U3 \cdot DIV1 \\
U4BR &= U4 \cdot DIV2 \\
F2 &= U1BR \cdot U4BR \\
F4 &= U3BR \cdot U4BR \\
F6 &= U2BR \cdot U4BR
\end{aligned}
$$

Substituting successively in the top event terms,

$$
\begin{aligned}
\mathrm{F2 \cdot F4} &= \mathrm{U1BR \cdot U3BR \cdot U4BR = U1 \cdot U3 \cdot U4 \cdot DIV1 \cdot DIV2} \\
\mathrm{F4 \cdot F6} &= \mathrm{U2BR \cdot U3BR \cdot U4BR = U2 \cdot U3 \cdot U4 \cdot DIV1 \cdot DIV2} \\
\mathrm{F2 \cdot F6} &= \mathrm{U1BR \cdot U2BR \cdot U4BR = U1 \cdot U2 \cdot U4 \cdot DIV1 \cdot DIV2}
\end{aligned}
$$

Rare event approximation can be used here and the probability of the top event can be calculated by adding the probability of all the cut sets.

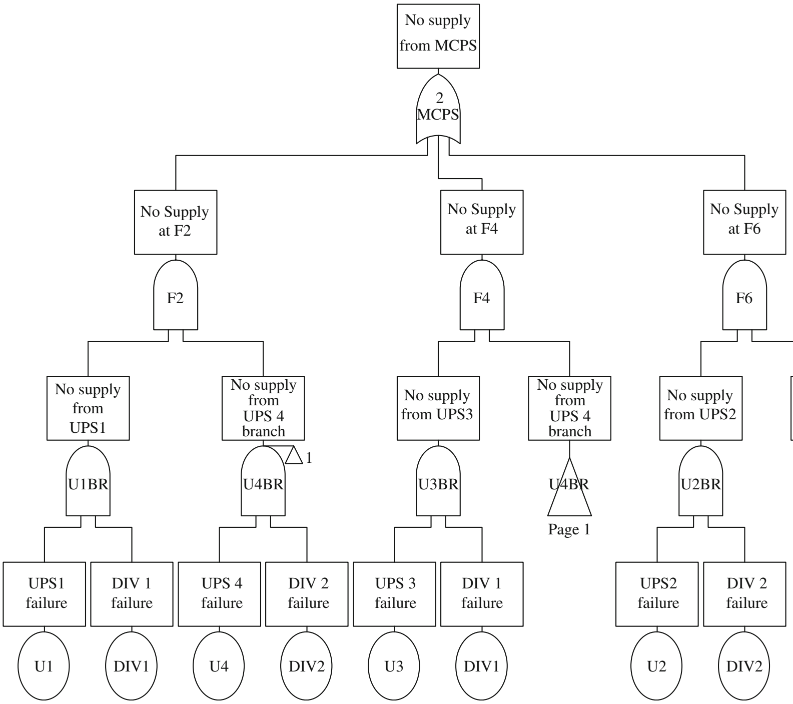


Fig. 3.31 Fault tree of MCPS

Exercise Problems

1. Calculate the reliability of the following pumping system shown in Fig. 3.32.
2. A simplified line diagram of emergency case cooling system of NPP is shown in Fig. 3.33. Calculate the availability of ECCS using cut set or path set method.
3. A system has 11 components. Components 1 through 7 are different and have reliabilities 0.96, 0.98, 0.97, 0.96, 0.94, 0.98, 0.99 respectively. Components 8 through 11 are the same, with reliability of 0.9. Components 4 and 5 are critical, and each must operate for the system to function. However, only one of the components 1, 2, and 3 has to be working and the same for 6 and 7. At least two of the four identical components must work, as well. The block diagram of the system is shown in Fig. 3.34 and find the probability the system survives.
4. Construct the typical state time diagram for the dynamic fault tree shown in Fig. 4.17. Typical component up and down states, each gate output, and the final top event should be reflected in diagram.
5. Construct the Markov model for RRS shown in Fig. 4.29. Assume different transition rates between various states. Derive the unavailability expression for the failure of RRS.

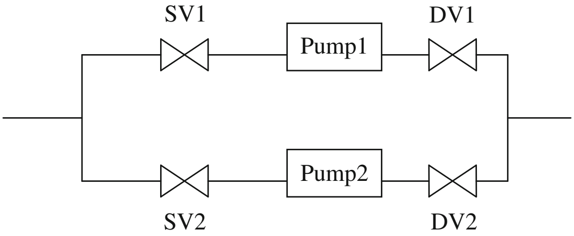


Fig. 3.32 A pumping system

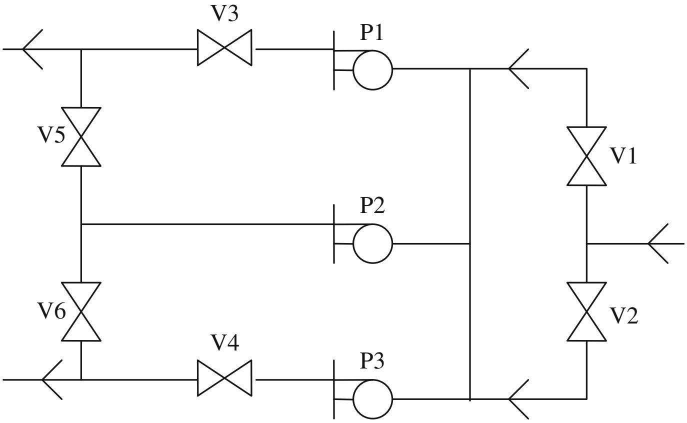


Fig. 3.33 Emergency case cooling system

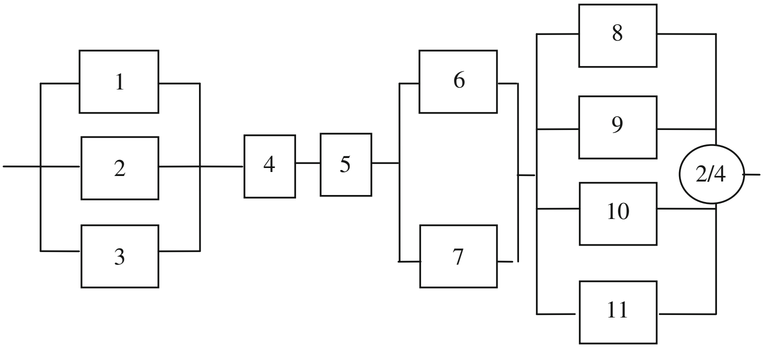


Fig. 3.34 Eleven-component system

References

1. Bureau of Indian Standards (2002) Analysis technique for dependability—Reliability block diagram method. IS 15037, Bureau of Indian Standards, New Delhi
2. Norma B. Fuqua, "The Applicability of Markov Analysis Methods to Reliability, Maintainability, and Safety", Selected Topics in Assurance Related Technologies, Vol. 10, No. 2, Reliability Analysis Center, USA
3. Dugan JB (1993) Fault trees and Markov models for reliability analysis of fault-tolerant digital systems. Reliab Eng Syst Saf 39(3):291–307
4. Durga Rao K, Gopika V, Sanyasi Rao VVS, Kushwaha HS, Verma AK, Srividya A (2009) Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. Reliab Eng Syst Saf 94(4):872–883 (ISSN: 0951-8320)
5. Vinod Gopika et al (2003) A comprehensive framework for evaluation of piping reliability due to erosion–corrosion for risk-informed inservice inspection. Reliab Eng Syst Saf 82(2):187–193
6. Vesely W et al (1981) Fault Tree Handbook. NUREG-0492, Nuclear Regulatory Commision
7. NASA (2002) Fault Tree Handbook with aerospace applications. NASA, Washington

Chapter 4
Reliability of Complex Systems

This chapter presents two advanced reliability modeling techniques, i.e. Monte Carlo simulation and dynamic fault tree analysis. They are particularly useful for modeling the reliability of complex systems.

4.1 Monte Carlo Simulation

System reliability modeling with analytical approaches such as reliability block diagram, Markov model and fault tree analysis are discussed in the previous chapter. Simulation based reliability approach using Monte Carlo methods can be useful in modeling complex systems. This section presents various elements of Monte Carlo simulation based system reliability modeling.

4.1.1 Analytical versus Simulation Approaches for System Reliability Modeling

Analytical techniques represent the system by a mathematical model and evaluate the reliability indices from this model using direct mathematical solutions. The disadvantage with the analytical approach is that the model used in the analysis is usually a simplification of the system; sometimes to an extent it becomes totally unrealistic. In addition, the output of the analytical methods is usually limited to expected values only. The complexity of the modern engineering systems besides the need for realistic considerations when modelling their availability/reliability renders analytical methods very difficult to be used. When considering only the failure characteristics of the components, the analytical approach is generally used. The models are only applicable with exponential failure/repair probability density functions. They are difficult to apply for components having non-exponential failure/repair PDFs. Analyses that involve repairable systems with multiple additional events and/or other maintainability information are very difficult (if not

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_4

impossible) to solve analytically. Modern engineering systems have complex environment as depicted in Fig. 4.1. In these cases, analysis through simulation becomes necessary.

Simulation technique estimates the reliability indices by simulating the actual process and random behaviour of the system in a computer model in order to create a realistic lifetime scenario of the system. This method treats the problem as a series of real experiments conducted in a simulated time. It estimates the probability and other indices by counting the number of times an event occurs in simulated time. Simulation is a very valuable method which is widely used in the solution of real engineering problems. Lately the utilization of this method is growing for the assessment of availability of complex systems and the monetary value of plant operations and maintenances [1–4].

The simulation approach overcomes the disadvantages of the former method by incorporating and simulating any system characteristic that can be recognised. It can provide a wide range of output parameters including all moments and complete probability density functions. It can handle very complex scenarios like inconstant transition rate, multi state systems and time dependent reliability problems. The uncertainties that arise due to simplification by the analytical mathematical models can be eliminated with simulation. However, the solution time is usually large and there is uncertainty from one simulation to another. But the recent studies show the demerits of simulation can be easily overcome with few modifications in the simulation. It is to be noted that the experimentation required is different for

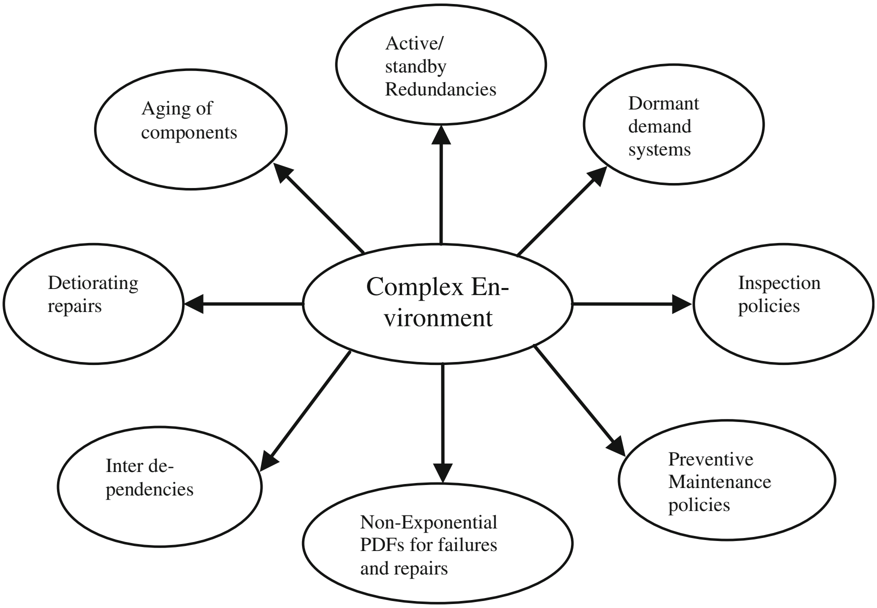


Fig. 4.1 Complex environments for system modeling

Table 4.1 Comparison of analytical and simulation techniques

Issue	Analytical techniques	Simulation techniques
Approach	Direct mathematical solutions	Numerical calculations over the simulated model
Methods	RBD, FTA, Markov model	Monte Carlo simulation
Complex scenarios	Adopt simplified mathematical models with questionable assumptions and approximations	Realistic modelling
Analysis results	Limited to point estimates only	Wide range of output parameters
Computational time	Once the algebraic analysis is over, the calculations are very simple	Large number of computer calculations

different types of problems and it is not possible to precisely define a general procedure that is applicable in all circumstances. However, the simulation technique provides considerable flexibility in solving any type of complex problem. Table 4.1 gives comparison of both the approaches with various issues.

Benefits/Applications of Simulations Based Reliability Evaluation

- Realistic Modelling of System behaviour in complex environment
- The number of assumptions can be reduced significantly
- Handling of inconstant hazard rate models at component level
- Wide range of out put parameters at the system level like failure frequency, MTBF, MTTR, unavailability, failure rate, etc.
- Dynamics in sequence of operations and complex maintenance policies can be adopted in system modelling
- Simulation model can be used for optimizing inspection interval or the replacement time of components in the system [5]
- Quantification of aleatory uncertainty associated with the random variable time to failure of overall system.
- Importance measures can be obtained from the analysis which is helpful in identifying the critical components and ranking them [6, 7].

4.1.2 Elements of Monte Carlo Simulation

In simulation, random failure/repair times from each components failure/repair distribution are generated. These failure/repair times are then combined in accordance with the way the components are reliability-wise arranged within the system. The overall results are analyzed in order to determine the behavior of the entire system. Sound understanding of the system behaviour is the prerequisite for system success/failure logic. It is assumed that the reliability values for the components have been determined using standard (or accelerated) life data analysis techniques, so that the reliability function for each component is known. With this component-level reliability information available, simulation can then be performed to determine the reliability of the entire system. The random failure/repair times of components is obtained using uniform random numbers and converting these into required density function as per the component PDF.

Evaluation of Time to Failure (or Time to Repair) of a Component
Consider a random variable x is following exponential distribution with parameter λ, f(x) and F(x) are given by the following expressions.

$$f(x) = \lambda \exp(-\lambda x)$$

$$F(x) = \int_0^x f(x)dx = 1 - \exp(-\lambda x);$$

Now x derived as a function of F(x),

$$x = G(F(x)) = \frac{1}{\lambda}\ln(\frac{1}{1 - F(x)})$$

A uniform random number is generated using any of the standard random number generators. Let us assume 0.8 is generated by random number generator then the value of x is calculated by substituting 0.8 in place of F(x) and say 1.825/yr (5e-3/h) in place of λ in the above equation

$$x = \frac{1}{5\text{e-}3}\ln(\frac{1}{1 - 0.8}) = 321.88\,\text{h}$$

This indicates time to failure of the component is 321.88 h (see Fig. 4.2).

This procedure is applicable similarly for repair time also. If the shape of PDF is different accordingly one has to solve for G(F(x)), Table 4.2 gives mathematical expressions for generating random samples for different distributions frequently used in reliability calculations. Here U_i represents a standard random number generated for *i*th iteration.

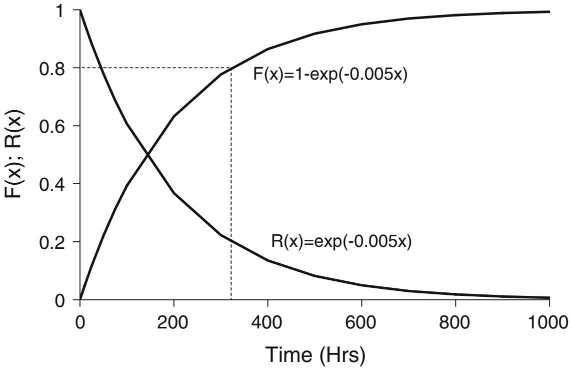


Fig. 4.2 Exponential distribution

Table 4.2 Generation of random samples for different distributions

Distribution	Random samples
Uniform (a, b)	$a + (b - a)U_i$
Exponential (λ)	$-\frac{1}{\lambda}\ln(U_i)$
Weibull (α, β)	$\alpha(-\ln U_i)^{1/\beta}$
Normal (μ, σ)	$X_i = X_s\sigma + \mu$ $X_s = (-2\ln U_i)^{1/2}\cos(2\pi U_{i+1})$
Lognormal (μ, σ)	Generate Y = ln(X) as a normal variate with mean μ and standard deviation σ and then compute $X_i = \exp(Y_i)$

4.1.3 Repairable Series and Parallel System

Components are simulated for a specified mission time for depicting the duration of available (up) and unavailable (down) states. Up and down states will come alternatively, as these states are changing with time they are called state time diagrams. Down state can be due to unexpected failure and its recovery will depend upon the time taken for repair action. Duration of the state is random for both up and down states. It will depend upon PDF of time to failure and time to repair respectively.

To first understand how component failures and simple repairs affect the system and to visualize the steps involved, the simulation procedure is explained here with the help of the two examples. The first example is a repairable series system and the second example is two unit parallel system.

Example 1—Series System A typical power supply system consists of grid supply, circuit beaker, transformer and bus. The success criterion is that the availability of power supply at the bus, which demands the successful functioning of all the components. So, it is simple four component series system. The reliability block diagram (Functional diagram) is shown in Fig. 4.3.

In addition to success/failure logic, failure and repair Probability Density Functions (PDF) of components are the input to the simulation. The PDF of failure and repair for the components are given in Table 4.3. It is assumed that all the component failure/repair PDFs are following exponential distribution. However, the procedure is same even when component PDFs are non-exponential except that the random variants will be different as per the PDF. The simulation procedure is as follows:

Step 1: Generate a random number

Step 2: Convert this number into a value of operating time using a conversion method on the appropriate times to failure distribution (exponential in the present case)

Step 3: Generate a new random number

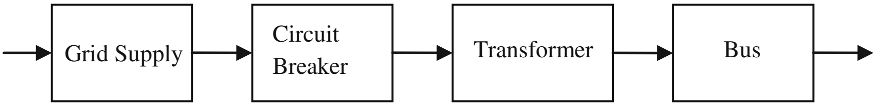


Fig. 4.3 Functional diagram of typical Class IV supply system (Problem 1)

Table 4.3 Failure and repair rate of components

S. no.	Component	Failure rate (/h)	Repair rate (/h)
1	Grid supply	2e-4	2.59
2	Circuit breaker	1e-6	0.166
3	Transformer	2e-6	0.0925926
4	Bus	1e-7	0.0925926
5	Pump (1 and 2)	3.7e-5	0.0925926

Step 4: Convert this number into a value of repair time using conversion method on the appropriate times to repair distribution

Step 5: Repeat step 1–4 for a desired period of operating life.

Step 6: Repeat steps 1–5 for each component

Step 7: Compare the sequences for each component and deduce system failure times, frequencies and other parameters.

Step 8: Repeat steps 1–7 for the desired number of simulations

Typical overview of up and down states for Class IV supply system is shown in Fig. 4.4. System failure time is sum of the component failure times if they are mutually exclusive. If there is any simultaneous failure of two or more components, failure time of component having largest value is taken for system failure time.

Reliability Evaluation with Analytical Approach

In the analytical (or algebraic analysis) approach, the system's PDF/other reliability indices are obtained analytically from each component's failure distribution using probability theory. In other words, the analytical approach involves the determination of a mathematical expression that describes the reliability of the system in terms the reliabilities of its components.

Considering components to be independent the availability expression for power supply system (A) is given by the following expression:

$$A = A_1 A_2 A_3 A_4$$

$$A_i = \frac{\mu_i}{\mu_i + \lambda_i}$$

$$A = \frac{\mu_1 \mu_2 \mu_3 \mu_4}{(\mu_1 + \lambda_1)(\mu_2 + \lambda_2)(\mu_3 + \lambda_3)(\mu_4 + \lambda_4)}$$

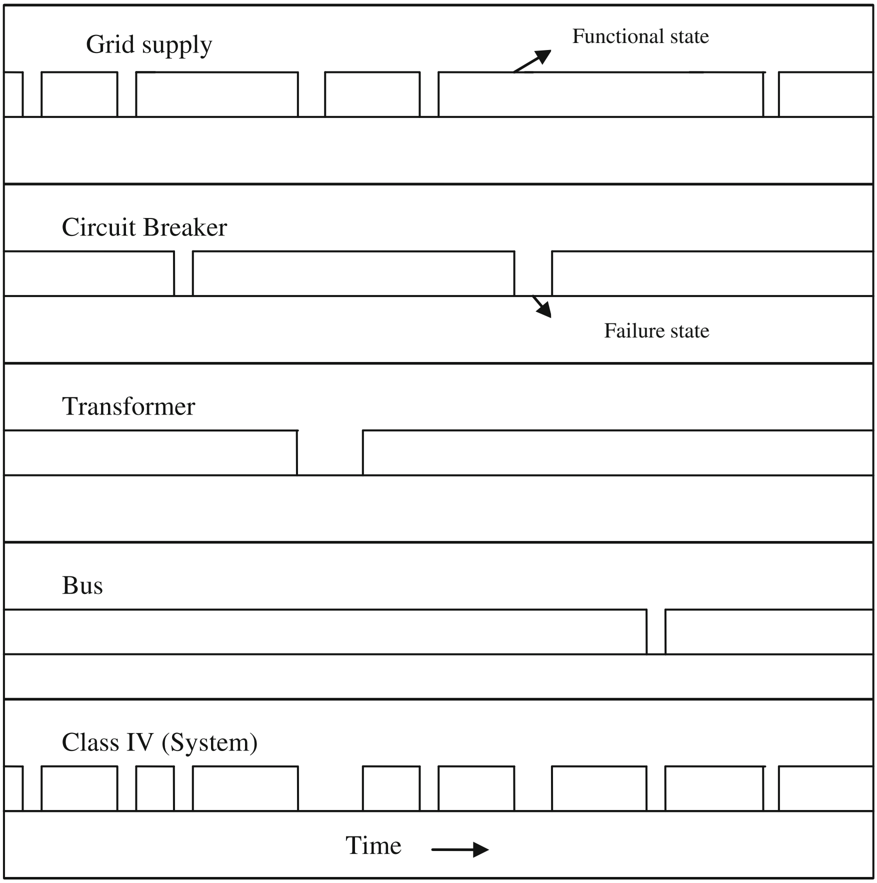


Fig. 4.4 Overview of up and down states for power supply system

A_i, λ_i, and μ_i are the availability, failure rate and repair rate of *i*th component (i = 1, 2, 3 and 4).

Example 2—Parallel System Typical emergency core cooling system of Nuclear Power Plant consists of a two unit injection pump active redundant system. One pump operation is sufficient for the successful operation of the system. The failure of the system occurs when both the pumps fail. The reliability block diagram (Functional diagram) is shown in Fig. 4.5.

Typical overview of up and down states for emergency injection pumps branch having two pumps in parallel is shown in Fig. 4.6. System failure time is the time when there is simultaneous failure of two pumps.

Considering components in the two-unit active redundant parallel pump system, to be independent, the unavailability (Q) is given by the following expression:

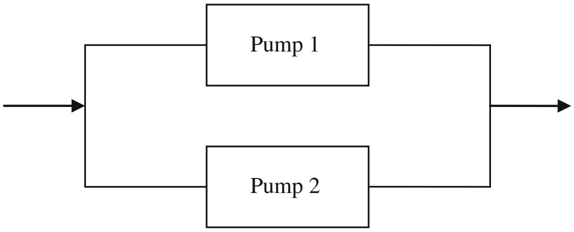


Fig. 4.5 Functional block diagram of two unit pump active redundant system

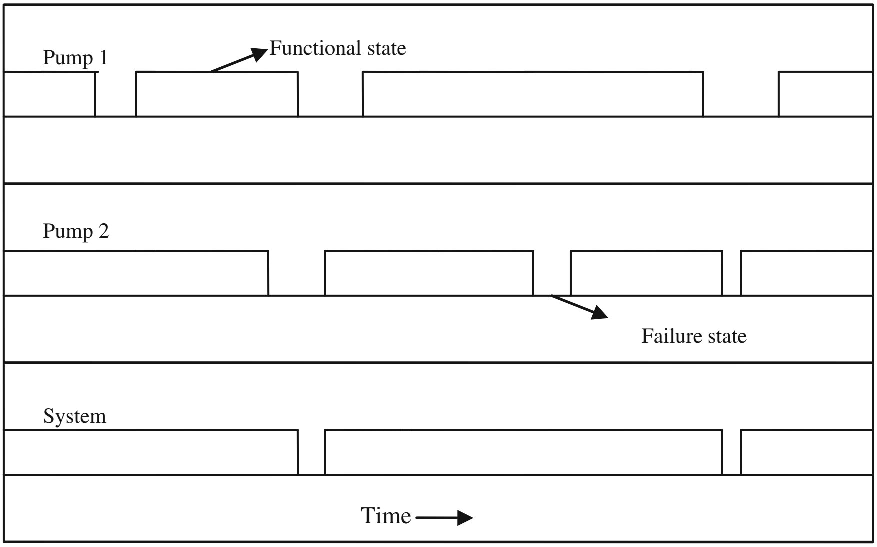


Fig. 4.6 Overview of up and down states for emergency injection pumps branch

$$Q = Q_1 Q_2$$

$$Q_i = \frac{\lambda_i}{\mu_i + \lambda_i}$$

$$Q = \frac{\lambda_1 \lambda_2}{(\mu_1 + \lambda_1)(\mu_2 + \lambda_2)}$$

Q_i, λ_i, and μ_i are the unavailability, failure rate and repair rate of *i*th component (i = 1 and 2).

Table 4.4 gives the comparison of both the approaches, analytical and simulation, for the two problems. In addition to the parameters such as average unavailability, expected number of failures, failure frequency, Mean time between failures and mean time to repair, simulation can give Cumulative Density Function (CDF) of random variable time between failures for the system under consideration.

Table 4.4 Summary of results

Parameter	Series		Parallel	
	Analytical	Simulation	Analytical	Simulation
Average unavailability	1.059e-4	1.059e-4	1.59e-7	1.61e-7
Avg. no. of failures	2030.78	2031.031	2.955	2.997
Failure frequency (/h)	2.031e-4	2.031e-4	2.95e-8	2.99e-8
Mean time between failure (h)	4924.21	4923.51	33.84e+6	33.36e+6
Mean time to repair (h)	0.5214	0.5214	5.39	5.37

Fig. 4.7 CDF of series system

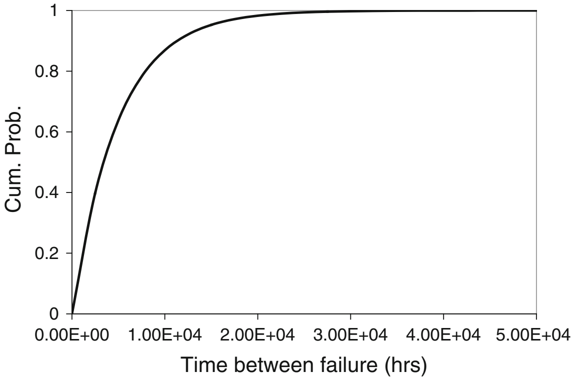
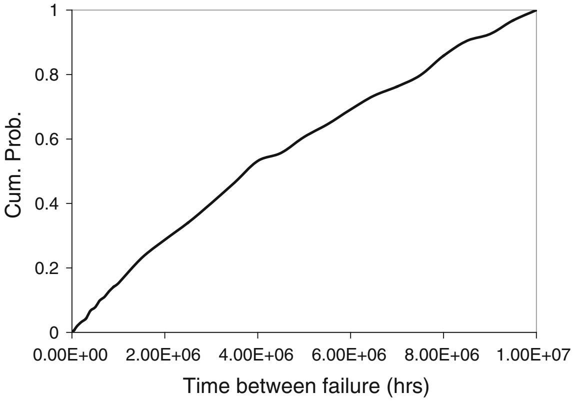


Fig. 4.8 CDF of parallel system



The CDF of problem 1 and problem 2 are shown in Figs. 4.7 and 4.8 respectively. Mission times of 10^7 and 10^8 h are considered for problem 1 and problem 2 respectively. Simulation results are from 10^4 iterations in both the cases.

4.1.4 Simulation Procedure for Complex Systems

The simulation procedure is explained below for systems having complex operating environments [8]:

1. System failure logic is obtained from qualitative FTA or RBD in the form of minimal cut-sets (combination of minimum number of component failures leading to system failures)
2. Probability density functions for time to failure/repair of all basic components are obtained from the past experience or lab testing. Maintenance policies of all components have to be collected from the system technical specifications record. Information such as interval and duration of tests and preventive maintenance are obtained in this step.
3. Generation of Component State Profiles Components are simulated for a specified mission time for depicting the duration of available (up) and unavailable (down) states. If component is repairable as is the case for most of practical systems, up and down states will come alternatively. Down state can be due to failure or scheduled maintenance activity. Duration of the state is random for up state and also for down state if it is unscheduled repair, where as scheduled maintenance activity may be a fixed value.

   Active Components: Active component is the one which is in working condition during normal operation of the system. Active components can be either in success state or failure state. Based on the PDF of failure of component, time to failure is obtained from the random variant calculations. The failure is followed by repair whose time depends on the PDF of repair time. This sequence is continued until it reaches the predetermined system mission time.

   Standby/Dormant Components: These components are required on demand due to the failure of active components. When there is no demand, it will be in standby state or may be in failed state due to on-shelf failure. It can also be unavailable due to test or maintenance state as per the scheduled activity when there is a demand for it. This makes the component to have multi states and such stochastic behaviour need to be modelled to exactly suit the practical scenario. Down times due to the scheduled test and maintenance policies are first accommodated in the component state profiles. In certain cases test override probability has to be taken to account for its availability during testing. As the failures occurred during standby period can not be revealed till its testing, time from failure till identification has to be taken as down time. It is followed by imposing the standby down times obtained from the standby time to failure PDF and time to repair PDF. Apart from the availability on demand, it is also required to check whether the standby component is successfully meeting its mission. This is incorporated by obtaining the time to failure based on the operating failure PDF and is checked with the mission time, which is the down time of active component.
4. Generation of system state profile System state profile is developed by integrating components state profiles with the system failure logic. Failure logic of

complex systems is generally derived from fault tree analysis, which is logical and graphical description of various combinations of failure events. Fault tree analysis represents failure logic of the system with the sum of minimal cut-sets. In other words, system logic is denoted with series configuration of parallel subsystems. Each minimal cut-set represents this subsystem which will have certain basic components in parallel.

5. State profile for each minimal cut-set is generated based on component state profiles obtained from step 3. Down state is identified by calculating the duration that all the components in the cut-set under consideration are simultaneously unavailable as it is equivalent to a parallel configuration. MCS state is in up state in the remaining duration of the mission. Thus, state profile for MCS is also in up and down states alternatively through out its mission.
6. System states are generated from state profiles of MCS which are obtained from step 4. As system is in series configuration of all MCS, down state of every MCS imposes the same down state on the system. Thus all down states of all MCS are reflected in system state profile and the remaining time of the mission is in the up state.
7. Steps 3 and 4 are repeated for sufficient number of simulations and required measures of reliability are obtained from the simulation results.

4.1.4.1 Case Study—AC Power Supply System of Indian NPP

Reliability Analysis for a practical system by adopting the above discussed procedure is presented here. AC Power Supply System is chosen as the case of application as it is very important system in the safe operation of Nuclear Power plant. This system is having redundant components having multi state systems with different maintenance policies. System specific information to the extent possible is used in the modelling.

Description of the System

Electrical Power supply is essential in the operation of process as well as safety systems of any NPP. To ensure high reliability of power supply systems, high redundancy and diversity are provided in the design. Loss of off-site power supply coupled with loss of on-site AC power is called station blackout. In many PSA studies [9], severe accident sequences resulting from station blackout conditions have been recognized to be significant contributors to the risk of core damage. For this reason the reliability/availability modelling of AC Power supply system is of special interest in PSA of NPP.

The electrical power supply system of Indian NPP consists of four classes. In the station blackout criteria, Class IV and Class III systems are only there. Class IV power is supplied from two sources (i) Grid supply and (ii) Station Alternator Supply. Class III can be termed as redundant to Class IV supply. Whenever Class IV is unavailable, two Class III buses are fed from dedicated standby Diesel Generators (DGs) of 100 % capacity each. There are three standby DGs. These DGs start

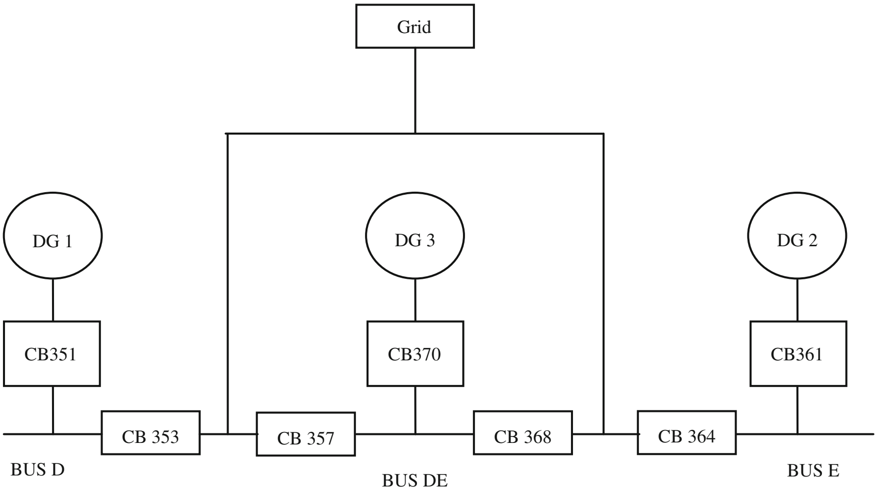


Fig. 4.9 Schematic diagram of AC electrical power supply

automatically on failure of Class IV power supply through emergency transfer scheme. Two of the DGs supply power to the buses to which they are connected. In case of failure/unavailability of any of these two DGs, the third DG can be connected automatically to any of the two Class III buses. In case only one DG is available the tie breaker between the buses closes automatically. The class III loads are connected to the buses in such a way that failure of any bus will not affect the performance of systems needed to ensure safety of the plant. Thus one DG is sufficient for all the emergency loads and this gives a redundancy of one out of three. The line diagram of AC Power supply system in Indian NPP is shown in Fig. 4.9.

System Modelling

Failure/Success logic of system can be obtained from developing Reliability Block Diagram (RBD) or Qualitative Fault Tree Analysis. The interaction between failure of components and their impact on system success state is depicted with RBD or FTA. The later method is suitable when there is complex configuration. However, both the approaches are adopted here to give the list of minimal cut-sets. RBD for the system is shown in Fig. 4.10. There can be dependency between the cut-sets and this is properly accounted in the analysis. Parameters of distribution for all the components in the systems are shown in the Table 4.5 [10]. Time to failure and time to repair are observed to follow exponential distribution from the operating experience. However, by changing the random variant in the simulation one can do simulation for any kind of PDF for time to failure or time to repair.

System specific test and maintenance information is obtained from the operating experience. All DGs are tested with no-load once in a week and tested with load once in two months. Scheduled maintenance is carried out once in 3 months on all the DGs. However, maintenance is not simultaneously carried out for more than one

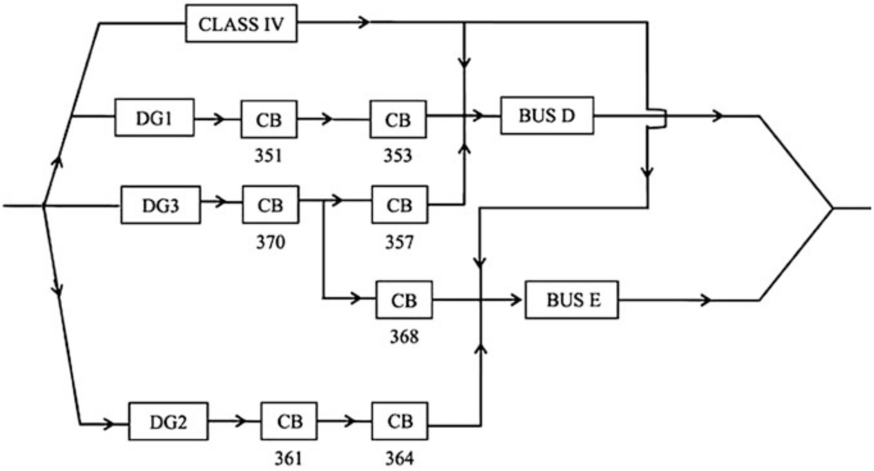


Fig. 4.10 Reliability block diagram of AC power supply system

Table 4.5 Failure rate and repair rate of components

S. no.	Component	Description	Failure Rate (/h) (operating)	Failure rate (/h) (standby)	Repair rate (/h)
1	CLIV	Class IV supply	2.34E-04	–	2.59
2	DG1	Diesel generator 1	9.00E-05	5.33E-04	8.69E-02
3	CB351	Circuit breaker 351	3.60E-07	2.14E-05	0.25
4	CB353	Circuit breaker 353	3.60E-07	2.14E-05	0.25
5	BUSD	Bus D	3.20E-07	–	0.125
6	DG3	Diesel generator 3	9.00E-05	5.33E-04	8.69E-02
7	CB370	Circuit breaker 370	3.60E-07	2.14E-05	0.25
8	CB357	Circuit breaker 357	3.60E-07	2.14E-05	0.25
9	CB368	Circuit breaker 368	3.60E-07	2.14E-05	0.25
10	BUSE	Bus E	3.20E-07	–	0.125
11	DG2	Diesel generator 2	9.00E-05	5.33E-04	8.69E-02
12	CB361	Circuit breaker 361	3.60E-07	2.14E-05	0.25
13	CB364	Circuit breaker 364	3.60E-07	2.14E-05	0.25
14	DG-CCF	Common cause failure	1.00E-05	5.92E-05	4.166E-02

DG. During no-load or full load test, DGs can take the demand which makes override probability as one and test duration will not come under down time. Schedule maintenance is carried out on all CBs once in a year during the reactor shut-down. Test and maintenance policy for standby components of the system is given in Table 4.6.

Table 4.6 Test and maintenance policy for standby components

S. no.	Component	No-load test (h)		Load test (h)		Preventive maintenance (h)	
		Interval	Duration	Interval	Duration	Interval	Duration
1	DG1	168	0.0833	1440	2	2160	8
2	CB351	168	0.0833	1440	2	8760	2
3	CB353	168	0.0833	1440	2	8760	2
4	DG3	168	0.0833	–	–	2184	8
5	CB370	168	0.0833	–	–	8760	2
6	CB357	–	–	–	–	8760	2
7	CB368	–	–	–	–	8760	2
8	DG2	168	0.0833	1440	2	2208	8
9	CB361	168	0.0833	1440	2	8760	2
10	CB364	168	0.0833	1440	2	8760	2

Results and Discussion

Fault tree analysis approach with suitable assumptions is often used for unavailability assessment as a part of Level-1 Probabilistic Safety Assessment of NPP. It is assumed that the unavailability of a standby system can be reasonably approximated by the use of fault trees (or some other logic models) in which the component time averaged unavailabilities are used as the probabilities of basic events [11]. To reduce the burden of calculations, the time dependent unavailabilitites of the components are substituted in some logic models by their average values over the period of analysis. In addition to these assumptions and approximations (rare event), actual processes (complex interaction and dependencies between components) and random behaviour of the systems are depicted with simplified logic models. The output results from this approach are limited to point estimates only. Using this fault tree (cut-set) approach, unavailability thus obtained is 5.87e-7.

An alternative approach could be based on Markov models. These models can take into account wide range of dependencies; however, they are restrictive in terms of number of components, preventive maintenance and failure/repair time distributions. Furthermore it is not possible to take into account any trends or seasonal effects. Another alternative could be the use of semi-Markov models. The scalability in terms of number of possible states of the system, and number of maintenance actions, is an important advantage of this models, however they are also complex and therefore very difficult to handle when the number of system possible states increases.

The subsystems of AC Power Supply System have multi-states due to surveillance tests and scheduled maintenance activities. In addition, the operation of DG involves starting and running (till its mission time) which is a sequential (or conditional) event. Furthermore, the redundancies and dependencies are adding to the complexity. Thus, this complexity or dynamic environment of the chosen problem is making Monte-Carlo simulation approach obvious choice as this method allows

Table 4.7 Summary of results

S. no.	Parameter	Value
1	Average unavailability	7.14e-7
2	Failure frequency (/h)	2.77e-6
3	Mean time between failure (h)	3.62e5
4	Mean time to repair (h)	0.673

considering various relevant aspects of system operations which cannot be easily captured by analytical methods.

Number of iterations is kept as the convergence criteria for simulation. Crude sampling approach is adopted in the present problem, however, variance reduction methods such as Latin hypercube sampling or importance sampling also can be used to improve the performance of simulation. Table 4.7 gives the summary of results obtained from simulation of 10,000 iterations and mission time of 10^6 h of operation. Average unavailability calculated from simulation approach is 7.14e-7 where as from analytical approach (fault tree-cut set approach) is 5.87e-7. The under estimation of unavailability in case of analytical approach is due to its inability to incorporate down time due to scheduled maintenance and surveillance test activities in the model. The output results from analytical approach are limited to point estimates of unavailability only. But simulation approach in addition to the parameters such as average unavailability, expected number of failures, failure frequency, Mean time between failures and mean time to repair, it can give Cumulative Distribution Function (CDF) of random variables time between failures and time to repair for the system under consideration (Figs. 4.11 and 4.12). The generated failure times of the system can be used to see how the hazard rate is varying with time. Furthermore, average unavailability with respect to time is plotted against mission time (Fig. 4.13). The results of the analysis are very important as severe accident resulting from loss of power supply is a significant event to the risk of core damage of NPP. This Simulation model can also be used for optimizing inspection interval or the replacement time of components in the system, for example, surveillance interval standby power supply can be optimized based on this model.

The Monte Carlo simulation approach is having flexibility in solving any kind of complex reliability problem. It can solve problems of dynamic in terms of sequence occurrences, time dependent, having any kind of component PDF and it can give the required system attribute. However, the solution time is usually large and there is uncertainty from one simulation to another. It is to be noted that the experimentation required is different for different types of problems and it is not possible to precisely define a general procedure that is applicable in all circumstances. However, the simulation technique provides considerable flexibility in solving any type of complex problem.

The incredible development in the computer technology for data processing at unprecedented speed levels are further emphasizing the use of simulation approaches to solve reliability problems. Use of simulation approach eliminates many of

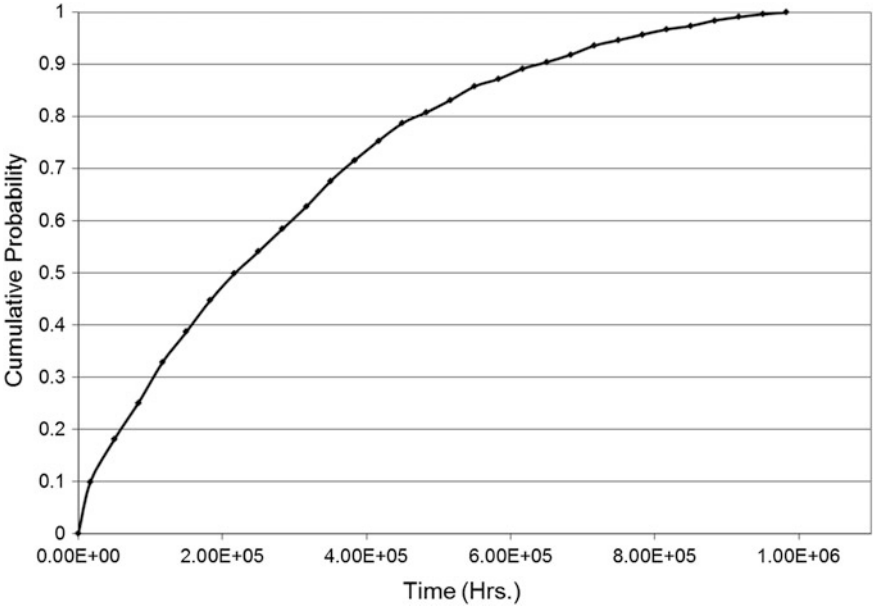


Fig. 4.11 Cumulative distribution function for the time to failure

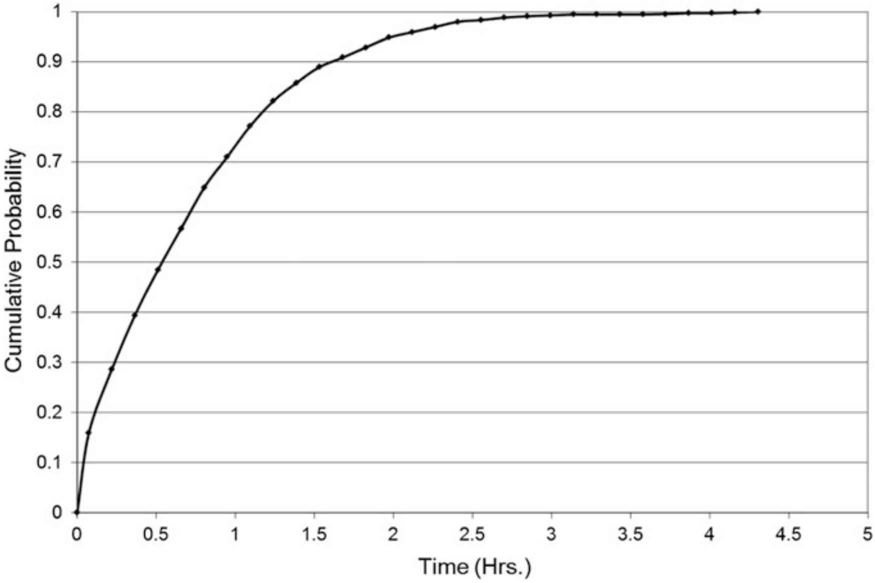


Fig. 4.12 Cumulative distribution function for the time to repair

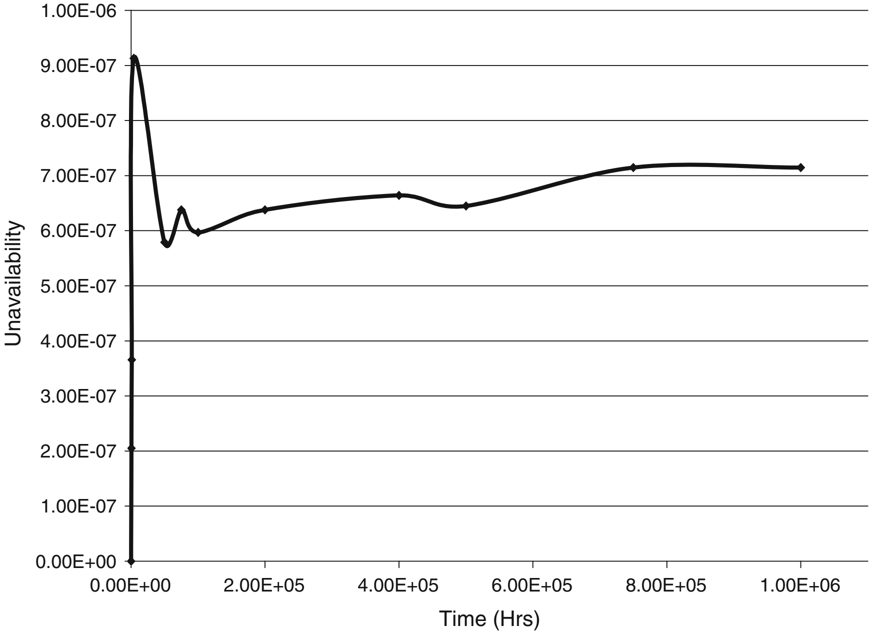


Fig. 4.13 Unavailability versus time

the assumptions that are inevitable with analytical approaches. In order to simplify the complex reliability problems, analytical approaches make lot of assumption to make it to a simple mathematical model. On the contrary, Monte Carlo simulation based reliability approach, due to its inherent capability in simulating the actual process and random behaviour of the system, can eliminate the uncertainty in system reliability modelling. One shall not forget the Einstein's quotation in this regard, "A theory should be as simple as possible, but no simpler."

4.1.5 Increasing Efficiency of Simulation

Monte Carlo sampling gives an excellent approximation of the output distribution with a sufficiently large sample size. Since it is a random sampling technique, the resulting distribution of values can be analyzed using standard statistical methods [12]. Monte Carlo sampling being subject to standard statistics, statistical techniques can be used to draw conclusions about the results.

Monte Carlo simulations demand a lot of computational resources, especially for large scale practical problems. Implementation of convergence criteria in simulation helps to improve the efficiency of simulations. As simulations run, the current percentage of error and estimate of the number of runs required to achieve a specified percentage error are tracked for convergence of the results. The convergence criterion is based on the specified confidence level and percentage error. The method used by Driels and Shin [13] in Monte Carlo simulations of weapon effectiveness is briefly discussed here. Let risk y is a function of aleatory variables whose uncertainties to be propagated. Let 'n' is the initial number of Monte Carlo simulations run (sample size). Sample mean and standard deviation are calculated. The current percentage error and estimate of number of runs required to achieve a specified percentage of error are determined using the following equations [13]. Assuming 'y' as a normally distributed random variable, the percentage error of the mean risk is

$$E = \left(\frac{100 Z_c S_y}{\bar{y}\sqrt{n}} \right)$$

where Z_c confidence coefficient, S_y standard deviation, and mean of sample is $\bar{y}$.

A relationship between the number of trial runs necessary, confidence interval, and acceptable error is shown in the following equation.

$$n = \left(\frac{2 Z_c S_y}{E\bar{y}} \right)^2$$

It was reported that the estimate of number runs convergence quickly after a few initial runs.

The random sampling or crude sampling approach discussed here is a basic sampling technique, but variance reduction techniques such as importance sampling and Latin-Hypercube sampling techniques discussed in Chap. 13 are particularly useful in reducing the computations.

4.2 Dynamic Fault Tree Analysis

Dynamic reliability methods focus on modeling the behavior of components of complex systems and their interactions such as sequence and functional dependent failures, spares and dynamic redundancy management, and priority of failure events. As an example of sequence dependent failure, consider power supply system in a Nuclear Power Plant where one active system (grid supply) and one standby system (Diesel Generator supply) connected with a switch controller. If the switch controller fails after the grid supply fails, then the system can continue operation with the DG supply. However, if the switch fails before the grid supply fails, then the DG supply can not be switched into active operation and the power supply fails when the grid supply fails. Thus, the failure criterion depends on the sequence of events also apart from combination of events. One of the most widely used approaches to address these sequential dependencies is dynamic fault tree analysis which is the marriage of conventional fault tree analysis and Markov models or Monte Carlo simulation.

4.2.1 Dynamic Fault Tree Gates

The traditional static fault trees with AND, OR, and Voting gates cannot capture the behavior of components of complex systems and their interactions. In order to overcome this difficulty, the concept of dynamic fault trees is introduced by adding sequential notion to the traditional fault tree approach [14]. System failures can then depend on component failure order as well as combination. This is done by introducing dynamic gates into fault trees. With the help of dynamic gates, system sequence-dependent failure behavior can be specified using dynamic fault trees that are compact and easily understood. The modeling power of dynamic fault trees has gained the attention of many reliability engineers working on safety critical systems.

Dynamic Fault Trees (DFT) introduces four basic (dynamic) gates: the priority AND (PAND), the sequence enforcing (SEQ), the warm spare (WSP), and the functional dependency (FDEP) [14]. They are discussed here briefly.

The PAND gate reaches a failure state if all of its input components have failed in a pre-assigned order (from left to right in graphical notation). In Fig. 4.14, a failure occurs if A fails before B, but B may fail before A without producing a failure in G. A truth table for a PAND gate is shown in Table 4.8, the occurrence of event is represented as 1 and its non occurrence as 0. In the second case though both A and B have failed but due to the undesired order, it is not a failure of the system.

Example of PAND Gate

Fire alarm in a chemical process plant gives signal to fire fighting personnel for further action if it detects any fire. If the fire alarm fails (got burnt in the fire) after giving alarm, then the plant will be in safe state as fire fighting is in place. However, if the alarm fails (failed in standby mode which got undetected) before the fire accident, then the extent of damage would be very high. This can be modeled by PAND gate only as the scenario exactly fits into its definition.

A SEQ gate forces its inputs to fail in a particular order: when a SEQ gate is found in a DFT, it never happens that the failure sequence takes place in different orders (Table 4.9). While the SEQ gate allows the events to occur only in a pre-assigned order and states that a different failure sequence can never take place,

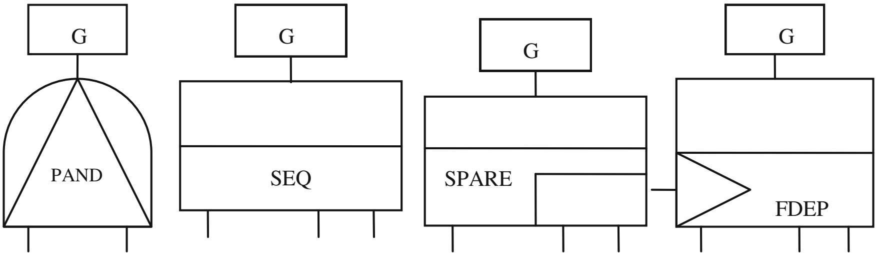


Fig. 4.14 Dynamic gates

Table 4.8 Truth table for PAND gate with two inputs

A	B	Output
1 (first)	1 (second)	1
1 (second)	1 (first)	0
0	1	0
1	0	0
0	0	0

Table 4.9 Truth table for SEQ gate with three inputs

A	B	C	Output
0	0	0	0
0	0	1	Impossible
0	1	0	Impossible
0	1	1	Impossible
1	0	0	0
1	0	1	Impossible
1	1	0	0
1	1	1	1

the PAND gate does not force such a strong assumption: it simply detects the failure order and fails just in one case.

Example of SEQ Gate
Considering a scenario where pipe in pumping system fails in different stages. There is a minor welding defect at the joint of the pipe section, which can become a minor leak with time and subsequently it lead to a rupture.

SPARE gates are dynamic gates modeling one or more principal components that can be substituted by one or more backups (spares), with the same functionality (Fig. 4.14; truth table in Table 4.10). The SPARE gate fails when the number of operational powered spares and/or principal components is less than the minimum required. Spares can fail even while they are dormant, but the failure rate of an unpowered spare is lower than the failure rate of the corresponding powered one. More precisely, λ being the failure rate of a powered spare, the failure rate of the unpowered spare is $\alpha\lambda$, where $0 \leq \alpha \leq 1$ is the dormancy factor. Spares are more properly called “hot” if $\alpha = 1$ and “cold” if $\alpha = 0$.

Table 4.10 Truth table for FDEP gate with two inputs

A	B	Output
1	1	1
0	1	0
1	0	0
0	0	0

Table 4.11 Truth table for FDEP gate with two inputs

Trigger	Output	Dependent event 1	Dependent event 2
1	1	1	1
0	0	0/1	0/1

Example of SPARE Gate
Reactor regulation system in NPP consists of dual processor hot standby system. There will be two processors which will be continuously working. Processor 1 will be normally doing the regulation; in case it fails processor 2 will take over.

In the FDEP gate (Fig. 4.14; truth table in Table 4.11), there will be one trigger-input (either a basic event or the output of another gate in the tree) and one or more dependent events. The dependent events are functionally dependent on the trigger event. When the trigger event occurs, the dependent basic events are forced to occur. In the Markov-chain generation, when a state is generated in which the trigger event is satisfied, all the associated dependent events are marked as having occurred. The separate occurrence of any of the dependent basic events has no effect on the trigger event.

Example of FDEP Gate
In the event of power supply failure, all the dependent systems will be unavailable. The trigger event is the power supply and systems which are drawing power are dependent events.

4.2.2 Modular Solution for Dynamic Fault Trees

Markov models can be used to solve dynamic fault trees. The order of occurrence of failure events can be easily modeled with the help of Markov models. Figure 4.15 shows the Markov models for various gates. However, the solution of a Markov model is much more time and memory consuming than the solution of a standard fault tree model. As the number of components increase in the system, the number of states and transition rates grows exponentially. Development of state transition diagram can become very cumbersome and mathematical solution may be infeasible.

Dugan proposed modular approach for solving dynamic fault trees. In this approach, the system level fault tree is divided into independent modules, and the modules are solved separately, then the separate results can be combined to achieve a complete analysis. The dynamic modules are solved with the help of Markov models and the solution static module is straight forward.

For example, consider the fault tree for dual processor failure, the dynamic module can be identified as shown in Fig. 4.16. The remaining module is having only static gates. Using Markov model approach the dynamic module can be solved and plugged into the fault tree for further analysis.

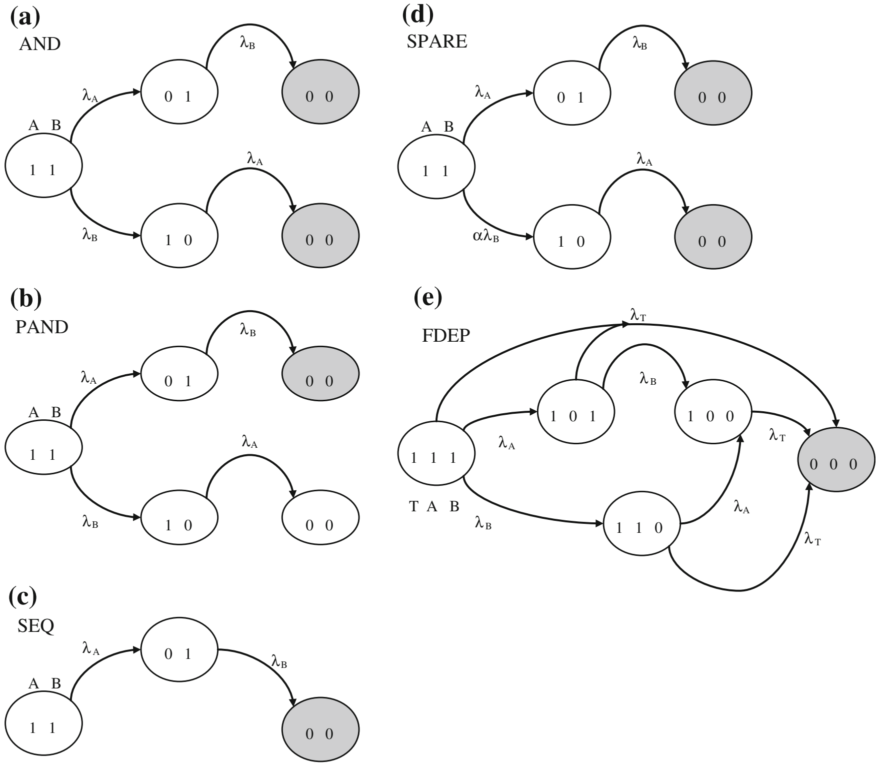


Fig. 4.15 Markov models for **a** AND gate, **b** PAND gate, **c** SEQ gate, **d** SPARE gate, **e** FDEP gate

4.2.3 Numerical Method

Amari [15], proposed a numerical integration technique for solving dynamic gates, which is explained below.

PAND Gate

A PAND gate has two inputs. The output occurs when the two inputs occur in a specified order (left one first and then right one). Let T_1 and T_2 be the random variables of the inputs (sub trees). Therefore,

$$\begin{aligned} \mathrm{G(t)} &= \Pr\{\mathrm{T_1} \le \mathrm{T_2} < \mathrm{t}\} \\ &= \int\limits_{x_1=0}^{t} dG_1(x_1)\left[\int\limits_{x_2=x_1}^{t} dG_2(x_2)\right] \\ &= \int\limits_{x_1=0}^{t} dG_1(x_1)[G_2(t) - G_2(x_1)] \end{aligned} \tag{4.1}$$

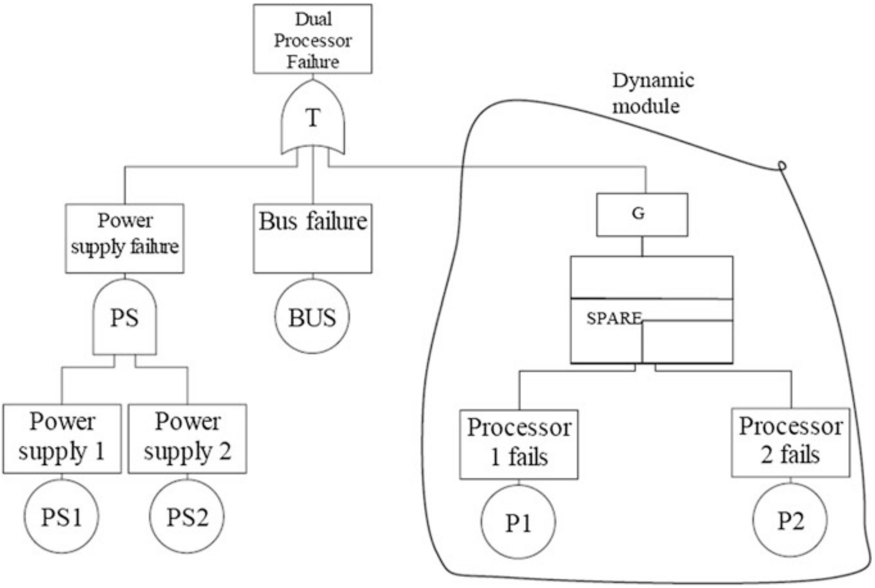


Fig. 4.16 Fault tree for dual processor failure

Once we compute $G_1(t)$ and $G_2(t)$, we can easily find G(t) in Eq. (4.1) using numerical integration methods. In order to illustrate this computation, Trapezoidal integral is used. Therefore,

$$G(t) = \sum_{i=1}^{m} [G_1(i \times h) - G_1((i-1) \times h] \times [G_2(t) - G_2(i \times h)]$$

where M is the number of time steps/intervals and h = t/M is step size/interval. The number of steps, M, in the above equation is almost equivalent to the number of steps (K) required in solving differential equations corresponding to a Markov chain. Therefore, the gain in these computations can be in the orders of n^{3n}. It shows that this method takes much less computational time than the Markov chain solution.

Example 3 Consider a PAND gate with AND and OR gates as inputs (see Table 4.12 and Fig. 4.17). For mission time 1000, calculate the top event probability?

Table 4.12 Failure data for the basic events

Gate	Failure rate of basic events				
AND	0.011	0.012	0.013	0.014	0.015
OR	0.0011	0.0012	0.0013	0.0014	0.0015

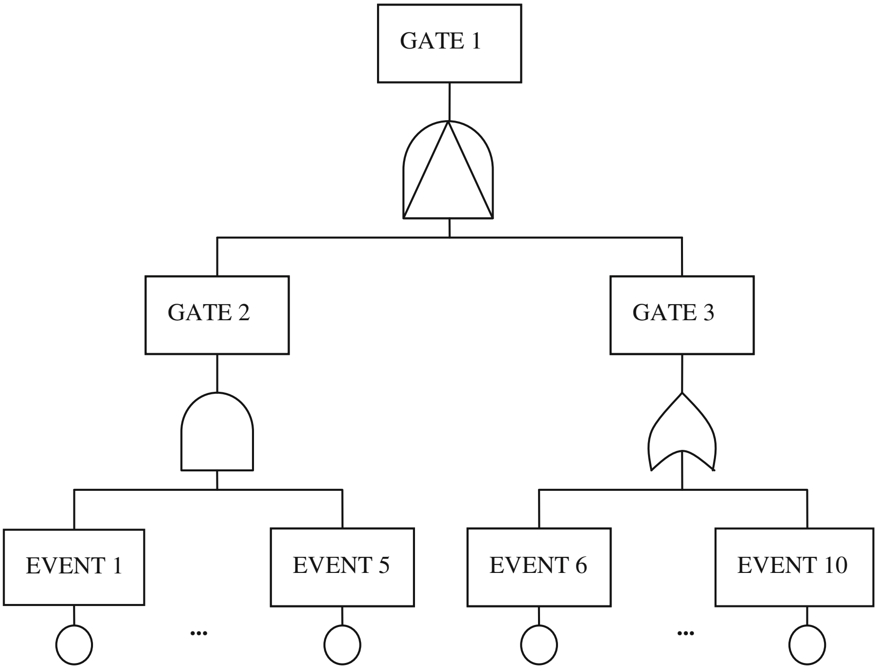


Fig. 4.17 Fault tree having dynamic gate (PAND)

Solution: Based on the numerical integration technique to solve this problem and compared it with Markov model approach. For mission time 1000 h, the top event probability is 0.362, and overall computation time is less than 0.01 s. State space approach generated 162 states and computation time is 25 s.

SEQ Gate
A **SEQ** gate forces events to occur in a particular order. The first input of a SEQ gate can be a basic event or a gate, and all other inputs are basic events.

Consider that the distributions of time to occurrence of input i is G_i; then, the probability of occurrence of the SEQ gate can be found by solving the following equation.

$$\begin{aligned} G(t) &= \Pr\{T1 + T2 + \cdots + Tm < t\} \\ &= G1 * G2 * \cdots * G_m(t) \end{aligned}$$

SPARE Gate
A generic spare (SPARE) gate allows the modeling of heterogeneous spares including cold, hot, and warm spares. The output of the SPARE gate will be true when the number of powered spares/components is less than the minimum number

required. The only inputs that are allowed for a SPARE gate are basic events (spare events). Therefore,

- If all the distributions are exponential, we can get the closed-form solutions for G(t)
- If the standby failure rate of all spares are constant (not time dependent), then G (t) can be solved using non-homogeneous Markov chains.
- Otherwise, we need to use conditional probabilities or simulation to solve this part of the fault tree.

Therefore, using the above method, we can calculate the occurrence probability of a dynamic gate without explicitly converting it into a Markov model (except for some cases of the SPARE gate).

4.2.4 Monte Carlo Simulation

Monte-Carlo simulation is a very valuable method which is widely used in the solution of real engineering problems in many fields. Lately the utilization of this method is growing for the assessment of availability of complex systems and the monetary value of plant operations and maintenances. The complexity of the modern engineering systems besides the need for realistic considerations when modelling their availability/reliability renders analytical methods very difficult to be used. Analyses that involve repairable systems with multiple additional events and/or other maintainability information are very difficult to solve analytically (Dynamic Fault trees through state space, numerical integration, Bayesian Network approaches). Dynamic fault tree through simulation approach can incorporate these complexities and can give wide range of output parameters.

The four basic dynamic gates are solved here through simulation approach [16].

PAND Gate

Consider PAND gate having two active components. Active component is the one which is in working condition during normal operation of the system. Active components can be either in success state or failure state. Based on the PDF of failure of component, time to failure is obtained from the procedure mentioned above. The failure is followed by repair whose time depends on the PDF of repair time. This sequence is continued until it reaches the predetermined system mission time. Similarly for the second component also state time diagrams are developed.

For generating PAND gate state time diagram, both the components state time profiles are compared. The PAND gate reaches a failure state if all of its input components have failed in a pre-assigned order (usually from left to right). As shown in the Fig. 4.18 (first and second scenarios), when the first component failed followed by the second component, it is identified as failure and simultaneous down time is taken into account. But, in third scenario of Fig. 4.18, both the components

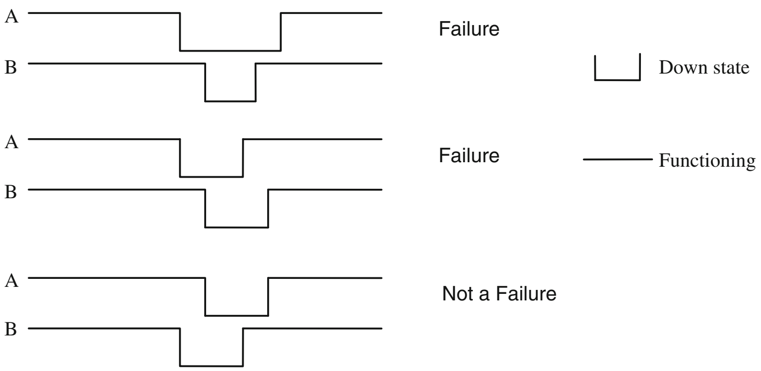


Fig. 4.18 PAND gate state-time possibilities

have failed simultaneously but second component has failed first hence it is not considered as failure.

Spare Gate
Spare gate will have one active component and remaining spare components. Component state-time diagrams are generated in a sequence starting with the active component followed by spare components in the left to right order. The steps are as follows:

- *Active components*: Time to failures and time to repairs based on their respective PDFs are generated alternatively till they reach mission time.
- *Spare components*: When there is no demand, it will be in standby state or may be in failed state due to on-shelf failure. It can also be unavailable due to test or maintenance state as per the scheduled activity when there is a demand for it. This makes the component to have multi states and such stochastic behaviour needs to be modelled to represent the practical scenario. Down times due to the scheduled test and maintenance policies are first accommodated in the component state-time diagrams. In certain cases test override probability has to be taken to account for its availability during testing. As the failures occurred during standby period can not be revealed till its testing, time from failure till identification has to be taken as down time. It is followed by imposing the standby down times obtained from the standby time to failure PDF and time to repair PDF. Apart from the availability on demand, it is also required to check whether the standby component is successfully meeting its mission. This is incorporated by obtaining the time to failure based on the operating failure PDF and is checked with the mission time, which is the down time of active component. If the first stand-by component fails before the recovery of the active component, then demand will be passed on to the next spare component.

Various scenarios with the spare gate are shown in Fig. 4.19. The first scenario shows, demand due to failure of the active component is met by the stand-by

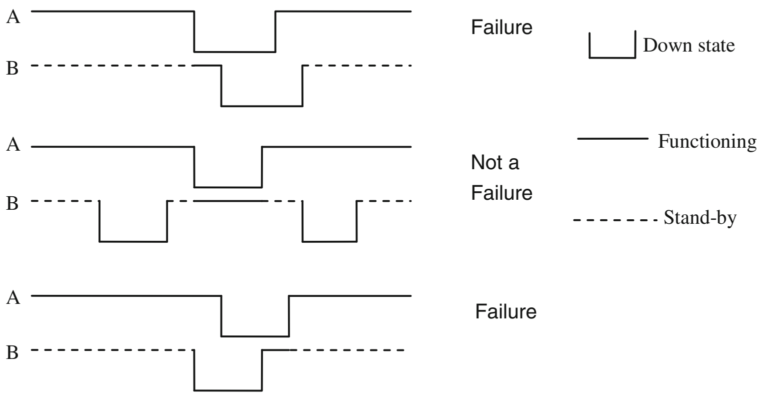


Fig. 4.19 SPARE gate state-time possibilities

component, but it has failed before the recovery of the active component. In the second scenario, demand is met by the stand-by component. But the stand-by failed twice when it is in dormant mode, but it has no effect on success of the system. In the third scenario, stand-by component is already in failed mode when the demand came, but it has reduced the overall down time due to its recovery afterwards.

FDEP Gate
The FDEP gate's output is a 'dummy' output as it is not taken into account during the calculation of the system's failure probability. When the trigger event occurs, it will lead to the occurrence of the dependent event associated with the gate. Depending upon the PDF of the trigger event, failure time and repair times are generated. During the down time of the trigger event, the dependent events will be virtually in failed state though they are functioning. This scenario is depicted in the Fig. 4.20. In the second scenario, the individual occurrences of the dependent events are not affecting the trigger event.

SEQ Gate
It is similar to Priority AND gate but occurrence of events are forced to take place in a particular fashion. Failure of first component forces the other components to follow. No component can fail prior to the first component. Consider a three input SEQ gate having repairable components (Fig. 4.21). The following steps are involved with Monte Carlo simulation approach.

1. Component state time profile is generated for first component based upon its failure and repair rate. Down time of first component is mission time for the second component. Similarly the down time of second component is mission time for the third component.
2. When first component fails, operation of the second component starts. Failure instance of the first component is taken as t = 0 for second component. Time to failure (TTF2) and time to repair/component down time (CD2) is generated for second component.

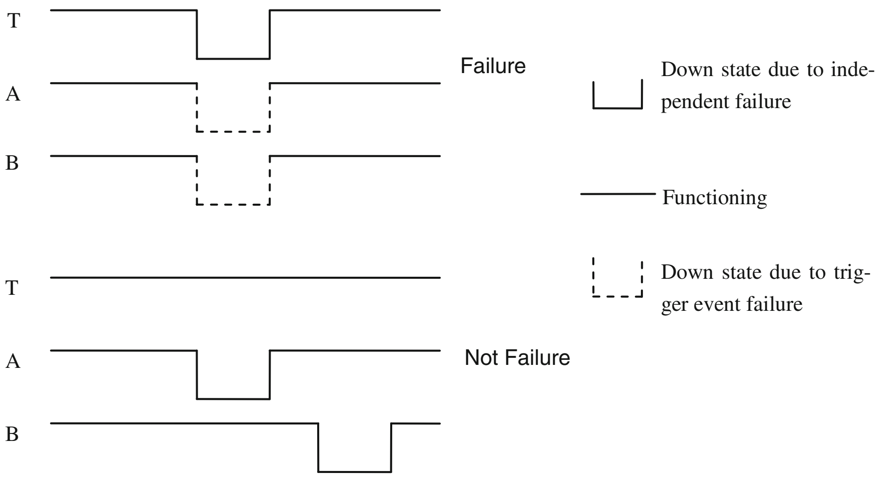
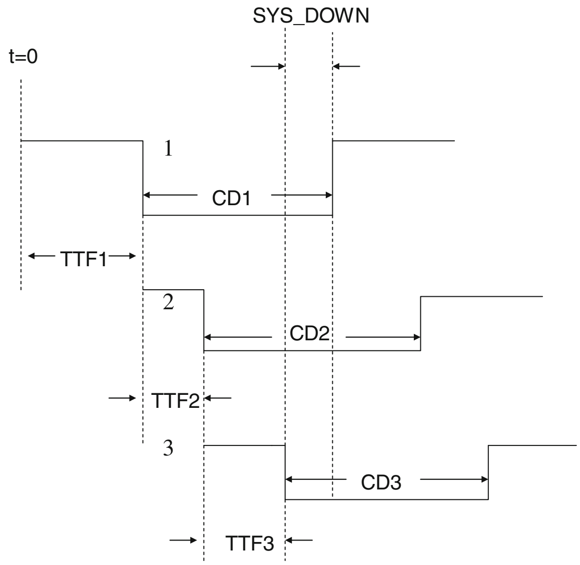

T
A
B
Failure
T
A
B
Not Failure
Down state due to independent failure
Functioning
Down state due to trigger event failure

Fig. 4.20 FDEP gate state-time possibilities

Fig. 4.21 SEQ gate state-time possibilities



3. When second component fails, operation of the third component starts. Failure instance of the second component is taken as t = 0 for third component. Time to failure (TTF3) and time to repair/component down time (CD3) is generated for third component.
4. The common period in which all the components are down is considered as the down time of the SEQ gate.
5. The process is repeated for all the down states of the first component.

TTFi	Time to failure for *i*th component
CDi	Component down time for *i*th component
SYS_DOWN	System down time.

4.2.4.1 Case Study 1—Simplified Electrical (AC) Power Supply System of NPP

Electrical power supply is essential in the operation of process and safety system of any NPP. Grid supply (Off-site-power supply) known as Class IV supply is the one which feeds all these loads. To ensure high reliability of power supply, redundancy is provided with the diesel generators known as Class III supply (also known as on-site emergency supply) in the absence of Class IV supply to supply the loads. There will be sensing and control circuitry to detect the failure of Class IV supply which triggers the redundant Class III supply. Loss of off-site power supply (Class IV) coupled with loss of on-site AC power (Class III) is called station blackout. In many PSA studies [9], severe accident sequences resulting from station blackout conditions have been recognized to be significant contributors to the risk of core damage. For this reason the reliability/availability modelling of AC Power supply system is of special interest in PSA of NPP.

The reliability block diagram is shown in Fig. 4.22. Now this system can be modeled with the dynamic gates to calculate the unavailability of overall AC power supply of a NPP.

The dynamic fault tree (Fig. 4.23) has one PAND gate having two events, namely, sensor and Class IV. If sensor fails first then it will not be able to trigger the Class III, which will lead to non-availability of power supply. But if it fails after already triggering Class III due to occurrence of Class IV failure first, it will not

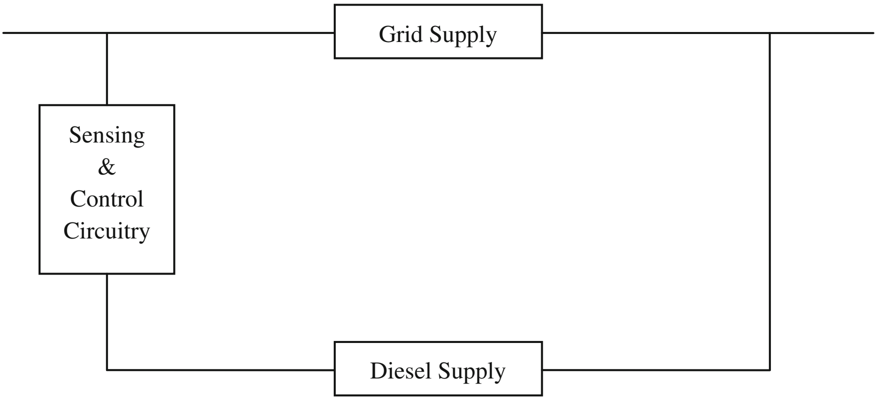


Fig. 4.22 Reliability block diagram of electrical power supply system of NPP

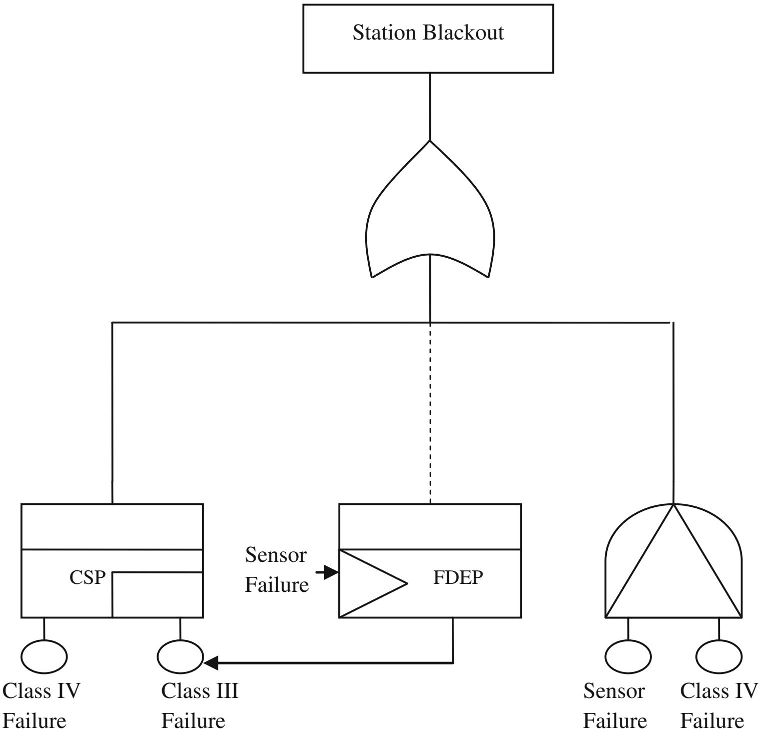


Fig. 4.23 Dynamic fault tree for station black out

affect the power supply. As Class III is a stand-by component to Class IV, it is represented with a spare gate. This indicates their simultaneous unavailability will lead to supply failure. There is a functional dependency gate as the sensor is the trigger signal and Class III is the dependent event.

This system is solved with Analytical approach and Monte Carlo simulation.

Solution with Analytical Approach
Station blackout is the top-event of the fault tree. Dynamic gates can be solved by developing state-space diagrams and their solutions give required measures of reliability. However, for sub-systems which are tested (surveillance), maintained and repaired if any problem is identified during check-up, can not be modeled by state space diagrams. Though, there is a school of thought that initial state probabilities can be given as per the maintenance and demand information, this is often debatable. A simplified time averaged unavailability expression is suggested by IAEA P-4 [11] for stand-by subsystems having exponential failure/repair characteristics. The same is applied here to solve stand-by gate. If Q is the unavailability of stand-by component, it is expressed by the following equation. Where λ is failure rate, T is test interval, τ is test duration, f_m is frequency of preventive maintenance, T_m is duration of maintenance, and T_r is repair time. It is sum of contribution from

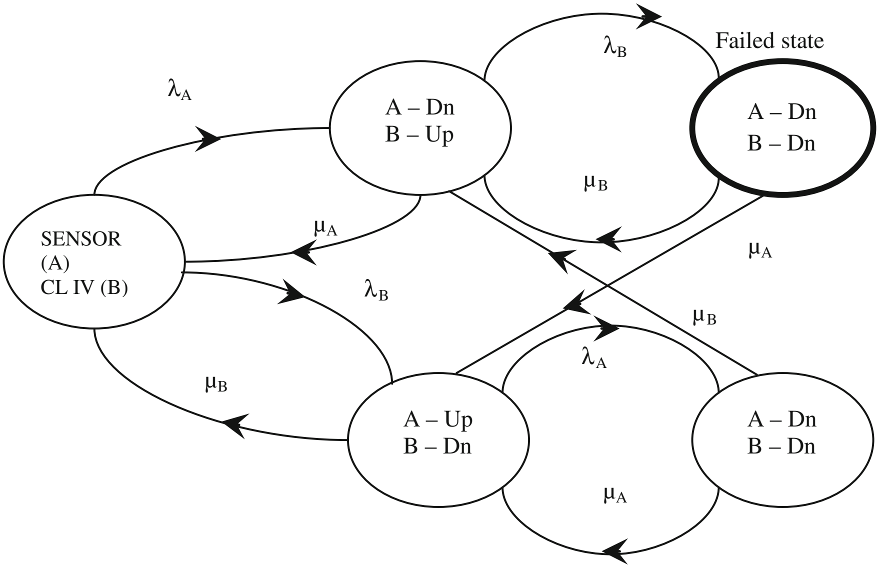


Fig. 4.24 Markov (state-space) diagram for PAND gate having sensor and Class IV as inputs

failures, test outage, maintenance outage and repair outage. In order to obtain the unavailability of stand-by gate, unavailability of Class IV is multiplied with the unavailability of stand-by component (Q).

$$Q = \left[1 - \frac{1 - e^{-\lambda T}}{\lambda T}\right] + [\frac{\tau}{T}] + [f_m T_m] + [\lambda T_r]$$

The failure of Sensor and Class IV is modeled by PAND gate in the fault tree. This is solved by state-space approach by developing Markov model as shown in Fig. 4.24. The bolded state where both the components failed in the required order is the unavailable state and remaining states are all available states. ISOGRAPH software has been used to solve the state-space model. Input parameter values used in the analysis are shown in Table 4.13 [10]. The sum of the both the values (PAND and SPARE) give the unavailability of station blackout scenario which is obtained as 4.847e-6.

Table 4.13 Component failure and maintenance information

Component	Failure rate (/h)	Repair rate (/h)	Test period (h)	Test time (h)	Maint. period (h)	Maint. time (h)
CLASS IV	2.34e-4	2.59	–	–	–	–
Sensor	1e-4	0.25	–	–	–	–
CLASS III	5.33e-4	0.08695	168	0.0833	2160	8

Solution with Monte Carlo simulation
As one can see Markov model for a two component dynamic gate is having 5 states with 10 transitions, thus state space becomes unmanageable as the number of components increases. In case of stand-by components, the time averaged analytical expression for unavailability is only valid for exponential cases. To address these limitations, Monte-Carlo simulation is applied here to solve the problem.

In simulation approach, random failure/repair times from each components failure/repair distributions are generated. These failure/repair times are then combined in accordance with the way the components are reliability wise arranged with in the system. As explained in the previous section, PAND gate and SPARE gate can easily be implemented through simulation approach. The difference from normal AND gate to PAND and SPARE gates is that the sequence of failure has to be taken into account and stand-by behavior including the testing, maintenance, dormant failures have to be accommodated. The unique advantage with simulation is incorporating non-exponential distributions and eliminating S-independent assumption.

Component state-time diagrams are developed as shown in Fig. 4.25 for all the components in the system. For active components which are independent, only two states will be there, one is functioning state (UP—operational state) and second is repair state due to failure (DOWN-repair state). In the present problem, CLASS IV and sensor are active components where as CLASS III is stand-by component. For class III, generation of state-time diagram involves more calculations than former. It is having six possible states, namely: testing, preventive maintenance, corrective

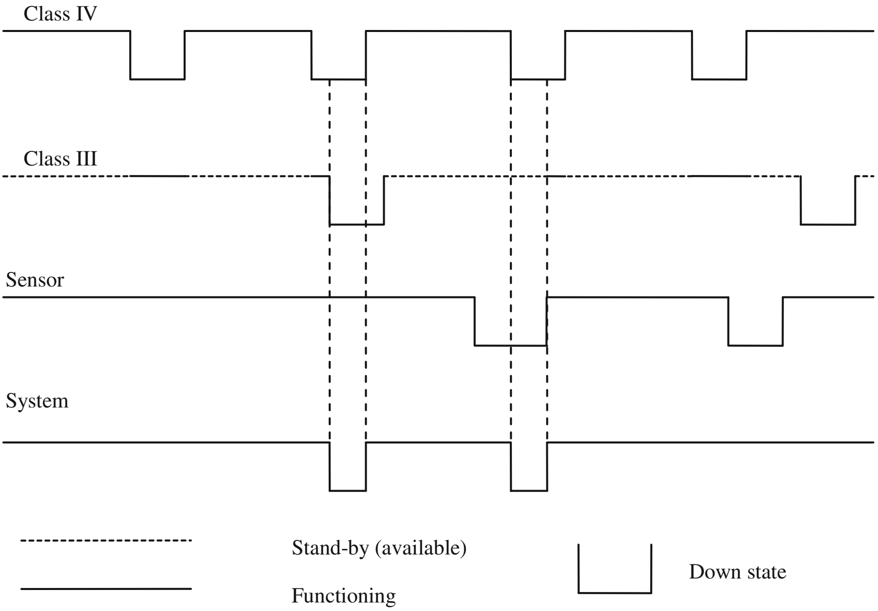


Fig. 4.25 State-time diagrams for Class IV, Sensor, Class III and overall system

maintenance, stand-by functioning, stand-by failure undetected, and normal functioning to meet the demand. As testing and preventive maintenance are scheduled activities, they are deterministic and are initially accommodated in component profile. Stand-by failure, demand failure and repair are random and according to their PDF the values are generated. The demand functionality of CLASS III depends on the functioning of sensor and Class IV. Initially after generating the state-time diagrams of sensor and CLASS IV, the DOWN states of CLASS IV is identified and sensor availability at the beginning of the DOWN state is checked to trigger the CLASS III. The reliability of CLASS III during the DOWN state of CLASS IV is checked. Monte-Carlo simulation code has been developed for implementing the station blackout studies. Unavailability obtained is 4.8826e-6 for a mission time of 10,000 h with 10^6 simulations which is in agreement with the analytical solution. Failure time, repair time and unavailability distributions are shown in Figs. 4.26, 4.27 and 4.28 respectively.

Fig. 4.26 Failure time distribution

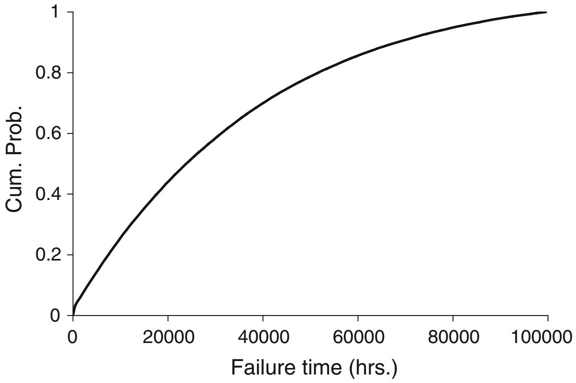
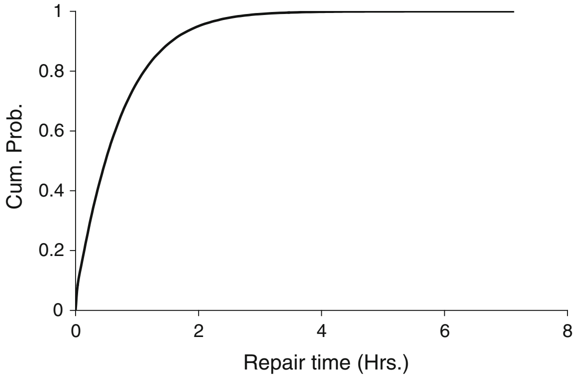


Fig. 4.27 Repair time distribution



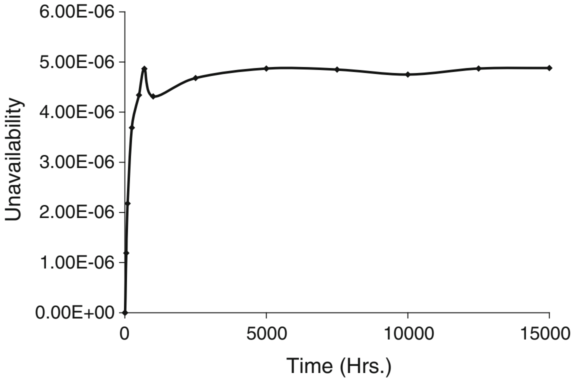


Fig. 4.28 Unavailability with time

4.2.4.2 Case Study 2—Reactor Regulation System (RRS) of NPP

The Reactor Regulation System (RRS) regulates rector power in NPP. It is a Computer-based Feedback Control System. The regulating system is intended to control the reactor power at a set demand from 10^{-7} FP to 100 % FP by generating control signal for adjusting the position of adjuster rods and adding poison to the moderator in order to supplement the worth of adjuster rods [17, 18]. The simplified block diagram of RRS is shown in Fig. 4.29. The RRS has Dual Processor Hot Standby configuration with two systems namely, system-A and system-B. All inputs (analog and digital or contact) are fed to system-A as well as system-B. On failure of system-A or B, Control Transfer Unit (CTU) shall automatically change over the control from System-A to System-B vice versa, if the system to which control is transferred is healthy. Control transfer shall also be possible through manual command by an external switch. This command shall be ineffective if the system, to which control is desired to be transferred, is declared unhealthy. Transfer

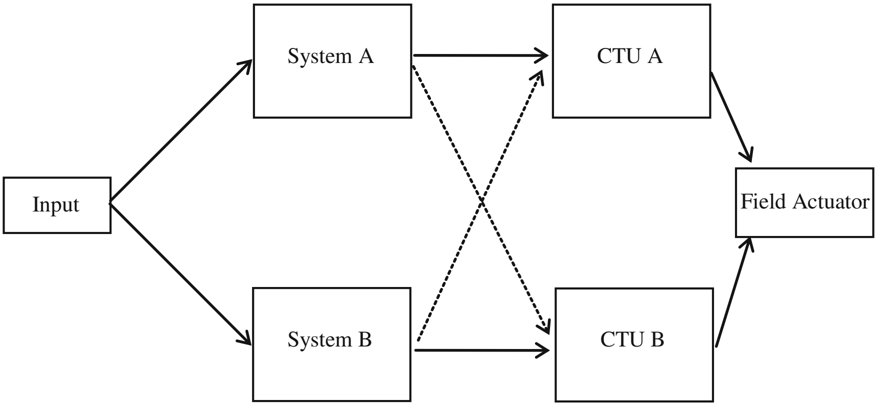


Fig. 4.29 Simplified block diagram of reactor regulator system

logic shall be implemented through CTU. To summarize, the above described computer-based system has failures needs to happen in a specific sequence, to be declared as system failure. Dynamic fault tree is constructed for realistic reliability assessment.

Dynamic Fault Tree Modeling

The important issue that arises in modeling is the dynamic sequence of actions involved in assessing the system failure. The top event for RRS, "Failure of Reactor Regulation", will have following sequence of failures to occur:

1. Computer system A or B fails
2. Transfer of control to hot standby system by automatic mode through relay switching and CTU fails
3. Transfer of control to hot standby system by manual mode through operator intervention and hand switches fails after the failure of auto mode

PAND and SEQ gate are used, as shown in Fig. 4.30, to model these dynamic actions. PAND gate has 2 inputs, namely, Auto Transfer and System A/B failure. Auto transfer failure after the failure of system A/B does not affect as the switching action has already taken place. Sequence gate has 2 inputs, one from PAND gate and another from manual action. Chances of manual failure only arise after the failure of Auto and SYS A/B. Manual Action has four events, in which three are

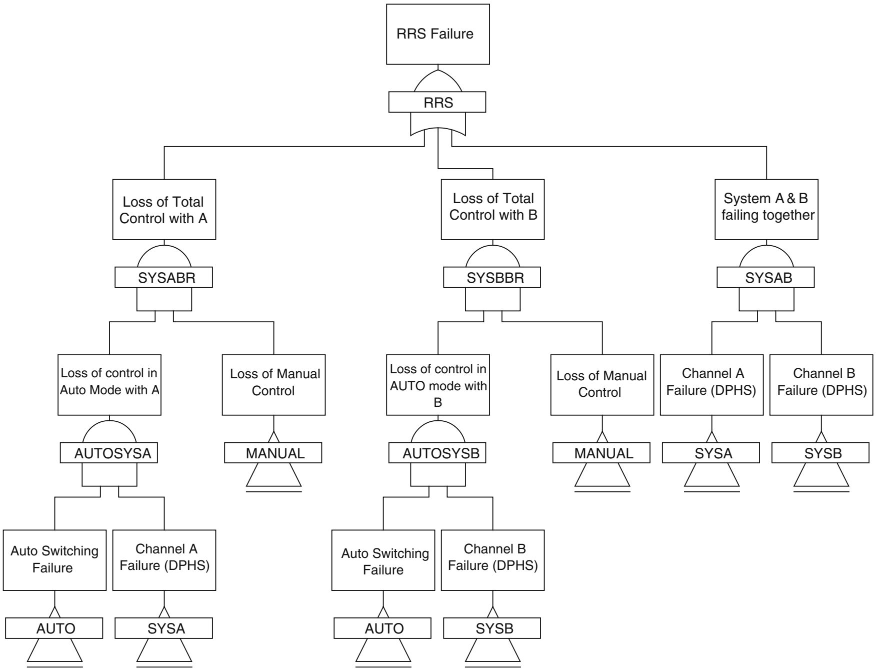


Fig. 4.30 Dynamic fault tree of DPHS-RRS

hand switch failures and one is OE (Operator Error). AUTO has only two events, failure of control transfer unit and failure of relay. System A/B has many basic events and failure of any these basic events will lead to the failure, represented with OR gate.

Exercise Problems

1. Monte Carlo simulation is being run to calculate the reliability of a system. The following observations for failure times (in months) of the system have been reported after 50 random experiments: 24, 18, 12, 10, 60, 40, 11, 36, 9, 13, 5, 12, 30, 15, 48, 1, 12, 3, 15, 31, 56, 75, 10, 25, 15, 12, 20, 3, 45, 24, 33, 50, 9, 12, 42, 18, 6, 13, 11, 25, 4, 14, 24, 8, 50, 75, 10, 2, 15. Determine the current percentage error assuming a normal distribution and 95 % confidence level.
2. Considering the data mentioned in the Problem 1, estimate the number of runs required to obtain 10 % acceptable error in the final results. Also, track the online convergence by plotting the current percentage error and number of runs required with a step of 10 samples.
3. Let us assume a uniform random number generator gives the following 30 random numbers: 0.5, 0.12, 0.30, 0.15, 0.48, 0.1, 0.612, 0.39, 0.95, 0.31, 0.856, 0.75, 0.10, 0.825, 0.915, 0.712, 0.20, 0.63, 0.745, 0.424, 0.533, 0.50, 0.9, 0.712, 0.42, 0.18, 0.6, 0.53, 0.0511. Determine the corresponding failure times for a component having exponential distribution with a failure rate of 1.5 per year.
4. Construct the typical state time diagram for the dynamic fault tree shown in Fig. 4.16. Typical component up and down states, each gate output, and the final top event should be reflected in diagram.
5. Construct the Markov model for RRS shown in Fig. 4.29. Assume different transition rates between various states. Derive the unavailability expression for the failure of RRS.
6. Determine unavailability of control power supply system explained in Chap. 3 using dynamic fault tree analysis. Compare the results with classical fault tree analysis.

References

1. Zio E, Podofillini L, Zille V (2006) A combination of Monte Carlo simulation and cellular automata for computing the availability of complex network systems. Reliab Eng Syst Saf 91:181–190
2. Yanez J, Ormfio T, Vitoriano B (1997) A simulation approach to reliability analysis of weapon systems. Eur J Oper Res 100:216–224
3. Taylor NP, Knight PJ, Ward DJ (2000) A model of the availability of a fusion power plant. Fusion Eng Design 52:363–369
4. Marseguerra M, Zio E (2000) Optimizing maintenance and repair policies via combination of genetic algorithms and Monte Carlo simulation. Reliab Eng Syst Saf 68:69–83

5. Alfares H (1999) A simulation model for determining inspection frequency. Comput Ind Eng 36:685–696
6. Marseguerra M, Zio E (2004) Monte Carlo estimation of the differential importance measure: application to the protection system of a nuclear reactor. Reliab Eng Syst Saf 86:11–24
7. Zio E, Podofillini L, Levitin G (2004) Estimation of the importance measures of multi-state elements by Monte Carlo simulation. Reliab Eng Syst Saf 86:191–204
8. Durga Rao K, Kushwaha HS, Verma AK, Srividya A (2007) Simulation based reliability evaluation of AC power supply system of Indian nuclear power plant. Int J Qual Reliab Manag 24(6):628–642
9. IAEA-TECDOC-593 (1991) Case study on the use of PSA methods: station blackout risk at Millstone unit 3. International Atomic Energy Agency, Vienna
10. IAEA TECDOC 478 (1988) Component reliability data for use in probabilistic safety assessment. International Atomic Energy Agency, Vienna
11. IAEA (1992) Procedure for conducting probabilistic safety assessment of nuclear power plants (level 1). Safety series No. 50-P-4, International Atomic Energy Agency, Vienna
12. Morgan MG, Henrion M (1992) Uncertainty—a guide to dealing uncertainty in quantitative risk and policy analysis. Cambridge University Press, New York
13. Driels MR, Shin YS (2004) Determining the number of iterations for Monte Carlo simulations of weapon effectiveness. Naval Postgraduate School, Monterey
14. Dugan JB, Bavuso SJ, Boyd MA (1992) Dynamic fault-tree for fault-tolerant computer systems. IEEE Trans Reliab 41(3):363–376
15. Amari S, Dill G, Howald E (2003) A new approach to solve dynamic fault trees. In: Annual IEEE reliability and maintainability symposium, pp 374–379
16. Durga Rao K, Gopika V, Sanyasi Rao VVS, Kushwaha HS, Verma AK, Srividya A (2009) Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. Reliab Eng Syst Saf 94:872–883
17. Gopika V, Santosh TV, Saraf RK, Ghosh AK (2008) Integrating safety critical software system in probabilistic safety assessment. Nucl Eng Des 238(9):2392–2399
18. Khobare SK, Shrikhande SV, Chandra U, Govindarajan G (1998) Reliability analysis of microcomputer circuit modules and computer-based control systems important to safety of nuclear power plants. Reliab Eng Syst Saf 59:253–258

Chapter 5
Electronic System Reliability

The dominating failure mechanisms for various electronic components such as resistors, capacitors, relays, silicon devices, etc. and the corresponding failure modes are briefly explained. Also the failure rate prediction methods, namely part count and part-stress methods, are discussed. One case study is also presented. This is based upon the failure rate calculation using MIL-HDBK 217 notice 2 of a circuit used for the electrical isolation between a microprocessor and the actuator. Reliability prediction based on physics of failure mechanisms for resistors, capacitors, metal oxide semiconductor (MOS) devices, and field programmable gate array (FPGA) are also discussed in the chapter.

5.1 Importance of Electronic Industry

As the technology grows day by day, the electronic systems are becoming the core components of almost all the safety critical and process system. Now a day electronic circuits are widely used because of their high accuracy and reduced hardware space. From the transistor to highly sophisticated components like microcircuits, very large scale integrations (VLSIs), field programmable gate arrays (FPGAs) etc., these electronic components provided tremendous flexibility in design. Apart from these qualities, the key utilization of electronic systems is on account of their software control. Microcontrollers and other programmable chips are the backbone of many control systems as they can be programmed accordingly whenever designer wants to change without replacing the actual hardware block. Not only the analog but the digital electronic circuits also have their own advantages. One of the key features of digital circuits is that different circuits can be used in order to deliver the same functionality and hence the designer has advantage in selecting the appropriate design. Most of the times, reliabilities of these designs are used for the selection.

One of the most important and critical use of electronic systems is in developing advanced weapons. This practice of building powerful and precession weapons by the use of electronic systems and there software controls are not new. In fact, they have been in this business from the World War II. Many old systems are also being replaced by newer and better electronic systems. Because of wide applications, it is

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_5

important to have an excellent prediction of failures and reliability of electronic systems. Most electronic systems have huge complex circuit and it is almost impossible for the designer to trace out the faulty spot once the failure has occurred. Usually the failures in electronic system are introduced by high voltage or current stress and wear out. As these systems are quite small in size heating is one of the most dominating factors for the failure. Hence, proper cooling should be made in order to avoid failures as well as to save the component too. Typically, in weapons large heat is produced which can cause a failure to electronic circuitry associated with it.

5.2 Various Components Used and Their Failure Mechanisms

Nowadays, electronic systems have quite large circuits having many components though many of them are of similar type. A lot of new components are also being developed and studies are going on for recognition of their failure mechanisms. Typical electronic circuit has components like resistors, capacitors, inductors, microcircuits (ICs), connectors, switches and others. We will have a brief overview for some of the components and discuss their failure mechanisms.

5.2.1 Resistors

Resistors are the basic components of any electronic circuit. A failure occurred with resistor usually make it an open circuit or a very high resistance is developed across the ends. A failure in resistance can occur due to high current stress or high voltage stress that results in excessive heating of the components and as the heating continues increasing its temperature, there may be a time the temperature gets over the melting point of the material used. This causes the resistor to be fused and hence an open circuit is developed. Fabrication defects and electrostatic discharge also some time causes failure to the components. This may usually make the component noisy. Sometimes instead of an open circuit the parameters of the component also get changed due to above mentioned causes.

5.2.2 Capacitors

Capacitors are used in almost every electronic circuit as a storing component. The failures in capacitor usually make it open circuit except in some cases it gets short circuit after failure as in the case of electrolyte capacitor. If no voltage is applied over a long period, they get short-circuited. High voltage stress is usually the dominating aspect for the failure of capacitors. Some special purpose capacitor, as in the case of electrolyte capacitors it has got polarity so, reversing the polarity may damage the component. Generally, a diode or other protecting circuit is used to save valuable component and to avoid the failures as well.

5.2.3 Inductors

Inductors are also part of many electronic systems. Inductors are very prone to the failure due to excessive current stress. High current may cause the heating of the conductor, which as a result may damage the insulation and causes a failure. In addition, when there is a large variation in current through the inductor the designer should choose proper insulation and conducting material. A diode is used across the ends to protect an inductor which provides a path for the current to flow when the inductor suddenly get out of the circuit.

5.2.4 Relays

Relays are very important parts of any electrical or electronic circuits from the safety point of view. They not only save the system from any damage due to some faulty situation in the system itself or from the outer side but they also take care of the parts, which are not really going to be affected by these faults. Thus, the failure in relay itself may sometime cause vary dangerous situation. Electro-mechanical type relay which are being used for a long time have metal contact which is used to trip the circuit when high current or voltage or any other parameter get out of the tolerance of the circuit. The main failure cause for this type of relay is due to the large heat, which generate excessive power and results in the contact failure. Apart from this as it is a mechanical element as well mechanical failure may also occur if proper handling is not done. Now a days, pure solid-state relays are used which do not have any mechanical contact in there. These types of relays are also sensitive to non-resistive loads, surge currents that may create high junction temperatures that degrade the component.

5.2.5 Semiconductor Devices

Semiconductor devices are always part of a larger, more complex piece of electronic equipment. Semiconductor devices like diode, transistor, MOSFET, solar cells etc. have P-N junctions. For avoiding failure of these components, manufacturers provide failure characteristics for the components, which are determined with the application of stress bias voltages. A semiconductor device generally fails when excessive reverse voltage is applied across the P-N junction, which results in the breakdown of the P-N junction. That is why the peak inverse voltage (PIV) is usually specified for these devices. Like other electronic devices, these components are also very sensitive to the ambient temperature. Heating may produce excessive charge carriers, which results in widening of the depletion region in P-N junction. One of the important failure mechanisms of semiconductor devices is related with the dislocation in silicon such as diffusion, precipitation or photo effects. Experiments have shown that dislocations are usually unavoidable for practical devices. Failure generally caused through doping non-uniformities caused by diffusion enhancement and precipitation of metals at dislocations, which may destroy the P-N junction.

5.2.6 Microcircuits (ICs)

Integrated circuits (ICs) are one of the important elements in any electronic circuit. Fabrication defects in silicon chip are major failure causes for these components. Apart from this, ICs are very prone to failure due to electrostatic discharge (ESD), electro-migration and antenna effect. Electrostatic discharge causes the metal to melt and bond wires to fuse, usually causes an open circuit. To avoid failure due to ESD some assembly protection are used like RIF/EMI design zoning in which sensitive parts are shielded by less sensitive parts and Faraday shielding. Electro-migration causes large current density in the conductors and results in slow wear out. Impact of electrons causes gradual shifting of aluminum atoms (conducting material) from their normal lattice sites, which also give rise to voids between grains. It also increases the resistance of the conductor. Some alloys are being used instead of aluminum as the conducting material in order to reduce this phenomenon. Proper packaging of the silicon chip is also an important issue for the failure due to excessive heating. Most of the times, failure in integrated circuits results in modification of their actual functions. Specially, at high temperature ICs start giving incorrect outputs. Therefore, proper temperature should be maintained for sophisticated electronic circuits.

There are a lot other electronic components, which are also being developed to provide more flexibility in designs. Some of these components are Field Programmable Gate Arrays (FPGAs), Micro-Electro-Mechanical Systems (MEMS), embedded systems and others. The failure mechanisms for these systems and components are being studied and will be discussed later in details.

Table 5.1 summarizes the different failure modes of some of the electronic components discussed above and their failure causes with an estimation of the corresponding probability of the failure modes. Comprehensive list is given in Electronic Reliability Design Handbook [1].

Table 5.1 Failure modes of different electronic components

Component	Failure causes	Failure modes	Probabilities
Resistors			
Fixed	High current or voltage stress	Open circuit	0.31
		Parameter change	0.66
		Short	0.03
Variable resistors	Fabrication defects	Open circuit	0.53
		Erratic output	0.4
		Short	0.07
Capacitors	High voltage stress		
Electrolyte capacitor	Reverse polarity connection	Open circuit	0.35
		Short circuit	0.53
Tantalum capacitor	Temperature may change the capacitance	Excessive leakage	0.1
Ceramic capacitor	Distortion in analog signals	Parameter change	0.02
Inductors	High current stress		
	Weak insulation	Insulation distortion	0.7
	Sudden change in current	Open winding	0.3
Relays Electro-mechanical	Heat generation due to high current during faulty situation	Contact failure	0.75
		Open coil	0.05
		Other	0.25
Semiconductor devices			
Diodes	High current stress	Short circuit	0.1
		Open circuit	0.2
	High reverse voltage	High reverse current	0.7
Transistors	Electrostatic discharge	Low gain	0.2
		Open circuit	0.3
	Dislocation in silicon	Short circuit	0.2
		High leakage collector base	0.3

5.3 Reliability Prediction of Electronic Systems

Many reliability models are available for different electronic components in different handbooks and guides like MIL-HDBK [2], PRISM [3, 4] and others. There are two methods for the estimation of the reliability of electronic systems namely Parts Count Method and Parts stress Method. These methods give more or less the same results only the difference is that they needed different information in determining the reliability of the system. Usually when there is less information available, the

Part Count Method is used i.e. in the initial phase of the designing. Modeling based on both of these methods is available in MIL-HDBK 217F [2]. Part Stress method is used at a later stage of the designing.

5.3.1 Parts Count Method

As mentioned earlier this method requires less number of information and hence used in the initial phase of the designing. This method is as simple as the name says it starts with the counting of the parts, which are going to be used in design. Then based upon the above handbooks a generic failure rate is determined for the component. Then a quality factor is multiplied with the corresponding failure rate, which modifies it to give the failure rate accordingly. The quality factor is an estimation of the quality on the component material and the testing standard against the military standard. As there may be a number of similar components used in an electronic circuit, that number multiplies this modified failure rate. Finally summing up the all failure rate gives the actual failure rate of the system. Apart from the quality factor for specific systems like microelectronic systems, another factor called learning factor is also used for the further modification of the failure rate. The learning factor represents the number of years that a component has been in production. Mathematically the total failure rate for a system based upon the Parts Count method can be expressed as (as given in MIL-HDBK-217F)

$$\lambda_E = \sum_{i=1}^{n} N_i (\lambda_g \pi_Q)_i \tag{5.1}$$

where

λ_E Total equipment failure rate per 10^6 h

λ_g Generic failure rate for the *i*th generic part

π_Q Quality factor of *i*th generic part

N_i Quantity of *i*th generic part

n Number of different generic part categories in the equipment

5.3.2 Parts Stress Method

At a later stage of the designing when the designer has the actual design, this method is used for the reliability estimation of the system. This method requires more number of information such as the detailed parts lists and circuit schematics. These are needed because the stress analysis takes into consideration the electrical and thermal stress that will be experienced by the each component. The mathematical models for the parts stress method are available in MIL-HDBK-217 for each component type, i.e., microelectronics, resistors, capacitors and other electro/mechanical devices. The first approach for the stress analysis method is to find out the base failure rate for the components. The base failure rate is then modified by the different factors, which are the measurement of the environmental conditions and the stresses under which the system has to perform.

For resistors the model given in [2] is as follows:

$$\lambda_p = \lambda_b \pi_T \pi_P \pi_S \pi_Q \pi_E \times 10^{-6}\,\text{Failures/h} \tag{5.2}$$

where,

λ_p Part failure rate
π_T Temperature factor
π_S Power stress factor
π_E Environment factor
λ_b base failure rate
π_P Power factor
π_Q Quality factor

This handbook also provides the default values for the base failure rates for almost all types of resistors. For other factors tables are given which can be used to determine the value according to the given condition also expressions for calculating the factors are also given.

Power factor: $\pi_P = (p.d.)^{0.39}$
where, p.d. = power dissipation.

Power stress factor: It has two expressions for different types of resistors.
$\pi_S = 0.71e^{1.1(S)}$ For fixed film resistors and variable resistors
$0.54e^{2.04(S)}$ For fixed wire wound resistors.
S is the Power stress under which the component is working and is defined as the ratio of the actual power to the rated power.

Temperature factor:

$$\pi_T = 1 \quad \text{At } 25\,^\circ\text{C i.e. at room temperature.}$$

5.4 PRISM

This is a method for reliability prediction developed by the Reliability Analysis Center (RAC) [3, 4]. In the previous method the reliability prediction is estimated using component factor rate and various factor affecting where as this method also take care of the non-component failures such as software failure, poor management etc.

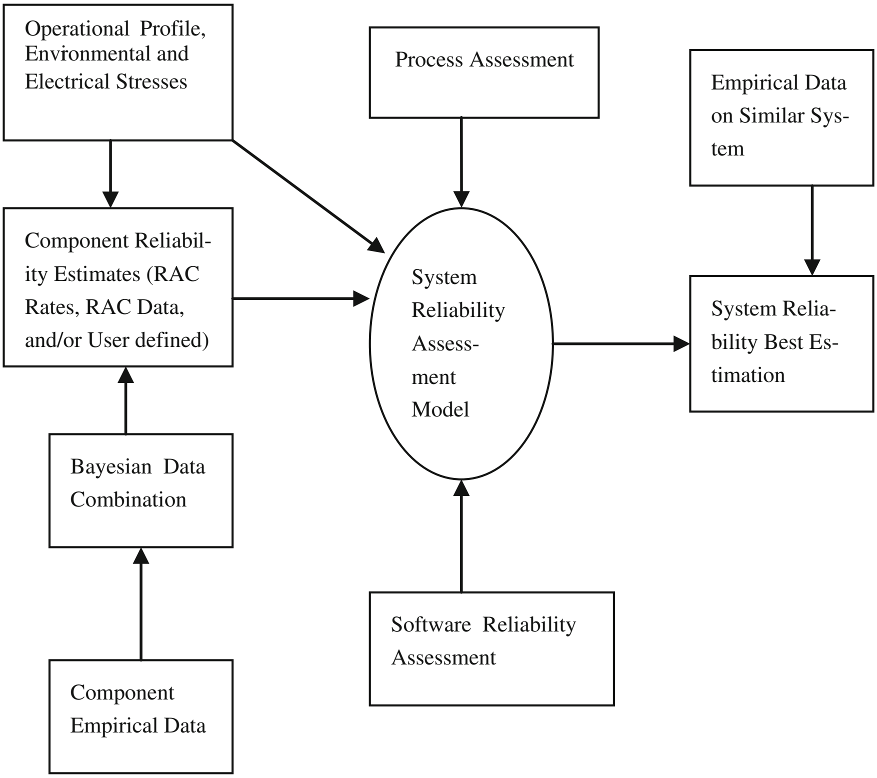

Operational Profile, Environmental and Electrical Stresses
Process Assessment
Empirical Data on Similar System
Component Reliability Estimates (RAC Rates, RAC Data, and/or User defined)
System Reliability Assessment Model
System Reliability Best Estimation
Bayesian Data Combination
Software Reliability Assessment
Component Empirical Data

Fig. 5.1 The PRISM schematics for reliability prediction of electronic systems

In this method, first the initial assessment of the failure rate is made which is given in PRISM models of various components. This method also has software associated with it which provides lots of flexibilities in estimating the reliability of the system at various stages of the design. Figure 5.1 explains the PRISM method for determining the reliability of an electronic system.

The failure rate model for a system in PRISM method is given as

$$\lambda_P = \lambda_{IA}\begin{pmatrix} \pi_P\pi_{IM}\pi_E + \pi_D\pi_G + \pi_M\pi_{IM}\pi_E\pi_G \\ +\pi_S\pi_G + \pi_I + \pi_N + \pi_W \end{pmatrix} + \lambda_{SW} \tag{5.3}$$

where,

λ_{IA} Initial assessment of failure rate
π_{IM} Infant mortality factor
π_D Design process multiplier
π_M Manufacturing process multiplier
π_W Wear out process multiplier
π_S System management process multiplier

λ_{SW}	Software failure rate prediction
π_P	Parts process multiplier
π_E	Environment factor
π_G	Reliability growth factor
π_I	Induced process multiplier
π_N	No-defect process multiplier

The software failure rate is obtained from the capability maturity model (CMM) by the Software engineering Institute (SEI). Other factors are to take care of the process conditions both components related and non-component type.

5.5 Sneak Circuit Analysis (SCA)

This is a kind of different analysis used in reliability prediction of all type of system such as hardware, software or both. This analysis is based upon the identification of sneak paths in the system which inadvertently designed into the system. A sneak path is basically an unwanted path or logic flow in a system which results in the mal functioning of the system.

The followings are the four categories of sneak circuits:

1. *Sneak Paths*: This causes current or logic flow occurs in an unwanted path.
2. *Sneak timing*: This is the case when some event occurs in an undesirable sequence.
3. *Sneak indications*: This causes the false display of the operating conditions which are going to be taken by the operator and ultimately results in a wrong action by the operator.
4. *Sneak labels*: This may mislead the operator by labeling incorrect system function like input, output, power etc.

5.5.1 Definition of SCA

The Sneak Circuit Analysis is the group of different techniques which are used to identify the sneak paths in a system. Based upon the different type of systems followings are three SCA techniques:

1. Sneak Path Analysis
   In this method all the electrical path are investigated in a hardware system. Sneak path analysis is a technique used for identifying the sneak circuits in a hardware system, primarily power distribution, control, switching networks, and analog circuits. The technique is based on known topological similarities of sneak circuits in these types of hardware systems.

2. Digital Sneak Circuit Analysis
   An analysis of digital hardware networks for sneak conditions, operating modes, timing races, logical errors, and inconsistencies. Depending on system complexity, digital SCA may involve the use of sneak path analysis techniques, manual or graphical analysis, computerized logic simulators or computer aided design (CAD) circuit analysis.
3. Software Sneak Path Analysis
   An adaptation of sneak path analysis to computer program logical flows. The technique is used to analyze software logical flows by comparing their topologies to those with known sneak path conditions in them.

5.5.2 Network Tree Production

In order to identify the sneak circuit the actual built (schematics) of the system is required. But this information is not provided by the manufacturer and also the complexity of the actual data makes it very difficult for implementation in practical situation. Therefore the designer needs to convert this information in the usable form which can be analyzed easily. For this conversion software automation is used. Automation has been used in sneak circuit analysis since 1970 as the basic method for tree production from manufacturing detail data. Computer programs have been developed to allow encoding of simple continuities in discrete "from-to" segments extracted from detail schematics and wire lists. The encoding can be accomplished without knowledge of circuit function. The computer connects associated points into paths and collects the paths into node sets. The node sets represent interconnected nodes that make up each circuit. Plotter output of node sets and other reports are generated by the computer to enable the analyst to easily sketch accurate topological trees. The computer reports also provide complete indexing of every component and data point to its associated tree. This feature is especially useful in cross indexing functionally related or interdependent trees, in incorporating changes, and in troubleshooting during operational support.

5.5.3 Topological Pattern Identification

After tree production the next step is to identify the basic topological sneak paths in each tree. There are five basic topological pattern exists:

1. Single line (no node) topograph
2. Ground dome
3. Power dome
4. Combination dome
5. H pattern.

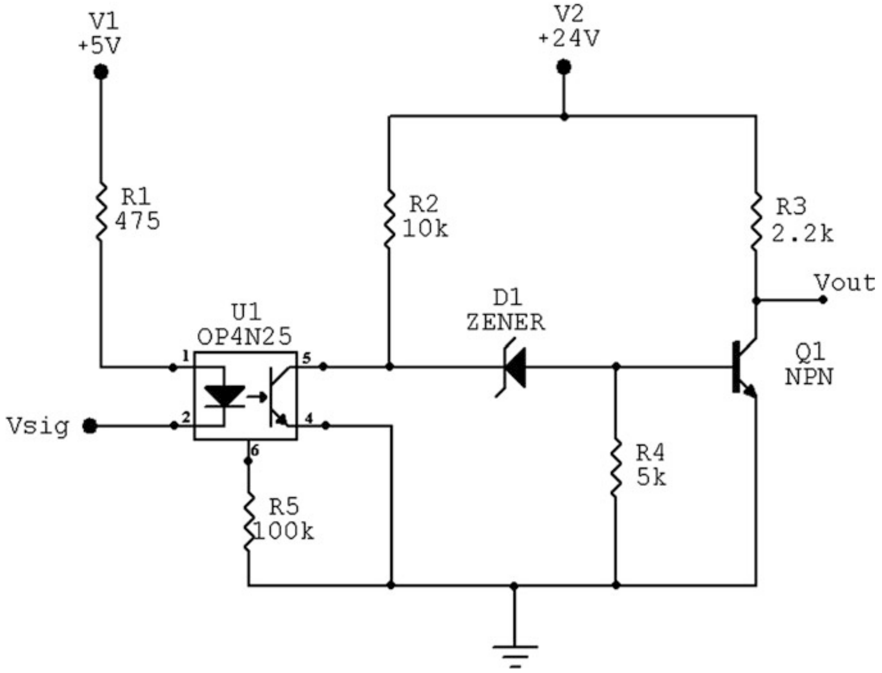


Fig. 5.2 Typical circuit for isolation between the microprocessor and actuator

5.6 Case Study

The circuit shown in Fig. 5.2 is used to make an electrical isolation between the microprocessor and the actuator to avoid any electrical damage to the processor. The circuit consists of an opto-coupler IC 4N25, a bipolar transistor 2N2222, a zener diode and resistors. The circuit generates logic 0 at the output if the signal V_{sig} is at the logic high (at 5 V) and if this is 0 then the output becomes 24 V (logic 1).

To understand the working of the circuit let V_{sig} be at logic high i.e. $V_{sig} = 5\,\text{V}$. The diode (LED) of the opto-coupler will not conduct, as it is not forward biased. This results in the cut-off of the transistor and the collector voltage becomes 24 V, which give rise to the breakdown of the zener diode. As the diode breakdown occurs the transistor becomes saturated and the output becomes 0 (logic 0). In the other case when $V_{sig} = 0\,\text{V}$ the LED starts conducting and the transistor inside the opto-coupler becomes saturated. This makes the collector voltage to become 0 and as no zener diode breakdown can occur in this case the second transistor remains in cut-off state and hence the output in this case is 24 V (logic 1).

The next step for the FMEA analysis is to find out the unsafe modes of failure of the various components. For that, we fail each component in the respected failure mode and simulate the circuit to know whether the particular failure mode results in incorrect output or it has no effect on the overall system.

Circuit has been simulated using OrCaD PSpice 9.0 software and it has been found that the following failure modes result in safe operation of the circuit and all other failure modes give unwanted output. However, in practical situation these failure modes may not be considered as safe mode failures because their failure may damage other components.

1. Short mode failure of resister R1 (475 Ω).
2. Short mode failure of zener diode.
3. Open Mode failure of resister R4 (5 k).

All the failure modes of the various component and their effects on the overall performance are shown in Table 5.2.

Now we will determine the failure rate based upon the MIL-HDBK 217 notice 2. For that, we have to take each component and their respective operating conditions i.e. temperature, power dissipation etc. Table 5.2 also shows the failure rate calculations of various components.

5.6.1 Total Failure Rate

Depending upon the failure mode probabilities of various components, now we will find out the effective failure rate of individual component and summing all the failure rates gives us the total failure rate of the overall system (Table 5.3).

Table 5.2 The Failure mode effect analysis and the failure rate calculations

Component Name	Failure	Modes	Effect	Remarks
	Open	Short	Others	
R1	Unsafe	Safe	–	475, Metal film, 1/8 W, 1 %
R2	Unsafe	Unsafe	–	10 k, Metal film, 1/8 W, 1 %
R3	Unsafe	Unsafe	–	2.2 k, Metal film, 1 W, 1 %
R4	Safe	Unsafe	–	5 k, Metal film, 1/8 W, 1 %
R5	Unsafe	Unsafe	–	100 k, Metal film, 1/8 W, 1 %
DZ	Unsafe	Safe	–	24 V, Zener diode
Q1	Unsafe	Unsafe	–	40 W, bipolar transistor 2N2222
4N25	Unsafe	Unsafe	Unsafe (fail to function)	Optocoupler IC

1. Optoelectronics: $\lambda_p = \lambda_b \pi_T \pi_Q \pi_E$

Component Name	λ_b	Π_T	Π_Q	Π_E	FR (/10^6 h)	Remarks
4N25	0.013	0.083	2.4	1.0	2.59×10^{-3}	Optocoupler, Power dissipation = 0.95mW $\theta_{JC} = 70$ ˚C/W

(continued)

Table 5.2 (continued)

2. Resistors: $\lambda_p = \lambda_b \pi_T \pi_P \pi_S \pi_Q \pi_E$

Component Name	λ_b	Π_T	Π_P	Π_S	Π_Q	Π_E	FR (/ 10^6 h)	Remarks Power dissipation

2. Resistors: $\lambda_p = \lambda_b \pi_T \pi_P \pi_S \pi_Q \pi_E$

Component Name	λ_b	Π_T	Π_P	Π_S	Π_Q	Π_E	FR (/ 10^6 h)	Remarks Power dissipation
R1	0.0037	1.0	0.26	0.936	3.0	1.0	2.7e-3	31.5 mW
R2	0.0037	1.0	0.354	1.162	3.0	1.0	4.56e-3	56.02 mW
R3	0.0037	1.0	0.592	0.946	3.0	1.0	6.21e-3	261 mW
R4	0.0037	1.0	0.028	0.711	3.0	1.0	2.21e-4	0.11 mW
R5	0.0037	1.0	0.0082	0.710	3.0	1.0	6.3e-5	4.59 μW

3. Zener Diode: $\lambda_p = \lambda_b \pi_T \pi_S \pi_C \pi_Q \pi_E$

Component Name	λ_b	Π_T	Π_S	Π_C	Π_Q	Π_E	FR (/ 10^6 h)	Remarks
SOT23	0.002	1.42	1.0	1.0	2.4	1.0	6.826e-3	24 V, Power diss = 8.49 mW θ_{JC} = 70 C/W Case temp = 35 °C

4. Transistor: $\lambda_p = \lambda_b \pi_T \pi_A \pi_R \pi_S \pi_Q \pi_E$

Component Name	λ_b	Π_T	Π_A	Π_R	Π_S	Π_Q	Π_E	FR (/ 10^6 h)	Remarks
NPN—Transistor 2N2222	7.4e-4	1.0	0.7	3.6	0.199	2.4	1.0	3.9e-4	Switching application

Table 5.3 Failure rate of components

Component name	Failure mode (unsafe)	FR (/10^6 h)	Probability	Effective FR (/10^6 h)
R1	Open	2.7e-3	0.59	1.5e-3
R2	Open + Short	4.56e-3	0.74	3.37e-3
R3	Open + Short	6.21e-3	0.74	4.59e-3
R4	Short	2.21e-4	0.05	1.1e-3
R5	Open + Short	6.3e-5	0.74	4.66e-5
DZ	Open	6.826e-3	0.18	1.23e-3
Q1	All	3.9e-4	1.0	3.9e-4
4N25	All	2.59e-3	1.0	2.59e-3

Hence the Total Failure Rate = Sum of the Failure Rates of all the components = 0.0148/10^6 h

5.7 Physics of Failure Mechanisms of Electronic Components

5.7.1 Physics of Failures

The physics-of-failure approach proactively incorporates reliability into the design process by establishing a scientific basis for evaluating new materials, structures and electronics technologies. Information to plan tests and screens and to determine electrical and thermo-mechanical stress margins are identified by the approach. Physics of failure encourages innovative, cost-effective design through the use of realistic reliability assessment. Generic failure models are used by physics of failure, which are as effective for new materials and structures as they are for existing designs.

A central feature of the physics-of-failure approach is that reliability modeling, which is used for the detailed design of electronic equipment, is based on root-cause failure processes or mechanisms. These failure-mechanism models explicitly address the design parameters which have been found to influence hardware reliability strongly, including material properties, defects and electrical, chemical, thermal and mechanical stresses. The goal is to keep the modeling in a particular application as simple as possible without losing the cause-effect relationships, which benefits corrective action.

Some basic electronic components and associated failure mechanisms are discussed in the following section.

5.7.2 Failure Mechanisms for Resistors

5.7.2.1 Failure Due to Excessive Heating

High power dissipation is the general cause for resistor failure. If the current exceeds from a certain specified value the temperature of the conducting material gets over the melting point and this gives rise to an open mode failure.

Let the current be I and the resistance be R then the electrical power will be I^2R. This electrical power may raise the temperature until some steady state value is achieved and also heat transfer may occur due to the temperature difference between the resistor and the surrounding. Assuming the surrounding temperature constant and using the Stefan-Boltzmann equation we have (assuming no heat lose due to conduction and convection),

$$I^2R = e\sigma A(T^4 - T_0^4) + ms\frac{dT}{dt} \tag{5.4}$$

where,

e	Emissivity of the surface
σ	Stefan Boltzmann constant = 5.67 × 10^{-8} J/(s m^2 K^4)
A	Area
T	Temperature of the resistance
T_o	Temperature of the surrounding
m	Mass
s	Specific heat capacity

In order to find the maximum current without failure the temperature at steady state should be less than T_m.

$$I_{\max}^2 R = e\sigma A(T_{\mathrm{m}}^4 - T_0^4).$$

or

$$I_{\max} = \sqrt{\frac{e\sigma A(T_m^4 - T_o^4)}{R}} \tag{5.5}$$

5.7.2.2 Failure Due to Metal Diffusion and Oxidation

In thin film resistors, the metal slowly diffuses and gets oxidized and results in increasing resistance value. The metal oxide film follows parabolic equation with time [5],

$$x^2 = At + B.$$

A is a temperature dependent constant which is proportional to the diffusion coefficient and B is the square of the thickness at time t = 0 i.e. $x_0 = \sqrt{B}$.

Hence the conductance at time t = 0:

$$C_0 = \rho(l - x_0) = \rho(l - \sqrt{B}).$$

At time t:

$$C = \rho(l - x) = \rho(l - \sqrt{At + B}).$$

Percentage change in conductance,

$$\frac{\Delta C}{C_0} = \frac{\sqrt{B} - \sqrt{At + B}}{l - \sqrt{B}} \tag{5.6}$$

By Assigning required error we can find out what will the time of failure.

5.7.3 Failure Mechanisms for Capacitor

5.7.3.1 Dielectric Breakdown

In capacitor when the electric field exceeds certain value in the dielectric material it may breakdown and results in the open circuit.

Capacitors have small series resistance let it be r and the capacitance is C. Let a battery of emf E is applied across the capacitor for charging it.

We know that the capacitor will get charged exponentially and the potential difference across the capacitor plates (assuming parallel plate capacitor) will be

$$V_C = E(1 - e^{-t/rC}) \tag{5.7}$$

Hence the electric field in the dielectric if the distance between the plates is d will be

$$\zeta = \frac{V_C}{d} \tag{5.8}$$

$$\zeta = \frac{E}{d}(1 - e^{-t/rC}).$$

If the breakdown E.F. for the dielectric is ζ_B then we have

$$\zeta_B = \frac{E}{d}(1 - e^{-t/rC}) \tag{5.9}$$

From where we get the time to failure as

$$t = rC\ln\left(\frac{E}{E - \zeta_B d}\right) \tag{5.10}$$

This Breakdown failure generally does not occur as the designer takes care of the voltage applied across the capacitor. However there may be fluctuation in the voltage which may cause this failure.

5.7.4 MOS Failure Mechanisms

The dominating failure mechanisms for these devices are [6]:

1. Electro migration.
2. Time Dependent Dielectric Breakdown-TDDB.
3. HOT carrier injection.
4. Negative bias temperature instability.

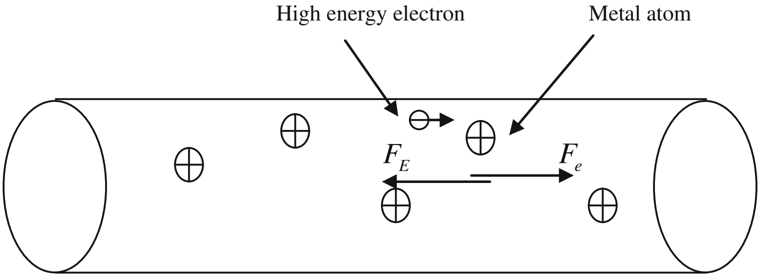


Fig. 5.3 Electro-migration, F_E = Force due to Electric field. F_e = Force due to Electron collision

5.7.4.1 Electro Migration (EM)

Electro-migration is the transport of material caused by the gradual movement of the ions in a conductor due to the momentum transfer between conducting electrons and diffusing metal atoms (Fig. 5.3). The effect is important in applications where high direct current densities are used, such as in microelectronics and related structures. As the structure size in electronics such as integrated circuits (ICs) decreases, the practical significance of this effect increases.

The electro-migration mainly reduces the conductance due to the creation of voids in the conductor by shifting of metal atoms towards the edges. This happens in case of high current density which causes the high impact collision of electrons with the positively charged atoms. When the force due to the strike exceeds the electrostatic force on the atoms they start moving towards the anode.

The EM activation energy is the energies of electrons at which electro migration occurs. This depends on the material of the conductor.

Black developed an empirical model to estimate the MTTF (mean time to failure) of a wire, taking electro-migration into consideration [7]:

$$MTTF = AJ^{-n}e^{Ea/KT} \tag{5.11}$$

This equation is known as Black's equation. J is the current density and A is a material dependent constant and also depends on the geometry. The variable n is a scaling factor which set to 2 according to Black.

5.7.4.2 Time Dependent Dielectric Breakdown

Time dependent dielectric breakdown (TDDB), also known as oxide breakdown, is a source of significant reliability concern. When a sufficiently high electric field is applied across the dielectric gate of a transistor, continued degradation of the material results in the formation of conductive paths, which may short the anode and cathode. This process will be accelerated as the thickness of the gate oxide decreases with continued device down-scaling.

It's a two stage process:

1. Oxide damaged by the localized hole and bulk electron trapping within it and at its interfaces.
2. The increasing density of traps within the oxide forms a percolation (conduction) path through the oxide.

The short circuit between the substrate and gate electrode results in oxide failure. This process has been successfully modeled using Monte Carlo simulations. Trap generation is the key factor determining oxide degradation and breakdown. Three general models are discussed in the literature for trap generation.

AHI (Anode Hole Injection)

The AHI model (1/E model) was proposed by Schuegraf and Hu [8]. This is based on the impact ionization event due to electron injection from gate metal cathode into the oxide. Holes are generated in this process and some holes tunnel back into the cathode and create electron traps in the oxide. The physics of the trap creation process is still speculative [6].

There have been contradicting opinions on the exact field acceleration law of time-to-breakdown—t_{BD}. According to the AHI model (1/E model) the field dependence of the t_{BD} takes the form:

$$t_{BD} = \tau_o e^{G/Eox} \tag{5.12}$$

where E_{ox} = the electric field across the dielectric and τ_0 and G are constants.

Thermo-Chemical Model

This is also known as E model. McPherson and Mogul reviewed the development of this model and proposed a physical explanation. This model proposes that the defect generation is a field driven process. This happens when joule heating occurs due to the formation of sub-band by dipole action under the applied electric field.

According to the thermo-chemical model (E model) the field dependence of the t_{BD} is of the form [6]:

$$t_{BD} = \tau_o e^{-\gamma Eox} \tag{5.13}$$

where τ_0 and γ are constants.

Anode Hydrogen Release (AHR)

In this process H^+ is released at the time of hole generation which diffuses through the oxide. This may trap the electrons.

Additionally, there is evidence that the temperature dependence of ultra-thin oxides is non-Arrhenius, but rather the temperature acceleration factor is larger at higher temperatures. To account for these observations, Wu has proposed a relationship in the form of [9]

$$MTTF = T_{BDO}(V)e^{a(V)/T+b(V)/T^2} \tag{5.14}$$

where T_{BDO}, a and b are temperature dependent constant.

5.7.4.3 Hot Carrier Injection

Hot carriers in the semiconductor device are the cause of a distinct wear out mechanism, the hot carrier injection (HCI). When the source-drain current gets very high and exceeds the lattice temperature hot carriers are produced. Hot carriers have high energy and can be injected into the gate oxide.

Rate of hot carrier injection is directly related to the channel length, oxide thickness and operating voltage of the device. In nMOS hot electrons are produced while in pMOS hot holes are produced. This may cause the electrons or holes trapping.

The failure rate is according to Hu [10]:

$$\lambda = B \cdot i_{drain} \cdot \left(i_{sub}/i_{drain}\right)^m \tag{5.15}$$

The MTTF is modeled as Arrhenius Equation.

N-Channel model: The N-Channel model is for nMOS devices. In these devices the substrate current is an indicator of hot carriers. The MTTF equation is

$$MTTF = B \cdot i_{sub}^{-N} \cdot e^{Ea/kT} \tag{5.16}$$

where B is a scale factor and i_{sub} is the substrate current.

P-channel model: The P-Channel model is for pMOS devices. In pMOS devices, hot holes do not show up as substrate current. However, the gate current can serve as an indicator of hot carriers.

$$MTTF = B \cdot i_{gate}^{-M} \cdot e^{Ea/kT} \tag{5.17}$$

i_{gate} is the peak gate current. Both M and N are between 2 to 4.

5.7.4.4 Negative Bias Temperature Instability

NBTI is caused because of the hole trapped within the interface between the SiO_2 gate insulator and the Si substrate. It happens in pMOS where holes are thermally activated. NBTI decreases absolute drain current I_{Dsat} and transconductance g_m and increases the absolute off current the threshold voltage V_{th}.

The threshold is given by the expression:

$$V_{th} = V_{FB} - 2\phi_F - \frac{|Q_B|}{C_{ox}} \tag{5.18}$$

where V_{FB} is the Flat-band voltage which is given by

$$V_{FB} = \phi_{MS} - \frac{Q_f}{C_{ox}} - \frac{Q_{it}(\phi_s)}{C_{ox}} \tag{5.19}$$

where Q_f is the fixed oxide charge and Q_{it} is the interface trapped charge.

From these equation we get,

$$\Delta V_{th} = -\frac{\Delta Q_f}{C_{ox}} - \frac{\Delta Q_{it}(\phi_s)}{C_{ox}} \tag{5.20}$$

During the NBTI degradation, the threshold voltage shifts to more negative direction, affecting either the interface traps or the fixed oxide charges.

5.7.5 Field Programmable Gate Array

Different FPGA models based upon the configurations of tiles and CLBs (complex logic blocks) [11]:

5.7.5.1 Hierarchical Model

This model has two levels: (a) Tiles and (b) CLBs.

The FPGA is operational if not more than g (= the number of spare tiles) tiles fails. Hence,

$$R_{ov} = \sum_{i=0}^{g} {}^{m}C_i (1 - R_{tile})^i R_{tile}^{m-i} \tag{5.21}$$

m = The total number of tiles

where R_{tile} is the reliability or the probability that tile is working fine which can be determined as

$$R_{tile} = \sum_{i=0}^{n} {}^{l}C_i (1 - R_{CLB})^i R_{CLB}^{l-i} \tag{5.22}$$

n the totlal number of spare CLBs per tile

l the total number of CBLs in one tile

5.7.5.2 Optimal Model

In this configuration CLB plays the basic role. A faulty CLB can be replaced by the spare one.

So if we have M columns and rows the number of CLBs will be M^2. If there are N number of spare CLBs then the reliability on overall system can be determined by

$$R_{ov} = \sum_{i=0}^{N} {}^{M^2}C_i (1 - R_{CLB})^i R_{CLB}^{M^2-i} \tag{5.23}$$

5.7.5.3 Coarse Model

In this configuration only tiles can be replaced. So the overall reliability is determined by

$$R_{ov} = \sum_{i=0}^{g} {}^{M^2}C_i (1 - R_{tile})^i R_{tile}^{M^2-i} \tag{5.24}$$

where g = the spare number of tiles.

5.7.5.4 Tile Based Model

In this model all the tiles should be working and each tile has n number of spare CLBs.

So the reliability that all the tiles are working fine if there is k numbers of tiles:

$$R_{ov} = \prod_{i}^{k} R_{tile} = R_{tile}^{k} \tag{5.25}$$

Again the probability that a tile works fine if total number of CLBs per tile is l.

$$R_{tile} = \sum_{i=0}^{n} {}^{l}C_i (1 - R_{CLB})^i R_{CLB}^{l-i} \tag{5.26}$$

References

1. DOD (1998) Electronic reliability design handbook. MIL-HDBK-338B. Department of Defense, US, Washington, DC
2. DOD (1995) Reliability prediction of electronic equipment. MIL-HDBK 217 notice 2. Department of Defense, Washington, DC
3. 217Plus™ (1999) System reliability assessment software tool. Reliability Information Analysis Center (RIAC)
4. FIDES Guide (2004) Issue A, reliability methodology for electronic systems
5. Lewis CW, Bohmn JJ Physics of resistor failure. International Resistance Company, Philadelphia 8, Pennsylvania
6. Bernstein JB, Gurfinkel M, Li X, Walters J, Shapira Y, Talmor M (2006) Electronic circuit reliability modeling. Micro Electr Reliab 46:1957–1979
7. Haythornthwaite R (2000) Failure mechanisms in semiconductor memory circuits. In: 8th IEEE international workshop on memory technology, design, and testing (MTDT 2000), 7–8 Aug 2000. IEEE Computer Society, San Jose
8. Schuegraf KF, Hu C (1994) Hole injection SiO_2 breakdown model for very low voltage lifetime extrapolation. IEEE Trans Electron Dev 41:761–767
9. Wu E, Suné J, Nowak E, McKenna J, Harmon D (2002) Interplay of voltage and temperature acceleration of oxide breakdown for ultra-thin gate oxides. Solid-State Electron 46:1787–1798
10. Hu C, Tam SC, Hsu FC, Ko PK, Chan TY, Terrill KW (1985) Hot-carrier induced MOSFET degradation—model, monitor, and improvement. IEEE Trans Electron Dev 32:375–384
11. Pontarelli S, Ottavi M, Vankamamidi V, Salsano A, Lombardi F (2006) Reliability evaluation of repairable/reconfigurable FPGAs. In: Proceedings of the 21st IEEE international symposium on defect and fault-tolerance in VLSI systems (DFT'06). IEEE Press, New York

Chapter 6
Software Reliability

6.1 Introduction to Software Reliability

Since the early days of computers, keeping bugs out of the software has been a concern. Over the years, the reliability of the hardware and software has increased dramatically. Even with this dramatic increase, reliability has not kept up with the increase in complexity and the importance the customer places on it. Now that everything we do seem to depend on some type of computer and its software—from the life-sustaining devices in hospitals to the airplanes and satellites to the cars we travel, to the house hold items we use—more reliable software has become an economic necessity.

The proliferation of computers has also generated more and more novice users. Software must be more robust to withstand the onslaught of these novices. Software reliability engineering is the focus of practical technology transfer efforts in many organizations with advanced software processes. Many companies are adapting software reliability as a part of their process. Software Reliability Engineering is adapted as best practice by AT&T way back in 1991. Many organizations like NASA, Lockheed are practicing it extensively. It is also being used in many industries like aerospace industry, automobile, networking etc. This increased interest in software reliability engineering is driven by the expectations that adaptation of adequate Software reliability engineering technology will increase the competitiveness of a project or the organization.

IEEE defines software reliability as "the probability that a system will not cause a system failure for a specified time under specified conditions. The probability is a function of inputs to, and use of, the system as well as function of the existence of faults in the software. The inputs to the system determine whether existing faults, if any encountered" [1].

The benefits of focusing software reliability are

- Improvement in satisfaction of customer needs
- Better resource control
- Better schedule control

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_6

- Increased productivity
- Improvement in systematic completion of project.
- reducing the incidence of customer reported problems, maintenance problems, and maintenance costs

Examples of organizations that are using, experimenting with or researching software reliability engineering are

- Alcatel used reliability prediction for the development of Alcatel 1000 S12 switching software [2]
- AT&T used incremental development and operational-profile, statistical testing in development of PBX which resulted in increase in customer satisfaction with product quality and a decrease in development and testing costs and intervals [3]. It also applied software reliability engineering (SRE) technology to telecommunications network operations systems which are crucial to AT&T's backbone telecommunications transport network. Key steps followed for applying SRE are: deriving an operational profile, developing a simulator test environment, and executing load, stress and stability tests. SRE program also incorporated customer-focused techniques such as operational scenario testing [4]
- Microsoft's Software Reliability Research group works on problems like how program analysis, program verification and software measurement techniques can be used to improve the quality of software. They have developed tools like CHESS (a tool for finding concurrency errors in systems software), HAVOC (a tool for specifying and checking properties of systems software) and focusing on areas like Empirical Software Engineering [5]
- NASA The Software Assurance Technology Center at the NASA Goddard Space Flight Center using software reliability modeling extensively [6]

Other organizations using software reliability are

- Motorola
- US army
- Toshiba
- Lucent
- Hewlett-Packard
- Hitachi
- IBM corporation

6.2 Past Incidences of Software Failures in Safety Critical Systems

The role of software has changed from simply generating financial or mechanical data to monitoring and controlling equipments that directly affects human life, reliability and safety. Due to this we need to prevent the failure of the system to prevent the loss of human life. To achieve the safety objectives of the software and to achieve the desired reliability, a thorough understanding and familiarity with the specialized assessment techniques are needed. In order to highlight the need for reliable software, a brief description of three most published software failures are described below.

Therac 25 Failure

The Therac-25 was a radiation therapy machine produced by Atomic Energy of Canada Limited (AECL) and CGR MeV of France. Between 1985 and 1987, it was involved with at least six accidents in which patients were given massive overdoses of radiation, approximately 100 times the intended dose. Out of six, three of the patients died. These accidents highlighted the dangers of software control of safety-critical systems.

The machine offered two modes of Radiation therapy:

1. Direct electron-beam therapy, for delivering low doses of high-energy (5–25 MeV) electrons over short periods of time;
2. Megavolt X-ray therapy, for delivering X-rays produced by colliding high-energy (25 MeV) electrons into a “target”.

While operating in direct electron-beam therapy mode, a low-powered electron beam was emitted directly from the machine, then spread to safe concentration using scanning magnets. While operating in megavolt X-ray mode, the machine was designed to rotate four components into the path of the electron beam: a target, which converted the electron beam into X-rays; a flattening filter, which spread the beam out over a larger area; a set of movable blocks (also called a collimator), which shaped the X-ray beam; and an X-ray ion chamber, which measured the strength of the beam.

Some of the features of the Therac-25 are necessary to review in relation with the accidents. The Therac-25 was designed to be completely computer controlled, whereas the previous versions were linked to other machines. Another feature was that the safety controlling was the responsibility of the software whereas, the previous versions had separate pieces of machinery and hardware to monitor safety factors. The designers believed that by using only software safety control, they could save time and money in the Therac-25. Some of the old source code used in the older versions (Therac-6 and Therac-20) was used in Therac-25. A Bug found in Therac-25 was later discovered in Therac-20.

First problem was discovered in May 1986. As a typical feature, Therac-25 allowed to change the parameters during the setup, which takes around 8 s to complete. The bug observed was that though screen shows that the changes has been taken care, sometimes changes were ignored, This has resulted in setting the indicator flag being in the wrong place. During the first accident scenario that happened on May 1986, Operator selected photon by mistake and set up was initiated. Realizing the mistake, the operator changed the energy level within 8 s, but these changes were ignored. The accidents occurred when instead of the intended low power beam, the high-power electron beam was activated without the beam spreader plate rotated into place. The machine's software did not detect this problem, and therefore did not prevent the patient from receiving a potentially lethal dose of radiation. The high-powered X-ray beam struck the patients with approximately 100 times the intended dose of radiation, which was described as "an intense electric shock". Later, three of the injured patients died from radiation poisoning.

In January 1987, the second bug was discovered. As a feature, when turntable not correctly positioned, the software controlled interlock prevents activation of the beam. The problem occurred when interlock failed, allowing beam to be activated. This demonstrates the consequence of replacing all hardware interlocks with relying completely on software interlocks. In safety critical applications, the software interlocks and hardware interlocks should be kept as backup systems.

Poor software engineering practices and building a machine that completely relying on software for safe operation are the basic mistake committed.

Ariane 5 Failure

The maiden flight of the Ariane 5 launcher on 4th June 1996 was a disaster. 40 s after commencement of the flight sequence, the launcher drifted out of the flight path, broke up and exploded. The flight control system of the Ariane 5 calculates the angle and velocities on the basis of information from laser gyros and accelerometers. The data captured by the flight control system is transmitted to the on board computer on Ariane 5 to execute the flight program and to control the equipments. In order to improve the reliability, every system was duplicated and was running in parallel. The accident occurred when the software declared a unit as failure due to a software exception. This software exception was caused when a data conversion of 64-bit floating point data to 16-bit integer values. The floating point data which was converted had a value higher than the maximum value that could be represented by a 16-bit integer.

Patriot Failure

During the Kuwait war, the Patriot missile defense system of United States was widely praised as a savior of war. Government sources and media praised it as a system with near perfect success rate in destroying the scud missiles of Iraq. After the war was over, it was revealed by US army that determined that only 10–24 of more than 80 were successful in intercepting scud missiles.

When the system is in operation, the Patriot system determines whether the target it spotted in air was actually an incoming missile or a false alarm by tracking the target and checking whether it is following the exact path of a ballistic missile. In order to calculate the path, the Patriot uses an internal clock. Since the memory available is limited, the clock value is truncated slightly when stored. Even though this may not cause significant error, the software was written in such a way that the error was compounded over time. The more the Patriot was running, the more the error become. Due to this when the Patriot is running for longer duration, it wrongly calculates the expected position of the incoming missile. Therefore the Patriot determines that the incoming missile is a false alarm and ignores it which resulted in disastrous results.

6.3 The Need for Reliable Software

Past instances of software failures has emphasized the need to develop and use reliable software especially in life critical applications. There are four technical methods applicable to achieve reliable software [7]

(i) Fault prevention: Avoid fault occurrences during design and development through engineering of software specification process, usage of good design methods, enforcement of structured programming and encouragement of writing clear codes. Recently formal methods are widely used to ensure software quality. In formal method approaches, requirement specifications are developed and maintained using mathematically trackable languages and tools.

Another technique is software reuse. Object oriented paradigm is an example. In order to measure the quality of software, various attributes are used such as product and process attributes.

(ii) Fault removal: Software testing techniques are relied upon to remove faults. Another practical fault removal scheme is formal inspection, which is a rigorous process focused on finding faults, correcting faults and verifying the corrections. Formal inspection is carried out by a small group of peers with a vested interest in the work product during pretest phases of the life cycle.

(iii) Fault tolerance, which is the survival attribute of software systems.

(iv) Fault/failure forecasting involves formulation of the fault/failure relationship, an understanding of the operational environment, the establishment of reliability models, the collection of failure data, the applicability of reliability models by tools, the selection of reliability models by tools, the analysis and interpretation of results and the guidance for management decisions. These issues are handled under the umbrella of “Software Reliability”.

A steady progression from functional decomposition to structured analysis and then adoption of object-oriented analysis and sophisticated modeling languages are part of technological advances. Increasingly sophisticated languages have emerged from C, C++ to Java and C# [8]. The libraries that come with each of these languages provide more opportunities for large scale reuse. Concomitant with these improved methodologies and programming languages are software development tools. Enterprise software developers have seen advances in software development environment, configuration management, version control systems and automated testing. There is higher degree of integration among these tools contributing to the success of the software development project. Improvements in people dimension involved equipping human resources with the software engineering concepts, upcoming technologies and software development tools.

6.4 Difference Between Hardware Reliability and Software Reliability

Hardware reliability was first introduced in 1950s to evaluate the probability of success of ballistic rockets [9]. By 1960s, reliability engineering had established itself as an integral part of end user product development in commercial products as well as military applications. Software reliability made its first entry in 1970s, when the presence of software in various applications was bare minimum. Hence the field was not given much attention as hardware reliability. But over the years, a surge if new technology, new structured analysis concepts, new paradigms and new ways of developing software emerged in early 90s and continues to this date. Increased presence of software systems in safety critical application led to an increased attention on software reliability.

There exits considerable difference between software and hardware reliability. Software reliability is different from hardware reliability in the sense that software does not wear out or burn out. The software itself does not fail unless flaws within the software result in a failure in its dependent system. The reliability metric for software is used to describe the probability of the software operating in a given environment within the designed range of input without failure. Hence, software reliability is a function of the input to and use of the system as well as the presence of latent software faults.

Hardware reliability often assumes that the hazard rate (i.e., failure rate per unit time, often shortened to the failure rate) follows the "bathtub" curve, illustrated in Fig. 6.1. Failures occur throughout the item's life cycle; the hazard rate initially is decreasing, then is uniform, and finally is increasing.

Infant mortality is the period that appears after product design and development and finally it is put into use. After that useful life starts. The user is confident that the component will remain in service during this period. The probability that the component will function until useful life period is expressed as the probability of success or the reliability. Failures occurring during this period are assumed to be random, i.e., not due to any specific factor. At the end of the useful life, components begin to exhibit end-of-life failures. Those failures occurring during Period are considered to be due to wear out.

The same "bathtub" curve for hardware reliability strictly does not apply to software since software does not typically wear out. However, if the hardware life cycle is likened to the software development through deployment cycle, the curve can be till useful life period. The equivalence to infant mortality of hardware is the debug phase in software. Coding errors (more specifically, errors found and corrected) or operation not in compliance with the requirements specification are identified and resolved. Similarly, the useful life period corresponds to the initial deployment (distribution) time. Failures occurring during that period are found either by users or through post deployment testing. For these errors, work-around or subsequent releases typically are issued (but not necessarily in direct correspondence to each error reported). Failures reported after deployment may be the basis

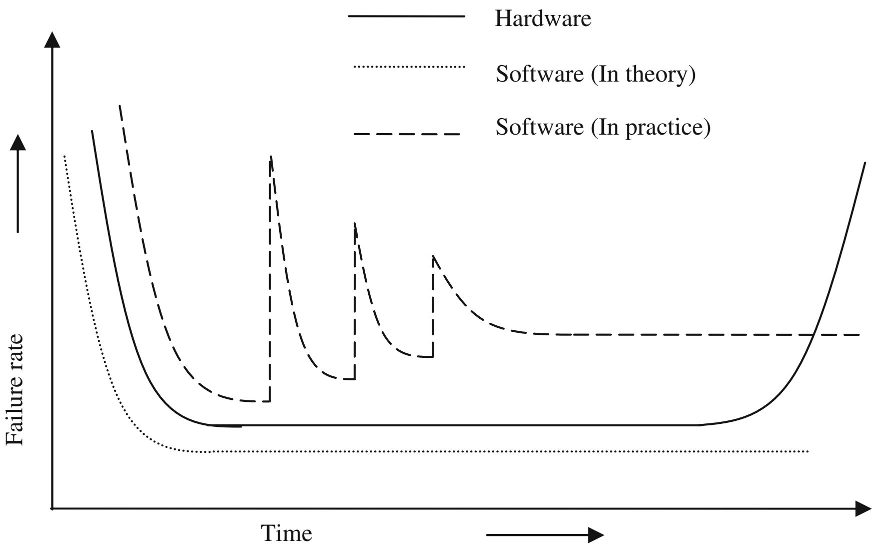


Fig. 6.1 Comparison of hardware and software bathtub curves

for generating the requirements for a new system or commonly referred to as upgrades. Since each upgrade represents a mini development cycle, modifications may introduce new defects in other parts of the software unrelated to the modification itself. Ideally, the bathtub curve for software should look like the "software in theory". Software upgrades may introduce errors, which is depicted as spikes in the useful life period in "Software in practice". The wear out period in software is the obsolescence of the software. With this, the software reaches the end of its useful life. Table 6.1 gives summary of comparison between hardware and software reliability.

6.5 Software Reliability Modeling

Software Reliability Engineering includes

- Software reliability measurement, which includes estimation and prediction, with the help of software reliability models (Fig. 6.2).
- The attributes and metrics of product design, development process, system architecture, software operational environment, and their implication on reliability.
- The application of this knowledge in specifying and guiding system software architecture, development, testing, acquisition, use and maintenance.

Table 6.1 Comparison between hardware and software

Phenomenon	Hardware	Software
Failure rate dependence on age	Failures can depend on time dependent mechanisms such as burn-in or wear out, which may be preceded with warnings at times	The age of the software has nothing to do with its failure rate. If the software has worked in the past, it will work in the future, everything else remaining the same (i.e., no hardware, software or interface changes). Software does not rust or exhibit other hardware wear out mechanisms
Repeated usage	Physical parts wear from usage, resulting in failure	The frequency of software use does not influence software reliability. The same software can be used over and over and, if it did not fail the first time, it will not fail any other time in identical usage (same range of inputs with no hardware, software or interface changes)
Inspection	Various non destructive methods are available for inspecting hardware	Software cannot be judged prior to use by the same methods as hardware
Definition of success and failed state	Hardware will either work or not in a given application	Software, aside from total failure, has varying degrees of success according to its complexity and functionality

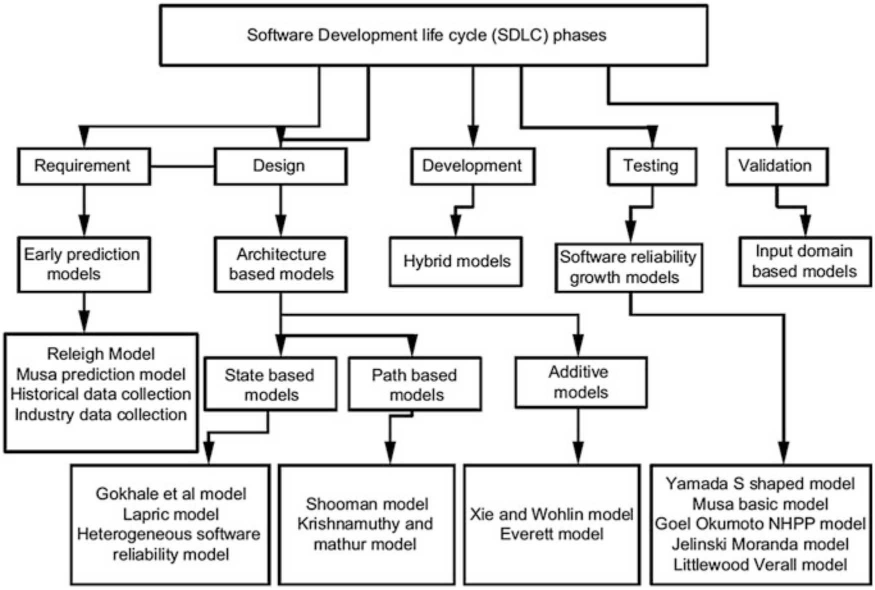


Fig. 6.2 Different models used in different phases of software life cycle [10]

6.5.1 Software Reliability Growth Models

In the software development process, a product may have many design defects, i.e. faults, or popularly known as bugs. For a certain input to the software these faults are activated, resulting in a deviation from its specified behavior i.e. a failure. Once failures are detected through the testing process and the corresponding fault(s) are located, then assuming that these faults are perfectly fixed, i.e. the process of fixing a fault did not introduce a new fault, software reliability increases. If the failure data is recorded either in terms of number of failures observed per given time period or in terms of the time between failures, statistical models can be used to identify the trend in the recorded data, reflecting the growth in reliability. Such models are known as software reliability growth models or growth models in general. They are used to, both, predict and estimate software reliability.

There are basically two types of models: black box software reliability models and white box software reliability models. A brief summary about these models is given below.

6.5.2 Black Box Software Reliability Models

All software reliability growth models are of the black box type since they only consider failure data, or metrics that are gathered if testing data are not available. Black box models do not consider the internal structure of the software in reliability estimation and are called as such because they consider software as a monolithic entity, a black box.

Black box models can be classified into

- *Failure rate models* Failure rate models which try to capture how the failure rate changes as more faults are detected and corrected. The estimations are based on the failure data which is collected during testing phase.
- *Error seeding models* Error seeding models introduces errors to software and tests are performed on that. While testing both inherent and induced errors will be discovered. Estimation of the total number of inherent errors in the software is determined using the ratio of inherent and induced errors detected and the total number of induced
- *Curve fitting models* Curve fitting models use statistical regression method to study the relationship between software complexity and the number of errors in the program, the number of changes and the failure rates, etc.
- *Bayesian model* This model uses Bayesian framework to determine the reliability growth and prediction. In this both subjective expert judgments and objective experimental results can be included into one model.

Some of the major black box models

- The Jelinski-Moranda Model [11]
- The Goel-Okumoto Model [12]
- Musa's basic execution time model [13]
- Musa-okumoto logarithmic Poisson model [13]
- The enhanced NHPP model [14]
- Littlewood–Verrall Bayesian model [15]

6.5.3 White Box Software Reliability Models

As opposed to black box models which only model the interactions of software with the system within which it operates, white box software reliability models consider the internal structure of the software in the reliability estimation. Black box models are inadequate to be applied to software systems in the context of component-based software, increasing reuse of components and complex interactions between these components in a large software system. White box reliability models consider component reliabilities, in the computation of overall software reliability, and hence give more realistic estimates.

In the white box models, components and modules are identified, with the assumption that modules can be, designed, implemented and tested independently. The failure behavior for these modules is specified in terms of failure rates or reliabilities. The failure behavior is then combined with the architecture to estimate overall software reliability as a function of component reliabilities. Mainly there are three generic classes of white box software reliability models exist: path based models, state based models and additive models.

Most popular white box reliability models are

- Krishnamurthy and Mathur's path based model
- Gokhale et al.'s state based model

6.6 How to Implement Software Reliability

Introduction of software reliability engineering will be a strong function of the software process maturity of that organizations, start up costs may include deployment of system to collect failure, fault and effort, calibration of existing and development of organization specific reliability models and tools, staff training, modification of the organizational culture, modifications in the current processes to suit the above steps, etc. Software reliability engineering to be implemented incrementally, starting with the activities needed to establish a baseline and learn about the product, find out the customer expectations and the constraints that the

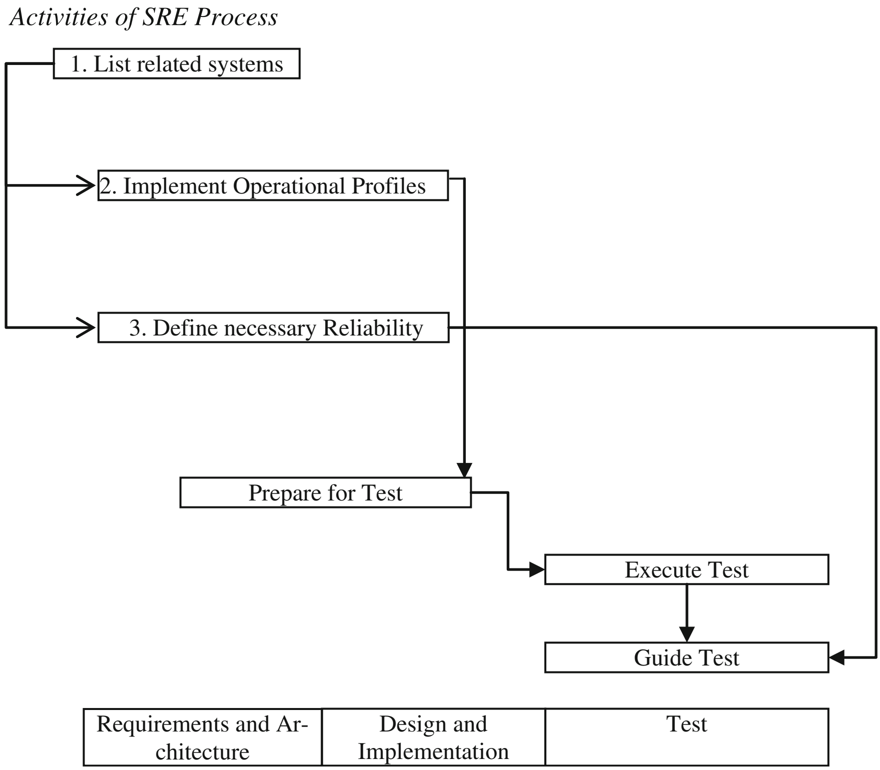

Activities of SRE Process
1. List related systems
2. Implement Operational Profiles
3. Define necessary Reliability
Prepare for Test
Execute Test
Guide Test
Requirements and Architecture
Design and Implementation
Test

Fig. 6.3 Steps in software reliability engineering process [13]

organizational business model imposes on its software production. High maturity organizations like CMMI level 5 organizations; it will be easy to adapt these changes.

The initial effort includes the collection of data, monitoring of reliability growth during system tests, field trails and software operation, and the initial formulation of the operational profiles (Fig. 6.3). This is to be followed by the development of detailed operational profiles, detailed classification of system failures and faults, and development of business—based reliability objectives. More advanced stages include continuous tracking of customer satisfaction, trade off studies, quantitative evaluation of software process capabilities with respect to quality, and proactive process control.

Activities of SRE Process
Example—Operational Profile Model
In the operational profile model, the system is divided into five levels, where each one is more detailed than the parent level, see Fig. 6.4. On every level there exist alternatives that together have a probability of 100 %. The upper most level is called “customer profile”. A customer is a person or institute who obtain the system.

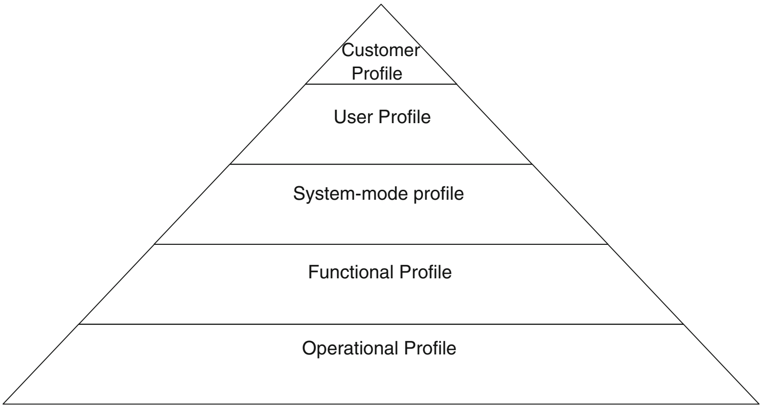


Fig. 6.4 System profiles [13]

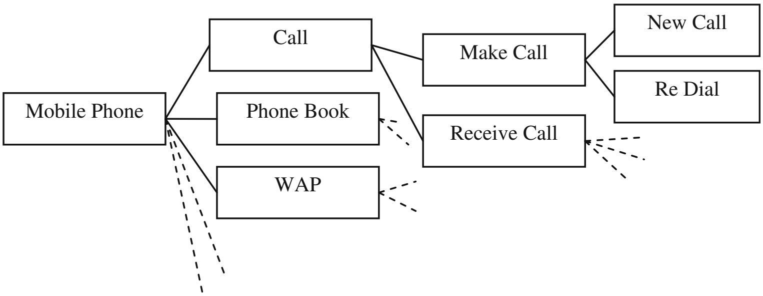


Fig. 6.5 Operational profile model

The next level is the "user profile" which consists of, for example, age groups or different business segments within the chosen customer. The users are the ones that actually employ the system. If the customers are the same as the users, only one of these levels is needed. The next level is the "system-mode profile", which describes the different states of the system. Below the "system-mode profile" is the "functional profile", where all functions available to the user are gathered. On the last level, the "operational profile" contains the operations that implement the functions.

In Fig. 6.5, an example is shown to illustrate the model. The advantages here are that it is fairly simple to achieve a realistic model if sufficient usage information is available and that it can handle large systems. The downside however is, that it does not support the detailed behavior of the user.

Case Study

A software organization is developing software for different mobile phone manufactures. Normal mobile phone software typically consists of many modules like call, phonebook, games, messages etc. Each module contains different sub modules or scenarios, which will be used by the users.

When a normal software application is being tested, normally the test cases are prepared based on the requirements. The main drawback here is that the usages of different requirements are not considered. When the requirements are given to the developers who develop and test the software, the thought process will be mainly from the developer's angle. By this, the complicated or advanced sub modules as per developers' angle will be tested more rigorously. It may also be possible that the user rarely uses these complicated or advanced sub-modules. This creates a possibility that in spite of the software is tested vigorously; the user may find out defects in the very early stage of the usage and may occur very frequently. Hence it was decided that during the integration testing, the software reliability concepts would be used.

Steps Involved
The step by step approach to use the operational profile model is given below.

Step 1. *Determine all possible modules, sub-modules and scenarios*
The mobile phone software contains many sub modules and scenarios. Using the requirements captured from the customer, all the possible scenarios can be captured. It is possible that these scenarios can be triggered at the same time. For example it is possible to receive a call while typing a message. These types of scenarios have to be captured for the foolproof testing.

Step 2. *Create n × n matrix*
Create n × n matrix by arranging all the possible sub-modules as the rows and column headings of the n × n matrix. Then the interception point defines one complex scenario. Find the outcome of the possible combination. An example of n × n matrix is shown in Table 6.2. If the generated scenario is valid then it is numbered as per some naming convention. E.g. all valid scenarios are marked here as T1, T2, T3 etc.
If the generated scenario is valid then it is numbered as per some naming convention. E.g. all valid scenarios are marked here as T1, T2, T3 etc.
It is found that individual scenarios are valid but their combination may not be always valid. For e.g. Trying to run following two scenarios, "Reject Incoming Call" and "Receive Voice Call". In this case, its interception happens to be invalid. Invalid scenarios are marked as "F".

Step 3. *Add the possible scenarios from n × n matrix to the list of scenarios*
After finding out the complex scenarios, add those scenarios to the list of scenarios in step 1.

Step 4. *Assign probability of modules*
The main purpose of this testing is to conduct the testing from users' angle. To do this, the probability of usage for each module is to be captured. Conduct an internal/external survey and decide the probabilities.
Before testing, based on the past experience in the similar software testing, the team decided that the testing time would be 180 min for each iteration (Table 6.3). The time for each sub-module will be derived from this time considering the individual probabilities.

Table 6.2 n × n matrix to find out all scenarios

Modules	Parameters	Make voice call using key pad	Make voice call using call log	Make voice call using phone book	Receive voice call	Reject incoming call	Volume level
Call	Make voice call using key pad	T1	T2	T3	T4	T5	T6
Call	Make voice call using call log	T10	T11	T12	T13	T14	T15
Call	Make voice call using phone book	T19	T20	T21	T22	T23	T24
Call	Receive voice call	T	T	T	T	T	T
Call	Reject incoming call	F	F	F	F	F	F
Call	Volume level	F	F	F	T	T	T
Media player	Playing music file	T	T	T	T	T	T
Media player	Media player function (Rewind, Pause, Forward)	F	F	F	T	T	F
Phone book	Adding contacts (view contact list)	F	F	T	T	T	F
Phone book	Assign ringtone to a contact	F	F	F	T	T	F
Phone book	Deleting contact (view contact details)	F	F	T	T	T	F
Phone book	Editing contact	F	F	T	T	T	F
File browser	Create folder	F	F	F	T	T	F
File browser	Delete folder	F	F	F	T	T	F
Organiser and tools	Creating task	F	F	F	T	T	F
Organiser and tools	Calender-reminder	F	F	F	T	T	F
Phone profile	Normal mode	T	T	T	T	T	T

Table 6.3 Probabilities of modules

Total time: 180 min				
S. no.	Mode	Probability	Cumulative probability	Time
1	Call	0.5	0.5	=180 × 0.5 = 90
2	Media player	0.2	0.7	=180 × 0.2 = 36
3	Phone book	0.1	0.8	=180 × 0.1 = 18
4	File browser	0.1	0.9	=180 × 0.1 = 18
5	Organiser and tools	0.05	0.95	=180 × 0.05 = 9
6	Phone profile	0.05	1	=180 × 0.05 = 9

Cumulative probability is determined by sorting the modules in the descending order of probability and using the formula.

$$\mathit{Cumulative\,probability}_x = \sum_{1}^{x} \mathit{individual\,probability}$$

Step 5. *Assign probability of sub-modules*

Once the probability of modules is determined, the probability of each sub-module inside the module is determined. Conduct an internal/external survey and decide the probabilities.

After finding the probabilities for each sub-module, the probabilities of each module were split again to find out the testing time for each sub module (Table 6.4). Cumulative probability is determined by sorting the sub modules in the descending order of probability and using the formula.

$$\mathit{Cumulative\,probability}_x = \sum_{1}^{x} \mathit{individual\,probability}$$

Step 6. *Assign probability of scenarios*

Once the probability of sub-modules is determined, the probability of each scenario inside the sub-module is determined. Conduct an internal survey and decide the probabilities.

Now, each sub module is split into the valid scenarios. There exist single scenarios as well as combination of scenarios as mentioned above. These valid scenarios are clubbed into the respective sub modules and the probabilities of the respective scenarios are calculated. An example of the scenarios under the sub module receive voice call is given in Table 6.5.

Step 7. *Generate random numbers*

After determining the scenarios and the cumulative probabilities, generate a set of random numbers for module, sub-module and scenario. Conduct the test of the scenario, whose cumulative probability is just above the random number.

For example, Random numbers generated are as in Table 6.6.

Table 6.4 Probabilities of sub modules

Sr no.	Module name (min)	Sub module	Sub module probability	Submodule—cumulative probability	Testing time (min)
1	Call (90)	Receive voice call	0.3	0.3	27
		Make voice call using key pad	0.2	0.5	18
		Make voice call using call log	0.2	0.7	18
		Make voice call using phone book	0.2	0.9	18
		Volume level	0.1	1	9
2	Media player (18)	Playing music file	1	1	18
3	Phone book (36)	Adding contacts (view contact list)	0.5	0.5	18
		Assign ringtone to a contact	0.2	0.7	7.2
		Editing contact	0.2	0.9	7.2
		Deleting contact	0.1	1	1.8
4	File folder (18)	Create folder	0.5	0.5	9

Table 6.5 Scenarios under software sub modules

Module	Sub module	Scenario
Call	Receive voice call	
0.5	0.3	Receive a incoming voice call, and receive another incoming voice call
		Receive a incoming voice call and reject another incoming voice call
		Receive a incoming voice call and make a outgoing voice call through phone book
		Receive a incoming voice call and make a outgoing voice call through call log
		Receive a incoming voice call and make a outgoing voice call by dialling key pad
		Receive a incoming voice call
		Reject a incoming voice call

Table 6.6 Random numbers generated

	Module	Sub-module	Scenario
Random number	0.620	0.227	0.583

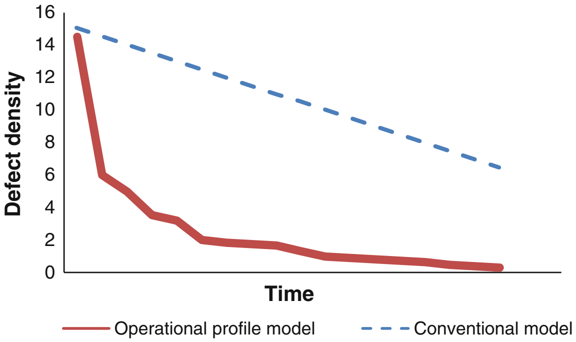


Fig. 6.6 General representation of benefit of operational profile model

For module, the random number is 0.620, this between the cumulative probability of 0.5 and 0.7. Hence the module to be tested is media player whose cumulative probability is 0.7 (Table 6.3). Then select the sub-module of media player, in this case only one.

If there are more than one sub module, use the same method used for module. Repeat the same for scenario and do the testing that the scenario selected by the random number. Repeat the same by generating another set of random number.

Benefits

The benefits of software reliability based testing are more precise satisfaction of customer needs, better effort and schedule control, increase in productivity, more systematic management of project etc.

Many undetected defects during the normal testing were detected in this test. It was observed that the defects, which were leaked to the customer, were reduced drastically. A general graphical representation of the benefit of software reliability based testing is shown in Fig. 6.6.

6.7 Emerging Techniques in Software Reliability Modeling—Soft Computing Technique

Increase in the budgetary allocation towards computerization/up gradation of the existing systems, in almost all the sectors has resulted in an increase in demand for developed software. The statistics of the last few decades show an exponential rise in the demand for developed software. This increase in demand has created a milieu of competition among the software developing organization, to provide high quality software in shorter duration and at lower cost. Considering the increase in demand for software, proper performance prediction in the early stages of the development is a must to sustain in the market. To provide this, software services organizations have adopted various software engineering process models such as capability maturity model (CMM), capability maturity model integration (CMMI), ISO 9001:2000, etc. [16, 17] and practice of the project management concepts defined in the project management body of knowledge [18]. However, as per the data published by Standish group [19, 20], one cannot find any significant change in project success rate over the last one-decade, even though there is an increase in percentage of successful projects. It shows that while the percentage of challenged projects (the project is completed and operational, but over budget, over the time estimate and fewer features and functions than initially specified) reduced significantly from 40 % in 1996 to 19 % in 2004, The percentage of successful projects (The project is completed on time and on budget, with all features and functions originally specified) has not improved and lies between 26 to 35 %. In the last 10 years, the percentage of 'failed' projects (the project is canceled before completion or never implemented) is fluctuating between 46 to 53 % [19, 20]. This means that knowledge gained during this period has helped in converting projects from 'challenged' to 'success' category. Considering the fact that various quality process models were implemented largely during this period, one can safely assume that; this was one of the important contributory factors for this shift of projects from 'challenged' to 'success' category. This is a real concern and need to be addressed, so that the projects falling in 'failure' category can be moved to 'challenged' and 'success' categories. In order to develop economically viable software, the performance prediction during the software development life cycle should be more accurate, so that it will help the developer to correct the lacunae or flaws. A more accurate prediction will help the organization to correct the flaws well in advance for better resource utilization.

The software size and complexities are increasing and software project management has become crucial. The industry demands for consistent software quality within the stipulated cost and time frame. In order to achieve quality, cost and schedule target, quantification and prediction of the software product characteristics early in the life cycle of development have become an increasingly important problem. The primary factors affecting the determination of the characteristics of the software product are the nature of the development process and the specification of the product. Software does not manifest its quality properties directly; instead it is exhibited through certain contributory measures of the process steps and intermediate work products. A quantitative model which can relate product and process attributes of the software development is needed.

Benefits of quantitative prediction of the product attributes and process attributes are two fold: first it will improve the process and second it will lead to the better project management. Improved software process and better project management is needed in order to deliver high quality product, at low cost, at agreed time and schedule with high customer satisfaction.

While predicting the project parameter performance, one must consider the environmental factors which affect the performance of the organization along with the other technical and process parameters. A set of new environmental parameters such as Group maturity rating (GMR), Defect rating (DR), Project risk index, process compliance index (PCI) and coefficient of variation of historical data are developed for predicting the project performance along with the in-project parameters.

6.7.1 Need for Soft Computing Methods

There exist a number of software prediction models defined by many researchers [21–29]. However, end to end metrics predicting the software life cycle phases are very less. In addition, most of the studies in the area of software performance prediction does not talk about working environment or assumes that there is no change in environment. Pham [30] defined a set of environmental parameters, but are limited to the software reliability models. Most of the prediction models available in the three major software engineering journals from 1980 to 2005 repeatedly use some of the better known and publicly accessible data sets [31, 32]. The usages of actual industrial data for validating the models are not in seen regularly. Hence, there is a need to identify the environmental parameters for end to end prediction of software life cycle parameters and to validate the model with the industry data. There is scope to develop a performance prediction model incorporating in-project and environmental parameters to nullify the influence of environment in the model. The model needs to be flexible enough to use in industry without major modifications. It is proved that the usage of soft computing methods for prediction gives better results than the conventional methods [33–37].

There are many software performance prediction models available. However, there is no universally acceptable model available that can be trusted to give accurate results in all circumstances. Depending on the situation, we have to choose the proper prediction model. In addition, while using most of these models, prediction is possible at the end stages of the project. This makes difficult for the industry to take corrective actions to the quality of software. True reliability cannot be measured until the software is completed and delivered to the customer. It will be better if the industry is getting the information about the performance of the project early in its life cycle. This will make the developers to act on the quality problems well in time, which will be cost effective also better than fixing it lately at a high cost. Since developing environment is very dynamic, trusting the past projects for predicting the future may not yield good results. It will be better if we construct a metrics, which will use the organizational baseline to predict the performance in the early stage of the project. As the project progresses, the data from the project will be picked and will refine the prediction. Ultimate aim is to develop a metrics model that will consider all aspects of the software life cycle and predicts the reliability dynamically as the project progresses in order to meet the software reliability target with ease.

6.7.2 Environmental Parameters

A set of environmental parameters (Group maturity rating, defect rating, project risk index, process compliance index and coefficient of variation of historical metrics) are defined and validated. These parameters can be used for effective tracking of the projects. Using these parameters along with the in-project parameters, a set of performance prediction models are defined. These models are defined using artificial

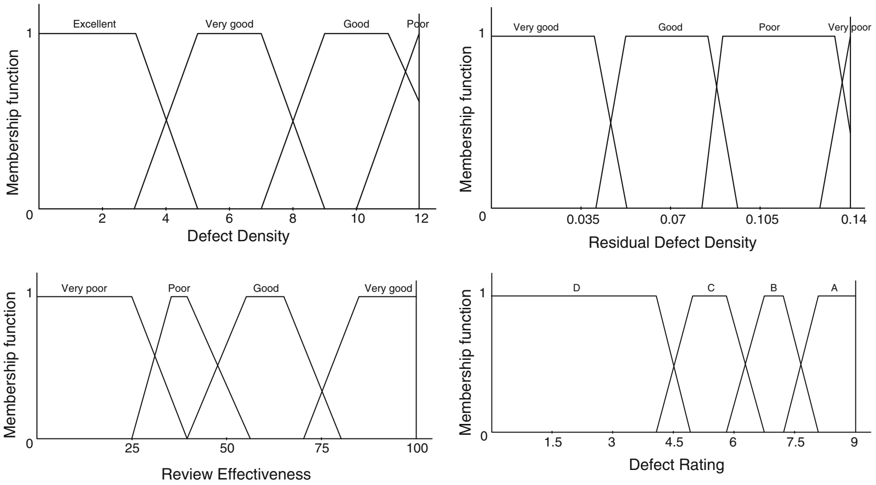


Fig. 6.7 Fuzzy membership functions for defect rating

neural networks and predict the performance of the subsequent phases. These performance prediction models will help the project manager to plan and execute the project in optimally. A brief on the environmental parameters defined is given below.

Defect Rating (DR)

There exists a unique relationship between Defect density (DD), Residual Defect density(RDD) and Review Effectiveness(RE) and these three parameters are to be treated together. Low DD and low RDD is the best. When RDD is more and DD is less, it implies to the ineffective in-house testing and review. Here the influence of review effectiveness comes into picture. An effective review will definitely helps the defect densities to come down, but may not be in a linear scale. Considering these, a new parameter called Defect rating (DR) is developed using the different combinations of DD, RDD and RE (Fig. 6.7 Fuzzy membership functions for defect rating). Where,

1. Defect Density

   Defect density is one of the important metrics of software organizations and gives a picture of the quality of the projects of that organization. Defect density is defined as the defects per unit size of the software entity being measured. Defect density can be correlated with many parameters like the project management practices and processes followed by the project team, the technical knowledge of the organization, and on the competency of the people. Due to these factors, the historical information about the defect density of projects will always help the organization to decide on the time required for review and testing and stoppage rules of testing.
2. Residual Defect Density

   Residual defect density shows the quality of the projects delivered by an organization and this is also one of the important defect metrics for an organization.

Residual defect density (RDD) is the measure of the unresolved defects after release of the software entity per unit size. This number indicates the number of defects passed on to the customers after completing the in-house testing. RDD plays a crucial role in the customer satisfaction since it directly affects the customer whereas; DD defines in the quality of the in-house development.

3. Review Effectiveness

During software development, there exist many opportunities for errors. Even though, in ideal conditions, one expects no defects are injected during the development process, the same is an impossible target. In this scenario, the best possible method is to remove the maximum possible error injected as soon as possible. The first possible chance for finding out the errors while developing software is the review process. Review effectiveness (RE) is the ratio of total defects found during reviews to the total no of defects found during the entire life cycle. This can be expressed as,

$$\text{RE} = \frac{\text{Number of defects found during review of defects found during lifecycle}}{\text{Number of defects found during lifecycle}} \times 100\,\%$$

This will help the organization to know the health of the project. It also avoids the problem of comparing projects in different technologies since DD and RDD are correlated to the technology and review effectiveness is independent of technology. Tables 6.7, 6.8 and 6.9 illustrate the formulae used to find the membership values of DD, RDD, and RE, respectively.

A fuzzy logic model was created for defect rating. Sixty four different rules were created based on the input–output combination and fed to the fuzzy engine.

Project Risk Index

During project execution, every project is considering some assumptions. There exists a set of risks with each assumption. Also there is a possibility of the influence of external parameters in each and every project. Before project kick off, the project team analyzes all the anticipated risks associated with the project. For better management of the risk, quantitative tracking of risks is mandatory. Project risk

Table 6.7 Defect rating—evaluation criteria—defect density

Membership function	Membership values
Very good	$0, \mu - \frac{9\sigma}{2}, \mu - \frac{7\sigma}{2}, \mu - \frac{5\sigma}{2}$
Good	$\mu - \frac{7\sigma}{2}, \mu - \frac{5\sigma}{2}, \mu - \frac{3\sigma}{2}, \mu - \frac{\sigma}{2}$
Poor	$\mu - \frac{3\sigma}{2}, \mu - \frac{\sigma}{2}, \mu + \frac{\sigma}{2}, \mu + \frac{3\sigma}{2}$
Very poor	$\mu, \mu + \sigma, \mu + 2\sigma, \infty$

Table 6.8 Defect rating—evaluation criteria—residual defect density

Membership function	Membership values
Very good	$0,\ 0,\ \mu - \frac{3\sigma}{2},\ \mu - \sigma$
Good	$\mu - \frac{3\sigma}{2},\ \mu - \sigma,\ \mu + \frac{3\sigma}{4},\ \mu + \frac{5\sigma}{4}$
Poor	$\mu + \frac{3\sigma}{4},\ \mu + \sigma,\ \mu + \frac{13\sigma}{4},\ \mu + \frac{15\sigma}{4}$
Very poor	$\mu + 3\sigma,\ \mu + \frac{7\sigma}{2},\ \mu + \frac{9\sigma}{2},\ \infty$

Table 6.9 Defect rating—evaluation criteria—review effectiveness

Membership function	Membership values
Very good	$0,\ 0,\ \mu-\frac{9\sigma}{4},\ \mu-\frac{3\sigma}{2}$
Good	$\mu-\frac{9\sigma}{4},\ \mu-\frac{7\sigma}{4},\ \mu-\frac{3\sigma}{2},\ \mu-\frac{3\sigma}{4}$
Poor	$\mu-\frac{3\sigma}{2},\ \mu-\frac{3\sigma}{4},\ \mu-\frac{\sigma}{4},\ \mu+\sigma$
Very poor	$\mu+\frac{\sigma}{4},\ \mu+\frac{3\sigma}{4},\ 100,\ 100$

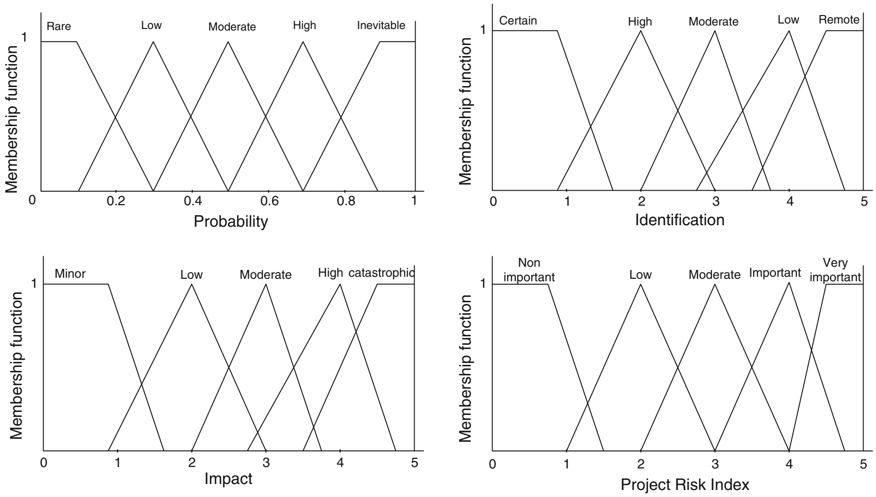


Fig. 6.8 Fuzzy membership functions for project risk

index is used for this purpose. Each associated risks are categorized based on its probability of occurrence, its impact on the projects and the possibility of identifying them in advance. Each of these parameters is ranked into different classes for example the probability of occurrence is classified into “Rare”, “Low”, “Moderate”, “High” and “Inevitable” (Fig. 6.8: Fuzzy membership functions for project risk). A fuzzy logic method is used to identify the final risk index. The average risk index of all the risks of the project is considered as the project risk index. The risk index can be calculated as the product of the probability of the risk, its impact on the project and the possibility of identification

Process Compliance Index (PCI)

Success of the project execution largely depends on well defined process. Most of the organizations have developed well defined processes for their project execution. However, even if an organization defines the best available processes, it will not yield any result unless the same is being followed in the organization with its right spirit. Process Compliance Index (PCI) is the quantitative representation of the process being executed as per the standards defined with in the organization. Steps to formulate the PCI is given below

1. Identify the key processes that will have a great impact on business performance.
2. Identify the key activities which control the processes and can be monitored on a periodic basis.
3. Provide ratings for the compliance of each activity, like 1 if activity is completely done, 0.5 if activity is partially done, 0 if activity is not done and "NA" is the activity is not applicable for that project.
4. Provide clear guidelines for assessment of the implementation levels of each activity, i.e., when to give rating of 1 for an activity and when to give 0.5 for the same activity, etc.
5. Provide rating for each activity, since the impact one activity on project may not be same as that of another activity.
6. The PCI can be calculated using the formula

$$PCI = \left(\frac{\sum_{i=1}^{m} \phi_i}{\sum_{i=1}^{m} \phi_{\max}}\right) \cdot 100\%$$

Here,

$$\phi_i = \begin{cases} \psi_i \rho_i & \rho_i = 0, 0.5, 1 \\ 0 & \text{otherwise} \end{cases}$$

and,

$$\phi_{\max} = \begin{cases} \psi_i & \rho_i = 0, 0.5, 1 \\ 0 & \text{otherwise} \end{cases}$$

ψ_i is the weight associated with activity i, ρ_i is the rating of activity i and m is the total number of activities.

Group Maturity Rating (GMR)

The maturity of an organization depends on the success of the projects they have executed in the recent past and on the capability of the people in the organization. Hence the historical data on the recently executed projects and data of the ongoing projects are playing a very important factor in determining the maturity of the group. The historical data from the past projects of the organization is considered for rating the different groups within the organization. A new environmental parameter called Group maturity rating (GMR) [38] is developed using fuzzy logic approach. This rating can provide information about the capability of the group which develops the software. Since the experience in developing software plays a major part in the success of the future projects, this rating is an important environmental parameter. There are five metrics parameters are considered for developing the GMR. They are

1. *Schedule Variance (SV)*

   Schedule Variance is percentage of variance of the actual duration for an activity to the planned duration. It is a measure of variation in meeting with the software project's planned deadline date. It can be calculated using the formula

$$SV = \frac{\delta_{actual} - \delta_{planned}}{\delta_{planned}} \times 100\,\%$$

   Where, δ is the duration.

2. *Effort Variance (EV)*

   The effort variance (EV) is the percentage variance of the actual effort with respect to the planned effort. It is a measure of how effectively the estimation and planning was conducted for a software project. It can be calculated using the formula

$$EV = \frac{\varepsilon_{actual} - \varepsilon_{planned}}{\varepsilon_{planned}} \times 100\%$$

   Where, ε is the effort.

3. *Customer Satisfaction Index (CSI)*

   A clear Understanding of customers' perceptions helps the software organizations to determine the actions required to meet the customers' needs. Customer satisfaction measurement helps to focus more on customer outcomes and stimulate actions for improvements in the work practices and processes used within the organization. The Customer Satisfaction Index represents the overall satisfaction level of that customer as one number in a scale of 1–5, where 1 is the minimum and 5 is the maximum. Sixteen questions in the area of project execution, quality of the service and the communication with the customer are given to the customer to rate. Each question is assigned with a weightage.

   CSI is calculated using the formula.

$$CSI = \left(\frac{\sum_{i=1}^{n} S_i}{\sum_{i=1}^{n} S_{\max}}\right) \times 5$$

Here,

$$S_i = \begin{cases} 0 & r_i = 1 \\ w_i r_i & r_i = 2,3,4,5 \end{cases}$$

and,

$$S_{\max} = \begin{cases} 0 & r_i = 1 \\ w_i \cdot 5 & r_i = 2,3,4,5 \end{cases}$$

where, w_i is the weight associated with question, n is the rating of question i and n is the number of questions.

4. *Process Compliance Index (PCI)*
   Process compliance index of the projects that are considered for calculating the GMR are determined in the same way as mentioned in Sect. 3.3.
5. *Defect Rating*
   Defect rating is calculated using the methodology mentioned in previous section is used as an input for group maturity rating.
   Fuzzy approach is selected since the parameters are either linguistic in nature or they are fuzzy in nature. In the this model, the fuzzy input sets are Process Compliance Index (PCI), Customer Satisfaction Index (CSI), Schedule Variance (SV), Effort Variance (EV) and Defect Rating (DR). The output parameter of the fuzzy system is Group Maturity rating is defined as the rating given to each project group in the organization based on its past performance. The output for the fuzzy system is linguistic variable Group Maturity rating and is defined as {“A”, “B”, “C”} (Fig. 6.9 Fuzzy membership functions for GMR). Based on the input-output combinations One thousand nine hundred and twenty rules are created using the fuzzy system editor contained in the Fuzzy Logic Toolbox of Matlab. These rules are fed to the fuzzy engine. By changing the input, the corresponding output can be arrived at. Using the organization’s historical data the maturity rating of the different groups can be found out. This will be a single measurement unit for the organization to assess different groups with in since most of the groups will be working on different domains, different technology

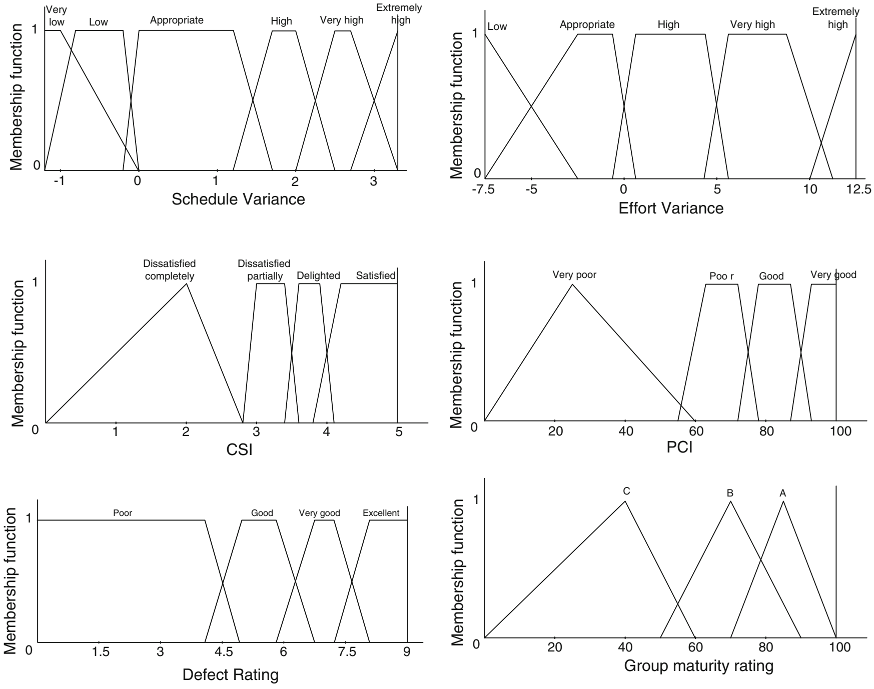


Fig. 6.9 Fuzzy membership functions for GMR

and on different type of projects, it will be difficult to compare them with out a single measurement unit.

Coefficient of Variation of Historical Data
Coefficient of Variation (Cv) is statistical measure of the dispersion of data points in a data series around the mean and defined as the ratio of the standard deviation to the mean. The coefficient of variation is a dimensionless number. It is a very useful statistic for comparing the degree of variation from one data series to another, even if the means are drastically different from each other. For the Anil-Verma model, different Cv's are used. These parameters are derived from the metrics of the historical projects. Cv is calculated using the mean and standard deviation of these metrics. They are mentioned below.

- Cv_DD—Coefficient of Variation–Defect Density
- Cv_ced—Coefficient of Variation–construction effort distribution
- Cv_DD—Coefficient of Variation–Defect Density
- Cv_ded—Coefficient of Variation–design effort distribution
- Cv_red—Coefficient of Variation–requirement effort distribution
- Cv_rwed—Coefficient of Variation–review effort distribution
- Cv_ted—Coefficient of Variation–testing effort distribution
- Cv_tev—Coefficient of Variation–total effort variance

6.7.3 Anil-Verma Model

A set of prediction models are developed using neural network for predicting the project parameters like effort, defect density, duration, review effort and review duration using the in-project and environmental parameters. The model can be used along with the current process models within the software development organization. Detailed implementation guidelines are prepared and it will help in systematic implementation of the model and supports the software development organization to attain higher maturity levels. The overall framework of the Anil-Verma models is depicted in the Fig. 6.10. The Anil-Verma model is trained and validated using this industrial data set. Validation of the models is carried out by data from three groups in an industry which are geographically and functionally apart. Bench marking of the model is carried out with the previous work and concluded that the current model is better.

Results Obtained from Anil-Verma Model
The framework of the prediction equations is developed for the parameters in the various phases of the software development life cycle. Data from a typical software development organization of high maturity is collected to instantiate the framework of prediction equations. Data from over 200 projects spanning over different geographical locations are collected. One can find different types of software developed in a typical large software organization. In order to make things more clear, the

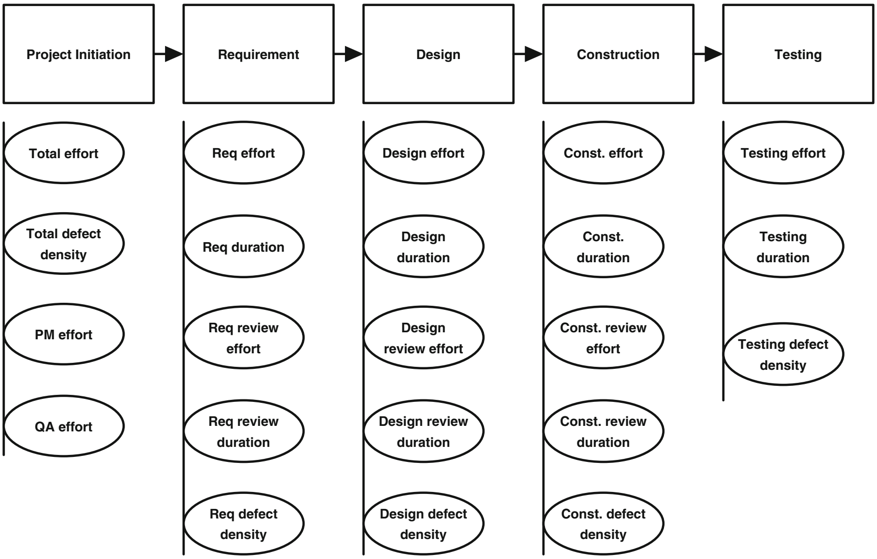


Fig. 6.10 Overall framework of the Anil-Verma models

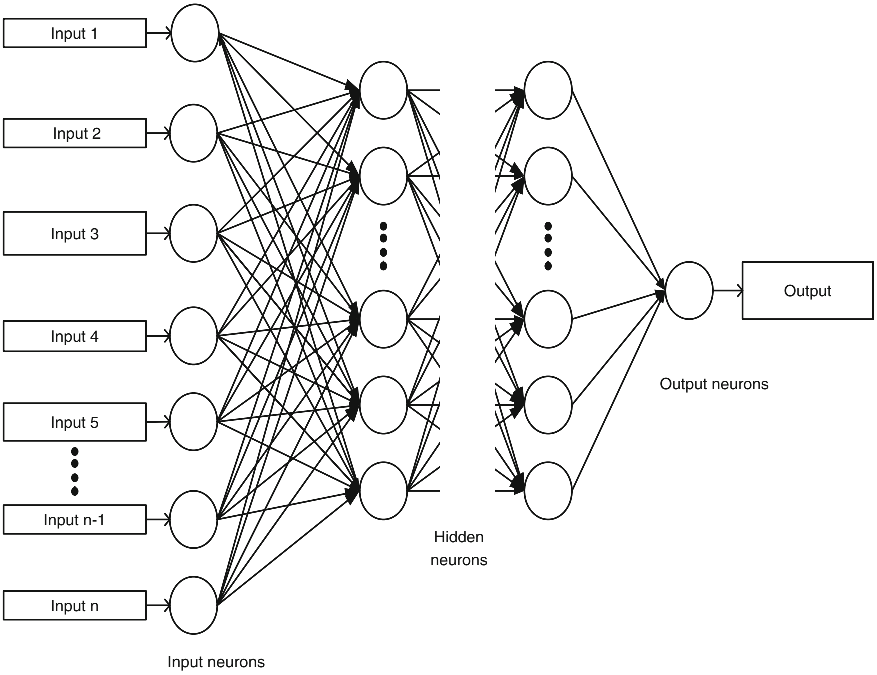


Fig. 6.11 General structure of the Anil-Verma models

concentration was on 3rd generation language (3GL). The concentration of this study is limited to development type of projects. Collected data is analyzed to eliminate the outliers and ensured that the outliers are removed from the data-set. The training data set used to train different neural networks. Multilayer perceptrons (MLP), Generalized feedforward networks (GFF), Jordan and Elman networks (ELM) and Principal component analysis networks (PCA) are used for training the data set. Different number of hidden nodes are used in MLP and GFF to find the optimum number of hidden neurons. The data for validation is fed into these networks. Using the actual output obtained and the predicted output from these models, the performance of the networks are measured. General structure of the Anil-Verma model is depicted in Fig. 6.11. The summary of all the phases and the respective parameters are shown in Tables 6.10–6.14.

Table 6.10 Summary of the prediction model—project initiation phase

Project initiation				
	Total effort	Total defect density	QA effort	PM effort
Size	✓	✓	✓	✓
PCI_req	✓	✓	✓	✓
GMR	✓	✓	✓	✓
Risk	✓	✓	–	–
Cv_total effort variance	✓	–	✓	✓
Estimated effort	–	✓	–	–
Cv-defect density	–	✓	–	–
Defect rating	–	✓	–	–

Table 6.11 Summary of the prediction model—requirement phase

Requirement phase					
	Req effort	Req duration	Req review effort	Req review duration	Req defect density
Size	✓	✓	✓	✓	✓
PCI_req	✓	–	✓	✓	✓
GMR	✓	–	–	–	✓
Risk	✓	–	–	–	✓
Cv—total effort variance	✓	–	–	–	✓
Team size_req	–	✓	–	✓	–
Cv—req effort dist. effort variance	–	✓	–	–	✓
Effort_req	–	–	✓	✓	✓
Cv—review effort distribution	–	–	✓	✓	–
Estimated effort	–	–	–	–	✓
Cv—defect density	–	–	–	–	✓
Defect rating	–	–	–	–	✓

Table 6.12 Summary of the prediction model—design phase

Design phase					
	Design effort	Design duration	Design review effort	Design review duration	Design defect density
Size	✓	–	✓	✓	–
Effort_req	✓	✓			
DD_req	✓	–	–	–	–
PCI_design	✓	✓	✓	✓	✓
GMR	✓	–	–	–	✓
Cv—design effort distribution	✓	✓	–	✓	–
Risk	✓	–	–	–	–
Cv_total effort variance	✓	–	–	–	–
Duration_req	–	✓	–	–	–
Team size-design	–	✓	–	✓	–
Effort_design	–	–	✓	✓	✓
Cv—review effort distribution	–	–	✓	–	–
Defect rating	–	–	–	–	✓
Effort_design review	–	–	–	–	✓
Cv—defect density	–	–	–	–	✓
Duration_design review	–	–	–	–	✓
Estimated effort	–	–	–	–	✓
DD_req	–	–	–	–	✓
Duration_design	–	–	–	–	✓

To validate the model, the model is applied into three different geographical locations of a high maturity software development organization. These three geographical locations are acting as independent entities and are working under different working environments. They serve entirely different customer base and the area of expertise is also not the same. In sort, we can consider them as separate organizations. The model can be applied to different parts of an industry without any modification. The results of the validation are mentioned in Table 6.15).

From the results obtained, it can be concluded that the environmental parameters like Group maturity rating, defect rating, project risk index, process compliance index and coefficient of variation of historical metrics are playing an important role in the process performance prediction. The model which uses the environmental

Table 6.13 summary of the prediction model—construction phase

Construction phase	Construction effort	Construction duration	Construction review effort	Construction review duration	Construction defect density
Effort_req	✓	✓	–	–	–
Effort_design	✓	✓	–	–	–
Size	✓		✓	✓	✓
Cv_const effort distribution	✓	✓	–	–	–
PCI_const	✓	✓	✓	✓	✓
GMR	✓	–	–	–	✓
Risk	✓	–	–	–	–
Duration_req	–	✓	–	–	–
Team size_const	–	✓	–	✓	–
Duration_design	–	✓	–	–	–
Effort_construction	–	–	✓	✓	✓
Cv_review effort dist	–	–	✓	✓	–
DD_req	–	–	–	–	✓
DD_design	–	–	–	–	✓
Defect rating	–	–	–	–	✓
Effort_const review	–	–	–	–	✓
Cv-defect density	–	–	–	–	✓
Duration_const review	–	–	–	–	✓

Table 6.14 Summary of the prediction model—testing phase

Testing phase			
	Testing effort	Testing duration	Testing defect density
Size	✓	✓	✓
Effort_const	✓	–	✓
PCI_const	✓	✓	✓
Cv_testing effort distribution	✓	✓	–
Team size_testing	–	✓	–
DD_req	–	–	✓
DD_design	–	–	✓
DD_const	–	–	✓
Duration_const	–	–	✓
Teamsize-const	–	–	✓
Defect rating	–	–	✓
GMR	–	–	✓
Cv_defect density	–	–	✓

Table 6.15 Validation of models using industrial data

Project prediction parameters	Mean magnitude relative error (%)				
	Testing data	Validation data			
		Set 1	Set2	Set 3	Average
Total effort	0.095	0.06	0.053	0.145	0.084
Project management effort	0.058	0.051	0.029	0.08	0.056
Quality assurance effort	0.097	0.125	0.035	0.152	0.112
Total defect density	0.257	0.329	0.176	0.23	0.26
Requirement effort	0.106	0.061	0.078	0.086	0.078
Requirement duration	0.09	0.08	0.087	0.088	0.087
Requirement review effort	0.128	0.088	0.048	0.147	0.13
Requirement review duration	0.24	0.16	0.219	0.175	0.196
Requirement defect density	0.114	0.133	0.126	0.08	0.107
Design effort	0.106	0.111	0.108	0.101	0.108
Design duration	0.03	0.041	0.042	0.039	0.041
Design review effort	0.032	0.034	0.021	0.024	0.03
Design review duration	0.138	0.122	0.086	0.073	0.102
Design defect density	0.229	0.237	0.202	0.269	0.259
Construction effort	0.065	0.082	0.044	0.07	0.071
Construction duration	0.159	0.193	0.088	0.215	0.16
Construction review effort	0.04	0.059	0.033	0.069	0.057
Construction review duration	0.129	0.168	0.104	0.085	0.126
Construction defects	0.096	0.089	0.094	0.095	0.093
Testing effort	0.095	0.08	0.07	0.065	0.084
Testing duration	0.108	0.097	0.105	0.111	0.108
Testing defect density	0.104	0.105	0.082	0.136	0.104

parameters as inputs performs better than the models which does not uses the environmental parameters as input parameters. Project phase parameters from the current development phase are used to predict the performance of the subsequent phase along with the environmental parameters.

Implementation guidelines for Anil-Verma Model

Anil-Verma model can be implemented by following the steps given below (Fig. 6.12).

Step 1. *Identify metrics*
Identify all metrics that are important for the organization and arrive at the methodology of capturing it on a regular basis. Ensuring the integrity of the data is an important step.

Step 2. *Identify environmental parameters*
Identify all environmental parameters that affect the performance of the projects and arrive at the methodology of capturing it on a regular basis.

Step 3. *Develop Historical data repository*
Develop a methodology for collecting and depositing the historical data.

Step 4. *Develop current project data repository*
Develop a methodology for collecting and depositing the current project data across organization.

Step 5. *Develop framework of the model*
Using the metrics and environmental parameters, develop the framework of the model considering the most appropriate metrics and environmental parameters.

Step 6. *Pilot model*
Pilot the implementation of the model in small group within the organization.

Step 7. *Train the model*
Train the model using the past project information and find the best neural network model.

Step 8. *Validate the model*
Use the model in running projects and calculate the error. Fine tune the model for minimum error.

Step 9. *Train people*
Train the people to collect the metrics, how to analyze the metrics and on the usage of the model.

Step 10. *Organizational roll-out*
If results from pilot are within the required accuracy, roll out the model across the organization.

Step 11. *Continual improvement*
Improve the model on a continuous basis

Step 12. *Merge the model with legacy system*
After implementation, plan for merging of the model with the legacy system to get online prediction.

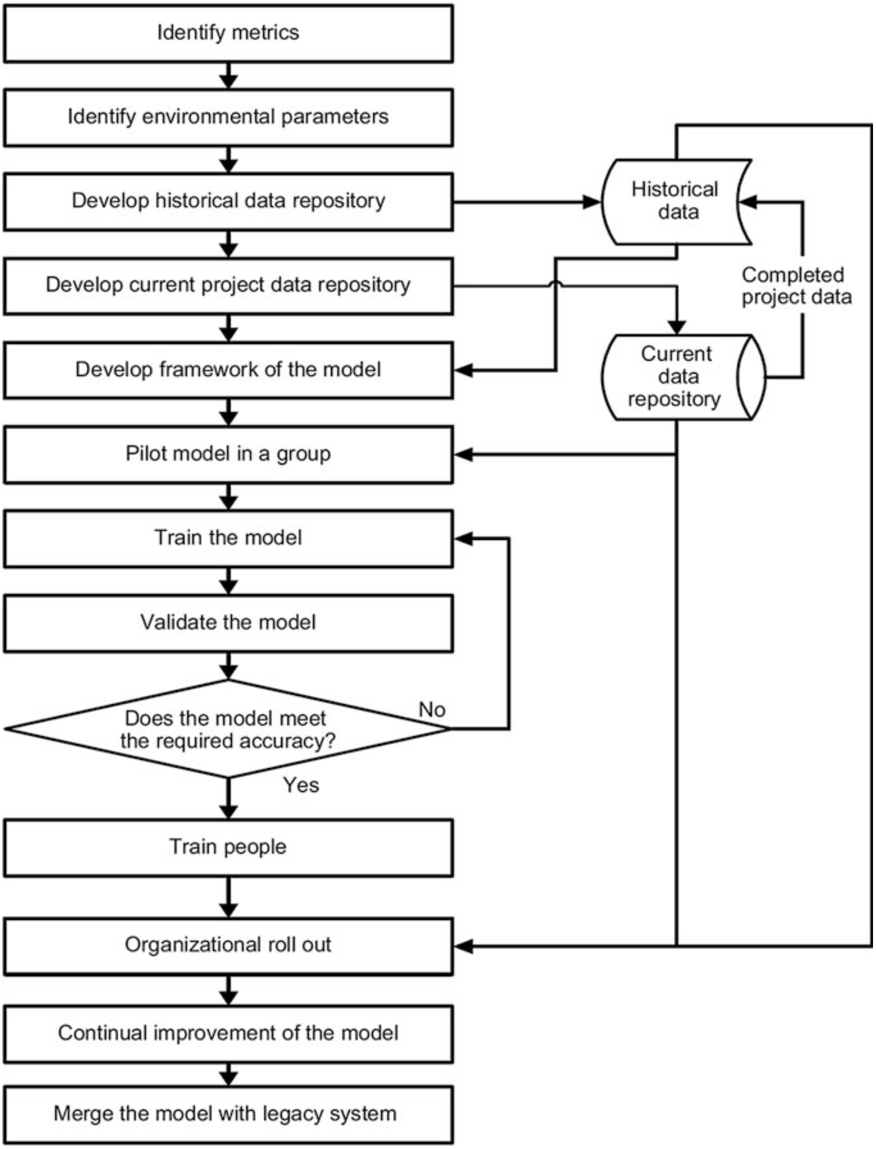

Identify metrics
Identify environmental parameters
Develop historical data repository
Develop current project data repository
Develop framework of the model
Pilot model in a group
Train the model
Validate the model
Does the model meet the required accuracy?
No
Yes
Train people
Organizational roll out
Continual improvement of the model
Merge the model with legacy system
Historical data
Completed project data
Current data repository

Fig. 6.12 Implementation guidelines for Anil-Verma model

6.8 Future Trends of Software Reliability

Software reliability traveled a lot from the initial models which were concentrated mainly on the testing phase to the new soft computing models where the models are distributed throughout the lifecycle. The concentration is slowly shifting to the cognitive nature of software development. The need of considering the environment in which the software is being developed is identified and being worked upon. However, this is a small step towards the future. As the world depends more and more on software on day to day activities as well as for mission critical applications, more reliable software is the need of the hour. In order to fulfill this requirement, the software reliability has to cover a lot of ground. Considering the fact that the reliability of the software largely depends on the human beings who develops it, in the near future, the concentration will be on the human factor which affects the reliability of the software.

References

1. IEEE Standards Board (1990) IEEE standard glossary of software engineering terminology. IEEE std 610.12
2. Ebert C, Liedtke T, Baisch E (1999) Improving reliability of large software systems. Ann Software Eng 8:3–51
3. Jensen BD (1995) A software reliability engineering success story. In: Proceedings of sixth international symposium on software reliability engineering, pp 338–343
4. Kropfl D, Ehrlich W (1995) Telecommunications network operations systems: experiences in software reliability engineering. In: Proceedings sixth international symposium on software reliability engineering, pp 344–349
5. http://research.microsoft.com/en-us/groups/srr/
6. http://sw-assurance.gsfc.nasa.gov/index.php
7. Lyu MR (1996) Handbook of software reliability engineering. IEEE computer society press
8. Marasco J, Ravenflow CEO (2006) Software development productivity and project success rates: are we attacking the right problem? http://www-128.ibm.com/developerworks/rational/library/feb06/marasco/index.html
9. Reliability Analysis Center (RAC) Introduction to software reliability: a state of the art review, New York. http://src.alionscience.com/pdf/RAC-1ST/SWREL_1ST.pdf
10. Asad CA, Ullah MI, Rehman MJU (2004) An approach for software reliability model selection. In: Proceedings of the 28th annual international computer software and applications conference, pp 534–539
11. Jelinski Z, Moranda PB (1972) Software reliability research. Statistical computer performance evaluation. Academic Press, New York, pp 465–484
12. Goel AL, Okumoto K (1979) Time-dependent error-detection rate model for software reliability and other performance measures. IEEE Trans Reliab 28:206–211
13. Musa JD, Iannino A, Okumoto K (1990) Software reliability: measurement, prediction, application, professional edn. McGraw-Hill Inc, New York
14. Gokhale S, Hong WE, Trivedi K, Horgan JR (1998) An analytical approach to architecture based software reliability prediction. In: Proceedings of the 3rd IEEE international computer performance and dependability symposium
15. Littlewood B, Verrall JL (1973) A Bayesian reliability growth model for computer software. Appl Stat 22:332–346
16. Lyu MR (1996) Handbook of software reliability engineering. In: IEEE computer society press
17. Rosenberg L, Hammer T, Shaw J (1998) Software metrics and reliability. http://satc.gsfc.nasa.gov/support/ISSRE_NOV98/software_metrics_and_reliability.html
18. Musa JD (1975) A theory of software reliability and its applications. IEEE Trans Software Eng 1(3):312–327

19. Goel AL (1975) Software reliability models: assumptions, limitations, and applicability. IEEE Trans Software Eng 11(12):1411–1423
20. Musa J, Iannino A, Okumoto K (1990) Software reliability: measurement, prediction, application. McGraw-Hill, New York
21. Musa JD, Okumoto K (1984) A logarithmic Poisson execution time model for software reliability measurement. In: ICSE '84: proceedings of the 7th international conference on software engineering. IEEE Press, pp 230–238
22. Goel AL, Okumoto K (1979) Time-dependent error detection rate model for software reliability and other performance measures. IEEE Trans Reliab 28:206–211
23. Goel AL (1985) Software reliability models: assumptions, limitations, and applicability. IEEE Trans Software Eng 11(12):1411–1423
24. Lyu MR (1996) Handbook of software reliability and system reliability. McGraw-Hill Inc, Hightstown
25. Musa JD, Iannino A, Okumoto K (1990) Software reliability: measurement, prediction, application. McGraw-Hill Inc, New York
26. Musa JD (1975) A theory of software reliability and its application. IEEE Trans Software Eng 1(3):312–327
27. Littlewood B (1987) Software reliability: achievement and assessment. Blackwell Scientific Publications, Oxford
28. Jelinski Z, Moranda PB (1972) Software reliability research. Statistical computer performance evaluation. Academic Press, New York, pp 465–484
29. Mehta PN (2006) Integration of product and process at tributes for quantiative modeling in software. PhD thesis, Indian Institute of Technology Bombay, Mumbai, India
30. Pham H (2006) System software reliability. Springer, London
31. Mair C, Shepperd M, Jørgensen M (2005) An analysis of data sets used to train and validate cost prediction systems. In: PROMISE '05: Proceedings of the 2005 workshop on predictor models in software engineering. ACM Press, New York, NY, USA, pp 1–6
32. Shepperd M (2005) Evaluating software project prediction systems. In: Proceedings of the 11th IEEE international software metrics symposium (METRICS'05). IEEE Computer Society, Washington, DC, USA
33. Karunanithi N, Malaiya YK, Whatley D (1991) Prediction of software reliability using neural networks. In: International symposium on software reliability engineering, IEEE Computer Society Press, Los Alamitos, California, pp 124–130
34. Khoshgoftaar TM, Panday AS, More HB (1992) A neural network approach for predicting software development faults. In: Proceedings of the third international symposium on software reliability engineering, IEEE Computer Society Press, pp 83–89
35. Adnan WA, Yaacob MH (1994) An integrated neuralfuzzy system of software reliability prediction. In: First international conference on software testing, reliability and quality assurance, pp 154–158
36. Karunanithi N, Whitley D, Malaiya YK (1992) Prediction of software reliability using connectionist models. IEEE Trans Software Eng 18:563–574
37. Huang X, Ho D, Ren J, Capretz LF (2007) Improving the COCOMO model using a neurofuzzy approach. Appl Soft Comput 7(1):29–40
38. Verma AK, Anil R, Jain OP (2007) Fuzzy logic based group maturity rating for software performance prediction. Int J Autom Comput 4(4):406–412

Chapter 7
Mechanical Reliability

Mechanical reliability is a very old subject, for as long as human has built things, he/she has wanted to make them as reliable as possible. Mechanical Systems were overdesigned by using larger safety factors in the past to avoid failures. Mechanical reliability takes consideration of material engineering, durability of the components, tribology aspects of product, operating conditions, environment and mechanics. Further, understanding of statistics and probability is primary to understanding and creating a reliable mechanical system.

It is very difficult to predict the Reliability of Mechanical components designed for a specific system. The variables affecting the reliability include manufacturing variation, material variation, variation in operational loading, duty cycle, environment, etc. There are some models developed using physics of failure technique in order to predict the reliability of these components. Though these methods are useful to know the sensitivity of the design parameters on the overall reliability of the product, it is important to validate the product in the expected loading and environmental conditions.

Part of generating the valuable historical data to predict future reliability of mechanical components is classifying their failure. For example, the best data on when the maintenance for a bearing in grinding equipment should be replaced, knows when the bearings in the similar type of grinding equipments needed replacing previously. Obviously, for new systems, this is not possible. Reliability data from the existing systems can be considered for the new designs, If the new design is quite similar to the current systems. For completely new designs, however, alternative means of estimating reliability must be employed.

It is imperative that mechanical parts, like most other items, do not survive indefinitely without maintenance. A large portion of mechanical reliability is determining when maintenance should be done in order to prevent a failure.

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_7

7.1 Reliability Versus Durability

Reliability is defined as, (1) The duration or probability of trouble free performance under stated conditions. (2) The probability that an item can perform its intended function for a specified time under stated conditions. For non-redundant items this is equivalent to definition 1. For redundant items this is equivalent to mission reliability, which is the probability that the product will not fail to complete the mission considering all possible redundant modes of operation.

Reliability is figured as the ability to meet criteria consistently, dependability, trustworthiness.

Reliability engineering address two types of failures, product functional failures, and failures like degraded performance. Normally failures are caused by mistakes (ex: design, manufacturing, logistics or management), and lack of robustness. Eliminating mistakes is primarily a matter of vigilance. Robust design requires statistical engineering techniques.

"Reliability means failure mode avoidance".

Durability is perceived as useful operating life (special case of reliability). It can also be stated as the period of time before the failure rate increases due to wear-out failure mode. Balbir S. Dhillon, and Hans. Reiche [1] says, it is concerned with the selection of material (properties like endurance, hardness, toughness, etc.) and performing design details in such a way that the resulting system is resistant to degradation from factors such as fatigue, erosion, wear and corrosion.

Durability is the study of time dependent failure modes such as wear and fatigue.

Durability is that function of a product that determines how long the product will last under normal operating conditions. It is very unlikely that customers are willing to pay for durable product when the product will soon be phased-out. Durability is given priority out of all the dimensions of Quality when the product is very expensive, is difficult to install or replace, and will not be soon obsolete.

An easy to grasp example of the value of durability is a 10 year light bulb for hard to reach fixtures. It would be smart to emphasize the durability factor simply because of the expense and trouble of replacement. They might cost four times as much as a cheap bulb, but the cheap bulbs may need replacing every month. In a similar fashion, we might market engine gaskets, brake linings, or any product where the costs of replacement outweigh the cost of the product.

Some examples to clarify the definition are, Automobile Tire wear is a Durability Issue. However, the Tire wears quickly (may be varied) by the suspension unreliability. Oxygen cylinder carried by the mountaineers. Here the Durability is depends upon the amount of oxygen. Reliability is failure of components like valve stuck closed, etc. in spite of the oxygen content.

Table 7.1 compares reliability and durability. There is wide literature available on the subject, mechanical reliability, for example, see reference [2–5].

Table 7.1 Comparison of reliability versus durability

	Reliability	Durability
Definition	Survival probability	It is related to the ability of item to withstand the time dependent mechanisms such as fatigue, wear, corrosion, etc. It is expressed as the minimum time before the occurrence of wear out failures
Essential difference	Reliability is the probability of survival, in general terms i.e., regardless of the underlying distribution of failures (decreasing, constant, and increasing). The period of time must be stated	Durability is a measure of how long (time, cycles, etc.) to the FIRST FAILURE, when the failure mechanism is of a wear out nature. (e.g.: fatigue, wear, corrosion, etc.)
Parameter	Consistency is checked	Degradation levels are determined
Method of measurement	Distribution of life is plotted. Shown in probabilistic quantity	Deterministic quantity
Tools	Statistical analysis such as weibull analysis, hazard analysis, stress-strength analysis, etc.	Usage profile/duty cycle data, CAD analysis (fatigue), endurance tests fatigue tests
Measurement	B_x life, survival probability, failure rate	Single life figure
	Ex: reliability of oil seal at 50,000 miles is: 0.9	Ex: durability of the brake liner is: 50,000 miles
Prediction	Prediction of life of design to be released	Prediction of design limits can be found
Problems raised due to:	1. Inconsistent design and manufacturing process. 2. Unsuitability of design to application viz: environments, loads, duty cycle	1. Strength 2. Endurance limits, 3. Wear characteristics, 4. Stiffness
Design requirement	Robust design is suitable	Rugged design is suitable
Examples–how customer perceived:	Failure over time, frequent failures, MTBF (e.g. regular car troubles, refrigerator service, etc.)	Life (e.g.: engine timing belt, head lamp, etc.)

7.2 Failure Modes in Mechanical Systems

The failure modes for mechanical components are classified into three categories,

1. Failures due to operating load
2. Failures due to environment
3. Failures due to poor manufacturing quality.

This type of failures can be avoided by good product design as well as process design. The designer should consider each of these modes to ensure that there is sufficient margin of safety and design the process for minimum variability to meet the reliability goals.

7.2.1 Failures Due to Operating Load

Tensile-Yield-Strength Failure: This type of failure occurs under pure tension. It occurs when the applied stress exceeds the yield strength of the material (Fig. 7.1). The result is permanent set or permanent deformation in the structure. A plastic strain of 0.2 % is usually used to define the yield strength.

Ultimate Tensile-Strength Failure: This type of failure occurs when the applied stress exceeds the ultimate tensile strength and causes total failure of the structures at a cross-sectional point (Fig. 7.2). The entire cross section is highly stressed and consequently is sensitive to material defects. This generally requires a good surface finish, and good manufacturing quality controls to minimize material defects.

1. Ultimate tensile Strength
2. Yield strength

Compressive Failures: Compressive failures are similar to the preceding tensile failures, except under compressive loads (Fig. 7.3). They result in permanent deformation or total compressive failure causing the cracking or rupturing of the material.

Brittle Fracture: Materials like cast iron, ceramic parts, glass which have little capacity for strain hardening and are generally brittle, are extremely susceptible to material defects and imperfections. The material is elastic until the fracture stress is reached, so there is not yield point (Figs. 7.4 and 7.5). Then the crack propagates rapidly and completely through the component. One of the characteristics of a

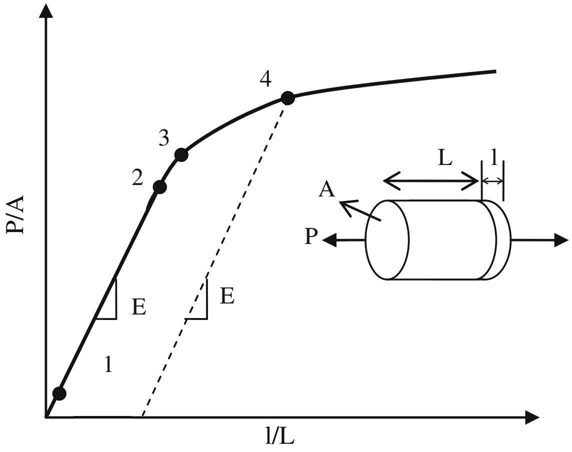
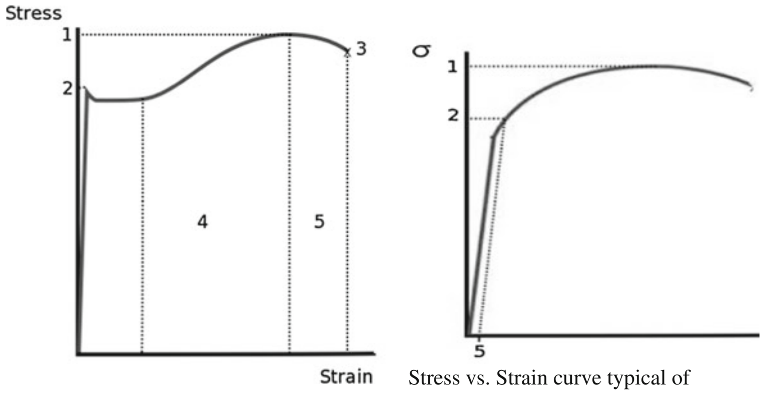


Fig. 7.1 Stress versus strain: *1*. True elastic limit, *2*. Proportionality limit, *3*. Elastic limit, *4*. Offset yield strength. *P* = applied load, *A* = area of cross-section, *L* = initial length, *l* = deformation, *E* = Young's modulus, σ = stress, ε = strain



Stress vs. Strain curve typical of structural steel

Stress vs. Strain curve typical of Aluminum

Fig. 7.2 Stress versus strain curves: **a** curve typical of structural steel **b** curve typical of aluminum. *1*. ultimate tensile strength, *2*. yield strength, *3*. rupture, *4*. strain hardening region, *5*. necking region

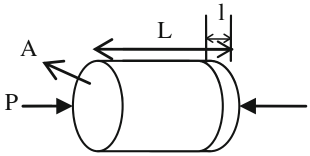
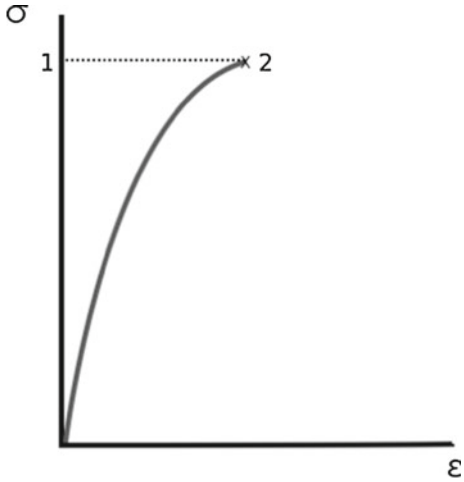


Fig. 7.3 Compressive load. *P* = applied load, *A* = area of cross-section, *L* = initial length, *l* = deformation

Fig. 7.4 Stress versus strain curve of a brittle material *1*. Ultimate Strength, *2*. Tensile strength



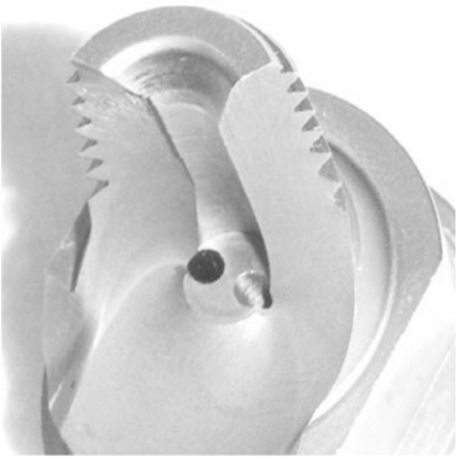


Fig. 7.5 Brittle fracture

brittle failure is that the broken pieces can be rejoined to produce the same shape as the original component. Reliability generally requires a good surface finish and very few internal flaws.

Failures due to Shear Loading: Failures occur when the shear stress exceeds the shear strength of the material when applying high torsion or high shear loads. These failures generally occur on a 45° axis with respect to the principal axis.

Failures due to Contact Stresses: The stresses caused by the pressure between elastic bodies like a round, cylindrical surface bearing on either a flat or a curved surface. Ex: ball and roller bearings, gears, etc. Calculations of contact stresses, contact area (circular, elliptical or rectangular area) are important for the investigation of long term wear of the mating parts during its operation.

Creep Failures under Long term Loading: More materials will creep or flow to some extent and eventually fail under constant stress less than the short-term ultimate strength. Creep accelerates at elevated temperatures. It is seldom important in materials at temperatures less than 40–50 % of their melting temperatures. Creep should always be checked under conditions where high loading for long periods of time are anticipated. The material tends to anneal and weaken over a long period of time or at an elevated temperature. For the Creep damage is characterized by reduction of Creep strength due to damage accumulation.

Bending Failures: A bending failure is a combined failure where an outer surface is in tension and the inner surface is in compression. The failure can be represented by tensile rupture of the outer material. The outer surfaces are highly stressed, and consequently the tensile side is sensitive to surface defects. Reliability generally requires good surface finish.

Fatigue Failures: Fatigue failures result from numerous repetitions of stress on the part that is not as large as the stress required for immediate fracture (Fig. 7.6). The microscopic cause of fatigue damage is due to the cyclic plastic flow in the material at the source of a fatigue crack such as sharp corners. When the stress

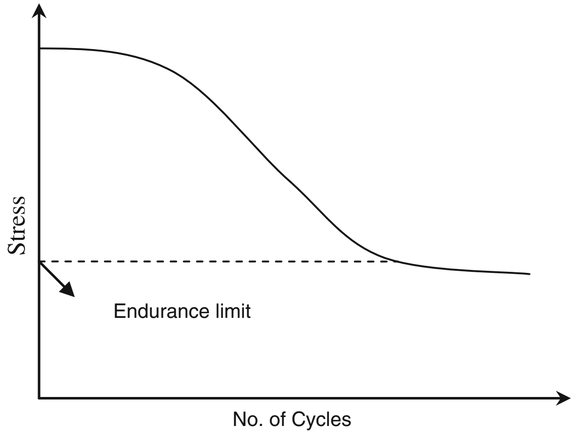


Fig. 7.6 Stress versus number of cycles

amplitude is constant and the variation is cyclic, the life of the component can be determined using the standard S/N (applied stress vs fatigue life) diagram available in the literature. Sharp radii (Stress concentration areas), surface finish, corrosion, temperature will affect the endurance limits of the material.

For design process, Minors rule is used to calculate the life of the component for a given duty cycle.

Minor’s rule:

$$\sum_{i=1}^{k} \frac{n_i}{N_i} = D \tag{7.1}$$

where

D	Damage
Life (L)	1 − D
S_i	Stress magnitude

There are k different stress magnitudes in a loading spectrum, S_i $(1 \leq i \leq k)$, each contributing $n_i(S_i)$ cycles, then if $N_i(S_i)$ is the number of cycles to failure of a constant stress reversal S_i, failure occurs

Failures due to Cavitation: Cavitation is a phenomenon of vapour or bubble formations of flowing liquid, in a region where the pressure of the liquid falls below its vapour pressure. These bubbles will collapse when they pass into higher regions of pressures, causing noise, vibration and damage to many components. In case of fuel injectors, this kind of mechanism will eventually reduce the efficiency. Mostly cavitation occurs due to poor geometry design, and flow turbulences, etc.

7.2.2 Failure Due to Environment

Product failures may occur due to extreme oxidation or operation in corrosive environments. Certain environmental conditions accelerate the failure conditions.

For products which operate at high temperature environment it is very much important to consider thermal stresses, coefficient of expansion of materials. Constant temperature will not create thermal stresses. Transient conditions cause expansion and contraction of the material.

These factors (Corrosion, temperature) are all a function of time and magnitude.
Failures Due to Poor Manufacturing Quality

This is generally due to improper inspection of materials, casting defects, weld defects, heat treatment errors, cracks and defects in manufacturing. These reduce the allowable strength of the material and result in infant mortality failures. Poor heat treatment leads to improper material properties result into premature failure.

7.3 Reliability Circle

The development of an engineering product is a process with several steps such as defining functional, performance requirements, conceptual design, preliminary design, detailed design, validation of the product to customer specifications, manufacturing the product to design specifications, shipping the product to customer and last but not least is to take the feedback from product usage in the hands of customer to gain knowledge for further improvements or in future designs. This section explains the reliability activities in this product development life cycle and the decision making involved.

Product development is a decision-making process, and reliability constitutes one of the aspects that decisions are based on. Usually, it is the ability to meet criteria consistently, dependability, and trustworthiness. It is not a subjective parameter but rather a measurable parameter. Reliability is represented by the probability that the product will satisfy functional requirements during a specified period of time without failure under specified operating environments. Failure means any event that prevents the product from meeting its functional requirements. It may be catastrophic failures but also the performance deterioration below an acceptable level, i.e., vibrations, reduced efficiency, etc. Generally, neither manufacturing nor service stages can increase the inherent reliability of the product. The reliability of the product is built into its specifications and design process. If the Manufacturing process does not meet the drawing specifications, the reliability will be reduced. In this respect it is important to understand how reliability is built into the product design.

At conceptual design stage the system/product configuration is determined and also the system reliability requirements. Overall reliability can be increased by choosing a better configuration irrespective of the reliability of the individual components. The Product reliability specifications will be decided from customer requirements, competitive benchmarking and past experience with similar products.

At the preliminary design stage reliability engineer analyses the alternative designs and performs reliability modeling and reliability assessment. Only the components critical to the product functionality should be thoroughly analyzed. The design concept will freeze based on performance parameters like speed, flow rate, output, efficiency, etc., cost, reliability, maintainability and other constraints.

At the detailed design stage, reliability engineer anticipate the possible service conditions and reliability techniques will be implemented accordingly. The development of working drawings proceeds in parallel with the analysis of product performance based on finalized dimensions, materials, and configurations, and with experimental investigations of critical components. The reliability is estimated based on stresses, usage cycle, and environmental conditions under which the product is intended to operate. The discrepancy between the predicted reliability and the real life behavior of the product in the service is a reflection of the deviation between the state of knowledge and reality. Reliability engineers should minimize this gap.

At Design verification and validation stage, Reliability testing is necessary because designs are seldom perfect and because designers can not usually foresee, or be able to analyze, all the likely causes of failure of the product in service. To provide the basis for a properly integrated development test program, the design specification includes all criteria to be tested (function, normal environment, abuse conditions, safety). The development program should be detailed to validate all the customer specifications. Reliability test program cover the range of environmental conditions like temperature, vibration, shock, humidity, dirt, etc. Some tests are designed with combined environments.

During manufacturing stage, plans will be detailed to manufacture the product in conformance with the design specifications and decisions should be made with respect to manufacturing machinery, fixtures and tools to be used, assembly, and quality control system. Sound Quality assurance methods will be required to meet the inherent reliability specifications.

After the product is shipped to customer during service period, field performance data is collected to improve reliability prediction techniques and to develop more realistic expectations on products design life. The data is also useful for future product development programs. These reliability engineering activities during the product development process follows in a closed loop manner as shown in Fig. 7.7. It is a multifunctional department effort to deliver a reliable product to customer.

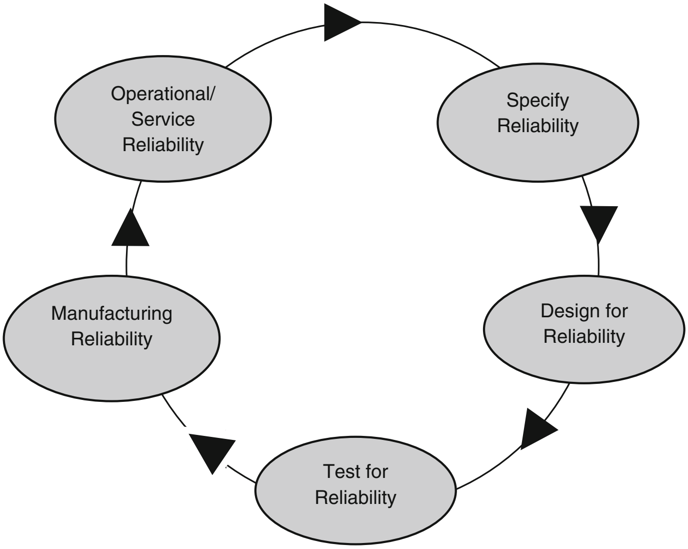


Fig. 7.7 Reliability circle

7.3.1 Specify Reliability

The first step in the reliability circle is to establish the reliability specifications/targets. It is essential that the requirements come from customer needs and wants and program objectives.

The following are the different methods to collect the reliability information: House of Quality (Customer needs and wants), customer surveys, benchmarking, customer duty cycles and environment, experience from similar existing products such as warranty data, etc. Gather the data from above sources and prioritize them to set the targets.

Reliability requirements are statements that detail functional, mission oriented requirements with minimum Life Cycle cost, resources and maximum probability of success. It is essential to understand the Reliability metric's customer impact & financial impact.

a. *Quality Function deployment (QFD)*— capturing the voice of the customer
   This is a tool to interface customer-marketing-design at the concept stage of new products/services.
   Objectives

   1. Determine customer's needs, requirements, and expectations before conceptual design is translated into prototype design.
   2. Let the customer rate each requirement in terms of importance and in terms of your performance on similar products versus those of your best competitors.

3. Based on the ‘House of Quality’ matrix, determine the important, the difficult, and the new aspects of your design.
4. Deploy product specifications into part specifications, process specifications, and production specifications using similar house of quality matrices.

   In QFD, on far left, the customers’ most relevant requirements (the what) are listed in order of importance. On the far right are the customers’ evaluations of each requirement, with a rating of your company’s performance versus competition. In the middle is a relationship matrix, comparing the linkage (strong, medium, or weak) between each customer requirement and each design specification (the how). A simple calculation then pinpoints those engineering specifications that must be concentrated on to meet both customer requirements as well as competitive strengths. At the bottom, there is a comparison of each specification against a target value and against competition, based on reverse engineering (competitive analysis). On the roof is a correlation matrix that shows whether each pair of engineering specifications has a reinforcing correlation or a conflicting correlation.

   Similar House of Quality matrices are developed to translate the, what of engineering specifications into the how of parts specifications, with similar translations cascading from parts to process, from process to production, from production to test, and from test to quality requirements.

b. *Reliability Measures* Although we speak of measuring the reliability, it is common to estimate the unreliability of equipment. Common Reliability Measures/Metrics are MTBF, MTTF, Road calls/day, Repairs for Hundred units in a year, B_{10} life, failure free operating period, Fatalities per trip etc. MTTF is typically used for non repairable items. If the products underlying life distribution is known it is very easy to calculate remaining parameters.

   Mean time between failures (MTBF) is defined as the reciprocal of the failure rate during the flat portion of the failure rate curve.

   MTBF = Total time of all units/ Total failures

   The unit of failure rate is ‘*failures per hour*’. The unit of MTBF is ‘*hours per failure*’. So it is easy to confuse ‘MTBF’ and ‘life’. The fact that a product has a product has an MTBF of one million hours does not imply that it will last one million hours. For example in case of projector lamp, the design life is specified as 800 h. During the period between 10 and 600 h very few burn out. In fact, the MTBF approaches one million hours. However, between 600 and 1000 h, all will burn out. Sometimes the reliability targets are associated with confidence limits. Ex: Target B_5 life for a fuel injection system is 5000 h with 70 % confidence.
c. *Environment and Usage* Environment and usage can kill the equipment, for example the following problems were experienced during Gulf war:

   - Engine life—Sand ingestion and high temperatures
   - Sand ingestion—everywhere
   - Differential expansion—clearance to interference fit
   - Small animal infestation

It is very important to get the knowledge of user environment and usage profile. In some cases all aspects in the user specification could not be identified.

d. *Reliability Apportionment* Reliability apportioning is an important task in the design and development of systems such as automotive systems (power train, chassis, electric system, etc.), aircraft systems (power management system, Landing gear systems, hydraulic system, high lift system, etc.). Following factors should be taken into consideration in the reliability allocation process.

Criteria that should be used in System Reliability Apportion

1. *Failure data* The failure data of assemblies/subassemblies of existing systems should be utilized in design of new system. The assembly that has a very low failure rate is already reliable. In the new design it is very likely to apportion a high reliability goal to this assembly. It is suggestible to improve the reliabilities of these assemblies proportionally in order to improve the reliability of a system in new design.
2. *Criticality* The criticality of failure of assembly represents the impact of its failure on the system, its surroundings, and/personal; For example, If the Nose landing gear system's failure may cause catastrophic damage to the aircraft, so that the criticality of the failure of this subsystem is high. This is the relative effect of each subsystem upon the achievement of the flight's mission objectives. The criticality of the subsystem has a direct relationship with reliability allocation. The subsystem with high criticality of failure should be allocated a high reliability.
3. *Maintainability* Maintainability is the inherent characteristics of the product related to its ability to be restored when the specified maintenance task is performed as required. The higher or longer the repair cost or down time, the worse the maintainability of the system is. The subassembly with poor maintainability is allocated a high reliability.
4. *Complexity* The complexity of an assembly is defined as the ratio between the number of essential parts within the assembly (whose failures will cause the assembly to fail) and the total number of such essential parts in the whole system. The assembly with low complexity should be allocated high reliability.
5. *Manufacturing data* The reliability goal specified by the designer for an assembly is assured through the manufacturing process. For an item that is produced with sophisticated manufacturing processes obviously can get very good Cpk, so it is relatively easy to assure reliability. For the item there is no good manufacturing process means lower Cpk values, it is difficult to assure high reliability. So, the item which produced with sophisticated manufacturing process should be allocated a high reliability.
6. *Operating environment* This represents the temperature, moisture, vibration, electromagnetic interference, contamination, corrosion, UV and so on under which the item has to work. If the item operates in a worse condition, it is very difficult to guarantee its reliability. For the items which operate in nice and known environments should be allocated with high reliability.

7. *Cost* The sensitivity of cost to reliability could be should be taken into account when improving the reliability of a particular assembly. The cost sensitivity to reliability is defined as the ratio $\frac{C_2 - C_1}{R_2 - R_1}$ of the cost increment $(C_2 - C_1)$ and the reliability increment $(R_2 - R_1)$. The higher the cost sensitivity to reliability, the more cost to improve reliability of the subsystem. The assembly with low cost sensitivity to reliability should be allocated a high reliability.

7.3.2 Design for Reliability

Design for reliability guidelines assist the engineers with a rule driven system to achieve an inherently more robust design to improve the performance over time of products and processes under customer usage and manufacturing process conditions.

Design for reliability objectives are Identification of failure modes and preventing them or minimize the effects of these failure modes. It is possible by successful implementation of the techniques such as Failure mode and effects analysis, Fault tree analysis, stress analysis, reliability modeling, design of experiments, root cause analysis techniques and by implementing redundancy in the design. The reliability will be built into product by providing safety factors to the design.

The other objective is reduction of variability in presence of the noise. It is achieved by applying design of experiments, parameter design and tolerance design during product design.

The first major tool to be used is Failure Modes and Effects Analysis (FMEA). This is an important tool to ensure that reliability is integrated with product design. The FMEA tool can identify both specified and unspecified customer requirements for a design, how failure may occur, the severity of such failure, and the probability of the failure occurring. With these factors identified, we can focus the design process on the major issues of the product and its potential use environment.

Reliability modeling is used to make initial product Reliability or failure rate estimates. These estimates are important in understanding the feasibility of a design's capability of meeting the reliability goals needed to satisfy customer requirements. Also, such calculations direct and assist in the determination of design tradeoffs to ensure that the best design approach is taken.

Example 1 Calculate the Reliability of an actuator (Fig. 7.8)? Reliabilities of cylinder, piston, Rod end, and piston seal at 50,000 flight cycles are 0.992, 0.99, 0.995, and 0.97.

Solution: Since all the components are essential for the successful extension and retraction of the actuator, all the components fit in a series reliability model. So,

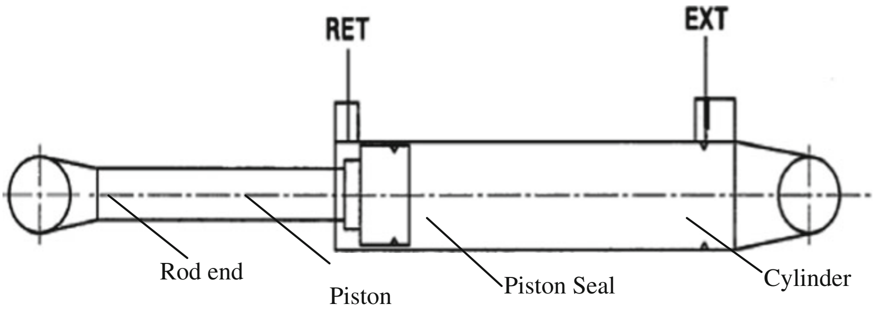


Fig. 7.8 Simplified actuator

$$
\begin{aligned}
R_{\text{Actuator}} &= R_{\text{Cylinder}} \times R_{\text{piston}} \times R_{\text{Rod end}} \times R_{\text{piston seal}} \\
&= 0.992 \times 0.99 \times 0.995 \times 0.97 \\
R_{\text{actuator}} &= 0.9479 \text{ @50,000 flight cycles}
\end{aligned}
$$

Example 2 A system has 12 components. Components 1 through 8 are different and have reliabilities 0.98, 0.99, 0.992, 0.975, 0.984, 0.978, 0.96, 0.995 respectively. Components 9 through 12 are the same, with reliability of 0.95. Components 4, 5 and 6 are critical, and each must operate for the system to function. However, only one of the components 1, 2, and 3 has to perform its function and the same for 7 and 8. At least two of the four identical components must work, as well. Diagram the system and find the probability the system survives.

Solution: The block diagram is shown in Fig. 7.9.

Reliability of components 1 to 3 is:

$R_a = 1 - (1 - R_1) \cdot (1 - R_2) \cdot (1 - R_3) = 1 - (1 - 0.98) \cdot (1 - 0.99) \cdot (1 - 0.992) = 0.999998$

Reliability of components 4 to 5 is:

$R_b = R_4 \cdot R_5 \cdot R_6 = 0.975 \times 0.984 \times 0.978 = 0.938293$

Reliability of component 7 to 8 is:

$R_c = 1 - (1 - R_7) \cdot (1 - R_8) = 1 - (1 - 0.96) \cdot (1 - 0.995) = 0.9998$

Reliability of components 9 to 12 is:

$R_d = 4C_2\, R^2(1 - R)^2 + 4C_3\, R^3(1 - R) + R^4 = 6 \times 0.95^2 \times (1 - 0.95)^2 + 4 \times 0.95^3 \times (1 - 0.95) + 0.95^4 = 0.9995$

Total reliability of the system = $R_a \times R_b \times R_c \times R_d = 0.9377$

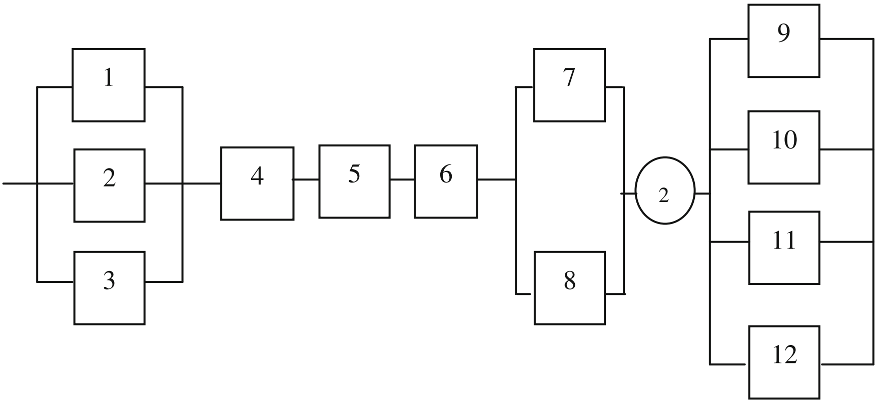


Fig. 7.9 Block diagram of system

7.3.2.1 Reliability Analysis and Prediction

Performing a reliability prediction provides visibility of reliability requirements in the early development phase and an awareness of potential failure modes during products life cycle.

Databases such as MIL-HDBK-217 were available for electronic components, NPRD (Nonelectronic parts reliability data notebook) contain failure rate and failure mode information for mechanical and hydraulic parts under the field conditions in military, industrial and commercial applications. This kind of database information is very helpful while the design is still on the drawing board.

In many cases similar type of components can exhibits different failure rates in reality due to their application use, it would difficult to use published data base like NPRD (Nonelectronic parts reliability data notebook) for failure rates.

There are several characteristics which contribute to differences in failure rate for mechanical components.

a. Mechanical components such as gearboxes, Landing gear locks, and fuel injection pumps, pistons, etc. often perform multiple functions. It would be rare to find the failure data for each failure mode for specific application.
b. Failure modes such as wear, fatigue, corrosion, etc. do not follow constant failure rate distribution because of cumulative damage in nature.
c. Mechanical components failure rate varies due to variable stresses, usage pattern, modes of operation.
d. Failure definition is more critical for mechanical components. For example, failure due to excessive noise, or failure due to leakage. It can be interpreted differently at the product level, subsystem level or system level. Data banks do not provide such kind of information.

Reliability analysis and prediction starts with identification of failure modes, component level failure effects, subsystem level failure effects, system level failure effects, critical safety and regulatory issues, and maintenance actions. Each failure mode can have multiple failure causes/failure mechanisms. Reliability Engineer has to estimate failure rate for each failure cause. All of these failure modes such as corrosion, erosion, creep, cavitation, vibration and fatigue operate on the component simultaneously which effects reliability of the component. Again, stresses on the component may be static, cyclic with varying degrees, and transient behavior also affects the durability of the mechanical components. Other these items which can complicate reliability predictions are material properties variability, process parameters variability, operating conditions such as temperature, vibration, different fuels/liquids.

The reliability of mechanical parts is computed by:

1. Developing a failure rate model for each component
2. Probabilistic stress and strength theory for a particular failure mode

Failure rate model for a component involves the use of large scale data collection from the field or controlled test data, which will be used to derive a relationship between design and generic reliability factors and developing factor for adjusting the reliability to estimate field reliability for the required application.

The general form of expression to compute part failure rate is [12]

$$\lambda_{\mathrm{part}} = \lambda_{\mathrm{base}}(\pi_{\mathrm{e}}, \pi_{\mathrm{A}}, \pi_{\mathrm{Q}}, \ldots \pi_{\mathrm{in}}) \tag{7.2}$$

where, λ(lamda) part is the part failure rate.

The reliability prediction model for a failure mode is based on the following parameters:

1. Component to component variation
2. Variation in dimensions, strength over a period of time
3. Variation in usage/application
4. Variation from external environment (climate and operating environment)
5. Variation from internal environment created by stresses from neighboring components

Stress-Strength interference model is developed using the above parameters to predict reliability.

Failure Rate Model for Compression Spring

Spring is a device used to exert force, provide flexibility, and to store or absorb energy. Spring's application may be static, cyclic, variable, light duty or heavy duty. Reliability of a spring depends on material, its design characteristics, and operating environment.

Table 7.2 Failure modes for spring

Failure mode	Failure causes
Fracture	Material flaws
	Hydrogen embrittlement
	Surface roughness
	Misalignment
	Excessive loading
Wear	Material defect
	Improper surface finish
	Misalignment
Loss of spring rate (Set)	Material defect
	Excessive loading
	Fatigue

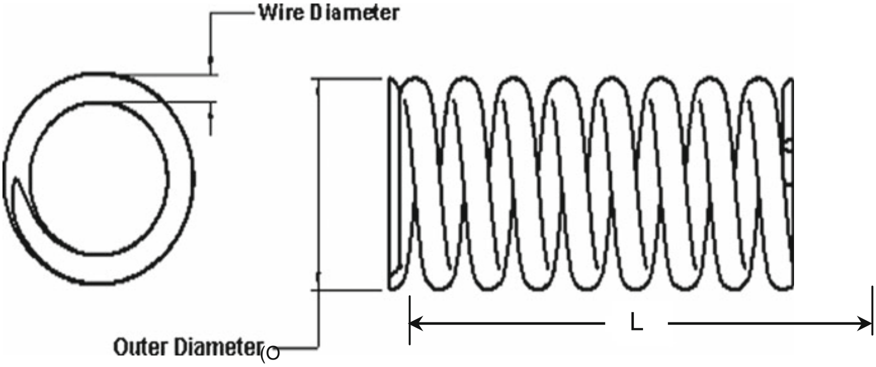


Fig. 7.10 Helical compression spring

Table 7.2 shows failure mechanisms and causes of spring failure. Typical failure rate considerations include: level of loading, loading frequency, operating temperature and corrosive environment.

The following example describes the failure rate model for a compression spring (Fig. 7.10). The details of physical and mathematical concepts of Spring can be seen in references [6, 7].

The spring failure rate depends upon the stress on the spring and the spring rate provided by the material. The spring rate (change in load per unit deflection), 'k' for a compression spring is calculated using Eq. 7.3.

$$k = \frac{P}{f} = \frac{Gd^4}{8D^3 N_a} \tag{7.3}$$

where

k Spring rate, N/m

G Shear modulus, N/m^2

d Wire diameter, m

D Mean diameter of spring, m

N_a Number of active coils

P Load, N

F deflection = $L_1 - L_2$

L_1 Initial length of spring, m

L_2 Final deflection of spring, m

Torsional stress 'S' is proportional to the load, P according to the following expression:

$$S = \frac{8K_w PD}{\pi d^3} \tag{7.4}$$

where

S Torsional stress, N/m^2

K_w spring stress factor

D mean coil diameter, m

d wire diameter, m

The spring stress correction factor, K_W *is* a function of the spring index (ratio of the coil diameter to wire diameter).

$$K_w = \frac{4C - 1}{4C - 4} + \frac{0.615}{C} \tag{7.5}$$

where: C = spring index = D/d

Stress can be calculated from Eqs. (7.2) and (7.3), and the ratio of stress to the material tensile strength gives failure rate of spring (Ref. 7):

$$\lambda = \lambda_b \left(\frac{S}{TS}\right)^3 = \lambda_b \left(\frac{kfDK_w}{TS * d^3}\right)^3 \tag{7.6}$$

where: λ = Failure rate of spring, failures/million hours

λ_{b} Base failure rate for spring

TS Material tensile strength, N/m^2

Base failure rate is calculated from field data, in the absence of field data it is calculated from experimental data.

The above equation is modified to a generic equation that adjusts the base failure rate of a compression spring for different operating conditions.

$$\lambda = \lambda_b \cdot \pi_G \cdot \pi_d \cdot \pi_D \cdot \pi_N \cdot \pi_{TS} \cdot \pi_f \cdot \pi_{Kw} \cdot \pi_r \cdot \pi_e \cdot \pi_q \tag{7.7}$$

where,

π_G Multiplying factor which considers the effect of shear modulus on base failure rate

π_d Multiplying factor considers the effect of wire diameter on base failure rate

π_D Multiplying factor considers the effect of coil diameter factor on base failure rate

π_N Multiplying factor considers the effect of number of active coils on base failure rate

π_{TS} Multiplying factor considers the effect of tensile strength on base failure rate

π_f Multiplying factor considers the effect of spring deflection on base failure rate

π_{Kw} Multiplying factor considers the effect of spring stress correction factor on base failure rate

π_r Multiplying factor considers the effect of application spring cycle rate on base failure rate (normally > 0.1)

π_e Multiplying factor considers the effect of environment on base failure rate

π_q Multiplying factor considers the effect of manufacturing Quality on base failure rate

The parameters in the failure rate equation can be taken from the engineering knowledge or by actual measurements. Other duty cycle, manufacturing, quality, and maintenance contributions to failure rate can also be included to the base failure rate equation as the experience grows.

For example, if a music wire of diameter 0.08 is fatigue tested with a cycle rate of 250 cycles/min produced a failure rate of 2.5×10^{-5} failures per hour.

The $\pi_{d,}$ π_r for a helical spring having a diameter of 0.09 operates at 250 cycles/min is calculated as,

$$\pi_d = \left(\frac{d}{0.08}\right)^3 = \left(\frac{0.09}{0.08}\right)^3 = 1.424$$

$$\pi_r = \left(\frac{r}{250}\right)^3 = \left(\frac{250}{250}\right)^3 = 1$$

Environmental Effects

Corrosion will reduce the fatigue strength limit of a spring. Corrosion is a progressive type failure mode. When fatigue is combined with progressive mode of

Corrosion, spring may fail prematurely. In non-corrosive environments, cyclic loading frequency generally has little effect on fatigue behavior of a spring. On the other hand, fatigue behavior is strongly dependent on frequency in corrosive environments. The corrosion fatigue strength decreases with decreasing frequency and the fatigue crack propagation rate becomes faster at low frequencies.

The exact results of corrosive environment on spring functionality is difficult to predict, also the reliability is difficult to quantify. If a spring is to be subjected to a corrosive environment, selection of material, design, fabrication and processing of spring material are best control measures against corrosion. Design and Material selection can be based on environment, stress, compatibility, movement, and temperature. Protective coatings such as zinc cadmium, chrome plating and rust inhibitors such as phosphates, chromates, etc. can also be applied. In special situations, galvanized wire before coiling, shot peening, in case of stainless steel springs cleaning springs before applying stress relief can be used to prevent stress corrosion.

Fatigue failures can also happen as a result of electrical fields, which may magnetize the spring material.

Multiplying factor, π_e of 1.0 is used in conjunction with the base failure rate, if the design takes into consideration of the above guidelines. Values of π_e greater than 1.0 are used based on in-house historical data with the spring and the operating environment.

Quality Factor

Burrs, sharp edges during wire forming process has to be minimized. Also, dings, nicks, dents can occur during handling, these can reduce fatigue life. The hardness of the spring material can be sensitive to heat treat process. Quality control procedures for these operations should be reviewed. A multiplying factor, $\pi_{q,}$ of 1.0 should be used in conjunction with the base failure rate for known acceptable quality control procedures (Such as Cpk > 1.33); otherwise a higher value for the multiplying factor should be used based on previous experience with the manufacturer.

Reliability Prediction of Bearings

From the stand point of reliability, bearings are among the few components that are designed for a finite life because of the fatigue properties of the materials used. Most bearings can be assigned a B_{10} life, which is the number of time units (Hrs or Cycles) at a specified load that 90 % of bearings of similar type will complete or exceed. Usually Lundberg-Palmgren method is used to calculate the B_{10} life. There are a number of other factors that can be applied to the B_{10} life so that it more accurately correlates with the intended operating environment. These factors include material, process parameters, lubrication film thickness, misalignment, speed, loading type and subjection to contaminants.

The Lundberg/Palmgren bearing equation for B_{10} life is:

$$B_{10} = ((C/P)^{a} \cdot 10^{6} \text{ revolutions} \tag{7.8}$$

where C dynamic capacity of the bearing,
P equivalent load
a 3 for Ball bearings, 3.3 for Roller bearings

Bearing Failure Modes

The common bearing failure modes, mechanisms and causes are listed in Table 7.3. The most common mechanism of bearing failure is spalling/flaking. It is the consequence of fatigue. Excessive loading and inadequate lubrication will lead to failure of bearing. When flaking has proceeded to a certain state, vibration or noise can be felt. This is the warning sign. Indents, scratches deep gouges are usually caused by hard abrasive particles, being trapped in bearing or foreign debris ingress. This failure mechanism may be caused by inadequate sealing, debris in the lubricant, or installation damage.

Roller and tapered bearings have other failure mode defined as scuffing of the bearing surfaces, this is caused by metal to metal contact. Initially it starts at microscopic level, removal and transfer for material from one component to the mating components and then progresses steadily once it start.

Table 7.3 Failure modes of bearing

Failure mode	Failure mechanism	Failure cause
Wear	Abrasive particles (foreign ingress)	Lubricant contamination
		Excessive load
		Vibration
Fatigue damage	Flaking or spalling of ball/roller raceway	Excessive load and speed
		Impact loading
	Brinelling	Vibration, shock
	Smearing	Improper lubrication
		Excessive contact stress
Noise	Surface fatigue	Improper lubrication
	Micro spalling of stressed surfaces	Housing bore out of round distorted bearing seals
Seizure	Crack formation races or balls/rollers	Inadequate heat removal capacity
		Inadequate lubrication
		High temperature
		Excessive loading and speed
Vibration	Scuffing pitting of surfaces	Misalignment, excessive loading/unbalanced load
Corrosion		

Overfilling a bearing with too much grease can lead to excessive churning and high temperature during operation. Overheating is indicated by surface discoloration (blue/brown). This situation happens when the generated heat can't dissipate correctly.

Failure Rate Prediction of Bearing

Bearing fatigue life estimation is combination of large number of design parameters in relation to the sensitivity of the operating environment. Statistical methods are used to calculate the failure rate, B_{10}, B_5 life of bearings based on the laboratory testing results of large groups of the same type of bearing. B $_x$ life, is defined as the time (hours/cycles/mileage) at which (100-x) % of the bearings operating at their rated load and speed, can be expected to complete or exceed before exhibiting the first evidence of fatigue.

Many developments took place in quality of materials and manufacturing since the original development of the B_{10} concept to predict the bearing life. For instance, materials with high cleanliness levels that are vacuum degassed or vacuum melted are now widely used for bearings. Also, bearing components are manufactured to higher precision standards for geometry, surface finishes. Because of these variables, bearing manufacturers have modified their B_{10} ratings with correction factors. To evaluate a manufacturer's bearing for reliability, it is best to utilize the published B_{10} life and modify it according to the particular application. The following is an expression for predicting the failure rate of bearings:

$$\lambda_{Bearing} = \lambda_{base} \cdot \pi_y \cdot \pi_A \cdot \pi_v \cdot \pi_c \cdot \pi_t \tag{7.9}$$

$$\lambda_{Bearing} = \lambda_{base} \cdot \left(\frac{L_S}{L_A}\right)^y \left(\frac{A}{0.006}\right)^{2.36} \left(\frac{v_O}{v_L}\right)^{0.54} \cdot \pi_c \cdot \pi_t \tag{7.10}$$

where

π_y Multiplying factor for applied load
π_v Multiplying factor for lubricant
π_c Multiplying factor for water contaminant level
π_t Multiplying factor for operating temperature
A Angularity error, in radians

Loading Factor: $\pi_y = \left(\frac{L_S}{L_A}\right)^y$, multiplying factors for the effect of lubrication viscosity on the failure rate of bearing is shown in Fig. 7.11

Lubricant Factor: $\pi_v = \left(\frac{v_O}{v_L}\right)^{0.54}$, multiplying factors for the effect of lubrication viscosity on the failure rate of bearing is shown in Fig. 7.11

Alignment Factor: $\pi_A = \left(\frac{A}{0.006}\right)^{2.36}$, multiplying factors for the effect of lubrication viscosity on the failure rate of bearing is shown in Fig. 7.11

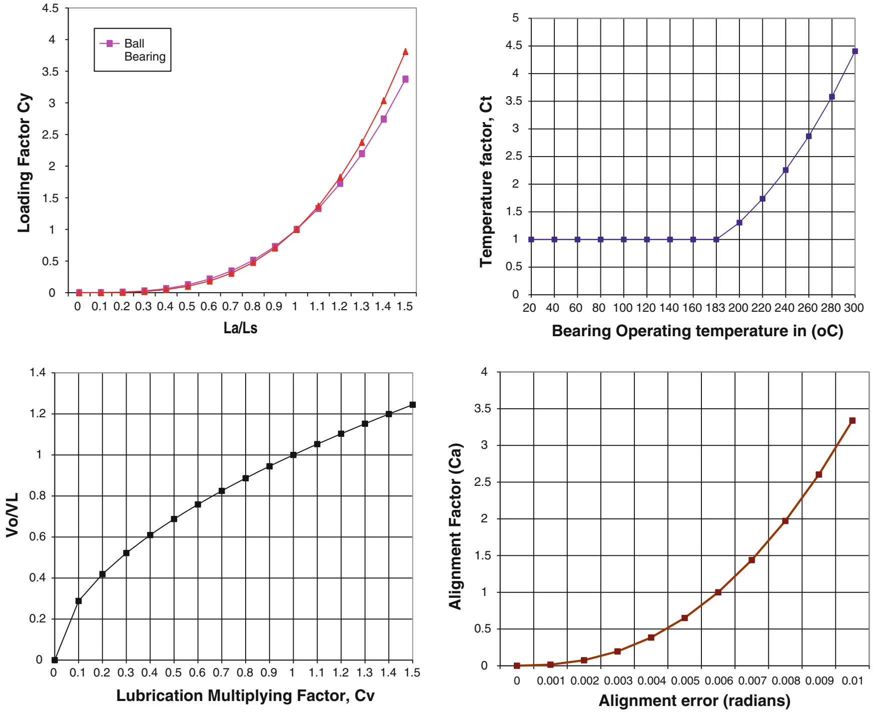


Fig. 7.11 Factors affecting the failure rate of bearings: **a** loading **b** temperature **c** lubrication**d** alignment

Contamination Factor

Water contamination has a detrimental effect on fatigue. A water contamination multiplying factor takes into account of bearing life degradation. This factor is represented by the following equations derived from data in Ref. [8].

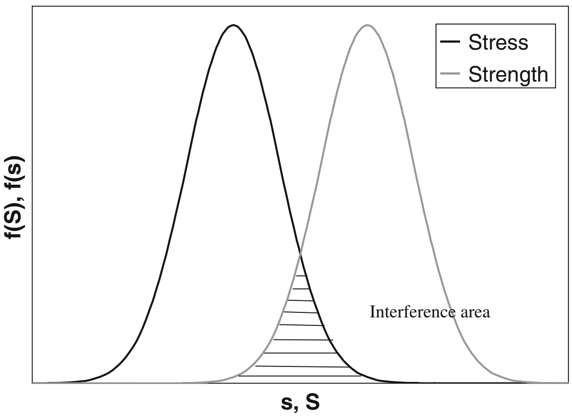
$$\pi_c = 1.04 + 1.03 * (\%\,\text{of water in lubri.}) - 0.065 * (\%\,\text{of water in lubri.})^2 \quad (7.11)$$

y 3.0 for Ball Bearings; 3.3 for Roller Bearings
L_A Equivalent radial load, lbs
L_S Bearing load capacity, lb
v_O Specification lubricant viscosity, lb-min/in^2
v_L Operating lubricant viscosity, lb-min/in^2

7.3.2.2 Stress-Strength Interference Theory

Normally safety factor is calculated considering strength of the material and stresses acting on the component. In reality both of these are not deterministic quantities,

Fig. 7.12 Stress—strength relationship



but are random variables. Both can be represented by Probability distributions as shown in Fig. 7.12. The reliability is calculated as the probability that the strength will exceed the stress.

$$R = P(S > s) = P\ (S - s) > 0 \tag{7.12}$$

where:

R Reliability
P Probability
s Stress random variable
S Strength random variable
$\overline{S}$ mean of the component's strength
$\bar{s}$ mean value of the load imposed on the component
σ_S Standard deviation of the component's strength
σ_s Standard deviation of the stresses imposed

Standard deviation is a simple measure of the variation of attributes like stress, strength, etc. about its mean value.

Interference area

If these pdf's are completely separated means there is no interference between them, then it is an absolutely reliable component.

If, however, the pdfs of both strength and stress are shown to interfere, in that they intersect one another, as shown in Fig, then there is a probability the load applied to an individual component will exceed the strength of the component, and it will fail. The numerical value of this probability is a function of the area of the overlap, and the larger the area of overlap the higher the probability that the component will fail.

Reliability depends on variance and mean values of the distributions of strength and stress. For the same safety factor, reliability may be different depending on the variance. It is clear that the reliability decreases as standard deviation increases.

Reliability can be improved either by increasing the mean value or by decreasing variance of strength, but higher variance causes product-to-product variability which is perceived as a sign of poor quality by the customer.

An established method, related to strength and stress interference, used in design, is the use of safety margins. When designing reliability into a component the term 'safety margin' (SM) takes on a special meaning and is calculated by the following formula:

$$SM = \frac{\overline{S} - \overline{s}}{\sqrt{\sigma_S^2 + \sigma_s^2}} \tag{7.13}$$

The steps to estimate the reliability using Stress-Strength interference approach are,

a. Identification of Failure Modes or Failure mechanisms (mechanical (static/dynamic), chemical, electrical, physical, structural or thermal) of the component
b. Identification of appropriate failure models means Stress/Strength Characteristics
c. Identification of Design Parameters for stress and Strength
d. Collect the appropriate data to calculate the statistics for stress and Strength.
e. Calculate the Reliability and safety Margin of the design.

Identification of Failure Modes or Failure Mechanisms for the Component
The 'Failure Mode and Effects Analysis' identify failures, which alone or in combination have undesirable or significant effects on the product performance and safety. Subsequently it identifies the potential causes for the failure modes upon which the designer can take actions to eliminate the failure modes or reduce their severity on the product performance.

FMEA takes into account of Historical failure information from all available sources, such as warranty, internal test reports, Supplier testing reports, benchmarking, etc. Failure modes are then prioritized based on severity/customer satisfaction impact and other requirements.

Table 7.4 Typical stress/strength characteristics

Stress	Strength
Mechanical stress	Ultimate tensile, yield strength
Cyclic stress	Endurance limit of the material
Temperature	Material properties, thermal coefficient of expansion
Corrosion	Material selection, coating thickness, corrosion resistance
Impact load	Energy absorption capability
Wear/pitting	Contact strength

For example:

1. A large impacting load during the aircraft landing may cause a bogie beam failure
2. Cyclic loads from different types of roads may cause fatigue failure to the body structures, the initial cracks in the components, such as in engine, chassis, and body structure may cause fracture failure.
3. The corrosive environment deteriorates the components and its load-carrying capacity.

Identify the Appropriate Failure Models (Stress/Strength Characteristics)
In the stress/strength interference approach, Stress includes mechanical stress (tensile, compression, etc.), strain, thermal loads, contact stress, etc. The strength includes material strength (yield, ultimate), stiffness, and absorption capability. Table 7.4 shows typical stress/strength characteristics.

Identification Design Parameters for Stress and Strength
The design parameters are those factors, which considered during the design stage of product. These design parameters are specified in the drawings. These factors affect either the strength or stress of the system.

Example: Gear design factors, which affect the stress, are cyclic loads, duty cycles, and the speed at which gear operates.

The design factors, which influence the strength are the bending strength, number of teeth, pitch diameter, lead angular error, adjacent pitch error and profile error, etc.

Collect the Relevant Data and Calculate the Statistics for Stress and Strength
Most of the design parameters are not deterministic and have inherent uncertainty because of variation in the material properties, component geometry, dimensions (diameter, thickness, etc.), manufacturing or assembly process, heat treatment and loads, etc. Aging is also a very important factor in causing variation in design parameter values. Stress related data can be gathered from the customer usage profiles. In general the duty cycle developed for product validation should represent at least 95 % of customers' usage. Strength data is gathered from in-lab test, manufacturing audit reports, control charts, etc.

Such data is plotted to some statistical distribution to calculate the required statistics (ex: Mean, Standard deviation).

Reliability and Safety Margin Calculation
After identifying and collecting the data of design parameters, Stress and strength should be modeled as a function of these parameters. In most of the times it is a tedious task, software analysis techniques can be used.

For example there are standard Gear life calculation programs from SAE (Society of Automotive Engineers) or AGMA (American Gear Manufacturers Association) are commercially available. Monte Carlo simulation is used to evaluate the stress and strength parameters to obtain a distribution of gear life values. These values will be plotted using appropriate statistical distribution.

If the calculated failure rate does not meet the target specifications, Based on the reliability model, Reliability engineer selects the parameters which affect the failure rate and take appropriate actions like change of material, or by tightening manufacturing quality procedures, etc.

7.3.3 Test for Reliability

Reliability Test Objectives

Reliability data is commonly obtained from laboratory tests, evaluation and qualification tests, and acceptance tests. Reliability tests are designed with the objectives of,

1. Gathering the data which is necessary to measure or demonstrate reliability with the degree of statistical confidence, and the given design is truly acceptable for its intended application,
2. Determining a corrective and preventive maintenance program required to keep the equipment in satisfactory operating condition,
3. Provide data which indicate necessary design modifications or operational procedures and policies especially as they influence reliability and maintainability,
4. Verifying the reliability analyses previously performed, and effectiveness of design improvements done in design reliability
5. Determining
    i. Warranty period that will enhance sales while assuring reasonable profile
    ii. Maintenance/overhaul intervals to plan the relevant maintenance activities.
6. Providing information which can be used in later activities.

Types of Testing

Failure Mode Identification testing (FMIT): Failure mode identification testing method is able to use as few as one prototype. The method is used to establish multiple design inherent failure modes, rank the failure modes and estimate the potential for improvement in the design. The outcome of this test is a matured Design.

Highly Accelerated Life Testing/Over Stress testing: is a type of failure mode identification test, which use one/two samples to establish multiple design inherent failure modes, and establish operating and destruct limits of a product.

Reliability Demonstration Testing: Multiple samples are tested for known duration for example, one equivalent life or 3 times the design life, etc. with all known stress sources present. The outcome of the test is reliability prediction, and target reliability achievement.

Reliability Test Program

A reliability test program is a dynamic procedure, which changes and evolves with the needs of design and development efforts. The first step is the preparation of a comprehensive plan detailing the specific requirements of each category of testing and described the testing responsibility of this departments involved. This plan should have sufficient flexibility to allow modification as the program progress.

A major input to preparation of the test plan is a review of available data pertinent to the specific product. Such data may satisfy some of the test objectives and also may pinpoint potential trouble areas.

A test procedure must be prepared for each nonstandard part, material, subcontracted unit, assembly, subsystem, and for the system itself. This procedure has step-by-step approach so that a given kind of test provides a basis for estimating and scheduling the test program.

The major elements of a test are:

1. *Objective*: why is the test conducted? In most of the projects requirements are often intended for overall equipment. These must be modified to suit individual unit. Incomplete resolution leads to conflicts.
2. *Performance Criteria*: What is considered to be acceptable performance? Define the failure?
3. *Location and Test Equipment*: where the test will be conducted? What type of test rigs used?
4. *Sample*: what was tested? System or subsystem or unit? How many samples are tested? Is the sample size adequate to demonstrate reliability with adequate statistical confidence level?
5. *Time*: How long the test will be conducted? Are all test samples need to be tested for same time? Or it will be a bogie test?
6. *Conditions*: What are the usage conditions to which the product is exposed? Does the test cycle represent 95 % of customer duty cycles? Is it required to test under multiple environmental conditions? Or, is it necessary to perform sequential test? Must it perform one or more functions during each usage during or after each exposure? What are the environmental conditions associated with each usage condition? What kind of stresses can cause failure modes?
7. *Results*: Is the performance acceptable? Did the test generate any failures? How the data analysis will be done? Find the appropriate statistical distribution?
8. *Recommendations*: If the target reliability doesn't meet, what are the corrective actions to improve design reliability?

These are further explained in a different manner as below, since the product failures are due to lack of robustness, the stresses induced by variation in hardware, conditions of use, and environment. Authors suggest to refer [9] for additional details on this approach.

1. Piece to piece variation of part dimensions and material properties
   The test should be conducted on a large enough sample size, using statistical theory, to replicate 'piece to piece variation'.
   Sample size:
   The sample size is determined by the desired confidence level but this is often modified, sometimes rather drastically, by the allowable cost and the time available to run the test program. Sometimes Customers will specify the confidence level goals in the Reliability target specification.

Example 3 How many numbers of shaft seals need to be tested to demonstrate a B_5 life of 1000 h with 80 % confidence? Shaft Seal life follows Weibull distribution with shape parameter 1.3 and the test time is limited to 500 h.

Solution: The reliability expression to demonstrate reliability when zero failures are allowed:

$$R(t) = \exp\left[\frac{\ln(1-\alpha\%)}{\sum_{i=1}^{k}\left(\frac{T_i}{t}\right)^{\beta}}\right]$$

Here,

Test Goal = t = 1000
Testing time = (T_i) = 500
R(1000) = 0.95
α = 80 %

$$0.95 = \exp\left[\frac{\ln(1-0.8)}{n\left[\frac{500}{1000}\right]^{1.3}}\right]$$

By solving the above equation, n = 77.25
So, 77 seals need to be tested for duration of 500 h, without any leakage or degradation to demonstrate B_5 life of 1000 h with 80 % confidence.

2. Changes in geometry or Degradation of strength over time/mileage/flight cycles (i.e., wear out and fatigue)
   The test should be designed to generate the 'variation in changes in geometry or strength over time/mileage/flight cycles'. If this factor cannot be simulated, For example by performing a test on parts that are already worn, or have been manufactured to represent the worn parts. To illustrate this, It is well known fact that Teflon seals used in a fuel injection pump produce wear on the drive shaft, So it is important to perform a test on worn out shafts to find out the degradation effects. Such kind of situation occurs during warranty part replacement or service replacement.

Table 7.5 Testing on oil seal

Noise parameter	Considerations during the ‘oil seal’ test
Piece to piece variation	‘5’ Seals
Changes in geometry or degradation of strength over time	Test continued till failure on all samples and analyze its geometry, physical properties, etc.
Customer usage and duty cycle	1. Speed is cycled from 30 to 3000 rpm for every 30 min.
	2. Testing in the oil used by the customer (different brands/grades)
External environment	Temperature: −20 to 100 °C, dust
Internal environment	Variations from the matting components is taken in the form of,
	Run-out on shaft = 0.25 mm
	Perpendicular offset = 0.25 mm

3. Customer usage and duty cycle
   Generally the test cycle is derived from 95 % of customer’s usage profile. For example: Vehicle manufactures collect the real time stress and strain data of a chassis frame by installing the strain gauges at critical locations by driving the vehicle at different customer operated terrains.
4. External environment
   These factors reflect the basic test cycle. External environmental data such as temperature, humidity, and EMI, etc. will be considered during the testing.

5 Internal environment created by stresses from neighboring components.
This factor based on the specific application. This source of noise often gets ignored and paying attention to this noise factor can make the biggest gain in test efficacy, and hence contribution to the reliability of the wider system.
To obtain the maximum benefits from the reliability test, it should contain:

1. Simultaneous combination and interaction of different types of physical simulation of real action (environment, vibration, mechanical, electrical, etc.) on the actual car components.
2. Providing each type of above action (testing) as a complicated simultaneous combination of different types of simulation. For example, the environment testing of the ECU (Electronic control unit) used in car does not envisage not only the temperature and humidity, but also the simultaneous combination of the temperature, humidity, dust, radiation, electromagnetic field, etc.
3. Providing each type of influences simulation as a complex process, which is accurately similar to real life.

Table 7.5 shows the example of testing an Oil seal used in a gear box. All the five noise parameters were considered during the reliability test, to demonstrate B_{10} life of 1000 h.

Table 7.6 Models for generating pseudo failure times

Model	Expression
Linear	$Y = A \cdot X + B$
Exponential	$Y = B \cdot e^{AX}$
Logarithmic	$Y = A\ LN(X) + B$
Power	$Y = B\ X^{A}$

7.3.3.1 Degradation Data Analysis

High reliability systems require individual components to have extremely high reliability for a long time. Often, the time for product development is short, imposing severe constraint on reliability testing. Traditionally, methods for the analysis of censored failure time data are used to extrapolate mission reliability from the longest test times-even though there may be few observed failures. This significantly limits the accuracy and precision of the conclusions, motivating us to search for better methods.

Many failure mechanisms can be traced to an underlying degradation process. Degradation eventually leads to a reduction in strength or a change in physical state that causes failure. Degradation measurements, when available, often provide more information than failure time data for assessing and providing product reliability.

The basic approach is generate pseudo failure times for unfailed units by extrapolating their degradation paths using some of the following models, in Table 7.6.

where Y represents the parameters like wear, performance, quality levels, etc.

X represents duration, and
A, and B are model parameters to be solved for.

Once the model parameters A_i, B_i are estimated for each sample i, a time, X_i, can be extrapolated, which corresponds to the defined level of failure Y. The computed x_i values can be used as times-to-failure for subsequent analysis.

Some advantages of using relevant degradation data in reliability analysis over, or in addition to traditional failure data, are:

1. More informative analyses-especially when there are few or no failures.
2. Useful data often become available much earlier.
3. Degradation, or some closely related to surrogate, may allow direct modeling of the mechanism causing failure, provides more credible and precise reliability estimates and establishes a firm basis for often needed extrapolations in time or stress.
4. Degradation data may increase physical understanding, and there by, enable earlier rectification of reliability issues.

7.3.4 Maintain the Manufacturing Reliability

The purpose of this step is to maintain the quality of the product to ensure functional performance over time. In order to achieve it the manufacturing process need to be monitored continuously, if any problems are identified during process capability studies, it need to be fixed.

No amount of good manufacturing can fix a poor design. On the other hand, poor manufacturing can ruin the best of engineering design. Therefore there are three requirements for achieving a reliable product:

1. The design must have margin with respect to the stresses to which it will be subjected during manufacturing and actual field use.
2. The manufacturing process must be stable and completely documented. Variations from the “tried and true” must be considered experimental until proved.
3. There must be an effective feedback and corrective action system, which can identify and resolve problems, quickly, in engineering, manufacturing, and field.

Process Control Methods

Process FMEAs (PFMEAs) can be used to examine the ways the reliability and quality of a product or service can be jeopardized by the manufacturing and assembly processes. Control Plans can be used to describe the actions that are required at each phase of the process to assure that all process outputs will be in a state of control. Factory Audits are necessary to ensure that manufacturing activities (such as inspections, supplier control, routine tests, storing finished products, Measurement System Analysis and record keeping) are being implemented according to requirements.

The manufacturing process is also prone to deviations. The reliability engineer ought to communicate to the production engineer the specification limits on the KPVs (Key Process variable) that would define a “reliability conforming” unit. The production engineer is then responsible for ensuring that the manufacturing process does not deviate from the specifications. Here more aspects of reliability engineering discipline merge with quality engineering. Statistical Process Control (SPC) methods can be useful in this regard.

Burn-in and Screening are designed to prevent infant mortality failures, which are typically caused by manufacturing-related problems, from happening in the field.

Table 7.7 Relationship between Cp, sigma, and defect levels [11]

Cp	Sigma (s)	Defect levels
0.67	± 2σ	5 %
1.0	± 3σ	0.13 %
1.33	± 4σ	60 ppm
1.66	± 5σ	1 ppm
2.0	± 6σ	2 ppb

Online Quality Control

Before examining the sources and causes of variation and their reduction, we must measure variation. Two yardsticks, Cp (meaning capability of a process) and Cpk (Capability of a process, but corrected for non centering have become a standard language of quality at its most basic or parametric level.

Cp is defined as the specification width (S) divided by the process width (P) or range. It is a measure of spread. Another metric directly related to Cp is sigma. Table 7.7 shows relationship between Cp, Sigma and the associated defect levels. This is the true statistical meaning of Six Sigma, not the statistical dribble of 3.4 ppm, but a goal of two parts per billion (ppb) [11]. Industry level accepted definition for six sigma process is the process which produces 3.4 defective parts per million parts. Statistically normal distribution with 4.5 standard deviation on both sides of mean value covers 99.99932 % parts, which means only 6.8 ppm. However, in reality there will be natural movement in the process mean from its target. This natural movement can come from systematic cause(s), or combination of small random causes over time. Six sigma methodology has taken this into account by 1.5 sigma variation to 4.5 sigma process mean.

Cp is used only as a simple introduction to the concept of process capability. It does not take into account any noncentering of the process relative to specification limits of a parameter. Such noncentering reduces the margin of safety therefore has a penalty imposed, called a ‘K’ or correction factor.

$$C_p = \frac{S}{P}$$

$$K = \frac{D - \overline{X}}{X/2} or \frac{\overline{X} - D}{S/2} \text{ (Whichever makes K positive)}$$

$$C_{pk} = (1 - k)C_p$$

where

S Specification width

P Process width (±3 σ limits)

D Design center (D need not be at the midpoint of the specification width)

$\overline{X}$ Process average

Cpk is an excellent measure of variability and process capability because it takes into account both spread and non-centering. (In process control, centering a process is much easier than reducing spread. Centering requires only a simple adjustment, whereas spread reduction often requires patient application of design of experiment techniques). As in Cp, the objective should be to attain a higher and higher Cpk, with a Cpk of 2.0 considered merely as a passing milestone on the march past zero defects to near-zero variation.

7.3.5 Operational Reliability

Does the Reliability process end with only maintaining Manufacturing reliability/quality? The answer is a definite ‘No’. Continuous monitoring and field data analysis are necessary in order to observe the behavior of the product in its actual use (and abuse) conditions in the hands of customer, and use the gained knowledge for further improvements or in future designs. In other words, loop need to be closed, review the successful activities as well as the mistakes, and ensure that the lessons learned are not lost in the process. Service Data analysis also provides information regarding expected warranty returns in the near time, cost estimation, and spare parts requirements at dealer facilities, etc. Tools such as Failure Reporting, Analysis and Corrective Action Systems (FRACAS) can assist in capturing the knowledge gained, as well as the necessary data, and can be deployed throughout the Product Development Cycle.

Warranty failure data is analyzed using different approaches.

Weibull Analysis

The Weibull cumulative density function is:

$$\mathrm{F(t)} = 1 - e^{-(t/\theta)^{\beta}}.$$

The Weibull Reliability function is:

$$\mathrm{R(t)} = e^{-(t/\theta)^{\beta}}.$$

β = The shape parameter

θ = The scale parameter. Also called characteristic life; 63.2 % of the population fails by the characteristic life point regardless the value of the β. Bhote and Bhote [11] covers wide range of examples and applications of Weibull distributions in real time use like analysis of test data, field data, and comparing the designs, etc.

The Weibull distribution can be used in a wide variety of situations and, dependent on the value of β, is equal to or can approximate several other distributions. For example if,

β = 1 The Weibull distribution is identical to the exponential distribution.

β = 2 The Weibull distribution is identical to the Rayleigh distribution.

β = 2.5 The Weibull distribution approximates the lognormal distribution.

β = 3.6 The Weibull distribution approximates the normal distribution.

β = 5 The Weibull distribution approximates the peaked normal distribution.

The Dauser Shift for Weibull Analysis

When a Weibull Analysis is performed on a data set in which not all of the units in population have been run to failure, then the suspended items (those that have run a period of time and have not yet failed) must be accounted for. There are different ways of accounting for these suspended items depending on the information available. This section details a method to analyze warranty data.

First, if the time (for ex: trucks-miles, Hrs) on each suspended item is known then this data can be entered into the Weibull Analysis completing the data input to the analysis.

Second, if the times on the individual suspended items is not known but there exists sufficient knowledge about the suspended items with which to construct a histogram of the times on these suspensions, then this histogram can be entered to complete the data input to the analysis. Note: For a meaningful Weibull Analysis, the histogram must be reasonably accurate. Otherwise the Weibull Analysis will be misleading or down right wrong.

Third, if there is insufficient information either to enter the individual times on each suspended item or to enter a truly representative histogram of the suspended items, and, if only the total number of suspended items is known, the a Dauser Shift can be used to complete the Weibull Analysis. Fred Dauser, of Pratt & Whitney, division of United Technologies is the Statistician who developed this method to adjust the Weibull line when the number of suspended units in the population are known. The Dauser Shift, simply put, is first performed on the failed items as if it were the complete population of items. The resultant Weibull line is then shifted to adjust for the fact that the failed items don't represent the total population of items but rather a known (usually a small) portion of the population.

An outline of the method is as follows:

1. Plot the failure data on Weibull Probability Paper
2. Estimate the Weibull Parameters β and η.
3. Calculate the mean time to failure (MTTF).

$$\mathrm{MTTF} = \frac{\sum \text{Times to failure for each part}}{\text{No. failures}}$$

4. Draw a vertical line through the MTTF.
5. Calculate the proportion failed in the total population, calculate the cumulative failure point, and draw a horizontal line from this point.

$$\text{Proportion} = \frac{\text{No. of failures}}{\text{No. of failures} + \text{No. of Suspensions}}$$

$$\text{Cumulative failure point} = \left(1 - e^{-proportion}\right) \times 100$$

6. At the intersection of the vertical and horizontal lines draw a line parallet to the failure distribution. This is an estimate of the 'true' Weibull distribution.

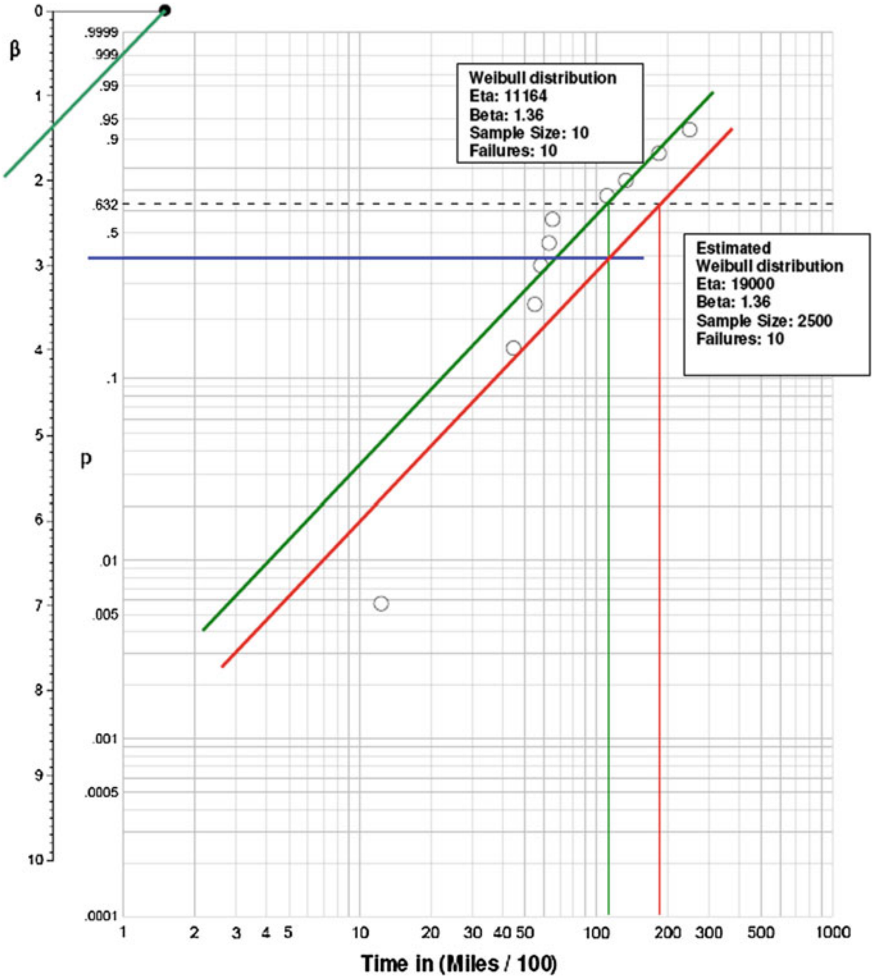


Fig. 7.13 Weibull probability plot

Example 4 Suppose there have been ten pulley failures with times of 1238, 4765, 5800, 5984, 6200, 6453, 12084, 14758, 18732, 23843 miles in a population of 2500; however, the times on the unfailed units are unknown. Estimate the characteristics of failure distribution.

Solution: The procedure to estimate the 'true' Weibull distribution can be used:
Steps 1 and 2: See (Fig. 7.13), β = 1.36, η = 11164 miles

Step 3:

$$MTTF = \frac{1238 + 4765 + 5800 + 5984 + 6200 + 6453 + 12084 + 14758 + 18732 + 23843}{10} = 9985.7$$

No. of failures/(No. of failures + No. of suspensions) = 10/2500 = 0.004

$$\text{Therefore, cum} \,\%\, \text{failed} = \left(1 - e^{-0.004}\right) \times 100 = 0.399\ \%$$

Steps, 4, 5 and 6:

The estimated distribution has a β = 1.36 (same as the 10 failure Weibull), but the characteristic life is η ≅ 19000 miles

References

1. Dhillon BS, Reiche H (1985) Reliability and maintainability management. Van Nostrand Reinhold Company, New York
2. Dhillon BS (1988) Mechanical reliability. American Institute of Aeronautics & Ast, Washington, D.C.
3. Vinogradov O (1991) Introduction to mechanical reliability. Taylor and Francis, Dordrecht
4. O'connor PDT (2002) Practical reliability engineering. Wiley, New York
5. Parmley RO (1985) Mechanical components handbook. McGraw-Hill Book Co., New York
6. Carson Harold (1983) Springs: troubleshooting and failure analysis. Marcel Dekker Inc., New York
7. Kothari H (1980) Optimum Design of helical springs. Machine Design
8. Hindhede U et al (1983) Machine design fundamentals. Wiley, New York
9. Strutt JE, Hall PL (2003) Global vehicle reliability. Wiley, New York
10. Abernathy RB (2006) The new weibull handbook (ISBN 0-9653062-3-2)
11. Bhote KR, Bhote AK (1999) World class quality, 2nd edn. AMA Publications
12. Handbook of Reliability prediction procedures for Mechanical Equipment, Carderockdiv, NSWC-11 (May 2011)

Chapter 8
Structural Reliability

In this chapter component reliability and system reliability assessment methods used in structural engineering are discussed. The first-order reliability method (FORM), which has evolved from the advanced first-order second-moment method (AFOSM) is explained, together with the second-order reliability method (SORM), which takes into account curvature of failure surface at the design point. Application of these methods in cases of correlated variables is also discussed. Unimodal and bimodal bound methods, the first-order multi normal (FOMN) and product of conditional margins (PCM) methods, which are used for system reliability assessment of structures, are also discussed.

8.1 Deterministic versus Probabilistic Approach in Structural Engineering

The design of structures represents a challenging task for civil and mechanical engineers. As safety and economy are the main issues in the design of structures and designer targets best compromise between safety and cost of the structures. Parameters involved in design such as loads and material properties are rarely certain and designer has to take into account the uncertainty present. Traditionally, empirical safety factors are used which are based on experience to account for uncertainty. This approach of using safety factor cannot ensure the required safety level, as these factors are calibrated for a large class of structures. Further, these safety factors do not give any information on the influence of the different parameters have on the safety. Therefore, it is difficult to design a system with uniform distribution of safety among the different components using empirical safety factors. Probabilistic design method is free from this drawback. In probabilistic approach, uncertainty involved in various parameters is modeled using different probability density function and design is carried out for specified reliability level. A structure is usually required to have a satisfactory performance in the expected lifetime, i.e. it is required that it does not collapse or become unsafe and that it fulfills certain functional requirements. In structural reliability assessment

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_8

methods the failure probability of the structure is evaluated when material properties and loads acting on structure are random variables. First Order Second Moment Method (FOSM), Advance First Order Second Moment Method (AFOSM), First Order Reliability Method (FORM) and second Order Reliability Method (SORM) are used for component reliability assessment. Unimodal and bimodal bound methods, First Order Multinormal (FOMN) Method, Product of Conditional Margins (PCM) methods are used for system reliability assessment.

8.2 The Basic Reliability Problem

Consider a solid bar (Fig. 8.1) with load carrying capacity R and S is load acting on it. Both S and R are independent random variables with probability density function *f*(*R*) and *f*(*S*) and cumulative distributions *F*(*R*) and *F*(*S*) respectively. Bar fails if load exceeds resistance

$$\begin{aligned} p_f &= P(failure) \\ &= P(R \leq S) \end{aligned}$$

If r is realization of random variable R then failure probability

$$\begin{aligned} p_f &= P(r \leq S) \\ &= \int_r^{\infty} f(s)ds = 1 - F_s(r) \end{aligned}$$

As *r* is random quantity

$$p_f = \int_{-\infty}^{\infty} (1 - F_s(r))f_r(r)dr \tag{8.1}$$

Equation 8.1 can be used for calculating failure probability if probability density functions of stress and resistance are known.

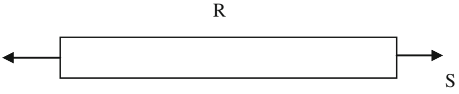


Fig. 8.1 Probability of failure, fundamental case

8.2.1 First Order Second Moment (FOSM) Method

It is convenient to define limit state function or performance function as

$$Z = g(R, S) \tag{8.2}$$

such that

$Z < 0$ is unsafe state
$Z > 0$ is safe state
$Z = 0$ is limit state

The First Order Second Moment FOSM method, explained here, is based on a first-order Taylor's approximation of the performance function [1–4]. It uses only second moment statistics (means and covariances) of the random variables.

Consider a case where R and S are normally distributed variables and they are statistically independent. μ_R and μ_S are mean and σ_R and σ_S are standard deviations of R and S respectively.

Then mean of Z is

$$\mu_Z = \mu_R - \mu_S$$

and standard deviation of Z is

$$\sigma_Z = \sqrt{\sigma_R^2 + \sigma_S^2}$$

So that failure probability is

$$\begin{aligned} p_f &= P(Z < 0) \\ &= \Phi\left(\frac{0 - (\mu_R - \mu_S)}{\sqrt{\sigma_R^2 + \sigma_S^2}}\right) \\ p_f &= \Phi\left(\frac{-\mu_Z}{\sigma_Z}\right) \end{aligned}$$

The probability of failure depends on the ratio of mean value of Z to its standard deviation.

$$= \Phi(-\beta)$$

where β is called as reliability index.

$$\beta = \frac{\mu_z}{\sigma_z}$$

Consider a case of generalized performance function of many random variables

$$Z = g(X_1, X_2, X_3, X_4, \ldots X_n)$$

Expanding this performance function about the mean gives

$$Z = g(\mu_x) + \sum_{i=1}^{n} \frac{\partial g}{\partial X_i}(X_i - \mu_{Xi}) + \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n} \frac{\partial^2 g}{\partial X_i \partial X_j}(X_i - \mu_{Xi})(X_j - \mu_{Xj}) + \ldots \tag{8.3}$$

where the derivatives are evaluated at the mean values.

First order of approximation of mean μ_Z is

$$\mu_Z \approx g(\mu_{X1}, \mu_{X2}, \mu_{X3}, \mu_{X4} \ldots \mu_{Xn}) \tag{8.4}$$

Approximate variance of Z is

$$\sigma_Z^2 \approx \sum_{i=1}^{n}\sum_{j=1}^{n} \left(\frac{\partial g}{\partial X_i}\right)\left(\frac{\partial g}{\partial X_j}\right) Cov(X_i, X_j) \tag{8.5}$$

where $Cov(X_i, X_j)$ is the covariance of X_i and X_j.

If variables are uncorrelated then variance is

$$\sigma_Z^2 \approx \sum_{i=1}^{n} \left(\frac{\partial g}{\partial X_i}\right)^2 Var(X_i) \tag{8.6}$$

Reliability index β is

$$\beta = \frac{\mu_Z}{\sigma_Z}$$

MOSM method can be used for calculating reliability index.

Example 1 A circular bar of 25 mm diameter is made up of carbon steel and is subjected to axial force F. The mean yield strength of the material is 250 MPa and mean value of force F is 70 KN. Both yield strength and force are random variables and are following normal distribution. Coefficient of variation of both variables is 10 %. Calculate the reliability index?

Solution: Stress induced in the bar is $S = \frac{F}{\pi d^2/4}$

Performance function of the bar is

$$Z = Y - S = Y - \frac{F}{\pi d^2/4}$$

where Y is yield strength of material.

Mean value of Z

$$\mu_Z = \mu_Y - \frac{\mu_F}{\pi d^2/4} = 250 - \frac{70 \times 10^3}{3.142 \times 25^2/4} = 107.43$$

Standard deviation of Z

$$\begin{aligned}
&\frac{\partial g}{\partial Y} = 1, \frac{\partial g}{\partial F} = \frac{1}{\pi d^2/4} = 2.0372 \times 10^{-3} \\
&\sigma_Z = \sqrt{\left(\sigma_y \frac{\partial g}{\partial Y}\right)^2 + \left(\sigma_F \frac{\partial g}{\partial F}\right)^2} \\
&\quad = \sqrt{(25 \times 1)^2 + (700 \ \times 2.0372 \times 10^{-2})^2} \\
&\sigma_Z = 28.78
\end{aligned}$$

Reliability indexis

$$\beta = \frac{107.43}{28.78} = 3.734$$

However this method has some deficiencies. This method gives different reliability index for the same problem if the performance function is formulated in different way.

Case 1

If safety margin is defined as

$$\begin{aligned}
Z &= R - S \\
\mu_Z &= \mu_R - \mu_S \\
\sigma_Z &= \sqrt{\sigma_R^2 + \sigma_S^2} \\
\beta &= \frac{\mu_R - \mu_S}{\sqrt{\sigma_R^2 + \sigma_S^2}}
\end{aligned}$$

Case 2

If safety margin is defined as

$$\begin{aligned}
g &= \frac{R}{S} - 1 \\
\mu_Z &= \frac{\mu_R}{\mu_S} - 1 \\
\sigma_Z &= \sqrt{\frac{\sigma_R^2}{\mu_S} + \frac{\sigma_S^2}{\mu_S^2} \mu_R}
\end{aligned}$$

Hence,

$$\beta = \frac{\mu_Z}{\sigma_Z}$$
$$\beta = \frac{\mu_R - \mu_S}{\sqrt{\mu_S \sigma_R^2 + \mu_R \sigma_S^2}}$$

Example 2 Find the probability of failure for the performance function $g(x) = x_1 - x_2$. Variable x_1 and x_2 are normally distributed random variables. Mean and standard deviation of these variables are given in Table 8.1.

Solution:
$$\mu_Z = g(x)_{x=\mu}$$
$$\sigma_Z = \sqrt{\sum_{i=1}^{n} \left(\frac{\partial g}{\partial x_i}\right)^2 \sigma_i^2}$$
$$\mu_Z = 1;\ \sigma_Z = 0.2\sqrt{2} = 0.2828$$

Reliability index is given by,

$$\beta = \frac{\mu_Z}{\sigma_Z} = \frac{1}{0.2828} = 3.53$$

Probability of failure is given by,

$$p_f = \Phi(-\beta) = 2.03476\mathrm{e} - 4$$

Example 3 Solve Example 2 using performance function as $g(x) = \frac{x_1}{x_2} - 1$.

Solution:
$$\mu_Z = g(x)_{x=\mu}$$
$$\sigma_Z = \sqrt{\sum_{i=1}^{n} \left(\frac{\partial g}{\partial x_i}\right)^2 \sigma_i^2}$$
$$\mu_Z = 1;\ \sigma_Z = \sqrt{0.2} = 0.4472$$

Reliability index is given by,

$$\beta = \frac{\mu}{\sigma} = \frac{1}{0.4472} = 2.236$$

Probability of failure is given by,

$$p_f = \Phi(-\beta) = 7.706e - 4$$

Table 8.1 Parameters of random variables

Variables	Distribution	Mean	Std. Deviation
x_1	Normal	2	0.2
x_2	Normal	1	0.2

It is seen that failure probability obtained using FOSM method is different for the same problem if the performance function is formulated in different way. Further it does not take into account type of distribution of the random variable.

8.2.2 *Advanced First Order Second Moment Method (AFOSM)*

Advanced First Order Second Moment (AFOSM) method was developed by Hasofer-Lind and is applicable for normal variables [5]. In this method basic normal variables are transformed into standard normal variables using following equation

$$u = \frac{X - \mu_x}{\sigma_x}$$

where u is random variable following standard normal distribution. Above equation is used to transform original performance function $g(x) = 0$ to reduced performance function $g(u) = 0$. The reliability index β is defined as

$$\beta = \left(u^* u^{*T}\right)^{\frac{1}{2}}$$

where u^* is the minimum distance point on the failure surface.Consider a simple problem with two basic independent variables X_1 and X_2 and a linear failure function:

$$g(x) = a_0 + a_1 x_1 + a_2 x_2$$

If normalized stochastic variables u_1 and u_2 with zero mean value and unit standard deviation are introduced by:

$$u_i = \frac{x_i - \mu_{x_i}}{\sigma_{x_i}} \quad i = 1, 2 \tag{8.7}$$

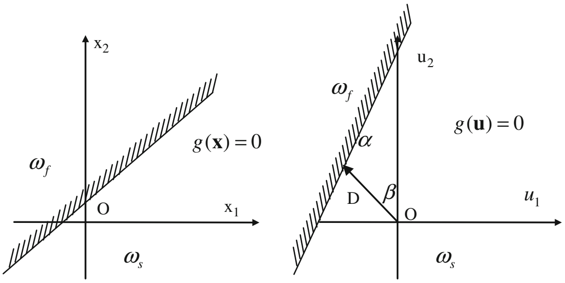
then the failure function can be written:

$$g(u) = a_0 + a_1\left(\mu_{X_1} + \sigma_{X_1} u_1\right) + a_2\left(\mu_{X_2} + \sigma_{X_2} u_2\right)$$

or equivalently if the reliability index β is introduced:

$$g(u) = \beta - \alpha_1 u_1 - \alpha_2 u_2$$

Fig. 8.2 Linear failure functions in two coordinate systems



Original Coordinate System

Normalized Coordinate System

where:

$$\beta = \frac{a_0 + a_1\mu_{X_1} + a_2\mu_{X_2}}{\sqrt{a_1^2\sigma_{X_1}^2 + a_2^2\sigma_{X_2}^2}}$$

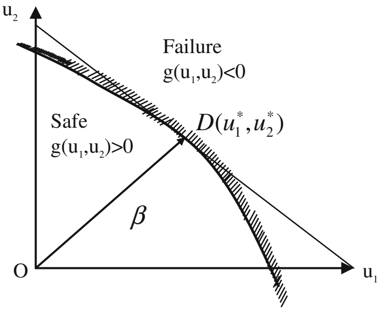
$$\alpha_i = \frac{-a_i\sigma_{X_i}}{\sqrt{a_1^2\sigma_{X_1}^2 + a_2^2\sigma_{X_2}^2}} \qquad i = 1, 2$$

In Fig. 8.2 the failure function in the x-space and in the u-space is shown. It is seen that β is the shortest distance from origin to the failure surface in the normalized space and that the coefficients α_1 and α_2 are elements in a unit vector, $\boldsymbol{\alpha}$, normal to the failure surface. The point D is the design point and lies on the failure surface. This point is also called the check point for the safety of the structure. Now β is related to the failure surface (and not to the failure functions). The safety measure obtained is invariant to the failure function, since equivalent failure functions will result in same failure surface.

8.3 First Order Reliability Method (FORM)

AFOSM method can also be used for a non-linear performance function by expanding the performance function about the design point. This corresponds to approximating the non-linear performance function by its tangent plane at the design as shown in Fig. 8.3. Thus for a non-linear failure surface, the shortest distance of the origin (normalized coordinate system, see Fig. 8.2) to the failure surface is not unique as in the case of a linear failure surface. It has been proved that the point D on the failure surface with minimum distance to the origin (normalized coordinate system) is the most probable failure point. The tangent plane on the design point D may then be used to approximate the value of β. If the failure surface is concave towards the origin, the approximation will be on the conservative for the surface convex towards the origin it will be on the unconservative side.

Fig. 8.3 Formulation of safety analysis in normalized coordinates



The problem therefore reduces to finding out the minimum value of the distance OD (Fig. 8.3). Thus it becomes an optimization problem.

$$\text{Minimize, } D = \sqrt{u^T u} \tag{8.8}$$

Subjected to constraints, $g(X) = g(u) = 0$.

Using the method of Lagrange multiplier we can obtain the minimum distance as

$$\beta_{H-L} = \frac{u_*^T \left(\frac{\partial g}{\partial u}\right)_*}{\left(\left(\frac{\partial g}{\partial u}\right)_*^T \left(\frac{\partial g}{\partial u}\right)_*\right)^{1/2}} = \frac{\sum_{i=1}^{n} u_i^* \left(\frac{\partial g}{\partial u}\right)_*}{\sqrt{\sum_{i=1}^{n} \left(\frac{\partial g}{\partial u}\right)_*^2}} \tag{8.9}$$

where $\left(\frac{\partial g}{\partial u}\right)_*$ is the partial derivative evaluated at the design point $\mathbf{u}_*$. Design point in the reduced coordinate is given by

$$u = -\alpha\beta_{H-L} \tag{8.10}$$

where

$$\alpha = \frac{\left(\frac{\partial g}{\partial u}\right)_*}{\left(\left(\frac{\partial g}{\partial u}\right)_*^T \left(\frac{\partial g}{\partial u}\right)_*\right)^{1/2}} = \frac{\left(\frac{\partial g}{\partial u_i}\right)_*}{\sqrt{\sum_{i=1}^{n} \left(\frac{\partial g}{\partial u_i}\right)_*^2}} \tag{8.11}$$

Design point in the original co-ordinates is given by [from Eq. (8.1)]

$$X_i^* = \mu_{X_i} - \alpha_i \sigma_{X_i} \beta_{H-L} \quad i = 1, \ldots, n \tag{8.12}$$

Following algorithm is formulated by 'Rackwitz' to compute $\beta_{H\text{-}L}$ and $u*$ the steps are:

1. Write the limit state function $g(X) = 0$ in terms of the basic variables
2. Normalize the basic variables using Eq. (8.7) and obtain the failure surface equation in normalized coordinate system.
3. Assume initial values of design point $X*$ (usually mean values) and compute the reduced variable $u*$.
4. Evaluate $\left(\frac{\partial g}{\partial u}\right)_*$ and α at design point.
5. Obtain the new design point in terms of $\beta_{H\text{-}L}$ from Eq. (8.9).
6. Substitute the new u^* in the limit state equation $g(u*) = 0$ and solve for $\beta_{H\text{-}L}$.
7. Using the $\beta_{H\text{-}L}$ value obtained in the step VI, reevaluates $u*$ from Eq. (8.7).
8. Repeat steps 4 to 7 until $\beta_{H\text{-}L}$ converges.

Example 4 Solve Example 3 using FORM method.
Solution: Transformation to std. normal space is, $\{x\} = [\sigma]\{u\} + \{\mu\}$;

$$\frac{\partial g}{\partial x_1} = \frac{1}{x_2}; \frac{\partial g}{\partial x_2} = -\frac{x_1}{x_2^2}; \frac{\partial x_1}{\partial u_1} = \sigma_1; \frac{\partial x_2}{\partial u_2} = \sigma_2;$$

From FORM iteration scheme(Calculations in Table 8.2),

$$u_i^* = \left(\frac{\partial g}{\partial u_i}\right) \frac{\sum u_i \frac{\partial g}{\partial u_i} - g(u_i)}{\sum \left(\frac{\partial g}{\partial u_i}\right)^2}$$

$$p_f = \Phi(-\beta) = 2.03476\text{e - }4$$

Example 5 For circular pipe with circumferential through wall crack subjected to bending moment performance function is given by

$$g(x) = 4t\sigma_f R^2(\cos(\theta/2) - 0.5\sin(\theta)) - M$$

Table 8.2 Calculations

Iter. No.	1	2	3	4	5	6
u_1^*	0	−1	−2.1	−2.4701	−2.5007	−2.5
u_2^*	0	2	2.7	2.5342	2.4993	2.5
g	1	0.285	0.0259	−0.00057	2.66E-06	3E-10
$\left(\frac{\partial g}{\partial u_1}\right)^*$	0.2	0.142	0.129	0.1327	0.1333	0.1333
$\left(\frac{\partial g}{\partial u_2}\right)^*$	−0.4	−0.183	−0.133	−0.1327	−0.1333	−0.1333
α_1	0.447	0.613	0.698	0.7073	0.7071	0.7071
α_2	−0.894	−0.789	−0.716	−0.7069	−0.7071	−0.7071
β	2.236	3.420	3.539	3.5355	3.5355	3.5355

Table 8.3 Parameters of random variables

Variables	Distribution	Mean	Std. Deviation
σ_f	Normal	301.079	14.78
θ	Normal	0.503	0.049

where σ_f, θ, M, R and t are flow stress, half crack angle, applied bending moment, radius of the pipe and thickness of the pipe respectively.

$$\begin{aligned} \mathrm{R} &= 0.3377\ \mathrm{m}, \\ \mathrm{t} &= 0.03377\ \mathrm{m} \\ \mathrm{M} &= 3\ \mathrm{MN-m}. \end{aligned}$$

σ_f and θ are randomly distributed. Their properties are given in Table 8.3. Find reliability index and probability of failure.

Solution: First Order Reliability Method (FORM)

Transformation to std. normal space is,

$$\{X\} = [\sigma]\{u\} + \{\mu\}$$
$$\frac{\partial X}{\partial u} = [\sigma]$$

From FORM-2 iteration scheme (Calculations in Table 8.4),

$$u_i^* = \left(\frac{\partial g}{\partial u_i}\right)\frac{\sum u_i \frac{\partial g}{\partial u_i} - g(u_i)}{\sum \left(\frac{\partial g}{\partial u_i}\right)^2}$$

$$p_f = \Phi(-\beta) = 0.033065$$

Table 8.4 Calculations

Iter. No.	1	2	3	4	5	6
$u_{\sigma_f}^*$	0	−1.4159	−1.471	−1.4726	−1.4727	−1.4727
u_θ^*	0	1.0927	1.1	1.0991	1.099	1.099
g	0.374	0.009754	2.85E-6	−1.6E-08	0	0
$\left(\frac{\partial g}{\partial u_{\sigma_f}}\right)^*$	0.165	0.1588	0.158	0.1587	0.1587	0.1587
$\left(\frac{\partial g}{\partial u_\theta}\right)^*$	−0.127	−0.1188	−0.118	−0.1185	−0.1185	−0.1185
α_1	0.791	0.8006	0.801	0.8014	0.8014	0.8014
α_θ	−0.611	−0.5991	−0.598	−0.5981	−0.5981	−0.5981
β	0	1.7883	1.837	1.8375	1.8375	1.8375

SORM

$$\beta = 1.83754$$

$$D = \begin{bmatrix} 0 & -6.3e-3 \\ -6.3e-3 & 2.5e-4 \end{bmatrix}$$

$$R0 = \begin{bmatrix} 1 & 0 \\ 0.801 & -0.598 \end{bmatrix}$$

$$R = \begin{bmatrix} 0.598 & 0.801 \\ 0.801 & -0.598 \end{bmatrix}$$

Gradient length = 0.198076

$$A = \begin{bmatrix} -0.030 & -9.6e-3 \\ -9.6e-3 & 0.031 \end{bmatrix}$$

$$k = -0.029538$$

$$w = \beta\Phi(-\beta) - \varphi(-\beta) = -0.01298$$

$$x = \prod_{i=1}^{n-1} (1 + \beta k_{\mathrm{i}})^{-0.5} = 1.028296$$

$$y = \prod_{i=1}^{n-1} (1 + (1 + \beta)\mathrm{k}_{\mathrm{i}})^{-0.5} = 1.044741$$

$$z = \mathrm{Real}\left(\prod_{i=1}^{n-1} (1 + (i + \beta)\mathrm{k}_{\mathrm{i}})^{-0.5}\right) = 1.02792$$

$$\psi(-\beta) = \frac{\varphi(-\beta)}{\Phi(-\beta)} = 2.230136$$

$$p_{f_{FORM}} = \Phi(-1.83754) = 0.033065$$

$$p_{f_{SORM}(Breitung)} = \Phi(-1.83754)x = 0.034001$$

$$p_{f_{SORM}(Hohenbichler)} = \Phi(-1.83754)\prod_{\mathrm{i}=1}^{n-1} (1 + \mathrm{k_i}\psi(-\beta))^{-0.5} = 0.034211$$

$$p_{f_{SORM}(Tvedt)} = \Phi(-1.83754)\mathrm{x} + w(x - y) + (1 + \beta)w(x - z) = 0.03420$$

$$p_{f_{SORM}(exact)} = 0.0341998$$

8.4 Reliability Analysis for Correlated Variables

The FORM methods described so far in this implicitly assume that the basic variables X_1, …, X_n are not correlated. However, usually some variables are correlated. If the basic variables X_1, …, X_n are correlated with mean μ_{X1}, …, μ_{Xn} and standard deviations σ_{X1}, ..., σ_{Xn}, then the covariance matrix in original variable and reduced variable respectively are,

$$C = \begin{bmatrix} \sigma_{X_1}^2 & \cdots & \rho_{1n}\sigma_{X_1}\sigma_{X_n} \\ \vdots & \ddots & \vdots \\ \rho_{n1}\sigma_{X_n}\sigma_{X_1} & \cdots & \sigma_{X_n}^2 \end{bmatrix} \text{ and}$$

$$C' = \begin{bmatrix} 1 & \cdots & \rho_{1n} \\ \vdots & \ddots & \vdots \\ \rho_{n1} & \cdots & 1 \end{bmatrix}$$

where ρ_{ij} is the correlation coefficient between the variables X_i and X_j.

8.4.1 Reliability Analysis for Correlated Normal Variables

The FORM methods can be used if the X is transformed into uncorrelated reduced normal variables Y and the limit state equation is expressed in terms of Y. This can be done using the following equation,

$$X = \left[\sigma_X^N\right][T]\,Y + \mu_X^N \tag{8.13}$$

where $[\sigma_X^N]$ is a diagonal matrix of the equivalent standard deviations

μ_X^N is the vector of the equivalent means

$[T]$ is the transformation matrix, whose columns are the eigen vectors of the correlation matrix in reduced variable $C^{'}$.

In an *alternative* way the correlated variables are transformed into uncorrelated variables through an orthogonal transformation of the form

$$Y = Lu + \mu_X$$

where L is the lower triangular matrix obtained by *Cholesky factorization* of the correlation matrix.

Once basic normal correlated variables are transferred to uncorrelated standard normal variables the rest procedure are as discussed earlier.

8.4.2 Reliability Analysis for Correlated Non-normal Variables

There are two ways one can transform correlated Non-normal variables into uncorrelated normal variables.
Rosenblatt Transformation
The transformation required are

$$\begin{aligned} x_1 &= F^{-1}_{X_1}[\Phi(u_1)] \\ x_2 &= F^{-1}_{X_2|X_1}[\Phi(u_2)|X_1 = x_1] \\ &\ldots \\ x_n &= F^{-1}_{X_n|X_1 \ldots X_{n-1}}[\Phi(u_n)|X_1 = x_1, \ldots, X_{n-1} = x_{n-1}] \end{aligned}$$

where $F_{X_i|X_1 \ldots X_{i-1}}[x_i|X_1 = x_1, \ldots, X_{i-1} = x_{i-1}]$ is the CDF of X_i given X_1 = $x_1 \ldots X_i$ $_{-1}$ = x_{i-1}, given by

$$F_{X_i|X_1 \ldots X_{i-1}}\left[x_i \middle| X_1 = x_1, \ldots, X_{i-1} = x_{i-1}\right] = \frac{\int\limits_{-\infty}^{x_i} f_{X_1 \ldots X_{i-1} X_i}[x_1, \ldots, x_{i-1}, t]dt}{f_{X_1 \ldots X_{i-1}}[x_1, \ldots, x_{i-1}]}$$

where $f_{X_1 \ldots X_i}[x_1, \ldots, x_i]$ is the joint PDF of X_1, …, X_i. The transformation starts for given u_1, …, u_n by determination of x_1. Next x_2 is calculated using the value of x_1 determined in the first step. $x_1, \ldots, x_n$ are then calculated in the same stepwise manner.

The inverse transformation is given by:

$$\begin{aligned} u_1 &= \Phi^{-1}[F_{X_1}(x_1)] \\ u_2 &= \Phi^{-1}[F_{X_2}|_{x_1}(x_2|x_1)] \\ &\ldots \\ u_n &= \Phi^{-1}[F_{X_n}|_{x_1 \ldots x_{n-1}}(x_n|x_1 \ldots x_{n-1})] \end{aligned}$$

The Rosenblatt transformation is very useful when the stochastic model for a failure mode is given in terms of conditional distributions. This is often the case when statistic uncertainty is included.
Nataf Transformation
The transformation is done in two stages

1. The basic random variables, X are transformed into a space of correlated standard normal variables, Z, such that $Z_i = \Phi^{-1}[F_{X_i}(x_i)]$. The variates have a correlation matrix R_0.

2. The vector Z is now transformed into the space of uncorrelated standard normal variates such as:

$$u = \Gamma_0 Z$$

where Γ_0 is a lower triangular matrix resulting from the *Cholesky factorization* of the correlation matrix of Z, i.e. R_0.

The elements of the matrix R_0 are the correlation coefficients $\rho_{z_i z_j}$. These, in turn, are related to the related to the correlation coefficients, $\rho_{x_i x_j}$ of the basic random variables X through the following implicit integral relationship:

$$\rho_{x_i x_j} = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \left[\frac{x_i - \mu_i}{\sigma_i}\right] \left[\frac{x_j - \mu_j}{\sigma_j}\right] \varphi_2\left(z_i, z_j, \rho_{z_i z_j}\right) dz_i dz_j \tag{8.14}$$

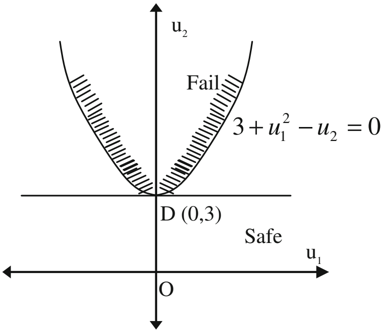
where $\varphi_2\left(z_i, z_j, \rho_{z_i, z_j}\right)$ is the bivariate normal density function of standard normal variates with correlation coefficient ρ_{z_i, z_j}. μ_i and σ_i are the mean and standard deviation of X_i, respectively. For each pair of $F_{X_i}(x_i)$ and $F_{x_j}(x_j)$, and for a given correlation coefficient ρ_{x_i, x_j}, the above equation can be iteratively solved to obtain ρ_{z_i, z_j}. Der Kiureghian et al., however, provided a set of empirical formulae relating ρ_{z_i, z_j} to ρ_{x_i, x_j} for some known marginal distributions. This greatly simplifies the calculations and overcomes the tedious process of iterative solution.

8.5 Second Order Reliability Methods (SORM)

The limit state could be nonlinear either due to nonlinear relationship between the random variables in the limit state equation or due to some variables being non-normal. A linear limit state in the original space becomes nonlinear when transformed to the standard normal space if any of the variables in non-normal. Also, the transformation from correlated to uncorrelated variables might induce nonlinearity. If the joint PDF of the random variables decays rapidly as one moves away from minimum distance point, then the first-order estimate of failure probability in quite accurate. If the decay of the joint PDF is slow and the limit state is highly nonlinear, then use of higher-order approximation for the failure probability seems to be more reasonable.

Consider the well-known parabolic failure surface where the FORM result gives the probability of failure $P_f = \Phi(-3)$, thus giving highly conservative solution whereas the actual result will have lesser value of probability of failure (Fig. 8.4). The reason for this indifference can be given to the fact that FORM uses only a first

Fig. 8.4 Failure surface



order approximation at minimum distance point and ignores the curvature of the limit surface. SORM tries to take care of nonlinearity to some extent.

Second order reliability method is used to estimate the probability of failure with a partial consideration of curvature or nonlinear nature of performance function [6, 7]. Different formulation for SORM has been given out of which Breitung, Hohenbichler and Tvedt are most popular. These formulae needs finding of curvature the process of which is explained below.

Failure probability using SORM, given by Breitung is,

$$p_f = \Phi(-\beta)\prod_{i=1}^{n-1}(1+\beta k_i)^{-1/2} \tag{8.15}$$

where k_i denotes principle curvatures of the limit state at the Most Probable failure Point (MPP) and β is the reliability index using FORM.

To compute principle curvatures k_i Y_i variables are rotated to another set of variables Y_i' such that last variable coincides with unit gradient vector of the limit state at the MPP.

This transformation is orthogonal transformation:

$$Y' = RY$$

where R is the rotation matrix.

R matrix can be calculated in two steps. In step 1, first a matrix, R_0, is constructed as follows:

$$R_0 = \begin{bmatrix} 1 & 0 & . & . & . & 0 \\ 0 & 1 & 0 & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ \alpha_1 & \alpha_2 & . & . & . & \alpha_n \end{bmatrix}$$

where α_1, $\alpha_2, \ldots \alpha_n$ are the direction cosines of the unit gradient vector at MPP.

In step 2, a Gram-Schmidt orthogonalization procedure is used. This procedure is explained below.

Consider a matrix R$_0$, with row vectors r_{01}, r_{02}, $\ldots r_{0n}$. This has to be transformed to a matrix R, whose row vectors r_1, r_2, $\ldots r_n$ are orthogonal to each other, with the nth row same as in matrix R_0.

The Gram-Schmidt method to achieve this may be written as follows. The nth row vector of matrix R is simply, $r_n = r_{0n}$. The other rows of matrix R are computed using the formula

$$r_k = r_{0k} - \sum_{j=k+1}^{n} \frac{r_j r_{0k}^t}{r_j r_j^t} r_j$$

where the subscript t implies the transpose of the row vector. To orthonormalize R each row of R is orthonormalized separately. Once the R matrix is calculated, a matrix AA, whose elements are denoted as a_{ij}, is computed as

$$a_{ij} = \frac{(RDR^t)_{ij}}{|\nabla F(y^*)|} \quad i,j = 1,2,\ldots,n-1$$

where D is second order matrix of the limit state surface in the standard normal space evaluated at MPP given by

$$D = \begin{bmatrix} \frac{\partial^2 g}{\partial u_1^2} & \frac{\partial^2 g}{\partial u_1 \partial u_2} & \cdot & \cdot \\ \frac{\partial^2 g}{\partial u_1 \partial u_2} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \frac{\partial^2 g}{\partial u_n^2} \end{bmatrix}$$

and $|\nabla G(y^*)|$ is the length of the gradient vector in the standard space.

Finally, the main curvatures k_i are computed as the eigenvalues of the matrix obtained by excluding last row last column of matrix AA (Given by matrix AB). Once curvatures are computed, Breitung formula can be used to compute second order estimate of failure probability.

Better Approximations for SORM can be obtained using Hohenbichler or Tvedt as given below.

$$\begin{aligned}
w &= \beta\Phi(-\beta) - \varphi(-\beta) \\
x &= \prod_{i=1}^{n-1} (1 + \beta k_i)^{-0.5} \\
y &= \prod_{i=1}^{n-1} (1 + (1 + \beta)k_i)^{-0.5} \\
z &= \text{Real}\left(\prod_{i=1}^{n-1} (1 + (i + \beta)k_i)^{-0.5}\right) \\
\Psi(-\beta) &= \frac{\varphi(-\beta)}{\Phi(-\beta)} \\
p_{f_{FORM}} &= \Phi(-\beta) \\
p_{f_{SORM}}(Breitung) &= \Phi(-\beta)x \\
p_{f_{SORM}}(Hohenbichler) &= \Phi(-\beta)\prod_{i=1}^{n-1} (1 + k_i\Psi(\beta))^{-0.5} \\
p_{f_{SORM}}(Tvedt) &= \Phi(-\beta)x + w(x - y) + (1 + \beta)w(x - z)
\end{aligned}$$

Tvedt gave an exact result in terms of a one-dimensional integral given here for easy reference.

$$P_f = \frac{1}{2} - \frac{1}{\pi}\int_0^{\infty} \sin\left(\beta t + \frac{1}{2}\sum_{i=1}^{n-1} \tan^{-1}(-k_i t)\right) \frac{\exp\left[-\frac{1}{2}t^2\right]}{t\left[\prod_{i=1}^{n-1} (1 + k_i^2 t^2)\right]^{1/4}} dt \tag{8.16}$$

Example 6 The stress in a piping system is not allowed more than gross plastic deformation due to primary load. The limit state function and distribution of random variables (Table 8.5) are given below. Find β and p_f.

Table 8.5 Parameters of random variables

Variables	Distribution	Mean	Std. deviation	Other parameters
S_y	Lognormal	35,000	3500	$\overline{\mu} = 10.458128175$
				$\overline{\sigma} = 0.09975134$
t	Lognormal	0.4	0.04	$\overline{\mu} = -0.92126590$
				$\overline{\sigma} = 0.09975134$
p	Lognormal	750	25	$\overline{\mu} = 6.61951795$
				$\overline{\sigma} = 0.03332408$
M_A	Lognormal	2.5e5	300	$\overline{\mu} = 12.4292154$
				$\overline{\sigma} = 0.00120000$

$$g(x) = S_y - \frac{pD_0}{4t} - \frac{0.75iM_A}{Z}; i = \frac{0.9}{h^{2/3}}; h = \frac{tD_0}{2r^2}; z = \pi r^2 t$$
$$g(x) = S_y - \frac{9p}{t} - \frac{(9.4741e-3)M_A}{t^{2/3}}; r = 6''; D_0 = 36'';$$

where S_y, t, p, M_A, D_0, r and i are yield strength of the material used, thickness of the pipe, internal pressure inside pipe, moment due to the sustained load, average radius of the pipe, outer diameter of the pipe and stress intensity factor respectively.
Solution: First Order Reliability Method (FORM)
Transformation to std. normal space is,

$$\{X_i\} = e^{(\overline{\sigma_i}u_i + \overline{\mu_i})};$$
$$\frac{\partial g}{\partial S_y} = 1; \frac{\partial g}{\partial p} = -\frac{9}{t}; \frac{\partial g}{\partial M_A} = -\frac{(9.4741E-3)}{t^{5/3}}; \frac{\partial g}{\partial t} = \frac{9p}{t^2} + \frac{5(9.4741e-3)M_A}{3t^{8/3}};$$
$$\left\{\frac{\partial X_i}{\partial u_i}\right\} = X_i\overline{\sigma_i};$$

From FORM-2 iteration scheme (Calculations in Table 8.6),

$$u_i^* = \left(\frac{\partial g}{\partial u_i}\right)\frac{\sum u_i\frac{\partial g}{\partial u_i} - g(u_i)}{\sum\left(\frac{\partial g}{\partial u_i}\right)^2}$$

$$p_f = \Phi(-\beta) = 0.087555$$

SORM

$$\beta = 1.35597$$
$$D = \begin{bmatrix} 318.948 & 0 & 0 & 0 \\ 0 & -550.925 & 62.960 & 0.627 \\ 0 & 62.960 & -21.033 & 0 \\ 0 & 0.627 & 0 & 0.052 \end{bmatrix}$$
$$R0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0.613 & 0.781 & -0.121 & -3e-3 \end{bmatrix}$$
$$R = \begin{bmatrix} 4.9e-3 & 0 & 0 & 1 \\ -0.786 & 0.618 & 0 & 3.9e-3 \\ 0.075 & 0.095 & 0.993 & -3.7e-4 \\ 0.613 & 0.781 & -0.121 & -3e-3 \end{bmatrix}$$

Table 8.6 Calculations

Iter. No.	1	2	3	4	5	6	100
$u^*_{S_y}$	0	−0.965	−0.83	−0.83	−0.83	−0.83	−0.83157
$u^*_{\sigma_{\min}}$	0	−0.977	−1.059	−1.058	−1.058	−1.058	−1.05838
$u^*_{a_i}$	0	0.1568	0.164	0.164	0.164	0.164	0.164153
$u^*_{M_A}$	0	0.0036	0.004	0.004	0.004	0.004	0.004093
g	6878.8	−89.68	0.982	0.0001	−1.4E-9	0	0
$\left(\frac{\partial g}{\partial u_{S_y}}\right)^*$	3473.9	3155.2	3197.8	3197.4	3197.4	3197.4	3197.43
$\left(\frac{\partial g}{\partial u_t}\right)^*$	3519.1	4024.5	4069.9	4069.4	4069.4	4069.4	4069.496
$\left(\frac{\partial g}{\partial u_p}\right)^*$	−564.8	−625.9	−631.2	−631.1	−631.1	−631.1	−631.172
$\left(\frac{\partial g}{\partial u_{M_A}}\right)^*$	−13.19	−15.52	−15.7	−15.73	−15.73	−15.73	−15.7363
$\alpha_{u_{S_y}}$	0.698	0.6124	0.613	0.613	0.613	0.613	0.613271
α_{u_t}	0.707	0.781	0.780	0.78	0.78	0.78	0.780534
α_{u_p}	−0.113	−0.121	−0.12	−0.12	−0.12	−0.12	−0.12106
α_{u_P}	−0.002	−0.003	−0.003	−0.003	−0.003	−0.003	−0.00302
β	1.3820	1.3557	1.355	1.355	1.355	1.355	1.355966

Gradient length = 5213.730167

$$A = \begin{bmatrix} 1.2e-5 & -1.6e-4 & 3.4e-5 & 2.8e-4 \\ -1.6e-4 & -2.5e-3 & -2.4e-3 & -0.081 \\ 3.4e-5 & -2.4e-3 & -2.3e-3 & 4.7e-3 \\ 2.8e-4 & -0.081 & 4.7e-3 & -0.044 \end{bmatrix}$$

$$B = \begin{bmatrix} 1.2e-5 & -1.6e-4 & 3.4e-5 \\ -1.6e-4 & -2.5e-3 & -2.4e-3 \\ 3.4e-5 & -2.4e-3 & -2.3e-3 \end{bmatrix}$$

$$k = [\,1.4e-4 \quad -1.3e-4 \quad -4.8e-3\,]'$$

$$w = \beta\Phi(-\beta) - \varphi(-\beta) = -0.04037$$

$$x = \prod_{i=1}^{n-1} (1+\beta k_i)^{-0.5} = 1.00328$$

$$y = \prod_{i=1}^{n-1} (1+(1+\beta)k_i)^{-0.5} = 1.00571$$

$$z = \text{Real}\left(\prod_{i=1}^{n-1} (1+(i+\beta)k_i)^{-0.5}\right) = 1.00327$$

$$\Psi(-\beta) = \frac{\varphi(-\beta)}{\Phi(-\beta)} = 1.81707$$

$$p_{f_{FORM}} = \Phi(-1.35597) = 0.08756$$

$$p_{f_{SORM}}(Breitung) = \Phi(-\beta)x = 0.08784$$

$$p_{f_{SORM}}(Hohenbichler) = \Phi(-\beta)\prod_{i=1}^{n-1} (1+k_i\Psi(\beta))^{-0.5} = 0.08794$$

$$p_{f_{SORM}}(Tvedt) = \Phi(-\beta)x + w(x-y) + (1+\beta)w(x-z) = 0.08794$$

$$p_{f_{SORM}}(exact) = 0.08794$$

Example 7 The state of stress at most critical point is written in terms of principle stresses as:

$$\sigma_1 = 600P_2 + 9P_1$$
$$\sigma_2 = 400P_2 + 18P_1$$
$$\sigma_3 = -18P_1$$

Table 8.7 Parameters of random variables

Variables	Distribution	Mean	Std. Deviation
P_1	Normal	150	30
P_2	Normal	6	3
σ_y	Normal	16,000	1600

The limit state function (Von Mises theory) is

$$g(X) = \sigma_y^2 - \left(\sigma_1^2 + \sigma_2^2 + \sigma_3^2 - \sigma_1\sigma_2 - \sigma_2\sigma_3 - \sigma_1\sigma_3\right)$$

Distribution parameters of random variables are given in Table 8.7. Find reliability index and failure probability?

where $P_{1,}$ $P_{2,}$ and σ_y are applied loads in lbs and yield strength of material used respectively.

Solution: From FORM iteration scheme (Calculations in Table 8.8),

$$u_i^* = (\frac{\partial g}{\partial u_i})\frac{\sum u_i \frac{\partial g}{\partial u_i} - g(u_i)}{\sum (\frac{\partial g}{\partial u_i})^2}$$

$$p_f = \Phi(-\beta) = 2.731\text{e - }4$$

Table 8.8 Calculations

Iter. Number	1	2	3	4	5
$u_{P_1}^*$	0	0.8547	1.327	1.3448	1.3401
$u_{P_2}^*$	0	1.3432	2.1504	2.2058	2.2002
$u_{\sigma_y}^*$	0	−2.985	−2.4117	−2.2966	−2.3053
g	1.96E8	1.46E7	−2.00E6	2.33E4	2.43E1
$\frac{\partial g}{\partial u_{P_1}}$	−1.47E7	−2.0E7	−2.28E7	−2.29E7	−2.29E7
$\frac{\partial g}{\partial u_{P_2}}$	−2.30E7	−3.2E7	−3.73E7	−3.76E7	−3.76E7
$\frac{\partial g}{\partial u_{\sigma_y}}$	5.12E7	3.59E7	3.89E7	3.94E7	3.94E7
$\alpha_{u_{P_1}}$	−0.2527	−0.38	−0.389	−0.3876	−0.3877
$\alpha_{u_{P_2}}$	−0.3971	−0.616	−0.6381	−0.6364	−0.6364
$\alpha_{u_{\sigma_y}}$	0.8823	0.6904	0.6644	0.6668	0.6668
β	3.383	3.493	3.4566	3.457	3.457

SORM

$$\beta = 3.457006$$

$$D = \begin{bmatrix} -2106 & -28800 & 0 \\ -28800 & -560000 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

$$R_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -0.387664 & -0.636447 & 0.66682 \end{bmatrix}$$

$$R = \begin{bmatrix} 0.86452 & 0 & 0.502598 \\ -0.319877 & 0.7713204 & 0.5502213 \\ -0.387664 & -0.636447 & 0.66682 \end{bmatrix}$$

Gradient length = 3.490709e15

$$A = \begin{bmatrix} -0.0020865 & 0.003582 & 0.0639336 \\ 0.003582 & -0.00615 & 0.07388 \\ 0.0639336 & 0.07388 & -0.02249 \end{bmatrix}$$

$$B = \begin{bmatrix} -0.0020865 & 0.003582 \\ 0.003582 & -0.00615 \end{bmatrix}$$

$$\begin{aligned}
k &= [0 \quad -0.008236] \\
w &= \beta\Phi(-\beta) - \varphi(-\beta) = -6.933e-5 \\
x &= \prod_{i=1}^{n-1} (1 + \beta k_i)^{-0.5} = 1.01455 \\
y &= \prod_{i=1}^{n-1} (1 + (1+\beta)k_i)^{-0.5} = 1.0189 \\
z &= \mathrm{Real}\left(\prod_{i=1}^{n-1} (1 + (i+\beta)k_i)^{-0.5}\right) = 1.01452 \\
\Psi(-\beta) &= \frac{\phi(-\beta)}{\Phi(-\beta)} = 3.7109 \\
p_{f_{FORM}} &= \Phi(-1.35597) = 2.731e-4 \\
p_{f_{SORM}}(Breitung) &= \Phi(-\beta)x = 2.770787e-4 \\
p_{f_{SORM}}(Hohenbichler) &= \Phi(-\beta)\prod_{i=1}^{n-1}(1 + k_i\Psi(\beta))^{-0.5} = 2.773773e-4 \\
p_{f_{SORM}}(Tvedt) &= \Phi(-\beta)x + w(x-y) + (1+\beta)w(x-z) = 2.773703e-4 \\
p_{f_{SORM}}(exact) &= 2.7737027e-4
\end{aligned}$$

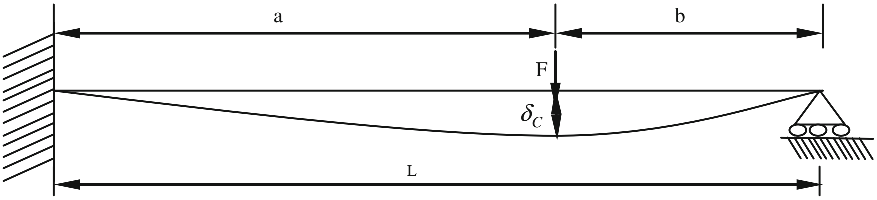


Fig. 8.5 Deflection of prismatic beam

Example 8 A prismatic beam of length L with moment of inertia I is clamped on one side and simply supported on the other side (Fig. 8.5). It is loaded by a point force F at point C at a distance 'a' from the clamped side. The deflection at the point of application of load, δ_C is written as,

$$\delta_c = \frac{Fa^2b}{2EI}\left[\left(\frac{2a+3b}{6L}\right)\left\{3-\left(\frac{b}{L}\right)^2\right\}-1\right]$$

Determine the probability when δ_C greater than 3 mm. The performance function and distribution parameters of random variables are given in Table 8.9.
Solution: Performance function is

$$\delta_c = \frac{Fa^2b}{2EI}\left[\left(\frac{2a+3b}{6L}\right)\left\{3-\left(\frac{b}{L}\right)^2\right\}-1\right]$$

This is a non-linear performance problem with random variables having extreme-I and lognormal distributions. In this problem Rosenblatt transformation is used.

First Order Reliability Method (FORM)

Approach using Rosenblatt Transformation

The transformations required are:

$$F = x_0 - \frac{1}{\alpha}\ln(-\ln(\Phi(u_F)))$$
$$E = e^{\overline{\mu}+\overline{\sigma}u_E}$$

Table 8.9 Performance function and random variables

Performance function	$g(x) = 3 - KF/E$; $K = 1.4523e8$;			
Variables	Distribution	Mean	Std. deviation	Other parameters
F	Extreme TypE-I	995	78	$\alpha = 0.01644$ $x_0 = 959.897$
E	Lognormal	7e10	7e9	$\overline{\mu} = 24.9717115$ $\overline{\sigma} = 0.09975134$

Table 8.10 Calculations

Iter. no.	1	2	3	4	5	6	100
u_F^*	0	2.2	2.221	2.1768	2.169	2.1677	2.1674
u_E^*	0	−3.08	−1.72	−1.6873	−1.6966	−1.6983	−1.6987
g	0.952	−0.46	−0.029	−0.00022	−2.4E-06	−7.2E-08	0
$\left(\frac{\partial g}{\partial u_F}\right)^*$	−0.146	−0.44	−0.389	−0.3826	−0.382	−0.3819	−0.3818
$\left(\frac{\partial g}{\partial u_E}\right)^*$	0.204	0.34	0.302	0.2993	0.2993	0.2993	0.2993
α_{u_F}	−0.58	−0.79	−0.79	−0.7877	−0.7872	−0.7871	−0.7871
α_{u_E}	0.81	0.614	0.6126	0.6161	0.6167	0.6168	0.6169
β	3.79	2.813	2.7542	2.7538	2.7537	2.7537	2.7537

From FORM iteration scheme (Calculations in Table 8.10),

$$u_i^* = (\frac{\partial g}{\partial u_i})\frac{\sum u_i \frac{\partial g}{\partial u_i} - g(u_i)}{\sum (\frac{\partial g}{\partial u_i})^2}$$

$$p_f = \Phi(-\beta) = 0.0029459$$

SORM

$$\beta = 2.78409$$

$$D = \begin{bmatrix} -0.128 & -0.038 \\ -0.038 & 0.03 \end{bmatrix}$$

$$R_0 = \begin{bmatrix} 1 & 0 \\ -0.789 & 0.615 \end{bmatrix}$$

$$R = \begin{bmatrix} 0.615 & 0.789 \\ -0.789 & 0.615 \end{bmatrix}$$

Gradient length = 0.486925

$$A = \begin{bmatrix} -0.138 & 0.177 \\ 0.177 & -0.064 \end{bmatrix}$$

$$k = -0.1376$$

$$w = \beta\Phi(-\beta) - \varphi(-\beta) = -8.03e - 4$$

$$x = \prod_{i=1}^{n-1} (1 + \beta k_i)^{-0.5} = 1.27312$$

$$y = \prod_{i=1}^{n-1} (1 + (1 + \beta) k_i)^{-0.5} = 1.44429$$

$$z = \mathrm{Real}\left(\prod_{i=1}^{n-1} (1 + (i + \beta) k_i)^{-0.5}\right) = 1.2502$$

$$\begin{aligned}
\Psi(-\beta) &= \frac{\varphi(-\beta)}{\Phi(-\beta)} = 3.08319 \\
p_{f_{FORM}} &= \Phi(-1.35597) = 0.0026839 \\
p_{f_{SORM}}(Breitung) &= \Phi(-\beta)x = 0.003417 \\
p_{f_{SORM}}(Hohenbichler) &= \Phi(-\beta) \prod_{i=1}^{n-1} (1 + k_i \Psi(\beta))^{-0.5} = 0.003537 \\
p_{f_{SORM}}(Tvedt) &= \Phi(-\beta)x + w(x - y) + (1 + \beta)w(x - z) = 0.0034849 \\
p_{f_{SORM}}(exact) &= 0.0034742228
\end{aligned}$$

8.6 System Reliability

A real structure consists in general of many elements. Performance of these elements affects the overall performance of system. In many cases individual element can have different modes of failure. These failure modes affect system reliability. In system reliability analysis overall system reliability is calculated [8–12].

8.6.1 Classification of Systems

Depending upon how performance of system gets affected by performance of different components they are classified into series system, parallel system and combined series-parallel system.

8.6.1.1 Series System

Different components of system are in series when failure of any one component leads to failure of system.

Consider the truss shown in Fig. 8.6 as a system. Failure of any member of this truss leads to failure of system. Hence this is example of series system. Series system is also called as weakest link system.

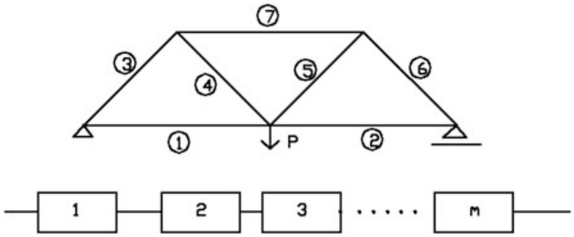


Fig. 8.6 Statically determinate structure as series system

If E_i denotes the failure of component i, then the failure of a series system is the event

$$E_s = E_1 \cup E_2 \cup \ldots \cup E_m$$

Series system fails if at least one-safety margin is negative.

The failure probability is thus

$$P_f = P\left[\bigcup_{j=1}^{k} \{g_j(z) \leq 0\}\right]$$

8.6.1.2 Parallel System

Different components of system are in parallel (Fig. 8.7) when failure of all components leads to failure of system. In other words system is safe if any of the component of system is safe.

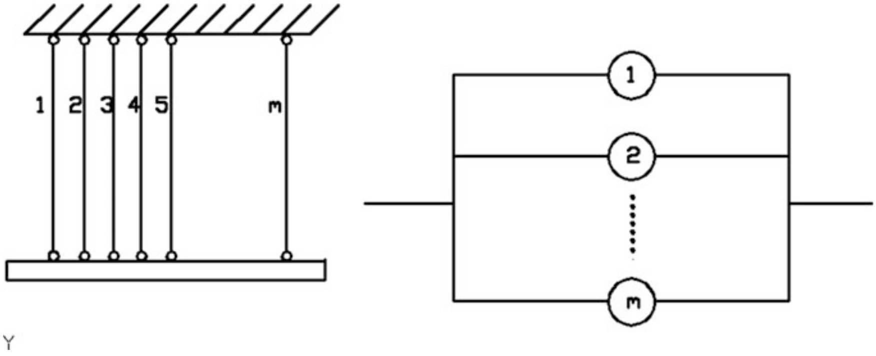


Fig. 8.7 Parallel system

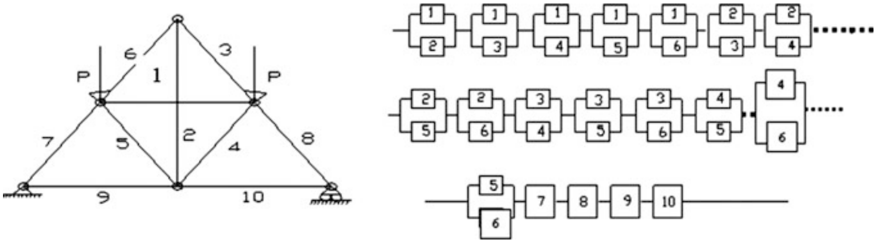


Fig. 8.8 Combined series-parallel system

If E_i denotes the failure of component i, then the failure of a parallel system is the event

$$E_s = E_1 \cap E_2 \cap \ldots \cap E_m.$$

Parallel system fails if all safety margins are negative.

The failure probability is thus

$$P_f = P\left[\bigcap_{j=1}^{k} \{g_j(z) \leq 0\}\right]$$

8.6.1.3 Combined Series-Parallel Systems

Many structures can not be modeled as either series systems nor parallel systems. Such systems are modeled as combined series-parallel system (Fig. 8.8)

These types of systems are modeled as series system of parallel subsystems (series arrangement of minimal cut structures) or parallel systems of series subsystems (parallel arrangement of minimal path series structures).

The failure probability of a series system of parallel subsystem is

$$P_f = P\left[\bigcup_{i=1}^{k}\left(\bigcap_{\gamma=1}^{l_i} \{g_{i\gamma}(z) \leq 0\}\right)\right]$$

where k is number of subsystems and l_i is the number of element in ith parallel subsystem.

8.6.2 Evaluation of System Reliability

In a first order reliability analysis, the failure set is approximated by the polyhedral set bounded by the tangent hyperplanes at the design point. Then evaluation of reliability of structural system with several potential modes involves the integration of multivariate distributions, $\Phi_m(c, R)$, defined as

$$\Phi_m(c,R) = P\left[\bigcap_{k=1}^{m}(X_k \le c_k)\right] = \int_{-\infty}^{c_m} \cdots \int_{-\infty}^{c_1} \frac{|R|^{1/2}}{(2\pi)^{m/2}} \exp\left[-\frac{1}{2}X^T R^{-1} X\right] dx_1 \ldots dx_m \tag{8.17}$$

where m denotes number of failure modes, $c(m)$ is vector of reliability indices, $x(m)$ is a vector of normal standard correlated normal variables, and $R(m \times m)$ is the correlation matrix.

Methods for multinormal integration can be classified into four broad categories:

1. Numerical integration
2. Bounding techniques
3. Approximate methods
4. Monte-Carlo simulation

8.6.2.1 Numerical Integration

Direct numerical integration of multinormal distributions with high accuracy and efficiency is difficult and impractical, especially when $m > 5$. However, the evaluation can be reduced to a one-dimensional integration, if the correlation structure is of the form, $r_{ij} = \lambda_i \lambda_j$.

$$\Phi(c,R) = \int_{-\infty}^{+\infty} \varphi(u) \prod_{i=1}^{m} \Phi\left(\frac{c_i - \lambda_i u}{\sqrt{1-\lambda_i^2}}\right) du \tag{8.18}$$

where $\varphi(u)$ is the standard normal density function. The advantage of such a single integral representation is that it is easy to evaluate numerically. In case that all the correlations are equal, i.e., $r_{i,j} = r$ and $c_i = c$, above can be further simplified to

$$\Phi(c,R) = \int_{-\infty}^{+\infty} \varphi(u) \Phi\left(\frac{c - u\sqrt{r}}{\sqrt{1-r}}\right)^m du \tag{8.19}$$

8.6.2.2 Bounding Techniques

Conceptually, the estimation of upper and lower bounds to mathematically exact probability of failure is an attractive alternative over the calculation of multinormal integrals. Effective bounding formulae are available to estimate the reliability of series systems. The main benefit is that most bounding formulae require only 2nd and 3rd order intersection probabilities, which are easy to calculate. Bounding formulae developed for series systems are of little use for parallel systems, as they tend to be too wide to be meaningful.

Unimodal Bounds

Unimodal bounds for series system are given by

$$\max p_{Fi} \le p_F \le 1 - \prod_{i=1}^{k} (1 - p_{Fi}) \tag{8.20}$$

Unimodal bounds for parallel system are given by

$$0 \le p_F \le \min p_{Fi} \tag{8.21}$$

These bounds are too wide to use.

Bimodal bounds for series system are given by

$$p_{F1} + \sum_{i=2}^{k} \max\left[\left\{p_{Fi} - \sum_{j=1}^{i-1} P(E_i E_j)\right\}; 0\right] \le p_F \le \sum_{i=1}^{k} p_{Fi} - \sum_{i=2 j<i}^{k} \max\left[\left(P(E_i E_j)\right)\right] \tag{8.22}$$

where $P(E_i E_j)$ can be calculated using following integral,

$$P(E_i E_j) = \Phi_2\left(-\beta_i, -\beta_j; \rho_{ij}\right) = \varphi(-\beta_i)\varphi(-\beta_j) + \int_0^{\rho_{ij}} \varphi_2(-\beta_i, -\beta_j; z) dz \tag{8.23}$$

Bimodal bounds similar to above are not derived for parallel system. Although above bounds can be used on complimentary parallel system, they are very wide.

8.6.2.3 Approximate Methods

Recognizing the difficulties associated with the integration and bounding techniques Hohenbichler and Rackwitz applied first-order concepts to develop an efficient, and in fact, the most widely used method for multinormal integration (Crude FOMN and Improved FOMN). This approach was later refined by Tang and Melchers (Generalized FOMN) [8–10]. Pande proposed another method, called as PCM method, which is simple and computationally efficient.

FOMN

This method is explained below with aid of following example. Consider a parallel system with three equicorrelated and equireliable elements with $\beta_1 = \beta_2 = \beta_3 = 0.1$ and r = 0.5. Here correlation matrix is

$$\rho_{ij} = \begin{bmatrix} 1 & 0.5 & 0.5 \\ 0.5 & 1 & 0.5 \\ 0.5 & 0.5 & 1 \end{bmatrix}$$

By Choleskey's defactorisation

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 0.5 & 0.8666 & 0 \\ 0.5 & 0.288 & 0.816 \end{bmatrix}$$

Now three performance functions are

$$\begin{aligned} g_1 &= z_1 + \beta_1 \\ g_2 &= 0.5z_1 + 0.866z_2 + \beta_2 \\ g_3 &= 0.5z_1 + 0.288z_2 + 0.816z_3 + \beta_3 \end{aligned}$$

Failure probability of system is

$$p_f = P\left[\bigcap_{k=1}^{3}\left(\left(\sum_{j=1}^{3} b_{kj}z_j + \beta_j\right) \le 0\right)\right] \text{ or}$$

$$\begin{aligned} p_f &= P(E_1 \cap E_2 \cap E_3) = P(E_1) \times P(E_2 \cap E_3/E_1) \\ &= \Phi(-\beta_1) \times P[(E_2 \cap E_3)/z_1 + \beta_1 \le 0)] \end{aligned}$$

To solve second term of RHS: $P[(E_2 \cap E_3)/z_1 + \beta_1 \le 0)] = ?$
Conditional distribution of z_1 is $\Phi(z_1)/\Phi(-\beta_1)$. Using Rosenblatt transformation

$$z_1 = \Phi^{-1}(\Phi(\bar{z}_1) \times \Phi(-\beta_1))$$

Here $\bar{z}_1$ is standard normal variable.
Substituting above equation in performance functions g_2 and g_3

$$\begin{aligned} g_2 &= 0.5 \times \Phi^{-1}(\Phi(\bar{z}_1) \times \Phi(-\beta_1)) + 0.866z_2 + \beta_2 \\ g_3 &= 0.5 \times \Phi^{-1}(\Phi(\bar{z}_1) \times \Phi(-\beta_1)) + 0.288z_2 + 0.816z_3 + \beta_3 \end{aligned}$$

Above function are nonlinear. Linearizing these at MPP

$$\begin{aligned} g_2 &= 0.3168\bar{z}_1 + 0.948z_2 - 0.2942 \\ g_3 &= 0.3168\bar{z}_1 + 0.3161z_2 + 0.8942z_3 - 0.2942 \\ P[(E_2 \cap E_3)&/z_1 + \beta_1 \le 0)] = P(g_2 \le 0 \cap g_3 \le 0) \end{aligned}$$

This can be calculated using single integration.

$$P[(E_2 \cap E_3)/z_1 + \beta_1 \leq 0)] = 0.44$$
$$p_f = \Phi(-\beta_1) \times 0.44 = 0.2025$$

Method used for solving above problem is known as Crude-FOMN.

To improve the accuracy, the probability estimation of g_2 and g_3 needs to be improved. For this purpose, Hohenbichler suggested the shifting of the hyperplane at the design point without changing the direction cosines. This approach is referred to as Improved FOMN. As a further refinement, Tang and Melchers suggested to integrate exactly the conditional probability term. This can be done as

$$P[E_2/z_1 + \beta_1 \leq 0] = P(g_2 \leq 0) = \Phi_2(-\beta_1, -\beta_2, 0.5)/\Phi(\beta_1) = 0.3589$$

similarly,

$$P[E_3/z_1 + \beta_1 \leq 0] = 0.3589$$

Hence new linearized performance functions are

$$\begin{aligned} & g_2 = 0.3168\bar{z}_1 + 0.948z_2 - 0.3589 \\ & g_3 = 0.3168\bar{z}_1 + 0.3161z_2 + 0.8942z_3 - 0.3589 \\ & P[(E_2 \cap E_3)/z_1 + \beta_1 \leq 0)] = P(g_2 \leq 0 \cap g_3 \leq 0) = 0.4682 \\ & p_f = \Phi(-\beta_1) \times 0.4682 = 0.2155 \end{aligned}$$

The method employed above is known as G-FOMN. Exact failure probability of above problem is calculated using numerical integration which is 0.2150

PCM Method

This method is proposed by Pandey [13]. Multinormal integral can be approximated to the product of conditional marginals as

$$\Phi_m(c, R) = \prod_{k=1}^{m} \Phi(c_{k|k-1}) \tag{8.24}$$

where

$$c_{m|k} = \frac{c_{m|(k-1)} + r_{mk|(k-1)} A_{k|(k-1)}}{\sqrt{1 - r^2_{mk|(k-1)} B_{k|(k-1)}}} \tag{8.25}$$

where

$$r_{mk|(k-1)} = \frac{r_{mk|(k-2)} - r_{k(k-1)|(k-2)} r_{m(k-1)|(k-2)} B_{(k-1)|(k-2)}}{\sqrt{(1 - r^2_{k(k-1)|(k-2)} B_{(k-1)|(k-2)})} \sqrt{(1 - r^2_{m(k-1)|(k-2)} B_{(k-1)|(k-2)})}} \tag{8.26}$$

This method is computationally very efficient and its accuracy is comparable to G-FOMN.

Example 9 Consider a parallel system with seven components. Performance function for these components is given below.

$$\begin{aligned}
g_1 &= u_2 - 3\\
g_2 &= -0.7071u_1 + 0.7071u_2 - 1.94454\\
g_3 &= 0.7071u_1 + 0.7071u_2 - 1.94454\\
g_4 &= -0.8944u_1 + 0.4472u_2 - 0.89443\\
g_5 &= 0.8944u_1 + 0.4472u_2 - 0.89443\\
g_6 &= -0.9487u_1 + 0.31621u_2 - 0.23717\\
g_7 &= 0.9486u_1 + 0.3162u_2 - 0.23717
\end{aligned}$$

Calculate the probability of failure.

Solution: Performance function of all the components given have form

$$g = \alpha_1 u_1 + \alpha_2 u_2 - \beta$$

The correlation matrix is calculated by

$$\rho = \alpha\alpha'$$

$$\rho = \begin{bmatrix} 1 & 0.7071 & 0.7071 & 0.4472 & 0.4472 & 0.3162 & 0.3162 \\ & 1 & 0 & 0.9487 & -0.3162 & 0.8944 & -0.4472 \\ & & 1 & -0.3162 & 0.9487 & -0.4472 & 0.8944 \\ & & & 1 & -0.600 & 0.9899 & -0.7071 \\ & & sym & & 1 & -0.7071 & 0.9899 \\ & & & & & 1 & -0.800 \\ & & & & & & 1 \end{bmatrix}$$

Unimodal bounds

$$\begin{gathered} 0.998650 \le p_s \le 1 \quad \text{or} \\ 0 \le p_f \le 0.00134989803163 \end{gathered}$$

Bimodal bounds

From numerical integration (Table 8.11)

The bimodal bounds for the problem are given by,

$$\begin{gathered} 0.9990600 \le p_s \le 0.999488 \\ 5.1197\text{e}{-004} \le p_f \le 9.3941\text{e}{-004} \end{gathered}$$

Table 8.11 Calculations

i, j	$P(E_1E_2)$	$P(\bar{E}_1\bar{E}_2)$
1, 2	0.000939	0.973675
1, 3	0.000403	0.973675
1, 4	0.000756	0.814099
1, 5	0.001316	0.814099
1, 6	0.001234	0.593468
1, 7	0.00108	0.593468
2, 3	0.018309	0.948842
2, 4	0.025665	0.814447
2, 5	0.004808	0.789676
2, 6	0.003999	0.593735
2, 7	0.002062	0.569885
3, 4	0.025915	0.789676
3, 5	0.001138	0.814447
3, 6	0.00061	0.569885
3, 7	0.000138	0.593735
4, 5	0.008602	0.632209
4, 6	0.009355	0.593736
4, 7	0.003632	0.417546
5, 6	0.184735	0.417546
5, 7	0.18012	0.593736
6, 7	0.384302	0.221579

G-FOMN Method

$$p_f = 5.2393e{-4}$$

Exact system reliability can be calculated as follows.

$$\begin{aligned} p_F &= p_{F_1} - 2(p_{F_1} - P(1 \cap 2) + p_{F_2} - P(2 \cap 4) + p_{F_4} - P(4 \cap 6)) \\ &= 5.1607e{-4} \end{aligned}$$

Example 10 Consider a truss in Fig. 8.9. Since this is statically determinate structure, the failure of any member constitutes failure. Therefore the truss is a series system with its members representing the components. Let L denote the load acting on the truss. Neglecting the buckling failure mode, let X_i, i = 1, 2, …,7 denote tensile/compressive strength of member. Suppose the load has deterministic value L = 100 and the member strengths X_i, i = 1, 2, …,7. are jointly normally distributed random variables with X_1 and X_2 having means and standard deviations 20 and X_3-X_7 having means 200 and standard deviations 40.

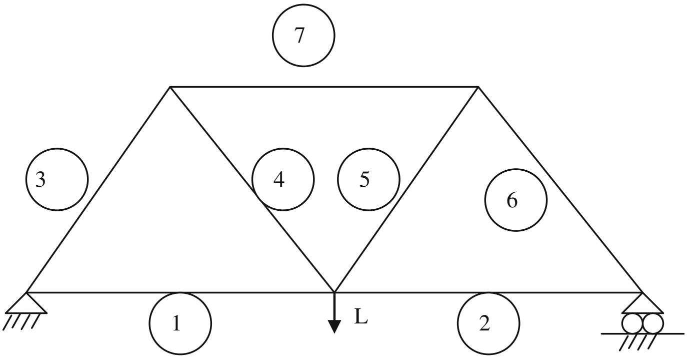


Fig. 8.9 Statically indeterminate structure as series system

Performance function is:

$$g_i = \begin{cases} X_i - L/2\sqrt{3} & for \quad i = 1,2 \\ X_i - L/\sqrt{3} & for \quad i = 3,4,\ldots,7 \end{cases}$$

Solution: Using mean value theorem—$\beta = 3.557$

Suppose that X_i have a correlation matrix, which is specified as $\rho_{ij} = r_i r_j$, where

$$r_1 = 0.9,\ r_2 = 0.96,\ r_3 = 0.91,\ r_4 = 0.95,\ r_5 = 0.92,\ r_6 = 0.94,\ \text{and}\ r_7 = 0.93$$

Unimodal Bounds

$$1.878e - 4 \leq p_f \leq 1.31e{-3}$$

Modified unimodal bounds—using Dunnet and Sobel Formula:

$$5.993e - 4 \leq p_f \leq 8.25e{-4}$$

Taking average correlation coefficient

$$p_f = 7.2334e{-4}$$

Bimodal Kounias, Hunter and Ditlevsen (*KHD*) *Bounds*

The bimodal intersection probabilities are:

$$p_{i,j} = \begin{bmatrix} - & 0.573 & 0.4345 & 0.5418 & 0.459 & 0.5126 & 0.4850 \\ & - & 0.6084 & 0.7794 & 0.6465 & 0.7315 & 0.6874 \\ & & - & 0.5747 & 0.4856 & 0.5432 & 0.5135 \\ & & & - & 0.6100 & 0.6883 & 0.6477 \\ & & sym & & - & 0.5758 & 0.5438 \\ & & & & & - & 0.6107 \\ & & & & & & - \end{bmatrix}$$

In truss system number of components are 7. There are 7! = 5040 ordering alternatives. Considering all orders sharpest bound obtained is

$$4.592e{-}4 \leq p_f \leq 9.122e{-}4$$

Crude-FOMN Method

$$p_f = 9.5557e - 4$$

I-FOMN Method

$$p_f = 7.5730e - 4$$

G-FOMN Method

$$p_f = 6.5529e - 4$$

Exact Result (Dunnet and Sobel formula)

$$p_f = 7.1886e - 4$$

References

1. Madsen HO, Krenk S, Lind NC (1986) Methods of structural safety. Prentice-Hall Inc, Englewood Cliffs
2. Melchers RE (1999) Structural reliability analysis and prediction. Wiley, Chichester
3. Nowak AS, Collins KR (2000) Reliability of structures. McGraw Hill Higher Education, Singapore
4. Ranganathan R (1990) Reliability analysis and design of structures. Tata McGraw-Hill Publishing Company Limited, New Delhi
5. Hasofer AM, Lind NC (1974) Exact and invariant second-moment code format. J Energy Mech Division ASCE 100(1):111–121
6. Rackwitz R (2001) Reliability analysis: a review and some perspectives. Struct Saf 23:365–395
7. Haldar A, Mahadevan S (2000) Reliability assessment using stochastic finite element analysis. Willey, New York
8. Hohenbichler M, Rackwitz R (1983) First-order concepts in system reliability. Struct Saf 1:177–188
9. Rackwitz R (1997) Methods of system reliability in multidimensional spaces. Probabilistic methods for structural design. Kluwer Academic Publishers, Netherlands, pp 161–212
10. Tang LK, Melchers RE (1987) Improved approximation for multinormal integral. Struct Saf 4:81–97
11. Thoft-Christensen P, Murotsu Y (1986) Application of structural systems reliability theory. Springer, Berlin
12. Ang AH-S, Tang WH (1984) Probability concepts in engineering planning and design, vol II. Decision, risk, and reliability. Wiley, New York
13. Pandey MD (1998) An effective approximation to evaluate multinormal integrals. Struct Saf 20(1):51–67

Chapter 9
Maintenance of Large Engineering Systems

9.1 Introduction

Engineering systems or plants such as that present onboard naval ships or large industrial installations are a very complex mix of equipment. The machinery can be classified based on their functions into plants such as the main propulsion plant, air conditioning plants, distilled water plants, power generation plants etc. These plants mostly function independently of each other and have their own redundancies however, for the operation of the whole industry or ship, it is important that these plants be operational. Each plant may further comprise many equipment such as motors, pumps, valves and in case of propulsion plants, diesel engines or gas turbines, reduction gears and so on. The hardware for each plant makes it unique to that particular configuration of similar makes and types of equipment. The operation and maintenance profiles of the machinery for industrial plants and that of naval ships are more or less similar except for the fact that for some of the onboard equipment, the expertise and resources required for maintenance may not exist onboard and the ship may have to return to harbor for purposes of maintenance or repair. Because such requirements incur high maintenance cost in terms of lost opportunities, such equipment and their specific maintenance/repair requirements are considered to be more critical than the others. Except for this peculiarity, the machinery set-up of a large industry and a ship are considered to be similar and therefore reference made to machinery set-up of ship in this chapter can be interchangeably used for that of any industry.

The types of equipment, their configurations and use, available redundancies, criticality of their operational availability for availability of the whole plant etc. each play a dominant role in framing of the maintenance policy for the plant. In addition to the above, operational profile of the plant, maintenance objectives for the plant as a whole, impact of non-availability of the plant on safety of men and environment, resource constraints, etc. too play a very significant role in shaping up the maintenance strategy for each specific type of plant. All this complex mix of

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_9

factors makes every plant unique, as far as its maintenance requirements to meet the chosen objectives go. It is this uniqueness of every plant that hinders development of a common general model to address all its maintenance decision problems. There are various factors that have a direct bearing on maintenance optimization models, Horenbeek et al. [1]. For instance, factors like the operating profile, planning horizon, operation cycle, failure data etc. would play the role of key inputs in defining the boundaries of the maintenance problem we want to model. On the other hand decisions regarding inclusion of wear or deterioration into the model, the type of the problem and its optimisation objectives would decide the technique to be used in generating the desired solutions from the model.

Un-availability of a common general maintenance optimization model is one of the key reasons that there is a wide gap between the academic models and its applications in a business specific context (Horenbeek et al. [1]). As far as the available literature on maintenance optimization models go, authors such as Dekker [2, 3], Scarf [4] and Horenbeek et al. [1] have collectively surveyed more than 300 works on the subject. It has been brought out by them that most of the research work on the subject has been carried out at an individual component or equipment level. Studies are often used only to demonstrate the applicability of a developed model, rather than finding an optimal solution to a specific problem of interest to a practitioner. Another limitation perceived in literature is that most of the models focus on only one optimization criterion, making multi-objective optimization models an unexplored area of maintenance optimization. Although single objective optimization is attractive from the modeling point of view, this approach does not capture all important aspects of a real life situation. The aim of this chapter is to address the maintenance optimization issues that are faced in a large industrial set-up or say a naval ship. Maintenance issues at individual equipment level that have been addressed in scores of papers on the subject have been purposely left out.

9.2 Peculiarities of a Large Setup of Machinery

Machinery and systems present on board a ship or an industry can be classified in accordance with their role or function they perform into broader groups called plants. Each plant consists of machinery that need some amount of maintenance periodically to keep them in a healthy working state. The peculiarity that exists with large machinery set-up is that any major maintenance required on particular plant machinery can render the whole ship ‘unavailable’ for its mission requirements. To maximize the availability of the ship, it is therefore prudent that the maintenance jobs on all the plants of the particular ship are synchronized to occur at the same time. Generally the maintenance jobs carried out during such time intervals, also called as ‘refit’, are the ones that are major in nature and generally beyond the scope of the maintenance personnel present onboard ships. Minor maintenance jobs that can be carried out by the ships’ staff themselves can however be progressed independently of the refit times in such a way so that the downtime of the concerned plant and that of the whole ship is kept to bare minimum.

Another issue with large machinery set-up is that the planned preventive maintenance jobs can at times be shelved for some immediate mission requirements. Such urgent missions for a finite duration can be preceded by a limited time window for maintenance jobs. In such a scenario, maintenance decisions need to be taken so as to choose the optimal set of maintenance actions on a host of machinery such that multiple objectives of maximum availability and minimum cost are met within the constraints of time and maintenance manpower resources.

Most of the maintenance decision models available in the literature talk about one or at the maximum two units. It is generally assumed that its application to multiple unit systems would be an extrapolation of the approach for the single unit system. However, such assumptions are incorrect because for a complex mix of equipment, existing for example on a ship, the various types of equipment, dependence of systems, their structure, redundancies etc. play a major part in influencing the overall maintenance decisions for the ship's machinery. Maintenance decisions for such complex systems therefore, need to be taken at different levels of the plant hierarchy. For example at the system level of a plant one may have to decide whether the policy to be adopted for a system valve or a pneumatic air reducer should be one of breakdown maintenance or preventive maintenance? For some other machinery for example a sea water pump, the question could be whether to adopt a time or a condition based maintenance. Criticality of the equipment, redundancies available, spares availability onboard ship, time taken to repair and cost thereof, corrective maintenance cost and outcomes, failure distributions for different modes, all play an important part in making such a decision. Once the policy for a particular equipment has been decided, the maintenance parameter (for e.g. time interval for preventive replacement) will then need to be considered in the decisions making process at the higher level of plant hierarchy.

Similarly, decisions such as to replace the entire equipment or only a failed component of an equipment is the one that needs to be taken at an equipment level. Failure distributions of the critical maintainable components of the equipment, their ages or time in operation, cost and downtime of repair for the equipment and its components, planning time horizon all play an important role in making such a decision. Here again, once the decision of handling the equipment at component or the equipment level is taken, it remains fixed and the relevant maintenance parameter is then considered in the decision making process at the higher level.

Other decisions that are taken at the lower level are logistics related, for example, number of spares of equipment, such as whole units (for e.g. valves) or spare critical components of equipment are also the ones that depend on the criteria mentioned above. These decisions also play a major role in improving the efficacy of the maintenance decisions taken at higher level of the ship machinery.

At a plant level however the maintenance decision may be taken for the optimum fixed time interval for maintaining the particular equipment along with the other major equipment of the plant. The need therefore is to view the ship machinery in its entirety and develop a frame work for making appropriate maintenance decision at equipment level and also at plant level so that the benefits of the maintenance actions on the entire ship machinery is maximized.

9.3 Prioritizing the Machinery for Maintenance Requirements

A solution strategy which caters to all the problems discussed in this sub-section is presented below. The steps have also been displayed graphically in Fig. 9.1.

Step 1 The ship machinery can be classified according to their functions into plants. Plants with common functions but different equipment need to be clubbed together for evaluation of the redundancy available to the ship in terms of their common functions. Each plant can be further classified into systems. For example, an air conditioning plant onboard a ship would have a Freon system consisting of AC compressor, heat exchanger, a chilled water system, a cooling water system etc.

Step 2 Once the systems level equipment have been identified, a FMECA (Failure Mode Effect and Criticality Analysis) will help identify the equipment that cause critical failure of the system of the chosen plant. Each failure mode that causes critical failure needs to be identified and taken forward for further analysis. Components (mostly screw down valves, strainers etc.) which do not get included can be covered under a corrective maintenance policy or may be suitably replaced during a major refit period of the ship. Data for systems which are newly installed may not be available for carrying out FMECA and therefore maintainers would be needed to use expert knowledge and data on failure/wear of similar equipment in use. The data can then be updated later after some more experience is gained on the system.

Step 3 Data on failure of equipment per failure mode would need a lot of filtering and refining before it can be used for further analysis. It has been brought out in Verma et al. [5] that many marine equipment are constantly monitored for their performance and parameters and therefore the deterioration data or wear data of either the whole equipment or for its various components are available with the operators of the machinery. Cases where there is lack of data, the deterioration data can be a good source for evaluation of the wear process. This is only applicable to equipment which are under monitoring. Statistical analyses are then carried out to arrive at the failure distribution parameters for each failure mode including the wear or deterioration induced failures.

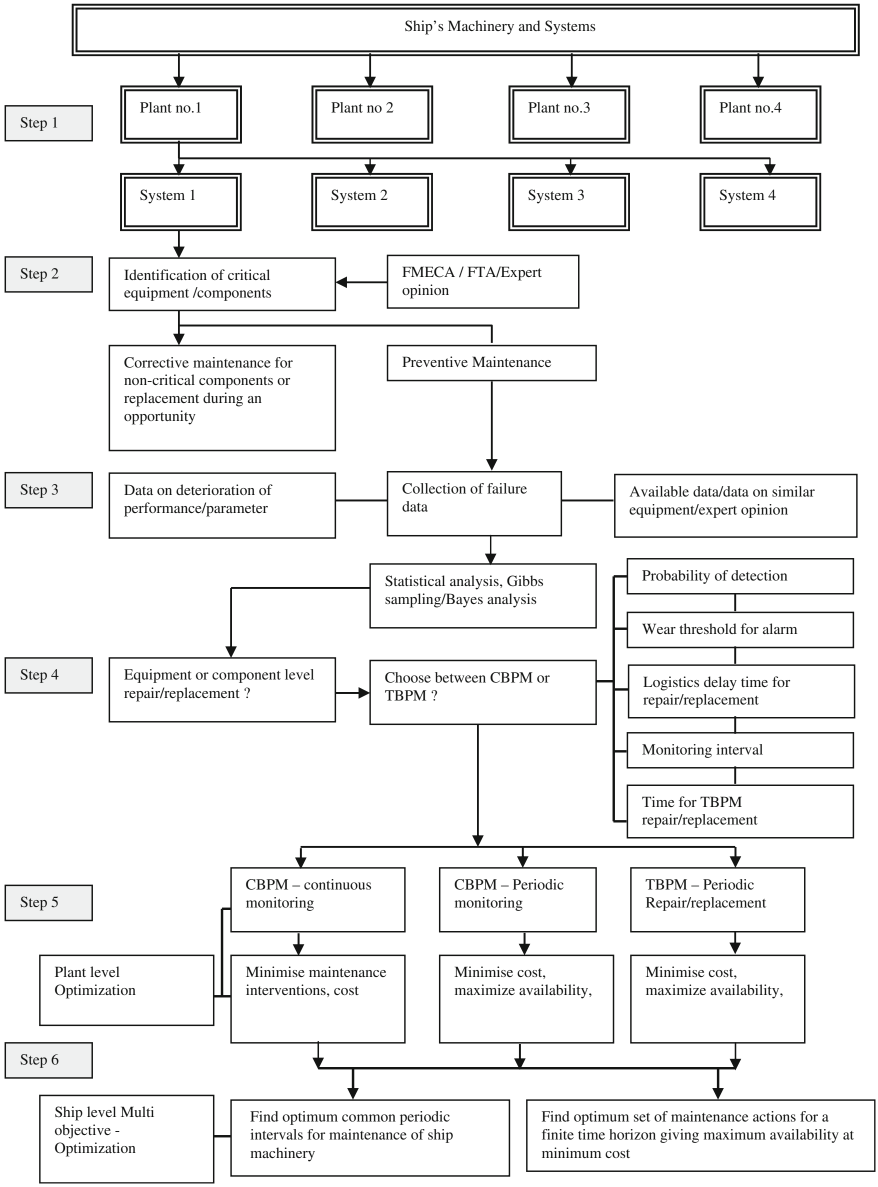

Ship's Machinery and Systems
Step 1
Plant no.1
Plant no 2
Plant no.3
Plant no.4
System 1
System 2
System 3
System 4
Step 2
Identification of critical equipment /components
FMECA / FTA/Expert opinion
Corrective maintenance for non-critical components or replacement during an opportunity
Preventive Maintenance
Step 3
Data on deterioration of performance/parameter
Collection of failure data
Available data/data on similar equipment/expert opinion
Statistical analysis, Gibbs sampling/Bayes analysis
Probability of detection
Wear threshold for alarm
Step 4
Equipment or component level repair/replacement ?
Choose between CBPM or TBPM ?
Logistics delay time for repair/replacement
Monitoring interval
Time for TBPM repair/replacement
Step 5
CBPM – continuous monitoring
CBPM – Periodic monitoring
TBPM – Periodic Repair/replacement
Plant level Optimization
Minimise maintenance interventions, cost
Minimise cost, maximize availability,
Minimise cost, maximize availability,
Step 6
Ship level Multi objective - Optimization
Find optimum common periodic intervals for maintenance of ship machinery
Find optimum set of maintenance actions for a finite time horizon giving maximum availability at minimum cost

Fig. 9.1 An overview of solution strategy

Step 4 This step includes decision to be taken at the equipment/component level. Before it can be decided whether the equipment maintenance should be covered under CBPM (Condition Based Predictive Maintenance) or TBPM (Time Based Preventive Maintenance), one needs to answer the question whether the repair needs to be done at equipment or at component level. For ships where the maintenance time for systems is at a premium, replacement rather than repair is an attractive option. Better still, if the high capital cost of equipment replacement can be balanced by less frequent failure of the components of the newly replaced equipment, it seems reasonable to go in for equipment replacement instead of replacing only the failed component of the equipment. Once the level of repair or replacement has been decided the second decision regarding going in for a TBPM or a CBPM or both needs to be made for the equipment. It is well established that the cost of preventive maintenance is always lesser than that of the corrective maintenance and therefore better the probability of ending up in PM, better is the policy chosen for the equipment. Probability of detection, wear thresholds, monitoring or PM time intervals play an important part in the decision.

Step 5 The choice of maintenance policy in the above steps is used to achieve the multiple objectives of the maintenance actions. For critical plant equipment which, are continuously monitored for multiple parameters or performances and which are periodically maintained on the basis of deterioration of the recorded parameters, there is always a need to minimize the maintenance interventions. The deterioration of the various parameters can be combined into one common parameter of overall wear or deterioration and the minor maintenance routines interventions can be minimized based on this overall parameter without running the risk of over crossing the individual wear failure levels.

Step 6 Once the maintenance policy for all the critical equipment has been identified, the stage is set for deciding on the optimum maintenance actions for the ship machinery. The unique feature of a large set up like a ship, imposes special conditions for carrying out maintenance actions on her machinery.

As brought out earlier, ship are brought into repair/maintenance periodically. This means that even though there are a large number of equipment whose maintenance is based on a TBPM and many other where the maintenance actions are based on a CBPM, there has to be found a common time interval where the maintenance actions of as many of them should be undertaken so as to minimise the overall maintenance cost and maximize the availability during the off-repair period. This is a MOOP (Multi-objective optimization problem) and needs an equivalent treatment. A similar problem is faced while deciding on the maintenance that needs to be taken in a short time so as to prepare the ship for a forthcoming urgent operational mission. In such a condition, the maintenance manager can be tasked to undertake best possible set of actions to see that given the constraints of manpower resource and time, availability of the ship is maximized during the mission time and the overall cost of maintenance and repair is minimized.

The present chapter focuses on the methods to prioritize the machinery for maintenance in a large set-up and to resolve the MOOP problems faced during scheduling of maintenance of such large setups as shown in step 6 of Fig. 9.1.

9.3.1 Hierarchical Level of Machinery

A breakdown of ship's machinery into various plants, into systems and then to equipment levels is shown in Fig. 9.2. We take an example of an air conditioning plant, a schematic diagram of which is shown in Fig. 9.3. The plant has got a variety of equipment such as pumps, motors, measuring devices, air blowers etc. Few of the equipment are such that they can cause serious problems in the availability of the plant and would need more time to repair, whereas failure of some others may have only marginal effect on the plant.

Defects on few of the equipment may become immediately evident; for example if the air blower shuts out or the chilled water pump fails, the plant will immediately become non-functional. There are some other equipment for example, the safety relays such as the low pressure (LP) cut-outs or the high pressure (HP) cut outs whose failure is not immediately evident. All these characteristics of the occurrence of the defects, their severity and detection can be summarised in the FMECA (Failure Mode Effect and Criticality Analysis) table. However, before we move onto such a table, we first briefly describe the functioning of the air conditioning plant shown in the Fig. 9.3 and touch briefly on the topic of the FMECA.

The AC (air conditioning) plant is one of the several plants onboard ship which provide conditioned air to living spaces and more importantly to machinery spaces and weapon compartments. The AC plant comprises many systems such as the refrigerant or the freon system, the sea water systems, chilled water system, control system etc. All these systems are essential for functioning of the AC plant.

Each of these systems have equipment, which are critical for the availability of the system and therefore for availability of the plant itself.

The AC plant systems have the following functions:

- Refrigerant or the Freon system: The freon is the medium which removes heat from the chilled water system. A compressor compresses the gaseous refrigerant and pumps it down to an oil separator. The oil separator separates the lubricating oil from the refrigerant gas. The gas is then pushed to a condenser. In the condenser the gas is cooled into liquid and pumped towards an oil filter and drier. The drier removes any moisture present in the refrigerant and then allows the refrigerant to pass through an expansion valve. The expansion valve helps in reducing the pressure on the condensed liquid and as a result the refrigerant vaporises, absorbs heat from the evaporator and cools the chilled water circulated through it (evaporator).

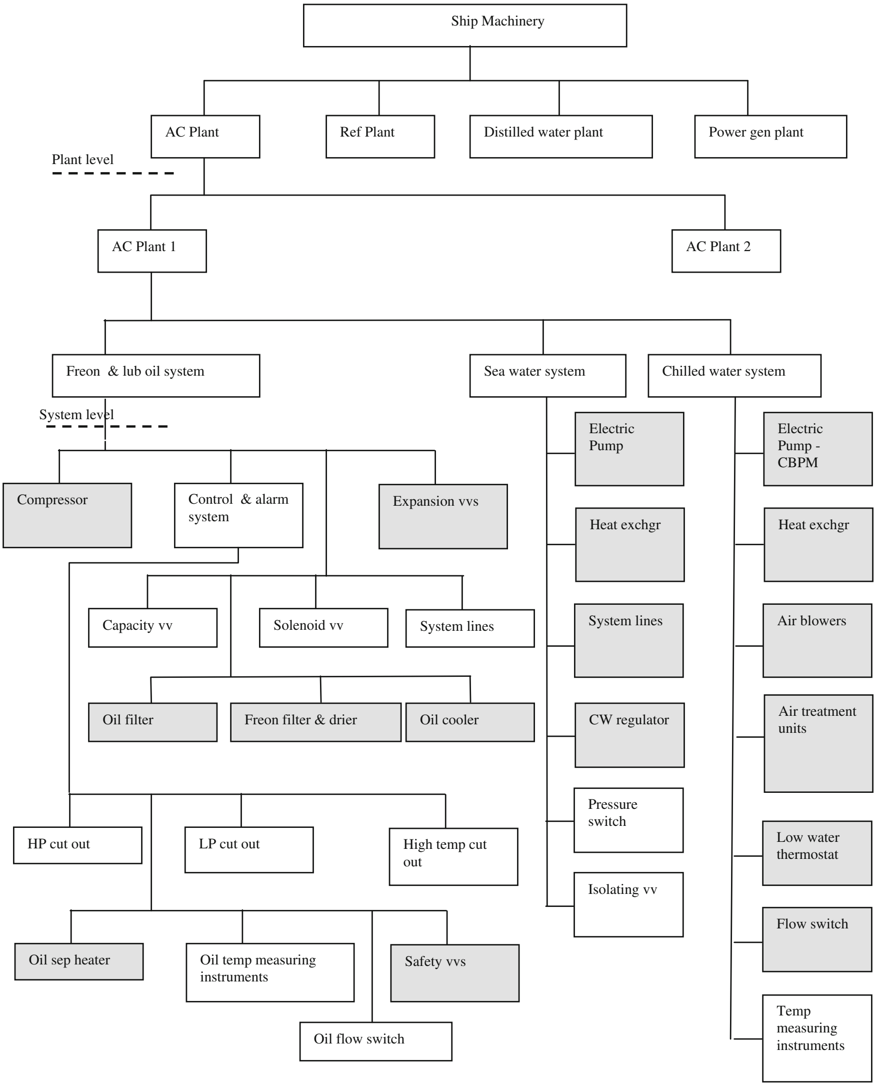


Fig. 9.2 Breakdown of ship's machinery into various levels: AC plant

- Lubricating oil system: The system does not have any moving components. The oil from compressor is separated from the freon gas in the oil separator and cooled inside a cooler before being returned to compressor again
- Chilled water system: The system consists of a motor driven pump which forces the chilled water through the evaporator. In the evaporator the chilled water is cooled down and it is then circulated inside air coolers. Air inside air coolers transfer their heat to the chilled water.

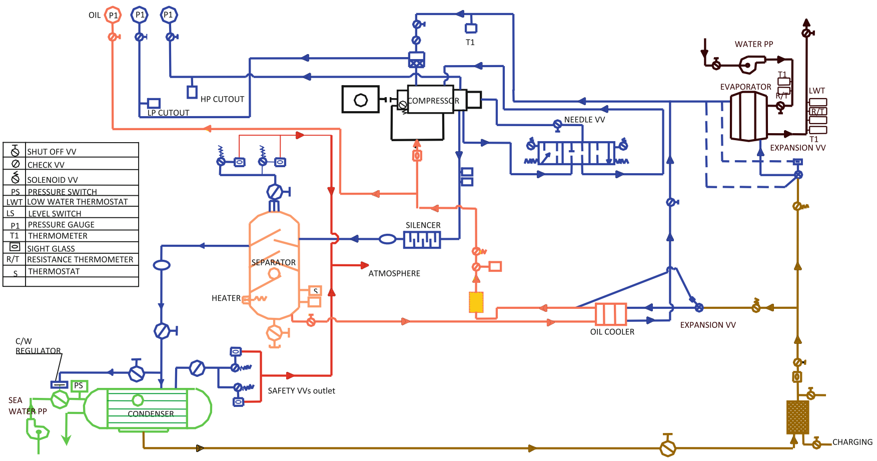


Fig. 9.3 Schematic diagram of a ship's AC plant

- Sea water system: A sea water pump circulates sea water through the condenser where it helps in condensing the freon vapours. The sea water is then pumped overboard.
- Control and instrumentation system: the system consists of a variety of equipment and instruments that provide safety to the plant and control its operation. These system devices are part of the various other systems mentioned above. A capacity control system is also part of this system. This system controls the cooling capacity according to the heat load on the system.

9.3.2 *FMECA (Failure Mode Effect and Criticality Analysis)*

FMECA is basically a systematic method to identify and rank potential failure modes of a system in terms of its criticality such that the remedial actions can be taken to rectify them in a cost effective way. Although FMECA should be initiated for a new system during the design phase, it is found to be beneficial even for a system already in use. FMECA provides a baseline for safety analysis, maintenance plan analysis and for failure detection and isolation of subsystem design. Although cost is not a main objective of this analysis, it typically does result in an overall reduction in cost to operate and maintain the plant. It also provides a baseline for identifying the corrective actions for a given failure. This information can then be used to perform various other analyses such as fault tree analysis (FTA) or a reliability centered maintenance (RCM) analysis.

FMECA is actually undertaken in two parts, the first is the FMEA (failure mode and effect analysis) and the second the CA (criticality analysis). The FMEA is carried out to study the results of effects of item failure on system operation and to classify each potential failure according to its severity. The CA on the other hand provides relative measures of the significance of the effects of a failure mode. It helps in ranking the significance of each potential failure for each component in the system's design based on failure rate (or occurrence), a severity ranking and its detectability. Details on procedure for performing a FMECA analysis is given in detail in a variety of manuals and documents as given below. Each such document may have its own subtle difference with one another in order to improve its applicability and usefulness to the organisation it serves.

- MIL-STD 1629A "Procedures for performing a failure mode, effects and criticality analysis"
- SEMATECH (1992) "Failure Modes and Effects Analysis (FMEA): A Guide for Continuous Improvement for the Semiconductor Equipment Industry"
- BS 5760-5 "Guide to failure modes, effects and criticality analysis (FMEA and FMECA)"
- SAE J1739 "Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes

The method of carrying out FMECA is available in the literature in detail and therefore only an example of such an analysis on the air conditioning plant shown above is demonstrated in this chapter.

9.3.2.1 FMEA

FMEA as described above is limited to the study the effects of item failure on the system or plant operation and to classify them in terms of their severity. However, the complexity of a plant or system may make it difficult to identify all the failures and its various effects on the system or plant. Therefore, generally two primary approaches are used for carrying out FMEA. One is the hardware approach which lists down individual hardware items of the plant (as shown in the AC plant schematic drawing above) and analyses their possible failure modes. The other is a functional approach. In this approach every hardware item's function is identified and listed down as its output. Failure to provide this output can then be termed as a failure mode for the item which will have its local effect and also some end effect on the plant to which it belongs. Help of reliability block diagrams (RBDs) can be taken as and when necessary to identify the functional interdependencies for the system while using the functional approach. Severity classification will be assigned to each failure mode which can then be utilised to establish priorities for corrective actions. Higher priority are assigned to severe failures and then to the next level and so on. An example of severity classification chart and occurrence classification are shown in the Tables 9.1 and 9.2. Table 9.3 gives an example of a FMEA carried out on the AC plant component namely, the AC compressor shown in Fig. 9.3.

Table 9.1 Severity classification [6]

Ranking	Effect	Comments
1	None	No reason to expect failure to have any effect on safety, health, environment or mission
2	Very low	Minor disruption to facility function. Repair to failure can be accomplished during trouble call
3	Low	Minor disruption to facility function. Repair to failure may be longer than trouble call but does not delay mission
4	Low to moderate	Moderate disruption to facility function. Some portion of mission may need to be reworked or process delayed
5	Moderate	Moderate disruption to facility function. 100 % of mission may need to be reworked or process delayed
6	Moderate to high	Moderate disruption to facility function. Some portion of mission is lost. Moderate delay in restoring function
7	High	High disruption to facility function. Some portion of mission is lost. Significant delay in restoring function
8	Very high	High disruption to facility function. All of mission is lost. Significant delay in restoring function
9	Hazard	Potential safety, Health or environmental issue. Failure will occur with warning
10	Hazard	Potential safety, Health or environmental issue. Failure will occur without warning

Table 9.2 Occurrence classification [6]

Ranking	Effect	Comments
1	1/10000	Remote probability of occurrence; unreasonable to expect failure to occur
2	1/5000	Very low failure rate. Similar to past design that has, had low failure rates for given volume/loads
3	1/2000	Low failure rate based on similar design for given volume/loads
4	1/1000	Occasional failure rate. Similar to past design that has, in the past, had similar failure rates for given volume/loads
5	1/500	Moderate failure rate. Similar to past design having moderate failure rates for given volume/loads
6	1/200	Moderate to high failure rate. Similar to past design having moderate failure rates for given volume/loads
7	1/100	High failure rate. Similar to past design having frequent failures that caused problems
8	1/50	High failure rate. Similar to past design having frequent failures that caused problems
9	1/20	Very high failure rate. Almost certain to cause problems
10	1/10+	Very high failure rate. Almost certain to cause problems

Table 9.3 Example of a FMEA sheet carried out on AC plant

Failure modes and effects analysis (FMEA)

	System: AC plant		Date: Dec 2011	
	Part name: AC compressor		Sheet: 2 of 56	
	Reference drawing: XX/46565/xx		Compiled by: XX	
	Mission: Compress refrigerant gas according to the heat load requirement		Approved by: XXX	

Item number	Item/functional ID	Potential failure modes	Failure mechanism	Failure effects			Detection method	Compensating provision	Severity class	Remarks
				Local	Next	End				
110.0	Compress refrigerant between: 5–10 bar At 50–80 °C Give noise and vibration less operation <80 dB and <6 mm/sec	No compression	Motor winding burnt, no power, relay malfunctioning, mechanical failure of compressor, coupling failure	AC plant down	–	No cooling	By operator	Redundant plant	4	–
		Low compression <5 bar	Gas leakage, capacity control valve malfunctioning, expansion valve choked	Low efficiency of plant,	High energy consumption	Reduced cooling effect	By operator	Redundant plant	3	–
		High compression > 10 bar and >80 °C	Air ingress into system, reduced cooling in condenser and relay faulty	Low efficiency of plant,	High energy consumption	Reduced cooling effect	By operator	Redundant plant	3	–
		Abnormal noise and vibration >80 dB and >6 mm/sec	Defective bearing, coupling failure, deteriorated SV mounts	No significant effect	–	Vibration and noise emanated to ship's hull	By operator	Redundant plant	6	Warship machinery need to be quiet during operation

9.3.2.2 CA (Criticality Analysis)

Criticality analysis can be carried out either qualitatively or quantitatively. Criticality analysis provides a comparison between the significance of various failure modes in terms of their failure rate (quantitative) or occurrences (qualitative) and the consequences of these failures. It is a tool that ranks the significance of each potential failure as well as the significance of an entire piece of equipment or system, on safe, successful operation and mission requirements. A quantitative method is generally used when parameters such as failure rates for each failure mode, failure mode ratios and the failure effect (once the failure has taken place) probabilities are known quantitatively. These parameters can then be used to calculate a parameter called the "failure mode criticality number" which is then used to prioritise the failure modes. The following definitions need to be understood before a quantitative approach can be used:

- Failure effect probability (β): Given that the relevant failure mode occurs, β is the probability that the end effect will occur. For example, if power failure occurs $\beta = 1$ that the end effect will be that the AC compressor will stop functioning. However, if a failure mode is say, a safety device not working and the end effect is AC plant failure, β in this situation will be less than 1.
- Failure rate (λ_p): it is the number of failures per unit of time of the item under consideration.
- Failure mode ratio (α): It is the probability that the given part or item will fail in the identified mode. The probability is expressed as a fraction of the sum of αs for all the failure modes of the item. For function failure, for example of the AC compressor, all the failure mode ratios (α) for failure modes of the compressor will equal to 1.
- Failure mode criticality number (C_m): It is a relative measure of the frequency of a failure mode. It is calculated as the product of β, α, λ_p and the operating time 't'. This parameter helps in ranking of the failure modes.
- Item criticality number ($C_r = \Sigma C_m$): It is the sum of failure mode criticality number of the same severity class.

Table 9.4 gives an example of a FMECA carried out on the AC plant compressor using the quantitatively approach. It may be noticed that the most of the information in the table is obtained from the FMEA carried out earlier in Table 9.3. The information of FMEA table is then carried out forward to perform a criticality analysis, in this case using a quantitative analysis.

A qualitative method of CA on the other hand, is used when the failure rates for the failure modes are not known and the criticality or risk associated with each failure is to be classified subjectively by the experienced personnel. In this approach, instead of using the failure rates for failure modes, an occurrence rank is used. However, while doing so care must be taken to use the occurrence classification equal in number of ranks to the severity classifications. An example of Occurrence Classification chart is shown in Table 9.2 below.

Table 9.4 Example of a FMECA sheet carried out on AC Plant using the quantitative approach

Quantitative failure modes, effects and criticality analysis (FMECA)

	System: AC plant								Date: Dec 2011		
	Part name: AC compressor								Sheet: 2 of 56		
	Reference drawing: XX/46565/xx								Compiled by: XX		
	Mission: Compress refrigerant gas according to the heat load requirement								Approved by: XXX		
Item number	Item/functional ID	Potential failure modes	Failure mechanism	Severity	Failure rate (λ_p)	Failure effect probability (β)	Failure mode ratio(α)	Operating time (t)	Failure mode criticality number (C_m)	Item criticality number (ΣC_m)	Remark
110.0	Compress refrigerant between: 5–10 bar At 50–80 °C Give noise and vibration less operation <80 dB and <6 mm/s	No compression	Motor winding burnt, no power, relay malfunctioning, mechanical failure of compressor, coupling failure	4	6.24×10^{-6}	1	0.5	10^4	0.0312	0.0312	
		Low compression <5 bar	Gas leakage, capacity control valve malfunctioning, expansion valve choked	3	1.2×10^{-4}	1	0.15	10^4	0.18	0.88	
		High compression >10 bar and >80 °C	Air ingress into system, reduced cooling in condenser and relay faulty	3	2.8×10^{-4}	1	0.25	10^4	0.7		
		Abnormal noise and vibration >80 dB and >6 mm/s	Defective bearing, coupling failure, deteriorated SV mounts	6	9.3×10^{-4}	1	0.1	10^4	0.93	0.93	

Some CA methods also use detection rankings to complete the analysis of the criticality of the failure modes. For qualitative methods it is essential that the detection rankings also be of same magnitude as that of the occurrence and severity rankings. After assigning the occurrence, severity and detection rankings, a risk priority number (RPN) is calculated as the product of these rankings. The RPN in a qualitative approach of CA is used for ranking the failure modes in terms of their occurrence and consequences (severity). Table 9.5 gives an example of a FMECA carried out on the AC plant compressor using the qualitative approach. In the given example detection rankings of the system has not been used.

9.3.2.3 Criticality Ranking

Once the FMECA analysis is completed, various failure modes can be listed down, starting with the highest RPN number or the failure mode criticality number, down to the least. This kind of ranking helps in having a quick overview of the failure modes in order of its priority. When the quantitative approach is used, criticality ranking can be carried out either on the basis of failure mode criticality or the item criticality number, however the former is considered to be a better choice.

FMECA Summary

FMECA helps in identification of the critical failure modes of a plant or a system so that the repair and the maintenance actions on the concerned equipment or component of the plant can be prioritized. The systematic nature of the analysis also helps in identification of potential failure modes that could have otherwise been skipped by the maintenance manager from addressing. It also helps bring to light the kind of monitoring or corrective actions that may be required to obviate the occurrence of the failure mode itself. In the FMECA example shown in Sect. 9.3.2 only a single component—AC compressor failure mode has been discussed. Since the aim of the present work is not to present a detailed application of FMECA technique, which is already available in literature (see Sect. 9.3.2), the example of the analysis of AC compressor failure modes gives a snap shot of how to list down the failure modes and mechanisms while carrying out an analysis in practice. Though in the present context FMECA was mainly being discussed for use in identification of a prioritized list of maintenance requirements, its real use is in the design stage of a system for carrying out maintainability, safety and logistics analysis. Here it is considered to be an iterative process, where the information is regularly updated and the efficacy of the FMECA keeps improving with time and experience. The subjective assessment made during the CA process gets improved to the quantitative assessments and the new methods of defect monitoring or prediction gets included in the process thus bringing down the severity of the concerned failure modes.

Table 9.5 Example of a FMECA sheet carried out on AC Plant using the qualitative approach

Qualtitative failure modes, effects and criticality analysis (FMECA)										
	System: AC plant							Date: Dec 2011		
	Part name: AC compressor							Sheet: 2 of 56		
	Reference drawing: XX/46565/xx							Compiled by: XX		
	Mission: compress refrigerant gas according to the heat load requirement							Approved by: XXX		
=Item number	Item/functional ID	Potential failure modes	Failure mechanism	Failure effects			Occurrence	Severity	RPN	Remark
				Local	Next	End				
110.0	Compress refrigerant between: 5–10 bar At 50–80 °C Give noise and vibration less operation <80 dB and <6 mm/sec	No compression	Motor winding burnt, no power, relay malfunctioning, mechanical failure of compressor, coupling failure	AC plant down	–	No cooling	1	4	4	–
		Low compression <5 bar	Gas leakage, capacity control valve malfunctioning, expansion valve choked	Low efficiency of plant,	High energy consumption	Reduced cooling effect	2	3	6	–
		High compression > 10 bar and >80 °C	Air ingress into system, reduced cooling in condenser and relay faulty	Low efficiency of plant,	High energy consumption	Reduced cooling effect	2	3	6	–
		Abnormal noise and vibration >80 dB and >6 mm/sec	Defective bearing, coupling failure, deteriorated SV mounts	No significant effect	–	Vibration and noise emanated to ship's hull	2	6	12	–

For the machinery which are present onboard a ship, all repair and maintenance actions which need attention of the repair personnel present ashore need to be identified separately. These maintenance actions need higher priority and need to be clubbed together as a group so as to optimise the period of stay of ship in harbour. All the maintenance actions which can be carried out by the ship's staff can be treated differently as a group and for these actions, optimal intervals for the time based PM actions and optimal monitoring intervals for condition based PM actions can be evaluated separately. The maintenance actions which are of low priority and need to be undertaken only in harbour can be undertaken during the major repair or refit period of the ship. Maintenance actions of low priority which can be undertaken by the ship's staff can be undertaken by them as and when it occur (corrective maintenance). Since maintenance actions that require yard assistance present ashore have high opportunity costs, corrective maintenance policy for such cases are avoided.

For the subject AC plant, maintenance actions in each of the discussed category have been brought out below.

Maintenance Actions in harbour by Ashore staff

- Time based maintenance actions: Compressor overhaul and mandatory replacement of parts, sea water system-heat exchanger cleaning and pressure testing, chilled water system-heat exchanger cleaning and pressure testing, sea water system line inspection and renewal, Freon system safety valve calibration
- Condition based maintenance actions: electric pump—chilled water system, electric pump—sea water system, air blowers—chilled water system, change of shock and vibration mounts

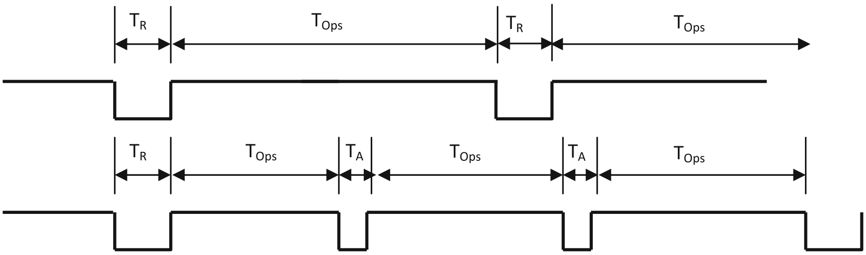
Maintenance Actions by Ship's staff

- Time based maintenance actions: checking of relays for operation, checking for Freon system leaks, cleaning of drier and filter
- Condition based maintenance actions: replacing of oil filter, charging of gas, expansion valve calibration and replacement
- Corrective maintenance: replacement of freon system valves, replacement of temperature sensors

9.4 Maintenance Scheduling of a Large Setup of Machinery

9.4.1 Introduction

As has been brought out earlier, a ship consists of a variety of plants each with a different function. There might also be redundancies available in the plants that improve its reliability. These plants in turn will consist of many equipment. There



T_R – Refit time. Major ship equipment are under repair. Ship is down.
T_{Ops} – Operational time. The ship is operational
T_A – A short maintenance period when a few select equipment are under maintenance. The ship is down.

Fig. 9.4 Operation and maintenance cycle of a ship

could be some equipment which follow a time based preventive maintenance, TBPM and there would be others that follow a CBPM. However, by virtue of being present on the same platform, as that of a ship, we will have to find out what is the most optimal time interval 'T' for carrying out maintenance on all these equipment. Such a time period for maintenance on the ship equipment is called 'Refit' in naval parlance.

The search for such an optimal time schedule seems to be a simple optimization problem, but it is not. The reason, as will be shown with an example, are the advantages that accrue from following a staggered, but grouped time schedules for some, but not all the equipment. The figure below would provide a much needed clarification.

In Fig. 9.4 above 'T_R' is the scheduled refit or repair period for the ship, wherein the majority or all of the equipment will be brought under maintenance. The T_{Ops} is the operational time for the ship where she fulfills all her mission commitments. In the first cycle of the figure, the maintenance manager finds out the optimal time for refit T_R. The objectives are cost rate and average reliability during the operational time of the ship. This is the general trend in the maintenance planning function. What has been observed in the research work is that, if the "operational time" of a ship is given to be say, not less than T_{ops}, then by bringing up a small select group of equipment under maintenance, both the above stated objectives can be improved. Such short maintenance intervals may be called "short maintenance period" (MP) and these can be scheduled in between the refit periods of the ship. Though in the Fig. 9.4 it appears that the bottom cycle has a shorter operational time T_{Ops} this may not be the case.

The strategy shown in Fig. 9.4 however requires solution of a multi-objective optimisation problem with multiple variables. The variables for the optimisation problem can be listed down as follows:

- Selection of equipment that need to be maintained during MP (maintenance period)
- Scheduling of the maintenance period T_A (T_{mp}) after completion of refit

- Total number of MPs (maintenance periods required between the refit period)
- Scheduling of refit period T_R (T_{rp}) after completion of the previous refit

Among the other variables are the MP and/or the refit duration, however, these are values that are generally ‘given’ and can be considered to be constraints of the multi-objective problem being discussed.

9.4.2 Example

The above approach to the problem can be demonstrated taking an example of a ship system. We consider a group of 03 main plants of a ship comprising 13 equipment (Fig. 9.5). The power generation plant has a redundancy. The life distribution and its assumed parameters are listed in Table 9.6. The search is for an optimal maintenance plan for the entire ship such that the ship is available for operations at least for a minimum period of ‘T_{Ops}’ at the maximum average reliability ‘AvgRelb’ and at the minimum maintenance cost rate ‘Costrate’.

Initially we consider the case without any MP (or short maintenance periods). In this case the search is for a common time where all the equipment would be maintained together. The problem equation can be written as:

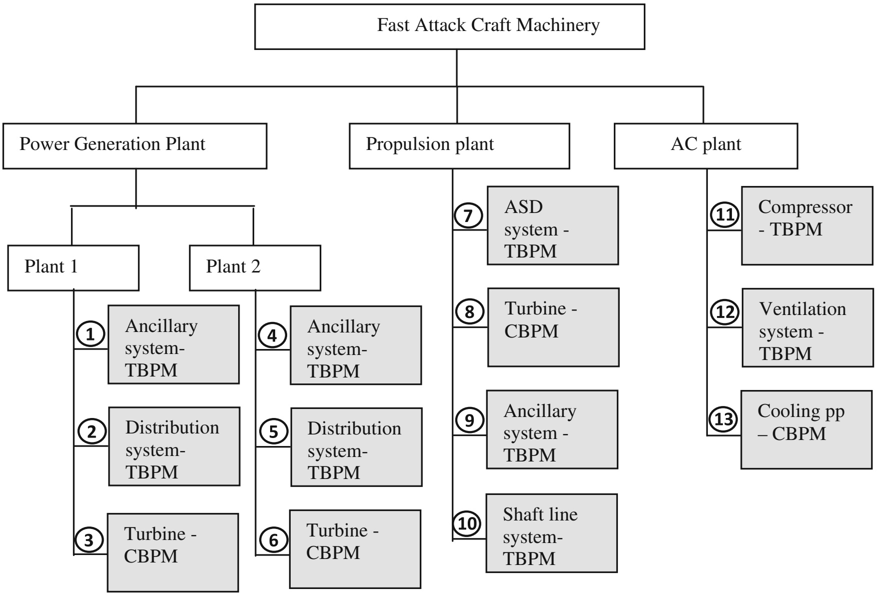


Fig. 9.5 Schematic list—group of three plants of a attack craft

Table 9.6 Parameters of distribution of the 13 equipment example

S. no.	Equipment/component	Distribution	Scale parameter	Shape parameter	Cost	Man power
1	Plant 1—ancillary system	Weibull	150	1.109	1200	3
2	Plant 1—distribution system	Weibull	465	1.3	4000	2
3	Plant 1—Turbine	Gamma	0.089	0.97	550	3
4	Plant 1—Ancillary system	Weibull	150	1.109	1200	3
5	Plant 1—distribution system	Weibull	465	1.3	4000	2
6	Plant 1—Turbine	Gamma	0.089	0.97	550	3
7	Propulsion plant—ASD system	Weibull	907	2.9	19000	2
8	Propulsion plant—Turbine	Gamma	0.075	0.52	5500	4
9	Propulsion plant—Ancillary system	Weibull	95	1.1	650	3
10	Propulsion plant—Shaft line system	Weibull	200	1.43	1100	2
11	AC plant—compressor	Weibull	340	2.109	1200	4
12	AC plant—Ventilation system	Weibull	139	1.02	1100	4
13	AC plant—Cooling pump	Gamma	0.045	0.82	1200	2

$$\begin{array}{l} \text{OBJECTIVES} \\ \min_T[Costrate(T)] \\ \max_T[Average\,\mathrm{Re}lb(T)] \\ \text{s.t.} \end{array} \tag{9.1}$$

$$\begin{aligned} \text{costrate(T)} &= \frac{Exp\,cost\,of\,failure(T) + C_{PM} \cdot \mathrm{Re}lb(T)}{\int_0^T \mathrm{Re}lb(t)dt} \\ Average\,Relb(T) &= \frac{\int_0^T \mathrm{Re}lb(t)dt}{T} \end{aligned} \tag{9.2}$$

where

$$\text{Relb(T)} = \prod_{i=1}^{i=n} R_i(T)\left(1 - \left[1 - \prod_{j=1}^{j=n} R_j(T)\right] \cdot \left[1 \prod_{k=1}^{k=n} R_k(T)\right]\right) \tag{9.3}$$

$$\mathit{Exp\ cost\ of\ failure}(T) = \sum_{\mathrm{j}=1}^{\mathrm{n}} \int_{0}^{\mathrm{T}} \mathrm{f_j}(x) \prod_{i \neq j}^{n} R_i(x) \cdot [1 - \prod R_k(x)] \\ \left(\mathrm{Cost_j} + \mathrm{N_{Rj}} \cdot \mathrm{T_{Rj}} \cdot \mathrm{Cost_R} + C_{Oprn}(\mathrm{T_{Rj}} + \mathrm{T_{RH}} + \mathrm{T_{LD}})\right) dx \tag{9.4}$$

Where j and k are equipment belonging to the plants which have a hot redundancy with each other and

E[]	set of equipment selected to undergo maintenance during MP
N_{Ri}	number of people required for maintenance of equipment ‘i’
T_{Ri}	Time required for maintenance of equipment ‘i’
T_{RH}	Time required for ship to reach harbour
T_{LD}	Logistics delay time
age_i	age of equipment ‘i’ measured from completion of previous refit. Since all equipment ε E[] are maintained at every MP, age for such equipment = 0 after every MP
$Cost_i$	‘i’ equipment cost
C_{Opm}	cost of opportunity
$Cost_R$	Cost of repair action per time per repair crew
$f_i(.)$	pdf of lifetime for equipment ‘i’
$F_i(.)$	cdf of lifetime for equipment ‘i’
$R_i(.)$	reliability of equipment ‘i’

$$\mathrm{C_{PM}} = \sum_{j=1}^{n} (\mathrm{Cost_j} + \mathrm{N_{Rj}} \cdot \mathrm{T_{Rj}} \cdot \mathrm{Cost_R})$$

Given an assumption of cost of opportunity of Rs 250,000/- and a cost of repair of Rs 3500/- per man per day and the cost of equipment and manpower as shown in the table below, we get the plots as shown in Fig. 9.6. The range of multiple objectives lay to the left of the optimal point “T = 30 days”. At this point the cost rate is 0.5478×10^5 and the average reliability during the operational duration is 0.7610.

Any time to the left of “T = 30” is also an acceptable point since the average reliability remains higher than 0.7610 but at a higher cost rate. At any time to the right of “T = 30 days” we approach a zone of lower average reliability at a higher cost rate and hence all time points to the right of “T = 30” are clearly sub-optimal. We now consider the case when we can introduce some minor/short MPs or maintenance periods in between the refit schedules. The problem equation can now be written as given in the next section.

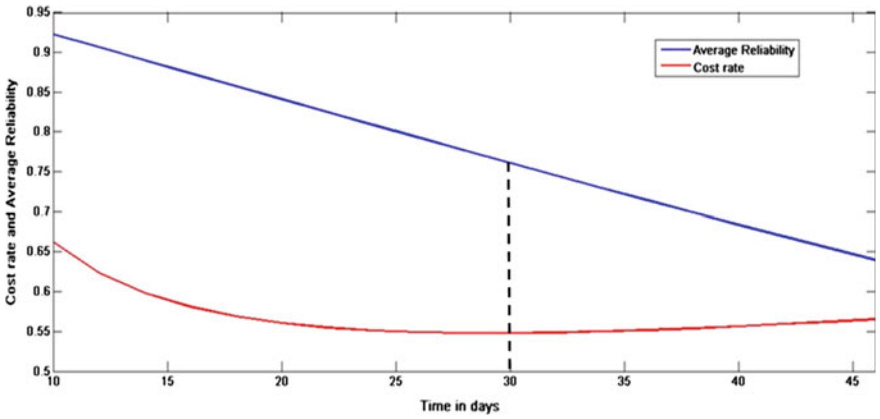


Fig. 9.6 Plot of cost rate and average reliability

9.4.3 Example—MOOP of Maintenance Interval Scheduling

We now allow some MP in between the refit periods and see what are the effects on the multiple objectives of average reliability and maintenance cost rate. The acceptance of minor maintenance intervals in between the refit period gives rise to multiple variables such as selection of equipment to be included in the minor maintenance period, time interval for carrying out such minor maintenance, time interval for scheduling the refit of the ship and number of maintenance period allowed to be carried out before the refit is carried out. The multi-objective problem for the present case can be written as follows:

$$\begin{aligned}&\text{OBJECTIVES}\\&\min\nolimits_{M[]}[Costrate(M[n_t, n_{amp}, E[], T])]\\&\max\nolimits_{M[]}[Average\,\mathrm{Re}lb(M[n_t, n_{amp}, E[], T])]\\&\text{s.t.}\end{aligned} \tag{9.5}$$

$$\text{costrate(T)} = \frac{Exp\,cost\,of\,failure(M[n_t, n_{amp}, E[], T]) + PM\,cost(M[n_t, n_{amp}, E[], T])}{\sum_{n_{amp}=1}^{n}\left[\int_{(T_{\text{Ops}}+n_t)\cdot(n_{amp}-1)}^{(T_{\text{Ops}}+n_t).(n_{amp})} \mathrm{Re}lb(t)dt\right] + \left[\int_{(T_{\text{Ops}}+n_t).(n)}^{\text{T}-\text{T}_{\text{Ramp}}} \mathrm{Re}lb(t)dt\right]} \tag{9.6}$$

$$Average\mathrm{Re}lb(M[n_t, n_{amp}, E[], T]) = \frac{\sum_{n_{amp}=1}^{n}\left[\int_{(\mathrm{T_{Ops}}+n_t)\cdot(n_{amp}-1)}^{(\mathrm{T_{Ops}}+n_t)\cdot(n_{amp})} \mathrm{Re}lb(t)dt\right]}{[T_{Ops}+n_t]n} + \frac{\left[\int_{(\mathrm{T_{Ops}}+n_t)\cdot(n)}^{\mathrm{T}-\mathrm{T_{Ramp}}} \mathrm{Re}lb(t)dt\right]}{(T-\mathrm{T_{Ramp}}) - [(\mathrm{T_{Ops}}+n_t)\cdot(n)]} \tag{9.7}$$

where

$$\mathrm{Relb}(x)\prod_{i=1}^{i=N}\frac{R_i(age_i+x)}{R_i(age_i)} \times \left(1-\left[1-\prod_{j=1}^{j=N}\frac{R_j(age_j+x)}{R_j(age_j)}\right]\cdot\left[1-\prod_{k=1}^{k=N}\frac{R_k(age_k+x)}{R_k(age_k)}\right]\right)_{\mathrm{age_i}=0\cdots\forall i\in E[]} \tag{9.8}$$

where j and k are equipment belonging to the plants which have a hot redundancy with each other

$$\mathrm{PMcost}(M[n_t, n_{amp}, E[], T]) = \left[\sum_{n_{amp}=1}^{n}\sum_{j=1}^{N}\left[\mathrm{Cost_j}+\mathrm{N_{Rj}}\cdot\mathrm{T_{Rj}}\cdot\mathrm{Cost_R}\right]\cdot\mathrm{Relb}((\mathrm{T_{Ops}}+\mathrm{n_t})\cdot\mathrm{n_{amp}})\right]_{j\in E[]} + \sum_{i=1}^{N}[\mathrm{Cost}_i+\mathrm{N_{Ri}}\cdot\mathrm{T_{Ri}}\cdot\mathrm{Cost_R}]\cdot\mathrm{Relb}((\mathrm{T}-\mathrm{T_{Ramp}}-(\mathrm{T_{Ops}}+\mathrm{n_t})\cdot\mathrm{n}) \tag{9.9}$$

$$\begin{aligned}
&\mathrm{Expcostoffailure}(M[n_t, n_{amp}, E[], T]) \\
&= \left[\sum_{\mathrm{n_{amp}}=1}^{n}\sum_{j=1}^{\mathrm{N}}\int_{(\mathrm{T_{Ops}}+n_t)\cdot(n_{amp}-1)}^{(\mathrm{T_{Ops}}+n_t).(n_{amp})}\frac{f_j(age_j+x)}{R_j(age_j)}\prod_{i\neq j}^{N}\frac{R_i(age_i+x)}{R_i(age_i)}\cdot\left[1-\prod\frac{R_k(age_k+x)}{R_k(age_k)}\right]\right]_{\mathrm{age_i}=0\ldots\forall i\in E[]} \\
&\quad\cdot\left[\mathrm{Cost_j}+\mathrm{N_{Rj}}\cdot\mathrm{T_{Rj}}\cdot\mathrm{Cost_R}+C_{Oprn}(\mathrm{T_{Rj}}+\mathrm{T_{RH}}+\mathrm{T_{LD}})\right]dx \\
&\quad+\left[\sum_{j=1}^{N}\int_{(\mathrm{T_{Ops}}+n_t)\cdot n}^{T}\frac{f_j(age_j+x)}{R_j(age_j)}\prod_{i\neq j}^{N}\frac{R_i(age_i+x)}{R_i(age_i)}\cdot\left[1-\prod\frac{R_k(age_k+x)}{R_k(age_k)}\right]\right]_{\mathrm{age_i}=0\ldots\forall i\in E[]} \\
&\quad\cdot\left[\mathrm{Cost_j}+\mathrm{N_{Rj}}\cdot\mathrm{T_{Rj}}\cdot\mathrm{Cost_R}+C_{Oprn}(\mathrm{T_{Rj}}+\mathrm{T_{RH}}+\mathrm{T_{LD}})\right]dx
\end{aligned} \tag{9.10}$$

where

M[] set of selected variables that affect the costrate and average reliability of the ship

$\mathrm{T_{Ops}}$ Minimum operational time the ship need to be operational after a refit or maintenance period

$\mathrm{n_t}$ Time after $\mathrm{T_{Ops}}$ when the MP is scheduled

$\mathrm{n_{amp}}$ number of MPs that are scheduled before the 'refit' of ship falls due

E[] set of equipment selected to undergo maintenance during MP

T	Time (after the previous refit) when the ship's refit falls due
T_{Ramp}	Cumulative maintenance time for equipment chosen for maintenance during MP
N_{Ri}	number of people required for maintenance of equipment 'i'
T_{Ri}	Time required for maintenance of equipment 'i'
T_{RH}	Time required for ship to reach harbour
T_{LD}	Logistics delay time
age_i	age of equipment 'i' measured from completion of previous refit. Since all equipment ϵ E[] are maintained at every MP, age for such equipment = 0 after every MP
$Cost_i$	'i' equipment cost;
C_{Opm}	cost of opportunity
$Cost_R$	Cost of repair action per time per repair crew
$f_i(.)$	pdf of lifetime for equipment 'i'
$F_i(.)$	cdf of lifetime for equipment 'i'
$R_i(.)$	reliability of equipment 'i'

9.4.4 Use of NSGA II—Elitist Genetic Algorithm Program

The above discontinuous, discrete, multi-objective, multi-variable optimisation problem can be best approached using the elitist NSGAII program [7]. A chromosome for the GA population is shown in Fig. 9.7. The chromosome contains all the multi-variables required for evaluating the health (or magnitude of its objectives).

The first 13 slots of the chromosome are for the equipment which, in this case are a total of 13. The slots can contain either a '1' or a '0' showing whether that specific equipment is selected to undergo replacement/repair during the MP or not. The 14th slot shows the number of MP (short maintenance period) selected by the chromosome. A '0' in this position would mean that there are no MPs for equipment and therefore the number '0' or '1' in any of the first 13 slots would then be irrelevant.

The 15th slot shows the time after the mandatory T_{Ops} period when the MP is being scheduled. Since time is continuous, this slot may have infinite choices. We therefore choose a small time interval Δt the multiples of which in integers can be shown in this 15th slot. A '0' in this slot would therefore mean that the MP has been scheduled right after completion of the mandatory T_{Ops} period. It has been brought

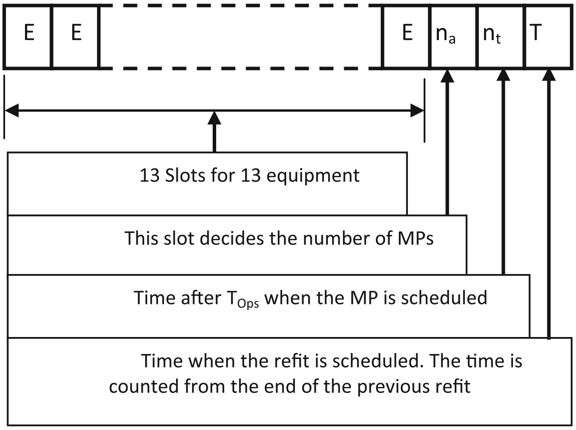

E
E
E
n_a
n_t
T
13 Slots for 13 equipment
This slot decides the number of MPs
Time after T_{Ops} when the MP is scheduled
Time when the refit is scheduled. The time is counted from the end of the previous refit

Fig. 9.7 A chromosome used for solving the NSGAII based MOOP

out before that the T_{Ops} period is the minimum time the ship should remain operational after maintenance to meet her operational commitments.

The 16th slot shows the time when the refit is scheduled. The time shown here is counted from the elapse of the previous refit period.

9.4.5 Assumptions and Result

We make the following assumptions for the example under discussion

- Maintenance actions considered are only replacement of equipment
- All maintenance actions require assistance of repair crew present ashore.
- All maintenance actions are considered sequential in nature. In actual practice simultaneous repair actions can be undertaken resulting in reduced downtime due to maintenance actions.
- Time required for maintenance is considered deterministic in nature.
- The failure of all the equipment are statistically independent in nature
- The equipment which are being monitored for wear or deterioration follow a non-stationary gamma wear process. All other equipment follow a Weibull process for failure.
- The equipment which have been selected for maintenance during MP remain fixed for every MP. In practice, we may consider to choose the equipment that can be maintained during every MP. The chromosome for solving the GA problem in this case would be 3 dimensional in nature.

The crossover probability for the example selected above is 0.8 and the mutation probability is 0.01. A random population of 40 chromosomes brings out interesting results after just 4 generations, as shown below through 02 solutions.

$$\text{Soln}\,1 = [1\quad 0\quad 1\quad 1\quad 0\quad 1\quad 0\quad 1\quad 1\quad 1\quad 1\quad 0\quad 1\quad 2\quad 0\quad 145];$$

$$\text{Cost rate} = 0.4647 \times 10^5;\ \text{Average reliability} = 0.6738$$

$$\text{Soln}\,2 = [1\quad 0\quad 1\quad 0\quad 0\quad 1\quad 1\quad 1\quad 0\quad 1\quad 1\quad 1\quad 1\quad 3\quad 6\quad 225];$$

$$\text{Cost rate} = 0.3993 \times 10^5;\ \text{Average reliability} = 0.6275$$

The above two solutions bring out two such non-dominated solutions. The first solution shows that if 09 equipment are selected to undergo 02 MPs exactly after completion of T_{Ops} of 30 days and the refit is scheduled after every 145 days the cost rate drops to 0.4647×10^5 down from 0.5478×10^5 that happens when no MP is selected. The average reliability of course drops from 0.7610 to 0.6738. The second solution also brings out another non-dominated solution. When 09 equipment are selected to undergo 03 MPs, 12 days after T_{Ops} of 30 days (or after every 42 days) and if the refit is scheduled after every 225 days, the cost rate drops further to 0.3993×10^5 but the average reliability also drops to 0.6275. When the T_{Ops} becomes 20 days we see improvement in both the objectives (Fig. 9.8). This shows that it is not optimal to put down all the equipment together for maintenance during a "refit" without keeping any short maintenance period MP in between the refit periods. The number of MPs and the scheduling of the MPs play a vital part in improving the cost rate and average reliability of the ship during the operation phase in between the refit periods. The NSGA II program routines for the example were written in Matlab 7.0. The objective values and the elite solutions are shown in Tables 9.7 and 9.8.

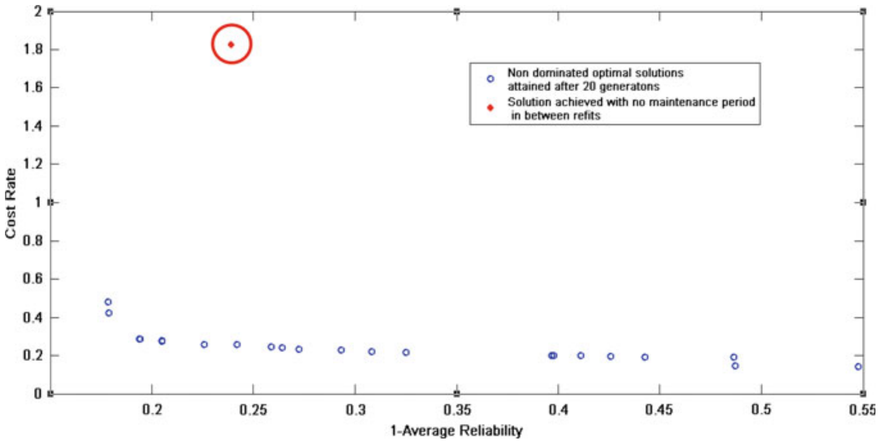


Fig. 9.8 Set of optimal solutions obtained from NSGA II program

Table 9.7 Objective values for a population of 40 after 20 generations

Solution no.	1	2	3	4	5	6	7	8	9	10
Cost rate	0.4815	0.2592	0.2861	0.2585	0.2449	0.1967	0.2426	0.4815	0.1418	0.2224
1—Avg Reliab	0.1785	0.2257	0.1943	0.2418	0.2587	0.4259	0.2643	0.1785	0.5476	0.3083
Solution no.	11	12	13	14	15	16	17	18	19	20
Cost rate	0.1927	0.4239	0.2426	0.2585	0.1967	0.2283	0.4815	0.1927	0.1418	0.1967
1—Avg Reliab	0.4426	0.1789	0.2643	0.2418	0.4259	0.2932	0.1785	0.4426	0.5476	0.4259
Solution no.	21	22	23	24	25	26	27	28	29	30
Cost rate	0.2449	0.1913	0.1967	0.1927	0.2794	0.4815	0.1927	0.2886	0.1913	0.2738
1—Avg Reliab	0.2587	0.4864	0.4259	0.4426	0.205	0.1785	0.4426	0.194	0.4864	0.2051
Solution no.	31	32	33	34	35	36	37	38	39	40
Cost rate	0.2224	0.2738	0.1458	0.1999	0.2283	0.201	0.2149	0.2338	0.1988	0.4815
1—Avg Reliab	0.3083	0.2051	0.4872	0.3977	0.2932	0.3968	0.3252	0.2723	0.4112	0.1785

Table 9.8 Forty solutions of the MOOP obtained through NSGAII

Soln no.	1	[1 1 0 1 1 1 0 1 1 1 0 0 1 2 1 101]
Soln no.	2	[1 1 0 0 0 0 1 0 0 1 0 0 1 5 1 183]
Soln no.	3	[0 1 0 1 1 1 1 1 0 1 0 0 1 5 1 209]
Soln no.	4	[0 1 1 1 1 1 1 0 0 1 0 0 1 5 2 211]
Soln no.	5	[0 1 1 1 0 1 1 0 0 1 0 0 1 5 2 209]
Soln no.	6	[0 1 0 0 0 0 0 1 0 0 1 0 1 5 13 312]
Soln no.	7	[1 1 1 1 0 1 0 0 0 1 0 0 1 5 2 209]
Soln no.	8	[1 1 0 1 1 1 0 1 1 1 0 0 1 2 1 101]
Soln no.	9	[0 0 0 0 0 0 1 0 0 0 1 0 1 5 11 312]
Soln no.	10	[0 1 1 0 0 0 1 0 0 1 0 0 1 5 2 211]
Soln no.	11	[0 0 0 0 0 0 0 1 0 0 1 0 1 5 13 312]
Soln no.	12	[1 1 0 1 0 1 0 1 1 1 0 0 1 5 1 209]
Soln no.	13	[1 1 1 1 0 1 0 0 0 1 0 0 1 5 2 209]
Soln no.	14	[0 1 1 1 1 1 1 0 0 1 0 0 1 5 2 211]
Soln no.	15	[0 1 0 0 0 0 0 1 0 0 1 0 1 5 13 312]
Soln no.	16	[0 1 1 1 0 1 0 0 0 1 0 0 1 5 2 209]
Soln no.	17	[1 1 0 1 1 1 0 1 1 1 0 0 1 2 1 101]
Soln no.	18	[0 0 0 0 0 0 0 1 0 0 1 0 1 5 13 312]
Soln no.	19	[0 0 0 0 0 0 1 0 0 0 1 0 1 5 11 312]
Soln no.	20	[0 1 0 0 0 0 0 1 0 0 1 0 1 5 13 312]
Soln no.	21	[0 1 1 1 0 1 1 0 0 1 0 0 1 5 2 209]
Soln no.	22	[0 1 0 1 1 1 0 0 0 1 0 0 1 5 9 312]
Soln no.	23	[0 1 0 0 0 0 0 1 0 0 1 0 1 5 13 312]
Soln no.	24	[0 0 0 0 0 0 0 1 0 0 1 0 1 5 13 312]
Soln no.	25	[0 1 1 1 0 1 1 1 0 1 1 0 1 5 2 218]
Soln no.	26	[1 1 0 1 1 1 0 1 1 1 0 0 1 2 1 101]
Soln no.	27	[0 0 0 0 0 0 0 1 0 0 1 0 1 5 13 312]
Soln no.	28	[1 1 0 1 0 1 1 1 0 1 0 0 1 5 1 209]
Soln no.	29	[0 1 0 1 1 1 0 0 0 1 0 0 1 5 9 312]
Soln no.	30	[1 1 1 1 0 1 0 1 0 1 0 0 1 5 2 209]
Soln no.	31	[0 1 1 0 0 0 1 0 0 1 0 0 1 5 2 211]
Soln no.	32	[1 1 1 1 0 1 0 1 0 1 0 0 1 5 2 209]
Soln no.	33	[0 0 0 0 0 0 1 0 0 0 1 0 1 5 11 275]
Soln no.	34	[0 0 0 0 0 1 0 1 0 0 1 0 1 5 13 286]
Soln no.	35	[0 1 1 1 0 1 0 0 0 1 0 0 1 5 2 209]
Soln no.	36	[0 0 0 0 0 1 0 1 0 0 1 0 1 5 13 284]
Soln no.	37	[0 1 1 0 0 1 0 0 0 1 0 0 1 5 2 209]
Soln no.	38	[0 1 1 0 1 0 1 0 0 1 0 0 1 5 2 209]
Soln no.	39	[0 1 0 0 0 1 0 1 0 0 1 0 1 5 13 312]
Soln no.	40	[1 1 0 1 1 1 0 1 1 1 0 0 1 2 1 101]

9.5 Decision Regarding Maintenance Before an Operational Mission

9.5.1 Introduction

It was brought out earlier that in a naval ship the maintainer is often faced with a dilemma of choosing the appropriate maintenance action plan for his equipment just prior to an urgent operational mission. The authorities could be kind enough to allow the ship to have a short maintenance period just before the operational mission to get the equipment ready for operation. However, the time and manpower resource available during this time have their own constraints. Under such circumstances the maintainer has two options

(a) Either to choose to carry out minor repair or replacement of the maximum number of equipment, thus inflating the maintenance budget but improving the availability of the equipment.
(b) Or the maintainer can minimize the cost of maintenance but this will come at a price in terms of low availability of the equipment.

Though there are many mathematical models available in the literature which focus on optimal maintenance decisions in terms of maintenance intervals, type of maintenance actions etc., there are none available to address this type of multi-objective maintenance decision model, which emphasizes on short term maximization of mission accomplishment probability at an appropriate maintenance cost within constraints of resources of time and manpower. Most of the models make the simplistic assumption that whenever the plant breaks down all the components are replaced. But this is only seldom true for plants which have a vast number of components and auxiliary equipment. In most of these cases the replacement may at best be limited to an auxiliary component. The rest of the auxiliary equipment may continue to exist in the plant with their relevant ages and still continue to function. Assuming these equipment to be as good as new will be completely unrealistic.

The biggest challenge for tackling the above type of problems comes from the overwhelming number of equipment and various factors to be considered before making optimal maintenance decision. For example the following will need to be considered by the maintenance manager:

(a) What are the critical equipment components and sub-components that need to be considered for maintenance action?
(b) What is the age distribution of the critical equipment or when were they last replaced? Since age of mechanical component plays an important part in determining the residual life, this is an important consideration for the maintainer.
(c) For equipment which are monitored for its condition/wear or deterioration, what is the probability that the maintenance will fall due during the upcoming operational phase of the ship? Will it be beneficial to carry out the maintenance action on these equipment before the operational phase itself?

(d) Which equipment have got redundancies? Will it be beneficial if these equipment maintenance be undertaken during the operational phase? Is it beneficial to undertake component level repair or replace the whole equipment itself or should one opt for opportunistic maintenance?

(e) Some minor maintenance actions can be undertaken by the ship crew, but there are some that must be undertaken only in harbor by experts. The maintenance on these equipment will certainly cost high in terms of interruption in the operations.

The problem gets compounded if the logistics to support the maintenance actions need to be considered. For the present case, since the maintenance period before the operational phase has been scheduled impromptu, we assume that all the logistics support is available so as to support the maintenance related decision taken by the maintenance manager.

9.5.2 The Model

Let a main propulsion plant be comprised of ‘n’ components with known ages. Let there be redundancies available for some equipment. The problem at hand is to choose between two actions, to replace or to leave it as it is. The objectives are minimization of maintenance costs and minimization of downtime. Both the objectives are conflicting and therefore the solutions should be available on a pareto-optimal front of the plot for the objectives.

We proceed by first discretizing the time and evaluating the expected cost and downtime in each discrete time zone. Later we make use of a NSGA II based algorithm to arrive at the optimal solutions for the given example of a single main propulsion plant system. The MOOP can be written down as follows:

$$\begin{aligned}&\text{OBJECTIVES}\\&\min\nolimits_{M[]}[\text{Expected Cost }(Th)]\\&\min\nolimits_{M[]}[\text{Expected Downtime (Th)}]\\&\text{s.t.}\end{aligned} \tag{9.11}$$

$$\sum_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{MC_i} + \{\text{Expected cost(Th)}] \leq \text{Budgeted cost}$$

$$\sum_{i}^{n} MP_i \cdot MT_i \leq \text{maintenance period X total maintenance manpower available}$$

$$\text{Prob(ODL(Th)} < \text{wear threshold level)} < \text{Given probability values}$$

$$1 - \left[\sum_{i=1}^{n} \int_{0}^{\infty} \frac{f_i(Th)}{1 - F_i(age_i)} \cdot \prod \frac{R_j(Th)\cdot dt}{1 - F_j(age_j)} \left[1 - \prod \frac{R_{ik}(Th)\cdot dt}{1 - F_{ik}(age_k)}\right]\right]_{i \neq j} > Given \tag{9.12}$$

Where

M[] are a set of actions for various equipment and components of the plant ‘Th’ is the time horizon the plant is to be in operational state immediately after the maintenance

MP_i is the manpower required for maintenance of component ‘i’

MT_i is the time required for maintenance of component ‘i’

MC_i is the cost involved for maintenance of component ‘i’

ODL(Th) is the overall deterioration on level of the components of the plant being monitored

age_i is the age of component ‘i’

$f_i(.)$ is the pdf of lifetime for component ‘i’

$F_i(.)$ is the cdf of lifetime for component ‘i’

$R_i(.)$ is the reliability of component ‘i’

$R_{ij}(.)$ and $F_{ij}(.)$ is the reliability and cdf of component ‘j’ which is redundant for component ‘i’

We take the case of a main propulsion plant which comprises many maintainable components identified through qualitative or quantitative methods like “reliability centered maintenance” or FMECA. A look at the components and subcomponents of such a plant is placed at Fig. 9.9. The critical inputs regarding age, cost, manpower and time required for maintenance etc. is given in Table 9.9. The sea water pump has a redundancy and all the components selected for maintenance are assumed to have been selected as per the chosen maintenance policy. The maintenance manager has got only limited time in his hand and if he has to maximize the availability of the ship at minimum cost, he has to choose the equipment which he needs to maintain, very wisely. The problem becomes compounded since the assumption that the equipment can fail only once within the time horizon under consideration has been dropped and now the ages (or times) the equipment are under service also need to be considered.

The mathematical model for the MOOP is given in Eqs. 9.11 and 9.12. The expected cost and downtime equations are shown in Eqs. 9.22 and 9.23.

9.5.3 Assumptions

The following assumptions are made with respect to the sample main propulsion plant:

- The failures of all components are statistically independent
- The components which are being monitored for condition/deterioration follow a gamma deterioration process and all the other components follow a Weibull process for failure. All the parameters of the assumed processes are known.

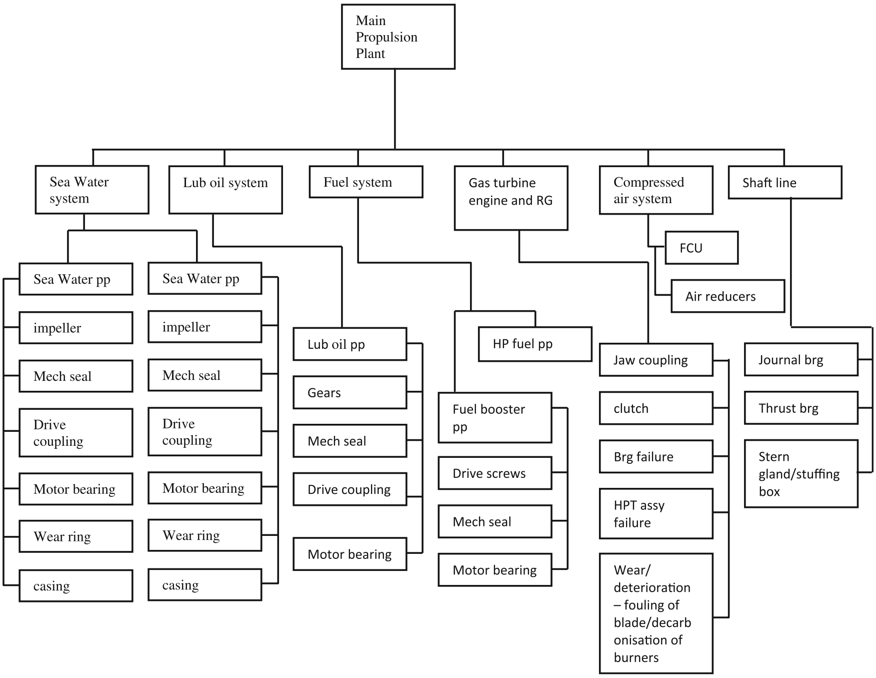


Fig. 9.9 Select maintainable components of a sample main propulsion plant

- The maintenance actions available is only replacement or no replacement except for fouling of GT blades or de-carbonisation of the burners which are chemically cleaned and fitted back.
- The repair times considered for components are deterministic for convenience of planning. Maintenance actions requiring work in harbor incur higher repair times and cost
- Though the time is assumed to be continuous, we make it discrete for ease of calculations. We therefore assume that no two failures occur at the same time. We assume no constraints for the given main propulsion plant problem with 29 components.

We also assume that the components which follow gamma wear process have the same scale parameter. The combined wear of such processes is also a gamma wear process with same scale parameter but the shape parameter is the sum of the individual parameters. The proof is shown in Eqs. (9.13)–(9.21) below. The probability of the combined wear exceeding the wear threshold can then be ascertained according to Eq. (9.21). For processes which have different scale parameters, the method to form a convolution is shown in Verma et al. [5].

Let x_1 and x_2 be two gamma random variables such that $y = x_1 + x_2; 0 \leq x_1 \leq \infty$ and $0 \leq x_2 \leq \infty$ and let the shape parameters of their gamma distribution be α_1 and

Table 9.9 Data on maintainable components of main propulsion plant

Sn	Component	Scale parameter	Shape parameter	Cost	Time	Manpower	Age at time t = 0	Repairs on ship or at harbor
1	Sea water pump–impeller	465	1.3	12000	2	3	100	Ship
2	Mechanical seal	380	0.95	1000	2	3	20	Ship
3	Coupling wear	600	2.2	450	1	3	100	Ship
4	Motor bearing	310	1.1	900	2.5	2	100	Ship
5	Wear ring	220	2	5000	2.5	4	100	Ship
6	Casing	500	1.5	19000	3	4	100	Harbor
7	Sea water pump (**redundant unit**)–impeller	465	1.3	12000	2	3	40	Ship
8	Mechanical seal	380	0.95	1000	2	3	40	Ship
9	Coupling wear	600	2.2	450	1	3	0	Ship
10	Motor bearing	310	1.1	900	2.5	2	40	Ship
11	Wear ring	220	2	5000	2.5	4	40	Ship
12	Casing	500	1.5	19000	3	4	40	Harbor
13	MD lub oil pump-gears	831	3.5	5500	2	3	250	Harbor
14	Flexible coupling	515	1.6	650	1	3	250	Harbor
15	Motor bearing	720	3.11	1100	2.5	3	250	Harbor
16	Fuel pump mech seal	682	3.5	1200	1	3	0	Harbor
17	Motor bearing	720	3.11	1100	2.5	3	335	Harbor
18	Rotor	815	1.9	12000	2.5	3	335	Harbor
19	Hp fuel pump	466	3	1,80,000	1	2	411	Ship
20	Jaw coupling of RG	330	1.4	80,000	3	5	540	Harbor
21	Air reducer	150	0.8	43,500	1	2	50	Ship
22	AFCU (automatic fuel control unit)	717	2.62	400,000	1	2	540	Ship
23	Clutch assembly	841	2.5	2500,000	10	8	720	Harbor

(continued)

Table 9.9 (continued)

Sn	Component	Scale parameter	Shape parameter	Cost	Time	Manpower	Age at time t = 0	Repairs on ship or at harbor
24	Bearing assembly	1020	0.8	1400,000	25	12	720	Harbor
25	HPT assembly	1500	0.8	900,000	25	12	720	Harbor
26	Wear/deterioration, fouling of blades, decarbonisation of burners etc.	0.82	0.095 × t	–	0.5	3	43	Ship
27	Shaftline—journal bearing	907	2.9	6,10,000	3	6	370	Harbor
28	Stern gland	650	0.96	2,20,000	12	8	370	Harbor
29	Stern tube bearing	1510	0.9	2200,000	12	8	370	Harbor

α_2 respectively and scale parameters be both equal to β. We have $x_2 = y - x_1$ as x_2 ranges from 0 to ∞; y ranges from x_1 to ∞ let a conditional distribution be

$$\Phi(\mathrm{y/x_1}) = f(x_2) \cdot \frac{\partial x_2}{\partial y} \tag{9.13}$$

where $f(x_2)$ is the gamma pdf for x_2 and it can be written as

$$= f(y - x_1) \cdot 1 = \frac{\beta^{\alpha_2}}{\Gamma(\alpha_2)} \cdot (y - x_1)^{\alpha_2 - 1} \cdot e^{-(y - x_1)\cdot\beta} \tag{9.14}$$

Hence joint density function, say g(x,y) will be =

$$\begin{aligned} &\Phi(\mathrm{y/x_1}) \cdot \mathrm{f}(\mathrm{x_1}) \\ &= \frac{\beta^{\alpha_2}}{\Gamma(\alpha_2)} \cdot (y - x_1)^{\alpha_2 - 1} \cdot e^{-(y - x_1)\cdot\beta} \cdot \frac{\beta^{\alpha_1}}{\Gamma(\alpha_1)} \cdot (x_1)^{\alpha_1 - 1} \cdot e^{-(x_1)\cdot\beta}; \\ &0 \le \mathrm{x_1} \le \infty \,\mathrm{and}\, \mathrm{x_1} \le \mathrm{y} < \infty \end{aligned} \tag{9.15}$$

Integrating wrt x_1, we can get the pdf for y. Changing limits of 'y' from 0 to ∞, we have x_1 ranging from 0 to y

$$\mathrm{f(y)} = \int_0^y \frac{\beta^{\alpha_2}}{\Gamma(\alpha_2)} \cdot (y - x_1)^{\alpha_2 - 1} \cdot e^{-(y - x_1).\beta} \cdot \frac{\beta^{\alpha_1}}{\Gamma(\alpha_1)} \cdot (x_1)^{\alpha_1 - 1} \cdot e^{-(x_1).\beta} \cdot dx_1 \tag{9.16}$$

$$= \frac{\beta^{(\alpha_1 + \alpha_2)}}{\Gamma(\alpha_1) \cdot \Gamma(\alpha_2)} .e^{-y\beta} \int_0^y x_1^{\alpha_1 - 1} (y - x_1)^{\alpha_2 - 1} \cdot dx_1 \tag{9.17}$$

Putting $x_1 = t \cdot y$ and changing the limit we can change the above equation to

$$\frac{\beta^{(\alpha_1 + \alpha_2)}}{\Gamma(\alpha_1) \cdot \Gamma(\alpha_2)} \cdot e^{-y\beta} \int_0^1 (t \cdot y)^{\alpha_1 - 1} (y - yt)^{\alpha_2 - 1} \cdot y \cdot dt \tag{9.18}$$

$$= \frac{\beta^{(\alpha_1 + \alpha_2)}}{\Gamma(\alpha_1) \cdot \Gamma(\alpha_2)} \cdot e^{-y\beta} \cdot y^{(\alpha_1 + \alpha_2 - 1)} \int_0^1 t^{\alpha_1 - 1} .(1 - t)^{\alpha_2 - 1} \cdot dt \tag{9.19}$$

but we have $\int_0^1 t^{\alpha_1 - 1} \cdot (1 - t)^{\alpha_2 - 1} \cdot dt = $ beta function $= \frac{\Gamma(\alpha_1) \cdot \Gamma(\alpha_2)}{\Gamma(\alpha_1 + \alpha_2)}$

Therefore Eq. (9.19) can be written as

$$f(y) = \frac{\beta^{(\alpha_1+\alpha_2)}}{\Gamma(\alpha_1+\alpha_2)} \cdot e^{-y\beta} \cdot y^{(\alpha_1+\alpha_2-1)} \tag{9.20}$$

Which is the same as the gamma function with scale parameter = β and shape = $\alpha_1 + \alpha_2$

$$\mathrm{F}(x) = \int\limits_0^{(W_{Th}-W_0)} \frac{\beta^{(\alpha_1+\alpha_2)\cdot t}}{\Gamma((\alpha_1+\alpha_2)t)} x^{(\alpha_1+\alpha_2)t-1} \cdot e^{-\beta x} \cdot dx \tag{9.21}$$

where,

F(x) is the cdf of the combined wear
$\mathrm{W_{Th}}$ is the combined wear threshold at the end of operational phase ‘Th’ and
$\mathrm{W_0}$ is the wear at the end of the maintenance phase

Consider the Fig. 9.10. To obtain the correct values of expected cost and downtime we break the time line into small discrete steps and recursively calculate the cost and downtime for every discrete step. A form of this method was shown by Perakis [8], however, there is a difference in the way the expected cost and downtime has been calculated in this work. The equation for estimation of cost and downtime can be represented as shown in Eqs. (9.22) and (9.23).

$$\begin{aligned} &\mathrm{E(Cost(Th))} \\ &= \sum_{\mathrm{i=1;}}^{\mathrm{n}} \int\limits_0^{\mathrm{Th}} \frac{\mathrm{f_i}(age_i+x)}{R_i(age_i)} \prod_{j\neq i}^{n} \frac{R_j(age_j+x)}{R_j(age_j)} \cdot \left(\prod\left(1-\frac{R_{ik}(age_k+x)}{R_{ik}(age_k)}\right)\right) \\ &\quad \times (Cost_{initl} + MC_i + Cost_R \cdot MP_i \cdot (T_{Ri}+\gamma_i)) + \ \mathrm{E(Cost(}Th - x - (T_{Ri}+\gamma_i))) \cdot dx \end{aligned} \tag{9.22}$$

And similarly for downtime we have

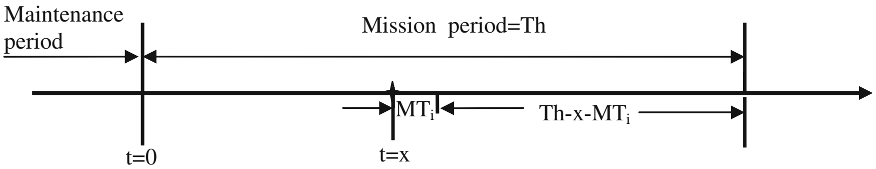


Fig. 9.10 Timeline for the mission period

$$\mathrm{E(DT(Th))} = \sum_{\mathrm{i=1}}^{\mathrm{n}} \int_{0}^{\mathrm{Th}} \frac{\mathrm{f_i}(age_i + x)}{R_i(age_i)} \prod_{j\neq i}^{n} \frac{R_j(age_j + x)}{R_j(age_j)} \cdot \left(\prod \left(1 - \frac{R_{ik}(age_k + x)}{R_{ik}(age_k)}\right)\right) \times (T_{Ri} + \gamma_i) + \mathrm{E(DT}(Th - x - (T_{Ri} + \gamma_i))) \cdot dx \tag{9.23}$$

Where

$\mathrm{T_{Ri}}$ time required for replacement of component ‘i’

$\mathrm{Cost_R}$ cost of repair action per time per repair crew

$\mathrm{Cost_{initl}}$ initial cost incurred during maintenance phase $\sum_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{M} \cdot (MC_i + Cost_R \cdot MP_i \cdot (T_{Ri})$

E(Cost(Th)) expected cost at time horizon ‘Th’

E(DT(Th)) expected down time

M[] is a vector of 0 and 1 s depicting action or no action on various components of the plant

‘Th’ is the time horizon the plant is to be in an operational state immediately after the maintenance

$\mathrm{MP_i}$ is the manpower required for maintenance of component ‘i’

$\mathrm{MC_i}$ is the fixed cost of component ‘i’

ODL(Th) is the overall deterioration level of components being monitored

$\mathrm{age_i}$ is the age of component ‘i’

$\mathrm{f_i(.)}$ is the pdf of lifetime for component ‘i’

$\mathrm{F_i(.)}$ is the cdf of lifetime for component ‘i’

$\mathrm{R_i(.)}$ is the reliability of component ‘i’

$\mathrm{R_{ij}(.)}$ and $\mathrm{F_{ij}(.)}$ is the reliability and cdf of component ‘j’ which is redundant for component ‘i’

The high number of components; 29 in the above case and the requirement of working on the problem through a recursive method makes the solution time intensive. Further, the multi-objective nature of the problem requires multiple evaluations of the expected cost and downtime to investigate the search space for optimal solutions. Taking the time horizon to be of 45 days, we begin with a random selection of 30 maintenance actions for components. The Matlab codes for the NSGA II have been generated using MATLAB 7.0. To speed up the evaluation process, the GA maintains a record of old solutions and for children with similar chromosomes as that of the parents the objective fitness are directly copied instead of evaluating them all over again.

9.5.4 Result

The elite 30 solutions obtained after 25 generations have been listed in the Table 9.10. The solution is given in the matrix form where, each element represents whether that particular component has to be replaced or not. The 14 solutions can be seen to form Pareto optimal front in Fig. 9.11 Based on the availability requirements and the budget considerations, the maintenance manager can choose from the 14 elite solutions, one that suits him the best. Further, we have not considered, opportunistic maintenance in the problem above. However, since the fixed cost of the components far outweigh the variable maintenance cost, it does not affect the solution much, except for bringing down the collective maintenance time prior to the operational phase. The maintenance manager can therefore make a note of that fact and choose his maintenance actions accordingly.

Table 9.10 Matrix of solutions for the main propulsion plant problem

Sl no.	Various solutions
1	[1 1 0 1 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 0 1 1 0 0 0 1 0 0];
2	[1 1 0 1 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 0 1 1 0 0 0 1 0 0];
3	[0 0 1 0 1 0 0 0 0 0 0 0 0 1 1 0 0 1 0 1 0 0 0 0 0 0 0 0 0];
4	[0 0 1 0 1 0 0 0 0 0 0 0 0 1 1 0 0 1 0 1 0 0 0 0 0 0 0 0 0];
5	[0 1 0 0 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 0 0 0 0 0 0 0 0];
6	[1 0 1 0 1 1 0 0 1 1 1 1 1 1 1 0 1 1 0 1 0 0 0 0 0 0 0 0 0];
7	[0 0 1 0 1 0 0 0 1 0 0 0 1 1 1 0 1 1 1 1 0 0 0 0 0 0 1 0 0];
8	[1 0 0 0 1 1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 0 1 0 0 0 0 1 0 0];
9	[0 1 0 0 1 1 0 0 1 1 1 1 1 1 1 0 1 1 1 1 0 0 0 0 0 0 0 0 0];
10	[1 1 0 1 1 1 0 0 0 0 0 1 0 1 1 1 1 1 0 1 0 0 1 0 0 0 1 0 0];
11	[0 0 0 0 0 1 0 0 0 0 0 1 0 1 1 0 1 1 1 1 0 0 1 0 0 0 0 0 0];
12	[0 0 1 0 1 0 0 0 1 0 0 0 1 1 1 0 1 1 1 1 0 0 0 0 0 0 1 0 0];
13	[1 0 1 0 1 1 0 0 1 1 1 1 1 1 1 0 1 1 0 1 0 0 0 0 0 0 0 0 0];
14	[1 1 0 1 1 1 0 0 1 0 0 1 1 1 1 0 1 1 1 1 0 0 1 0 0 0 1 0 0];
15	[1 0 0 0 1 1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 0 1 0 0 0 0 1 0 0];
16	[1 0 1 1 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 1 0 0 0 0 0 0];
17	[0 0 1 0 1 0 0 0 0 0 1 0 1 1 1 1 1 1 0 1 0 0 1 0 0 0 0 0 0];
18	[1 0 1 1 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 1 0 0 0 0 0 0];
19	[1 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 0 1 0 0 0 0 0 0 0 0];
20	[0 0 1 0 1 0 0 0 0 0 1 0 1 1 1 1 1 1 0 1 0 0 1 0 0 0 0 0 0];
21	[0 0 1 0 1 0 0 0 0 0 0 0 1 1 1 0 0 1 0 1 0 0 0 0 0 0 0 0 0];
22	[0 1 0 0 1 1 0 0 1 1 1 1 1 1 1 0 1 1 1 1 0 0 0 0 0 0 0 0 0];
23	[1 0 1 1 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 1 0 0 0 0 0 0];
24	[1 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 0 1 0 0 0 0 0 0 0 0 0];
25	[1 0 1 0 1 1 0 0 1 1 1 1 1 1 1 0 1 1 0 1 0 0 0 0 0 0 0 0 0];
26	[1 1 0 1 1 1 0 0 1 0 0 1 1 1 1 0 1 1 1 1 0 0 1 0 0 0 1 0 0];
27	[1 1 0 1 1 1 0 0 1 0 0 1 1 1 1 0 1 1 1 1 0 0 1 0 0 0 1 0 0];
28	[1 1 0 1 1 1 0 0 1 0 0 1 1 1 1 0 1 1 1 1 0 0 1 0 0 0 1 0 0];
29	[1 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 0 1 0 0 0 0 0 0 0 0 0];
30	[1 1 0 1 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 0 1 1 0 0 0 1 0 0];

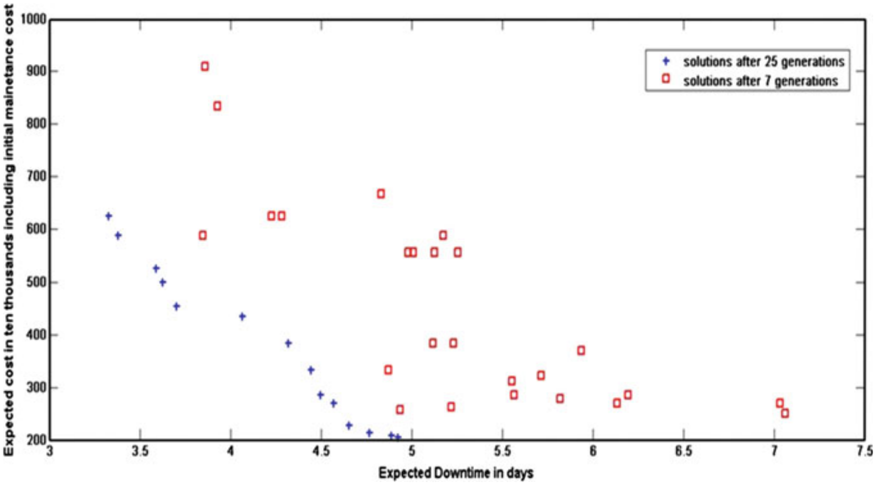


Fig. 9.11 A plot of solutions for the sample problem after 7 and 25 generations

9.6 Summary

The present chapter touched upon two different aspects of maintenance faced by maintenance manager of a large setup of machinery. The first was regarding prioritizing of machinery/equipment in terms of failure severity and criticality and the second regarding taking a group decision on maintenance actions keeping in mind objectives such as cost rate, average reliability, availability etc.

The prioritization of machinery was demonstrated using a FMECA method wherein equipment that are critical for functioning of the relevant system are identified and evaluated further for the kind of maintenance action it may need. It has been brought out earlier that the maintenance planning for machinery of a large set up like that of a ship is a complex activity. Since there a large number of plants with large number of systems and equipment, it is imperative that to arrive at an optimum decision on maintenance at the ship level, maintenance at every hierarchical level of her machinery be optimized. This means that the maintenance personnel need to decide not only at the plant level but also at equipment level whether a particular equipment needs to be covered under CBPM or TBPM, whether the replacement or repair need to be done on equipment level or component level etc. The methodology was briefly mentioned in Sect. 9.2. The present chapter however, focussed mainly on making group maintenance decision at the ship (or industry) level machinery, depicted in step 6 of Fig. 9.1.

The present chapter has also demonstrated the method of organizing the equipment into groups so that these groups of equipment can be specifically maintained during short maintenance periods called (MPs) scheduled in between the refits of the ships. The number of such MPs, the select list of equipment to be maintained during these MPs, the time interval for scheduling these MPs and the time interval for scheduling the refit (major maintenance) period of the ship were the variables that were used for solving the multi-objective optimization problem using the genetic algorithm based NSGAII program. The second maintenance problem discussed was that of choosing the optimal set of equipment for maintenance actions given the constraints of time and maintenance resources.

References

1. Horenbeek VA, Pintelon L, Muchiri P (2010) Maintenance optimization models and criteria. In: Proceedings of the 1st international congress on e-Maintenance. Lulea Sweden, pp 5–13, 22–24
2. Dekker R (1996) Applications of maintenance optimization models: a review and analysis. Reliab Eng Syst Safety 51(3):229–240
3. Dekker R (1995) On the use of operations research models for maintenance decision making. Microelectron Reliab 35(9–10):1321–1331
4. Scarf PA On the application of mathematical models in maintenance. Eur J Oper Res 99:493–506
5. Verma AK, Srividya A, Rana A (2011) Optimal time scheduling for carrying out minor maintenance on a steam turbine. Int J Syst Assur Eng Manag 1–12, Nov 09, 2011
6. Department of the Army, TM 5–698-4, Failure Modes, Effects and Criticality Analyses (FMECA for Command Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4SIR) Facilities, 29 Sep 2006
7. Deb K (2002) Multi-Objective optimization using evolutionary algorithms. Wiley
8. Perakis AN, Inozu B (1991) Optimal maintenance repair and replacement of Great Lakes marine diesel. Eur J Oper Res 55:165–182

Chapter 10
Probabilistic Safety Assessment

10.1 Introduction

Probabilistic Safety Assessment (PSA), also called Probabilistic Risk Assessment (PRA), is currently being widely applied to many fields, viz, chemical and process plants, nuclear facilities, aerospace and even to financial management. PSA 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. PSA provides the quantitative estimate of risk, which is useful for comparison of alternatives in different design and engineering areas. The main benefit of PSA is to provide insights for the identification of dominant risk contributors and the comparison of options in reducing risk. In addition, it provides inputs to decisions on design and back fitting, plant operation and maintenance, and on regulatory issues.

In spite of the benefits, it is well recognized that PSA has its own limitations. The accuracy of the PSA depends on the uncertainties in aspects like models and data on dependency (e.g. Common Cause Failures (CCFs)) and Human Reliability. The benefits that accrue from PSA overweigh its limitations. So worldwide, utilities are performing the PSA of their plants and many regulatory bodies are using it as a risk informed approach in decision making. Over the years, the PSA methodology has matured and even new applications like living PSA/Risk Monitor, technical specification optimization, reliability centered maintenance (RCM) and risk based in-service inspection have emerged.

10.2 Concept of Risk and Safety

The word risk is generally defined as "the chance of injury or loss resulting from exposure to a source of danger", while safety means "freedom from danger or hazard". A problem is that in a technological society, no activity has zero risk.

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_10

Thus, there can not be absolute safety and the two terms are related to one another, with low risk meaning the same as high level of safety. However, psychologically, we tend to be more comfortable with the term safety than with term ‘risk’, whether we are discussing nuclear reactors, air planes, chemicals or automobiles.

Risk is related to “chance” and loss. The qualitative definition can loss be converted into qualitative by putting risk on a mathematical foundation. Let the “chance” be probability and “loss” be consequences and “of” be multiplication. This is to define risk as probability times consequences, thus risk combines both probability and consequences.

$$\text{Risk} = \text{Probability} \times \text{Consequences} \tag{10.1}$$

Producing probability distributions for the consequences affects a much more detailed description of risk.

The notion of risk can be further refined by defining it as a set of triplets; as explained by Kalpan and Garrick [1], it is set of scenarios S_i, each of which has a probability p_i and a consequence x_i. If the scenarios are ordered in terms of increasing severity of the consequences then a risk curve can be plotted, for example as shown in Fig. 10.1.

$$\text{Risk} = \langle S_i,\ p_i,\ x_i \rangle; \quad \text{where } i = 1, 2, 3, \ldots, n. \tag{10.2}$$

The risk curve represents the probability that the consequences of the accident will be greater than some value of x. Mathematically, the exceedance probability is integral from x to ∞, the curves is known as complimentary cumulative distribution function.

Further, instead of probability of the event, frequency with which such event might take place can also be used.

Example 1 In a chemical plant, the following event probabilities and consequences are known (as shown in Table 10.1). Assuming the accidents are independent, construct the risk curve and determine the risk of each accident.

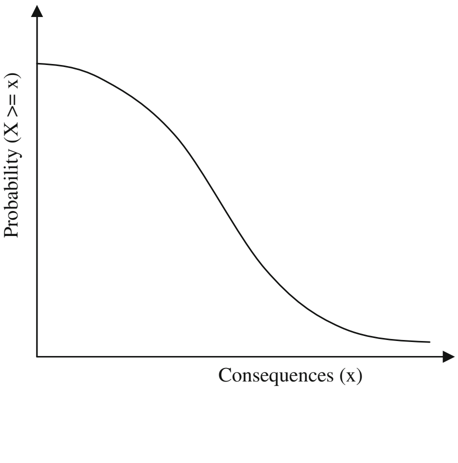


Fig. 10.1 Risk curve

Table 10.1 Probabilities and consequences

Event	Consequence xi	Probability
Accident A	1000$	4×10^{-2}
Accident B	500$	2×10^{-2}
Accident C	100$	1×10^{-2}
Accident D	1500$	8×10^{-2}
Accident E	10000$	5×10^{-4}
Accident F	5000$	5×10^{-3}
Accident G	2500$	1×10^{-3}
Accident H	750$	3×10^{-2}
Accident I	8000$	3×10^{-4}
Accident J	7000$	1×10^{-4}

Table 10.2 Calculations for risk curve

X	100	500	750	1000	1500
P(X > x)	0.1869	0.1769	0.1569	0.1269	0.0869
X	2500	5000	7000	8000	10,000
P(X > x)	0.0069	0.0059	0.0009	0.0008	0.0005

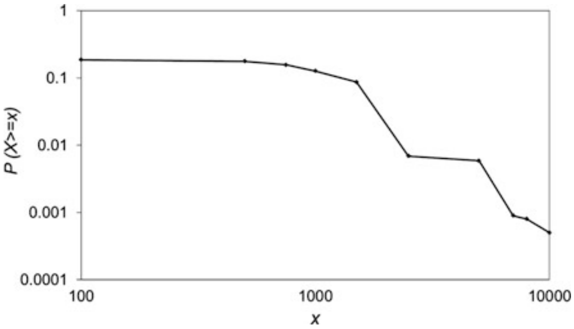


Fig. 10.2 Risk curve for a chemical plant

Solution:
The constructed risk curve is shown in Fig. 10.2 (Calculations in Table 10.2); high consequence events have low probability. Risk for each accident is the product of its probability and consequence as shown in Table 10.3. By providing safe grounds against accident D, A and F, risk can be reduced significantly.

Table 10.3 Risk of each event

Event	Risk	Event	Risk
Accident A	40	Accident F	25
Accident B	10	Accident G	2.5
Accident C	1	Accident H	22.5
Accident D	120	Accident I	2.4
Accident E	5	Accident J	0.7

10.3 An Overview of Probabilistic Safety Assessment Tasks

In the Risk Analysis, we primarily address these questions: what is the hazard? How likely is it? What are the consequences? How to improve the level of safety? A simple risk model for a fire accident scenario is shown in Fig. 10.3. Anticipating a fire accident, let us say there are safety equipment A (fire extinguisher in the room) and B (fire extinguisher of the facility/town). Both of them function, it is happy ending. If equipment B fails given A successful, seq 2 may not be a happy ending. Seq 3 represents the failure of A and success of B, it could be unhappy ending. Seq 4 represents the failure of both A and B, it could be disastrous situation. Having identified all the sequences, evaluation of risk corresponds to calculation of the likelihood of sequences and their associated consequences. A systematic and comprehensive methodology probabilistic safety assessment (PSA) is used to evaluate the risk associated with complex engineering systems like NPPs. All the sequences and their outcomes are identified, then evaluation of risk corresponds to calculation of the likelihood of sequences and their associated consequences.

The procedure presented here is general and is derived based on the insights from [2–8] as shown in Fig. 10.4.

PSA begins with the definition of objectives and scope of the analysis which are necessary for the organization and management of the study. This is also useful to

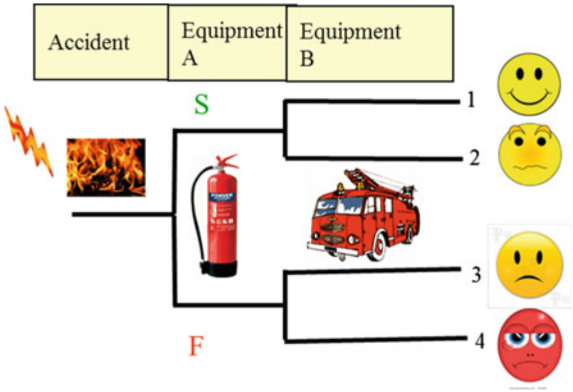


Fig. 10.3 Model for fire accident scenario

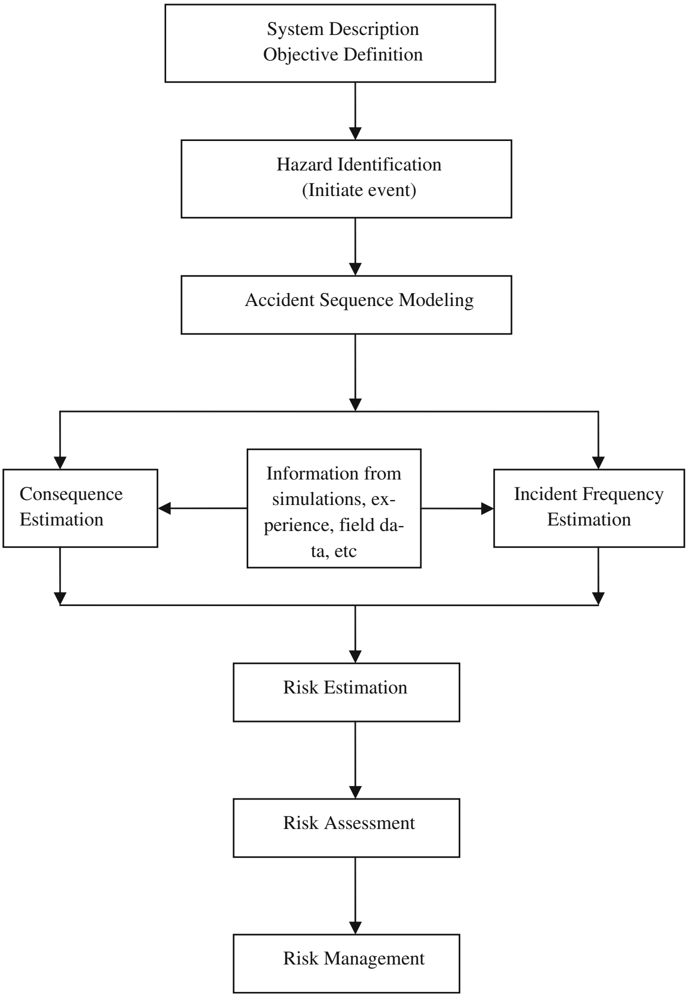


Fig. 10.4 PSA procedure

inform the specification of consequence categories (for accident sequence development) and frequency cut off that serve to bound the analysis.

Through understanding of the system is the prerequisite for doing PSA. System awareness through system/plant visits and discussions with designers, operating and maintenance engineers enhance the understanding. The information for system familiarization and for further analysis is obtained from design reports, toxic inventory, technical specification reports (for test, maintenance and operating description), history cards and safety related unusual occurrence reports.

A list should be made of all the sources of hazard (toxic or radio activity, or fire etc.) from which accident can progress. Several approaches are available for identifying the hazards or accident initiation. These include Preliminary Hazard Analysis, HAZOP, Master Logic Diagrams and the FMEA. The potential states of the plant to be analyzed are determined, and the safety functions incorporated in the plant are identified.

After identifying initiating events, the next step is development of model to simulate the initiation of an accident and the response of the plant/system. The relationships between initiating events, safety functions and systems are established and categorized. A typical accident sequence consists of initiating event, specific system failure/success, human errors and associated consequences. Accident sequence modeling can be divided into

1. Event sequence modeling,
2. System modeling and
3. Consequence analysis.

An event sequence model provides sequence of events, following an initiating event, leading to different consequences. There are several methods available for event sequence modeling viz.,

1. Event sequence diagram
2. Event trees and
3. Cause consequence diagrams.

Once the response of the plant to the initiating events has been modeled by one of the available event sequence modeling techniques, system modeling is used to quantify system failure probabilities and subsequently accident sequence frequencies. There are several methods available for system modeling, viz.,

1. Fault trees,
2. State space diagrams,
3. RBD and
4. Go charts.

Consequence analysis determines the expected severity of each sequence obtained from event sequence model. It is specific to the system and the units could be number of fatalities or radio activity dose or damage in terms of dollar. Risk estimation combines the consequences and frequencies (or likelihood) of all accident sequences to provide a measure of risk.

After obtaining quantitative measure from risk estimation, risk evaluation is carried out taking into account judgments about significance of hazardous events and risk levels. It also requires the introduction of acceptance standards. Risk assessment covers risk estimation and evaluation.

The risk assessment also identifies major contributions to the overall risk. This is main input to risk management where decisions are to be made regarding efforts to reduce the risk. Uncertainty analysis is an essential step in PSA, which is due inevitable uncertainties in model parameters and models themselves. Uncertainties are propagated to quantify upper bound and lower bound of the estimated risk. Finally, risk management focus on the development of implementation strategy, examination of policy options environmental monitoring and operations auditing. Thus, risk management includes risk estimation, evaluation and decision making.

Interested readers can refer to [9–12] in addition to [2–8] for further details on PSA and specific applications including the chemical and nuclear industries.

10.4 Identification of Hazards and Initiating Events

10.4.1 Preliminary Hazard Analysis

Preliminary hazard analysis (PHA) identifies major hazards of the system, their causes and severity of the consequences. PHA is usually used during the preliminary design stage. Guide list containing components, which are potentially hazardous (for example: toxic materials, fuels, pressure containers, heating devices and radio active materials), is very useful information for beginning PHA. Understanding the physics of these components and their interaction with neighboring equipment is useful in identifying hazardous situations. Typical format of PHA is shown in the Table 10.4. Through understanding of the system along with the operating experience of the specific system aids in completing the PHA tables. A typical PHA table for nuclear power plant is shown in Table 10.4. The information from PHA is very elementary and it does not identify specific components in the systems which have potential to create hazardous scenarios. FMEA and HAZOP are most widely used in chemical and process plants for hazard identification.

10.4.2 Master Logic Diagram (MLD)

MLD is a hierarchical, top-down display of IEs, showing general types of undesired events at the top, proceeding to increasingly detailed event descriptions at lower tiers, and displaying initiating events at the bottom. The goal is not only to support identification of a comprehensive set of IEs, but also to group them according to the

Table 10.4 PHA format, for a nuclear power plant

Hazardous element	Event causing hazardous situation	Hazardous situation	Event leading to potential accident	Potential accident	Effects	Preventive measures
Reactor core	Rupture of header due to corrosion	Reactor shutdown system failure	Safety system ECCS is unavailable	Release of radioactive material	Radiation dose to operator	Proper water chemistry to prevent corrosion

challenges that they pose (the responses that are required as a result of their occurrences). IEs that are completely equivalent in the challenges that they pose, including their effects on subsequent pivotal events, are equivalent in the risk model.

A useful starting point for identification of IEs is a specification of "normal" operation in terms of (a) the nominal values of a suitably chosen set of physical variables and (b) the envelope in this variable space outside of which an IE would be deemed to have occurred. A comprehensive set of process deviations can thereby be identified, and causes for each of these can then be addressed in a systematic way.

10.5 Event Tree Analysis

Event tree analysis is an inductive method which shows all possible outcomes resulting from an initiating event. Initiating event can be sub system failure or external event (like flood, fire, Earthquake) or operator error. Event tree models the sequences containing relationships among initiating event and subsequent responses along with the end states. The subsequence responses events (branches of event tree) are safety systems or also known as pivotal events. Various accident sequences are identified and probability of occurrence of each sequence is further quantified.

In order to determine the accident sequence outcomes (e.g. reactor core damage or not in a nuclear power plant) and success requirements for safety systems (e.g. number of pumps, available time for operator response), plant simulations are performed. For example, thermal-hydraulic codes in nuclear industry and process dynamics codes in chemical industry simulate the physical process and their dynamics in the accident scenario. These computationally intensive simulations should be performed to derive insights for constructing accident sequence models.

Although it is theoretically possible to develop risk models using only event trees or only fault trees, it would be very difficult in case of complex real systems. Hence a combination of event trees and fault trees are used to develop the risk models. Event tree models the accident sequences where as fault tree models individual system responses. However, if applicable probabilistic data are available for safety systems or pivotal events then fault tree modeling is not required.

Procedure for Event Tree Analysis
The following steps are used for carrying out event tree analysis (see Fig. 10.5). An exhaustive list of accident initiating events is identified from which accident sequences could be postulated during different operational states of overall system/plant/entity. There are several approaches available for preparation of list of initiating events such as operational history of the system, reference of previous list of similar systems, master logic diagrams and PHA/HAZOP. The initiating events include both internal events such as equipment failure or human error, or software failure and external events such as fires, floods and earthquakes.

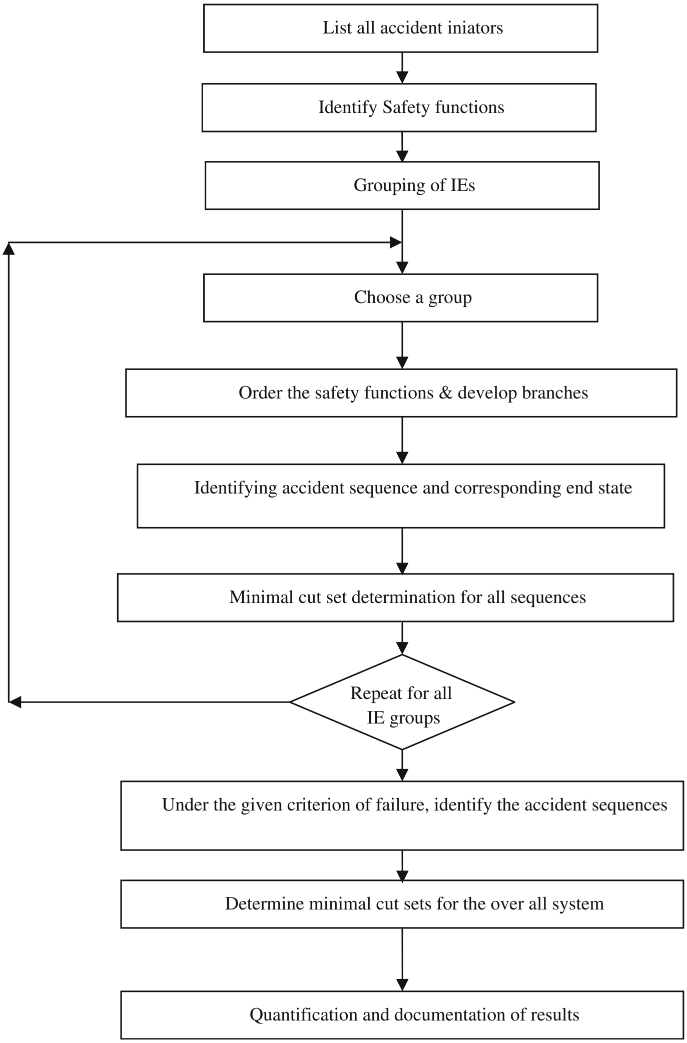

List all accident iniators
Identify Safety functions
Grouping of IEs
Choose a group
Order the safety functions & develop branches
Identifying accident sequence and corresponding end state
Minimal cut set determination for all sequences
Repeat for all IE groups
Under the given criterion of failure, identify the accident sequences
Determine minimal cut sets for the over all system
Quantification and documentation of results

Fig. 10.5 Procedure for carrying out event tree analysis

Once the exhaustive list of IEs is prepared, detailed analysis of each IE listed should be carried out to assess the causes and consequences. As the analysis of larger list results in wastage of resources, grouping of IEs is done which may have the same consequences. This can be done if the demands these IEs place on safety functions, front line systems, and support systems are the same. Hence, the safety functions that need to be performed of pivotal events involved in responding for each IEs are identified. Based on this information, initiating events group can be modeled using the same event tree analysis.

Event trees are graphical models that order and reflect events according to the requirements for mitigation of each group of initiating events. Events or 'headings' of an event tree can be any (or combination of) safety functions, safety systems, basic events and operator actions. The event tree heading are generally ordered according to their time of intervention. A support system must enter the sequence before the affected systems in order for a support system failure to fail the systems it supports.

For each heading of the event tree, the set of possible success and failure states are defined and enumerated. Each state gives rise to a branching of the event tree. The general practice is assigning "success" to the top branch and "failure" to the bottom branch.

Combination of all the states through the event tree branching logic gives different paths ending with accidental or healthy scenarios. In each path there is an initiating event and combination of safety system states, such a path is known as accident sequence. A typical event tree is shown in Fig. 10.6, it has 3 safety systems and with binary (success and failure) state combinations leading 8 (2^3) end states. Table 10.5 lists the Boolean expression sequences for all the accident sequences in the event tree. In complex systems there can be many safety systems making event tree with large number of sequences. However, the number of sequences can be reduced by eliminating physically impossible nodes. For example, a simplified event tree for large Loss of Coolant Accident (LOCA) in a PHWR is shown in Fig. 10.7. It has three pivotal events, viz.

1. Reactor protection system.
2. Total power supply system.
3. Emergency core cooling system.

Theoretically as shown in event tree (Fig. 10.6), it should have 8 paths, but it is having only 4 paths. This is because:

1. RPS failure will directly have significant consequence irrespective of other events and
2. ECCS is dependent on power supply.

The right side of event tree represents the end state that results from that sequence through the event tree. The end state can have healthy or accident consequences. To determine such consequence, through understanding of the system, operating experience, analyses of accidents (like thermal hydraulic or chemical reaction studies) is required.

The pivotal events (branches of event tree) may be simple basic events or may be a complex system which may require fault tree to get the minimal cut sets. The minimal cut set expression for each accident sequence is determined using Boolean algebra rules. This is illustrated with the following example.

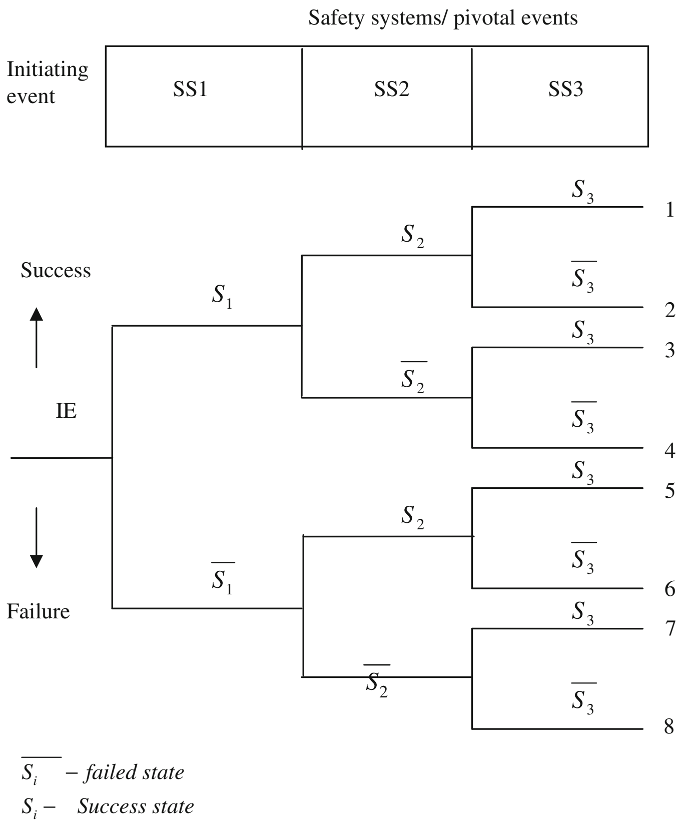


Fig. 10.6 Typical event tree having 3 safety systems; *S'* = failed state; *S* = success state

Table 10.5 Boolean expression for accident sequences

Accident sequence	Boolean expression
1	$\mathrm{I} \cap \mathrm{S}_1 \cap \mathrm{S}_2 \cap \mathrm{S}_3$
2	$\mathrm{I} \cap \mathrm{S}_1 \cap \mathrm{S}_2 \cap \bar{S}_3$
3	$I \cap S_1 \cap \overline{S_2} \cap S_3$
4	$I \cap S_1 \cap \overline{S_2} \cap \overline{S_3}$
5	$I \cap \overline{S_1} \cap S_2 \cap S_3$
6	$I \cap \overline{S_1} \cap S_2 \cap \overline{S_3}$
7	$I \cap \overline{S_1} \cap \overline{S_2} \cap S_3$
8	$I \cap \overline{S_1} \cap \overline{S_2} \cap \overline{S_3}$

Example 2 Consider the event tree shown in Fig. 10.8. Let SS_1 and SS_2 are derived from fault tree and SS_3 is a basic event given by the following expressions. Calculate the Boolean expression for accident sequence 8.

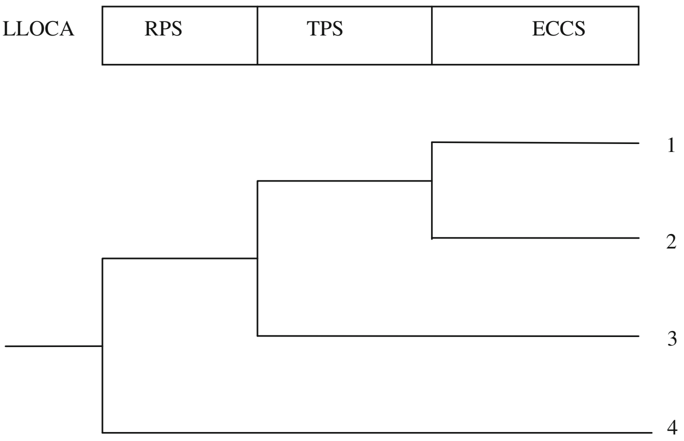


Fig. 10.7 Event tree for LLOCA

Solution: The Boolean expressions for the top events of fault tree are

$$\overline{S_1} = ab + ac$$
$$\overline{S_2} = (b + c)d$$
$$\overline{S_3} = e$$

The accident sequence 8 is having the Boolean expression.

$$AS_8 = I \cdot \overline{S_1} \cdot \overline{S_2} \cdot \overline{S_3}$$

Substituting the Boolean expression for each branch,

$$AS_8 = I(ab + ac) \cdot [(cb + c)d]e$$
$$AS_8 = [(ab + ac)(b + c)]d \cdot e$$
$$AS_8 = [ab + abc + abc + ac]d \cdot e$$
$$AS_8 = [ab + ac]d \cdot e$$
$$AS_8 = I \cdot a \cdot b \cdot d \cdot e + I \cdot a \cdot c \cdot d \cdot e$$

Quantitative evaluation, probability calculation of accident sequence, is similar to fault tree evaluation. The probability of accident sequence is

$$P(AS_8) = P(I \cdot a \cdot b \cdot d \cdot e) + P(I \cdot a \cdot c \cdot d \cdot e) - P(I \cdot a \cdot b \cdot c \cdot d \cdot e)$$

In complex systems like NPPs, there will be several initiating event groups. There will be an event tree for each initiating event group. The minimal cut sets (MCS) are determined for all the accident sequences in event trees. The accident

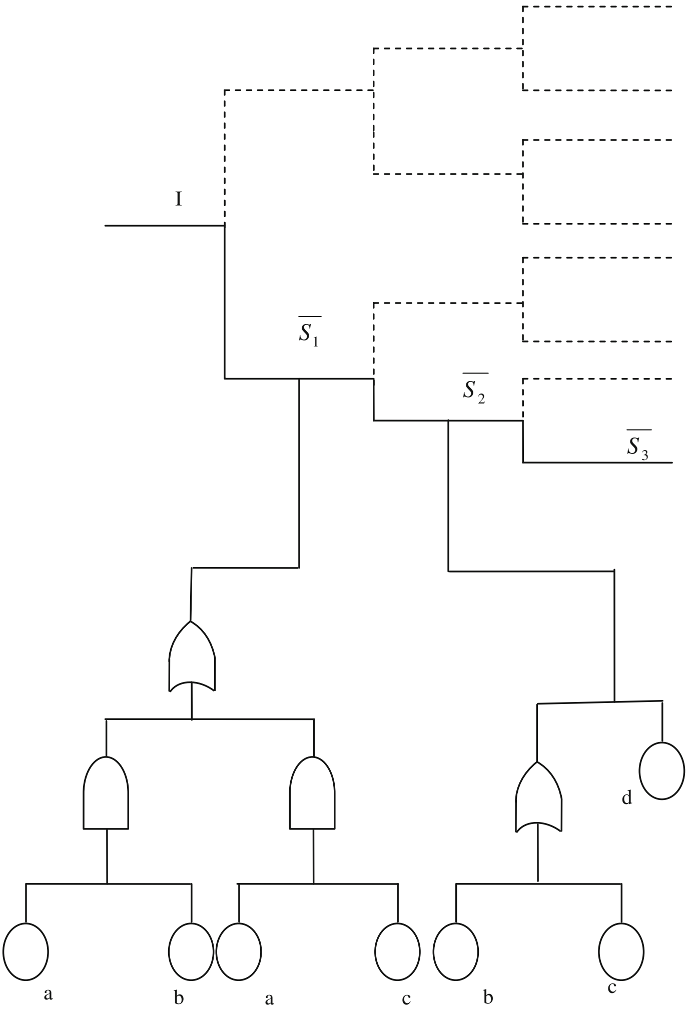


Fig. 10.8 Event tree with fault trees of associated branches

sequences having the same consequence (which satisfy the failure criterion) from these event trees are identified and the Boolean expression for the overall system (consequence) is obtained in the form of minimal cut sets. The probability of basic events will be subsequently used to quantify the system measure.

A simplified event tree for the initiating event class IV power supply failure for a PHWR is shown in Fig. 10.9. Software is required to do the analysis for such large event trees.

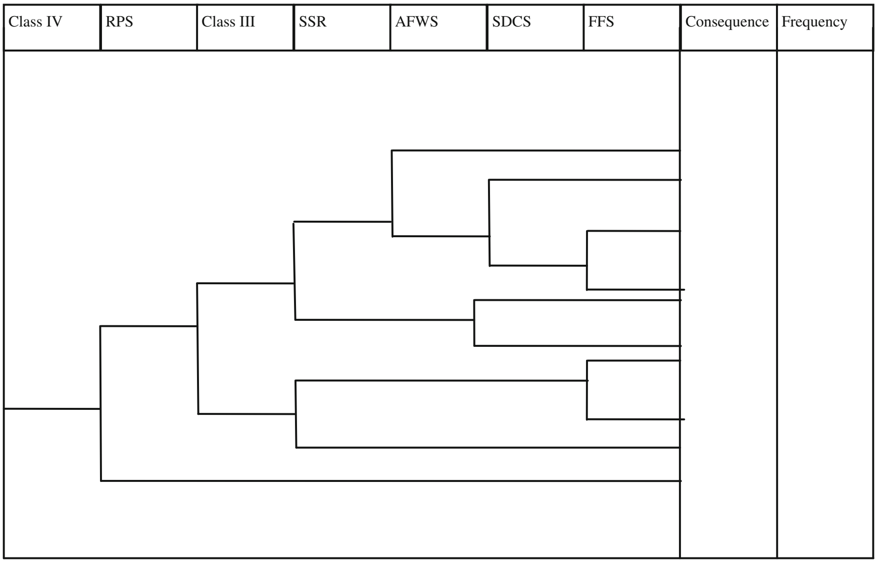


Fig. 10.9 A simplified event tree for CLASS IV failure of PHWR

10.6 Importance Measures

Quantification of system risk/reliability only gives the overall system performance measure. In case of improvement in the system reliability or reduction in risk is required, one has to rank the components or in general the parameter of system model. Importance measures determine the change in the system metric due to change in parameters of the model. Based on these importance measures, critical parameters are identified. By focusing more resources on the most critical parameters, system performance can be improved effectively. Importance measure also provides invaluable information in prioritization of components for inspection and maintenance activities. This section discusses various importance measures used in PSA.

Birnbaum Importance

The Birnbaum measure of importance is defined as the change in system risk for a change in failure probability for a basic event. The basic event can be component failure or human error or a parameter of system risk model. It is mathematically expressed as

$$I_i^B = \frac{\partial R}{\partial p_i} \tag{10.3}$$

where R is system risk or unavailability which is a function of n basic events.

$$R = f(x_1, x_2, \ldots, x_n) \tag{10.4}$$

p_i is the probability of basic event x_i.

In PSA or reliability analysis, R is expressed as probability over union of minimal cut sets. It is mathematically sum of products of basic event probabilities with the rare event approximation. Separating the terms having *i*th basic event probability p_i from the sum of products as shown in the following equation:

$$R = p_i A_i + B \tag{10.5}$$

where B is sum of products not having p_i and A_i is sum of products with p_i factored out. Now the Birnbaum importance measure can be defined as

$$I_i^B = \frac{\partial R}{\partial p_i} = \frac{\partial (p_i A_i + B)}{\partial p_i} = A_i \tag{10.6}$$

It can be observed from the final expression for Birnbaum measure of importance that it is not containing the probability of basic event p_i. This makes highly important but highly reliable basic events to have a high Birnbaum importance. For example, in case of a passive component like Bus in electrical power supply, may have high ranking. But the level of reliability Bus is already very high, if one want to focus on it for system metric improvement.

Inspection Importance
It is the Birnbaum importance of a basic event multiplied by the probability of that basic event. Inspection importance is the risk due to cut sets containing *i*th components. It is expressed as

$$\begin{aligned} I_i^I &= p_i \times \frac{\partial R}{\partial p_i} \\ \text{or} \quad I_i^I &= p_i \times A_i \end{aligned} \tag{10.7}$$

Fussel-Vesely Importance
It is the fractional change in risk for a fractional change in a basic event probability, i.e.,

$$I_i^{FV} = \frac{(\partial R/R)}{(\partial p_i/p_i)} = \frac{p_i}{R} \times \frac{\partial R}{\partial p_i} \tag{10.8}$$

As we have $\frac{\partial R}{\partial p_i} = A_i$, now

$$I_i^{FV} = \frac{p_i}{R} \times A_i \tag{10.9}$$

The three importance measure discussed previously deal with basic event probabilities one event at a time. Bolgorov and Apostalakis [13] proposed differential importance measure which considers all basic event probabilities. It is defined as follows

$$I_i^{DIM} = \frac{\frac{\partial R}{\partial p_i} dp_i}{\sum_{j=1}^{n} \frac{\partial R}{\partial p_j} dp_j} \tag{10.10}$$

Assuming a uniform change for all basic events, differential importance measure can be expressed as a function of Birnbaum importance

$$I_i^{DIM} = \frac{I_i^{BM}}{\sum_{j=1}^{n} I_j^{BM}} \tag{10.11}$$

Assuming a uniform percentage change for all basic event probabilities ($\delta p_i/p_i$), DIM can be expressed as a function of Fussel-Vesely importance

$$I_i^{DIM} = \frac{I_i^{FV}}{\sum_{j=1}^{n} I_j^{FV}} \tag{10.12}$$

This is applicable to all the analysis conditions, for example parameters of the model have different dimensions.

A detailed overview of importance measures used in PSA is discussed in [14].

Example 3 An emergency power supply has 3 diesel generators. One DG is sufficient for all the emergency loads and loads are connected to the buses in such a way that failure of any one bus will not affect the performance of the system. The line diagram of power supply is shown in Fig. 10.10. Construct the fault tree and calculate the minimal cut sets. Using importance measures rank the components of the system.

Solution: Fault tree for emergency power supply is shown in Fig. 10.11.

The minimal cut sets of the system are

$$\begin{aligned} T = {} & B1B2 + B1DG2DG3 + B1CB2DG2 + B2DG1DG3 + B2CB1DG1 \\ & + DG1DG2DG3 + CB1CB2DG1DG2 \end{aligned}$$

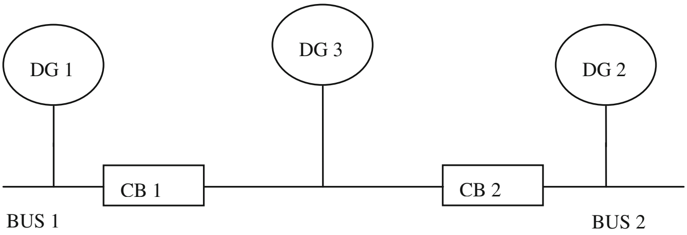


Fig. 10.10 Line diagram of emergency power supply

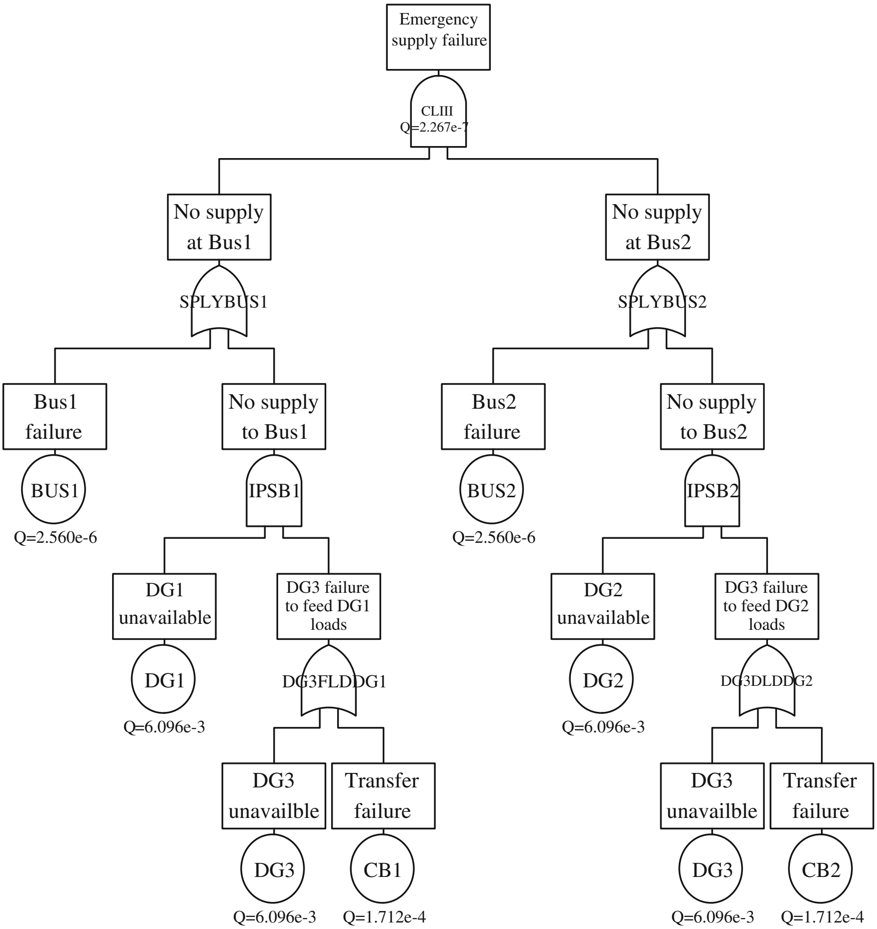


Fig. 10.11 Fault tree for emergency supply failure

Using the formulae mentioned above, importance measures are evaluated for each component as shown in the following Table 10.6.

Now the ranking is given to each component based on the obtained values as shown in Table 10.7.

10.7 Common Cause Failure Analysis

Dependencies that exist inherently in engineering systems possess limitation in achieving high reliability and safety. By providing high factor of safety and redundancy reliability and safety can be improved up to level, beyond that it is a

Table 10.6 Importance measures for each component

Comp	Birnbaum	Inspection	Fussel Vesely	DIM (1)	DIM (2)
B1	4.07E-5	1.043E-10	4.6E-4	0.211	1.53E-4
B2	4.07E-5	1.043E-10	4.6E-4	0.211	1.53E-4
DG1	3.71E-5	2.26E-7	9.995E-1	0.192	0.333
DG2	3.71E-5	2.226E-7	9.995E-1	0.192	0.333
DG3	3.719E-5	2.267E-7	9.999E-1	0.1926	0.3333
CB1	2.197E-8	3.76E-12	1.658E-5	1.13E-4	5.52E-6
CB2	2.197E-8	3.76E-12	1.658E-5	1.13E-4	5.52E-6

Table 10.7 Importance ranking

Comp	Birnbaum	Inspection	Fussel Vesely	DIM (1)	DIM (2)
B1	1, 2	4, 5	4, 5	1, 2	4, 5
B2	1, 2	4, 5	4, 5	1, 2	4, 5
DG1	4, 5	2, 3	2, 3	4, 5	2, 3
DG2	4, 5	2, 3	2, 3	4, 5	2, 3
DG3	3	1	1	3	1
CB1	6, 7	6, 7	6, 7	6, 7	6, 7
CB2	6, 7	6, 7	6, 7	6, 7	6, 7

challenge to improve due to the dependencies. For example, all redundancies may fail due to exposure to harsh physical environment. The recognition of dependent failures can provide insights into strong and weak points of system design and operation. All the dependencies should be listed separately and should also be properly included in fault tree/event tree models in order to evaluate correctly their impact on the level of risk. Nevertheless, all the dependent failures may not have specific root cause to incorporate directly into fault trees/event trees. Dependent failures whose root causes are not explicitly modeled are known as common cause failures (CCFs). This section provides a brief description of various CCF models available in the literature.

10.7.1 Treatment of Dependent Failures

In the probability framework, the simultaneous occurrence of two events A and B is given by

$$P(A \cap B) = P(A) \cdot P\left(\frac{B}{A}\right)$$

Generally in PSA calculation, it is assumed that A and B are independent and simply the product of P(A) and P(B) is used.

$$P(A \cap B) = P(A) \cdot P(B)$$

However, in the presence of positive dependency $P(A \cap B) > P(A) \cdot P(B)$, due to the fact that $P\left(\frac{B}{A}\right) > P(B)$.

Thus, independent assumption may underestimate the risk value if there exists positive dependency in reality.

There can be many different classifications of dependencies. As per the standard on CCF by NUREG/CR-4780 [15], and IAEA 50P-4 [4] dependences are categorized as three types. *Functional dependences* are due to sharing of hardware (e.g. common pump, valve, pipe, etc.) or due to process coupling (e.g. electrical, hydraulic, mechanical connections, etc.). *Physical dependences* are events that cause multiple failures or accident initiators from extreme environmental stresses, which could be external hazards (e.g. fire, flood, earthquakes, etc.) or internal events. *Human interaction dependences* are due to human errors (e.g. miscalibration of safety systems).

In all the dependencies categories, it is failure of two or more components due to a shared cause or event. If the clear cause-effect relationship can be identified which is making failure of multiple events, then it should be explicitly modeled in the system model. For Example fires, floods and earthquakes are treated explicitly as initiating events of events trees in PSA. Human errors are also included as branches of event trees. However, multiple failure events for which no clear root cause event identified, can be modeled using implicit methods categorized as CCF models thus CCF represent residual dependencies that are not explicitly modeled in ET/FTs. CCF can therefore belong to any of the above mentioned types.

CCFs are classified as due to design, construction, procedural and environmental causes. These can be further sub-divided as due to functional deficiencies, realization faults, manufacturing, installation, test and maintenance, operation, human error, normal extremes and energetic extremes. The predominant causes are design (30–50 %) operation and maintenance errors (30 %) and rest due to normal and extreme environmental causes (30 %). Examples of CCF failures reported in the past: Fire at Browns Ferry nuclear power plant; Failure of all 3 redundant auxiliary feed water pumps failed during TMI accident.

Defense against CCF

By adopting the following defenses during design and operating practices, one can eliminate or reduce vulnerabilities of the system for common cause failures.

1. Diversity (For example in NPP shut down can be achieved by inserting shut off rods or by injecting liquid poison into moderator, the physical principle of working is completely independent. Diversity can be provided from the manufacturing side also.)
2. Staggered testing
3. Staggered maintenance
4. Physical barriers

10.7.2 The Procedural Framework for CCF Analysis

The procedure for the CCF analysis is divided into three phases: (I) Screening Analysis (II) Detailed Qualitative Analysis and (III) Detailed Quantitative Analysis

Phase 1—screening analysis
Steps
1.1 Plant familiarization, problem definition and system modelling
1.2 Preliminary analysis of CCF vulnerability
1.2.1 Qualitative screening
1.2.2 Quantitative screening
Phase 2—detailed qualitative analysis
Steps
2.1 Review of operating experience
2.2 Development of root cause-defence matrices
Phase 3—detailed quantitative analysis
Steps
3.1 Selection of probability models for common cause basic events
3.2 Data analysis
3.3 Parameter estimation
3.4 Quantification
3.5 Sensitivity analysis
3.6 Reporting

Interested reader can refer [15–18] for detailed description of procedural framework that was developed in for performing a CCF analysis.

10.7.3 Treatment of Common Cause Failures in Fault Tree Models

Components having implicit shared causes of failure are identified in the model. The fault trees are then modified to explicitly include these shared causes. Based on the number of components, the new basic events are introduced to consider these common causes. Fault trees are then solved to obtain minimal cut sets which are now updated with common cause basic events. To illustrate the treatment of CCFs, consider a system having two identical redundant components. If CCF is not considered, the cut set is only one as shown in Fig. 10.12a, where A denote the failure of component A and B denote the failure of component B.

In the presence of CCF, an event C_{AB} can be defined as the failure of both components A and B due to common cause. Each component basic event becomes a sub tree containing its independent failure and common cause basic events. Figure 10.12b shows the fault tree model considering the common cause event. Using Boolean algebra, it can be simplified to fault tree shown in Fig. 10.12c. Thus, the Boolean expression of the system is given by: $T = A_I \cdot B_I + C_{AB}$.

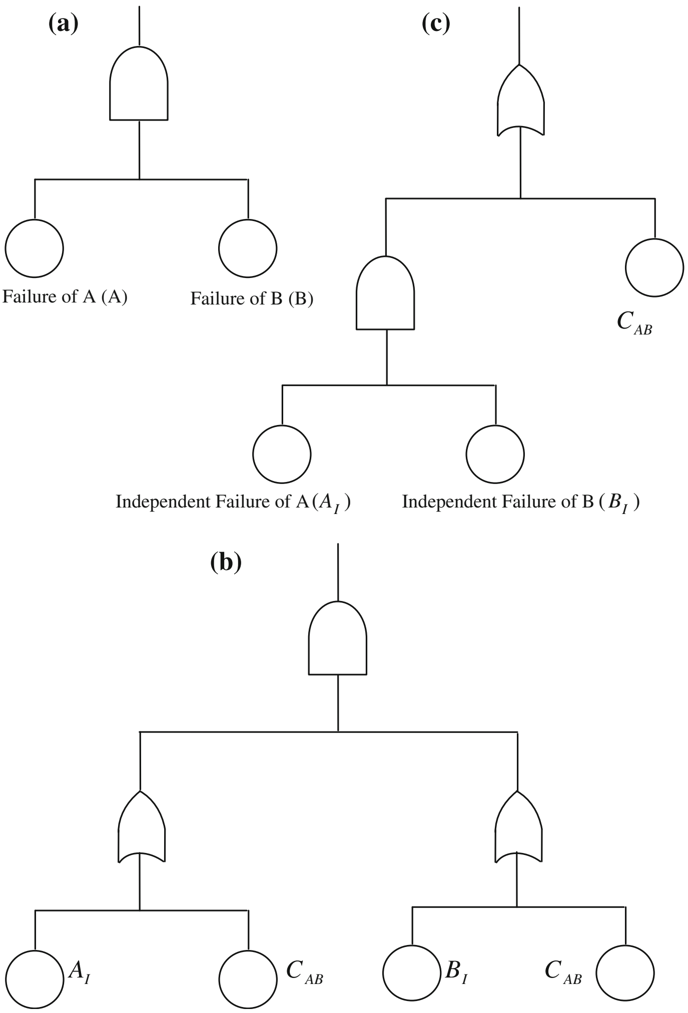


Fig. 10.12 Active parallel redundancy with/without CCF

To illustrate the difference between the case where CCF is not considered and the case with CCF, a numerical example is considered here.

Example 4 Let the total probability of failure of each component A and B is 0.05. It is known from the experience that 10 % times both the components fail due to common cause. Compare probability of failure of system constituting A and B in active parallel redundancy with respect to (i) Without considering CCF and (ii) considering CCF

Solution:
Case (i): Refer Fig. 10.12a

$$\begin{aligned} \mathrm{P(T)} &= \mathrm{P(A \cdot B)} \\ &= \mathrm{P(A) \cdot P(B)} \\ &= 2.5 \times 10^{-3} \end{aligned}$$

Case (ii): Refer Fig. 10.12b, c

$$\begin{aligned} P(T) &= P(A_I \cdot B_I + C_{AB}) \\ &= P(A_I \cdot B_I) + P(C_{AB}) - P(A_I \cdot B_I) \cdot P(C_{AB}) \\ &= 7.015 \times 10^{-3} \end{aligned}$$

Thus neglecting CCF can underestimate the final result.

In case of two redundant system, there is only one common cause basic event (CCBE), C_{AB}. In a system of three redundant components A, B and C, the CCBEs are C_{AB}, C_{AC}, C_{BC} and C_{ABC}. The first 3 events represent common cause events involving any two components and fourth is common cause event involving all three components. Each component can fail due to its independent cause and it associated CCBEs. For example, the component A failure can be represented by the sub tree shown in Fig. 10.13.

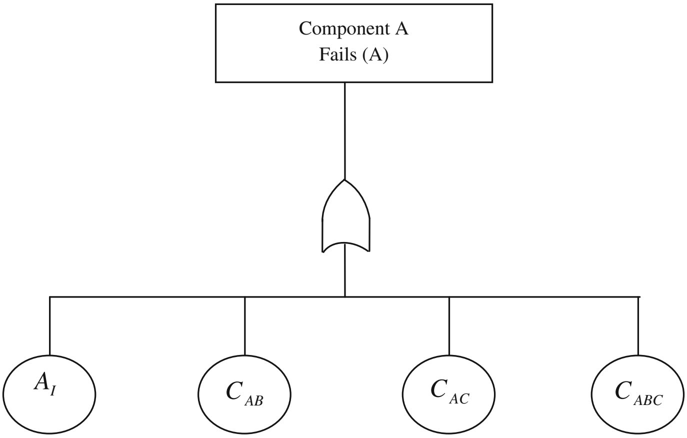


Fig. 10.13 Component A failure

The Boolean expression for the total failure of component A is given by

$$
\begin{aligned}
& A = A_I + C_{AB} + C_{AC} + C_{ABC} \\
& Let \quad P(A_I) = Q_1 \\
& P(C_{AB}) = P(C_{AC}) = Q_2 \\
& P(C_{ABC}) = Q_3
\end{aligned}
$$

Now,

$$P(A) = Q_1 + 2Q_2 + Q_3$$

Generalizing for ‘n’ component common cause group and assuming the probability of CCBE depends on the number and not on the specific components in that basic event.

Let Q_1—represents each independent failure probability

Q_i—represent probability of failure CCBE involving i number of components.

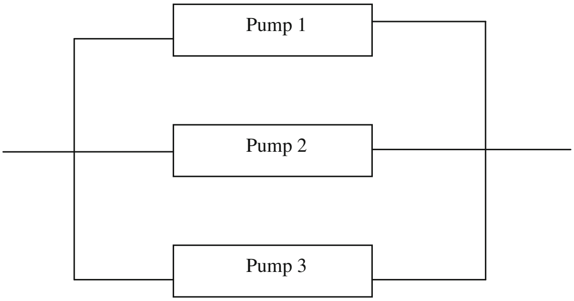
The total probability of failure of a component Q_t is expressed as

$$Q_t = \sum_{i=1}^{n} {}^{n-1}C_{i-1} Q_i \tag{10.13}$$

Q_i values can be computed from the experience. To account for the lack of data, parameter models such as β factor, ά factor, and multiple Greek letter models are used which put less stringent requirements on the data.

Example 5 Consider the following pumping system (Fig. 10.14) consistency of three identical parallel pumps. Operation of one pump is sufficient for successful operation of the system. Develop the fault tree with CCBEs and quantify the failure probability of the system given $Q_1 = 0.012, Q_2 = 1e.3$ and $Q_3 = 6e{-}4$

Fig. 10.14 Pumping system



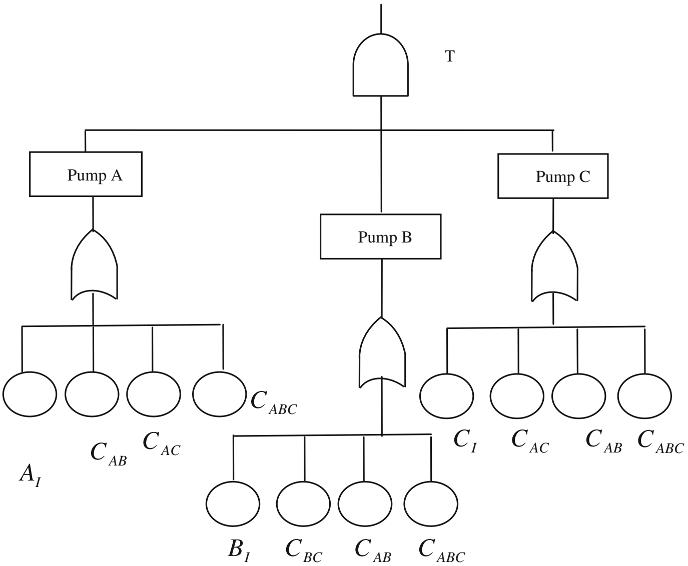


Fig. 10.15 Fault tree for pumping system

Solution: From the fault tree (Fig. 10.15), we have the following gate expressions.

$$
\begin{aligned}
T &= A \cdot B \cdot C \\
A &= A_I + C_{AB} + C_{AC} + C_{ABC} \\
B &= B_I + C_{AB} + C_{BC} + C_{ABC} \\
C &= C_I + C_{BC} + C_{AC} + C_{ABC}
\end{aligned}
$$

Using Absorption and Independent law of Boolean algebra, A · B can be simplified to

$$
\begin{aligned}
A \cdot B &= (A_I + C_{AB} + C_{AC} + C_{ABC}) \cdot (B_I + C_{AB} + C_{BC} + C_{ABC}) \\
A \cdot B &= A_I B_I + C_{AB} + A_I C_{BC} + C_{AC} \cdot C_{BC} + C_{ABC}
\end{aligned}
$$

$$
\begin{aligned}
A \cdot B \cdot C &= (A_I + C_{AB} + C_{AC} + C_{ABC}) \cdot (B_I + C_{AB} + C_{BC} + C_{ABC}) \cdot (C_I + C_{BC} + C_{AC} + C_{ABC}) \\
A \cdot B \cdot C &= (A_I B_I + C_{AB} + A_I C_{BC} + C_{AC} \cdot C_{BC} + C_{ABC}) \cdot (C_I + C_{AC} + C_{BC} + C_{ABC})
\end{aligned}
$$

After simplification, the final Boolean expression is

$$
\begin{aligned}
T = & C_{ABC} + A_I C_{BC} + B_I C_{AC} + C_I C_{AB} + C_{AB} \cdot C_{BC} \\
& + C_{AC} \cdot C_{BC} + C_{AC} \cdot C_{AB} + A_I B_I C_I
\end{aligned}
$$

Using rare event approximation and assuming

$$\begin{aligned} P(A_I) &= P(B_I) = P(C_I) = Q_1 \\ P(C_{AB}) &= P(C_{BC}) = P(C_{AC}) = Q_2 \\ P(C_{ABC}) &= Q_3 \end{aligned}$$

The failure probability of the system is $P(T) = Q_3 + 3Q_1Q_2 + 3{Q_2}^2 + 3{Q_2}^3$ Substituting the given values, P(T) = 6.71e-4.

10.7.4 Common Cause Failure Models

CCF models are used to quantify common cause basic events. Numerous CCF models are available in the literature, three of which are discussed below. Table 10.8 gives an overview of formulae for CCF basic event probabilities and estimate of CCF parameters for three CCF models. Currently, most of the commercial PSA tools come with CCF models implemented in logic models. The basic inputs required for such tools are only the CCF parameter values and total failure probability of the component including common cause contribution.

Beta Factor Model

Beta factor model was introduced by Fleming [19], which was the first CCF model used in PSA studies [17]. This model is based on the following assumptions:

1. A constant fraction (β) of component failure probability/rate is from common cause events.
2. The occurrence of common cause event results in simultaneous failure of all components in the CCF group

Table 10.8 CCF models and parameter estimates

Name of CCF model	General form for multiple component failure probabilities	Point estimators
Beta factor (β)	$Q_k = (1-\beta)Q_t \quad k = 1$ $Q_k = 0 \quad 2 \leq k \prec m$ $Q_k = \beta Q_t \quad k = m$	$\beta = \frac{\Sigma_{k=2}^m kn_k}{\Sigma_{k=1}^m kn_k}$
Multiple greek letters (β, ά, ν)	$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \prod_{l=1..k} (\rho_l)(1-\rho_{k+1})Q_t$ ρ1 = 1, ρ2 = β, ρ3 = γ, …, ρm+1 = 0	$\rho_l = \frac{\Sigma_{k=l}^m kn_k}{\Sigma_{k=l-1}^m kn_k}$
Alpha factor (ά)	$Q_k^{(m)} = \frac{k\alpha_k^{(m)}}{\binom{m-1}{k-1}\alpha_t} Q_t$ where $\alpha_t = \sum_{k=1}^m k\alpha_k^{(m)}$	$\alpha_k = \frac{n_k}{\Sigma_{k=1}^m n_k}$

Let Q_t is the total failure probability of a component, whose failure events are from independent and common cause events. Q_t is the sum of independent and common cause failure probabilities as expressed in Eq. 10.14.

$$Q_t = Q_I + Q_{CCF} \tag{10.14}$$

Q_I is the independent failure probability of the single component, Q_{CCF} is CCF contribution associated with 'm' components.

As per the assumption 1 mentioned earlier,

$$\begin{aligned} Q_{CCF} &= \beta Q_t \\ Q_I &= (1-\beta)Q_t \end{aligned} \tag{10.15}$$

By re-arranging for β:

$$\beta = \frac{Q_{CCF}}{Q_I + Q_{CCF}} \tag{10.16}$$

To generalize the equation, it can be written for m components involving failure of k components (k ≤ m),

$$\begin{array}{ll} Q_k = (1-\beta)Q_t & \mathrm{k} \ = 1 \\ Q_k = 0 & 2 \le k \prec m \\ Q_k = \beta Q_t & k = m \end{array} \tag{10.17}$$

where Q_k is the probability of basic event involving k specific components.

Estimator for the β—Factor Model Parameter

The parameters of CCF models are calculated using data from operational experience. The estimator for β is given by Eq. (10.18) as derived in [17]. '$\mathrm{n_k}$' is number of failures involving 'k' components.

$$\beta = \frac{\Sigma_{k=2}^{m} k n_k}{\Sigma_{k=1}^{m} k n_k} \tag{10.18}$$

Beta factor model is the most simple and stright forward CCF model. On the flip side, this method is more suitable for 2 component groups. This model gives conservative results for CCF groups that are more than 2 components.

Example 6 There are two redundant Diesel Generators (DGs) present as a part of emergency power supply to take safety loads at the time of grid supply failure. The following information is available from the operating experience, calculate $\mathrm{Q_t}$—the total failure probability of one component, $\mathrm{Q_I}$—the independent failure probability of the single DG, $\mathrm{Q_2}$—the probability of basic event failure involving both DGs.

Solution: No of demands = N_D = 1500
No of times DG_1 or DG_2 alone failed = n_1 = 50
No of times both DGs failed = n_2 = 4
Parameter Estimation: $\beta = \frac{\Sigma_{k=2}^{m} kn_k}{\Sigma_{k=1}^{m} kn_k}$
m = 2 in the given example
$\beta = 2n_2/(n_1 + 2n_2) = 0.138$

Calculation of Failure Probabilities:
The total failure probability considering independent and common cause failures is Q_t. The general expression for Q_t irrespective of CCF model is

$$Q_t = \frac{1}{mN_d} \sum_{k=1}^{m} kn_k \tag{10.19}$$

$$\mathrm{Qt} = (\mathrm{n}_1 + 2\mathrm{n}_2)/(2\ \mathrm{N_D}) = 0.01933$$
$$\mathrm{Q2} = \beta \times \mathrm{Qt} = 2.668 \times 10^{-3}$$

Multiple Greek Letter Model
The Multiple Greek Letter Model was introduced by Fleming et al., [20]. This model is an extension of beta factor model discussed earlier. The combinations of common cause component failures are defined, which overcomes the limitations of beta factor model in accounting higher order redundancies. As the name indicates multiple factors (e.g. γ, δ, etc.) are introduced to represent conditional probabilities of all the possible ways a common cause failure of a component can be shared with other components, which can be used to define probabilities of CCF combinations.

For a group of m redundant components and for each given failure mode, m different parameters are defined. For a general case,

$$Q_k^{(m)} = \frac{1}{\begin{pmatrix} m-1 \\ k-1 \end{pmatrix}} \underset{l=1\ldots k}{\Pi} (\rho_l)(1 - \rho_{k+1})Q_t \tag{10.20}$$

where $\rho_1 = 1$, $\rho_2 = \beta$, $\rho_3 = \gamma$, …, $\rho_{m+1} = 0$

The following equations express the probability of multiple component failures due to common cause, Q_k, in terms of the MGL parameters, for a 3-component group:

$$Q_1^3 = (1-\beta)Q_t; \quad Q_2^3 = \frac{\beta(1-\gamma)Q_t}{2}; \quad Q_3^3 = \beta\gamma Q_t;$$

For a 4-component group:

$$Q_1^4 = (1-\beta)Q_t; \quad Q_2^4 = \frac{\beta(1-\gamma)Q_t}{3}; \quad Q_3^4 = \frac{\beta\gamma(1-\delta)Q_t}{3}; \quad Q_4^4 = \beta\gamma\delta Q_t$$

Estimators for the MGL Parameters

The simple point estimators of the MGL parameters are defined as,

$$\rho_l = \frac{\Sigma_{k=l}^{m} kn_k}{\Sigma_{k=l-1}^{m} kn_k} \quad (l = 2,\, 3, \ldots \mathrm{m}) \tag{10.21}$$

where $\mathrm{n_k}$ is defined as the number of events involving the failures of exactly k components.

Example 7 For a four unit redundant system, the following data is available from operating experience: In 750 demands, 9 independent failures, 3 failures involving 2 subsystems, 1 failure involving 3 subsystems, and 2 failures involving all were reported. Estimate the parameters of MGL model and calculate the CCF basic event failure probabilities.

Solution:

The parameters of CCF model based on MGL are estimated using Eq. (10.21):

$$\beta = \frac{\Sigma_{k=2}^{4} kn_k}{\Sigma_{k=1}^{4} kn_k} = 0.654,$$

$$\gamma = \frac{\Sigma_{k=3}^{4} kn_k}{\Sigma_{k=2}^{4} kn_k} = 0.647$$

$$\delta = \frac{4n_4}{\Sigma_{k=3}^{4} kn_k} = 0.727$$

Total failure probability is determined using Eq. (10.19)

$$Q_t = \frac{1}{mN_d} \sum_{k=1}^{m} kn_k = 8.67\text{e-}3/\mathrm{d}$$

CCF basic event probabilities are calculates using Eq. (10.20)

$$Q_1^4 = (1 - \beta)Q_t = 3.0\text{e-}3$$

$$Q_2^4 = \frac{\beta(1 - \gamma)Q_t}{3} = 6.67\text{e-}4$$

$$Q_3^4 = \frac{\beta\gamma(1 - \delta)Q_t}{3} = 3.33\text{e-}4$$

$$Q_4^4 = \beta\gamma\delta Q_t = 2.67\text{e-}3$$

Alpha—Factor Model

The most widely used CCF model is the alpha factor model introduced by Mosleh [21]. The application of alpha factor model include aerospace [3, 22] besides nuclear PSAs. To overcome the difficulties in estimating the parameters for beta and

MGL CCF models from operating experience, alpha factor model is recommended because of its simpler statistical model.

In alpha factor model, CCF probabilities are defined as a function of failure frequency ratios ($\alpha_k^{(m)}$, alpha factor parameters) and the total component failure probability, Q_t. The failure frequency ratios or alpha factor parameters are defined as the ratio of the probability of failure events involving any k components over the total probability of all failure events in a group of m components, and $\Sigma_k \alpha_k^{(m)} = 1$.

$$\alpha_k^m = \frac{\binom{m}{k} Q_k^{(m)}}{\Sigma_{k=1}^m \binom{m}{k} Q_k^{(m)}} \tag{10.22}$$

The basic event probabilities can be expressed in terms of Q_t and the alpha factors as follows:

$$Q_k^{(m)} = \frac{k\alpha_k^{(m)}}{\binom{m-1}{k-1}\alpha_t} Q_t \quad \text{where } \alpha_t = \sum_{k=1}^{m} k\alpha_k^{(m)} \tag{10.23}$$

CCF basic event probabilities for three components

$$Q_1 = \frac{\alpha_1}{\alpha_t} Q_t; \quad Q_2 = \frac{\alpha_2}{\alpha_t} Q_t; \quad Q_3 = \frac{3\alpha_3}{\alpha_t} Q_t$$

CCF basic event probabilities for four components

$$Q_1 = \frac{\alpha_1}{\alpha_t} Q_t; \quad Q_2 = \frac{2\alpha_2}{3\alpha_t} Q_t; \quad Q_3 = \frac{\alpha_3}{\alpha_t} Q_t; \quad Q_4 = \frac{4\alpha_4}{\alpha_t} Q_t$$

Estimators for the α—Factor Model Parameters

The alpha factor model parameters (α_k) can be estimated with the following equation, which is based on its definition discussed earlier. As the equation indicate, information regarding number of demands is not necessary to estimate the parameters.

$$\alpha_k = \frac{n_k}{\Sigma_{k=1}^m n_k} \tag{10.24}$$

Example 8 Assuming the data mentioned in Example 7, calculate the CCF basic event probabilities for α Factor Model.

Solution:

Using Eq. (10.24), parameters of α Factor Model can be estimated as follows:

$$\alpha_1 = \frac{n_1}{\Sigma_{k=1}^{4} n_k} = 0.6$$
$$\alpha_2 = \frac{n_2}{\Sigma_{k=1}^{4} n_k} = 0.2$$
$$\alpha_3 = \frac{n_3}{\Sigma_{k=1}^{4} n_k} = 0.0667$$
$$\alpha_4 = \frac{n_4}{\Sigma_{k=1}^{4} n_k} = 0.1333$$

The total failure probability Q_t is determined using Eq. (10.19)

$$Q_t = \frac{1}{mN_d}\sum_{k=1}^{m} kn_k = 8.67\text{e-}3/\text{d}$$

Basic event CCF probabilities are calculated using Eq. (10.23)

Using $\alpha_t = \sum_{k=1}^{m} k\alpha_k^{(m)}$, $\alpha_t = 1.733$.

Substituting Q_t and α_i in Eq. (10.23) yields the CCF basic event failure probabilities

$$Q_1 = \frac{\alpha_1}{\alpha_t} Q_t = 3.0e{-3}$$
$$Q_2 = \frac{2\alpha_2}{3\alpha_t} Q_t = 6.67e{-3}$$
$$Q_3 = \frac{\alpha_3}{\alpha_t} Q_t = 3.33e{-4}$$
$$Q_4 = \frac{4\alpha_4}{\alpha_t} Q_t = 2.67e{-3}$$

The results of alpha factor model matched with multiple Greek letter model results obtained in Example 7.

Example 9 A power supply system (shown in Fig. 3.30) consists of four UPS and 3 Bus bars. Power supply at any of the three Buses is sufficient for feeding the loads. UPS4 is standby for any failed UPS. Considering CCF basic event for both UPS and Bus, develop the fault tree and calculate the system failure probability from the given following information. Total unavailability of the each UPS and Bus is 5.5e-4 and 1.6e-6 respectively. Assume the α factors for Bus as $\alpha_1 = 0.95$; $\alpha_2 = 0.04$; $\alpha_3 = 0.01$ and for UPS as $\alpha_1 = 0.95$; $\alpha_2 = 0.035$; $\alpha_3 = 0.01$ and $\alpha_4 = 0.005$. Calculate CCF basic event probabilities and unavailability of system?

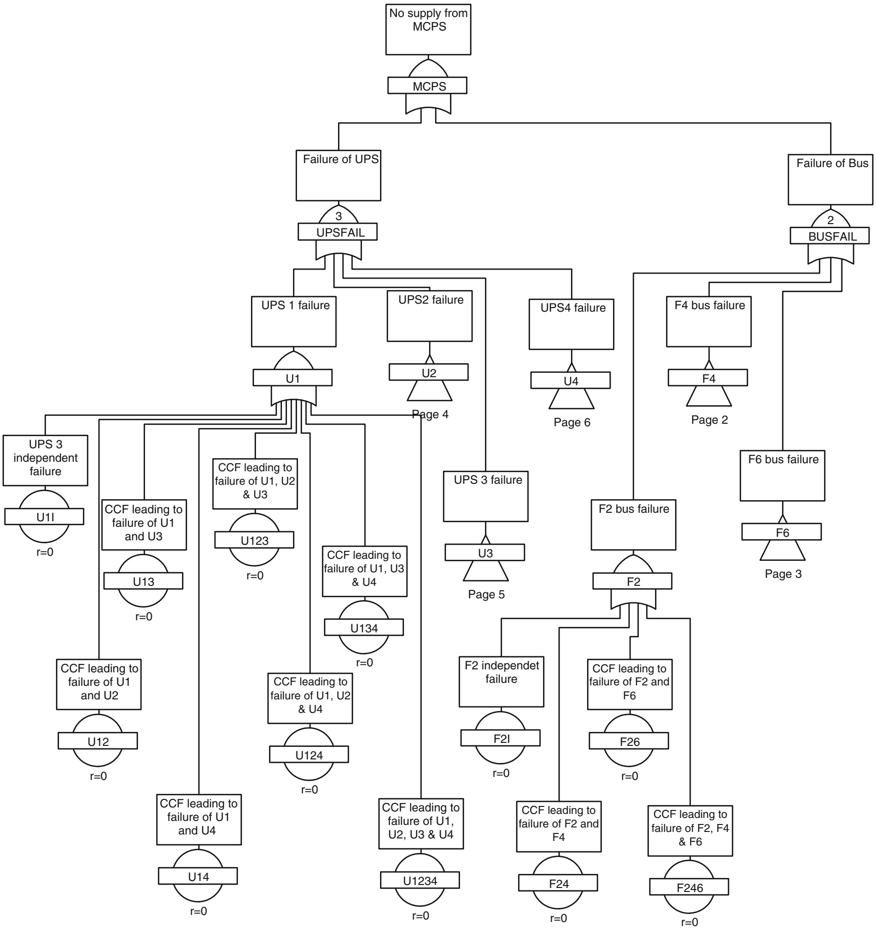

No supply from MCPS
MCPS
Failure of UPS
3
UPSFAIL
Failure of Bus
2
BUSFAIL
UPS 1 failure
U1
UPS2 failure
U2
Page 4
UPS4 failure
U4
Page 6
F4 bus failure
F4
Page 2
F6 bus failure
F6
Page 3
UPS 3 independent failure
U1I
r=0
CCF leading to failure of U1 and U3
U13
r=0
CCF leading to failure of U1, U2 & U3
U123
r=0
CCF leading to failure of U1, U3 & U4
U134
r=0
UPS 3 failure
U3
Page 5
F2 bus failure
F2
CCF leading to failure of U1 and U2
U12
r=0
CCF leading to failure of U1, U2 & U4
U124
r=0
F2 independet failure
F2I
r=0
CCF leading to failure of F2 and F6
F26
r=0
CCF leading to failure of U1 and U4
U14
r=0
CCF leading to failure of U1, U2, U3 & U4
U1234
r=0
CCF leading to failure of F2 and F4
F24
r=0
CCF leading to failure of F2, F4 & F6
F246
r=0

Fig. 10.16 Fault tree of MCPS with CCF

Fault tree for the given system is shown in Fig. 10.16. Minimal cut sets are shown in Table 10.9. There are 43 cut sets. Using symmetrical assumption and as the components are identical, the following notation is used.

For UPS:

$$\mathrm{U1I} = \mathrm{U2I} = \mathrm{U3I} = \mathrm{U4I} = \mathrm{P}_1$$

$$\mathrm{U12} = \mathrm{U23} = \mathrm{U24} = \mathrm{U14} = \mathrm{U13} = \mathrm{U34} = \mathrm{P}_2$$

$$\mathrm{U123} = \mathrm{U124} = \mathrm{U234} = \mathrm{U134} = \mathrm{P}_3$$

$$\mathrm{U1234} = \mathrm{P}_4$$

Table 10.9 Minimal cut sets of power supply system

No.	Cut set	No.	Cut set
1	U123	23	U24. U13
2	U124	24	U24. U34
3	U134	25	U2I. U34
4	U234	26	U12. U34
5	U1234	27	U13. U2I
6	F24	28	U12. U3I
7	F246	29	U23. U4I
8	F26	30	U23. U14
9	F46	31	U23. U24
10	U1I. U24	32	U23. U34
11	U13. U23	33	U12. U13
12	U12. U4I	34	U12. U23
13	U12. U14	35	F2I. F4I
14	U12. U24	36	U14. U2I
15	U14. U3I	37	F2I. F6I
16	U14. U34	38	U14. U24
17	U1I. U34	39	F4I. F6I
18	U1I. U23	40	U1I. U2I. U4I
19	U13. U4I	41	U2I. U3I. U4I
20	U13. U14	42	U1I. U2I. U3I
21	U13. U34	43	U1I. U3I. U4I
22	U24. U3I		

For Bus:

$$\mathrm{B1I} = \mathrm{B2I} = \mathrm{B3I} = \mathrm{Q}_1$$
$$\mathrm{B12} = \mathrm{B23} = \mathrm{B13} = \mathrm{Q}_2$$
$$\mathrm{B123} = \mathrm{Q}_3$$

The probability over sum of minimal cut sets using rare event approximation is now simplified to

$$P(T) = 4P_1^3 + 15P_2^2 + 12P_1P_2 + 4P_3 + P_4 + 3Q_1^2 + 3Q_2 + Q_3$$

CCF basic event probabilities for Bus:

$$\alpha_t = \sum_{k=1}^{m} k\alpha_k = \alpha_1 + 2\alpha_2 + 3\alpha_3 = 1.06$$

$$Q_1 = \frac{\alpha_1}{\alpha_t} Q_t = 1.43e{-6}; \quad Q_2 = \frac{\alpha_2}{\alpha_t} Q_t = 6.037e{-8}; \quad Q_3 = \frac{3\alpha_3}{\alpha_t} Q_t = 4.53e{-8}$$

CCF basic event probabilities for UPS:

$$\alpha_t = \sum_{k=1}^{m} k\alpha_k = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 = 1.07$$

$$P_1 = \frac{\alpha_1}{\alpha_t} P_t = 4.883e{-4}; \quad P_2 = \frac{2\alpha_2}{3\alpha_t} P_t = 3.59e{-5}; \quad P_3 = \frac{\alpha_3}{\alpha_t} P_t = 5.14e{-6}; \quad P_4 = \frac{4\alpha_4}{\alpha_t} P_t = 1.028e{-5}$$

Substituting all these CCF basic events in P(T), the unavailability of the system is obtained as 3.129e-5.

10.8 Human Reliability Analysis

Risk contributors not only include hardware and software failures but also events associated operator interactions. Traditional risk/reliability studies had assumed that majority of system failures were due to hardware failures, but it was found from the accident history that human error causes 20–90 % of all major system failures [12]. For example in aerospace industry 90 % of accidents were due to human error where as in nuclear power plants it was 46 %. The contribution of human error has grown to 60–80 % because of improvement in equipment reliability as well as maintenance [23]. Human reliability analysis (HRA) is extremely important because of significant human error contribution to risk. Human interactions are considered with special emphasis while doing PSAs. HRA is a key task in PSA of complex engineering systems such as NPPs and aerospace equipment.

10.8.1 HRA Concepts

HRA aims to identify human interactions, quantify the Human Error Probabilities (HEPs), and provide insights to reduce human errors. For example, human performance is enhanced by improved Man-Machine interface, procedures and training, increasing chance of recovery. The HEPs obtained from HRA are integrated into the PSA models which subsequently quantify total system risk.

Classification of Human Actions

Due to complex nature of human behavior, there are several classifications available in the literature. Rasmussen [24] classified human actions into three types based on work complexities, viz., Skill based actions, rule based actions, and knowledge based actions. Skill based actions are highly practiced activities, rule based actions are related to procedures followed, and knowledge based actions are tasks in unforeseen situations.

The most famous classification or taxonomy of human errors (by Swain and Guttmann [25]) is: *Error of Omission* occurs when an operator omits a step in a task or the entire task, amounting to an unintended or unnoticed action. *Error of Commission* occurs when the person does the task, but does it incorrectly, amounting to an unintended action excluding inaction. *Extraneous act*—wrong (unrequired) act performed.

In PSAs, human actions can be categorized into four types [26], types A, B, C, and C_R. Type 'A' actions are related to pre-accident initiator events or latent failures, resulting from test and maintenance actions, for example maintenance engineer forgetting to keep diesel generators in auto mode after its maintenance. Type 'B' actions are the actions leading to initiating event, operator unintentionally tripping a process system. Type 'C' actions are the actions required in response to initiating events, for example, often the recirculation or depressurization actions are manual actions required during accident scenarios in NPPs. Type 'C_R' are the recovery actions to mitigate the consequences in accident evolutions. Type 'A' actions are usually accounted in fault trees where as other actions are accounted in event trees as initiators or headers. For key actions required by the process, it is important to analyze what sub tasks need to be performed and by when (e.g. time window—the latest time by which operator must intervene) these tasks to be completed. Physical process simulations are usually performed to calculate the available time for human actions.

Performance Shaping Factors

Performance shaping factors (PSFs) is an essential element in HRA, which are the factors that influence human performance. PSFs can be categorized into three classes, viz., external (outside the individual, e.g. quality of environment), internal (that operate within the individual, e.g. cultural background, training, experience, motivation), and stressors (factor directly affecting mental and physical stresses, e.g. task speed and load, fatigue).

Dependence Analysis

A typical human action during an accident scenario encompasses detection/cue (e.g. see an alarm), diagnosis (assess the plant condition), decision (what to do), and execution (actual action affecting the system or plant). In a typical accident scenario in NPP, several such actions are required to be performed. Considering the possible dependence among the human actions ensures correct modeling in assessing HEPs. Dependence analysis explores how the failure of one task impacts the performance of another task.

10.8.2 HRA Process, Methods, and Tools

10.8.2.1 HRA Process

HRA process determines the contribution of human errors to system failures. A stepwise structured process of HRA was presented in [27] named systematic human action reliability procedure (SHARP, 1984). Briefly, the steps involved in the methodology are definition, screening, qualitative analysis, Representation and Model integration, quantification, and documentation. The interface between PSA and HRA is defined clearly. Screening is to identify human actions significant to safety of the plant/system. Detailed HRA methods such as technique for human error rate prediction (THERP), human cognitive reliability (HCR), and operator action tree (OAT) are applied to model the human actions and quantify HEPs.

IEEE standard 1082 [28], IEEE Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Systems (1997), gives a more detailed methodology for conducting HRA. Briefly, the steps in this HRA process are select and train HRA team, familiarize the team, build initial plant model, screen human interactions, characterize human interactions, quantify human interactions, update plant model, and review results. The additional feature of this process is building (or rebuilding) plant model by developing event sequence diagrams, which can lead to improvement in plant logic models and understanding of transient behavior. In quantifying human errors, this process does not select a specific HRA model as they depend on the specific needs and requirements. Despite the IEEE standard had been developed for NPP applications, it was also used in space application by National Aeronautics space administration (NASA) [26].

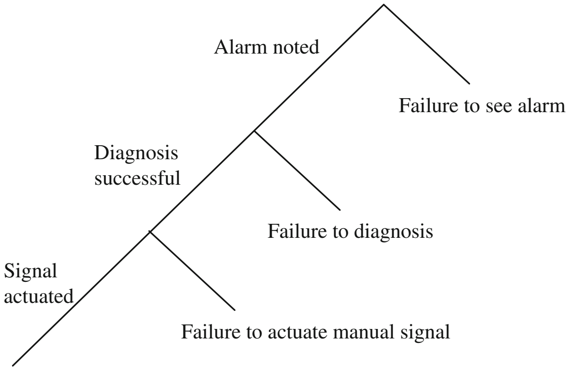
10.8.2.2 HRA Methods

Numerous HRA methods are available in the literature. Two methods are discussed briefly here.

The Technique for Human Error Rate Prediction (THERP)

The THERP method was developed by Swain and Guttmann in 1983 [25], which has been widely used in industrial applications and accepted by PSAs. The engineering approach of task analysis and the large human error database are the reasons for its popularity [23].

Fig. 10.17 A simplified HRA event tree for manual safety signal actuation



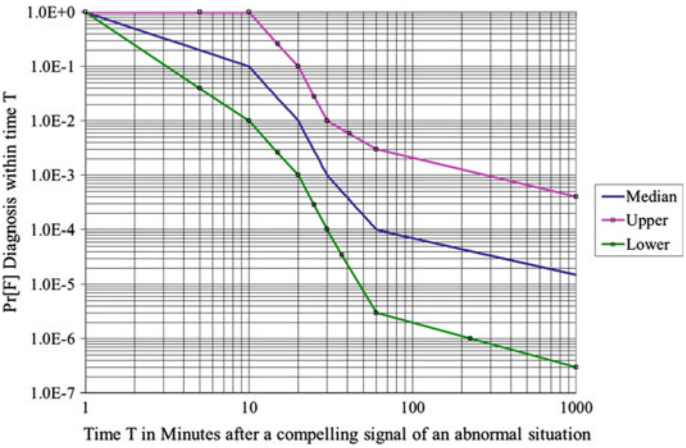


Fig. 10.18 THERP's nominal diagnosis model

THERP is based on task analysis which divides each task into subtasks for which basic HEPs are available in the database. The task and subtasks are represented with a HRA event tree (HRAET) as shown in Fig. 10.17. PSFs are used to adjust the base probabilities considering the scenario conditions. The concept of dependence model was introduced by THERP to modify HEPs according to dependencies involved. THERP also introduced recovery paths to account for corrective actions. The evaluation of HRAET gives overall HEP of the task.

THERP uses time reliability curves to model diagnosis and assigns a HEP value. The estimate of time window for diagnosis is the input to determine its failure probability. Figure 10.18 shows THERP's nominal diagnosis model giving median, upper bound and lower bound. THERP gives guidelines to use which of the three curves; for example, upper bound is used if the event is not covered in training, lower bound is used if the event is a well-recognized classic, and median if the event is well trained.

Example 10 In MLOCA scenario of NPPs, two operator actions, namely, recirculation and cooldown are often analyzed. Both actions are manually performed. Using THERP diagnosis model, determine HEP of diagnosis for both actions? Assume a diagnosis time window of 30 min for each action.

As recirculation is usually part of emergency operating procedures and a cue as an alarm is present, nominal median curve in THERP can be considered. Using the THERP's nominal diagnosis model as shown in Fig. 10.18, HEP for recirculation is obtained as 1.0e-3.

The cue for cooldown action comes not as an alarm rather a step in procedure that has to be determined. Considering its complexity, the upper curve in THERP is used, thus HEP for cooldown action is obtained as 1.0e-2.

The SPAR-H HRA Method

Idaho National Laboratory developed the standardized plant analysis risk human reliability analysis (SPAR-H) to support development of plant-specific PRA models of NPPs for the US NRC [29]. As mentioned in the NUREG report, this method is straight forward, easy to apply, and simple HRA method intended mainly for review of plant PSAs. When more detailed HRAs are necessary, the report suggests the HRA method ATHENA [30].

In SPAR-H method, the probability is decomposed into contributions from diagnosis and action (execution) failures. This method accounts for the context associated with human failure events by using performance shaping factors to adjust base probability. The dependency is accounted by adjusting base-case HEPs using decision trees and Swain weighing factors, which is a THERP-based numerical impact. To account for uncertainty, this method uses a beta distribution.

The method uses base HEP values for diagnosis and action as 1.0e-2 and 1.0e-3 respectively. An essential element of the method is worksheets, consists of 2 sets of worksheets (full power and low power/shutdown). In each set, there are worksheets for diagnosis, action, and dependency condition table. The multiplicative factors which characterize PSFs are defined in eight categories, namely, available time, stressors, complexity, experience/training, procedures, ergonomics/human machine interface, fitness for duty, and work processes. In each category, the analyst has to choose one of available PSF levels, which gives a multiplier. For example, there are four options for PSF category stress, namely, extreme, high, nominal, insufficient information; the multipliers are 5, 2, 1, and 1 respectively. After evaluating each PSF, diagnosis or action failure probability is calculated by the product of base probability and multiplicative factors:

Diagnosis failure probability = 1.0e-2 × time × stressors × complexity × experience × procedures × ergonomics or human machine interface × fitness for duty × work processes

In case of action failure probability, as mentioned earlier, the base failure probability is 1.0e-3. The formulation is same as diagnosis failure probability except base failure probability value. Since highly negative situations (assignment of larger values for several PSF factors) results in a numerical value larger than 1, an adjustment factor is used.

Comparison of HRA methods and tools

There are many HRA methods available in the literature. Besides THERP and SPAR-H, other methods include accident sequence evaluation program HRA procedure (ASEP), human error assessment and reduction technique (HEART), human cognitive reliability model (HCR), absolute probability judgment (APJ), success likelihood index method (SLIM), a technique for human event analysis (ATHENA), etc. The results from these methods differ considerably as the results depend on applicability of the method to given situation, analyst, and available data. Comparison of merits and demerits of these methods and tools is beyond the scope of this book. Interested reader may refer to specialized books on HRA for detailed comparison [23, 26]. To improve the consistency and capability of HRAs, a software tool the EPRI HRA calculator [31] was designed to facilitate a standardized approach to HRA. This tool uses different methods for various types of events; for example, user can select ASEP or THERP for pre-initiator human failure events, HCR or SPAR-H for cognitive actions, and THERP for execution.

Recently, an international empirical study was performed to validate the HRA methods and their predictions with empirical results obtained from a full-scope simulator (HAMMLAB). The NUREG/CR-6883 report gives results and discussions of the study [32] in detail. Fourteen crews addressed fifteen human failure events in the simulator. Thirteen analysis teams were involved in performing fourteen HRA analyses. The results provide clear evidence of method limitations and indicate specific ways to improve individual methods. The report clearly states ‘No method showed consistently conservative or optimistic tendencies in the HEPs obtained in this study’. All methods were found to have limitations in qualitative analysis and also the interface with quantitative models. To address the issue of variability in HRA results, a hybrid method called the integrated decision-tree human event analysis system (IDHEAS) is being pursued by USNRC and EPRI [33, 34].

References

1. Kaplan S, Garrick BJ (1981) On the quantitative definition of risk. Risk Anal 1:11–37
2. NASA (2002) Probabilistic risk assessment—procedures guide for NASA managers and practitioners. Version 1.1, NASA report
3. NASA (2011) Probabilistic risk assessment procedures guide for NASA managers and practitioners, NASA/SP-2011-3421
4. IAEA (1992) Procedure for conducting probabilistic safety assessment of nuclear power plants (level 1). Safety Series No. 50-P-4, International Atomic Energy Agency, Vienna
5. IAEA (2010) Development and application of level 1 probabilistic safety assessment for nuclear power plants, IAEA Safety Standards Series No. SSG-3
6. USNRC (1975) Reactor safety study. WASH-1400, NUREG-75/014, United States Nuclear Regulatory Commission
7. American Society of Mechanical Engineers, Standard for probabilistic risk assessment for nuclear power plant applications, ASME-RA-2002
8. AERB (2002) Probabilistic safety assessment guidelines. AERB Safety Guide, AERB, Mumbai
9. Vose D (2000) Risk analysis-a quantitative guide. Wiley, New York

10. Bedford T, Cooke R (2001) Probabilistic risk analysis: foundations and methods. Cambridge University Press, London
11. Fullwood RR (2000) Probabilistic safety assessment in the chemical and nuclear industries. Butterworth, Heinemann
12. Stewart MG (1997) Probabilistic risk assessment of engineering system. Chapman & Hall Publishers
13. Borgonovo E, Apostolakis GE (2001) A new importance measure for risk-informed decision making. Reliab Eng Syst Saf 72:193–212
14. van der Borst M, Schoonakker H (2001) An overview of PSA importance measures. Reliab Eng Syst Saf 72:241–245
15. Mosleh A et al (1988) Procedures for treating common cause failures in safety and reliability studies. U.S. Nuclear Regulatory Commission and Electric Power Research Institute, NUREG/CR-4780, and EPRI NP-5613, Volumes 1 and 2
16. USNRC (1993) Procedure for analysis of common-cause failures in probabilistic safety analysis. NUREG/CR-5801 (SAND91-7087)
17. Mosleh A et al (1998) Guidelines on modeling common-cause failures in probabilistic risk assessment, NUREG/CR-5485
18. USNRC (2007) Common-cause failure database and analysis system: event data collection, Classification, and coding, NUREG/CR-6268
19. Fleming KN (1975) A reliability model for common mode failure in redundant safety systems. General Atomic Report GA-A13284
20. Fleming KN, Kalinowski AM (1983) An extension of the beta factor method to systems with high level of redundancy. Pickard, Lowe and Garric, Inc., PLG-0289
21. Mosleh A, Siu NO (1987) A multi parameter event based common cause failure model. In: Proceeding of ninth international conference on structural mechanics in reactor technology, Lausanne, Switzerland
22. Stott JE et al (2010) Common cause failure modeling: aerospace vs. nuclear. NASA Technical Report
23. Kirwan B (1994) A guide to practical human reliability assessment. CRC Press
24. Rasmussen J (1979) On the structure of knowledge-a morphology of mental models in a man-machine context. RIS0-M-2192, RISO National Laboratory, Roskilde
25. Swain AD, Guttman HE (1983) Handbook of human reliability analysis with emphasis on nuclear power plant applications, NUREG/CR-1278. U.S. Nuclear Regulatory Commission, Washington, DC
26. Spurgin AJ (2010) Human reliability assessment. CRC Press
27. Hannaman GW, Spungin AJ (1984) Systematic human action reliability procedure (SHARP), EPRI NP-3583
28. IEEE (1997) Guide for incorporating human action reliability analysis for nuclear power generating stations, IEEE Standard 1082, IEEE 445 Hoes Lanne, Piscataway, NJ
29. Gertman D et al (2005) The SPAR-H Human Reliability Analysis Method, NUREG/CR-6883, prepared for USNRC, Washington, DC
30. Forster J et al (2007) ATHENA user's guide, final report, NUREG-1880, USNRC, Washington, DC
31. The EPRI HRA Calculator®, The Electric Power Research Institute, Inc
32. Forester J et al (2014) The international HRA empirical study, NUREG-2127. USNRC, Washington, DC

33. Hendrickson SML, Parry G, Forester J, Dang VN, Whaley A, Lewis S, Lois E, Xing J (2012) Towards an improved HRA method. In: Proceedings of the 11th international probabilistic safety assessment and management conference, 25–29 June 2012, Helsinki, Finland
34. Parry GW, Forester JA, Dang VN, Hendrickson SML, Presley M, Lois E, Xing J (2013) IDHEAS—a new approach for human reliability analysis. ANS PSA 2013 international topical meeting on probabilistic safety assessment and analysis, Columbia, SC, USA, 22–26 Sep 2013, American Nuclear Society, CD-ROM

Chapter 11
Dynamic PSA

This chapter first introduces dynamic Probabilistic Safety Assessment (PSA) emphasizing its need and gives a brief overview of the dynamic methods in the literature. Dynamic event tree method, one of main dynamic PSA approaches, is primarily focused in the chapter. The elements involved in dynamic event tree and a comparison among its implementations are presented. Application to a simple depleting tank problem explores the quantitative aspects of the method. Finally, to quantify risk in the light of uncertainties and dynamics, the practical issues and possible solutions are briefly discussed.

11.1 Introduction to Dynamic PSA

11.1.1 Need for Dynamic PSA

Probabilistic Safety Assessment (PSA) is extensively used to evaluate the risks associated with complex engineering systems like nuclear power plants, chemical and process plants, aeronautical systems, etc. The classical combination of fault tree and event tree analyses is used to develop risk models in PSA. Fault tree and event tree analyses are static and Boolean logic based approaches. Incorporating dynamic (time dependent) interactions into PSA models is difficult. Such challenges can arise due to human interactions [1, 2], digital control systems and passive components [3, 4], etc. *Increasing the realism in modeling of time dependent interactions in quantifying risk is the objective of Dynamic PSA approaches.*

In the current PSA practice, accident sequence outcomes (for event tree development) and success criteria requirements (for fault tree development) are derived based on plant simulations with thermal-hydraulic codes in nuclear industry and process dynamics codes in the chemical industry. Such calculations must account the dynamic interactions among the physical process, safety system and operator responses. When stochastic variabilities in these responses and their impact on the scenario dynamics and outcomes are considered, defining success criteria and event tree models may become cumbersome and complex [5]. In such a case, *Dynamic*

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_11

PSA framework can provide computationally efficient framework for integrated simulations.

The quantification of risk in PSA framework normally requires grouping of sequences and defining bounding success criteria. Bounding assumptions are essential in this process of developing accident sequence model. Although the bounding helps to simplify the accident sequence model to get a compact tree for practical use, in certain cases it may inadvertently introduce either unnecessary conservatism or even underestimation of risk estimate in some other cases. One way in which underestimation may occur is if the most challenging conditions for one safety function correspond to non-limiting conditions for other safety functions due to accident dynamics and the success criteria is identified without accounting such conditions. In contrast, *the Dynamic PSA does not require sequence grouping and success criteria analysis, thus bypassing the issues associated with them in risk quantification* [6].

In addition to accident dynamics, uncertainties that are present in model parameters, can significantly impact the simulated accident dynamics and ultimately the risk estimate; for example, uncertainty in model parameter of the physical process or operator action can change the outcome of an accident sequence affecting the final risk estimate. *Dynamic PSA provides a framework to consider epistemic and aleatory uncertainties in physical process and safety system responses* [7, 8].

11.1.2 Dynamic Methods for Risk Assessment

The term Dynamic PSA/PRA has been used with several different meanings. It is clear that accounting for time variations is an essential feature of a dynamic PRA. Mosleh [2] classified the time dependent effects in reference to the time duration of typical accident conditions. The dynamic effects with a long time constant can be addressed within the existing framework of PSA; for example, aging, plant configuration changes, environmental variations, and organizational changes. Treatment of dynamic effects with short time constants is not possible with conventional PSA. Some of the examples include time dependency of physical, stochastic processes, and operator response time. Mosleh [2] defines Dynamic PSA as "A PRA that models accident sequences and calculates their probabilities through integrated, interactive, time dependent, probabilistic and deterministic models of (1) plant systems, (2) thermal-hydraulic processes, and (3) operator behavior in accident conditions".

As per NUREG/CR-6942 [9], dynamic interactions can be classified into two types. Type I Interactions—Dynamic interactions between physical process variables (e.g., temperature, pressure, etc.) and the I&C systems that monitor and manage the Process—dynamic interactions between the different systems (process/safety/control). The methods focused on type I interactions are classified into continuous time (e.g. continuous event tree, continuous cell to cell mapping

Table 11.1 Summary of dynamic methods in PSA

Method	Key features	Remarks
Monte Carlo Simulation	Simulates the actual process and random behavior	Intensive computations
Continuous Event Trees	Models event dependencies in a single integral equation	Need for problem specific algorithms
Discrete Dynamic Event Trees	Simulates in the time discretization space	The most widely used
Dynamic Flow graph methodology	Digraph based technique	Pre-requirement of physical process response
Markov Modeling/Petri Nets	State space diagrams and analytical solutions	Difficult to solve large scale problems
Dynamic Fault Trees	Dynamic Gates (PAND, SEQ, etc.)	Pre-requirement of physical process response

technique), discrete time (dynamic event tree, cell to cell mapping technique), and methods with visual interface (petrinets, dynamic flow graph methodology, event sequence diagram, and GO-FLOW). Type II Interactions are the dynamic interactions within I&C system itself due to the presence of software/firmware (e.g., multi-tasking and multiplexing)—dynamic interaction between the components with in a system. For example, markov methodology, Dynamic Flow Graph Methodology, Dynamic Fault Trees, Petrinets, Bayesian methods, etc. are methods focused on type II interactions.

Table 11.1 gives a summary of dynamic methods in PSA. The Continuous Event Tree method models dynamic interactions by obtaining a set of partial differential equations under a Markovian assumption from the Chapman-Kolmogorov equation and the integral form is equivalent to an event tree where branching occurs continuously [10–12]. Application to large scale practical problems is difficult because of the need for problem specific algorithms [13]. The most widely used approach is the dynamic event tree method. The popularity of this method is due to its ease for practical implementation in solving large scale problems (complex systems like NPPs) and also computational advantages. The method Analog Monte Carlo simulation [14–18] estimates the risk measures from a randomly chosen sample of sequences. Monte Carlo method is insensitive to the size of the application, complexity, and modeling assumptions. As failure region depends on rare events, exhaustive sequence exploring (like DETs) is difficult and needs intensive computations than any other method.

Dynamic Flow graph methodology [19, 20] provides a system modeling environment that has some of the advantages of the full physical models used in simulation approaches, but that can be analyzed both deductively and inductively. This is achieved by using a multi valued and time dependent discrete logic modeling paradigm. The applications demonstrated its capability to integrate its results in existing PSA framework. The method needs physical process response as a pre-requirement before analysis.

The behavior of components (basic events) of complex systems and their interactions such as sequence- and functional-dependent failures, spares and dynamic redundancy management, and priority of failure events cannot be adequately captured by traditional FTs. Dynamic fault tree (DFT) extend traditional FT by defining additional gates called dynamic gates to model time varying dependencies between basic events. The dynamic gates were solved by Markov models [21], Bayesian Belief Networks [22] time dependent Boolean logic [23], and Monte Carlo simulation [24] approaches. DFT is limited to addressing type II interactions.

Further, interested readers may refer Labeau et al. [4] and Aldemir [13], which gave a detailed overview of some of these methods. Comparison of these methods is beyond the scope of the chapter. Next sections of this chapter are focused on DET method.

11.2 Dynamic Event Tree Analysis

11.2.1 Event Tree versus Dynamic Event Tree

Event trees are used to determine the sequences of system failures that can lead to undesired consequences. Event trees are graphical models that order and reflect events according to the requirements for the mitigation of initiating events. The order of events is usually preset by the analyst in the event trees. On the other hand, A DET is an ET in which branching is allowed to occur at different points in time. A DET simulation framework integrates both deterministic and probabilistic models. In response to an accident in the plant, several safety systems and crew actions are demanded by the process/plant. The branches represent the possible states of the safety systems or/and crew. The sequences and plant parameters with respect to time are obtained from the DET simulations.

11.2.2 DET Approach—Steps Involved

In a DET, the accident transient is simulated in deterministic dynamic model (physical) and the process parameter values are obtained from plant dynamic model with respect to time. A DET scheduler has the integrated model of the plant describing the behavior of the various elements as a set of rules. When the process parameter demands intervention of safety system or human action, one of the rule in scheduler gets fired, and branching takes place in the DET. As a result, event sequences are generated based on the rules in scheduler.

The DET simulation framework adapted from ADS implementation of DDET [2, 25–28] is shown in Fig. 11.1. Deterministic model has plant physics and stochastic model has control panel, safety system, and crew models. Figure 11.1b

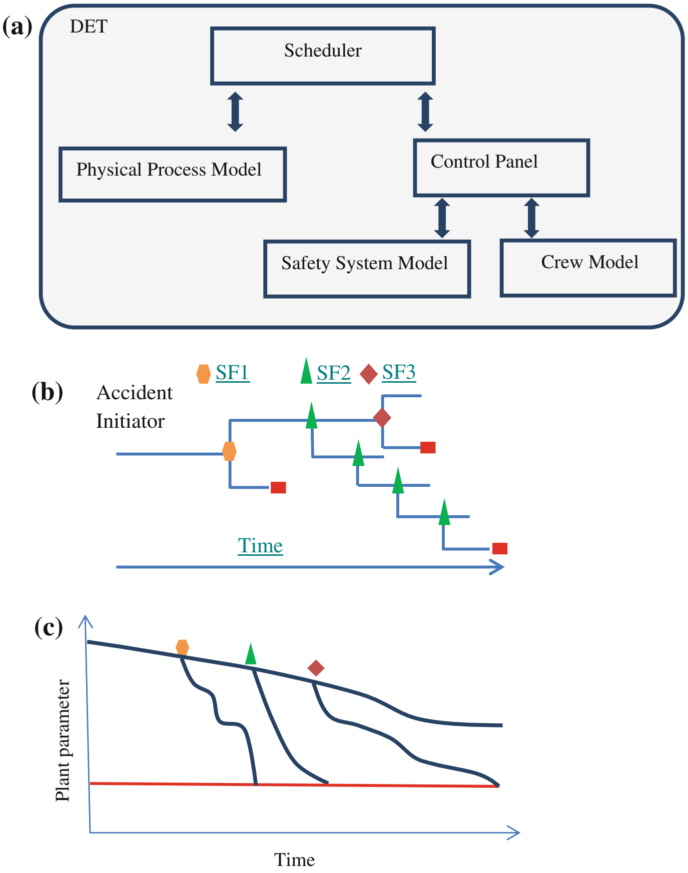


Fig. 11.1 Dynamic Event Tree framework

shows a typical DET generated from simulation and the profiles of process parameters is shown in Fig. 11.1c.

The elements required for DET implementation are shown with a flow chart in Fig. 11.2. The prerequisite for DET analysis is preparing the DET models, where the following tasks are involved. The variables (physical process and safety systems) of system or plant to be analyzed are identified. The DET scheduler rules are developed based on the plant behavior and accident dynamics involved. The different states (discrete or continuous) of safety system responses and their likelihood are also obtained. The physical model, where time dependent relationship between variables of plant is present, is an essential input.

The first step in DET analysis is initialization of the variables and initiating the accident. Physical module is a system code (e.g. RELAP or TRACE in case of nuclear plant simulations) takes the initial conditions (say at a time t) and gives the evolution of physical variables after a time interval Δt. The DET scheduler gets this update of

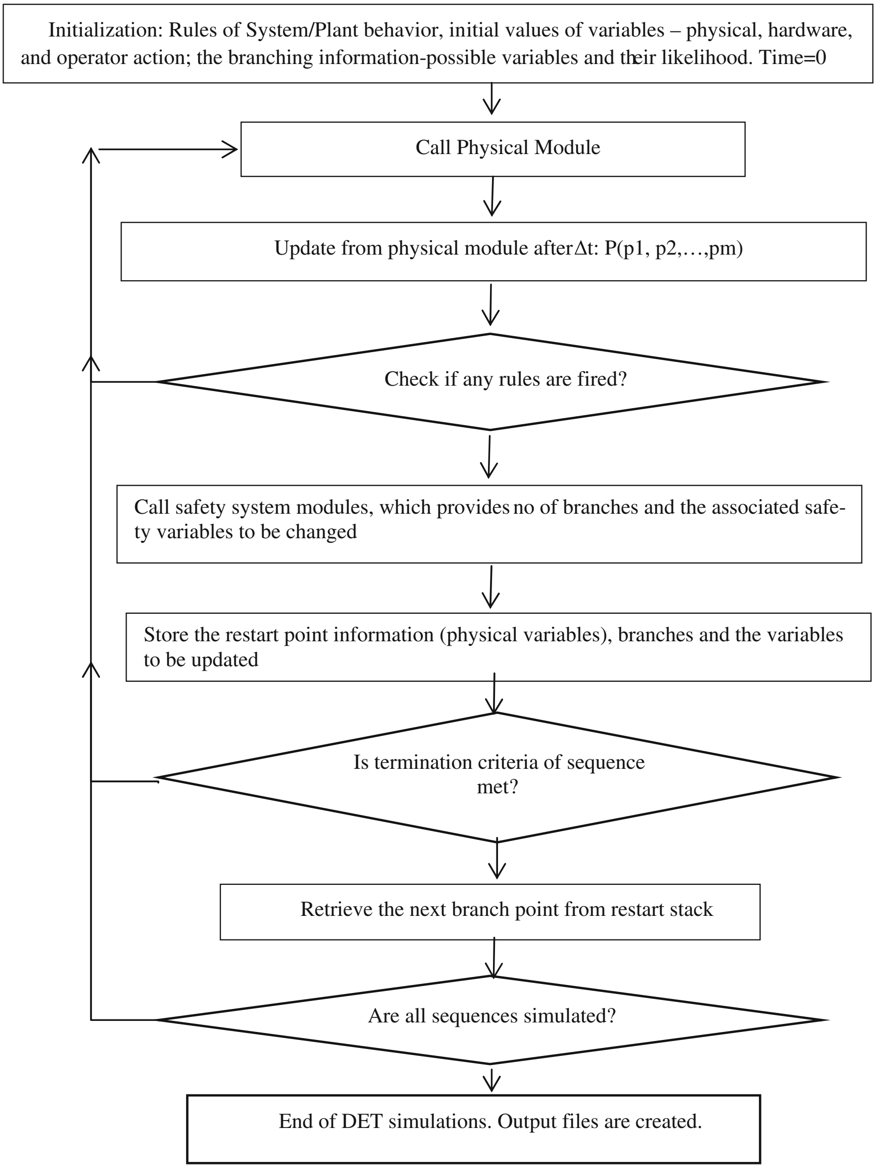

Initialization: Rules of System/Plant behavior, initial values of variables – physical, hardware, and operator action; the branching information-possible variables and their likelihood. Time=0
Call Physical Module
Update from physical module after Δt: P(p1, p2,…,pm)
Check if any rules are fired?
Call safety system modules, which provides no of branches and the associated safety variables to be changed
Store the restart point information (physical variables), branches and the variables to be updated
Is termination criteria of sequence met?
Retrieve the next branch point from restart stack
Are all sequences simulated?
End of DET simulations. Output files are created.

Fig. 11.2 Flow chart showing the required elements for DET implementation

physical variables. The scheduler rules are scanned and checked if any of these rules are fired or not. If none of the rules are fired, the simulation goes back to physical module for simulating the next time step. If any one of the rules is fired, it indicates the need for branching. Depending on the rule, which indicates the need for response of safety equipment or operator action, safety system module or operator response module is called. These modules provide the safety system response in the form of number of branches and associated safety variables to be changed. The information about each branch to be simulated is stored as a restart point, which also includes the history of the current sequence and conditions at the branching time.

All the branches except the first branch are kept in waiting in a queue until the end of current sequence. After storing the restart point and its branches, the first branch is continued to be simulated. Before simulating the new branch, a termination criteria is checked, for instance the likelihood of the sequence, total mission time of the sequence, etc. The simulation continues in the current sequence only if the criterion is not met. Otherwise, the next sequence waiting in the queue will be considered. Each sequence may have multiple restart (branching) points due to demand of several safety functions. After the end of current sequence, simulation switches to next sequence. The next sequence begins from the restart point, whose information is retrieved from the queue in restart stack. It is important to note that the restart stack is stored such that last branching point is on the top of the queue, in other words, the latest is simulated first. This ensures the simulation of sequence is as per the sequence number in resulting DET. The simulation continues until all branches are simulated or in other words until the restart stack is empty. After simulating all the sequences, the sequences, their likelihoods, the profiles of physical and safety variables in each of the sequences are analyzed.

11.2.3 DET Implementation—Comparison Among Tools

Several DET implementation tools can be seen in the literature. DYLAM (Dynamic Logical and Analytical Methodology) was first proposed approach for DET by JRC, Italy in 1986 [29–31]. DETAM (Dynamic Event Tree Analysis Method)—By generalizing DYLAM, Siu proposed DETAM for accident scenario analysis in NPP [1, 32]. ADS (Accident Dynamic Simulator)—Mosleh and his team developed a simulation tool for large scale dynamic accident sequence analysis [2, 25, 26]. It is the first tool to integrate a general thermal hydraulics code in the simulator. MCDET, ADAPT and SCAIS are some of more recent DET tools.

Table 11.2 gives a summary of comparison between four DET tools, viz., ADS, MCDET, ADAPT, and SCAIS. DET tool ADS incorporates discretization approach in treating continuous safety functions. This tool was applied to the accident scenario whose initiating event is steam generator tube rupture in a NPP [2]. This tool was coupled with thermal-hydraulics codes RELAP [26], TRACE [33], and MELCOR. The main focus of ADS has been on level-1 PSA with emphasis on operator modeling and its support in human reliability analysis [26]. ADS coupled with TRACE was applied to MLOCA scenario of Zion in success criteria analysis and DET informed PSA [34] and DET quantification of MLOCA risk [35]. Some work was also done in the post processing of analysis [36, 37]. Treating epistemic variables and direct quantification of risk are under investigation [38]. The DET tool SCAIS has been developed in Spain [39, 40]. This tool is based on integrated safety assessment

Table 11.2 Comparison of DET Tools

Tool	Features	"Unique" feature	Desirable features
ADS	• Level 1 PSA	• Sophisticated operator modeling	• Epistemic uncertainty treatment
	• RELAP/TRACE/MELCOR	• Post processing analysis	
MCDET	• Level 1 PSA	• Continuous aleatory variables (MC)	• Detailed treatment of operator actions
	• Epistemic & Aleatory variables		
	• MELCOR		
ADAPT	• Level 2 PSA	• Passive components handling	• Operator modeling
	• Epistemic & aleatory variable		
	• Parallel processing		
SCAIS	• Intended for regulatory decision support	• FTs integrated into DET	• Epistemic uncertainty treatment
	• Operator modeling	• BDD for final cut set analysis	
	• Parallel processing		

methodology using discrete DET approach. This tool is intended as a regulatory tool to evaluate safety criteria and assumptions of PSA. This tool was coupled with TH code MAAP4. The unique feature of this tool as claimed by the developers is fault trees being integrated into DET and binary decision diagrams for final cut set analysis. A tool aiming at simulating events related to human actions and able to interact with a plant simulation model, simulator of procedures (SIMPROC), has been recently coupled with SCAIS [41]. This tool also implemented distributed computing. Applications to NPP scenarios with this tool were on LOCA scenarios. However, the treatment of epistemic uncertainties is not addressed yet.

ADAPT tool has been developed by Ohio State University and Sandia National Laboratories, USA [8, 42, 43]. This tool is primarily focused on level-2 PSA, analysis of accident progression event trees. The TH code MELCOR was coupled to ADAPT. This tool was applied to evaluate containment response for station black out with auxiliary feed water system failure. The unique feature of this tool is handling passive components and treating epistemic variables. This tool has relatively better sophisticated computational infrastructure, which allows for flexibility in linking with different simulation codes, parallel processing, online scenario management, and user-friendly graphical capabilities [43]. Direct quantification of risk considering dependencies and also considering detailed operator modeling can be some of desirable features of the tool.

MCDET tool has been developed at GRS, Germany [7, 44–46]. MCDET is different from other DET tools in treating continuous safety functions; for example,

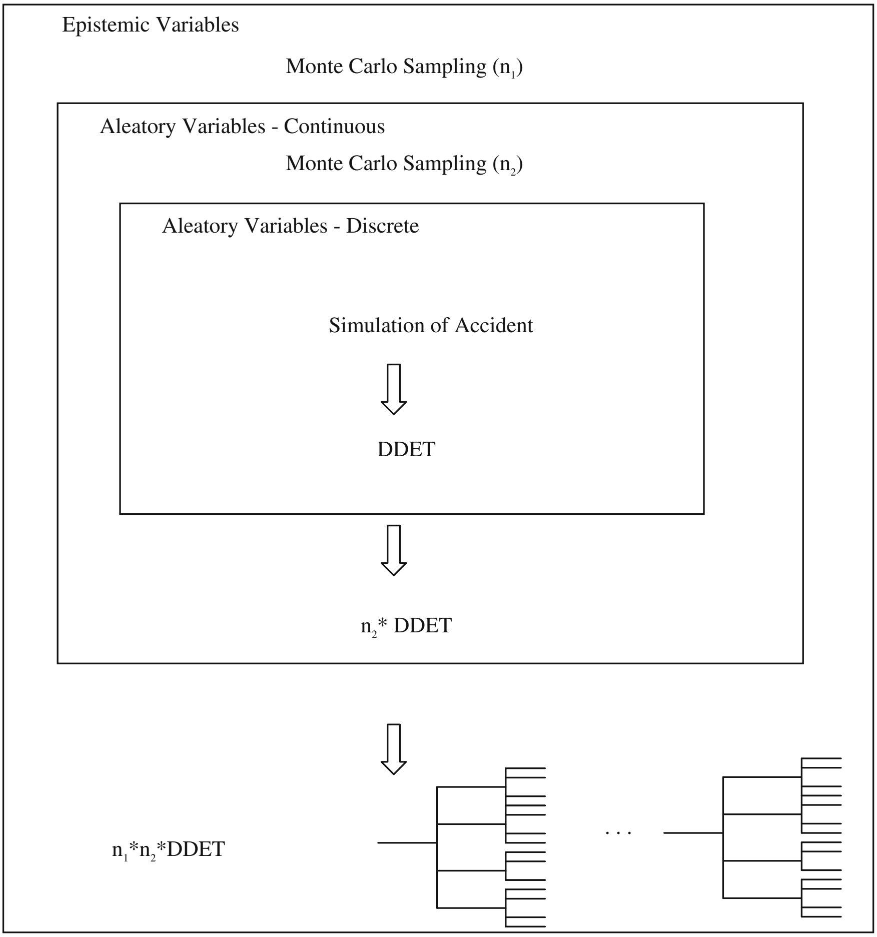

Epistemic Variables
Monte Carlo Sampling (n_1)
Aleatory Variables - Continuous
Monte Carlo Sampling (n_2)
Aleatory Variables - Discrete
Simulation of Accident
DDET
n_2* DDET
n_1*n_2*DDET
. . .

Fig. 11.3 MCDET approach—steps involved

discrete DET tools discretize continuous aleatory variables. In MCDET methodology as shown in Fig. 11.3, the continuous aleatory variables are sampled with Monte Carlo simulation while discrete aleatory variables are treated the same as Discrete DET approach. Approximate epistemic uncertainty quantification was also proposed for applications of large scale problems, where the performance of two-loop Monte Carlo sampling would be impractical [47]. This tool coupled with MELCOR was applied to station blackout scenario. Quantification of risk measure directly from DET tool is also a desirable feature in this tool.

Recent DET implementations include Genetic Algorithm based approach [48] for intelligent and adaptive resolution in the exploration of the plant scenario space and the DET tool RAVEN [49] coupled with the newly developed TH code RELAP-7.

11.3 Example—Depleting Tank

11.3.1 Description on Depleting Tank Problem

A tank problem was derived by [38] from a similar one defined for control system failures and dynamic reliability [50]; an operator response was introduced to consider stochastic timing. Detailed analysis of the results including epistemic treatment can be found in [38]. Here the focus is on aleatory results.

A cylindrical tank of diameter 'D' with an initial water level of $\mathrm{H_i}$ begins to deplete due to a spurious signal that opens a valve, which has a diameter of the leak as 'd' (Fig. 11.4). Operator has to close the valve before the tank level reaches a critical level $\mathrm{H_f}$. The objective is to estimate the likelihood of the tank reaching a critical level considering aleatory uncertainties in the scenario. Time taken for a depleting tank to reach a level $\mathrm{H_f}$ based on Bernouli's equation is [51, 52]:

$$TW = \frac{A}{aC}\left(\sqrt{H_i} - \sqrt{H_f}\right)\sqrt{\frac{2}{g}} \tag{11.1}$$

Nomenclature

TW	Time (time window-OA)
A	area of tank
a	area of the hole
$\mathrm{H_i}$	Initial tank level
$\mathrm{H_f}$	Critical tank level
C	discharge coefficient
g	gravitational force
$\mathrm{T_{OA}}$	Response time of operator
P(V)	Valve failure prob

The tank depletes to critical level when the operator does not act before a time window, which is the time taken for the tank to reach the critical level. Operator has

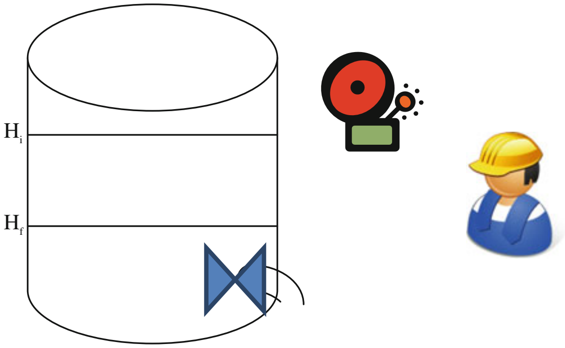


Fig. 11.4 A depleting tank with an initial level $\mathrm{H_i}$ and a critical level $\mathrm{H_f}$

Table 11.3 Aleatory uncertainties in the model

	Aleatory variables
Safety system models	Demand failure probability of Valve (2e-4)
	Response time of OA—g(t_{OA})
	Lognormal (median: 360 s, error factor: 2)
Physical process models	Initial tank level Hi—Normal (10, 0.3) m
Other data used in calculations	Discharge coefficient—0.85
	Diameter of the tank—2 m
	Critical tank level—2 m
	Diameter of the hole—0.05 m
	g—9.8 m/s^2

a cue from an alarm, which is due to fall of level, and in response operator needs to close the valve. The valve needs to function on demand to stop the leak. The failure probability (FP) depends on the failure probabilities of alarm, human error, and valve. Human error probability (HEP) depends on the available time (Eq. 11.1), which depends on initial level and other constants. This is the time dependent (dynamic) element in the problem.

Table 11.3 gives the summary of aleatory uncertainties assumed in the analysis. In physical process model, tank level is an aleatory variable. In safety system models, demand failure probabilities of valve and alarm, and operator response time are aleatory variables.

11.3.2 Analytical Solution

Tank failure probability FP can be expressed as a function of failure probabilities of alarm, valve, and human response, which is shown in Eq. (11.2).

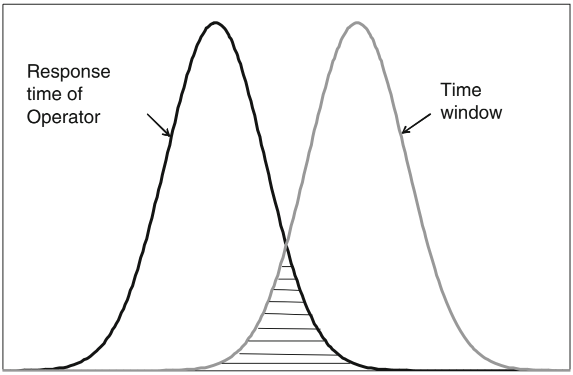
$$FP = f(P(A), HEP, P(V)) \tag{11.2}$$

The failure probability of alarm and valve are independent of physical parameters or time dependent elements. But the HEP is the probability of the aleatory variable response time (R) exceeding another aleatory variable time window (W) or time taken for the tank level to reach the critical level (see Fig. 11.5). The time window is an aleatory variable as it is a function of initial level, which is an aleatory variable. HEP is shown in Eq. (11.3), which can be simplified using reliability theory on load-resistance or stress-strength concept [53] as shown below:

$$HEP = P(R > W) \tag{11.3}$$

Probability of response time falling in a small interval 'dr' around r is

Fig. 11.5 Operator response time and time window



$$P\left(r - \frac{dr}{2} \le R \le r + \frac{dr}{2}\right) = f_R(r) \cdot dr$$

Differential HEP is the probability of response time falling in the interval ‘dr’ around r and the time window being smaller than the value ‘r’ simultaneously is

$$d(HEP) = f_R(r)dr \int_0^r f_W(w)dw$$

The HEP is given as the probability of time window ‘W’ being smaller than the response time ‘R’ for all possible values of R.

$$HEP = \int_0^\infty f_R(r)dr \int_0^r f_W(w)dw = \int_0^\infty f_R(r)F_W(r)dr \tag{11.4}$$

PDF of response time is known, but PDF of time window is not known; as time window is a function of core level whose pdf is known, we can derive its PDF using transformation of random variables [54] as shown below:

Equation (11.1) can be simplified to

$$W = \frac{A}{aC}\left(\sqrt{H_i} - \sqrt{H_f}\right)\sqrt{\frac{2}{g}} = k_1\sqrt{H} - k_2 \tag{11.5}$$

$$where\, k_1 = \frac{A}{aC}\sqrt{\frac{2}{g}}\; and\;\, k_2 = \sqrt{H_f} \times k_1$$

As mentioned in Table 11.2, H_i is a normal distribution, we have to find probability density or cumulative distribution function (CDF) of ‘W’. The CDF of W can be expressed as

$$F_W(w) = P(W \leq w) \tag{11.6}$$

Equation (11.5) can be rearranged to derive H as a function of w:

$$H = \left(\frac{w + k_2}{k_1}\right)^2$$

Substituting Eq. (11.5) in Eq. (11.6) and expanding further:

$$F_W(w) = P\left(k_1\sqrt{H} - k_2 \leq w\right) = P\left(H \leq \left(\frac{w + k_2}{k_1}\right)^2\right) = \int_0^{\left(\frac{w+k_2}{k_1}\right)^2} f_H(h)dh$$

$$F_W(r) = \int_0^{\left(\frac{r+k_2}{k_1}\right)^2} f_H(h)dh \tag{11.7}$$

Substituting Eq. (11.7) in Eq. (11.4) gives the HEP for final calculations:

$$HEP = \int_0^{\infty} f_R(r) \int_0^{(\frac{r+k_2}{k_1})^2} f_H(h)dh \cdot dr \tag{11.8}$$

Numerical integration method can be used to solve for HEP and with the data mentioned in Table 11.3.

11.3.3 Discrete DET Solution

This section presents the application of discrete DET solution as explained in the Sect. 11.2.2 on the tank problem. The resulting DDET is shown in Fig. 11.6.

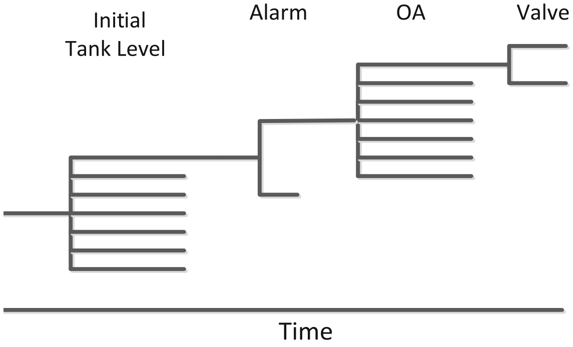


Fig. 11.6 Discrete DET of the tank problem considering aleatory uncertainties

Continuous aleatory variables, viz., tank level and operator response times are discretized. The alarm and valve have two branches either success or failure.

The initial tank level and operator response time are discretized as they are continuous random variables. The discretization strategies used in the literature [8, 28] are 3 percentiles which normally represent low, median, and high values. This strategy is ok in exploring the sequences, but overestimates in quantification. It is also important to know if the variable to be discretized is sensitive as a whole or in certain parts (e.g. upper or lower tails) of the distribution. Since the tank level is sensitive for all the values, it was discretized linearly on the whole distribution. The log discretization strategy [38] is used in case of operator response distribution on the upper tail (between 0.9 and 1.0 in cum. prob.). As a generalization of discretization approach and to improve the accuracy of the results in general with few runs, 'Log discretization approach' having 7 branches was proposed [38]. The premise of this discretization approach is based on assigning a human error probability over a range of (1e-4, 1e-3, 1e-2, 1e-1, 0.5, 0.95, 1.0); the lower values than this range would not contribute significantly compared with other risk contributors.

Five different discretization strategies (4, 5, 7, 10, and 20 Branches; the last 3 with log strategy, see Table 11.4) are considered and their results are compared with analytical result. Fig. 11.7 shows the 7 Br. log strategy, where the tail is divided into 3 branches (intervals) in log scale; the remaining 4 branches correspond to 5, 50, 90 %, and skip, which are necessary to see quick, normal, late, and never actions. Like the 7 br. log strategy, 10 and 20 br. strategies discretize cumulative probabilities between 0.9 and 1.0 in log scale into 6 and 16 branches respectively. Table 11.4 shows the discretization strategies for 4, 5, and 7 branches used in the calculations. The percentiles of response time and the branch probabilities are also shown. Figure 11.8 shows the branch percentiles and their probabilities.

Both analytical and DDET methods have been applied on the tank problem to determine the failure probability. In these calculations, aleatory uncertainties are only considered and epistemic parameters are kept at their mean values. The comparison between analytical and DDET aleatory results are shown in Table 11.5. The analytical method solved with numerical integration technique is the reference result. Several discretization strategies are compared with the reference result. DDET with 3 and 4 %tile methods that were used in the literature are found to be conservative in estimation. The former overestimates by 83.9 times and the latter depend on the percentile assigned to skip action giving different results. The sensitive to skip percentile indicates it may change from case to case. Although it is obvious that larger the number of discretization levels the better accuracy in DDET

Table 11.4 Discretization strategies for OA in DET simulations

	4 Br.	5 Br.	7 Br.
Operator response time	(5, 50, 95) tiles, skip	(5, 50, 95, 99.9) tiles, skip	(5, 50, 90, 99, 99.9, 99.99) tiles, skip
Branch probability	0.05, 0.45, 0.45, 0.05	0.05, 0.45, 0.45, 4.9e-2, 1e-3	0.05, 0.45, 0.4, 9e-2, 9e-3, 9e-4, 1e-4

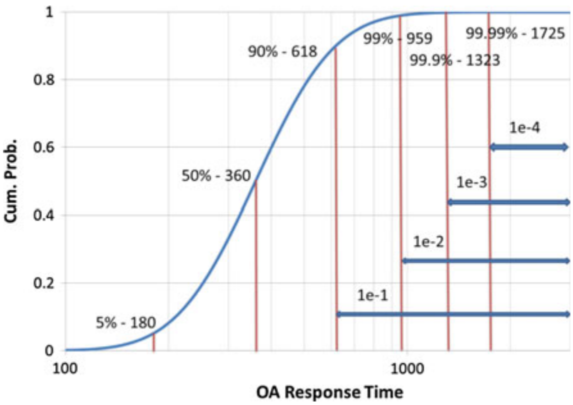


Fig. 11.7 Log discretization strategy for operator response time

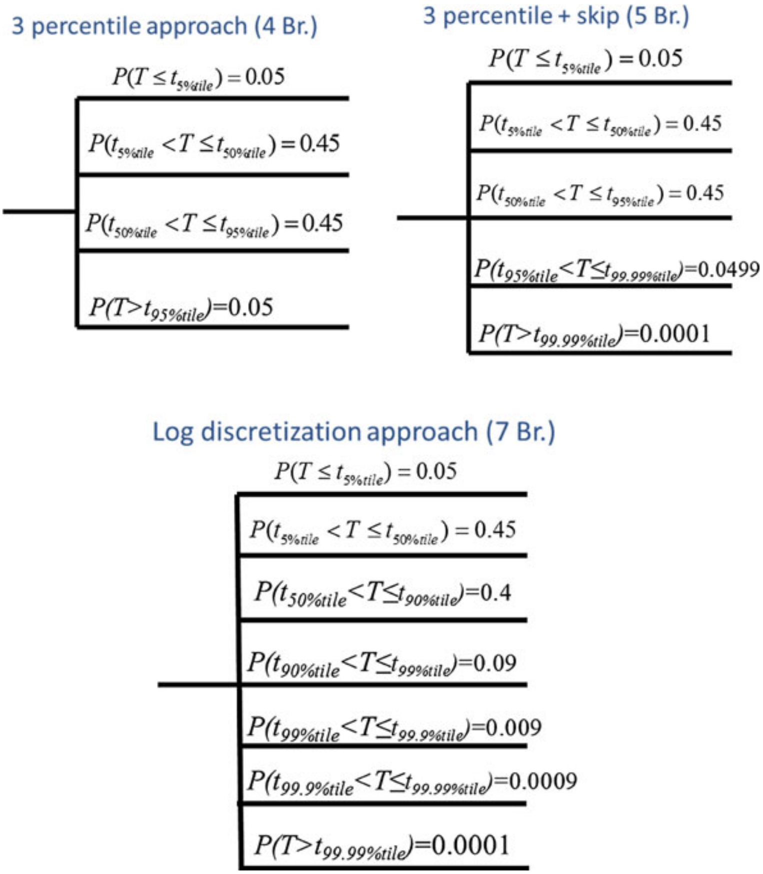

3 percentile approach (4 Br.)
$P(T \leq t_{5\%tile}) = 0.05$
$P(t_{5\%tile} < T \leq t_{50\%tile}) = 0.45$
$P(t_{50\%tile} < T \leq t_{95\%tile}) = 0.45$
$P(T > t_{95\%tile}) = 0.05$
3 percentile + skip (5 Br.)
$P(T \leq t_{5\%tile}) = 0.05$
$P(t_{5\%tile} < T \leq t_{50\%tile}) = 0.45$
$P(t_{50\%tile} < T \leq t_{95\%tile}) = 0.45$
$P(t_{95\%tile} < T \leq t_{99.99\%tile}) = 0.0499$
$P(T > t_{99.99\%tile}) = 0.0001$
Log discretization approach (7 Br.)
$P(T \leq t_{5\%tile}) = 0.05$
$P(t_{5\%tile} < T \leq t_{50\%tile}) = 0.45$
$P(t_{50\%tile} < T \leq t_{90\%tile}) = 0.4$
$P(t_{90\%tile} < T \leq t_{99\%tile}) = 0.09$
$P(t_{99\%tile} < T \leq t_{99.9\%tile}) = 0.009$
$P(t_{99.9\%tile} < T \leq t_{99.99\%tile}) = 0.0009$
$P(T > t_{99.99\%tile}) = 0.0001$

Fig. 11.8 Different DET discretization strategies

Table 11.5 Comparison of failure probability without considering epistemic uncertainties

	Analytical	DDET-discretization						
	Numerical Integration	4 Br.	5 Br.			7 Br.	10 Br.	20 Br.
			99 % tile[a]	99.9 % tile	99.99 % tile[a]			
Failure probability	5.98e-4	5.02e-2	1.02e-2	1.19e-3	5.02e-2	1.19e-3	7.83e-4	6.43e-4
Overestimation		83.9	17	1.98	83.9	1.98	1.31	1.07

[a]Sensitive cases for 5 branch discretization

calculations, log discretization strategy is found to give satisfactory results with few number of branches; for example, the percentage errors are 98 and 31 % for 7 and 10 log branches respectively and the 20 branch (log) case converged with the reference result.

11.4 DET Quantification of Risk—Practical Issues and Possible Solutions

11.4.1 Challenges in Direct Quantification of Risk with DET

Dynamic interactions among physical process, safety systems, and operator actions can be accounted in risk assessment with DET informed PSA, by means of additional sequences and appropriate success criteria definitions. Besides the accident dynamics, bounding issues that are inevitable with classical PSA approaches can be addressed with DET quantification. Nevertheless, direct quantification of risk with DET has a few challenges in practical implementation, which include dealing many sequences, treating dependencies by coupling Boolean algorithms with dynamic simulations, and better discretization approaches for treating overestimation of continuous variables. The first two issues depend on their implementation in the specific DET tool and available computational resources. The accuracy of discretization approach depends on number of discretization levels of continuous variables. It is also important to know if the variable to be discretized is sensitive as a whole or in certain parts (e.g. upper or lower tails) of the distribution. A few limiting calculations are necessary to provide information to decide the important parts of the distributions. It is also worth noting that limiting calculations should consider the relation between the system responses (e.g. critical level or temperature) and the variable; for example, lower the initial level higher the risk or later the operator response higher the risk. The intervals in discretization should be represented accordingly. In tank problem discussed in previous section, the discretized intervals are represented with the lower bound in case of level variable and upper bound of response time variable. Unless the relation between a variable and system response is non-monotonic, discretization approaches will not underestimate the risk as the intervals are represented conservatively.

In case of operator response time distribution, ‘Log discretization approach’ [38] reduces conservatism in risk estimate compared to discretization strategies used in the literature.The premise of this discretization approach is based on assigning a failure probability over a range of (1e-4, 1e-3, 1e-2, 1e-1, 0.5, 0.95, 1.0) in case of 7 branch discretization approach. This log strategy with 10–20 branches fairly converges with analytical result. Caution should be exercised about trade-off between accuracy and number of levels as further increase of levels could lead explosion of sequences when the number of continuous variables is large. Another alternative is use of Monte Carlo simulation as proposed by MCDET [7] in sampling aleatory continuous variables provided it has sound convergence criteria implemented, which needs a larger number of simulations.

11.4.2 Uncertainties and Dynamics in Risk Assessment

Typical accident scenario in a NPP involves complex interactions between physical process and safety systems (safety equipment and operator response). The response of a safety system is inherently random in nature, which is often referred as aleatory uncertainty. The response of physical process can also have aleatory elements; for example, initial level, break size, break location, etc. DET analysis provides a framework to simulate the accident scenario considering the dynamic interactions, where mathematical models of physical process and safety systems are used. The limitations in assessing the parameters of these models introduce another type of uncertainty, which is often referred as epistemic uncertainty [55]; for example, demand failure probability of safety equipment, human error probabilities, and thermal hydraulic parameters. These epistemic variables can significantly impact the simulated accident dynamics and ultimately the risk estimate; for example, uncertainty in TH parameter or operator response can change the outcome of an accident sequence affecting the final risk estimate. Hence risk quantification must consider both epistemic and aleatory uncertainties in both physical and safety system models along with their dynamic interactions.

In the current PSA practice [56], first accident sequence models are developed and then solved for a cut set equation. Best estimate of risk (e.g. Core Damage Frequency for level-1 PSA) is obtained using mean PSA parameters. A Monte Carlo simulation is run to propagate epistemic uncertainty in PSA parameters. The obtained CDF distribution has already considered epistemic and aleatory uncertainties of safety system responses. But the success criteria definitions are the interface between plant simulations and the PSA models, which are normally derived with mean values of Thermal-Hydraulic (TH) parameters. The current approach does not consider propagating uncertainties in TH parameters and its impact on risk models. The two-loop Monte Carlo simulation was used in the literature for similar problems [47, 57], sampling epistemic variables in the outer loop and sampling aleatory variables in the inner loop. In the problem of accident dynamics and uncertainties in risk quantification, the inner loop dealing with aleatory variables is a DET simulation. The DET approach along with an epistemic loop can also provide a framework to consider epistemic and aleatory uncertainties [38].

References

1. Siu N (1994) Risk assessment for dynamic systems: an overview. Reliab Eng Syst Saf 43:43–73
2. Hsueh K-S, Mosleh A (1996) The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants. Reliab Eng Syst Saf 52:297–314
3. Aldemir T (1989) Quantifying set point drift effects in the failure analysis of process control systems. Reliab Eng Syst Saf 24:33–50
4. Labeau PE, Smidts C, Swaminathan S (2000) Dynamic reliability: towards an integrated platform for probabilistic risk assessment. Reliab Eng Syst Saf 68:219–254
5. Karanki DR, Kim TW, Dang VN (2015) The impact of dynamics and variabilities in the development of accident sequence models of NPP: a dynamic event tree informed approach. Reliab Eng Syst Saf 142:78–91
6. Karanki DR, Dang VN Quantification of dynamic event trees: a comparison with event trees for MLOCA scenario. In: Communication with reliability engineering and system safety
7. Kloos M, Peschke J (2006) MCDET: a probabilistic dynamics method combining Monte Carlo simulation with the discrete dynamic event tree approach. Nucl Sci Engg 153:137–156
8. Hakobyan A et al (2008) Dynamic generation of accident progression event trees. Nucl Engg Des 238:3457–3467
9. Aldemir T et al (2007) Dynamic reliability modeling of digital instrumentation and control systems for nuclear reactor probabilistic risk assessments. NUREG/CR-6942, USNRC
10. Devooght J, Smidts C (1992) Probabilistic reactor dynamics. I. The theoryof continuous event trees. Nucl Sci Eng 111:229–240
11. Devooght J, Smidts C (1992) Probabilistic reactor dynamics—III: a framework for time dependent interaction between operator and reactor during a transientinvolving human error. Nucl Sci Eng 112:101–113
12. Smidts C (1992) Probabilistic reactor dynamics IV: an example of man machineinteraction. Nucl Sci Eng 112:114–126
13. Aldemir T (2013) A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. Ann Nucl Energy 52:113–124
14. Smidts C, Devooght J (1992) Probabilistic reactor dynamics II: a Monte Carlo studyof a fast reactor transient. Nucl Sci Eng 111:241–256
15. Marseguerra M, Zio E, Devooght J, Labeau PE (1998) A concept paper on dynamic reliability via Monte Carlo simulation. Math Comput Simul 47:371–382
16. Marseguerra M, Zio E (1993) Towards dynamic PSA via Monte Carlo methods. In: Proceedings of Esrel'93, pp 415–27
17. Marseguerra M, Zio E (1993) Nonlinear Monte Carlo reliability analysis with biasing towards top event. Reliab Eng Syst Saf 40:31–42
18. Marseguerra M, Zio E (1995) The cell-to-boundary method in Monte Carlo-based dynamic PSA. Reliab Eng Syst Saf 48:199–204
19. Guarro S, Yau M, Motamed M (1996) Development of tools for safety analysis of control software in advanced reactors. NUREG/CR-6465, US Nuclear Regulatory Commission, Washington, DC

20. Guarro S, Milici A, Mulvehill R (2001) Extending the dynamic flowgraph methodology (DFM) to model human performance and team effects. NUREGCR/6710, US Nuclear Regulatory Commission, Washington, DC
21. Dugan JB, Bavuso SJ, Boyd MA (1992) Dynamic fault-tree for fault-tolerant computer systems. IEEE Trans Reliab 41(3):363–376
22. Bobbio A, Portinale L, Minichino M, Ciancamerla E (2001) Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliab Eng Syst Saf 71:249–260
23. Cepin M, Mavko B (2002) A dynamic fault tree. Reliab Eng Syst Saf 75:83–91
24. Durga Rao K, Sanyasi Rao VVS, Gopika V, Kushwaha HS, Verma AK, Srividya A (2009) Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. Reliab Eng Syst Saf 94(4):872–883 (ISSN: 0951-8320)
25. Hsueh KS, Mosleh A (1993) Dynamic accident sequence simulator for probabilistic safety assessment. In: PSA international topical meeting, conference proceedings, Florida, 26–29 Jan 1993
26. Chang YHJ, Mosleh A (2007) Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents part 1–5: dynamic probabilistic simulation of the IDAC model. RESS 92:997–1075
27. Zhu D, Mosleh A, Smidts C (2007) A framework to integrate software behavior into dynamic probabilistic risk assessment. RESS 92(12):1733–1755
28. Mercurio D (2011) Discrete Dynamic Event Tree modeling and analysis of NPP crews for safety assessment. Ph.D. Thesis, Diss. ETH No. 19321
29. Amendola A, Reina G (1984) DYLAM-1, a software package for event sequence and consequence spectrum methodology. EUR-924, CEC-JRC ISPRA, Commission of the European Communities, Ispra, Italy
30. Cacciabue PC, Amendola A, Cojazzi G (1986) Dynamic logical analytical methodology versus fault tree: the case of auxiliary feedwater system of anuclear power plant. Nucl Technol 74:195–208
31. Cojazzi G (1996) The DYLAM approach to the dynamic reliability analysis of systems. Reliab Eng Syst Saf 52:279–296
32. Acosta C, Siu N (1993) Dynamic Event Trees in accident sequence analysis: application to steam generator tube rupture. Reliab Eng Syst Saf 41:135–154
33. Durga R, Karanki, Vinh N. Dang, Tae-Wan Kim (2011) Discrete Dynamic Event Tree analysis of MLOCA using ADS-TRACE. In: ANS PSA 2011 international topical meeting on probabilistic safety assessment and analysis, Wilmington, NC, 13–17 March 2011. On CD-ROM, American Nuclear Society, LaGrange Park
34. Karanki DR, Dang VN, Kim TW (2012) The impact of dynamics on the MLOCA accident model—an application of Dynamic Event Trees. In: Proceedings of 11th probabilistic safety assessment and management/European safety and reliability 2012 (PSAM11/ESREL2012), Helsinki, Finland, 25–29 June 2012, CD-ROM
35. Karanki DR, Dang VN (2013) Quantified Dynamic Event Trees Vs PSA—a comparison for MLOCA risk. In: ANS PSA 2013 international topical meeting on probabilistic safety assessment and analysis, Columbia, SC, USA, 22–26 Sept 2013. American Nuclear Society, CD-ROM
36. Mercurio D, Podofillini L, Zio E, Dang VN (2008) Identification and classification of Dynamic Event Tree scenarios via possibilistic clustering: application to a steam generator tube rupture event, Accident Analysis and Prevention
37. Podofillini L, Zio E, Mercurio D, Dang VN (2010) Dynamic safety assessment: scenario identification via a possibilistic clustering approach. Reliab Eng Syst Saf 95:534–549
38. Karanki DR, Dang VN, MacMillan MT (2014) Uncertainty progagation in Dynamic Event Trees—Initial results for a modified tank problem, PSAM 12, Hawaii, USA, 22–27 June 2014. CD-ROM

39. R. Munoz, Minguez E, Melendez E, Izquierdo JM, Sanchez-Perea M (1999) DENDROS: a second generation scheduler for Dynamic Event Trees. In: Mathematics and computation, reactor physics and environmental analysis in nuclear applications, conference proceedings, Madrid, Spain, 1999
40. Izquierdo JM et al (2009) SCAIS (Simulation Code System for Integrated Safety Assessment): current status and applications. In: Martorell et al (eds) Safety, reliability and risk analysis—ESREL 2008. Taylor & Francis Group, London
41. Gil J et al (2011) a code for simulation of human failure events in nuclear power plants: SIMPROC. Nucl Eng Des 241:1097–1107
42. Hakobyan A, Denning R, Aldemir T, Dunagan S, Kunsman D (2006) A methodology for generating dynamic accident progression event trees for level-2 PRA. In: Proceedings of PHYSOR-2006 meeting, Vancouver, CA, 10–14 Sept 2006
43. Catalyurek U et al (2010) Development of a code-agnostic computational infrastructure for the dynamic generation of accident progression event trees. Reliab Eng Syst Saf 95:278–294
44. Kloos M, Peschke J (2007) Consideration of human actions in combination with the probabilistic dynamics method MCDET, ESREL 1069–1077
45. Kloos M, Peschke J (2008) Consideration of human actions in combination with the probabilistic dynamics code MCDET. Journal of Risk and Reliability
46. Peschke J, Kloos M (2008) Impact of epistemic uncertainties on the probabilistic assessment of the emergency operating procedure secondary side bleed and feed, PSAM9
47. Hofer E, Kloos M, Krzykacz-Hausman B, Peschke J, Woltereck M (2002) An approximate epistemic uncertainty analysis approach in the resence of epistemic and aleatory uncertainties. Reliab Eng Syst Saf 77:229–238
48. Voroyev Y, Kudinov P (2011) Development and application of a genetic algorithm based dynamic PRA methodology to plant vulnerability search. PSA 2011. American Nuclear Society, LaGrange Park
49. Alfonsi A et al (2013) Dynamic Event Tree analysis through RAVEN, ANS PSA 2013 international topical meeting on probabilistic safety assessment and analysis, Columbia, SC, USA, 22–26 Sept 2013, American Nuclear Society, 2013, CD-ROM
50. Aldemir T (1987) Computer-assisted Markov failure modeling of process control systems, IEEE Trans Reliab R-36:133–144
51. http://www.LMNOeng.com, LMNO Engineering, Research, and Software, Ltd. 7860 Angel Ridge Rd. Athens, Ohio 45701 USA
52. Daugherty RL, Franzini JB, Finnemore EJ (1985) Fluid mechanics with engineering applications, 8 edn. McGraw-Hill Inc., New York
53. Rao SS (1992) Reliability-based design. McGraw-Hill Publishers, New York
54. http://www2.econ.iastate.edu/classes/econ671/hallam/documents/Transformations.pdf
55. Ferson S, Ginzburg LR (1996) Different methods are needed to propagate ignorance and variability. Reliab Eng Syst Saf 54(2–3):133–144
56. IAEA (1992) Procedure for conducting probabilistic safety assessment of nuclear power plants (level 1). Safety series no. 50-P-4. International Atomic Energy Agency, Vienna
57. Durag Rao K et al (2007) Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies. Reliab Eng Syst Saf 92:947–956

Chapter 12
Applications of PSA

Probabilistic safety assessment (PSA) studies not only evaluate risk but also their results are very useful in safe, economical and effective design and operation of the engineering systems. This chapter presents various practical applications of PSA. The use of PSA in evaluating surveillance test interval and in-service inspection intervals at acceptable risk and reduced cost for nuclear power plant (NPP) is discussed.

12.1 Objectives of PSA

PSA is one of the most efficient and effective tools to assist decision making for safety and risk management in nuclear power plants. As per the PSA base resource document IAEA 50 P-4 [1], it can have one or more of the following three major objectives:

1. *To assess the level of safety and compare it with explicit or implicit standards*;
   The first objective contains the element of overall adequacy, in that it is deemed desirable to compare the assessed safety related capabilities of plant against standards. These standards might be explicitly defined (fixed) criteria, as for example is the comparison is made against existing 'accepted as safe' plants and/or designs.
2. *To assess the level of safety of the plant and to identify the most effective areas for improvement*;
   The Second general objective aims at extending and widening the understanding of the important issue that affect the safety of nuclear power plant. By so doing, design or operational problem can be identified and areas for improvement or future study can be identified.
3. *To assess the level of safety to assist plant operation.*
   The Third general objective aims at providing information that can assist plant operations. For example, this may be in form of improved technical specifications, models and criteria for monitoring operational reliability, or advice for accident management.

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_12

Table 12.1 Summary of objectives of PSA

General objectives			
	1. Compare it with explicit or implicit standards	2. Identify the most effective areas for improvement	3. Assist plant operation and maintenance
Specific objectives	1.1. Comparison with target values	2.1. Identification of dominant accident sequences	3.1. Evaluation of plant technical specifications and conditions of operations
	1.2. Comparison with 'accepted' design	2.2. Identification of systems, components and human action important for safety	3.2. Prioritization of inspection/testing activities
			3.3. Evaluation of operating experience
	1.3. Comparison of 'alternative' design	2.3. Assessment of important dependences	3.4. Accident management
		2.4. Identification and evaluation of new safety issues	
		2.5. Analysis of severe accidents	
		2.6. Decisions on backfitting of generic and plant specific items	
		2.7. Design modification	
		2.8. Prioritization of regulations and safety research	

Specific objectives and corresponding uses of PSA related to all the three general objectives are summarized in Table 12.1.

12.2 PSA of Nuclear Power Plant

12.2.1 *Description of PHWR*

Pressurized Heavy Water Reactors (PHWR) are horizontal pressure tube reactors using natural uranium oxide fuel in the form of clusters. The fuel is cooled by a high pressure, high temperature circulating heavy water system called the primary heat transport (PHT) system. Heavy water is also used as moderator in a separate low-temperature, low pressure moderator system. Refueling of the reactor is carried out 'on power' by the fuel handling system. The heat from the reactor is carried away by the heavy water coolant in the PHT system and is given away to the secondary side in the steam generators (SG). The steam from SGs is fed to the turbine-generator in the conventional island for production of electricity. The nuclear island is described briefly below [2].

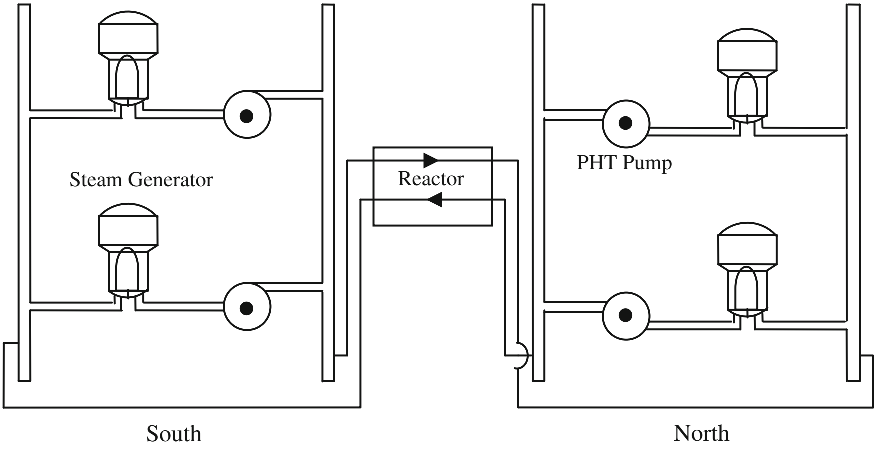


Fig. 12.1 PHWR simplified flow diagram

Reactor Process System

The PHT system circulates high pressure coolant through the fuel channels to remove the heat generated in fuel. The major components of this system are the reactor fuel channels, feeders, two reactor inlet headers, two reactor outlet headers, four pumps and interconnecting pipes and valves. The headers, steam generators and pumps are located above the reactor and are arranged in two symmetrical banks at both ends of the reactor. The headers are connected to fuel channels through individual feeder pipes. Figure 12.1 depicts simplified flow diagram of Indian PHWR.

The coolant circulation is maintained at all times during reactor operation, shutdown and maintenance. The PHT pumps are provided with flywheels to provide better flow coast down after pump trip. A separate showdown cooling system is provided to remove reactor decay heat during cold shutdown conditions. An emergency core cooling system provides adequate flow to prevent overheating of the fuel in the unlikely event of loss of coolant accident.

Reactor Protection System

The shutdown function in PHWRs is achieved by the reactor protection system which is capable of completely terminating any of the postulated reactivity transients in the most reactive state of the core. In PHWRs, the voiding introduced during large break loss of coolant accident (LOCA) gives rise to the highest rate of positive reactivity addition. The delay in actuation and the rate of insertion of negative reactivity provided by reactor protection system meets the requirements of terminating the effects of the positive reactivity transients caused by large break LOCA. These shutdown requirements are met by primary shutdown system comprising cadmium shutoff rods and a redundant, diverse secondary shutdown system comprising liquid shutoff rods.

Electrical Power System

The station service power supplies are classified on order of their level of reliability requirements. These differ in their nature and consequent security of their supply. Four classes of power are used to supply station requirements. 1. Class IV power supply: derived from grid and prone to long duration interruptions. 2. Class III power supply: Alternating current (AC) supply to connected auxiliaries available after short interruption (of the order of one to two minutes) in their normal power supplies. On-site standby generators provide an alternative power source to the Class III system. 3. Class II power supply: uninterruptible, AC supplies for essential auxiliaries, dedicated to match the redundant channels of station instrumentation and control systems. 4. Class I power supply: uninterruptible, direct current (DC) supplies for essential auxiliaries, triplicated and channelized to match the redundancy requirements of control logic and reactor safety circuits.

12.2.2 PSA of Indian NPP (PHWR Design)

PSA in the context of Nuclear Power Plants (NPPs) is associated with the models that predict the off site radiological release resulting from the potential reactor accidents. In its entirety, it comprises the following levels:

1. Identification of accident sequences and quantitative estimates of the frequency of each i.e. System Analysis
2. Radiological release to the environment associated with each class of accident sequence i.e. Containment Analysis
3. Analysis of the off-site consequences of the release i.e. Consequence Analysis

A full scope probabilistic model of a Pressurised Heavy Water Reactor (PHWR) which would be used in the safety and operational analysis of the reactor is briefly explained here. Interested reader can refer [3] for detailed information. The model would be a risk management tool to meet the following objectives.

a. Determining the core damage frequency using a set of internal Initiating Events (IEs) and external IEs like loss of off-site power
b. Identification and quantification of the dominating accident sequences, uncertainties and specific contributors to system failures
c. Identifying design and operational weaknesses
d. Supporting decisions on safety issues
e. Developing test and maintenance schedules and determining allowable outage times to assist in the establishment of criteria for Technical Specifications
f. Correlating accident sequences to release categories
g. Consequence modelling and risk estimation

The typical results of level-1 PSA contain the following information

a. Identification of dominating Initiating Events
b. Reliability analysis of various IEs and the Engineered Safety Functions (ESFs) using Fault Tree methods.
c. Identification of accident sequences leading to core damage using Event Tree methods
d. Quantification of accident sequences to obtain dominating accident sequences
e. Core Damage Frequency (CDF)
f. Uncertainty analysis and error propagation to account for the variability in component failure data, accident sequence and core damage frequency etc.

12.2.2.1 Dominating Initiating Events

Many important studies [4] have been performed on the use of PSA in case of Nuclear Power Plants (NPPs). In order to identify the IEs applicable to an Indian PHWR, it would be worthwhile to list the different design features. The PHWR is a heavy water cooled, heavy water moderated, natural uranium fuelled reactor which utilises the pressure tube concept. The pressure tubes containing the fuel run horizontally through the reactor core. Each pressure tube is isolated and insulated from the heavy water moderator by a concentric calandria tube and a gas annulus. The moderator is operated at low temperature and pressure. The reactivity control and shutdown mechanisms reside in the low pressure moderator, thus simplifying their design, construction and maintenance and eliminating virtually, the possibility of their ejection in an accident situation. In the standardised design, two fast acting, independent, diverse shutdown systems are provided and on a reactor trip, the moderator is not dumped. Thus, in case of loss of coolant accidents, the cool moderator can act as a heat sink.

The IEs can be generally classified into the following main groups

1. Decrease in reactor coolant inventory
2. Increase in reactor coolant inventory
3. Decrease in reactor coolant system flow rate
4. Decrease in heat removal by secondary system
5. Increase in heat removal by secondary system
6. Reactivity and power distribution anomalies
7. Anticipated transients without scram (ATWS)
8. Radioactivity releases from a sub-system or component
9. Others

Annex. 2 of Safety Guide SGD11 [5] gives a list of IEs generally analysed for the application of a license for LWRs in USA. A number of IEs listed below were added to account for the design differences between PHWRs and LWRs.

1. Leakage from the seal plug after refuelling (group 1)
2. Bleed valve stuck open (1)

3. Failure of a limited number of tubes in any heat exchanger other than steam generator in PHT system (1)
4. Failure of coolant channel including its end fitting (1)
5. Feed valve stuck open (2)
6. Bleed valve stuck closed (2)
7. Bleed isolation valve closed (2)
8. Flow blockage in any coolant channel assembly/any feeder (3)
9. Failure of reactor moderator flow (6)
10. Failure at any location of moderator system piping (6)
11. Failure of fuelling machine when off the reactor and full of irradiated fuel (8).

1. *Decrease in reactor coolant inventory*

- Inadvertent opening of a relief valve in PHT system.
- Feed water tube or instrument tube breakage.
- Steam generator tube/tubes failure.
- End plug fails to close after refuelling.
- PHT header and piping failure.
- Bleed valve stuck open.
- Pressure tube failure (followed by calandria tube failure releasing PHT coolant to the moderator).
- Failure of large number of tubes in any heat exchanger (other than steam generator) in PHT system (bleed cooler, gland cooler, shutdown cooler).
- Failure of end fitting of any channel assembly followed by the failure of lattice tube of end shield through which the end fitting runs.
- Failure of mechanical joint between pump cover and pump casing of main coolant pumps.
- Massive failure of a pump cover/casing of main coolant pump.

2. *Increase in reactor coolant inventory*

- Feed valve stuck open.
- Bleed valve stuck closed.
- Bleed isolation valve closed by mistake by the operator.

3. *Decrease in reactor coolant system flow rate*

- Single and multiple reactor coolant pump trips.
- Coolant pump shaft seizure.
- Coolant pump shaft breakage.
- Flow blockage in any reactor fuel channel assembly.
- Failure of all mechanical seals on PHT pump(s).

4. *Decrease in heat removal by the secondary system*

    - Boiler pressure control (BPC) system malfunction resulting in decrease in steam flow.
    - Loss of external electrical load.
    - Turbine trips
    - Inadvertent closure of main steam isolation valve.
    - Loss of condenser vacuum.
    - Class IV power failure i.e. coincident loss of station as well as grid supply.
    - Loss of normal feed flow.
    - Feed water piping break

5. *Increase in heat removal by secondary system*

    - Feed water system malfunction that results in decrease in feed water temperature.
    - Feed water system malfunction that results in an increase in feed water flow.
    - Steam Pressure Regulator (Regulating system) malfunction or failure that results in increasing steam flow.
    - Inadvertent opening of a relief valve resulting in steam flow increase.
    - Spectra of steam system piping failures inside and outside containment.

6. *Reactivity and power distribution anomalies*

    - Uncontrolled withdrawal of control rod (Reactivity control mechanism) assembly from a sub-critical or low power start up condition (assuming the most unfavourable conditions of the core and reactor coolant system).
    - Uncontrolled withdrawal of control rod assembly at a particular power (assuming the most unfavourable reactivity conditions of the core and the reactor coolant system) that yields the most severe result (low power to full power).
    - Chemical control (composition) system malfunction that results in a decrease in boron concentration in reactor coolant.
    - Fuel bundle ejection accident.
    - Failure of reactor moderator flow.
    - Failure at any location of any pipe of reactor moderator system.
    - Drop of a load on reactivity mechanisms.

7. *Anticipated transients without scram (ATWS)*

    - Inadvertent withdrawal of control rod (like 6.1 and 6.2 plus failure of trips).
    - Loss of feed water.
    - Loss of class IV power.
    - Loss of electrical load.
    - Loss of condenser vacuum.
    - Turbine trip.
    - Closure of main steam line isolation valve.

8. *Radioactivity release from a subsystem or component*

   - Tritium leakage.
   - Radioactive gas waste system leak or failure.
   - Radioactive liquid waste system leak or failure.
   - Postulated radioactive releases due to liquid tank failures.
   - Design basis fuel handling accident.
   - Accidental dropping of spent fuel cask (during transfer of fuel to reprocessing plants).
   - Failure of fuelling machine when off-reactor containing full complement of irradiated fuel.
   - Containment and associated system failure.
   - One door open of air lock or transfer chamber most critical for radioactive release from containment and seals on second door deflated (its impact, for example, when PHT system is leaking or has broken).
   - Failure to close any containment isolation device.

9. *Others*

   - Failure of instrument air.
   - Design basis fire.
   - Design basis earthquake.
   - Degraded operation of containment atmosphere cooling equipment (coupled with PHT failure).
   - Leaking containment (coupled with radioactive release from any other systems).
   - Turbine over speed protection failure.
   - Turbine break up.
   - Design basis tornado.
   - Failure of steam generator support.
   - Massive failure of station cooling water tunnel/discharge duct.

Detailed analysis of various IEs listed above has been carried out. Based on the analytical study of the causes and consequences, the following events are considered important for further studies.

1. PHT header and piping failure (group 1)
2. Steam generator tube(s) failure (1)
3. Coolant channel failure(s) (1)
4. Spectrum of steam system piping failure inside and outside containment (5)
5. Loss of normal feed flow (4)
6. Feed water pipe breaks (4)
7. Class IV failure i.e. coincident loss of station as well as grid supply (4)
8. Compressed air failure
9. Fuelling machine induced LOCAs (1)
10. Leakage from the seal plug after refuelling (1)

11. Loss of regulation (6)
12. Flow blockage in any coolant channel assembly/feeder (3)
13. Process water system failure (9)
14. Failure of moderator flow (6)

As can be inferred from the list above, the effect of internally generated missiles, man induced events (air craft crashes) and natural phenomena on the reactor and its associated systems is not considered in this analysis. Turbine trip is covered by other events (partly by class IV failure and partly by Instrumented Relief Valve (IRV) opening and/or secondary steam relief). Failure of moderator flow is not important as an initiating event. However moderator system is important in those situations where core cooling is impaired due to failure of other means of cooling. Generally, the factors considered in omitting an IE from the list of dominating events could be,

- An enveloping IE exists
- Slow transient, operator action is feasible
- Low frequency
- Consequences are not very significant.

The remaining events are analysed, in the subsequent sections, regarding their frequency and possible impact on the core depending upon the operability states of the various ESFs provided. Further, IEs included in group 7 are not considered since these correspond to radioactivity leakages from out of core components.

12.2.2.2 Reliability Analysis

It is important to differentiate between different categories of systems from the reliability viewpoint.

- Process Systems: Process Systems which are active during normal functioning of the reactor, e.g. Reactor Regulating System, Primary Heat Transport System etc. IEs are generally associated with failures in process systems.
- Safety Systems (ESFs): Safety systems are not active during the normal reactor operation but act following failure of a process system to limit the consequences thereof, e.g., Protective and Containment Systems.
- Support Systems: These are active during normal operation and are also essential for the functioning of the ESFs, e.g., Station Electric Supply, Compressed Air System.

Since process systems play an active role in plant operation, any process equipment failure would be immediately annunciated. But in case of protective and containment systems, being normally standby, there may be component failures which will be unrevealed till there is a demand on the system to function or it is tested. As a result a safety system will remain in a failed condition over the period of time from the occurrence of the failure till it is revealed by the test and repairs are affected. A process system failure during this interval would result in a dual failure. Thus, an accident sequence would arise if a process failure is coupled with the unavailability of one or more ESFs. Since redundancies are provided within every process and safety system to meet the single failure criteria, the frequency of an accident sequence is generally low.

Reliability Criteria

Based on the system definitions above, the reliability index of process systems or IEs has been computed in terms of frequency i.e. the probable number of failures per year while for the safety systems, the term unavailability is used which is the probable fraction of the time during which the system is not available. The unavailability is further related to component failure rates and test frequencies by the following equation,

$$Unavailability = Failure\ rate\ per\ year\ \times\ Failure - duration\ (Years)$$

where, the failure duration is assumed to be equal to half of the time between tests since the failure at any time between tests is equally probable. The contributions due to scheduled and breakdown maintenance are also incorporated. The distribution of downtime is assumed as lognormal, with a median duration of 24 h and a maintenance action rate of once in 6 months.

Failure Rate Data

The input data required for reliability analysis comprises of the following:

1. Component Failure Data
2. Component Maintenance Data
3. Human Error (HE) Data
4. Common Cause Failure (CCF) Data

The confidence in reliability analysis is determined to a large extent by the accuracy in failure rate data of the constituent components. It would be ideal to use data based on the operational experience. The other alternative is to use data from established sources which may not be always applicable due to variations in design, quality, operating environment etc. Bayesian techniques are used to obtain better estimates by using the limited information based on PHWRs experience and WASH-1400 as prior for a number of components like DGs, Transformers etc.

Common Cause Failures

The common cause failures are dependent, multiple failures arising from a common initiating cause. The main categories of CCFs considered in the analysis are:

- Design Errors
- Manufacturing Errors
- Test and Maintenance Errors
- Effect of External Environment.

As far as practicable, care is exercised to keep the process and safety systems independent of each other and safety systems among themselves to minimise the incidence of CCFs. Special qualification procedures where applicable, are adopted for the components to withstand the common causes such as earthquake, accelerated environment following an accident like LOCA etc. Beta factor or Alpha factor model are used for the analysis of CCFs and the plant specifics are considered in arriving at the appropriate beta/alpha factors. An extensive qualitative analysis of common cause failures with respect to independence in electrical supplies, process water cooling etc. and provision of physical diversity in case of various safety systems (e.g., Fire Fighting Water, Emergency Core Cooling and Class III Power Supply System etc.) has been carried out.

Human Reliability Analysis
Human Reliability Analysis deals with the identification of potential Human Errors (HEs) both during normal reactor operation and the post accident situations. During normal operation, HEs arise from the test and maintenance actions and are represented in the corresponding FT of the system, where as, the post accident HEs are associated with detection of the failure situation (IE), diagnostics and subsequent actions for mitigation of the IE and are represented in the ETs. An attempt has been made to identify the human actions called for, and carry out a detailed qualitative analysis to estimate the time required for doing the same so as to identify the critical human actions in the reactor during postulated accident conditions. It is important to realize that human actions can be characterized into the following categories:

1. Skill Based Actions
2. Rule Based Actions
3. Knowledge Based Actions

Obviously, the Human Error Probability (HEP) is minimum with skill based actions and becomes prohibitively large in case of knowledge based actions, with Rule Based HEP being a compromise or a median value. It is usually the objective of HRA to ensure that all human actions are skill/rule based and in case, the available time is too short, the actions must be performed automatically. This necessitates proper procedures and operator qualifications to be followed in the plants. HRA based on Systematic Human Action Reliability Procedure (SHARP) [6], as developed by Electric Power Research Institute (EPRI) of USA and recommended by IAEA, has been used in quantifying the HEPs in the study.

12.2.2.3 Accident Sequence Identification

In view of the 'Defence in Depth' approach applied in the design of reactor systems, an accident situation arises only when an IE is coupled with the unavailability of one or more ESFs. Thus dual or multiple failures are necessary for an accident to occur. These dual or multiple failures are known as Accident Sequences in PSA parlance. The significance of accident sequences can be understood from the definition of risk as follows:

$$Risk = Probability\ of\ occurrence \ \times \ Consequences$$

In a NPP, the probability of occurrence signifies the probability of all the accident sequences and the consequences are measured in terms of radioactivity releases. Thus risk from a NPP is

$$\begin{aligned} Risk = \sum Probability\ of\ accident\ sequence \\ \times \ Consequences\ All\ Accident\ Sequences \end{aligned}$$

and the overall risk can be quantified if we can identify all the accident sequences and evaluate their consequences. In level I PSA, the requirement is to identify all the accident sequences and relate them to component failures and human errors. In the present study, accident sequences relevant to the PHWR have been identified using Event Tree methodology. Event Trees for all the dominating IEs have been drawn, the brief details of important ETs are given in next section.

Accident Sequence Quantification
The accident sequence as identified by the Event Tree may be expressed as follows.

$$\text{Accident Sequence} = \text{Initiating Event} \times \text{ESF(s) Failure}$$

Obviously, in an accident sequence there are other terms implying the success of other systems. However, these can be ignored since the success probabilities are approximately 1.0. In terms of probabilities, the accident sequence frequency may be written as;

$$P = P_{IE} \cdot P_{ESF_1} \cdot P_{ESF_2} \cdot \ldots$$

where, P_{IE} is the frequency of the Initiating Event and P_{ESF_i} is the unavailability of that particular ESF_i which is obtained form the respective Fault Tree. In order to obtain correct accident sequence probability, the correct probabilities of the individual factors must be used, incorporating any dependency among the factors. Thus various system probabilities are treated as conditional probabilities and expressed as

$$P_{ESF_1} = P_{ESF_1/IE} \quad \text{and} \quad P_{ESF_2} = P_{ESF_2/ESF_1 \cdot IE} \quad \text{etc.}$$

where, $P_{ESF_1/IE}$ denotes the probability of ESF_1 failure given that the initiating event has occurred and so on. A simple multiplication of the probabilities can only be used when the various factors are independent. The dependencies, if any, are included in the discussion on the individual Event Trees.

System Dependencies
As mentioned before, various ESFs have been designed to operate independently—both among themselves and also, with respect to the IE. However, some form of dependency has been observed. Normally, it is expected that various components and equipment are designed to operate in the accelerated environmental conditions generated by the IE. In case of LOCA, an environment of high temperature, pressure, radiation and humidity prevails in the containment and various components e.g. pump seals, pump motors, junction boxes, coolers etc. are susceptible to it. Further, the presence of moderator as a heat sink is very important in case of PHWRs to prevent fuel failures if ECCS fails but the efficacy of the system need be ensured when a significant amount of energy is added into the moderator. The reliability of the moderator pumps, flange joints etc. will be affected in such cases. The effects of such common causes have been incorporated in the accident sequence quantification.

12.2.2.4 Event Trees

As explained before, ETs have to be developed to study the consequences of an IE on the core, PHT systems and containment etc. and also to determine the efficacy of various safety systems required to mitigate the effects of the IE.

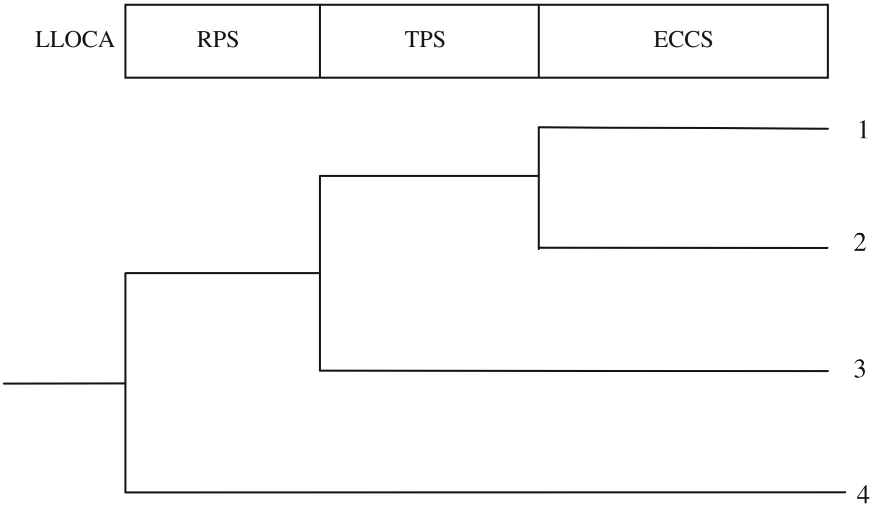
Loss of Coolant Accident (LOCA) Event Trees
Unlike in Pressurized Water Reactors (PWRs) and Boiling Water Reactors (BWRs) the diameter of the largest piping in PHWRs is much smaller, thereby limiting the coolant discharge rate in case of LOCAs. The coolant activity discharged into the containment is smaller due to the smaller PHT inventory in PHWRs. Depending upon the physical phenomena involved, LOCAs can be divided into;

1. Large LOCA—e.g. PHT header rupture
2. Medium LOCA—e.g. End fitting failure, Feeder rupture etc.
3. Small LOCA—e.g. Instrument tube rupture, SG tube rupture etc.,

and as a consequence the ESFs required to act upon are also different.

Large LOCAs are characterised by break areas greater than 10 % of 2A (A = area of the pipe). These lead to fast depressurisation of the PHTS which results in subsequent ECCS injection and recirculation. However, the initiation of light water injection also depends on the availability of the signal-pump room pressure high or high moderator level in calandria. Because of the speed with which the IE propagates, operator actions are not expected/anticipated and accordingly all the ESFs that have to be operated are designed to cut in automatically. Because of the fast depressurisation and subsequent low PHT pressure ECCS cuts in and continues to provide cooling.

The ET for the initiating event large LOCA is shown in Fig. 12.2. It is important to note that the coolant void coefficient of reactivity is positive in a PHWR and this warrants a fast shutdown in the present case. Since the moderator is not dumped on a reactor trip, the presence of a large volume of moderator which is cooled by an



RPS – Reactor Protection System; TPS: Total Power Supply System;
ECCS – Emergency Core Cooling System

Fig. 12.2 Event tree for LLOCA

independent circuit of pumps and heat exchangers acts as an ultimate heat sink. Various studies [7, 8] indicate that no fuel melting is likely to occur even if ECCS fails on LOCA. Thus fuel melting in a PHWR can be postulated to occur when there is a breach in the moderator circuit in conjunction with LOCA and emergency core cooling injection failure.

Class IV Power Supply Failure

Class IV is the main power supply provided both by the grid and generated by the station. This IE is significant in our context due to high frequency of class IV failure. Based on the operating experience, it is observed that the frequency is >1.0/year which is relatively high. It is usually 0.1–0.3/year in many other countries. Interdependence (common cause failure) of station supply on grid fluctuations and vice versa is a significant contributing factor to the class IV failure frequency.

The ET and the various ESFs required to mitigate the effects of the transient are shown in Fig. 12.3. The Secondary Steam Relief (SSR) is provided by a redundant configuration comprising Steam Discharge Valves (SDVs) and safety relief valves. Here, no credit for the safety relief valves is taken as these are meant for the protection of steam generators. On class IV failure, secondary cooling is provided by auxiliary feed water system which is further backed up by the firefighting system (FFS) comprising three dedicated diesel pumps. In case of loss of all secondary cooling, SG hold-up would last for about 30 min and by this time, the shutdown cooling system must be valved in. Similar criteria are applicable to valving in of FFS in case auxiliary feed water system (AFWS) is not available.

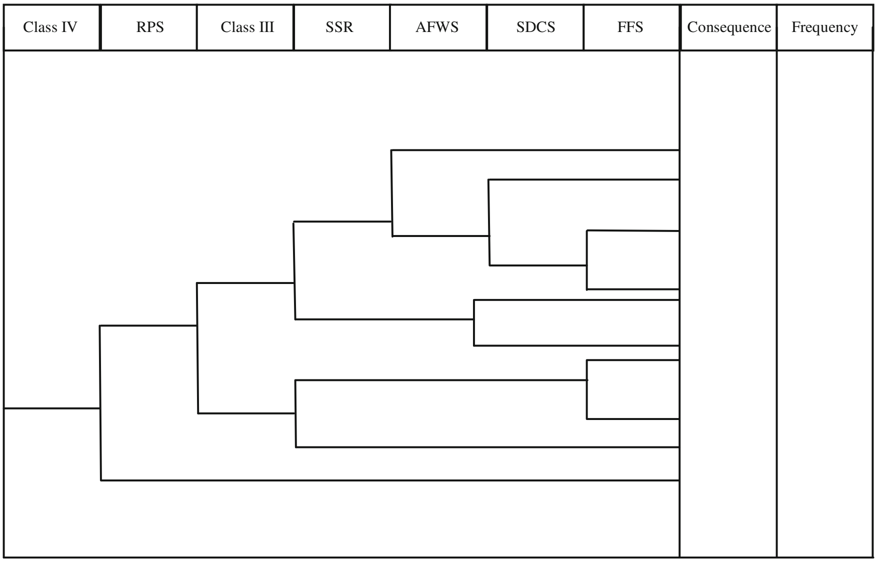


Fig. 12.3 Event tree for CLASS IV failure of PHWR

Accident sequences which depict the failure of both class IV and class III leading to the situation of Station Blackout are critical. The station batteries are usually rated for a duration of about 30 min and this primarily sets the limit to the available time within which the power supply must be restored. The probability of restoring the supplies in 30 min is low. NUREG-1032 of USNRC quotes a median value of (a) 30 min for the restoration of off-site power and (b) 8 h for DG downtime. In case of an extended blackout, it could result in a critical situation since AFWS, shutdown cooling system (SDC) would not be available. Also, the supply to control and protective systems (class I) would be lost, resulting in a total loss of monitoring and indication of the plant status. It may be essential to crash cool the primary which would result in large scale voiding in the system. However, with secondary cooling available, provided by the FFS, thermosyphoning would be effective. The reliability of FFS is thus crucial for mitigating the station blackout situation. In addition, FFS is essentially a low pressure system and manual actions are involved in 'valving in' of the same. In case of a station blackout, which is definitely an unusual situation, the stress on the operator is likely to be high and the time available is also ~half an hour. Hence the probability of the human error could be significant. However, since FFS is the only safety system available the chances of recovery would be high and the system could be 'valved in' after some delay.

It may be further inferred that in a PHWR a large coping time may be available during station blackout as long as thermosyphoning holds good on the primary side and fire water is injected into the SGs. Thus, a coping time of ~4 h may be assumed during which class IV or class III supply must be restored. This will reduce the contribution of this IE to CDF significantly.

12.2.2.5 Dominating Accident Sequences

The overall number of accident sequences identified through ET analysis is very large as described in the previous section. However, based on the probabilistic and analytical assessment of the consequences of the accident sequences, a relatively small number of accident sequences which are likely to result in varying degree of core/clad damage, are identified for further analysis. The extent of core damage is not assessed and in the next phase of the study wherein, the consequences in terms of the effect on the core, radioactivity released, effect on the containment and its failure modes etc. would be discussed. Accident sequences, where, some clad damage only is expected, are not included in CDF calculations. The accident sequences contributing to CDF known as dominating accident sequences are included in Table 12.2. Accident sequences initiated by class IV failures are highly significant due to high frequency of this IE (2/Yr). In case of failure of FFS following a station blackout sequence, FFS or class IV recovery over a period of 1 h may be considered. Failure probability of FFS is high because of the observed large downtime of the pumps. In fact, the CCFs have also been observed in the system due to failure in the DC supply. It is seen that accident sequences initiated by active

Table 12.2 Percentage contribution of accident sequences

	Initiating event	Safety systems			% Contribution to CDF
1	CLASS4	CLASS3	CLASS4RE	HEFFS	32.0336
2	APWCS	HEFFS			29.7723
3	CLASS4	CLASS3	CLASS4RE	FFS	10.2507
4	APWCS	FFS			9.5271
5	MSLB	HEECR	ML		7.9973
6	CLASS4	SSR	SDC		3.3864
7	CLASS4	RPS			1.8871
8	MLOCA	ECCI	ML		1.4217
9	CLASS4	SSR	HESDC		1.1870
10	MLOCA	ECCR	ML		0.5332
11	CLASS4	CLASS3	CLASS4RE	SSR	0.4741
12	APWS	AFWS	HEFFS		0.4019
13	FWS	RPS			0.2602
14	CLASS4	AFWS	HEFFS	HESDC	0.2165
15	CLASS4	AFWS	SDC	FFS	0.1977
16	FWS	SSR	HESDC		0.1636
17	APWS	AFWS	FFS		0.1286
18	CLASS4	AFWS	HESDC	FFS	0.0693
19	MLOCA	RPS			0.0458
20	FWS	AFWS	HESDC	HEFFS	0.0299
21	FWS	AFWS	HESDC	FFS	0.0096
22	SLOCA	RPS			0.0064

process water cooling system (APWCS) which is used for cooling the DGs, Compressors, etc. and also the APWS itself, are also dominating. The failure of APWCS and human error in firefighting system (HEFFS) is a significant contributor. However, it would be delayed core damage since the moderator pool is available till it boils off. As mentioned before, the presence of moderator in the core prevents fuel melting in case of LOCA and unavailability of the ECCS. Thus, all accident sequences originating from LOCAs, main steam line break (MSLB) and others resulting ultimately in LOCA would result in core damage only if the moderator is not available as a heat sink. The overall core damage frequency is found to be ~3.2E-06/Yr.

12.2.2.6 Risk Importance Measures

The results of PSA level-1 study can be utilised to derive the importance of various systems and components in terms of their contribution to risk/core damage frequency. Obviously, CDF is obtained from the accident sequences which are related to IEs and safety system failures which can be further expressed as a function of component failures and HEPs. This helps in adopting risk importance measures in an optimal way. Following risk measures have been considered in this context:

Risk Achievement Worth (RAW) of a system is defined as the increase in risk (or CDF) when this system has failed or is removed from service.
Risk Reduction Worth (RRW) of a system is defined as the reduction in risk (or CDF) when the system is fully reliable.

Thus, RAW signifies the importance of a system in achieving the present level of safety whereas RRW suggests the system/components which can reduce the risk effectively if modified suitably. It is seen that RPS has the highest RAW and this implies the high safety significance of the system. Emergency power supply (class III), FFS and human error in FFS are both significant in terms of their high RAW and RRW values. Thus improving the reliability of these systems or human actions would reduce the CDF. Moderator circulation and SSR also have significant RAW values. In addition, the contribution of each IE to CDF has also been obtained and the same is shown in Table 12.3. It is seen that APWCS and class IV contribute very significantly to CDF.

Table 12.3 Contributions of initiating events to core damage

Initiating event	Frequency	Percentage contribution
Small LOCA	1.42E-09	0.007
Medium LOCA	4.44E-07	2.027
CLASS 4	1.09E-05	49.77
APWCS	8.59E-06	39.21
APWS	1.15E-07	0.524
MSLB	1.75E-06	7.988
FWS	1.02E-07	0.467

12.3 Technical Specification Optimization

Probabilistic Safety Assessment (PSA) is performed to assess the risk of complex engineering systems like nuclear power plants (NPPs). PSA studies not only evaluate risk/safety of systems but also their results are very useful in safe, economical and effective design and operation of NPPs. The latter application is popularly known as “Risk-Informed Decision Making”. Evaluation of technical specifications is one such important application of Risk-Informed decision making. Technical specifications represent a set of parameters according to which systems should be operated, tested, maintained and repaired. Deciding Test Interval (TI), one of the important technical specifications, with the given resources and risk effectiveness is an optimization problem.

The criterion for regulation of the design and operation of NPP has been derived from deterministic engineering analysis methods. This traditional defence-in-depth philosophy continues to assure a safe condition of the plant following a number of postulated design basis accidents and also achieving several levels of safety. During recent years, both the nuclear utility and nuclear regulatory bodies have recognized that PSA has evolved to the point that it can be used increasingly as a tool in decision making. The key to this risk-informed approach to decision making is that it is complementary to the defence-in-depth philosophy. This has given rise to the advent of various methodologies for optimizing activities related to NPP operation and maintenance. Thus the risk-informed applications emphasize both effective risk control and effective resource expenditures at NPPs by making use of PSA results to focus better on what is critical to safety.

Several studies have emphasized the potential of risk-informed approach and its application to nuclear as well as non-nuclear/chemical industries also. The specific activities related for their resource effectiveness in risk-informed applications are evaluation of technical specifications, in-service inspection, and preventive maintenance. Evaluation of technical specifications is one of the important applications of Risk-Informed decision making. Technical specifications represent a set of parameters according to which systems should be operated, tested, maintained and repaired. Deciding Test Interval (TI), one of the important technical specifications, with the given resources and risk effectiveness is an optimization problem. Nowadays, special attention is being paid on the use of PSA for risk-informed decision making on plant specific changes to test intervals in technical specifications.

12.3.1 Traditional Approaches for Technical Specification Optimization

The various risk measures and methodology for TS modifications related to Allowed Outage Times (AOTs) and Surveillance Test Intervals (STIs) are discussed here [9]. The steps include the following. (a) identify the STIs and AOTs to be evaluated for consideration of changes, (b) determine the risk contribution associated with the subject STIs and AOT, (c) determine the risk impact from the change of proposed AOTs and STIs by evaluating risk measures of structure, system, and component (SSCs) for which change in AOT/STI is sought, (d) ascertain the acceptability or otherwise of the risk impact (e.g., change in system unavailability, CDF, release frequency, etc.) from target value established for risk informed decision (e) perform sensitivity and uncertainty evaluations to address uncertainties associated with the STI and AOT evaluation.

12.3.1.1 Measures Applicable for AOT Evaluations

Conditional Risk Given the Limiting Condition of Operation (LCO)
Increase in risk (ΔCDF or ΔLERF—large early release frequency) associated with component outage is shown in Fig. 12.4.
Incremental Conditional Core Damage Probability (ICCDP) or Single Downtime Risk

Increase in risk (e.g. single down time risk r_i of ith component is obtained by multiplying the increase in CDF by the duration of the configuration for the occurrence of a given configuration i.e., outage of ith component only).

$$\mathrm{r_i} = \Delta \mathrm{C_i} \times \mathrm{d} = \left(\mathrm{C_i^+} - \mathrm{C_i^0}\right) \times \mathrm{d_i} \tag{12.1}$$

r_i Single downtime risk of the ith component
C_i^+ CDF when component is known down including reconfigurations
C_i^0 CDF when component is known up
d_i downtime

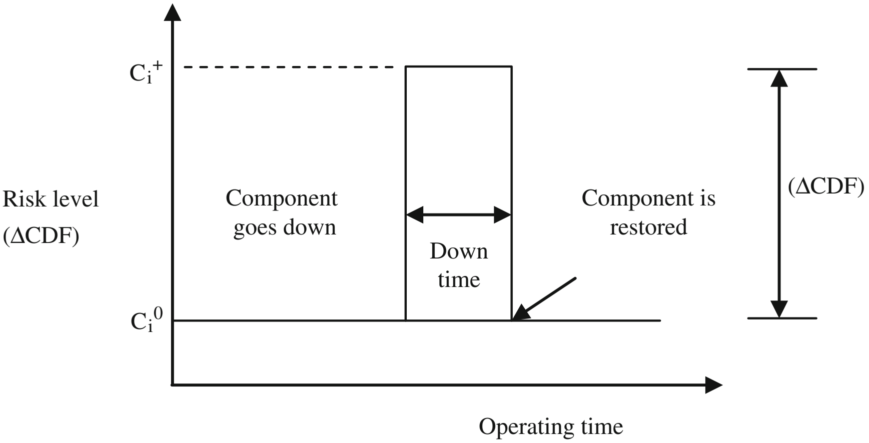


Fig. 12.4 Increase in risk associated with component outage

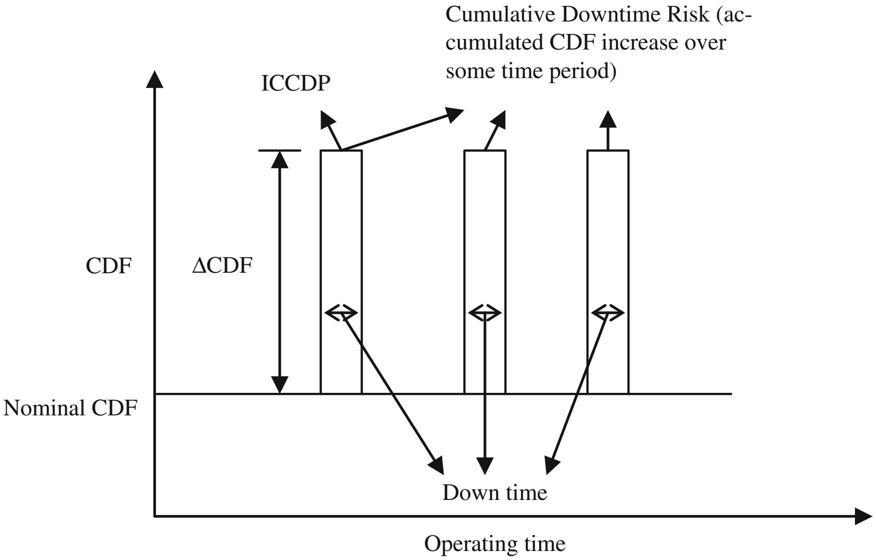

Cumulative Downtime Risk (accumulated CDF increase over some time period)
ICCDP
CDF
ΔCDF
Nominal CDF
Down time
Operating time

Fig. 12.5 Illustration of the different risks associated with downtimes

By imposing an acceptable limit (i.e., target or reference value for risk informed decision process) to the risk contribution of an AOT, a risk based AOT can be calculated, $d_{max} = r_{max}/\Delta R$ where ΔR is the change in risk (change in system unavailability, change in CDF (ΔC_i) or change in LERF). Then the risk based AOT can be compared to the real time duration of maintenance and to the AOT established in the TS.

Yearly AOT Risk
Risk increase from the projected (or expected) number of downtimes over 1 year period is yearly AOT risk. Figure 12.5 shows the single down time risk and cumulative downtime risk over some time period.

$$R_i = N_i r_i \tag{12.2}$$

R_i Yearly downtime risk for ith component
N Expected number of downtime occurrences in a year = wT
w downtime or maintenance frequency = $k\lambda$

where
k maintenance factor,
λ failure rate and
T time period, 1 year.

Maintenance frequency includes failure frequency and the frequency of maintenance due to degraded or incipient conditions.

When comparing the risk of shutting down with the risk of continuing power operation for a given LCO, the applicable measures are:

- risk of continued power operation for a given downtime, similar to ICCDP and
- risk of shutting down for the same downtime

The risk associated with simultaneous outages of multiple components, called configuration risk, is calculated as part of AOT changes. The applicable measures are similar to the AOT measures stated above.

12.3.1.2 Measures Applicable for STI Evaluations

Test-Limited Risk

The analysis of STIs is based on the risk contributions arising from failures occurring between tests and detected at the moment of the test. The STI risk contribution of a component is given by

$$\mathrm{R_D} = 1/2\,\lambda_\mathrm{s}\mathrm{T}\,\Delta\mathrm{R} \tag{12.3}$$

where $\varDelta R$ is the risk increase when the component is found failed at the moment of the test, λ_s is the standby constant failure rate and T is the STI. Similar to the AOT risk contributors, the STIs can be classified and set to a limiting value to the risk contribution,

$$T_{max} = (2R_{Dmax})/(\lambda_s \varDelta R) \tag{12.4}$$

Test-Caused Risk

To evaluate and identify the test-caused risk, events should be analysed and those caused by a test should be identified. These could be due to failure in human interactions or component wear out on testing. Failure due to Human Error Probability can be modelled and quantified from detailed Human Reliability Analysis. Component wear out can be addressed by ageing risk analysis. However an integrated approach to work out such test caused risk is a developing subject and presently is beyond the scope of this chapter.

12.3.2 Advanced Techniques for Technical Specification Optimization

The issue of risk effectiveness versus resource utilization is an optimization problem where the resources, viz., number of tests conducted, working hours required, costs incurred, radiation exposure, etc., is to be minimized while the performance or unavailability is constrained to be at a given level. As mentioned by Martorell [10], in optimizing test intervals based on risk (or unavailability) and cost, one normally faces multi-modal and non-linear objective functions and a variety of both linear and non-linear constraints. In addition, requirements such as continuity and differentiability of objective and constraints functions add yet another conflicting element to the decision process. Resolution of such complex optimization problems requires numerical methods. However, as traditional approaches usually give poor results under these circumstances, new methods based on Genetic Algorithms (GAs) were investigated in order to try to solve this kind of complex optimization problems [10–13]. This section presents a solution to test interval optimization problem with genetic algorithm along with a case study of a safety system for Pressurized Heavy Water Reactor (PHWR).

12.3.2.1 Mathematical Modeling of Problem

Notations:

T	Surveillance test interval
t	Mean time to test
Λ	Standby failure rate
ρ	Per-demand failure probability
d	Mean time to repair
M	Mean time to preventive maintenance
M	Maintenance interval
c_{ht}	Testing cost per hour
c_{hm}	Preventive maintenance cost per hour
c_{hc}	Corrective maintenance cost per hour

System unavailability model in the PRA is adopted to represent the risk function. It is obvious that by optimizing test intervals based on minimizing the corresponding safety system unavailability one can improve the safety level of NPP. Unavailability function of the system is generally derived from fault tree analysis, which is a logical and graphical description of various combinations of failure events. Minimal cut-sets are obtained from fault tree analysis which represents minimal combinations of basic events (components) leading to unavailability of system. Thus, system unavailability is expressed as a function of unavailability of components. As safety system is considered for case studies and normally all the components in a safety system are in standby mode, the following model (refer Eq. (12.5)) as explained in [10, 14] represents the unavailability of component. It is a function of unavailability arising from random failure during standby mode, surveillance testing, preventive maintenance activity, and corrective maintenance due to observed failure.

$$\mathrm{u(x) = u_r(x) + u_t(x) + u_m(x) + u_c(x)} \tag{12.5}$$

u(x)	Represents unavailability of component that depends on the vector of decision variables x.
u_r(x)	Contribution from random failures $\approx \rho + \lambda T/2$
u_t(x)	Contribution from testing $\approx t/T$
u_m(x)	Contribution from preventive maintenance $\approx m/M$
u_c(x)	Contribution from corrective maintenance $\approx (\rho + \lambda T)d/T$

thus,

$$u(x) = \rho + \lambda T/2 + t/T + m/M + (\rho + \lambda T)d/T \tag{12.6}$$

System unavailability is sum of j number of minimal cut sets and the product k extents to the number of basic events in the *j*th cut set as given in Eq. (12.7):

$$U(x) \approx \sum_j \prod_k u_{jk}(x) \tag{12.7}$$

u_{jk} represents the unavailability associated with the basic event k belonging to minimal cut set number j. Similarly the cost model is given as follows:

$$c(x) = c_t(x) + c_m(x) + c_c(x) \tag{12.8}$$

The total cost c(x) of the component (year wise contribution) includes costs due to testing c_t(x), preventive maintenance c_m(x) and corrective maintenance c_c(x).

$$c(x) = \frac{t}{T}c_{ht} + \frac{m}{M}c_{hm} + \frac{1}{T}(\rho + \lambda T)dc_{hc} \tag{12.9}$$

The total yearly cost of the system having i number of components is given by:

$$C(x) = \sum_i c_i(x) \tag{12.10}$$

Both risk and cost functions are important to decision making in effective, efficient and economical safety management of NPPs. In the first case, constraints are applied over one of the two objective functions, risk or cost function. These are referred to as implicit constraints, where, for example, if the selected objective function to be minimized is the risk, U(x), then the constraint is a restriction over the maximum allowed value to its corresponding cost. In the second case, the selected objective function to be minimized is the cost, C(x), and the constraint is stated through the maximum allowed value for the risk. One can also impose constraints directly over the values the decision variables in vector x can take, which are referred as explicit constraints.

12.3.2.2 Genetic Algorithm (GA) as Optimization Method

The GA is a stochastic global search method that mimics the metaphor of natural biological evolution. GA operates on a population of potential solutions applying the principle of survival of the fittest to produce better and better approximations to a solution. At each generation, a new set of approximations is created by the process of selecting individuals according to their level of fitness in the problem domain and breeding them together using operators borrowed from natural genetics. This process leads to the evolution of populations of individuals that are better suited to their environment than the individuals that they were created from, just as in natural adaptation. Individuals, or current approximations, are encoded as strings, chromosomes, composed over some alphabet(s), so that the genotypes (chromosome values) are uniquely mapped onto the decision variable (phenotypic) domain. The most commonly used representation in GAs is the binary alphabet {0, 1} although other representations can be used, e.g. ternary, integer, real-valued etc.

The main feature of the SSGA is the utilization of overlapping populations, as it can be observed in Fig. 12.6. The SSGA starts with an initial population of a given size. The number of individuals that constitute this base population, denoted by popsize, is selected by the user. This algorithm generates an auxiliary population, of size nrepl, constituted by the offspring obtained after the reproduction of certain individuals selected from the base population. Newly generated offspring is evaluated and then added to the base population. Each individual of the resulting population, composed by popsize + nrepl individuals, is penalized and then scaled to derive a ranking of individuals based on their fitness score. After scaling, the nrepl worst individuals in the ranking are removed in order to return the population to its original size (popsize). Therefore, after replacement, the best individuals remain in the new population constituting the new generation, generically denoted by g + 1, which descends from previous one, g. The number of individuals to be replaced, nrepl, is fixed as 6 in the present problem. Once the new population is generated, the algorithm checks if the termination criterion is satisfied. In case the criterion is not satisfied, then the evolution continues to produce new generation as described previously. The best fit of the population that satisfied termination criteria gives the optimum solution to the problem.

The binary encoding scheme of the decision variables is used for the current problem, test interval optimization, due to its simplicity in mutation operation and the range constraint is automatically implicit in the encoding. The roulette wheel method, which is a stochastic sampling method that picks the individuals by simulating the roulette-wheel, is used in for the process of selection. The one point crossover has been chosen for the crossover operation, which is a very simple method widely used that provides good results. Population size of 100 (popsize) and auxiliary population size of 6 (nrepl) is taken. Crossover and mutation probabilities of 0.7 and 0.1 are assumed in the calculations. More details about steady state genetic algorithm can be found in [10, 15].

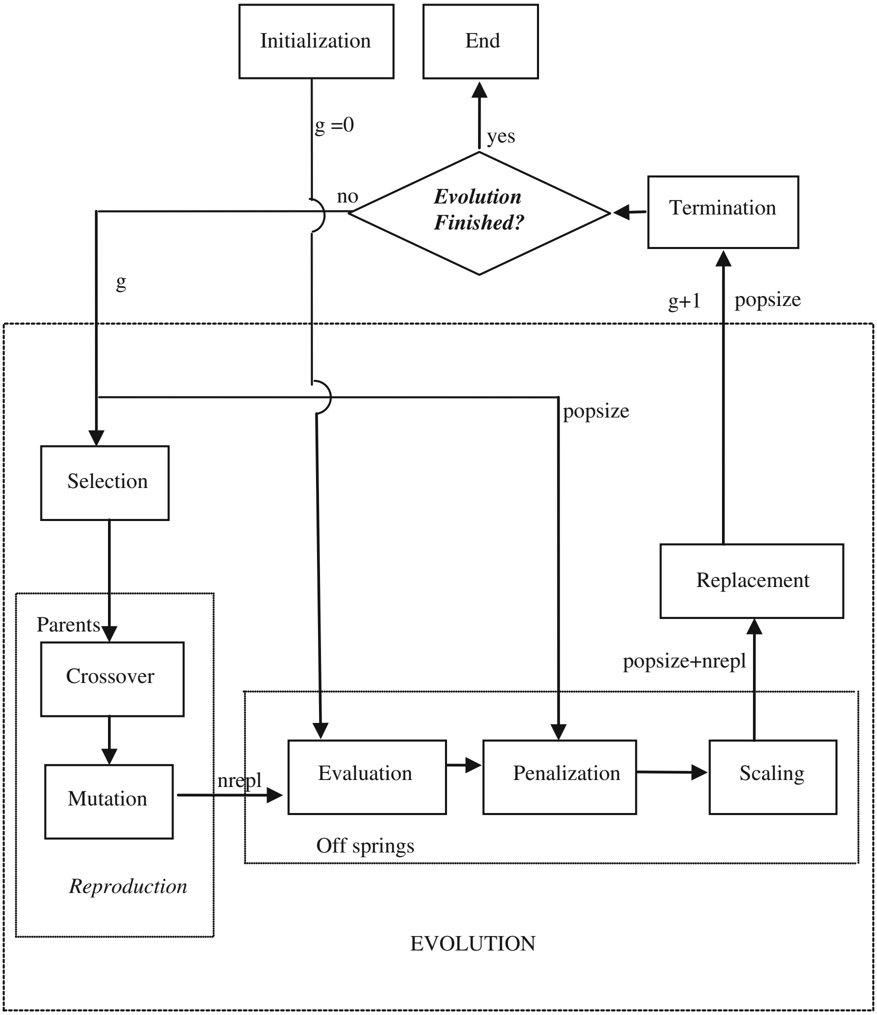


Fig. 12.6 Steady state genetic algorithm scheme

12.3.2.3 Case Studies: Test Interval Optimization for Emergency Core Cooling System of PHWR

Emergency core cooling system (ECCS), one of the important safety system in a Nuclear power Plant is designed to remove the decay heat from the fuel following a Loss Of Coolant Accident (LOCA) and provides means of transferring decay heat to the ultimate heat sink under all credible modes of failure of the Primary Heat Transport System (PHTS) pressure boundary. The operation of ECCS consists of two phases, viz., injection phase and recirculation phase. The surveillance testing is

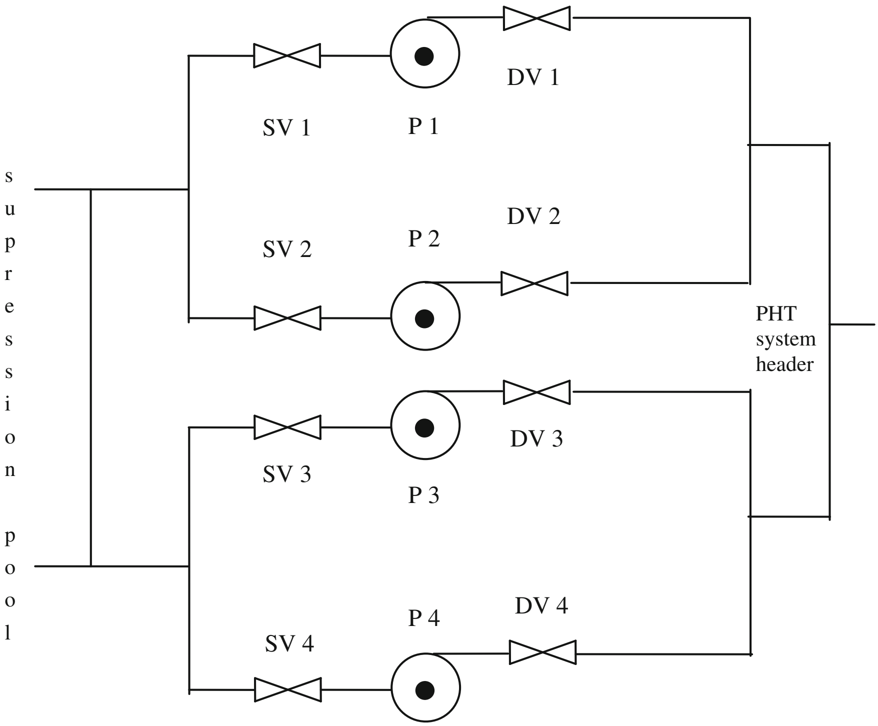


Fig. 12.7 Schematic diagram of ECCS recirculation

focused here on only recirculation part. This consists of four pumps which draw water from suppression pool and inject it into the PHT system header after the light water accumulator level becomes low. Upon the occurrence of LOCA, as sensed by low inlet header and header differential pressure signals, ECCS is initiated depending upon the location of LOCA as sensed by header differential pressure. The schematic diagram of ECCS (only recirculation part) in a typical PHWR is shown in Fig. 12.7.

In this problem, the system components are grouped into three different test strategies. Strategy 1 covers the four motor operated suction valves, namely, SV1, SV2, SV3 and SV4. Strategy 2 covers the four motor operated discharge valves, DV1, DV2, DV3 and DV4. Finally, four pumps, P1, P2, P3 and P4 are placed in the third strategy. It is assumed that all the components in the same group will have same test interval. Further, test strategies must satisfy the following relationship in our particular case of application:

$$T_2 = k_2 T_1 \text{ and } T_3 = k_3 T_2, \tag{12.11}$$

where T_1, T_2 and T_3 are test interval for strategy 1, 2, and 3 respectively. Where k_2 and k_3 are integers that must lie in between 1 to 10. T_1 must lie between [0, 8760].

Table 12.4 Unavailability and cost parameters

S. no.	Name	λ (per h)	ρ (/demand)	T (h)	T (h)	D (h)	c_{ht} (Rs/h)	c_{hc} (Rs/h)
1	P	3.89e-6	5.3e-4	4	2190	24	250	200
2	SV	5.83e-6	1.82e-3	1	2190	2.6	250	200
3	DV	5.83e-6	1.82e-3	1	2190	2.6	250	200

The current practice recommends 1 month for all the components and the cost of test and maintenance for the current practice is Rs. 74082.6 (in Indian Rupees (Rs.)) when it is calculated keeping the failure and repair parameters at their nominal values. It is to be noted that cost of maintenance is a function of failure rate, demand failure probability and repair time (refer Eq. (12.9)). The unavailability parameters of pumps and valves, and the cost parameters are shown in the Table 12.4.

In developing the cost function, costs of only repairs and testing are considered. Computer coding for the genetic algorithm based optimization has been used to solve the problem [16]. The parameters adopted for genetic algorithm and generic operators are shown in Tables 12.5 and 12.6 respectively.

The initial population in SSGA implementation is normally generated using a random method. However, it can not guarantee the criteria of satisfying constraints, therefore the actual test intervals implemented in the plant are considered for initial population. A generation dependent dynamic penalization model and termination criteria have been used in SSGA.

In the first case, the unavailability of the system has been considered as objective function and cost per year (Rs. 74082.6) as the constraint apart from satisfying above said intervals for decision variables T_1, k_2 and k_3. In the second case, cost per year has been considered as objective function and unavailability (3.86e-6) as the constraint. The results achieved for the optimized values of unavailability/cost, the cost/unavailability associated with that unavailability/cost and the optimized

Table 12.5 Genetic algorithm parameters

S. no.	Parameter	Values	S. no.	Parameter	Values
1.	Encoding	Binary	6.	Replacement	10
2.	Chromosome size	22	7.	Generations	5000
3.	Population size	100	8.	Conv. prob.	0.99
4.	Crossover probability	0.7	9.	Diversity	0.01
5.	Mutation probability	0.3			

Table 12.6 Genetic operators

S. no.	Operator	Method
1.	Selection	Roulette-wheel
2.	Crossover	One point
3.	Mutation	Flip mutator
4.	Scaling	Linear

Table 12.7 Optimized values

Variable	Initial values	Optimized values	
		Unavailability as objective function	Cost as objective function
T_1 (h), k_2, k_3	720, 1, 1	480, 1, 2	575, 1, 2
Unavailability	3.86e-6	2.86e-6	3.86e-6
Cost (Rs.)	74082.6	74082	61998.7

decision variables are shown in Table 12.7. In both the cases, the optimized test intervals are decreased for valves and increased for pumps with respect to their initial values. Finally, it is found that important reductions in both unavailability and cost measures have been achieved while all the explicit and implicit constraints are satisfied for the optimized test intervals in both the cases.

Remarks on Technical Specification Optimization
Risk-informed decision making ensures safe, economical and efficient design and operation of nuclear power plants. Test interval optimization, which is one of the important applications of risk-informed approach, has been applied to emergency core cooling system of PHWR. In the Sect. 12.3.2.3, Genetic algorithm has been successfully applied to perform the constrained optimization of test intervals at NPPs, where its capabilities of simplicity, flexibility, easy operation, minimal requirements and global perspective to find global optimum have been shown. From the case studies it is found that the recommended test strategy is better than the test strategy being followed currently. This methodology provides a framework not only for the mentioned constraints but also other constraints of concern to specific operational scenarios.

12.4 Risk Monitor

PSA has become a key tool as on today to identify and understand NPP vulnerabilities. As a result of the availability of these PSA studies, there is a desire to use them to enhance plant safety and to operate the nuclear stations in the most efficient manner. Risk Monitor is a PC based tool, which computes the real time safety level and assists plant personnel to manage day-to-day activities. Risk Monitor is used for modification and re-analysis of a NPP. Operation of Risk Monitor is based on PSA methods for assisting in day to day applications. Risk Monitoring programs can assess the risk profile and are used to optimize the operation of NPP with respect to a minimum risk level over the operating time.

Risk Monitoring can be defined as being the process whereby a complex technical facility is continuously monitored as regards the functioning or non-functioning of its different subsystems and the risk emanating from the facility is evaluated on the basis of this information. In the widest sense it can be regarded as being part of the risk management of a plant. Operation of Risk Monitor is based on PSA methods for assisting in day to day applications. Risk Monitoring programs can assess the risk profile and are used to optimize the operation in NPPs with respect to a minimum risk level over the operating time.

12.4.1 Necessity of Risk Monitor?

In Nuclear Power Plants, safety is the major concern. PSA analysis leads insight into plant processes and mechanisms and possible interaction between plant systems, both for existing plants with operating histories and for plants still in the design stage. In view of this, on-line safety assessment has received lot of attention from operation and maintenance personnel. Plant configuration undergoes changes due to changes in component status and/or operating/maintenance procedures. Some components are randomly down and/or others can be planned for test, maintenance and repair. This results in a variation of the risk level over operating time, which is termed as risk profile, and indicates the trends which could lead to deviation from desired CDF. PSA models can be used to quantify risk due to changes in components status, system design and operations consequent to changes in plant configuration.

Risk Monitoring provides safety status information for a plant and thus aids decision making about whether continued plant operation is tolerable under certain system function outages. It may also support operations and be of help deciding on maintenance strategies allowing immediate assessment of different plant configurations. Besides addressing specific plant requirements it is an on-line tool showing actual risk situation thus overcoming possibly unnecessarily restrictive elements of requirement and point out procedures not conducive to safety. The model used by the risk monitor is based on, and is consistent with, the Living PSA for the facility.

12.4.2 Different Modules of Risk Monitor

Operation of Risk Monitor is based on PSA methods for assisting in day to day applications. Hence, the inputs required by Risk Monitor include:

1. Information on initiating events and their corresponding frequencies.
2. Information on Safety Systems and their fault trees in terms of minimal cut sets for finding out the unavailability's of the systems.
3. Information on component data which include type of model (Tested, repairable, non repairable, mission time etc.,) and their corresponding parameters. These are given in the following table

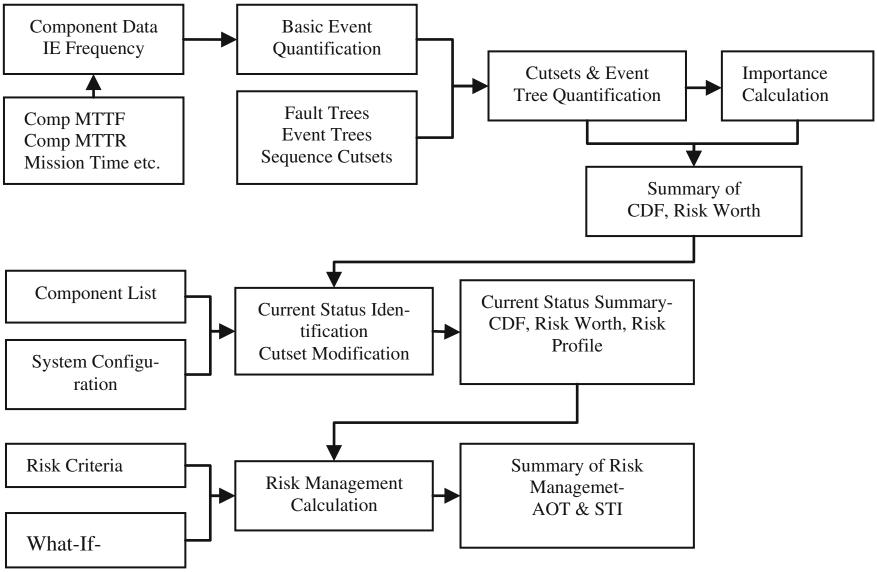

Component Data
IE Frequency
Comp MTTF
Comp MTTR
Mission Time etc.
Basic Event Quantification
Fault Trees
Event Trees
Sequence Cutsets
Cutsets & Event Tree Quantification
Importance Calculation
Summary of CDF, Risk Worth
Component List
System Configu-ration
Current Status Iden-tification
Cutset Modification
Current Status Summary-CDF, Risk Worth, Risk Profile
Risk Criteria
What-If-
Risk Management Calculation
Summary of Risk Managemet-
AOT & STI

Fig. 12.8 Data flow diagram of risk monitor

4. Information on common cause failures (CCF). This includes different number of CCF groups, basic events of each group and their corresponding factors (β factor, α factors etc.)
5. Information on Accident sequences either in the form of initiating events and safety systems or in the form of minimal cut sets for finding out the risk of a plant.

The Data Flow Diagram of Risk Monitor is shown in the Fig. 12.8.

The above diagram describes how the data flow in Risk Monitor and the out come of Risk Monitor. The input information needed in risk monitor is modeled using System Modelling Options and Component database and the output of Risk Monitor is modeled using Main Summary and On-Line Risk module and What-If analysis. In *System Modelling Options* user can provide the information on initiating events, safety systems, minimal cut sets of safety systems and core damage frequency, CCFs. The *Component Database* is a reliability data base used for the management of data which stores the PSA models. The *Main Summary and On-Line Risk*, module summarises status of the safety systems based on the status of the components, list of components which have been taken out from the service and risk profile (CDF vs. Time). *What-If Analysis* is the unique feature of the risk monitor. With this analysis one can analyse different combinations of component states and based on the change in the CDF value decision can be made on which combination of components can be taken for maintenance or can be restored.

As was discussed above once the inputs are specified Risk Monitor will calculate the risk coming from the plant (in terms of core damage frequency in case of nuclear power plants). This is called the base line risk which is based on the present configuration of the systems and components in the plant. The following section describes about the usage of Risk Monitor.

12.4.3 Applications of Risk Monitor

Some important applications of Risk Monitor towards Safety Issues are explained below:

Decision Making in Operations
Core Damage Frequency (CDF) value is an important parameter, which can provide risk insights. If CDF value exceeds the prescribed probabilistic safety criteria, that is termed as an unsafe condition. Also, efforts are always made to lower the CDF through different test and maintenance policies.

Since plant configuration undergoes changes due to changes in component status (some components are randomly down and/or others can be planned for test, maintenance and repair), the plant risk also change based on the present configuration of the systems and components. With help of Risk monitor one can calculate the change in risk based on the outage of the components. The following figure describes about the change in risk with time, in which the risk profile is changing based on the plant configuration. If the component is taken out of service then the component is fully unavailable, in this case risk will increase and is more than the baseline risk. If the component is made fully available in this case risk will come down and will be less than the base line risk. These changes can be seen on risk profile as shown in the following Fig. 12.9. The same is explained with the help of an example and is shown in the Table 12.8. In this table details of a component of one of NPP system are given. The unavailability of the component is calculated

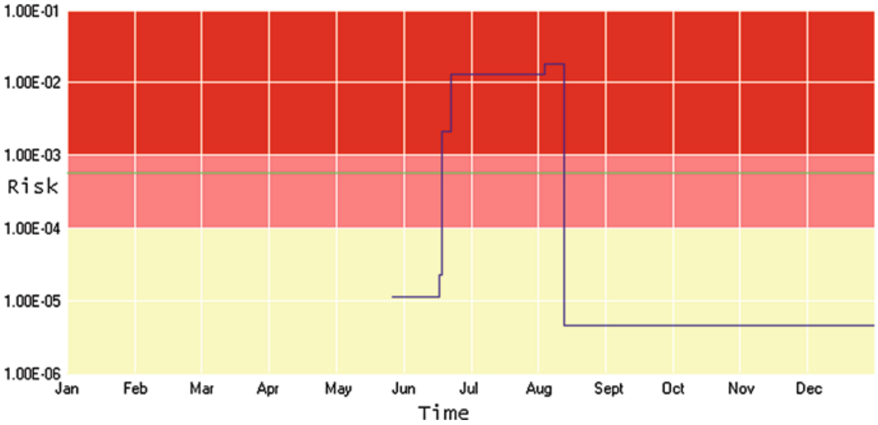


Fig. 12.9 Graphical representation of risk varying with time

Table 12.8 Details of the component which has been taken out from service

General		Parameter	Value
ID	KFFW-MV1	Failure rate	4.75e-6
Description	Motor operated valve	Test interval	720 h
System	Fire fighting water system	Time to first test	0
Model type	Tested	Unavailability	1.708e-3
Existing CDF value			4.487e-6/yr
Change in CDF value when this component is fully unavailable			3.078e-5/yr
Unacceptable risk level			>1.0e-4/yr

based on the component model type. When the component is taken out of service (unavailability has been changed from 1.708e-3 to zero in the risk calculations) then the change is risk is given terms of CDF as 3.078e-5/yr which is greater than the existing risk level (4.487e-6/yr) but it is well below the unacceptable risk level (>1.0e-4/yr). Hence, the component can be taken out of service based on its allowable outage time.

Maintenance Strategies

Importance measures are useful in identification of critical components for the purpose of design modifications and maintenance. Two commonly used importance measures are Risk Achievement Worth (RAW) and Risk Reduction Worth (RRW) of components in terms of CDF.

Risk achievement worth (RAW) is the best input for deciding maintenance policies. RAW and risk reduction worth (RRW) can be evaluated system wise and component wise. Components having higher RAW have to be maintained immediately, in order to minimize the CDF value. Similarly, component having higher RRW should be given attention from the design point of view, since it can enhance the reliability of the system. The RRW suggests the components that can reduce the risk effectively, if modified suitably. The RAW signifies the importance of the components in achieving the present level of safety. The details of importance measures of some of the components calculated from Risk Monitor are shown in the Table 12.9. These measures are calculated on the basis of unavailability of a particular system.

Risk Based In-Service Inspection

The Risk Informed In-Service Inspection (RI-ISI) programs aims at integrating traditional engineering evaluations with insights gained from PSA. The prime use of PSA is to obtain an estimate of risk and relegate it to various systems and down to components to obtain an idea of their importance in terms of contribution to the Risk. Risk Monitor can be effectively employed for analysing the change in CDF whenever there is a change in Inspection plans and thereby analyse for an optimum scheduling plan. Risk importance measures such as RAW, RRW, Fussell-Wessley etc. for various components and systems are readily evaluated in the Risk Monitor for risk based inspection planning.

Table 12.9 Importance measures of various components of ABFW system

System	ABFW	
Description	Auxiliary Boiler Feed Water System	
Unavailability	5.4523e-4	
S. no.	Component ID	RAW
1	ABFW-ACEP4321P4-FTS	53
2	ABFW-ACEP4321P3-FTS	52
3	ABFW-4321P93C-FTE	43
4	ABFW-4321P9-FTS	30
5	ABFW-4321P83C-FTE	19
6	ABFW-4321P8-FTS	5
7	ABFW-4321P43C-FTE	4
8	ABFW-4321P3-3C-FTE	3
9	ABFW-4211HX1-RUPT	2

Incident Severity Assessment
In many situations, it is required to assess the safety significance of failures to enable decision regarding safety issues.

Review of Technical Specification
The Technical Specifications are usually based on deterministic assessment and engineering judgement. Based on the PSA studies, technical specifications based on probabilistic considerations can be evolved to optimise the Allowable Outage Time (AOT) and Surveillance Test Interval (STI) for various Systems.

Emergency Operating Procedures and Risk Management
The Emergency Operating Procedures (EOPs) have been usually based on the considerations of failures in process systems only. EOPs based on dominating accident sequences as identified in PSA can be effectively used in risk management.

12.5 Risk Informed In-Service Inspection

Structural Components like piping, welds, fittings etc. are subjected to various loading due to fatigue damage as well as degradation mechanisms present on it. In order to ensure the structural integrity, In-Service Inspection has been taken up at periodic intervals. Some structural components may be very critical, but may not have active high degradation, while other may not be a critical component but have high degradation mechanism. So it has become necessary to perform ISI is a systematic manner consistent with safety level. Since large number of structural components is present in a NPP, it has become all the more essential to bring out an optimum inspection plan for allocation of inspection resources [17]. Various methodologies developed to achieve this objective are discussed in this section.

Risk-informed in-service inspections programs were initiated by ASME Section XI as an alternative to the current inspection programs. The progression from an implicit risk informed logic to an explicit risk informed logic, has been seen by many to be a natural progression. A principle difference, however, between the present code and the new risk-informed code, is not only the use of an explicit evaluation of risk but also that this risk is based primarily on the operational details of each specific plant rather than the design analysis. Beginning in late 1988, a multi-disciplined ASME Research Task Force on Risk-Based Inspection Guidelines has been evaluating and integrating these technologies in order to recommend and describe appropriate approaches for establishing risk-informed inspection guidelines. This task force is comprised of members from private industry, government and academia representing a variety of industries. The NRC, as part of the research effort, applied this technology in pilot studies of inspection requirements for both PWR and BWR plant systems. Later, it requested the ASME Research Task Force to make the risk-informed inspection process consistent with other Probabilistic Safety Assessment (PSA) applications. ASME Section XI formed a Working Group on Implementation of Risk-Based Examination to begin making Code changes based on risk for inspection of passive, pressure boundary components. The first efforts of this group have been to develop Code Cases [18, 19] providing risk-informed selection rules for Class 1, 2 and 3 piping.

The goal of Risk informed ISI is to allow the use of risk assessment, understanding of component specific degradation mechanisms, to establish an effective plant integrity management program, which maintains plant safety, while at the same time reducing the burden associated with current ISI requirements. These application also yield significant safety, worker radiation exposure and economic benefits. The main advantages of RI-ISI can be summarized as:

1. Decision making based on risk criteria and deterministic information
2. Better focus on allocating resources to high safety significant components.
3. Focus on justifying risk increase
4. In-Service Inspection based on failure modes of components and associated risk

12.5.1 RI-ISI Models

There are two independent methods for RI-ISI, viz. ASME/WOG model and EPRI models. Both are discussed in this section.

12.5.1.1 ASME/WOG Model

The methodology developed by ASME/WOG [20, 21] addresses the quantitative aspect of RI-ISI program, which include:

- Identification of systems and boundaries using information from a plant PSA
- Ranking of components (piping segments), applying the risk measures to determine the categories that are then reviewed to add deterministic insights in making final selection of where to focus ISI resources.

- Determination of effective ISI programs that define when and how to appropriately inspect or test the two categories of high safety significant and low-safety significant components
- Performing the ISI to verify component reliability and then updating the risk ranking based on inspection and test results

The first step in Risk based Inspection is the review of level 1 PSA results of the NPP in concern. The accident sequences, which result in core damage following the occurrences of pre-determined initiating events, are identified. Those basic events, which contribute significantly to the occurrence of the key accident sequence, are identified by applying the appropriate importance measures. These importance measures suggest the importance of systems/components with respect to Core Damage Frequency. Various importance measures like Fussel-Vesely, Birnbaum Importance, Inspection Importance measure etc. are employed for prioritization, which are discussed in the preceding chapter.

(i) *System Prioritization Methodology*

There are many importance measures that could be used to rank systems. For example, the Fussel-Vesely (FV) importance measure involves small changes in risk. Importance measures involving larger changes in risk are Birnbaum importance and RAW. Since pipe break probability is a small probability, Birnbaum importance does not reflect the likelihood of failure. A new parameter called inspection importance measure has been developed in order to prioritize the systems for ISI. System level ranking based on Inspection Importance Measure (I^w). **Inspection Importance (I^W)** of a component is defined as the product of the Birnbaum Importance (I^B) times the failure probability.

$$I_{sys}^{W} = I_{sys}^{B} \times P_{f_{sys}} \tag{12.12}$$

$P_{f_{sys}}$ System failure probability due to structural integrity failures

The Inspection Importance is an approximation of the Fussel-Vesely importance of pipe break for the system and has all the useful properties of the Fussel-Vesely importance measure for establishing the inspection priorities.

Birnbaum and Fussell Vesely importance measures have been suggested by ASME for Risk Informed In-Service Inspection. In most of the applications, the exact ranking is not important. Guidance and experience for applying importance measures for In-Service Testing/In-Service Inspection is mainly based on expert opinion. A sample categorization is given below in Table 12.10, where RAW refers to Risk Achievement Worth.

(ii) *Component (weld) Prioritization Methodology*

For the Systems selected for more detailed analyses (based on the above prioritization methodology), the most risk-important segments/components should be selected for inspection. Failure Modes and Effects Analysis

Table 12.10 Risk categorization based on importance measures

Risk category	Criterion
Potentially high	RRW > 1.005 and RAW > 2
High	RRW < 1.005 and RRW > 1.001
Low	RRW < 1.001 and RAW < 2

(FMEA), which is a systematic, logical processes for identifying equipment failure modes for a plant, system or component, has been selected as the methodology for component prioritization. The FMEA inductively determines the effects of such failures will have on the desired operational characteristic of the system being analyzed. The most useful outputs of an FMEA are the assessment of design adequacy of the system to perform its intended function.

The FMEA results can be used to calculate the importance index or relative importance of each weld (Table 12.11). This importance index is based on the expected consequence of the failure of weld, as measured as the probability of core damage resulting from the weld failure. In mathematical terms, the probability of core damage resulting from weld failures is defined as

$$\mathrm{P_{cd}} = \mathrm{P_{fi}} \times \mathrm{P_{cd|si}} \times \mathrm{P_{si|Pf}} \times \mathrm{R_i} \tag{12.13}$$

where

$\mathrm{P_{cd}}$	Probability of core damage resulting from weld failure
$\mathrm{P_{fi}}$	Failure probability of weld
$\mathrm{P_{cd\|si}}$	Conditional probability of core damage, given system i failure
$\mathrm{P_{si\|Pf}}$	Conditional probability of system i failure, given a weld failure
$\mathrm{R_i}$	Probability that operator fails to recover, given a system i failure

These ranking also form a basis for determining the inspection category and type of examination required. ASME code case 577 is developed for conducting RI-ISI based on WOG methodology.

Table 12.11 FMEA sample sheet

(1) Piping section (location)	(2) Failure probability	(3) Failure effect	(4) Recovery action	(5) Core damage probability	(6) Relative importance	(7) Remarks
•	•	•	•	•	•	•
•	•	•	•	•	•	•
•	•	•	•	•	•	•

12.5.1.2 EPRI Model

Another methodology has been developed by EPRI (Fig. 12.10). Fleming [22, 23] discusses their methodology, which analyses the degradation mechanisms in structures in detail. EPRI methodology blends PSA and deterministic insights.

Risk matrix [24] can be defined as a Decision matrix that is used to categorize the pipe segments into high, medium, and low importance, based on degradation mechanism and consequence of its failure (Fig. 12.11). By examining the service data, a basis has been established for ranking pipe segment rupture potential as High, Medium, or Low simply by understanding the type of degradation mechanism present (Table 12.12). Consequence can be quantified through the estimation of Conditional Core Damage Probability (CCDP).

The matrix defines three broad categories of relative failure potential that are derived from an underlying quantification of pipe rupture frequencies and four categories of relative consequences that are derived from an underlying quantification of conditional probability for a severe core damage accident given a postulated pipe ruptures. Different categories are defined which proposed different inspection plans. The bounding values of CCDP and rupture potential are shown in Table 12.13:

The consequence evaluation group is organized into two basic impact groups: (i) Initiating Event and (ii) Loss of Mitigating Ability. In *Initiating Event impact*

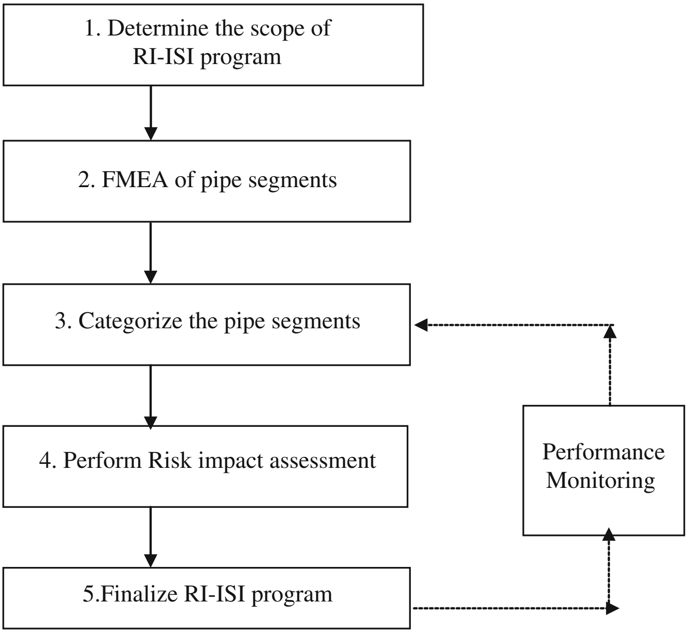
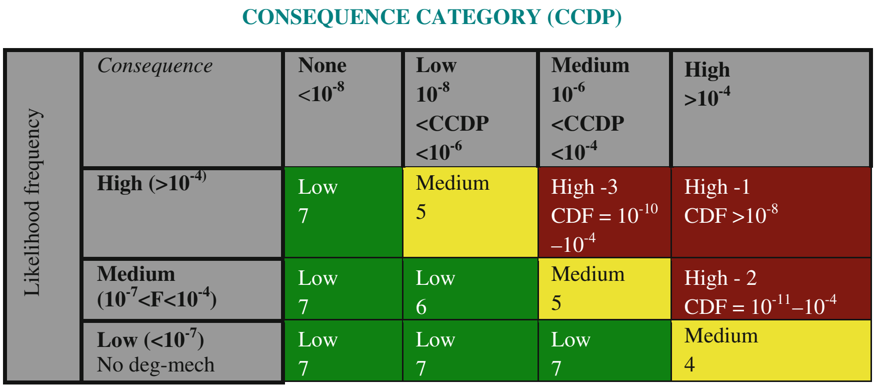

1. Determine the scope of RI-ISI program
2. FMEA of pipe segments
3. Categorize the pipe segments
4. Perform Risk impact assessment
5.Finalize RI-ISI program
Performance Monitoring

Fig. 12.10 Flow chart on RI-ISI program by EPRI



CONSEQUENCE CATEGORY (CCDP)

Likelihood frequency	*Consequence*	**None** **<10^{-8}**	**Low** **10^{-8}** **<CCDP** **<10^{-6}**	**Medium** **10^{-6}** **<CCDP** **<10^{-4}**	**High** **>10^{-4}**
	High (>10$^{-4)}$	Low 7	Medium 5	High -3 CDF = 10^{-10} –10^{-4}	High -1 CDF >10^{-8}
	Medium **(10^{-7}<F<10^{-4})**	Low 7	Low 6	Medium 5	High - 2 CDF = 10^{-11}–10^{-4}
	Low (<10^{-7}) No deg-mech	Low 7	Low 7	Low 7	Medium 4

Fig. 12.11 Risk matrix

Table 12.12 Classification of degradation mechanism

Potential	Degradation mechanism
High	Flow accelerated corrosion, vibration fatigue, water hammer
Medium	Thermal fatigue, corrosion fatigue, stress corrosion cracking, pitting, erosion corrosion
Low	No degradation mechanism

Table 12.13 Classification of consequence

	CCDP	Rupture frequency
High	1	1E-4
Medium	1E-4	1E-5
Low	1E-6	1E-6

Group, the event occurs when a pressure boundary failure occurs in a operating system. This could occur because of loss of fluid (LOCA, Feed water line break), a loss of system (like service water-cooling). The importance of every initiating event, caused by a pipe failure, needs to be assessed in order to assign it to its appropriate consequence category. CCDP can be directly obtained from the PSA results, by dividing the CDF due to the specific IE by the frequency of that IE. In the *Loss of Mitigating* Ability group, the event describes the pipe failures in safety system. Safety system can be in two configurations, Standby and Demand. While in standby configuration, the failure may not result in an initiating event, but degrades the mitigating capabilities. After failure is discovered, the plant enters the Allowed Outage Time (AOT). In consequence evaluation, AOT is referred to as exposure time.

$$\mathrm{CCDP_i} = \left[\mathrm{CDF}_{(\lambda i=1)} - \mathrm{CDF}_{(\mathrm{BASE})}\right] * \mathrm{T_E} \tag{12.14}$$

where

$\mathrm{CDF}_{(\lambda i\,=\,1)}$ CDF given the component failure in a given safety system
$\mathrm{CDF}_{(\mathrm{BASE})}$ BASE CDF
λ_i Pipe break frequency
$\mathrm{T_E}$ Exposure Time (Detection time + AOT)

While in demand configuration, the failure occurs when the system/train operation is required by an independent demand. Here, instead of exposure time, time since the last demand is considered, which is the test interval.

$$\mathrm{CCDP_i} = \left[\mathrm{CDF}_{(\lambda i=1)} - \mathrm{CDF}_{(\mathrm{BASE})}\right] * \mathrm{T_t} \tag{12.15}$$

where

$\mathrm{CDF}_{(\lambda i\,=\,1)}$ CDF given the component failure
$\mathrm{CDF}_{(\mathrm{BASE})}$ BASE CDF
λ_i Pipe break frequency
$\mathrm{T_t}$ Mean time between tests or demands

Measure of Risk due to pipe break:

$$\mathrm{CDF_i} = \lambda_i * \mathrm{CCDP_I}$$

In order to evaluate the impact of risk from changes in in-service inspection, the change in CDF from both the inspection methodologies has been used as a measure. The model described in Eq. 12.16 is based on the influence of pipe frequency at a location j due to the inspection program. The change in the risk of core damage at location j that is impacted by the changes in Risk informed inspection program can be estimated as:

$$\Delta\mathrm{CDF_j} = \left(\mathrm{F_{rj}} - \mathrm{F_{ej}}\right) * \mathrm{CDF_j} = \left(\mathrm{I_{rj}} - \mathrm{I_{ej}}\right) * \mathrm{F_{0j}} * \mathrm{CCDP_j} \tag{12.16}$$

where

$$\mathrm{F_{Aj}} = \mathrm{F_{0j}}\mathrm{I_{Aj}} \tag{12.17}$$

$\mathrm{CCDP_j}$ Conditional Core Damage Probability from pipe rupture at location j

The subscripts "rj" refer to risk informed approach and "ej" refer to existing strategy.
$\mathrm{F_{Aj}}$ Frequency of pipe rupture at location j subject to inspection strategy A
$\mathrm{F_{0j}}$ Frequency of pipe rupture at location j subject to no inspection

I_{Aj} Inspection effectiveness factor (0–1) = This is the probability that the flaw is detected = 1 − POD_{Aj}

After the estimation of risk impact or ΔCDF, depending on the acceptable criteria for ΔCDF, the decision shall be made regarding the adoption of inspection strategy. The decision criterion that has been suggested by EPRI is to ensure that the cumulative change in CDF is less than 1E-7/yr/system for the employment of the new methodology.

12.5.1.3 Comparison of RI-ISI Models

The EPRI RI-ISI process includes: selection of RI-ISI program scope, failure modes and effect analysis, risk categorization of pipe elements, selection of inspection locations and examination methods, evaluation of risk impacts of inspection program changes and final RI-ISI program definition.

After the identification of the critical systems/components, Failure Mode Effect Analysis (FMEA) should be carried out on the basic event. It is essential to identify the prominent failure modes and causes in order to establish the inspection items and guidelines. Risk Matrix is designed with different categories, depending on the CDF values and degradation mechanism for determining the inspection interval. Each segment is assigned the appropriate category depending on it ΔCDF and degradation mechanism.

The EPRI's risk-informed procedure for selecting an ISI programme gives a very straightforward approach to the issue. The method introduced in risk informed fashion combines both the plant specific PSA information and the deterministic insights in support of the system specific, detailed ISI programme selection. Piping of all systems important to safety are exposed to the selection procedure irrespective of the ASME class (1, 2, 3 or even non-code piping). The selection procedure includes four major steps such as:

- Selection of systems and identification of the evaluation boundaries and functions.
- Failure Mode and Effect Analysis (FMEA) including both consequence evaluation and qualitative degradation mechanism evaluation. These two factors are then used for dividing the systems into pipe segments representing common consequences and degradation mechanisms.
- Risk evaluation is made based on the results of FMEA. The risk matrix is built up on the basis of degradation category (low, medium, high) reflecting the potential for large break, and consequence category (low, medium, high) reflecting the core melt potential for limiting break size.
- The division of pipes into segments of various degradation categories is based mainly on qualitative identification of the mechanism, which the pipe segment is exposed to (such as erosion-corrosion, vibration fatigue, water hammer, thermal fatigue, stress corrosion cracking and others). Consequently, the piping failure

data were used to determine the severity and frequency of degradation mechanisms in order to determine the quantitative degradation categories,

- The division of pipes into segments of various consequence categories is based on conditional core damage frequency. High consequence category refers to the conditional core damage frequency class (CCDF) > 10^{-4}, medium consequence category to class 10^{-6} < CCDF < 10^{-4} and low consequence category to class CCDF < 10^{-6}. The degradation and consequence category pairs determine the risk classes, low, medium, high.
- Finally the pipe segments are divided into two main categories. One contains high and medium risk segments and another category contains low risk segments.

In EPRI's pilot study at least one fourth (1/4) of the welds in pipe segments of high risk and one tenth (1/10) of welds in pipe segments of medium risk are selected for examination, whereas the welds in pipe segments that fall in the low risk class will continue to be subject to system pressure and leak tests. The examination of specific elements of segments in high and medium risk classes is based on the degradation mechanism, as well as on inspection costs, radiation exposure and accessibility.

The ASME/WOG and EPRI's approaches (compared in Table 12.14) as well as the NRC's regulatory guide strongly emphasis and recommend that both deterministic and probabilistic engineering insights need to be carefully analyzed and combined for aiding the final decision making process while selecting the ISI programme on piping. A typical approach to combine the information is a panel discussion containing all affecting engineering disciplines. Such a panel discussion is a procedure to reduce the knowledge-based uncertainties which may seriously damage the decision making process.

The NRC's [25] regulatory guide recommends that the potential pipe break probabilities can be estimated by probabilistic fracture mechanics methods. The related computer codes, complex or simplified, can be used to estimate the piping failures as a function of time. An alternative method is to use expert opinion in conjunction with probabilistic fracture mechanics methods to determine the

Table 12.14 Comparison between WOG and EPRI RI-ISI approches

STEP	WOG	EPRI
Piping failure probability assessment	Quantitative	Qualitative
Risk evaluation	Classification using RRW	Categorization of segments in 3 risk regions
Expert panel	Required	Not required
Structural element/NDE selection	Statistical sampling on target reliability	Significant sampling—25, 10 and 0 % from high, medium and low risk region

degradation category of each pipe segment. The degradation categories (low, medium and high) reflect the potential for large break or rupture.

12.5.2 ISI and Piping Failure Frequency

Main tasks for RI-ISI revolve around determination of probability of failure and consequence of failure. For quantification of risk in Nuclear Power Plants, Probabilistic Safety Assessment (PSA) models are widely employed, which forms the basis for consequence quantification for RI-ISI. Various methods have been suggested for piping failure parameter estimation like Structural Reliability Analysis (SRA), Service Data Analysis, Expert Opinion, Remaining Life models etc. The degree to which one relies on one method or another is predicted on the availability of data from service experience, experts or structural reliability or risk models. These aspects are discussed in detail in the preceding section.

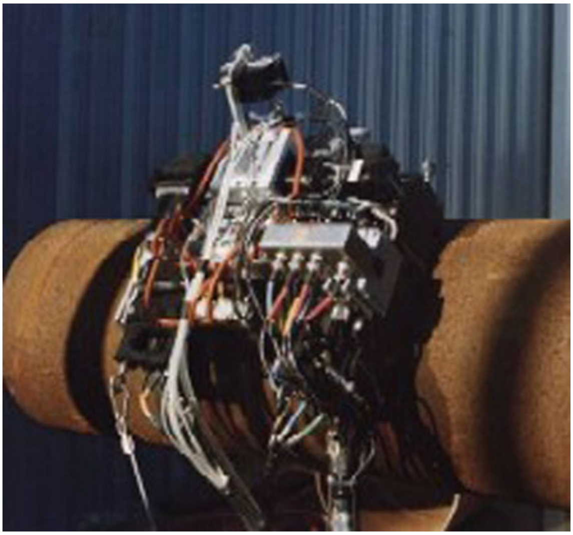
SRA employs the use of probabilistic fracture mechanics techniques to calculate the failure probability as a function of time, including the effects of inspection frequency, probability of detection (POD) and degradation mechanism. Through Monte Carlo sampling, the results of tracking a very large number of crack simulations can be used to determine what fraction of cracks will not be detected and repaired before failure results. This methodology provides models for determining the crack growth for different degradation mechanisms also. These models are computationally intensive. The results of these analyses are often driven by uncertainties in defining crack size distribution, stress history, detection probability and reference flaw size. Some models are available for incorporating ISI as discussed in preceding section and not amenable for various issues arising in maintenance activities. In Statistical approach, databases are an important source of information that can support the estimation. Database should comprise the cause of failure, thereby backtracking to the applicable degradation or damage mechanism, which culminated in the pipe failure. There are various problems associated with database ranging from reporting the event to the appropriate root cause analysis of each event reported. Also how far the effect of life management programme can be incorporated is still under review.

12.5.2.1 In-Service Inspection

Nondestructive Testing (NDT), Nondestructive Inspection (NDI) and Nondestructive Evaluation (NDE) denote variations in application of materials evaluation technology that range from process control to the measurement of a material characteristic that is critical to the structural integrity and safe operating life of an engineering system. Some of the important NDT techniques are:

- Liquid penetrant inspection;
- Magnetic particle inspection;

Fig. 12.12 NDT on piping



- Radiographic inspection (X-ray and gamma ray);
- Electromagnetic inspection;
- Ultrasonic inspection; and
- Thermographic inspection.

Figure 12.12 shows a picture of inspection on piping. Non-Destructive Testing (NDT) carries an important role in predicting the piping failure frequency. Depending on the technique used the confidence of finding defects varies. If any defect is detected, decision will be taken to undertake repair activity in piping. This will decrease the piping failure frequency and should be accounted for. The efficiency of inspection is quantified through the introduction of the concept of "Probability of Detection (POD)". The *POD* concept and methodology have gained widespread acceptance and continuing improvements have enhanced its acceptance as a useful metric for quantifying and assessing NDE capabilities [26]. Since a wide range of NDE methods and procedures are used in "fracture control" of engineering hardware and systems, a large volume of POD data has been generated to validate the capabilities of specific NDE procedures in a multitude of applications. Figure 12.13 presents a typical POD curve obtained from ultra sound inspection. Sometimes it will generate POD curves for the site equipments. In such cases, models are also developed for determining POD.

Failure parameter of the component gets modified according to the type and frequency of inspection applied on it. Hence, it is essential to account for the frequency of inspection and the type of inspection adopted for a component, while suggesting its failure probability/frequency.

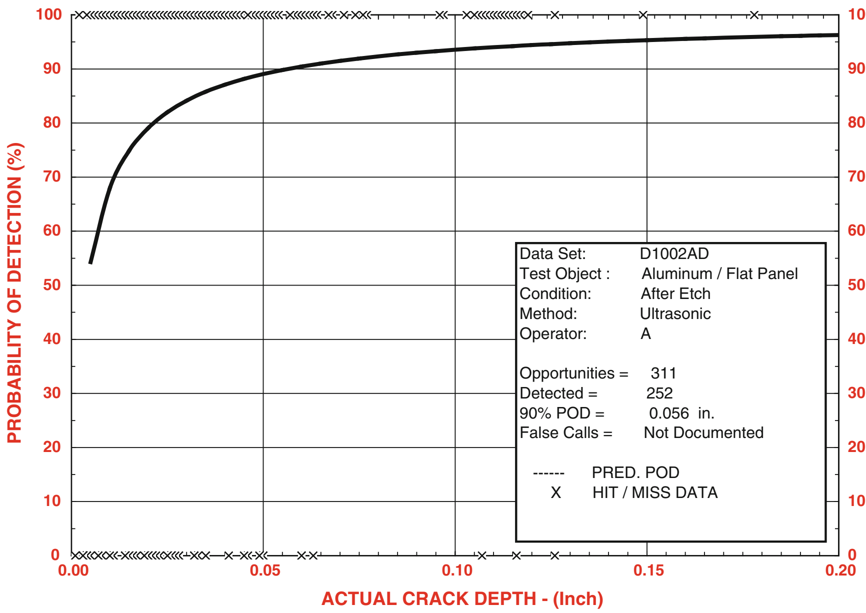


Fig. 12.13 A typical POD curve obtained from ultra sonic inspection

12.5.2.2 Models for Including ISI Effect on Piping Failure Frequency

Various issues are involved in realistic estimation of probability of failure like incorporating the effects of degradation mechanisms acting on it, repair activities, etc. In the context of RI-ISI [27], the models for piping failure probability estimation needs to incorporate the effects of In-Service Inspection frequency, inspection technique involved etc. The above methods incorporate this information in a manner, which is not amenable for RI-ISI. A suitable model needs to be devised which can be used flexibly to study the effects of inspection interval and techniques. Markov model has been found to be a suitable candidate to study these effects, which can be represented as a state–transition problem.

Piping failure analysis has always been a controversial topic. The unavailability models for active components comprises of failure rate, mission time, repair and maintenance parameters acting on it. The reliability model of piping systems should meet the following objectives:

- Account for statistical evidence and engineering insights from service experience accumulated through several thousand reactor years of commercial nuclear power plant operating experience.
- Predict the impacts that changes in the in-service inspection program may have on the frequency of pipe ruptures. These changes include adding and removing locations from the inspection program, changing from fixed to randomly selected locations from one inspection interval to the next, and qualitative

enhancements to the inspection process that could influence the non destructive examination (NDE) reliability of a given inspection.
- Account for the full set of pipe failure mechanisms found in the service experience including those due to active degradation mechanisms, severe and normal loading conditions and combinations of degradation and loading conditions.
- Account for leak before break characteristics of pipe failure modes when appropriate and also account for the possibility to detect and repair a leaking pipe before it degrades to rupture.
- Address uncertainties in the reliability assessment and database development and account for uncertainties in estimating pipe rupture, core damage frequency and large early release frequencies.
- The models and databases to address the above issues should be provided in forms that can be easily applied by utility personnel in implementing a risk informed evaluation of the piping inspection program.

During an independent review of the EPRI RI-ISI procedures, an approach to piping reliability assessment was envisioned. This approach makes use of a reliability modeling technique, Markov modeling [28]. A Markov model of a system is defined by assigning two or more discrete states that the system may occupy at any point in time. Transition is permitted from state to state to account for the occurrence of component failures and the possibility that failed components may be repaired. The model is used to develop a set of differential equations, the solution of which is the time dependent probability that the system occupies each state. Other reliability metrics such as system failure rate or hazard rate can also be derived from this model.

In applying the concept to pipes, it was seen that there are natural states that can be assigned to each element of the pipe, such as each weld and each small section of piping material. These states correspond to discreet levels of degradation such as flaw, crack, leak or rupture as well as the state where the pipe is free of any damage or degradation. The processes that can be modeled in this application of the Markov model include piping degradation either progressively from flaw to leak to rupture, or instantaneously to leak or rupture from any less severe state. The model can also treat the repair processes associated with inspection and detection of critical flaws, detection of leaks, and repair of the damaged pipes prior to occurrence of rupture.

The successful application of the Markov modeling process requires application of the following steps:

1. Development of an appropriate set of states and state transition possibilities.
2. Definition of the transition rate parameters that dictate the probability of transition from state to state
3. Development of the differential equations for the Markov model and solution of these equations for the time dependent probability of occupying each state.
4. Development of a hazard rate function to develop the time dependent frequency of pipe ruptures
5. Development of models for estimating the parameters of the Markov model in terms of observable quantities and reasonable and supportable assumptions.

These models include the development of uncertainty distributions for each of the parameters that capture key uncertainties in the degradation processes and in the interpretation of the service experience.

6. Development of a method of integrating the models from different pipe elements and segments into an overall model for a system for application of risk informed inspection programs.

Discrete State Markov Model for pipe failures

The objective of Markov modeling approach is to explicitly model the interactions between degradation mechanisms and the inspection, detection, and repair strategies that can reduce the probability that failure occurs or the failure will progress to rupture. This Markov modeling technique starts with a representation of "piping segment" in a set of discrete and mutually exclusive states. At any instant of time, the system is permitted to change state in accordance with whatever competing processes are appropriate for that plant state. In this application of Markov model the state refers to various degrees of piping system degradation or repairs, i.e., the existence of flaws, leaks, or ruptures. The processes that can create a state change are failure mechanisms operating on the pipe and process of inspecting or detecting flaws and leaks, and repair of damage prior to progression of failure mechanism to rupture.

Three state Markov model

This model would be applied to a pipe element such as a weld or small section of pipe that is uniquely defined in terms of the presence or absence of degradation mechanisms, loading conditions, and status in the inspection program. The model in Fig. 12.14 is developed to examine the singular role of the in-service inspection program, which can influence the total failure rate of pipe segments but has little if

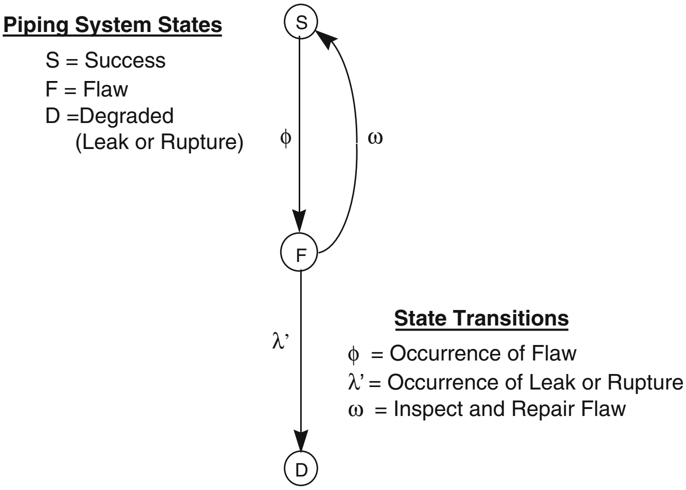


Fig. 12.14 Three state Markov model

any impact on the conditional probability that a failure will be a rupture. A limitation of this model is that it does not distinguish between leaks and ruptures, cannot model leak before break, and cannot be used to examine the role of leak detection as a means to reduce pipe rupture frequencies. Another limitation is that leaks and ruptures are only permitted once the system is in the flaw state. This limitation make the model suitable for degradation type failure mechanisms, but not for severe loading condition related causes such as vibration fatigue or water hammer. These limitations are removed in the next section in which a four state model is developed and more possibilities are introduced for leaks and rupture transitions from the success state. However, to build up the knowledge about pipe reliability modeling in a step by step fashion, this has been found instructive to analyze this more simplified model to understand some basic properties of this approach to reliability modeling such that the necessary details can be built up in an organized fashion.

The relative frequency of pipe ruptures to pipe failures is only a function of the specific failure mechanism that caused the failure as reflected by the "leak before break" characteristic of the failure, and the capability to detect an initially leaking pipe and repair it prior to further degradation to rupture, which in many cases is virtually instantaneous. The model in Fig. 12.14 will also enable us to determine the time dependent failure frequency of piping systems subject to inspections. Hence, the simplified model in Fig. 12.14 is adequate to study the impact of changes in the inspection program on the failure frequency of piping systems. As long as changes to the leak detection part of the problem are not affected, one can solve this model for the pipe rupture failure probability and frequency, and use estimates of the conditional probability of pipe ruptures given failures to obtain the corresponding pipe rupture probabilities and frequencies.

Differential Equations and Solution for Markov Model

The differential equations for the model in Fig. 12.14 are given by:

$$\frac{dS}{dt} = -\phi S + \omega F \tag{12.18}$$

$$\frac{dF}{dt} = \phi S - (\lambda' + \omega)F \tag{12.19}$$

$$\frac{dD}{dt} = \lambda' F \tag{12.20}$$

The left hand side of each equation represents the rate of change of the probability that the system occupies each state, S for the probability of success, F for the probability of a flaw and D for the probability of a degraded state, i.e., leak or rupture. The Greek letters are the parameters of the model as defined in Fig. 12.14. φ is the occurrence rate for flaws, $\lambda^{'}$ is the occurrence rate for leaks and ruptures given a flaw, and ω is the rate at which flaws are inspected, detected and repaired. The rate of leaks and ruptures, $\lambda^{'}$ can be further decomposed by:

$$\lambda' = \lambda_L + \lambda_c \tag{12.21}$$

where

λ_L Occurrence rate of leaks given from a flaw state
λ_C Occurrence rate of ruptures given a flaw state

Hence, the total pipe failure rate given a flaw used in Fig. 12.9 corresponds to the sum of the leak and rupture failure rates and the rates are conditional on the existence of a flaw.

The solution of the system of Eqs. (12.18)–(12.20) can be obtained using Laplace transforms or other suitable technique so long as the boundary conditions are specified. Since for safety related piping, all are inspected to be free of detectable flaws at the beginning of commercial operation the appropriate boundary conditions are:

$$S\{t = 0\} = 1$$
$$D\{t = 0\} = F\{t = 0\} = 0$$

The time dependent solutions for the state probabilities are given by:

$$D\{t\} = 1 - \frac{1}{(r_1 - r_2)}\left(r_1 e^{r_2 t} - r_2 e^{r_1 t}\right) \tag{12.22}$$

$$F\{t\} = \frac{\phi}{(r_1 - r_2)}\left(e^{r_1 t} - e^{r_2 t}\right) \tag{12.23}$$

$$S\{t\} = 1 - D\{t\} - F\{t\} = \frac{1}{(r_1 - r_2)}\left[(r_1 + \phi)e^{r_2 t} - (r_2 + A)e^{r_1 t})\right] \tag{12.24}$$

where the terms *A*, r_1, and r_2 are defined according to:

$$A = \phi + \lambda' + \omega \tag{12.25}$$

$$r_1 = \frac{-A + \sqrt{A^2 - 4\phi\lambda'}}{2} \tag{12.26}$$

$$r_2 = \frac{-A - \sqrt{A^2 - 4\phi\lambda'}}{2} \tag{12.27}$$

Hazard Rate for Markov Model

In a PSA model, pipe failures in process systems are normally represented as initiating events. The quantity needed for this case is the initiating event frequency, or pipe failure frequency. These initiating event frequencies are normally assumed constant in PSAs. With the Markov model, it is not necessary to make this

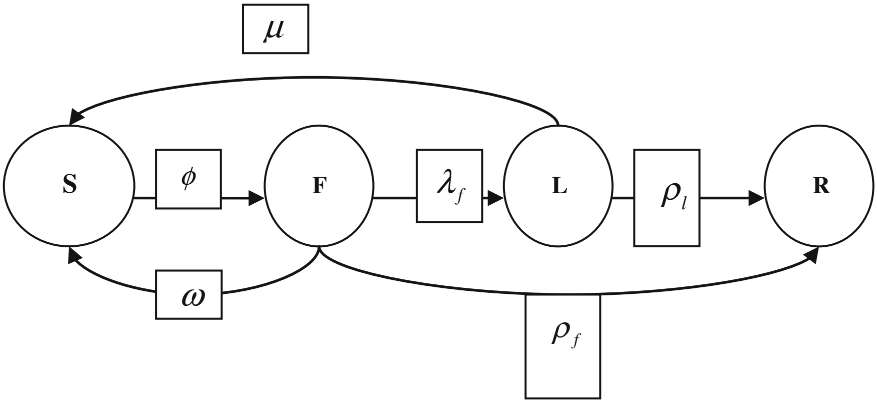


Fig. 12.15 Markov model for pipe elements with in-service inspection and leak detection

assumption as whether the failure frequency is constant or not is a byproduct of the particular model. The reliability term needed to represent the pipe failure frequency is the system failure rate or hazard rate, as defined in the following.

To determine the system failure rate or hazard rate we must first determine the system reliability function for this model. Since we are primarily concerned with pipe failures and seek to estimate pipe failure frequencies, we may declare any state except for failure a "success" state, which in this model includes both the success state S and the flaw state F. Using this concept, the reliability function for the Markov model, r{t}, is given by:

$$r\{t\} = S\{t\} + F\{t\} = 1 - D\{t\} \tag{12.28}$$

By definition the hazard function and the reliability function are related according to the following equation:

$$h\{t\} = -\frac{1}{r\{t\}}\frac{dr\{t\}}{dt} = \frac{1}{(1 - D\{t\})}\frac{dD\{t\}}{dt} \tag{12.29}$$

Applying the solution to the Markov model in Fig. 12.14, an expression for the hazard function is developed as follows:

$$h\{t\} = \frac{r_1 r_2 (e^{r_1 t} - e^{r_2 t})}{(r_1 e^{r_2 t} - r_2 e^{r_1 t})} \tag{12.30}$$

Taking the limit of Eq. (12.28) as t → infinity provides us the long term steady state hazard rate, h_{SS} as:

$$h_{SS} = -r_1 = \frac{A - \sqrt{A^2 - 4\phi\lambda'}}{2} = \frac{(\phi + \lambda' + \omega) - \sqrt{(\phi + \lambda' + \omega) - 4\phi\lambda'}}{2} \tag{12.31}$$

The model in Fig. 12.14 has now been completely solved for its state probabilities and failure frequencies and is now available for use. Quantification can be completed once the parameter values are estimated for use in specific applications. These equations can be used to compute point estimates of state probabilities and failure frequencies as a function of time, and for use in uncertainty analysis in which uncertainty distributions for each parameter is propagated through the equations in a Monte Carlo Sampling process.

Four State Markov Model

This model consists of four states of pipe segment reflecting the progressive stage of pipe failure mechanism: the state with no flaw, development of flaws or detectable damage, the occurrence of leaks and occurrence of pipe ruptures (Fig. 12.15). As seen from this model pipe leaks and ruptures are permitted to occur directly from the flaw or leak state. The model accounts for state dependent failure and rupture processes and two repair processes. Once a flaw occurs, there is an opportunity for inspection and repair to account for in-service inspection program that search for signs of degradation prior to the occurrence of pipe failures. Here the Leak stage L does not indicate actual leak, but represents a stage in which remaining pipe wall thickness is 0.45 × t–0.2 × t (pipe wall thickness).

S Success (depth of corrosion less than 0.1253t).
F Flaw (depth of corrosion is 0.1253t–0.453t).
L Leak stage (depth of corrosion is 0.453t–0.83t)
R Rupture (depth of corrosion beyond 0.83t).
t pipe wall thickness.

$$\begin{bmatrix} P'_s \\ P'_f \\ P'_l \\ P'_R \end{bmatrix} = \begin{bmatrix} -\phi & \omega & \mu & 0 \\ \phi & -\left(\omega + \lambda_f + \rho_f\right) & 0 & 0 \\ 0 & \lambda f & -(\mu + \rho_l) & 0 \\ 0 & \rho_f & \rho_l & 0 \end{bmatrix} \begin{bmatrix} P_s \\ P_f \\ P_l \\ P_R \end{bmatrix} \tag{12.32}$$

The Markov model diagram describes the failure and inspection processes as discrete state-continuous time problem. The occurrence rates for flaw, leaks and ruptures are determined from limit state function formulation. The repair rates for flaws and leaks are estimated based on the characteristics of inspection and mean time to repair flaws and leak upon detection. Setting up differential equations for different states and finding the associated time dependent state probabilities can solve the Markov model. These equations are based on the assumption that the probability of transition from one state to another is proportional to transition rates indicated on the diagrams and there is no memory of how current state is arrived at. Assuming the plant life of 40 years, state probabilities are computed at the plant life.

12.5.2.3 Case Study

The PHWR outlet feeder piping system is taken as a typical case study. There are 306 number of small diameter pipes of diameter ranging from 40 to 70 mm and length 2–22 m that connects coolant channels to the outlet header. The feeder pipe considered in this case study is made of carbon steel A106GrB, with a diameter (d) of 70 mm and thickness (t) of 6.5 mm. After estimating the degradation rate, it has to be applied in the suitable limit state function to estimate the failure probability.

Assumptions

1. It has been assumed that Erosion-Corrosion is present in outlet feeder.
2. A representative value has been assumed for corrosion rate.
3. To estimate the failure probability using FORM, normal distribution has been assumed for all the variables.

Consequence Analysis of Feeder Failure
The coolant channels are connected via individual feeder pipes to headers at both ends of the reactor. Figure 12.16 presents the schematic of Primary Heat Transport System, which includes feeder connections. Since feeder failure can result in Small Loss of Coolant Accident (SLOCA), it can be termed as an Initiating Event (IE). From the failure probability obtained from Markov models explained in previous sections, the IE frequency can be estimated using the equation given below:

$$Failure\ Rate_{IE,feeder1} = \frac{Failure\ Probability_{IE,feeder1}}{EOL} \tag{12.33}$$

where, EOL is the number of years the plant is licensed (e.g. 40 years).

In the event of feeder failure, Emergency Core Cooling System (ECCS) will be actuated. The ECCS is designed to provide enough coolant to the PHT system and to transport heat from the core to the ultimate hat sink in such a way as to ensure adequate reactor core cooling during all phases of LOCA. Event tree is drawn for this IE (Fig. 12.17) and accident sequences are found which can lead to core damage because of this IE. CDF due to the specific IE is estimated by adding the accident sequence frequencies from the IE.

Conditional Core Damage Probability ($CCDP_i$) for a component failure can be directly obtained from the PSA results, by dividing the CDF due to the specific IE by the frequency of that IE.

$$CCDP_i = \frac{CDF_{due\ to\ IE}}{IE_{frequency}} \tag{12.34}$$

For the case of SLOCA, there are three accident sequences viz., sequence number 4, 6 and 18, from this IE, which can result in Core Damage. The CCDP due to SLOCA is found to be 8.835E-06, which falls in medium category in risk matrix.

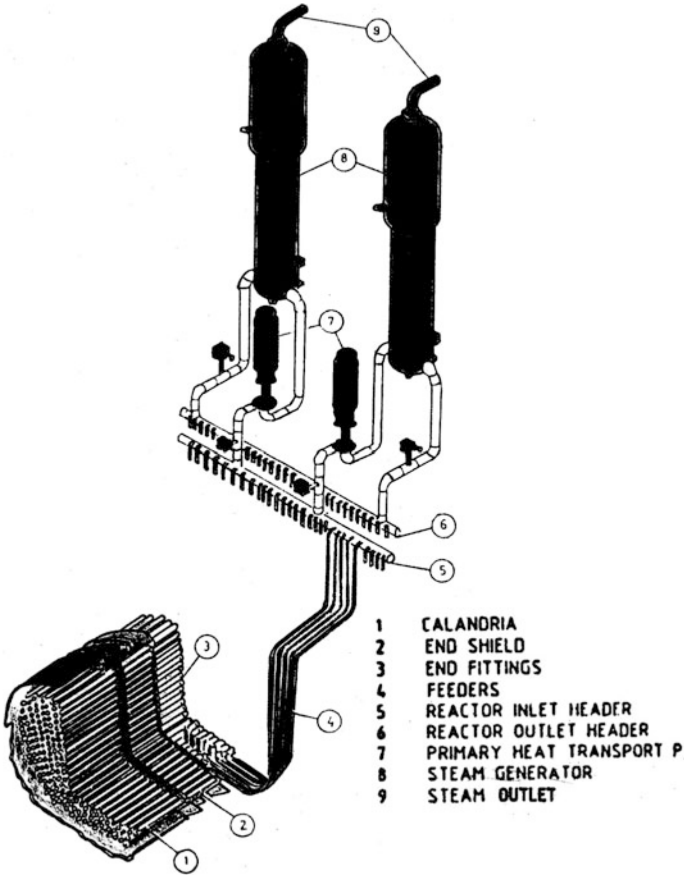


Fig. 12.16 Schematic of primary heat transport system

12.5.2.4 Using Three-State Markov Model

For three-state Markov models, three transition rates are involved as shown in Fig. 12.14. The first transition rate φ representing the occurrence of flaw, can be found out from limit state function or statistical method. However, in this case study a limit state function has been defined. Success State S represents a situation, in which flaw is less than 0.125 × t, and flaw state, F represents a situation,in which flaw is 0.45 × t. ϕ represents transition rate from state S to state F. The limit state function can be defined as

$$\mathrm{G1(d,\ T)} = 0.45 \times \mathrm{t} - (\mathrm{d} + \mathrm{rate} \times \mathrm{T}) \tag{12.35}$$

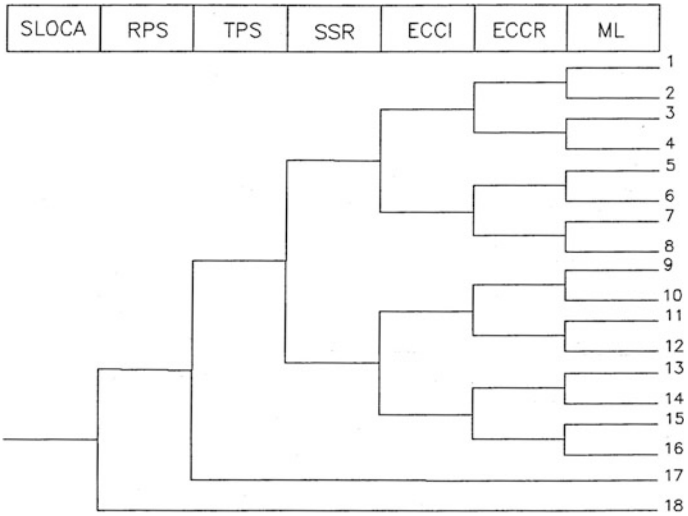


Fig. 12.17 Event tree for small LOCA

d undetected flaw = 0.125 × t.
T time of inspection usually 10 years.
Rate Erosion-corrosion rate (mm/year)

Corrosion rates can be established either from the operating experience or from models available in literature.

Table 12.15 presents mean and variance values for various parameters appearing in the limit state functions.

Next transition rate is defined as Occurrence of degraded state, represented by λ'. Degraded can be referred as either leak state or rupture state. the equation has already been given in Eq. 12.21. For parameters like λ', λ_L and $\lambda_{C,}$ we can apply the statistical model like Thomas model. Thomas defined the following relationship between the frequency of catastrophic rupture (λ_C) and frequency of leakage (λ_L);

$$\lambda_C = \lambda_L 3P(C|L) \tag{12.36}$$

where, P(C|L) is the conditional probability of rupture given leakage.

Table 12.15 Parameters for failure pressure model with mean and variance

Parameters	Mean Values	Variance
Thickness of the pipe (mm)	7	0.148
Outer diameter of the pipe (mm)	72	1.5
Rate of erosion corrosion (mm/year)	0.051	0.015
Time (year)	40	
Length of defect (mm)	300	

P(C|L) has been assumed to be 0.02, considering erosion-corrosion as the dominant degradation mechanism present in the feeder.

λ′ can also be found out using a limit state function. Typically, when a piping loses its 80 % of wall thickness it is considered to have reached a failed state. So the limit state function can be formulated as

$$\mathrm{G2} = 0.8 \times \mathrm{t} - (0.45 \times \mathrm{t} + \mathrm{rate} \times \mathrm{T}) \tag{12.37}$$

Third state is the transition from flaw state to success state. This occurs when that particular piping component is subjected to In-Service Inspection. This has been denoted as ω. This parameter in Markov model that accounts for the inspection process and can be further defined according to the following model.

$$\omega = \frac{P_I P_{FD}}{(T_{FI} + T_R)} \tag{12.38}$$

where

P_I probability that a piping element with a flaw will be inspected per inspection interval. In the case where inspection locations are inspected at random, this parameter is related to the fraction of the pipe segment that is inspected each interval and the capability of the inspection strategy to pinpoint the location of possible flaws in the pipe. When locations for the inspection are fixed, this term is either 0 or 1 depending whether it is inspected or not. This probability is conditioned on the occurrence of one or more flaws in the segment.

P_{FD} probability that a flaw will be detected given this segment is inspected. This parameter is related to the reliability of NDE inspection and is conditional on the location being inspected having an assumed flaw that meets the criteria for repair according to the ASME code. This term is often referred to as the “probability of detection” or POD.

T_{FI} mean time between inspections for flaws, (inspection interval)

T_R mean time to repair once detected. There is an assumption that any significant flaw that is detected will be repaired.

The software package for structural reliability analysis, STUREL has been used to estimate the failure probabilities from the limit state functions. The solutions are obtained from COMREL module of STUREL which are used to estimate the various transition rates, φ and λ′. Alternatively, λ′ has been estimated using Thomas model also. These results are presented in Table 12.16. These transition rates are applied on Markov model shown in Fig. 12.14. Software MKV 3.0 by ISOGRAPH is used for determining the various state probabilities in the Markov model, as shown in Table 12.17.

The unavailability graph for three state Markov model, considering the degraded state as unavailable for Thomas model and G function are given in Figs. 12.18 and 12.19 respectively. The failure frequency of the three state Markov model for Thomas model and G function are depicted in Figs. 12.20 and 12.21 respectively.

Table 12.16 Transition rates used in three state Markov model

Parameters	Values (/year)	Remarks
ϕ	3.812×10^{-4}	G-1
λ'	$\lambda_L = 8.76\text{E-}06$	Thomas model
	$\lambda_C = 1.75\text{E-}07$	
	0.115E-07	G-2 model
ω	0.09	90 % POD in 10 years ISI

Table 12.17 State probabilities

States	State probability (Thomas)	State probability (G)
Success (S)	0.9959	0.9959
Flaw (F)	4.1E-03	4.1E-03
Degraded (D)	1.102E-6	1.375E-9

Degraded state probabilities from Thomas model are found for different POD and ISI interval. Figure 12.22 shows the degraded state probabilities for different POD. With no repair transition the probability of feeder in degraded state was found to be 2.711E-6. The probability has been found to be increased to two fold from the probability with 10 years of ISI interval and 70 % POD detection technique.

Final aim of RI-ISI to categorizes the components and assign an appropriate inspection category from Risk matrix. The consequence of failure has already been discussed. It falls in medium category in risk matrix. To analyze the impact of different ISI interval and inspection technique on plant risk, the inspection category for these test cases were found out. It has been found that failure frequencies increase by a factor of 100 when Thomas model is used in place of G function. The results and categories obtained after placing them in Risk Matrix are shown in Tables 12.18 and 12.19 for Thomas model and G function respectively. It can be found that it has not made any change in final inspection category, since the failure frequencies obtained from Thomas model and G function falls in the medium range of failure frequency in Risk matrix.

12.5.2.5 Using Four-State Markov Model

To determine the different transition rates ϕ, λf, ρ_L and ρ_f, limit state functions, based on strength resistance, are used. The first limit state function is defined as the difference between the pipeline wall thickness t and depth of corrosion defect [28]. This limit state function describes the state of depth of the corrosion defects with a depth close to their maximum allowable depth before repair could be carried out that is 85 % of the nominal pipe wall thickness (0.45 × t). The probability that pipe fall thickness reduces to 0.45 × t will occur at a rate, ϕ, which is defined as occurrence of flaw. So, ϕ represents transition rate from state S, in which flaw is less

Fig. 12.18 Unavaila. from Thomas model

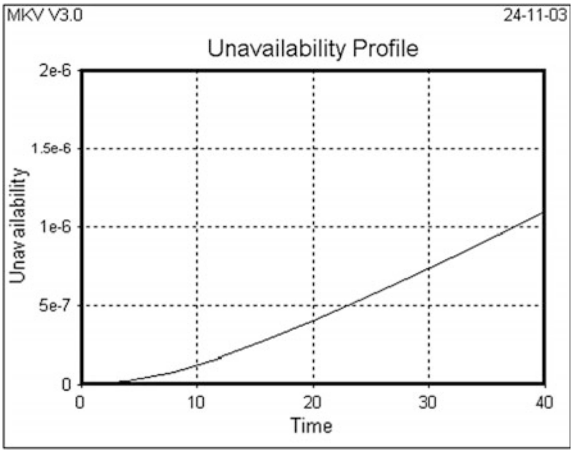
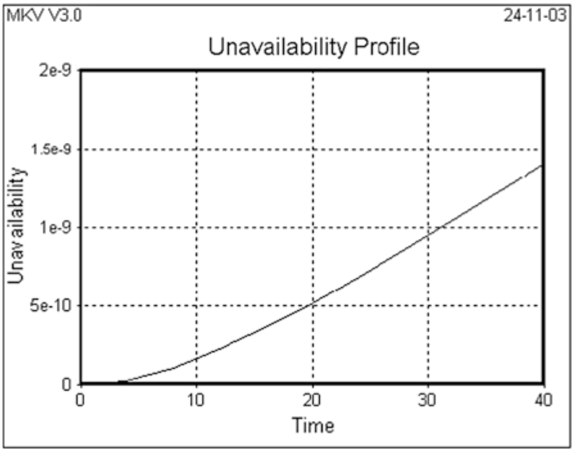


Fig. 12.19 Unavaila. from G function model



than 0.125 × t, to state F in which flaw is 0.45 × t. The limit state function has already been defined in Eq. 12.35.

The second limit state function is formulated to estimate the transition rate λ_f. λ_f represents transition rate from state F, which is already crossed the detectable range i.e., 0.45 × t, to the leak state L, i.e. 0.8 × t. The G for this case will be the same as given in Eq. 12.39.

There is a probability for the piping reaching directly the rupture state, R from the flaw state, F, because of encountering the failure pressure in the flaw state. For this case, a different limit state function needs to be formulated. The third limit state function is defined as difference between pipe line failure pressure P_f and pipeline operating pressure P_{op} [28].

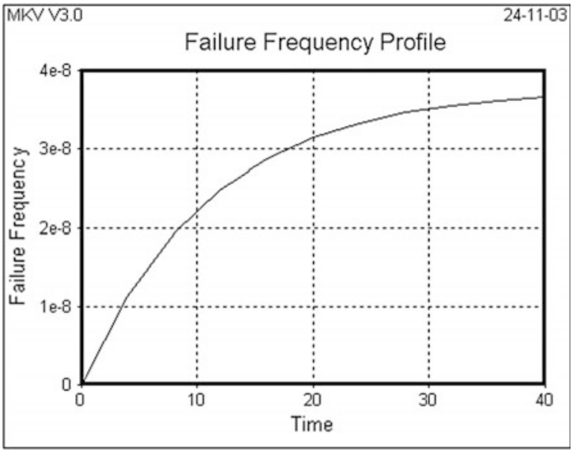


Fig. 12.20 Failure freq.—Thomas model

$$G3(P_f) = P_f - P_{op} \tag{12.39}$$

ω is the parameter in Markov model that accounts for the inspection process and can be further defined according to the following model given in Eq. 12.38. Another parameter is introduced in Four state Markov model to represent the leak repair. Repair rate

$$\mu = P_{LD}/(T_I + T_R) \tag{12.40}$$

P_{LD} probability that leak in the element will be detected per detection period (Typically assumed as 0.9)

Table 12.20 presents mean and variance values for various parameters appearing in the limit state functions.

The software package for structural reliability analysis, STUREL has been used to estimate the failure probabilities from the limit state functions. The solutions are obtained from COMREL module of STUREL, which are used to estimate the various transition rates, and are presented in Table 12.21. These transition rates are applied on Markov model shown in Fig. 12.15. Software MKV 3.0 is used for determining the various state probabilities in the Markov model, as shown in Table 12.22. Modified B31G estimates are considered for ρ_f and ρ_l in Markov model.

Depending on our definition of failure, state probability of either the leak state or the rupture state, can be considered as failure probability of the feeder. The failure frequency of the feeder can be estimated by dividing this probability by the design life of the component, which value can be further employed in RI-ISI for determining its inspection category for In-Service Inspection. The unavailability graph for four state

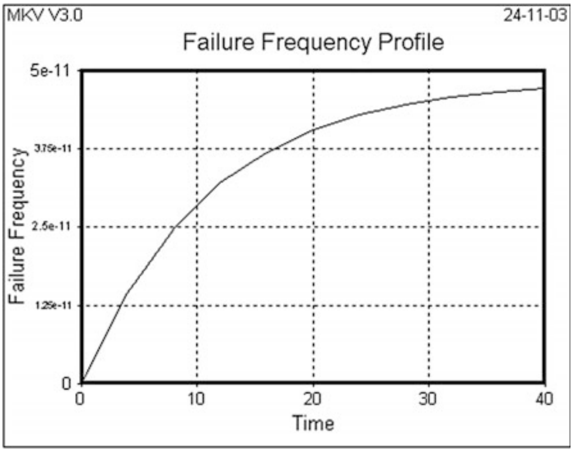


Fig. 12.21 Failure Freq.—G function model

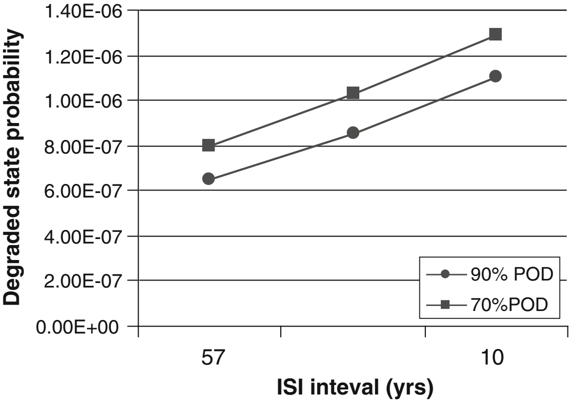


Fig. 12.22 Impact of inspection and repair strategies on piping failure probability

Table 12.18 Risk matrix category for Thomas model

ISI interval	90 % POD		70 % POD	
	Freq (/year)	Category	Freq (/year)	Category
5	1.63E-8	6	1.995E-8	6
7	2.13E-8	6	2.575E-08	6
10	2.55E-8	6	3.225E-8	6

Table 12.19 Risk matrix category for G model

ISI interval	90 % POD		70 % POD	
	Freq (/year)	Category	Freq (/year)	Category
5	2.1E-11	6	2.57E-11	6
7	2.73E-11	6	3.3E-011	6
10	3.55E-11	6	4.15E-11	6

Table 12.20 Parameters for failure pressure model with mean and variance

Parameters	Mean values	Variance
Yield strength (MPa)	358	25
Thickness of the pipe (mm)	7	0.148
Ultimate tensile strength (MPa)	455	32
Outer diameter of the pipe (mm)	72	1.5
Rate of erosion corrosion (mm/year)	0.051	0.015
Load (MPa)	8.7	0.9
Time (year)	40	
Length of defect (mm)	300	

Table 12.21 Transition rates obtained from COMREL modules

Parameters	Values (/year)	G method
ϕ	3.812×10^{-4}	G-1
λf	2.435×10^{-5}	G-2
ρ_f	0.115×10^{-7}	G-3: modified B31G
ρ_l	1.486×10^{-2}	G-3: modified B31G

Table 12.22 State probabilities for w = 0.09 and μ = 0.084

States	State probability
Success (S)	0.9956
Flaw (F)	4.362E-03
Leak (L)	9.303E-7
Rupture (R)	3.147E-7

Markov model, considering the rupture state as unavailable is given in Fig. 12.23. The failure frequency of the four states Markov model is depicted in Fig. 12.24.

Various inspection strategies are tried out changing the inspection interval and detection techniques employed. Figures 12.25 and 12.26 present the graphs on the results of these strategies on piping failure probability without and with leak repair respectively.

As per the consequence of failure, it falls in medium category in risk matrix. For different cases of inspection and repair strategies we can find which category the feeder will fall in the Risk matrix. Tables 12.23 and 12.24 provide the piping failure

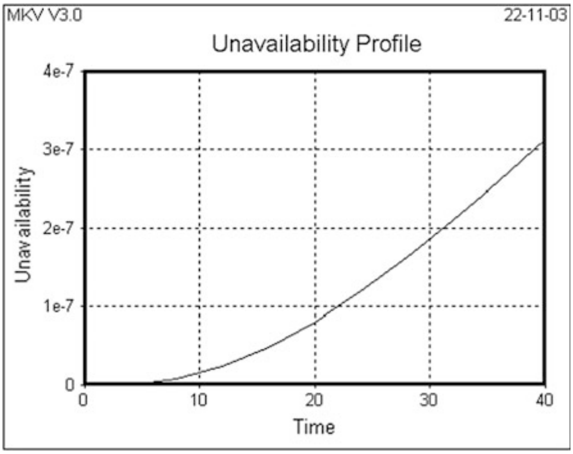


Fig. 12.23 Unavaila. for four state model

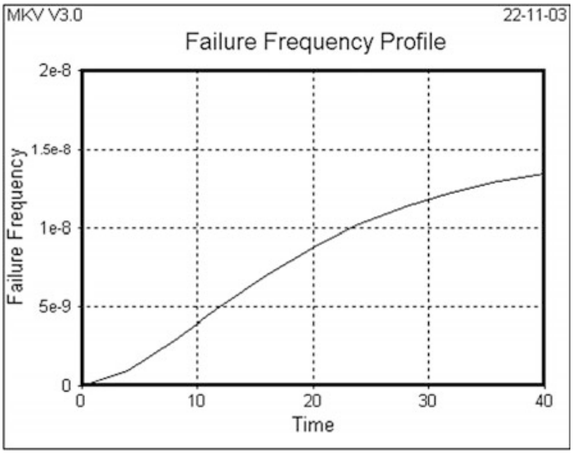


Fig. 12.24 Failure freq. for 4 state model

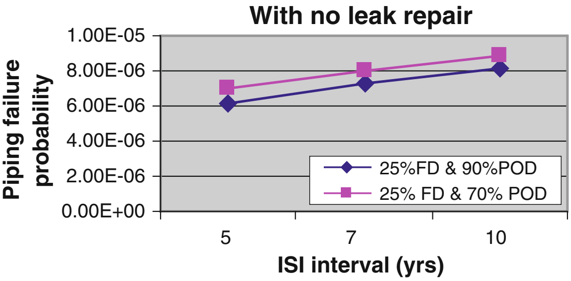


Fig. 12.25 Impact of inspection and repair strategies on piping failure probability with no leak repair

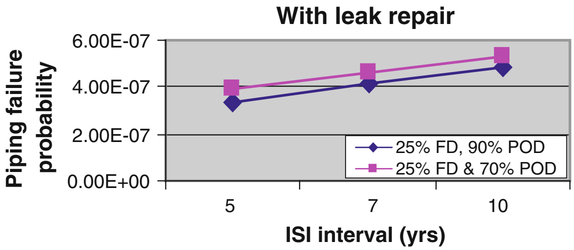


Fig. 12.26 Impact of inspection and repair strategies on piping failure probability with leak repair

frequency, the respective CCDP and inspection category number from risk matrix for different inspection and repair strategies.

LD—Leak Detection, POD—Probability of detection, FI—Flaw inspection.

Remarks on Risk Informed In-Service Inspection

The failure pressure models considered here to define the G function lead to similar failure probabilities for short pipeline service periods. Various parameters are assumed here to be normally distributed, but in actual practice this may not be the case. Instead of applying directly the probabilities obtained from limit state function in RI-ISI evaluation, it is recommended to find the state probabilities using MARKOV model, since it incorporates the effect of repair and inspection works in the pipeline failure frequency. Markov model also allows formulating a proper inspection program and period depending on the operating condition of the plant at any given time.

The ultimate aim of RI-ISI is to optimize the inspection strategies in terms of risk and cost functions. So it is necessary to address the issues involved in conducting ISI like what should be the optimum frequency of inspection without jeopardizing

Table 12.23 Risk Matrix category with leak repair

ISI interval	25 % FD, 90 % POD		25 % FD, 70 % POD	
	Freq (/year)	Category	Freq (/year)	Category
5	8.45E-9	6	9.85E-9	6
7	1.035E-8	6	1.1625E-08	6
10	1.215E-8	6	1.3325E-8	6

Table 12.24 Risk matrix category without leak repair

ISI interval	25 % FD, 90 % POD		25 % FD, 70 % POD	
	Freq (/year)	Category	Freq (/year)	Category
5	1.54E-07	5	1.74E-07	5
7	1.81E-07	5	1.98E-07	5
10	2.05E-07	5	2.2E-07	5

the risk of the plant, what should be inspection technique adopted which will have maximum probability of detection (POD) of flaw, etc. The term μ and ω in the Markov model presented in Fig. 12.15 incorporates ISI frequency and technique respectively. The POD values to be taken for different inspection techniques should be established experimentally taking into consideration, the sensitivity of the equipment used during inspection. There can be a source of uncertainty in POD values, which is assumed to have negligible impact on final failure probability values. It has been seen from Tables 12.23 and 12.24 that the changes in inspection and repair strategies can result in change in inspection category. In addition, it gives a direct indication to its effect on plant risk.

References

1. IAEA (1992) Procedure for conducting probabilistic safety assessment of nuclear power plants (level 1). Safety Series No. 50-P-4, International Atomic Energy Agency, Vienna
2. Bajaj SS, Gore AR (2006) The Indian PHWR. Nucl Eng Des 236(7–8):701–722
3. BARC (1996) Level 1 PSA report. Bhabha Atomic Research Centre, internal report, Mumbai
4. USNRC (1975) Reactor safety study, an assessment of accident risk in U.S. commercial nuclear plants. Appendix III, Failure Data, Appendix IV, Common Mode Failures. USNRC WASH 1400
5. IAEA Safety Series no 50-SG-D11, Safety guides-General design safety principles for NPPs. IAEA, Vienna
6. Systematic Human Action Reliability Procedures (SHARP) (1984) EPRI-NP-3583
7. CANDU safety research—a status report. In: Second annual conference, Canadian Nuclear Society, June 1981, Hancox, WT
8. Safety research for CANDU reactors. In: IAEA technical committee meeting on thermal reactor safety research, Moscow, Dec 1981, Hancox, WT
9. Samanta PK (1992) Optimisation of technical specifications applications in USA, Lecture 54.4.4, IAEA course: use of PSA in the operation of NPPs
10. Martorell S, Carlos S, Sanchez A, Serradell V (2001) Constrained optimization of test intervals using steady-state genetic algorithms: application to safety systems. Reliab Eng Syst Saf 72:59–74
11. Vinod G, Kushwaha HS, Verma AK, Srividya A (2004) Optimization of ISI interval using genetic algorithms for risk informed in-service inspection. Reliab Eng Syst Saf 86:307–316
12. Vaurio JK (1995) Optimization of test and maintenance intervals based on risk and cost. Reliab Eng Syst Saf 49:23–36
13. Munoz A, Martorell S, Serradell V (1997) Genetic algorithms in optimizing surveillance and maintenance of components. Reliab Eng Syst Saf 57:107–120
14. Vaurio JK (1999) Availability and cost functions for periodically inspected preventively maintained units. Reliab Eng Syst Saf 63:133–140
15. Goldberg DE (1989) Genetic algorithm in search, optimization, and machine learning, reading. Addison-Wesley, Reading
16. Durga Rao K, Gopika V, Kushwaha HS, Verma AK, Srividya A (2007) Test interval optimization of safety systems of nuclear power plant using Fuzzy-Genetic approach. Reliab Eng Syst Saf 92(7):895–901
17. IAEA (1994) Advances in reliability analysis and probabilistic safety assessment for nuclear power reactors. IAEA TECDOC-737, Vienna
18. ASME Code CASE N-560, Alternative examination requirements for class1, Category B-J Piping welds

19. ASME Code CASE N-578, Risk informed methods for in-service inspection of pipe welds
20. Balkey KR, Closky NB, Phillips JH (1997) Developments on USNRC-approved WOG/ASME research risk informed in-service inspection methodology. Westinghouse Energy Systems
21. Balkey et al (1998) ASME risk-based in-service inspection and testing: an outlook for the future. Risk Anal 18:407–421
22. EPRI, USNRC (1999) Risk informed in-service inspection evaluation procedure. TR-112657
23. COMED (2000) Risk informed in-service inspection evaluation. Engineering and Research Inc
24. NUREG-1661, Technical elements of risk informed in-service inspection for piping
25. USNRC (1998) An approach for plant specific risk informed decision making: in-service inspection, USNRC
26. Rouhan A (2002) Reliable NDT data for risk based inspection for offshore structures. In: Proceedings of the 3rd European–American workshop on reliability of NDE and demining, Berlin
27. RIBA Project (2001) Risk informed approach for in-service inspection of nuclear power plant components. EUR 20164 EN, Project Summary
28. Fleming KN, Gosselin S, Mitman J (1999) Application of Markov models and service data to evaluate the influence of inspection on pipe rupture frequencies. In: Proceedings of the ASME pressure vessels and piping conference, Boston

Chapter 13
Uncertainty Analysis in Reliability/Safety Assessment

13.1 Mathematical Models and Uncertainties

Model (“the model of the world”) does the structuring of the problem for a physical situation at hand. This may occasionally be referred as the “mathematical model”. There are two types of models of the world, deterministic and probabilistic. Newton’s laws are good examples for deterministic models. Many important phenomena can’t be modelled by deterministic expressions. For example, failure time of equipment exhibit variability that can’t be eliminated; given the present state of knowledge and technology, it is impossible to predict when the next failure will occur. This natural variability (or randomness) imposes the use of probabilistic models that include this uncertainty, which is central to Reliability/Risk analysis of engineering systems. This natural variability is sometimes referred as ‘randomness’ or ‘stochastic uncertainty’, commonly known as ‘aleatory uncertainty’, which can’t be reduced [1, 2].

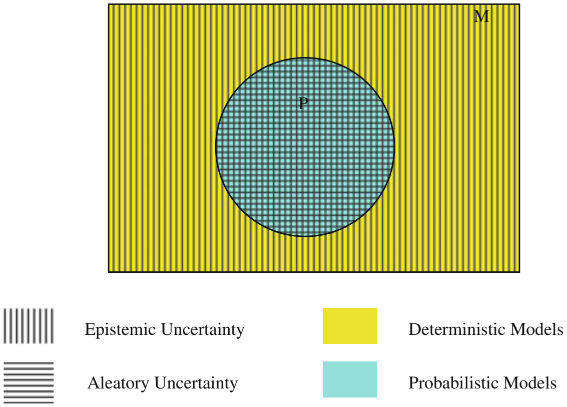
Nevertheless, both deterministic and probabilistic approaches are built on number of model assumptions and model parameters that are based on what is currently known about the physics of the relevant processes and the behavior of systems under given conditions. There is uncertainty associated with these conditions, which depends upon state of knowledge, is referred as ‘epistemic uncertainty’ or ‘subjective uncertainty’. For example, the length of a crack in a pipe line in a plant is not measured precisely due to its inaccessibility. It is clear that crack length is fixed value but not measured due to practical constraints. Model uncertainty is a good example of epistemic uncertainty as it can be reduced with more understanding of physical phenomena. Parameter uncertainty in a random variable also falls in epistemic uncertainty which is not measured precisely due to scarcity or lack of data. It is important that the uncertainties in natural variability of physical processes (i.e., aleatory uncertainty) and the uncertainties in knowledge of these processes (i.e., epistemic uncertainty) are properly accounted for [1, 2]. Table 13.1 gives comparison of both epistemic and aleatory uncertainties.

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_13

Table 13.1 Aleatory versus epistemic uncertainties

Aleatory uncertainty	Epistemic uncertainty
This arises from: Inherent variability, natural stochasticity, environmental or structural variation across space or through time, manufacturing heterogeneity among components and variety of other sources of randomness	*This arises from*: Incompleteness of knowledge, sources of this uncertainty include measurement uncertainty, small sample sizes, detection limits and data censoring, ignorance about the details of physical mechanisms and processes involved and other imperfections in scientific understanding.
Also known as: Randomness, variability, stochastic uncertainty, objective uncertainty, dissonance, or irreducible uncertainty	*Also known as*: Incertitude, ignorance, subjective uncertainty, non-specificity, or reducible uncertainty
Examples: Wind speed, heights or body weights among population, failure times and repair times of equipment	*Examples*: The length of a crack in a pipe line, Model uncertainty, Parameter uncertainty in a random variable
Representation and treatment: Only Probability theory	*Representation and treatment*: Probability theory, Fuzzy Set Theory, Dempster-Shafer Theory

Fig. 13.1 Deterministic and probabilistic models



Considering all mathematical models as a universal set M, probabilistic models are represented as a subset P of universal set M. Deterministic models are compliment of probabilistic models, P. This is represented as shown in Fig. 13.1 Epistemic uncertainty is common to both probabilistic and deterministic models. The vertical lines represent epistemic and horizontal lines represent aleatory uncertainty. It may be noted that the set of probabilistic models (P) have both epistemic and aleatory uncertainties.

Table 13.2 Uncertainties present in an extinction risk analysis for species of owls

	Aleatory uncertainty	Epistemic uncertainty
Model formulation	Do mortality mechanisms change from season to season?	Which model of density dependence should be used?
Parameter values	How does the number of owls vary in different parts of forest?	What is the number of owls present in the forest?

Example for Understanding of Epistemic and Aleatory Uncertainties
Scott and Lev [2] gave a very good example to understand the difference between epistemic and aleatory uncertainties. It is explained here: Table 13.2 gives questions exemplifying these two kinds of uncertainty in two aspects of an extinction risk analysis for an endangered species of owls. The sample questions in the first column refer to variability expressed over time and across space. This column could have been split into two columns to represent temporal and spatial variability separately if one so desired, with obvious examples for each new cell in the table. In fact, because variability can be expressed over almost any dimension, one could have multiplied the number of columns. As all such examples of uncertainty due to variability is put into one column for the sake of simplicity and to draw attention to the fact that the same mathematical techniques are used to propagate uncertainty whether the value changes over time, across space, among individuals or on some other axis of variability.

Epistemicuncertainty arises because of limits on empirical study. For instance, atsome moment in time the number of owls present in a well defined region of forest is a particular number that is not varying. Nevertheless, this number may not be precisely known to us, just because it can be extremely difficult to tally every single bird. This uncertainty is decidedly unlike the uncertainty, say, immortality rates arising from variability of the weather. For instance, ignorance and variability respond differently to empirical effort. Whereas ignorance can usually be reduced by additional study or by improving the techniques of measurement, variability has an objective reality that is independent of empirical study of it. Additional effort may yield a better estimate of the magnitude of variability, but it will not tend to reduce it.

13.2 Uncertainty Analysis: An Important Task of PRA/PSA

PSA is the study aimed at evaluating the risks of a system using probabilistic method. It is a comprehensive, structured approach to identifying failure scenarios, constituting a conceptual and a mathematical tool for deriving numerical estimate of risk. PSA is carried out to assess the level of safety and to aid in ranking safety issues by order of importance. The main benefit of PSA 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, plant operation,

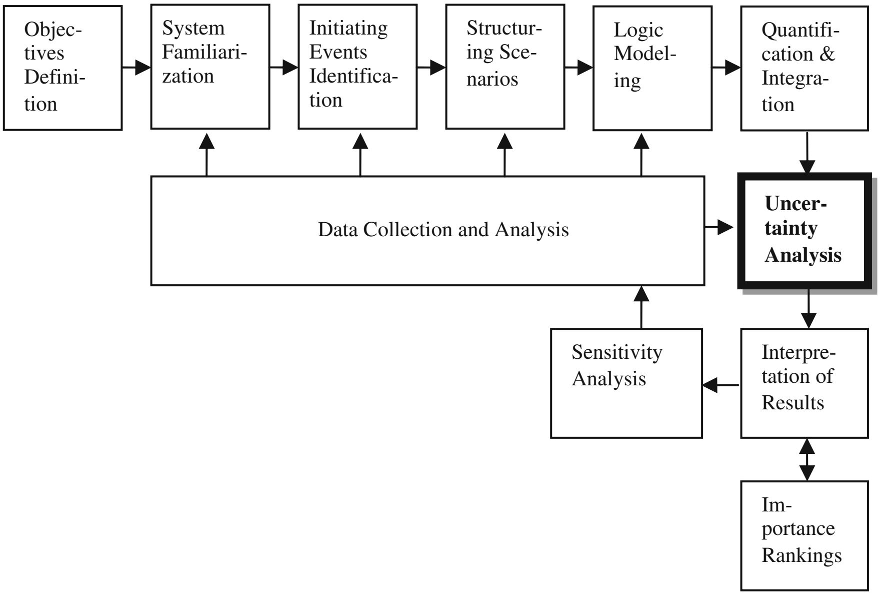


Fig. 13.2 Typical procedure of PRA/PSA., adapted from NASA [1]

safety analysis and on regulatory issues. PSA provides the quantitative estimate of risk which is useful for comparison alternatives in different design and engineering areas. PSA offers a consistent and integrated framework for safety related decision making. Typical procedure for carrying out PRA/PSA as recommended by NASA is shown in Fig. 13.2

Uncertainties are introduced at different stages of PRA (see Fig. 13.2). In the identification of initiating events step, completeness uncertainty will arise. This is because the identified list of initiating events may not be comprehensive. During the accident sequence and system modelling, uncertainty with respect to the mathematical models adopted is introduced as they simulate the reality. In the quantification of risk/reliability measures, uncertainty regarding parameters in the model is identified. Uncertainties are ever present in the PRA process and will by definition affect the practical usefulness of the results. Keeping this in mind, uncertainty analysis is adopted as an important task in the overall procedure of PRA. For example, in the procedure for PRA recommended by NASA [1], refer Fig. 13.2, uncertainty analysis is present after quantification and integration; in PSA procedure recommended for NPP by IAEA [3], step 30 is explicitly on uncertainty analysis.

One could regard uncertainty analysis as having three fundamental purposes as presented by Abrahamsson [4].

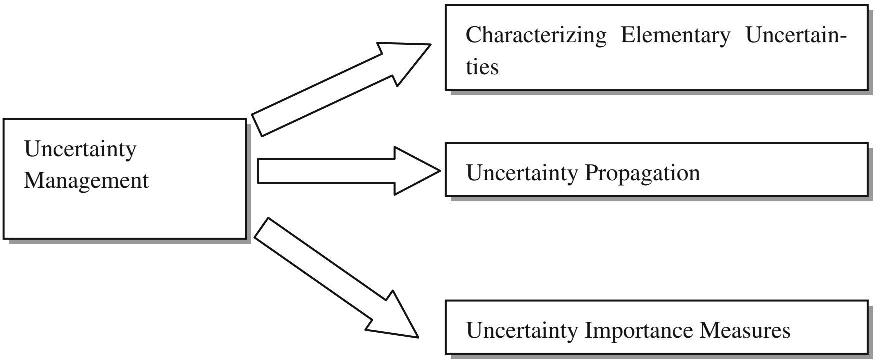

Uncertainty Management
Characterizing Elementary Uncertainties
Uncertainty Propagation
Uncertainty Importance Measures

Fig. 13.3 Tasks involved in uncertainty management

1. It is a question of making clear to the decision maker that we do not know everything, but decisions has to be based on what we have.
2. The task is to try to define how uncertain we are. Is the uncertainty involved acceptable in meeting the decision making situations we face, or is it necessary to try to reduce the uncertainty in order to be able to place enough trust in the information?
3. Try to reduce the uncertainty involved to an acceptable level.

Based on the above mentioned purposes, the problem of uncertainty management in PSA/PRA can be devised as having the following steps (see Fig. 13.3):

(i) Identification and characterising elementary uncertainties
(ii) Uncertainty propagation
(iii) Uncertainty importance measures

13.3 Methods of Characterising Uncertainties

13.3.1 The Probabilistic Approach

The most common approach used to represent uncertainty regarding a quantity, either epistemic or aleatory, is to use probability distributions. Within a Bayesian framework probability distributions for unknown or varying quantities can be constructed using both 'hard' data and subjective judgement. The resulting probability distribution is a representation of assessor's degree of belief regarding the probability of the assessed quantity to take a certain value, see Fig. 13.4. The uncertain quantity T is assumed to be normally distributed with mean = 10 and standard deviation = 0.8. Here, both Probability Density Function (PDF) and Cumulative Distribution Function (CDF) are shown. A description of methods of eliciting information regarding unknown quantities from experts and transforming

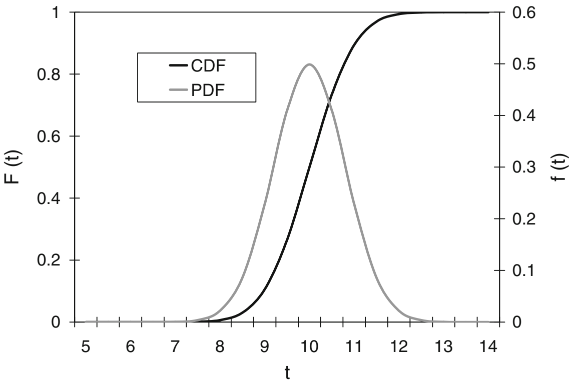


Fig. 13.4 Probabilistic representation of uncertainty

into probability distributions is given in Sect. 13.5. When evidence (for example, operating experience) becomes available, it is natural to change the probability distribution to reflect this new knowledge. The evidence is in the form of statistical observations. The analytical tool for updating probability distributions is Bayes' theorem, is widely used in practice.

13.3.2 Interval and Fuzzy Representation

Interval Representation

The uncertainty in the variables is specified as interval number in this approach. The intervals should represent the absolute bounds of the uncertain parameter that one wants to explore in the analysis. Interval analysis can be used to estimate the possible bounds on model outputs using bounds (intervals) to represent uncertainty about model inputs and parameters.

Fuzzy Representation

Fuzzy arithmetic can be regarded as a generalization of interval analysis in that a fuzzy number can be considered to be a nested stack of intervals, each at a different level of presumption α, $0 \leq \alpha \leq 1$, see Fig. 13.5. The range of values is widest at a presumption or 'possibility' level of zero. Just above α level zero is the interval that everyone would agree contains the true value, i.e. the most conservative range. At a α level of one the most optimistic range of values is given. This range may even be a point, i.e. the best estimate of the value. It is also possible to consider the α level in the following way: $\alpha = 1$ is the range of values that are identified as "entirely possible", while in contrast just above $\alpha = 0$ is the range of values that are "just possible" or only "conceivable".

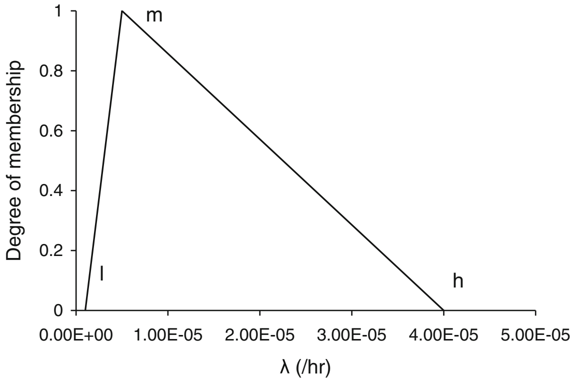


Fig. 13.5 Fuzzy representation of variable λ

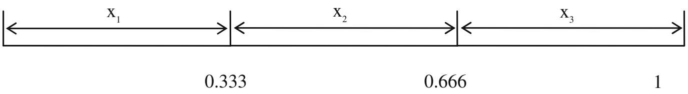


Fig. 13.6 Frame of discernment with elementary intervals

13.3.3 Dempster-Shafer Theory Based Representation

Dempster-Shafer theory also known as Evidence theory was originated by Arthur P. Dempster and it was developed by Glenn Shafer for both aleatory and epistemic uncertainties [5–7]. Evidence theory starts by defining a frame of discernment that is a set of mutually exclusive 'elementary' propositions. Any problem of likelihood takes some possible set as given. The given propositions might be nested in one another or they might partially overlap, however, the finest possible subdivision of the set becomes the 'elementary' proposition. The frame of discernment consists of all finite elementary propositions and may be viewed the same as a finite sample space in the probability theory. In the case of a system reliability modelling problem, uncertainty can exist in the component parameters of an analysis model as epistemic uncertainty. For the uncertain parameter, only interval information may be available as shown in Fig. 13.6, and in this case, the frame of discernment can be given as X = {x_1, x_2, x_3}, where, x_1, x_2, and x_3 are elementary propositions.

Various propositions can be expressed for negation, conjunction, and disjunction to elementary propositions. If we let 2^X denote the power set of X, then 2^X represents all the possible distinct propositions. Hence elementary propositions should be defined in order to reflect all the available evidence within the power set of X, 2^X. The power set of X = {x_1, x_2, x_3} is given as,

$$2^{\mathrm{X}} = \{\emptyset, \{\mathrm{x}_1\}, \{\mathrm{x}_2\}, \{\mathrm{x}_3\}, \{\mathrm{x}_1, \mathrm{x}_2\}, \{\mathrm{x}_2, \mathrm{x}_3\}, \{\mathrm{x}_1, \mathrm{x}_3\}, \mathrm{X}\}$$

Proposition $\{\mathrm{x}_1, \mathrm{x}_2\}$ in the set of 2^{X} means that one and only one of the two propositions is true but we don't know which one is true. Because elementary propositions are selected to be mutually exclusive of each other, the true value of an uncertain parameter is assumed not to be located in both of the elementary propositions.

Basic Belief Assignment (BBA)

In evidence theory, the basic propagation of information is through Basic Belief Assignment (BBA). BBA expresses our degree of belief in a proposition. It is determined by various forms of information, sources, experimental methods, quantity and quality of information and so forth. BBA is assigned by making use of a mapping function of BBA (*m*) to express our belief to a proposition with a number in the unit interval [0, 1]

$$m : 2^{\mathrm{X}} \rightarrow [0, 1]$$

The number *m*(*A*) represents only the *portion* of total belief assigned exactly to proposition *A*. The total belief will be obtained by considering belief and plausibility functions that will be discussed later. The measure *m*, basic belief assignment function, must satisfy the following *three axioms*

(i) $m(A) \geq 0 \; for \; any \; A \in 2^X$

(ii) $m(\emptyset) = 0$

(iii) $\sum\limits_{A \in 2^X} m(A) = 1$

Belief and Plausibility Functions

Due to lack of information, it is more reasonable to present bounds for the result of uncertainty quantification, as opposed to a single value of probability. Our total degree of belief in a proposition '*A*' is expressed within a bound [*Bel*(*A*), *Pl*(*A*)] which lies in the unit interval [0, 1] as shown in Fig. 13.7, where *Bel*() and *Pl*() are given as,

$$\begin{aligned} Bel(A) &= \sum_{c \subset A} m(C) : Belief \\ Pl(A) &= \sum_{c \cap A \neq \Phi} m(C) : Plausibility \end{aligned} \tag{13.1}$$

Bel(*A*) is obtained by summation of the BBAs for propositions that are included in the proposition *A*. With this viewpoint, *Bel*(*A*) is our 'total' degree of belief. The degree of plausibility *Pl*(*A*) is calculated by adding the BBAs of propositions whose

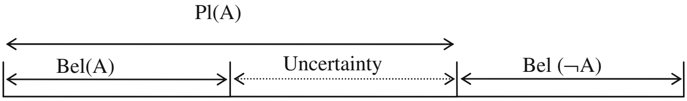


Fig. 13.7 Belief (*Bel*) and plausibility (*Pl*)

intersection with the proposition *A* is not an empty set. That is, every proposition that allows for the proposition *A* to be included at least partially is considered to imply the plausibility of proposition *A*, because BBA in a proposition is not divided in any way to its subsets. These two measurements consist of lower and upper probability bounds.

13.4 Bayesian Approach

Since the equipment failure tends to be a rare event, empirical data for parameter estimation are generally sparse. Classical approach is ill suited for this situation, leading to excessively wide confidence intervals. Partly because of this, most of the risk assessment community has turned to Bayesian analysis, (so called because they employ Baye's Theorem), as a natural means to incorporate a wide variety of information (in addition to statistical data i.e. r failures in n tests) in the estimation process [8].

Bayes's Theorem
The Bayes's theorem can be written as

$$P(A/B) = \frac{P(B/A)P(A)}{\sum_{i=1}^{n} P(A_i)P(B/A_i)} \tag{13.2}$$

Here A represents the proposition of interest and B represents some new information. P(A/B) denotes the analyst's probability for the truth of A, given the new evidence B.

The conditional probability of A, given B, P(A/B), measures the analyst's belief that proposition A is true, given that proposition B is true. Thus, mathematically we write

$$P(A/B) = \frac{P(A \cap B)}{P(B)} \tag{13.3}$$

We have to estimate a parameter θ the proposition typically of the form {θ < parameter value < θ +dθ} and the Baye's theorem takes the form

$$\pi_i(\theta/\mathrm{E}) = \frac{L(E/\theta)\pi_{i-1}(\theta)}{\int L(E/\theta)\pi_{i-1}(\theta)d\theta} \tag{13.4}$$

Here $\pi_i(\theta)$ is analogous to P(A) in the above Eq. 13.4 and it is the prior probability density function for the unknown parameter (prior to obtaining the evidence E). L(E/θ), is analogous to P(B/A), is the likelihood function. It is the conditional probability of observing E, given θ. The left hand side of the Eq. 13.4 π_i (θ/E) is posterior probability density function after E is obtained.

It is extremely important to note that as the amount of the evidence increases, the peak value of the distribution would be same as the parameter value that is obtained from the classical approach.

The following four steps are to be followed in Bayesian estimation [8].

Step 1 Identification of the parameter to be estimated
Step 2 Development of a prior distribution that is obtained from generic data
Step 3 Collection of evidence and construction of appropriate likelihood function
Step 4 Derivation of the posterior distribution using Bayes' Theorem

These concepts are incorporated as follows.
Step1
The two parameters to be estimated are

Failure Rate (λ)
Demand Failure Probability(λ_d)

Step 2
Lognormal distribution is taken as the prior distribution. The parameters taken from generic data are the median and the error factor of the distribution. Error factor is used to find the lower limit and the upper limit of the parameter in the distribution as:

λ_{lower} = Median/(Error factor)
λ_{upper} = Median x Error factor

The whole range is divided into n intervals as shown below:
Delta(δ) = ($\lambda_{\text{upper}} - \lambda_{\text{lower}}$)/n
Lambda values are found out as follows:

$$\lambda_i = (i + 0.5) \times \delta + \lambda_{lower}$$

i varies from 0 to n
The Probability Density Function for lognormal distribution is expressed as:

$$f_d(\lambda_i) = \frac{1}{\sigma\lambda_i\sqrt{2\pi}}\exp(-\frac{1}{2}\left[\frac{\ln\lambda_i - \mu}{\sigma}\right]^2)$$

where μ and σ are the parameters of Log-Normal distribution, can be found from the expression given below:

$$\sigma = \frac{\ln(\text{Error factor})}{1.646}$$
$$\mu = \ln(\text{median})$$

Step 3
The likelihood function used is the Poisson distribution. Data required are number of failures, total Operating Time/total number of demands.

Failure Rate

$$P_i(\text{r in T}|\lambda) = \frac{(\lambda_i T)^r}{r!}\exp(-\lambda_i T) \tag{13.5}$$

Demand Failure Probability

$$P_i(\text{r in D}\,|\lambda_d) = \frac{(\lambda_{di} D)^r}{r!}\exp(-\lambda_d D) \tag{13.6}$$

Step 4
This is last step in which we find the posterior distribution by using Baye's theorem given as follow.

$$p(\lambda_i/B) = \frac{p(\lambda_i)p(B/\lambda_i)}{\int_\lambda p(\lambda_i)p(B/\lambda_i)} \tag{13.7}$$

where,

P(λ_i) = Probability density function of parameter for a continuous variable, prior to having information B (Prior) = $f_d(\lambda_i)$

P(B/λ_i) = Probability of B, given the failure rate λ_i or demand failure probability

P(λ_i/B) = Probability density function of failure rate λ_i, given the information B (Posterior)

Thus, posterior probability distribution can be estimated from n different points obtained.

Characteristics Parameter of Posterior Distribution
Mean and Standard Deviation
Since the points are discretized, the formulae for the mean and the standard deviation are:

The square root of the variance is the standard deviation

$$\text{Mean} = \sum_{\mathrm{i}=1}^{\mathrm{n}} \lambda_{\mathrm{i}} p(\lambda_i/B)\delta$$

$$\text{Variance}= \sum_{\mathrm{i}=1}^{\mathrm{n}} (\lambda_{\mathrm{i}} - \text{mean})^2 \mathrm{p}(\lambda_{\mathrm{i}}/\mathrm{B})\delta$$

Lamda 0.95 gives the value of lambda when the area under the curve is 95 % of the total area. This is estimated as follows

$$0.95= \int_{0}^{\lambda_{0.95}} f_d(\lambda) d\lambda$$

The value of λ corresponding to the cumulative integrated value of 0.95 is taken as $\lambda_{0.95}$ or 95 percentile value of the failure rate. Similar approach is followed for other percentile values.

Estimation of Parameters from Multiple Sources of Information
Conventional Bayesian approach discussed in the preceding section is applicable when we have only two sources of information, for example one from generic information and other from operating experience. In this section, data come from a number of similar, but not identical sources. For example, the source of information is in terms of data from a number of NPPs. The situation is described by a hierarchical model with two levels. The first level models the plants as a family, with the numbers resembling each other. The second level models the data that are generated at each point.

Let us consider estimating failure rate/frequencies of process systems—continuously operating systems of NPP (having potential to be initiating event). The parameter of interest is λ. The input data from 'm' plants is of the form 'x_i' in 't_i' where x_i is the number of occurrence of initiating event in ith plant over an observed time t_i. The hierarchical model has two levels. Level 1 of the model says that λ varies among m plants, but only to a limited degree. This is modeled by a distribution 'g' that describes variability in the plant population. The distribution g could be gamma(α, β) distribution or could also be lognormal (μ, σ^2) or some other distribution. Before any data are generated, the distribution g is invoked m times, producing the values (λ_1, λ_2,..., λ_m). These values of λ_i are independently generated, but they all come from the same distribution, g.

Level 2 of the hierarchical model says that, conditional on the λ_i values, the plants independently produce data. Thus, for each i, plant i is observed for time t_i, and it experiences a random number of initiating events, X_i, with X_i having a Poisson distribution. The hierarchical model adopted from NUREG/CR-6823 [9] is shown in Fig. 13.8.

The hierarchical model consists of unknown parameters λ_1, λ_2,..., λ_m and any unknown parameters of g. To emphasize the difference between the two levels, the parameters of g are known as hyper parameters.

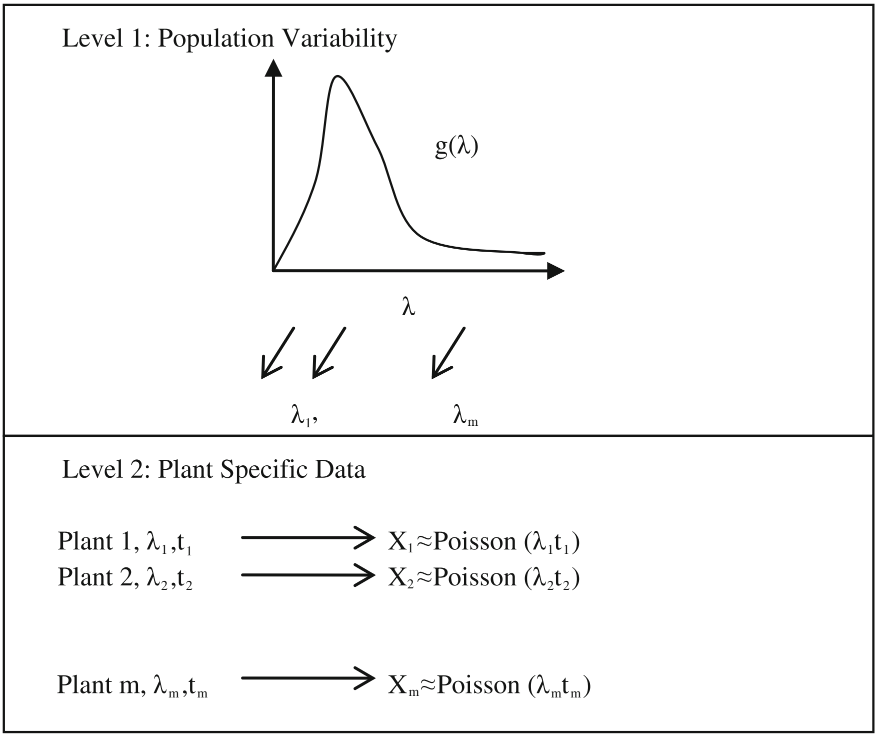


Fig. 13.8 The hierarchical model

There are two methods to analyze the data by means of hierarchical model: 1. Parametric empirical Bayes method and 2. Hierarchical Bayes method. The latter method is widely used than the former due to its easy implementation by means of Markov chain Monte Carlo simulation.

The Hierarchical Bayes Method

The hierarchical Bayes approach expresses the initial uncertainty about the unknown hyper parameters using yet another prior, known as hyper prior distribution or second order. The uncertainty in the state of knowledge about the values of α and β, if g is represented with gamma distribution, is expressed by a specified joint hyper prior distribution on α and β. Berger (1985) and Gelmen et al. (1995) discuss the basic notions of hierarchical Bayes modeling. The solution to the hierarchical Bayes method requires conditioning on the data and obtaining the required posterior distributions of all the parameters of interest. The desired point and interval estimates of the parameters are then directly obtained from these posterior distributions.

This approach is implemented using Markov chain Monte Carlo simulation, explained in detail in NUREG/CR-6823. Free downloadable software BUGS is available online to assist in such calculations.

13.5 Expert Elicitation Methods

Expert judgment techniques are useful in quantifying models in situations where the cost or technical difficulties involved or uniqueness of the situation under study make it difficult/impossible to make enough observations to quantify the models with real data. Expert elicitation methods techniques are used to estimate model parameter uncertainties. These are also used to refine the estimates obtained from real data as well.

13.5.1 Definition and Uses of Expert Elicitation

Expert opinion is the judgment based on knowledge and experience that an expert makes in responding to certain questions about a subject. These questions can be related to probabilities, ratings, uncertainty estimates, weighting factors, physical quantities etc. The expert-opinion elicitation process is defined as a formal, heuristic process of obtaining information or answers to specific questions about certain quantities, called issues, such as unsatisfactory-performance rates, unsatisfactory performance consequences and expected service life. Another reason for the use of experts is to assess the likelihood of a one-time event. Expert-opinion elicitation should not be used in lieu of rigorous reliability and risk analytical methods, but should be used to supplement them. Also, it should be used in cases where reliability and risk analytical methods are inappropriate or inconsistent.

Because of the complex, subjective nature of expert opinion, there has been no formally established methodology for treating expert judgment. An approach for quantification, based on the elicitation of consensus expert judgment can be used. The group consensus approach provides a reasonable means of quantifying situations where a broad range of indirect evidence exists and formal models for treating this evidence are lacking.

Some specific examples of expert use are Reactor Safety Study, IEEE-Standard-500, and Severe Accident Risk: An assessment for five US NPPs, where expert opinion is used to estimate the probability of component failures and other rare events. EPRI has relied on expert opinion to assess seismic hazard rates. Another example is the use of expert opinion in assessing human error rates discussed by Swain and Guttman [10].

13.5.2 Treatment of Expert Elicitation Process

The use of expert opinion in decision-making is a two-step process:

Elicitation: The method of elicitation may take the form of individual interviews, interactive group sessions or the Delphi Approach. Techniques for improving the accuracy of the expert estimates include calibration, improvement in questionnaire design, motivation techniques and other methods.

Analysis: The analysis portion of expert use involves combining expert opinions to produce an aggregate estimate that can be used for reliability analysts. Various aggregation techniques for pooling expert opinions exist, but of particular interest are those adopting the form of mathematical models.

Clemen and Winkler [11] classify the elicitation and aggregation processes of expert assessments into two groups:

Behavioral approaches: Behavioral approaches aim at producing some type of group consensus among experts, who are typically encouraged to interact with one another and share their assessments.

Mathematical approaches: In mathematical approaches, experts' individual assessments on an uncertain quantity are expressed as subjective probabilities. They are then combined through various mathematical methods by the decision-maker.

There are good reasons for using a consensus expert elicitation process or at least for not abandoning such an approach until more structured mathematical methods are developed that provide the same advantages. However, to gain the advantages of the expert evidence/consensus approach, a strong facilitator, or a group of strong analysts, who understands the process and enforces a formal and structured interaction is required. Each analyst is required to develop his distribution independently to defend their position with all the evidence of which they are aware. No one is allowed 'off-the-hook' (i.e. to capitulate to another analyst's unsupported opinion).

13.5.3 Methods of Treatment

Probability provides a measure of the likelihood of occurrence of an event. It is a numerical expression of uncertainty. However, it is common for experts to express uncertainty verbally using linguistic terms, such as *likely, probable, improbable* etc. Although the linguistic terms are fuzzy, Lichtenstein and Newman developed a table that translates the commonly used linguistic terms into probability values using responses from several subjects. A summary of such translation is shown in Table 13.3.

Indirect Elicitation Method

The indirect method is based on betting rates by experts in order to reach a point of indifference among presented options related to an issue.

Direct Elicitation Methods

This method elicits a direct estimate of the degree of belief of an expert on some issue. Methods that fall in this category are Delphi method and the nominal group technique.

Delphi Method: The Delphi technique is the first structured method for the "systematic solicitation and collation of judgments on a particular topic through a set of carefully designed sequential questionnaires interspersed with summarized information and feedback of opinions derived from earlier responses". This technique does not require face-to-face meeting with the participants, thereby making it useful

Table 13.3 Linguistic probabilities

Verbal Description	Probability Equivalent	Low Value	High Value
Virtually impossible	0.01	0.00	0.05
Very unlikely	0.10	0.02	0.15
Unlikely	0.15	0.04	0.45
Fairly unlikely	0.25	0.02	0.75
Fair Chance, Even Chance	0.50	0.25	0.85
Usually, likely	0.75	0.25	0.95
Probable	0.80	0.030	0.99
Very probably	0.90	0.75	0.99
Virtually certain	0.99	0.90	1.00

to conduct surveys from qualified people over a wide geographic area. The purpose and steps of the Delphi method depend on the nature of use. Primarily, the uses can be categorized into (1) technological forecasting, and (2) policy analysis.

The basic Delphi method consists of the following steps:

1. Selection of issues or questions and development of questionnaires. Typically three or four questionnaires mailed to the respondents are used to obtain the required data.
2. Selection of experts who are most knowledgeable about issues or questions of concern. Frequently a nominating process is used whereby key individuals may nominate someone with the expertise to participate in the study.
3. Selection of a sample size. Thirty is frequently used as an upper bound due to limited numbers of new ideas; three or four people is probably too few, and usually between ten and twenty people is reasonable.
4. Provision of familiarization to experts through sufficient details on the issues on the questionnaires.
5. Elicitation of expert opinions about the issues. Extreme opinions are discarded. The experts might not know who the other respondents are.
6. Aggregation and presentation of results in the form of median values and an inter-quartile range (i.e., 25 and 75 % percentile values).
7. Review of results by the experts and revision of initial answers by experts. This iterative reexamination of issues would sometimes increase the accuracy of results. Respondents who provide answers outside the inter-quartile range need to provide written justifications or arguments on the second cycle of completing the questionnaires.
8. Revision of results and review for another cycle. The process should be repeated until a complete consensus is achieved. Typically, the Delphi method requires two to four cycles or iterations.
9. A summary of the results is prepared with argument summary for the out of inter-quartile range values.

In this method, experts are asked to anonymously judge the assessments made by other experts in a panel. Each of the experts is then given a chance to reassess his/her initial judgment based on the review done by others. Typically, the process is repeated for several rounds until a smaller spread of experts' opinions is achieved. The median values are commonly taken as the best estimates for the issues or questions. Though Delphi method offers an adequate basis for expert-opinion elicitation, there is need to develop guidelines on its use to ensure consistency and result reliability. The Delphi method later incorporated a self-rating mechanism, allowing experts to rate their expertise.

It is generally agreed that mathematical approaches yield more accurate results than behavioral approaches in aggregating expert opinions.

Geometric Averaging Technique

Suppose *n* experts are asked to make an estimate of the failure rate of an item. The estimates can be pooled using the geometric averaging technique. For example, if λ_i is the estimate of the ith expert, then an estimate of the failure rate is obtained from:

$$\hat{\lambda} = \sqrt[n]{\prod_{i=1}^{n} \lambda_i} \tag{13.8}$$

This was the primary method in estimating the failure rate in IEEE-Standard-500. The use of geometric averaging implies that (i) all experts are equally competent, (ii) experts do not have any systematic biases, (iii) experts are independent and (iv) the preceding three assumptions are valid regardless of which value the experts estimate e.g., high, low or recommended.

Percentiles for Combining Expert Opinions

A p-percentile value of a random variable based on sample (x_1, x_2, …, x_n) can be defined as the value of the parameter such that p% of the data is less than or equal to x_p. A median is considered to be 50th-percentile value. Aggregating expert opinion can be based on computing the 25th, 50th, and 75th percentile values of the gathered opinions. The computation of these values is based on the number of experts providing these opinions. Table 13.4 [12] can be used for aggregating the opinion of various experts ranging from 4 to 20. For example, 6 experts provided the following subjective probability of an event sorted in decreasing order.

Probabilities = {5.0e-2, 1.0e-2, 5.0e-3, 1.0e-3, 7.0e-4, 5.0e-4}
The arithmetic 25, 50 and 75 percentile values are respectively given by

25th percentile = 1.0e-2
50th percentile = 3.0e-3
75th percentile = 7.0e-4

The geometric averaged values for the 25th and 75th percentile values are found to be the same as those obtained by arithmetic averaging. The 50th percentile value however is different (2.24e-03).

Table 13.4 Computation of percentiles

Number of experts (n)	25 Percentile		50 Percentile		75 Percentile	
	Arithmetic average	Geometric average	Arithmetic average	Geometric average	Arithmetic average	Geometric average
4	$(x_1 + x_2)/2$	$\sqrt{x_1 x_2}$	$(x_2 + x_3)/2$	$\sqrt{x_2 x_3}$	$(x_3 + x_4)/2$	$\sqrt{x_3 x_4}$
5	x_2	x_2	x_3	x_3	x_4	x_4
6	x_2	x_2	$(x_3 + x_4)/2$	$\sqrt{x_3 x_4}$	x_5	x_5
7	$(x_2 + x_3)/2$	$\sqrt{x_2 x_3}$	x_4	x_4	$(x_5 + x_6)/2$	$\sqrt{x_5 x_6}$
8	$(x_2 + x_3)/2$	$\sqrt{x_2 x_3}$	$(x_4 + x_5)/2$	$\sqrt{x_4 x_5}$	$(x_6 + x_7)/2$	$\sqrt{x_6 x_7}$
9	$(x_2 + x_3)/2$	$\sqrt{x_2 x_3}$	x_5	x_5	$(x_7 + x_8)/2$	$\sqrt{x_7 x_8}$
10	$(x_2 + x_3)/2$	$\sqrt{x_2 x_3}$	$(x_5 + x_6)/2$	$\sqrt{x_5 x_6}$	$(x_8 + x_9)/2$	$\sqrt{x_8 x_9}$
11	x_3	x_3	x_6	x_6	x_9	x_9
12	x_3	x_3	$(x_6 + x_7)/2$	$\sqrt{x_6 x_7}$	x_{10}	x_{10}

x_i represents the opinion of the expert

13.6 Uncertainty Propagation

Uncertainty propagation methods focus on how one can assess the impact of uncertainties in the input parameters on the model output. In case of system reliability/safety assessment, uncertainty in system characteristic such as unavailability or failure frequency is quantified by synthesizing the uncertainties in component characteristics; for example, uncertainty in system reliability Y is obtained by propagating uncertainties of its components (x_1, x_2, *and* x_3) as shown in Fig. 13.9. System model function as a precise analytical expression is required for the uncertainty propagation. Different methods of uncertainty propagation are discussed in this section.

13.6.1 Method of Moments

'Method of Moments' is an analytical technique for uncertainty propagation. This method is based on Taylor series expansion of the system model. The amount of information required on the input parameters of the system model is limited to only mean and variance. The final results of this approach give only the mean and variance of the model output.

Let $y = f(x_1, x_2, x_3, \ldots, x_n)$; x_i denotes expected values; The Taylor series expansion provides a way of expressing deviations in the output from its nominal value, $y - y^0$ in terms of deviations in its inputs from their nominal values, $x_i{-}x_i^{\mathrm{o}}$. Successive terms contain higher order powers of deviations and higher order derivatives of the function with respect to each input. Below, the expansion around the nominal scenario including the first three terms is shown [13]:

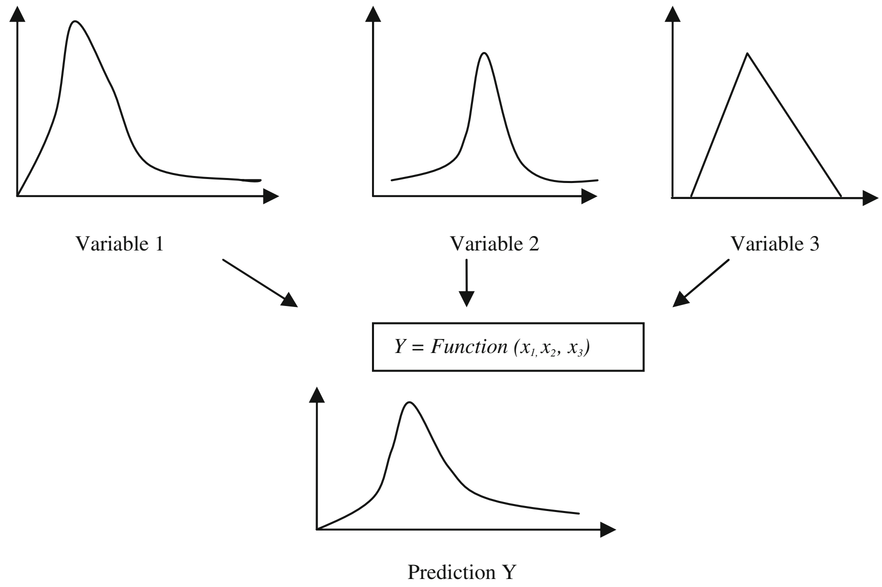


Fig. 13.9 Propagation of uncertainty through a model

$$y-y^{o}=\sum_{i=1}^{n}(\mathrm{x_i}-\mathrm{x_i^o})[\frac{\partial y}{\partial x_i}]_{X^o}+\frac{1}{2}\sum_{i=1}^{n}\sum_{\mathrm{j=1}}^{\mathrm{n}}(\mathrm{x_i}-\mathrm{x_i^o})(\mathrm{x_j}-\mathrm{x_j^o})[\frac{\partial^2 y}{\partial x_i\partial x_j}]_{X^o}+ \\ \frac{1}{3!}\sum_{i=1}^{n}\sum_{\mathrm{j=1}}^{\mathrm{n}}\sum_{\mathrm{k=1}}^{\mathrm{n}}(\mathrm{x_i}-\mathrm{x_i^o})(\mathrm{x_j}-\mathrm{x_j^o})(\mathrm{x_k}-\mathrm{x_k^o})[\frac{\partial^3 y}{\partial x_i\partial x_j\partial x_k}]_{X^o}+\cdots \tag{13.9}$$

The first order approximation is used for simplifying the calculations. Considering the first term in Eq. 13.9, the expected value of y can be approximated by the nominal value, since the expected value of the deviation in y is zero:

$$\begin{aligned} &E[y{-}y0]\approx 0, \\ &E[y]\approx y0\approx f(X0) \end{aligned} \tag{13.10}$$

The general first order approximation of the variance in the output can be obtained using only the first order term from Eq. (13.9):

$$Var[y]\ =E[(\mathrm{y{-}y0})^2]\approx \mathrm{E}\left[\{\sum_{i=1}^{n}(\mathrm{x_i}-\mathrm{x_i^o})[\frac{\partial y}{\partial x_i}]_{X^o}\}\right] \tag{13.11}$$

The above expression can be simplified to

$$Var[y] \approx \sum_{i=1}^{n} Var(x_i)[\frac{\partial y}{\partial x_i}]^2_{X^o} \tag{13.12}$$

The analytical methods for uncertainty propagation are rarely employed in reliability problems as they are suitable for only simple linear cases. The advantage with analytical methods is once the algebraic analysis has been performed, the numerical calculations are relatively simple. As it produces only moments of distributions, it is difficult to get clear cut tails of distributions. Analytical methods are often only approximate methods with somewhat constrained validity [4].

13.6.1.1 Consideration of Correlation Using Method of Moments

Quantification of fault tree analysis gives top event unavailability as an algebraic function of component unavailabilities, q_i, q_j,…, q_n. The Taylor series expansion provides a way to express deviations of output from its nominal value, $Q(q_i, q_j,\ldots, q_n) - Q(v_i, v_j,\ldots, v_n)$ in terms of deviations of its inputs from their nominal values, $(q_i - v_i)$. Here is the expansion around the nominal scenario with the first three terms [14, 15]:

$$\begin{aligned} Q(q_i, q_j, \ldots, q_n) - Q(v_i, v_j, \ldots, v_n) = {} & \sum_{i=1}^{n} c_i(q_i - v_{i1}) + \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}(q_i - v_{i1})(q_j - v_{j1}) \\ & + \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} c_{ijk}(q_i - v_{i1})(q_j - v_{j1})(q_k - v_{k1}) + \cdots \end{aligned} \tag{13.13}$$

By taking the expectation over Eq. (13.13), the following exact expression for the mean value of Q is obtained:

$$V_1 = Q(v_i, v_j, \ldots, v_n) + \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}J_{ijk} + \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} c_{ijk}J_{ijk} + \cdots \tag{13.14}$$

By squaring both sides of Eq. (13.13), then taking expectation of each side, the following expression for the variance of Q is obtained:

$$\begin{aligned} V_2 = {} & \sum_{\mathrm{i=1}}^{\mathrm{n}} c_i^2 v_{i2} + \sum_{i}^{n}\sum_{j}^{n} [2c_i c_j J_{ij} + c_{ij}^2(J_{ijij} - J_{ij}^2)] + 2\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} c_i c_{jk} J_{ijk} \\ & + 2\sum_{i}^{n}\sum_{j}^{n}\sum_{k}^{n}\sum_{l}^{n} c_i c_{jkl} J_{ijkl} + 2\sum_{i}^{n}\sum_{j}^{n}\sum_{k}^{n}\sum_{l}^{n} c_{ij} c_{kl}(J_{ijkl} - J_{ij}J_{kl}) + \cdots \end{aligned} \tag{13.15}$$

In similar manner, the third and higher moments of Q are obtained by raising both sides of (13.13) to the powers of third and higher, respectively, then taking mean of each side.

Calculation of Joint Moments for Two Correlated Random Variables
The expression for the joint central moment of two variables q_i and q_j is given by [15]:

$$J = E\left[(q_i - v_{i1})^l (q_j - v_{j1})^m\right], l\, and\, m\, are\, greater\, than\, or\, equal\, to\, 1 \tag{3.16}$$

If l = 1 and m = 1, J is called covariance of two random variables. The Eq. (13.6) can be expressed as:

$$J = J_a + \rho_{ij}(J_b - J_a) \tag{13.17}$$

$$\begin{aligned} \text{where } \mathrm{J_a} &= \mathrm{v_{il} v_{jm}}, \text{for } \mathrm{l > 1 \text{ and } m > 1} \\ &= 0, \text{for } \mathrm{l = 1 \text{ or } m = 1} \end{aligned} \tag{13.18}$$

$$\mathrm{J_b} = v_{it}^{l/t} v_{jt}^{m/t} \quad \mathrm{t = l + m} \tag{13.19}$$

ρ_{ij}—correlation coefficient between q_i and q_j

Example 1 The exact top event probability of a fault tree [15] is given by

$$\mathrm{Q = q_1 q_2 + (1 - q_2) q_3} \tag{13.20}$$

There are three basic events in the system, viz, their unavailabilities given by q_1, q_2 and $q_{3.}$ The unavailabilities are assumed to follow lognormal distribution with medians, m1, m2 and m3; and error factors EF_1, EF_2 and EF_3. It is assumed that there is no correlation between q_1 and q_2 or q_1 and q_3. But a correlation of ρ_{23} exists between q_2 and q_3. Considering three cases here, (i) ρ_{23} = 0, null correlation between q_2 and q_3; (ii) ρ_{23} = 1, full correlation between q_2 and $q_{3;}$ (iii) 0 < ρ_{23} < 1, partial correlation between q_2 and q_3; Calculate the unavailability.

Solution: The Taylor series coefficients in (13.13) are given in this problem by:

$$\mathrm{c_1 = v_{21}, c_2 = v_{11} - v_{31}, c_3 = 1 - v_{21}, c_{12} = 1, c_{23} = -1, c_{13} = c_{123} = 0.}$$

Now, the first and second moments of Q are obtained by substituting the above values in Eqs. 13.14 and 13.15.

$$V_1 = v_{11} v_{21} + (1 - v_{21}) v_{31} - J_{23} \tag{13.21}$$

$$\begin{aligned} \mathrm{V_2} &= \mathrm{v_{21}^2 v_{12} + (v_{11} - v_{31})^2 v_{22} + (1 - v_{21})^2 v_{32} + 2(v_{11} - v_{31})(1 - v_{21}) J_{23}} \\ &\quad \mathrm{+ v_{12} v_{22} + (J_{2323} - J_{23} J_{23}) - (v_{11} - v_{31}) J_{223} - 2(1 - v_{21}) J_{323}} \end{aligned} \tag{13.22}$$

There are three kind of joint moments present in (13.21) and (13.22), (i) moments involving only the two correlated variables q_2 and q_3 together. This is computed with the help of (13.17). (ii) Totally uncorrelated variables, this is computed with the help of (13.19). (iii) Moments involving the three variables. Both (i) and (ii) have to be used.

Evaluation of joint moment between q_2 and q_3, J_{23}:

Using Eq. (13.17)

$$J_{23} = \rho_{23}(v_{22})^{1/2}(v_{32})^{1/2} \tag{13.23}$$

Similarly the following joint moments are calculated as follows:

Evaluation of J_{2323}

$$\begin{aligned} J_a &= v_{22}v_{32} \\ J_b &= (v_{24})^{1/2}(v_{34})^{1/2} \\ J_{2323} &= J_a + \rho_{23}(J_b - J_a) \end{aligned} \tag{13.24}$$

Evaluation of J_{223}

$$\begin{aligned} J_a &= v_{22}v_{31} \\ J_b &= v_{23}^{2/3}v_{33}^{1/3} \\ J_{223} &= J_a + \rho_{23}(J_b - J_a) \end{aligned} \tag{13.25}$$

Evaluation of J_{323}

$$\begin{aligned} J_a &= v_{21}v_{32} \\ J_b &= v_{23}^{1/3}v_{33}^{2/3} \\ J_{323} &= J_a + \rho_{23}(J_b - J_a) \end{aligned} \tag{13.26}$$

As we have assumed lognormal distribution for unavailability of basic events, now we will work for the first, second, third and fourth moments given the median, m and error factor, EF of the distribution [3]:

The lognormal probability distribution function (PDF) is given by

$$f(x) = \frac{1}{\sqrt{2\pi}(\sigma x)} e^{\left(-\frac{1}{2}\left[\frac{\ln x - \mu}{\sigma}\right]^2\right)}$$

where μ and σ parameter of the distribution, given by

$$\begin{aligned} \mu &= E[ln(x)] = ln(m) \\ \sigma &= Var[ln(x)] = ln(EF)/1.645 \end{aligned}$$

The mean and central moments for lognormal PDF are given by:

$$\left.\begin{array}{l} v_{i1} = m_i exp(\sigma_i^2)/2) \\ v_{i2} = v_{i1}^2(exp(\sigma_i^2) - 1) \\ v_{i3} = v_{i2}^{3/2}(exp(\sigma_i^2) - 1))^{1/2}(exp(\sigma_i^2) + 2); \\ v_{i4} = v_{i2}^2(exp(4\sigma_i^2) + 2exp(3\sigma_i^2) + 3exp(2\sigma_i^2) - 3); \end{array}\right\} \qquad (13.27)$$

For the present problem i = 1, 2 and 3.

Assuming: m_1 = 1e-3; m_2 = m_3 = 2e-3;

$$\mathrm{EF}_1 = 3; \mathrm{EF}_2 = \mathrm{EF}_3 = 6;$$

Case (*i*) No correlation among q_1, q_2, and q_3 (ρ_{23} = 0)

Table 13.5 gives the comparison of method of moments and Monte-Carlo simulation with ρ_{23} = 0 for mean and variance of Q.

Case (*ii*) Full correlation between q_2 and q_3 (ρ_{23} = 1)

Table 13.6 gives the comparison of method of moments and Monte-Carlo simulation with ρ_{23} = 1 for mean and variance of Q.

Case (*iii*) Partial correlation between q_2 and q_3 (0 < ρ_{23} < 1)

Table 13.7 gives values of mean and variance of Q using method of moments with ρ_{23} = 0.2, 0.4, 0.6 and 0.8.

Table 13.5 No correlation between q_2 and q_3 (ρ_{23} = 0)

Method/Moments	Method of Moments	Monte-Carlo Simulation
V1	3.61095e-3	3.60964e-3
V2	2.9593e-5	3.1256e-5

Table 13.6 Full correlation between q_2 and q_3 (ρ_{23} = 1)

Method/Moments	Method of Moments	Monte-Carlo Simulation
V1	3.58114e-3	3.58025e-3
V2	2.7067e-5	3.25384e-5

Table 13.7 Partial correlation between q_2 and q_3

ρ_{23}/Moments	0.2	0.4	0.6	0.8
V_1	3.60975e-3	3.60618e-3	3.60022e-3	3.59187e-3
V_2	2.9081e-5	2.8572e-5	2.8066e-5	2.7565e-5

13.6.2 Monte Carlo Simulation

Given Monte Carlo simulation is used widely in solving many engineering problems. Figure 13.10 gives the steps involved in uncertainty propagation using Monte Carlo simulation. The steps are explained below.

The first step is to obtain the required information for simulation. The relation between the system characteristic and the components/parameters in the form of a mathematical expression is required. Information about probability distribution and their associate parameters for each component/parameter of the system model is also required.

The next step is to generate a uniformly distributed random number on [0, 1] for each of the parameters. If the distribution of the parameter is normal or lognormal, it

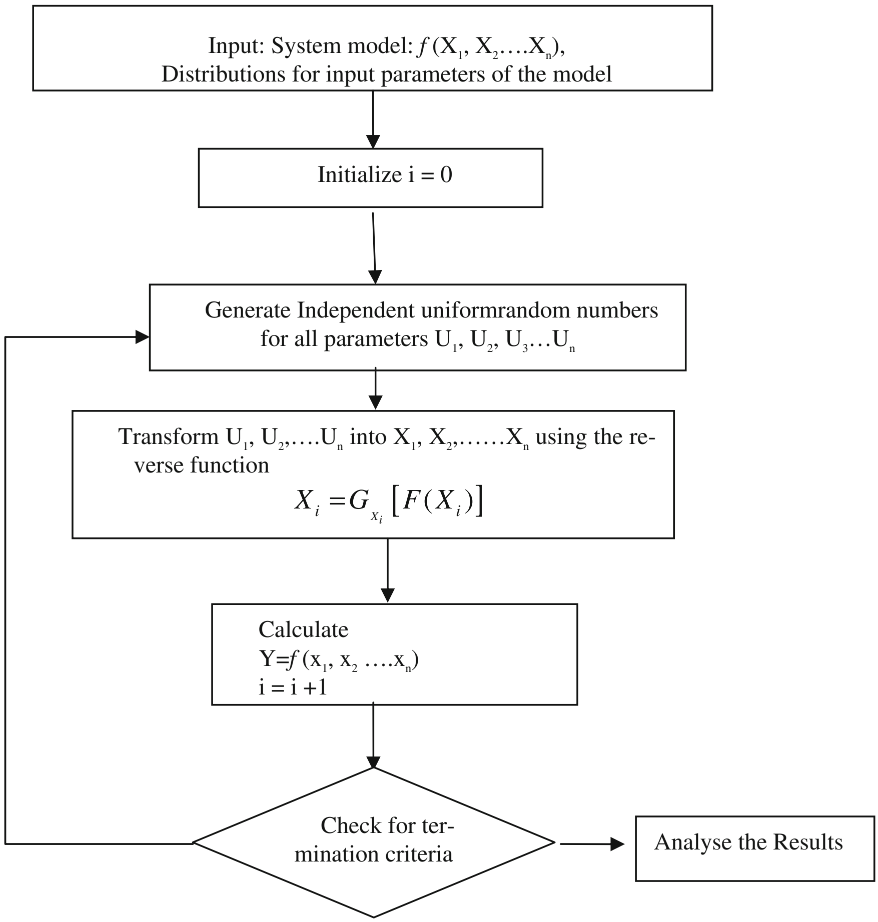

Input: System model: $f\,(X_1, X_2 \ldots X_n)$,
Distributions for input parameters of the model
Initialize i = 0
Generate Independent uniformrandom numbers for all parameters $U_1, U_2, U_3 \ldots U_n$
Transform $U_1, U_2, \ldots U_n$ into $X_1, X_2, \ldots \ldots X_n$ using the reverse function
$X_i = G_{x_i}\left[F(X_i)\right]$
Calculate
$Y = f\,(x_1, x_2 \ldots x_n)$
i = i +1
Check for termination criteria
Analyse the Results

Fig. 13.10 Steps in uncertainty propagation based on Monte Carlo simulation

Table 13.8 Generation of random samples for different distributions

Distribution	Random Samples
Exponential (λ)	$-\frac{1}{\lambda}\ln(U_i)$
Weibull (α, β)	$\alpha(-\ln U_i)^{1/\beta}$
Normal (μ, σ)	$X_i = X_s\sigma + \mu$ $X_s = (-2\ln U_i)^{1/2}\cos(2\pi U_{i+1})$
Lognormal (μ, σ)	Generate $Y = ln(X)$ as a normal variate with mean μ and standard deviation σ and then compute $X_i = exp(Y_i)$
Uniform (a, b)	$a + (b - a)U_i$

may need two uniform random numbers. Uniform random number is a variable that can take any value between 0 and 1 with equal likelihood. Computer algorithms for uniform random numbers follow a pattern so they are called pseudo random number generator. Good characteristics of a random number generator are

- Large period
- Reproducibility
- Computational efficiency

The next step is to determine the corresponding random variates (x_i) using the reverse function G(F(x)) for each parameter. The reverse function is a function which gives the value of x for a given CDF value F(x) and its parameters. The reverse function depends on the type of distribution. Table 13.8 gives the mathematical expression for the reverse function for various distributions, which is used for calculating the random samples. The determination of reverse function for exponential distributions is explained below:

Consider a random variable 'x' following exponential distribution with parameter λ. f(x) and F(x) are given by the following expressions:

$$f(x) = \lambda\ \exp(-\lambda x) \tag{13.28}$$

$$F(x) = \int_0^x f(x)dx = 1 - \exp(-\lambda x) \tag{13.29}$$

Now x is derived as a function of F(x),

$$x = G(F(x)) = \frac{1}{\lambda}\ln(\frac{1}{1 - F(x)}) = -\frac{1}{\lambda}\ln(1 - F(x)) \tag{13.30}$$

If (1-F(x)) is assigned with a random number Uithen,

$$x = -\frac{1}{\lambda}\ln(U_i) \tag{13.31}$$

A value of the system characteristic is synthesized from the selected random variates according to the system model. These calculations are repeated until the desired number of values of system characteristic has been generated. The mean and variance as well as the percentiles of the simulated distribution of system characteristic may then be calculated.

Example 2 Consider a random variable x is following exponential distribution with parameter λ, f(x) and F(x) are given by the following expressions. Calculate x given λ = 1.825/yr and random number 0.8.

$$f(x) = \lambda\ \exp(-\lambda x)$$

$$F(x) = \int_0^x f(x)dx = 1 - \exp(-\lambda x)$$

Solution: Now x derived as a function of F(x)

$$x = G(F(x)) = \frac{1}{\lambda}\ln(\frac{1}{1 - F(x)})$$

A uniform random number is generated using any of the standard random number generators. Many algorithms have been developed to generate a series of uniformly distributed random numbers between zero and one. Let us assume 0.8 is generated by random number generator then the value of x is calculated by substituting 0.8 in place of F(x) and 1.825/yr (5e-3/h) in place of λ in the above equation

$$x = \frac{1}{5e - 3}\ln(\frac{1}{1 - 0.8}) = 321.88\,H$$

This indicates time to failure of the component is 321.88 h (see Fig. 13.11). If the shape of PDF is different accordingly one has to solve for G(F(x)).

Termination Criteria

The simple termination criterion is to fix the number of iterations before the simulation. Monte Carlo simulation gives an excellent approximation of the system model distribution with a large sample size. The 'large' is always subjective and changes with problem to problem. For example, the low probability events in case of structural engineering or seismic problems demands for more than 1 million iterations to get a required event. The problem of uncertainty propagation in system reliability assessment is simple and we can fix the number of iterations at the beginning to 10,000 or more. But there are techniques to determine the number of

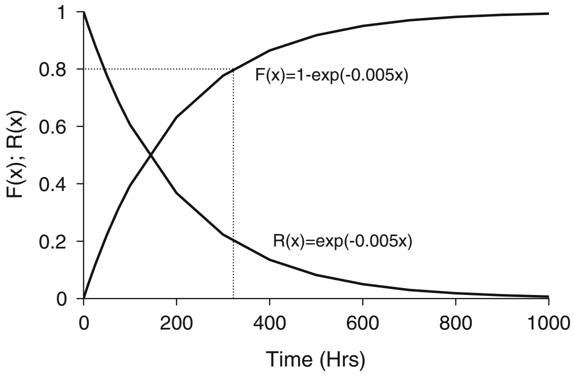


Fig. 13.11 The relationship between x, F(x) and G(F(x))

iterations during the simulation. One such useful technique is that the sample size required to obtain a result that is within a pre-specified confidence interval can be determined. Some details about termination criteria are discussed in Chap. 4.

Monte Carlo sampling technique may require intensive computational resources as the minimum sample size can be large in most of the problems. Some of following discussed variance reductions techniques can be used to reduce the computational time. Nevertheless, the present sophistication in computational developments makes the number of iterations as no longer an issue in most of the cases.

13.6.2.1 Latin Hypercube Sampling

Mckay, Beckman and Conover (1979) developed Latin Hypercube Sampling (LHS) [16]. In LHS, the range of each input distribution is divided into n intervals of equal margin probability. Figure 13.12 illustrates an example of the stratification that is produced for 20 iterations of a normal distribution (with mean 100 and SD 10). In the first iteration, one of these intervals is selected using a random number. A second random number is then generated to determine where, within that interval, $F(x)$ should lie. $x = G(F(x))$ is calculated for that value of $F(x)$. The process is repeated for the second iteration but the interval used in the first iteration is marked as having already been used and so will not be selected again. This process continues till '*n'* number of iterations is performed.

The stratification of the input distributions into n equal probability intervals ensures that samples are taken from the entire range of the distributions even with a relatively small sample size compared to random Monte Carlo sampling. The primary disadvantage of LHS is that, because it is not a purely random sampling technique, the results are not subject to analysis by standard statistics. Therefore, one cannot determine in advance the sample size necessary for a desired degree of convergence, as is possible for random Monte Carlo sampling.

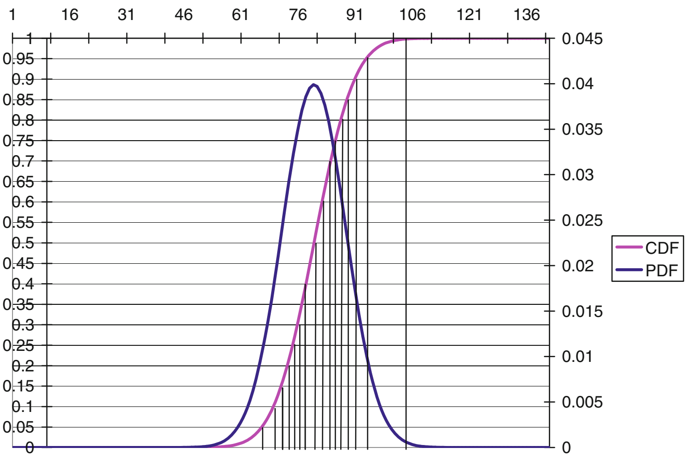


Fig. 13.12 Example of the effect of stratification in Latin hypercube sampling

Importance Sampling

Importance sampling is a general technique for estimating the properties of a particular distribution, while only having samples generated from a different distribution than the distribution of interest. Importance sampling helps us sample from the important regions of the sample space. The sampling from an importance density helps us estimate the mean with a much better statistical accuracy for a given sample size.

13.6.3 Interval Analysis

The uncertainty about many things is represented in real life in the form of intervals. An interval contains two numbers, one optimistic and the other pessimistic. The analysis is computationally inexpensive as it involves very simple calculations. The results of interval analysis are very conservative. This approach can be used in worst case analysis and also in screening phase of uncertainty analysis. This method is useful in understanding the fuzzy arithmetic and also probability bounds analysis. The arithmetic is explained below:

Let $A = [a_1, a_2]$ *and* $B[b_1, b_2]$ are two interval numbers then $C[c_1, c_2] = A[a_1, a_2]$ $*B[b_1, b_2]$ can be defined as (* denotes any arithmetic operation)

$$C[c_1,c_2] = A[a_1,a_2] + B[b_1,b_2] = [a_1 + b_1, a_2 + b_2]$$
$$C[c_1,c_2] = A[a_1,a_2] - B[b_1,b_2] = [a_1 - b_2, a_2 - b_1]$$
$$C[c_1,c_2] = A[a_1,a_2] \times B[b_1,b_2] = [min(a_1 \times b_1, a_1 \times b_2, a_2 \times b_1, a_2 \times b_2), max(a_1 \times b_1, a_1 \times b_2, a_2 \times b_1, a_2 \times b_2)]$$
$$C[c_1,c_2] = A[a_1,a_2]/B[b_1,b_2] = A[a_1,a_2] \times B[1/b_2, 1/b_1]$$

We can generalize expression

$$c_1 = min(a_1 * b_1, a_1 * b_2, a_2 * b_1, a_2 * b_2) \tag{13.32}$$

$$c_2 = max(a_1 * b_1, a_1 * b_2, a_2 * b_1, a_2 * b_2) \tag{13.33}$$

Results are generally over conservative. However, methods are available to reduce the conservatism with interval arithmetic [17]. This method can be applied when little information is available, at the conceptual design levels.

Example 3 Assuming X = [4, 8] and Y = [−2, 6], determine various arithmetic operations between X and Y using interval arithmetic.

Using Eqs. 13.32 and 13.33, X + Y, X−Y, X * Y, Y/X can be calculated as shown in Fig. 13.13.

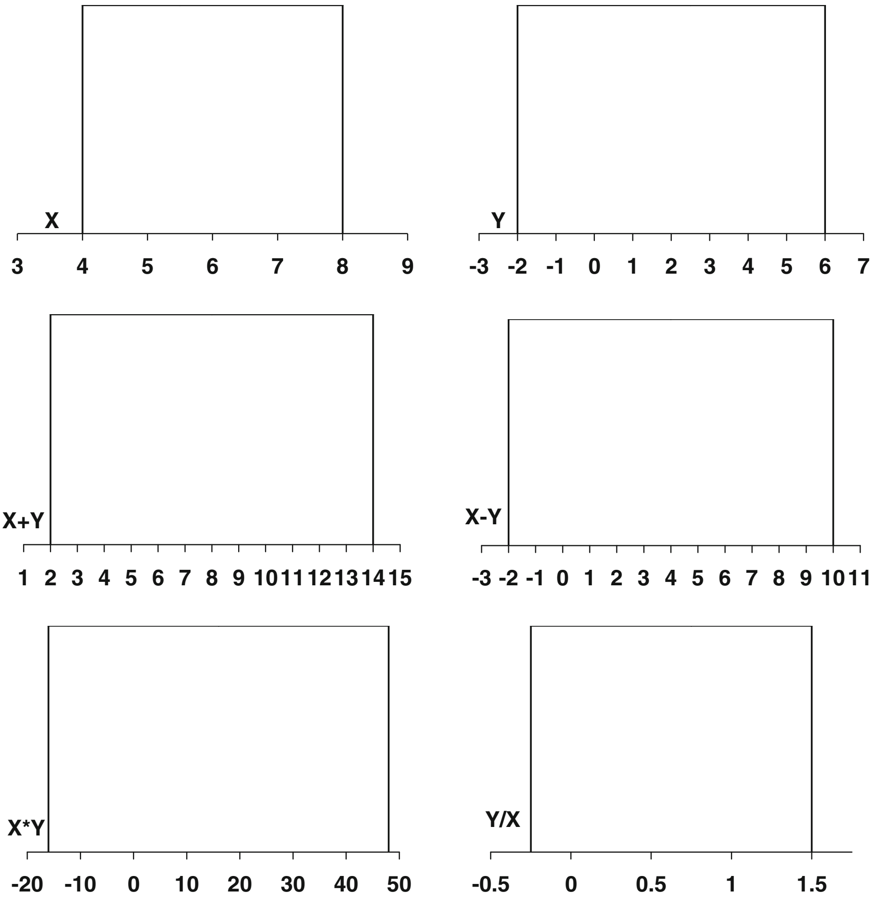


Fig. 13.13 Examples of basic arithmetic operations on interval numbers

13.6.4 Fuzzy Arithmetic

The fuzzy set theory is an extension of the traditional set theory that generalizes the membership concept (Characteristic value) by using the Membership function that assigns a value between 0 and 1 that represents the *degree of membership* of an object x to set F. Fuzzy sets are used to provide a more reasonable interpretation of linguistic variables (variables whose values are words or sentences in natural or artificial languages). A fuzzy set assigns membership values between 0 and 1 that reflects more naturally a member's association with the set. The membership functions can have various shapes such as triangular, normal, and exponential, etc. Uncertainty in the input parameters of the model can be represented with the fuzzy numbers. The possible range of numbers with different membership value represents the uncertainty about the model parameter.

Fuzzy arithmetic is an offshoot from fuzzy set theory and the rules for combining fuzzy numbers in calculations are given within this framework. The arithmetic of fuzzy numbers essentially reduces to interval analysis repeated once for each α level. The difference is that fuzzy arithmetic generates an entire distribution instead of a simple interval or range. The interpretation on α level and some applications can be found in [4, 18]

Example 4 Let us calculate fuzzy arithmetic of two triangular fuzzy numbers (Fig. 13.14) using the concept of interval analysis. At α = 0, X is an interval [4, 8] and Y is [−2, 6]. Now carrying out interval arithmetic over these two intervals:

$$\begin{aligned}
\mathrm{X}+\mathrm{Y} &= [4,8]+[-2,6]=[2,14]\\
\mathrm{X}-\mathrm{Y} &= [4,8]-[-2,6]=[-2,10]\\
\mathrm{X}\times\mathrm{Y} &= [4,8]\times[-2,6]=[-16,48]\\
\mathrm{Y}/\mathrm{X} &= [-2,6]/[4,8]=[-0.25,1.5]
\end{aligned}$$

Similarly for all levels of α interval arithmetic is computed to arrive at the full shape of membership function of the resultant fuzzy number (see Fig. 13.14, for calculation of different arithmetic operations over X and Y). This method is known as alpha-cut method.

The alpha-cut method is explained below for uncertainty propagation in reliability calculations. Consider the main event (e.g., system unavailability) as a function of basic events $\Phi = x_1 + x_2(x_3 + x_4)(x_5x_6x_7 + x_8)$. The numerical procedure is listed as follows:

Step 1 The Solution model is derived from the above equation as

$$\begin{aligned}
\Phi_L &= min(x_1+x_2(x_3+x_4)(x_5x_6x_7+x_8)),\\
\Phi_R &= max(x_1+x_2(x_3+x_4)(x_5x_6x_7+x_8))
\end{aligned}$$

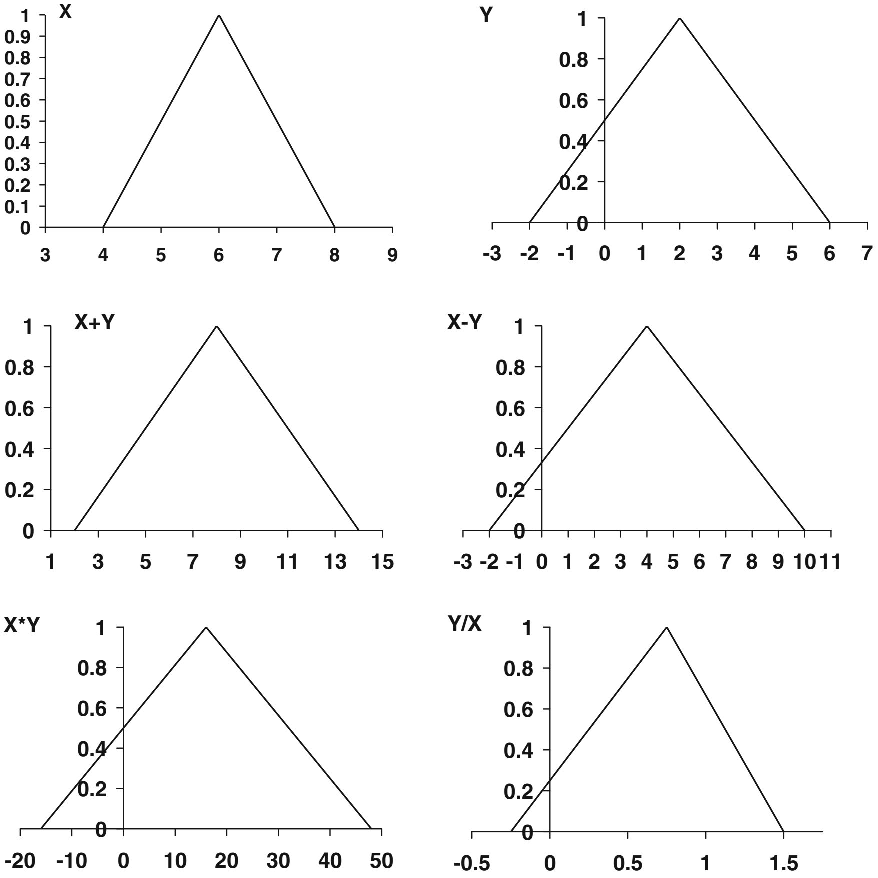


Fig. 13.14 Examples of basic arithmetic operations on fuzzy numbers

Step 2 Compute the interval of confidence for all the basic events for α = 0, 0.1, …, 1

Step 3 Calculate the interval of confidence of main event [Φ_L, Φ_R] for α = 0, 0.1, …, 1

Fuzzy arithmetic can also be carried out based on extension principle [19]. Extension principle works where operations on real numbers are extended to operations on fuzzy numbers. Let * denote any of the four basic arithmetic operations and let A, B denote fuzzy numbers. Then, we define a fuzzy set on $\Re$, A*B, by the Equation

$$(A * B)(z) = \sup_{z=x*y} \min[A(x), B(y)]$$

For all z∈$\mathfrak{R}$. More specifically, we define for all z∈$\mathfrak{R}$:

$$\begin{aligned}(A+B)(z) &= \sup_{z=x+y} \min[A(x), B(y)],\\ (A-B)(z) &= \sup_{z=x-y} \min[A(x), B(y)],\\ (A\times B)(z) &= \sup_{z=x\times y} \min[A(x), B(y)],\\ (A/B)(z) &= \sup_{z=x/y} \min[A(x), B(y)].\end{aligned} \tag{13.34}$$

In fuzzy approach, the input parameter is treated as a fuzzy number and the variability is characterized by a membership function, which can be obtained based on the available information or the expert's opinion. The membership function of each fuzzy set is generally assumed to be a triangular or a trapezoidal function and is treated as a possibility distribution. Of course, this assumption is made just for the sake of simplicity. If the available information is probability distribution, transformation from probability to possibility methods can be used. One of such methods is mentioned below.

Probability to Possibility Transformations
Let X = {x_i | i = 1,…,n) be the universe of discourse. The x_i's are ordered such that $p_1 \geq p_2 \geq \cdots \geq p_n$, where p_i is the probability of occurrence of x_i, i.e., p_i = P ({x_i}). Let π_i denote the corresponding possibility value.

A bijective transformation between probabilities and possibilities may be defined as [19]:

$$\pi_i = \sum_{j=1}^{n} \min(p_i, p_j) = ip_i + \sum_{j=i+1}^{n} p_j \,\text{and}\, p_i = \sum_{j=i}^{n} (\pi_j - \pi_{j+1})/j \tag{13.35}$$

This was derived from the definition that the degree of necessity of event A in X is the extra amount of probability of elementary events in A over the amount of probability assigned to the most frequent elementary event outside A. The most common transformations p < - > π are based on the ratio scale: $\pi_i = \beta p_i$ for all i, where β is a positive constant. They are expressed by equations:

$$\pi_i = p_i/p_1 \, and \, p_i = \pi_i/(\pi_1 + \pi_2 + \cdots + \pi_n) \tag{13.36}$$

Exercise Problems

1. Consider bridge network shown below, calculate the uncertainty bounds over the unavailability of the whole system with the data mentioned in the Table 13.9. The unavailability of the components is expressed as intervals, use interval arithmetic and calculate system unavailability (Figure 13.15).
2. For the above mentioned problem, use fuzzy arithmetic to calculate the membership function for unavailability of the system with the below mentioned component data (Table 13.10).

Table 13.9 Unavailability intervals of components

Component	Low	High
1	9.15E-04	3.66E-03
2	9.15E−04	3.66E-03
3	3e-6	3e-4
4	1.33E-04	1.2E-03
5	1.33E-04	1.2E-03

Fig. 13.15 Bridge network

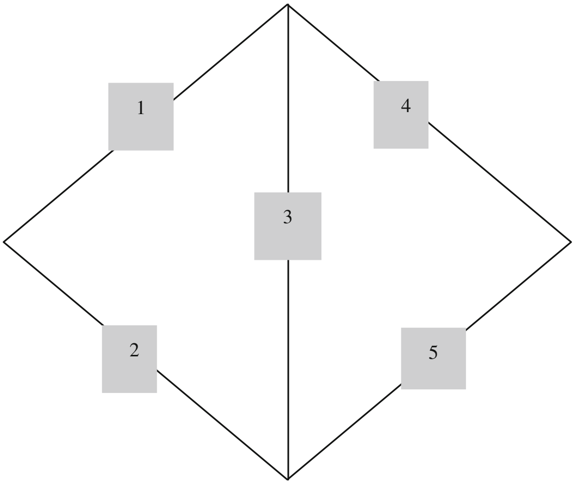


Table 13.10 Unavailability membership functions of components

Component	Low	Median	High	MF
1	9.15E-04	1.83e-3	3.66E-03	Triangular
2	9.15E-04	1.83e-3	3.66E-03	Triangular
3	3e-6	3e-5	3e-4	Triangular
4	1.33E-04	4E-04	1.2E-03	Triangular
5	1.33E-04	4E-04	1.2E-03	Triangular

Table 13.11 Probability distributions of model parameters

Performance function		$g = T_m - \left(\frac{Q_0 L^2}{2k} + \frac{Q_0 L}{h} + T_\infty\right)$		
	Variable	Mean	Std. Dev	Distribution type
1	Conductivity, K	20	4	Normal
2	Heat transfer coefficient, h	4000	800	Normal
3	Melting point, T_m	800	80	Normal
4	Volumetric heat generation, Q_0	8×10^7	–	Deterministic
5	Bulk temperature	100	–	Deterministic
6	Length of slab	0.01	–	Deterministic

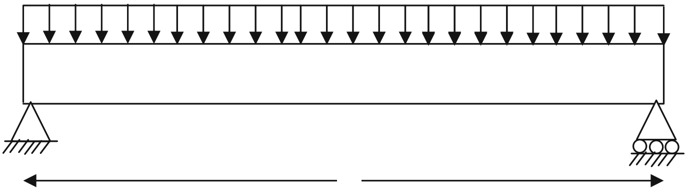
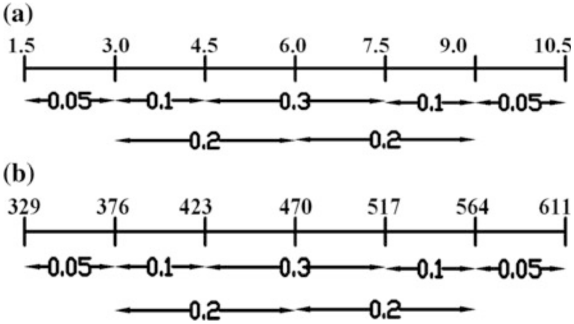


Fig. 13.16 Simply supported beam

Fig. 13.17 Basic belief assignments **a** Load, **b** Bending capacity



3. A slab of thickness (L) 10 mm is insulated on one side at x = 0 and cooled by fluid having bulk temperature100 °C. The heat generated (Q_0) in the slab is equal to 8 × 10^7 W/m^3. Determine the probability of melting of slab. Thermal conductivity, heat transfer coefficient and melting temperature of material is given in Table 13.11.
4. A simply supported beam subjected to a uniformly (Fig. 13.16) distributed load w, may fail in flexure. Suppose the beam is a rolled 18 WF 70 section of A36 steel. Length of beam is is 20 ft. Load '*w*', Bending capacity of the beam 'M_0', are uncertain variables with basic belief assignments as shown in Fig. 13.17. Beam fails if bending moment exceeds its capacity. Find the belief and plausibility of failure.

   Performance function for the problem is: $g_1(x) = M_o - \frac{1}{8}wL^2$
5. The operating experience of power supply failure in a plant shows there are 5 outages in two years. Assuming a prior generic information as lognormal with median 1 and error factor 3, calculate the posterior distribution for the failure rate of power supply?

References

1. NASA (2002) Probabilistic risk assessment procedures guide for NASA managers and practitioners. Version 1.1, NASA Report
2. Scott F, Lev RG (1996) Different methods are needed to propagate ignorance and variability. Reliab Eng Syst Saf 54:133–144
3. IAEA (1992) Procedure for conducting probabilistic safety assessment of nuclear power plants (level 1). Safety Series No. 50-P-4, International Atomic Energy Agency, Vienna
4. Abrahamsson M (2002) Uncertainty in quantitative risk analysis. Report 1024, Lund University
5. Bae H, Grandhi RV, Canfield RA (2004) Epistemic uncertainty quantification techniques including evidence theory for large scale structures. Comput Struct 82:1101–1112
6. Bae H, Grandhi RV, Canfield RA (2003) Uncertainty quantification of structural response using evidence theory. AIAA J 41(10):2062–2068
7. Bae H, Grandhi RV, Canfield RA (2004) An approximation approach for uncertainty quantification using evidence theory. Reliab Eng Syst Saf 86:215–225
8. Siu NO, Kelly DL (1998) Bayesian parameter estimation in probabilistic risk assessment. Reliab Eng Syst Saf 62:89–116
9. USNRC (2003) Handbook of parameter estimation for probabilistic risk assessment. NUREG/CR-6823, U.S. Nuclear Regulatory Commission, Washington, DC
10. Swain AD, Guttman.HE (1983) Handbook of human reliability analysis with emphasis on nuclear power applications. NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, DC
11. Clemen RT, Winkler RL (1999) Combining probability distributions from experts in risk analysis. Risk Anal 19(2):187–203
12. Ayyub BM (2001) Elicitation of expert opinions for uncertainty and risks. CRC Press, New York
13. Morgan MG, Henrion M (1992) Uncertainty—a guide to dealing uncertainty in auantitative risk and policy analysis. Cambridge University Press, London
14. Rushdi AM, Kafrawy KF (1988) Uncertainty propagation in fault tree analyses using an exact method of moments. Microelectron Reliab 28:945–965
15. Kafrawy KF, Rushdi AM (1990) Uncertainty analysis of fault tree with statistically correlated failure data. Microelectron Reliab 30:157–175
16. Iman RL, Davenport JM, Ziegler DK (1980) Latin hypercube sampling, Sandia National Laboratories, Albuquerque, Technical Report, SAND79–1473
17. Ganesh K, Veeramani P (2005) On arithmetic operations of interval numbers. Int J Uncertainty Fuzziness Knowl-Based Syst 13(6):619–631
18. Ferson S, Kuhn R (1992) Propagating uncertainty in ecological risk analysis using interval and fuzzy arithmetic. In: Zannetti P (ed) Computer techniques in environmental studies IV. Elsevier Applied Science, London, pp 387–401
19. George JK, Yuan B (1995) Fuzzy sets and fuzzy logic. Prentice-Hall of India Pvt. Ltd., New Delhi

Chapter 14
Advanced Methods in Uncertainty Management

14.1 Uncertainty Analysis with Correlated Basic Events

The uncertain parameters (epistemic in nature) of a PSA model are propagated to quantify the uncertainty in the system measure, e.g. core damage frequency. In propagating the uncertainty, the epistemic parameters of model are sometimes assumed to be either uncorrelated or independent. The propagation of uncertainties in PSA may assume that the input parameters of identical basic events are fully correlated but some uncertainty studies assume that the variables are statistically independent. Apostolakis [1] pointed out that there is correlation or coupling among the data of identical basic events such as the failure of two identical pumps, circuit breakers, etc. This correlation means that the parameters for basic events that represent identical components should not be treated as statistically independent random variables in the uncertainty analysis. The samples for these random variables need to be correlated; if there is complete correlation, they should be treated as a single random variable. Neglecting the correlation among the variables will impact the distribution of the output distribution, affecting in particular the confidence bounds. Hence, it is important to account for statistical dependencies among the variables if they exist [2–4]. Statistical correlations are introduced into failure data by many causes. Three typical ones are [5]: 1. Use of identically designed and manufactured components. 2. Plant operation and maintenance by the same staff and 3. Dependent failure modes.

While fully correlated epistemic parameters are relatively easy to handle, there are challenges to treating partial correlations. There are several obstacles that complicate the handling of correlation among basic events. One is that empirical information is usually lacking. A second is distinguishing between the causes of correlation and those for common-cause failures. This is partially addressed in next section. Finally, if the correlation among basic events is partial, the propagation of uncertainties become complex (complete correlation is easy to implement).

A.K. Verma et al., *Reliability and Safety Engineering*,
Springer Series in Reliability Engineering,
DOI 10.1007/978-1-4471-6269-8_14

To handle the propagation of uncertainties in PSA in the presence of correlations, only three of above mentioned methods are useful: (i) Method of moments [6–8], (ii) P-box approach [9, 10] and (iii) Monte Carlo simulation. There are several strategies a Monte Carlo analyst can use to account for knowledge and uncertainty about correlations. These include assuming independence, assuming perfect covariance, assuming linear dependency, or assuming observed correlations. The probability bounds approach can account for dependencies among variables in the similar manner as the Monte Carlo approach. However, the method of moments and bounds method are difficult to implement in large scale problems when partial correlations are present instead of fully correlated data. Section 14.1.2 presents an approach based on Monte Carlo simulation with Nataf Transformation of generating correlated random variables for uncertainty propagation in FTA. A case study on Main Control Power Supply System (MCPS) of Nuclear Power Plant (NPP) has been carried out. Section 14.1.3 presents the case study and discussion on the obtained results. The effect of correlated basic events on the mean and uncertainty bounds of the top event is investigated with and without the common cause failure models.

14.1.1 Dependency: Common Cause Failures versus Correlated Epistemic Parameters

PSA/FT analyses for complex engineering systems inevitably involve uncertainties due to uncertainties present in models, parameters of the model, phenomena and assumptions. Randomness in the failure/repair phenomena and given the limitations in assessing the parameters of the failure/repair probability density functions lead to two types of uncertainties. The inherent variability of failures and repairs times of equipment is referred as ‘randomness’, ‘stochastic uncertainty’, ‘aleatory uncertainty’, and cannot be reduced. The aleatory uncertainty for a random variable (time to failure or repair) is represented with probability distributions. Limitations (scarcity or lack of data) in exactly assessing the parameters of these probability distributions are a further source of uncertainty. This uncertainty is known as “epistemic uncertainty”; it depends on the state-of-knowledge and can in general be reduced with more information. PSA models, by combining Fault Trees (FTs) and Event Trees (ETs), produce a mathematical expression for a system measure (e.g. unavailability or failure probability) as a function of failure rate/failure probability of constituting components and human actions. PSA inherently contains both the uncertainties. Treatment of both the types of uncertainties in PSA is essential for effective decision making in safety management [11–14]. FT/ET analysis addresses the aleatory uncertainty in the PSA models. Uncertainty analysis quantifies uncertainty in the model output arising due to epistemic uncertainties in input parameters of the model.

Dependencies exist inherently in engineering systems among the constituting components (in general basic events) due to several reasons (USNRC 1993, 2007) [15, 16]. Dependent failures whose root causes are not explicitly modeled are known as common cause failures (CCFs). Multiple failure events for which no clear root cause event identified, can be modeled using implicit methods categorized as CCF models thus CCF represent residual dependencies that are not explicitly modeled in ET/FTs. CCFs are classified as due to design, construction, procedural and environmental causes. These can be further sub-divided as due to functional deficiencies, realization faults, manufacturing, installation, test and maintenance, operation, human error, normal extremes and energetic extremes. CCF models dependency in these aleatory random variables of PSA.

In uncertainty analysis of PSA, unavailability or failure rate of basic events is considered as uncertain parameter (is epistemic due to its nature) and generally characterized with a lognormal distribution with median and error factor as parameters of the distribution [17]. The uncertainty analysis of PSA quantifies uncertainty in system characteristic by synthesizing uncertainties in basic event characteristics.

Table 14.1 gives the summary of comparison between dependencies of epistemic and aleatory variables. CCF analysis models dependency in aleatory random variables. CCF groups are defined for identical components in redundant trains of a system and should have implicit dependency leading to simultaneous failures. However, in large engineering systems, identical components may also be used in diverse, non-redundant systems. Moreover, the epistemic uncertainty in unavailability/failure rate of all the identical components will have dependency. This dependency is taken into consideration by taking correlation coefficient among the identical epistemic parameters [5–8].

Table 14.1 Comparison between different dependencies in PSA

	Dependency in aleatory variables	Dependency in epistemic variables
Phenomena in PSA	Failure on demand, time to failure, time to repair, etc.	Failure rate or repair rate or unavailability
Source	Identical redundant components in a system, etc.	Epistemic parameters of identical components
Where is it modeled?	In fault tree/event tree by CCF models	Uncertainty analysis over system risk function considering correlation
Higher dependency	Simultaneous failure of redundant components	Simultaneous high/low values for parameters of correlated components
Lower dependency	Lesser tendency for simultaneous failure	Lesser tendency for similar values for parameters of correlated components
Impact on the results	Both on mean and tails of the distribution for system measure	Both on mean and tails of the distribution for system measure

14.1.2 Methodology for PSA Based on Monte Carlo Simulation with Nataf Transformation

Monte Carlo simulation is most widely used technique for uncertainty propagation in PSA [18]. System model function as a precise analytical expression is required for the uncertainty propagation. Fault tree analysis can be used to get an analytical expression for the system model as a function of parameters of the basic events. The uncertain input parameters of the the system model are characterized as random variables, represented with a probability distribution. Uncertainty propagation with Monte Carlo consists of generating a random sample of the input parameters and determining the system measure from each set of inputs in the sample.

There are various random sampling approaches like crude sampling, Latin hypercube sampling, importance sampling, etc. This approach is good as long as the input parameters are independent or fully dependent. When some input parameters are fully dependent, a single random variable can be used to represent them in the simulation. The complexity arises when there is partial correlation and the probability distributions are non-normal. The correlations among the parameters then need to be accounted for in generating the random samples. Nataf transformation based approach was used in solving structural reliability problems where there were correlations among the input parameters [19]. The same approach is adopted here to generate correlated random samples for uncertainty propagation.

Uncertainty propagation for correlated basic events through Monte Carlo simulation with Nataf Transformation is presented in the Fig. 14.1, and the procedure is explained below [20]:

1. The first step is to obtain the required information for simulation. Information regarding Minimal Cut Set (MCS) from FTA of the given system, the Probability Density Function (PDF) of uncertain parameters, correlations between the parameters is obtained.
2. Uncertainty propagation model, $Y = f(X_1, X_2 \ldots.X_n)$, as an analytical expression is determined. Y is the system measure (e.g. unavailability, failure probability) or model output. X_i is the *i*th parameter of 'n' number of uncertain input parameters.
3. The simple termination criterion is to fix the number of iterations before the simulation. Monte Carlo simulation gives an excellent approximation of the system model distribution with a large number of iterations. The large number of iterations requires more computational resources. It is important to check how much number of iterations is large enough for the given problem. The problem of uncertainty propagation in FTA or in the PSA model does not take large computational time for the whole simulation. Hence, 10^4–10^5 iterations can be chosen with the crude sampling method. However, there are several methods (sampling approaches and termination criteria) to improve the efficiency of simulation [21, 22]. For example, determining the number of iterations during the simulation; one such useful technique is that the sample size required to obtain a result that is within a pre-specified confidence interval can be determined [21].

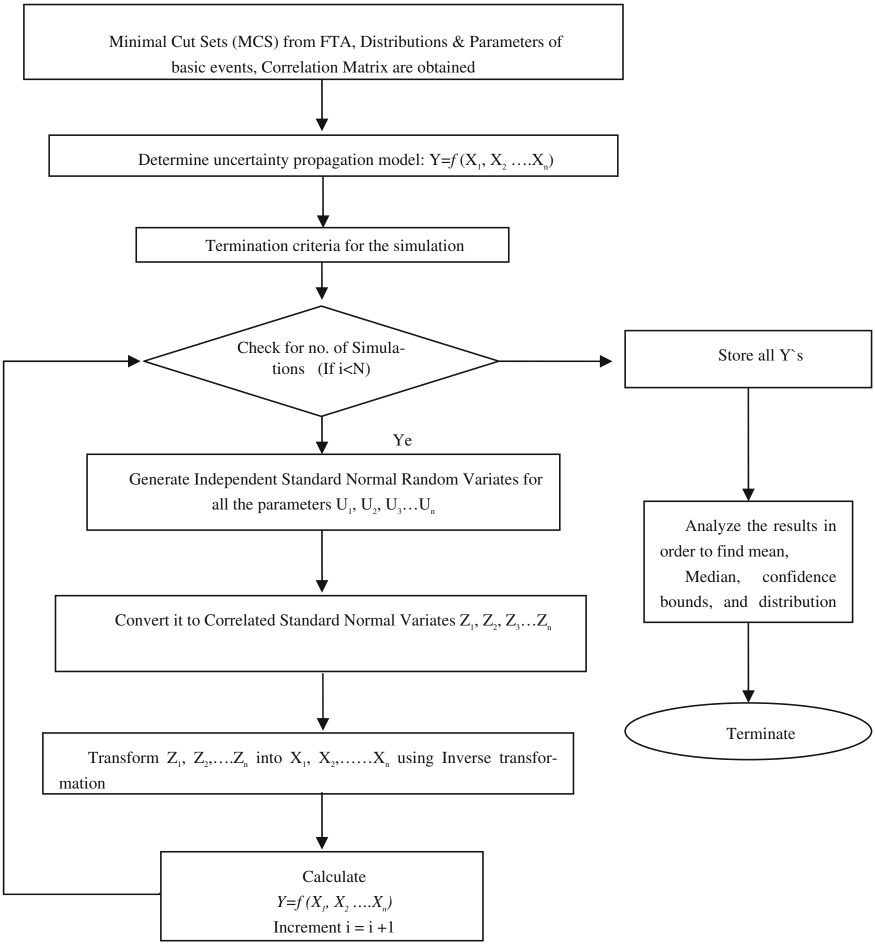

Minimal Cut Sets (MCS) from FTA, Distributions & Parameters of basic events, Correlation Matrix are obtained
Determine uncertainty propagation model: Y=*f* (X_1, X_2 ….X_n)
Termination criteria for the simulation
Check for no. of Simulations (If i<N)
Store all Y`s
Ye
Generate Independent Standard Normal Random Variates for all the parameters U_1, U_2, U_3…U_n
Analyze the results in order to find mean, Median, confidence bounds, and distribution
Convert it to Correlated Standard Normal Variates Z_1, Z_2, Z_3…Z_n
Terminate
Transform Z_1, Z_2,….Z_n into X_1, X_2,……X_n using Inverse transformation
Calculate
$Y=f(X_1, X_2 ….X_n)$
Increment i = i +1

Fig. 14.1 Uncertainty propagation for PSA having correlated basic events based on MC simulation with Nataf Transformation

4. For each iteration up to the pre-defined number ***N***, correlated random variates for the basic events are generated using the Nataf transformation [19, 23]. The steps for generating correlated random samples is as follows:

   4.1 Generate ‘n’ independent standard normally distributed random variates, Say U_1, U_2, U_3… U_n. Two uniform random numbers are required to generate a normal variate.

4.2 Calculate ρ'', using ρ and F by the formula given by Eq. (14.1).

$$\rho'' = \begin{pmatrix} \rho_{11} & \cdots & \rho_{1n} \\ \vdots & \ddots & \vdots \\ \rho_{n1} & \cdots & \rho_{nn} \end{pmatrix} \times \begin{pmatrix} F_{11} & \cdots & F_{1n} \\ \vdots & \ddots & \vdots \\ F_{n1} & \cdots & F_{nn} \end{pmatrix} \tag{14.1}$$

Where
ρ'' is modified correlation coefficient matrix used for further calculations
ρ is correlation matrix of input parameters
F is a coefficient defined by Nataf which has the following properties

a. F is independent of ρ_{ij} if one of the variables is normal.
b. F is invariant to increasing linear transformation of X_i and X_j.
c. F is independent of the parameters of Group I distributions (Normal, Uniform, Exponential, Rayliegh).
d. F is a function of the coefficient of variation $\delta = \sigma/\mu$ of Group II distributions (Lognormal, Gamma).

Based on this 4 properties 5 categories of formulae for F were mentioned in [19, 23], they are as follows

i. $F = Constant$ for X_j belonging to group I and X_i normal.
ii. $F = f(\delta_j)$ for X_j belonging to Group II and X_i normal.
iii. $F = f(\rho_{ij})$ for X_i and X_j belonging to Group I.
iv. $F = f(\rho_{ij}, \delta_j)$ for X_i belonging to Group I and X_j belonging to Group II.
v. $F = f(\rho_{ij}, \delta_i, \delta_j)$ for both X_i and X_j belonging to Group II.

4.3 Calculate correlated standard normally distributed random numbers by

$$\begin{bmatrix} Z_1 \\ Z_2 \\ Z_n \end{bmatrix} = Cholesky[\rho''] \times \begin{bmatrix} U_1 \\ U_2 \\ U_n \end{bmatrix} \tag{14.2}$$

4.4 Now transform $Z_1, Z_2, \ldots Z_n$ into $X_1, X_2, \ldots X_n$ using inverse transformation

$$X_i = F_{X_i}^{-1}[\phi(Z_i)] \tag{14.3}$$

5. The system measure is evaluated using the function 'Y' with the random sample generated from step 4.4. The value of system measure Y_i is stored.
6. Steps 4 to 5 are repeated until the termination criteria (pre defined number of simulations) is satisfied.
7. The results are analyzed to calculate the mean, confidence bounds, and distribution of the system measure.

14.1.3 Case Study

The 240 V AC Main Control Power System (MCPS) [24] is an important support system in Nuclear Power Plant (NPP) which supplies uninterrupted AC power to safety related loads such as reactor regulation systems and safety system loads such as shut down systems. The schematic diagram of MCPS is shown in Fig. 14.2. There are four Uninterrupted Power Supplies (UPSs) namely, UPS-1, UPS-2, UPS-3 and UPS-4; and four UPS batteries (BY) viz., BY-1, BY-2, BY-3 and BY-4. UPS-1, UPS-2 and UPS-3 have built-in static switches for transferring the load to a standby UPS, UPS-4. Ch-A/D/Y (Bus F2) loads are fed from UPS-1, Ch-B/E/Z (Bus F6) loads are fed from UPS-2, Ch-C/F (Bus F4) loads are fed from UPS-3, and UPS-4 is standby UPS. The standby UPS replaces a failed UPS within 20 ms through a static switch. Each BY provides 60 min battery back-up to the respective UPS loads in case the input supply to UPS fails. Input supply to UPS-1 and UPS-3, and UPS-2 and UPS-4 is taken from division I and division II of class III respectively. To ensure high reliability of the system, diversity and redundancy is provided from the input power supply side.

In order to compare the impact of correlations in epistemic parameters and CCF, two set of calculations have been done. In the first case, it is assumed that CCF failures are not present. In the second case, CCF failures are considered in the modeling.

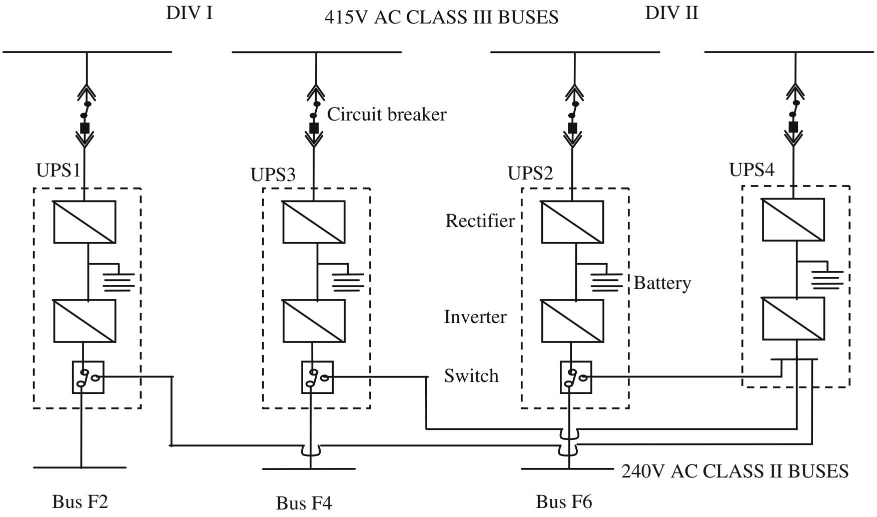


Fig. 14.2 Schematic diagram of 240 V AC control power supply system of NPP

14.1.3.1 Case A: Effect of Correlation Alone: No CCF Modeled in Fault Tree

An unavailability model is obtained with the help of fault tree analysis technique. The failure criterion is unavailability of power supply at 2 out of 3 buses (F2, F4, and F6). A fault tree is developed and the minimal cut-sets and unavailability of the system are obtained using Risk Spectrum [25]. There are 380 minimal cut sets in total. The first 20 minimal cut sets are shown in Table 14.2. The unavailability data of basic events is shown in Table 14.3. Uncertainty propagation has been carried out with this information. The correlation coefficient is varied from 0 to 1. Figure 14.3 gives the comparison of cumulative distribution function for the unavailability with different correlation coefficients. The summary of percentile values of unavailability is given in Table 14.4. The mean value has changed by 48 % when the correlation coefficient changes from 0 (no correlation) to 1. The 5 % value and 95 % value has changed by 59 and 104 % respectively for the same. As expected the 5 % value has decreased whereas the 95 % value has increased. In this case, neglecting correlations among epistemic parameters can have considerable impact on the mean and also on the tails of the uncertainty distribution.

Table 14.2 List of first 20 minimal cut sets (MPCS model without CCF)

S. no.	Probability	%	Event 1	Event 2	Event 3
1	1.562E-10	22.75	U1SW	U3SW	
2	1.562E-10	22.75	U1SW	U2SW	
3	1.562E-10	22.75	U2SW	U3SW	
4	3.200E-11	4.66	F6	U3SW	
5	3.200E-11	4.66	F2	U2SW	
6	3.200E-11	4.66	F6	U1SW	
7	3.200E-11	4.66	F2	U3SW	
8	3.200E-11	4.66	F4	U2SW	
9	3.200E-11	4.66	F4	U1SW	
10	6.554E-12	0.95	F2	F4	
11	6.554E-12	0.95	F2	F6	
12	6.554E-12	0.95	F4	F6	
13	1.331E-12	0.19	UPS1INV	UPS2INV	UPS4INV
14	1.331E-12	0.19	UPS1INV	UPS3INV	UPS4INV
15	1.331E-12	0.19	UPS1INV	UPS2INV	UPS3INV
16	1.331E-12	0.19	UPS2INV	UPS3INV	UPS4INV
17	1.512E-13	0.02	U1SW	UPS3INV	UPS4INV
18	1.512E-13	0.02	U2SW	UPS3INV	UPS4INV
19	1.512E-13	0.02	U2SW	UPS1INV	UPS4INV
20	1.512E-13	0.02	U3SW	UPS2INV	UPS4INV

Table 14.3 Unavailability of basic events

Component description	Component code	Unavailability	Remarks
Bus	Fi	2.56e-6	i = 1, 2, 3
UPS SWITCH	UiSW	1.25e-5	i = 1, 2, 3
UPS Inverter	UPSiINV	1.1e-4	i = 1, 2, 3, 4
UPS Battery	UPSiBATR	2.5e-4	i = 1, 2, 3, 4
UPS Rectifier	UPSiRECT	2.24e-5	i = 1, 2, 3, 4
UPS Circuit Breaker (CB)	UPSiCB	9e-6	i = 1, 2, 3, 4
Division Supply	DIVi	5.5e-4	i = 1, 2

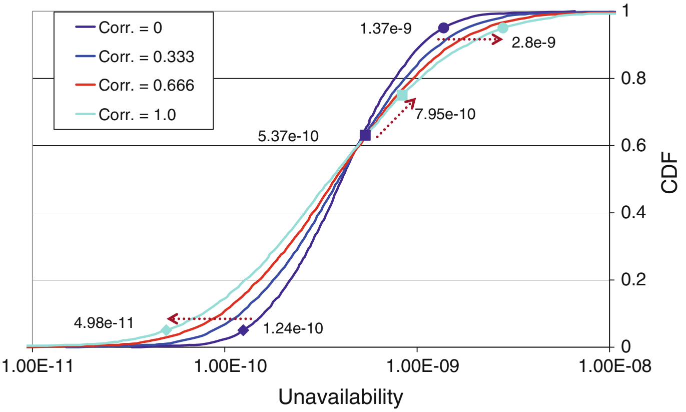


Fig. 14.3 Cumulative distribution of the system unavailability for various correlations (correlations alone, no CCF)

Table 14.4 Percentile values of unavailability with different correlations

	Unavailability			
Correlation	Mean	5 %	50 %	95 %
0	5.37e-10	1.24e-10	4.06e-10	1.377e-9
0.333	6.10e-10	8.73e-11	3.92e-10	1.79e-9
0.666	6.94e-10	6.503e-11	3.72e-10	2.28e-9
1.0	7.95e-10	4.98e-11	3.55e-10	2.805e-9

14.1.3.2 Case B: Effect of Correlation Combined with CCF Modeling

There are four common cause failure groups considered in the analysis, viz., UPS switch, Circuit Breaker (CB), UPS BYs, and division supplies. A CCF group for three static switches. In case of the CBs and BYs, there are four elements in each CCF group. The CCF group for division supply has two elements. An alpha-factor

Table 14.5 List of first 10 minimal cut sets (MPCS model with CCF)

S. no.	Probability	%	Event 1	Event 2
1	1.471E-07	25.28	UPSW-12	
2	1.471E-07	25.28	UPSW-13	
3	1.471E-07	25.28	UPSW-23	
4	1.398E-07	24.02	UPSW-ALL	
5	1.456E-10	0.03	U2SW	U3SW
6	1.456E-10	0.03	U1SW	U3SW
7	1.456E-10	0.03	U1SW	U2SW
8	3.835E-11	0.01	DIV-ALL	UPSBATR-ALL
9	3.089E-11	0.01	F6	U3SW
10	3.089E-11	0.01	F2	U2SW

model is used for CCF modeling and the parameters for CCF are taken from Vaurio (2007) [26], as shown in Table 14.6. There are 51 basic events (Table 14.7) identified in the system and 11968 minimal cut sets are obtained from the analysis. The first 10 minimal cut sets are shown in Table 14.5.

As discussed in Sect. 14.1.1, CCF analysis models dependency in the aleatory random variables. The elements of CCF group have to be in a redundant system and should have implicit dependency leading to simultaneous failures. However, there may be identical components in large engineering systems which may not be in a redundant system. Moreover, the epistemic uncertainty in unavailability of all the identical components will have dependency. This dependency is taken into consideration by taking correlation coefficient among the identical epistemic parameters. In the present system, apart from the CCF group elements, we have rectifiers, inverters, and buses as correlated epistemic random variables. The exact correlation value between the components is unknown. Hence simulations are carried out for correlations 0, 0.333, 0.666, and 1.

A lognormal distribution is considered for all epistemic distributions, with the mean value specified in Table 14.7 and an error factor of 3. Uncertainty propagation has been carried out for 10^4 iterations. Cumulative distribution function plots are shown for various correlation values in the graph in Fig. 14.4.

Table 14.6 CCF data

Component	Alpha factors			
	α_1	α_2	α_3	α_4
Division Supply	0.9686	0.0314		
Circuit Breaker	0.9549	0.0175	0.0103	0.0172
Battery	0.9757	0.0151	0.0069	0.0023
UPS-Switch	0.9842	0.012	0.0038	

Table 14.7 Unavailability of basic events

Component description	Component code	Unavailability	Remarks
Bus	Fi	2.56E-06	i = 1, 2, 3
UPS SWITCH	UiSW	9.65E-06	i = 1, 2, 3
CCF group of Switch with 2 elements	UPSW-ij	1.18E-07	ij: 12, 13, 23
CCF group of Switch with all	UPSW-ALL	1.12E-07	
UPS Inverter	UPSiINV	1.10E-04	i = 1, 2, 3, 4.
UPS Battery	UPSiBATR	0.00024	i = 1, 2, 3, 4
CCF group of Battery with 2 elements	UPSBATR-ij	2.4E-06	ij: 12, 13, 14, 23, 24, 34
CCF group of Battery with 3 elements	UPSBATR-ijk	1.7E-06	ijk: 123, 134, 234
CCF group of Battery with all	UPSBATR-ALL	2.2E-06	
UPS Rectifier	UPSiRECT	2.24E-05	i = 1, 2, 3, 4
UPS Circuit Breaker (CB)	UPSiCB	7.9E-06	i = 1, 2, 3, 4
CCF group of CB with 2 elements	UPSCB-ij	9.6E-08	ij: 12, 13, 14, 23, 24, 34
CCF group of CB with 3 elements	UPSCB-ijk	8.5E-08	ijk: 123, 134, 234
CCF group of CB with all	UPSCB-ALL	5.7E-07	
Division Supply	DIVi	5.33E-04	i = 1, 2
CCF group of both the divisions	DIV-ALL	1.73E-05	

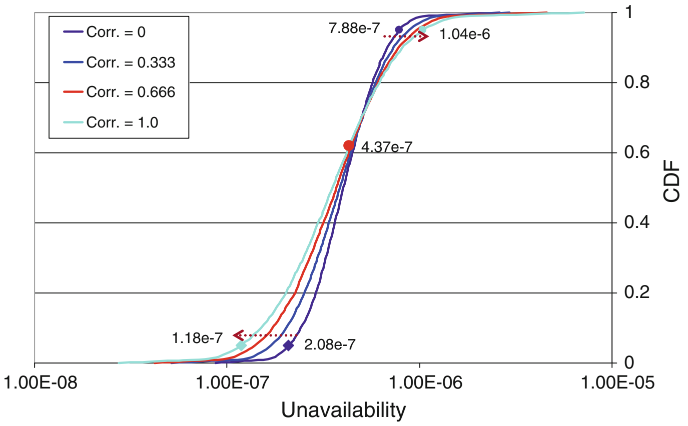


Fig. 14.4 Cumulative distribution of the system unavailability for various correlations with CCF treated

Table 14.8 Results obtained from Monte Carlo Simulation for 10^5 iterations

Correlation	Unavailability			
	Mean	5 %	50 %	95 %
0	4.39-7	2.08e-7	4.01e-7	7.88e-7
0.333	4.37e-7	1.68e-7	3.85e-7	8.84e-7
0.666	4.38e-7	1.39e-7	3.69e-7	9.69e-7
1.00	4.39e-7	1.18e-7	3.52e-7	1.04e-6

The result obtained from Monte Carlo simulation for 10^4 iterations is shown in Table 14.8; following important conclusions can be drawn from the values of unavailability:

1. 5 % values of unavailability are decreasing as correlation between the components is increasing from 0 to 1.
2. 50 % values of unavailability are decreasing as correlation between the components is increasing from 0 to 1.
3. 95 % values of unavailability are increasing as correlation between the components is increasing from 0 to 1.
4. Mean values remain almost same.

It is clear from Fig. 14.4 that the CDFs are crossing each other at 0.7, and the confidence interval of the unavailability increases as correlation among the components increases, hence the uncertainty.

In case (A), the correlation of the basic event parameters was observed to affect the mean unavailability of the MPCS as well as the confidence interval. In this case (B), the mean value is constant. The reason is that when CCF is modeled, CCF basic events will tend to be among the dominant minimal cut sets (refer Table 14.5). The top 4 minimal cut sets, contributing more than 99 % of the unavailability of the system, are not products but single (CCF) basic events (cf. Table 14.5). The mean values of these dominant sets are therefore not affected by the correlation. In contrast, the top 12 cut sets, which contribute about 99 % of the unavailability in Case (A), where CCF is not modeled, are all products. Table 14.9 summarizes the overall effect of varying correlation for case A (where CCF is not considered) and case B (where CCF is considered) on the mean, 5th percentile and 95th percentile of the unavailability. Increasing correlation in both cases increases the confidence interval. However, in comparison, the impact of common cause failures on the

Table 14.9 Comparison of percentile values of unavailability

	Mean		5 %		95 %	
Correlation	No CCF	CCF	No CCF	CCF	No CCF	CCF
0	5.37e-10	4.39e-7	1.24e-10	2.08e-7	1.37e-9	7.88e-7
0.333	6.10e-10	4.37e-7	8.73e-11	1.68e-7	1.79e-9	8.84e-7
0.666	6.94e-10	4.38e-7	6.50e-11	1.39e-7	2.28e-9	9.69e-7
1.00	7.95e-10	4.39e-7	4.98e-11	1.18e-7	2.80e-9	1.04e-6

Table 14.10 Mean and 95th percentile, multiplicative factor

	Mean system unavailability		
Correlation	No CCF	CCF	
0	5.37e-10	4.39e-7	$\frac{U_{ccf}(\rho=0)}{U_{no\_ccf}(\rho=0)}=818$
1.0	7.95e-10	4.39e-7	$\frac{U_{ccf}(\rho=1)}{U_{no\_ccf}(\rho=1)}=552$
	$\frac{U_{no\_ccf}(\rho=1)}{U_{no\_ccf}(\rho=0)}=1.5$	$\frac{U_{ccf}(\rho=1)}{U_{ccf}(\rho=0)}=1.0$	
	95th percentile		
Correlation	No CCF	CCF	
0	1.37e-9	7.88e-7	$\frac{U_{ccf}(\rho=0)}{U_{no\_ccf}(\rho=0)}=575$
1.0	2.80e-9	1.04e-6	$\frac{U_{ccf}(\rho=1)}{U_{no\_ccf}(\rho=1)}=371$
	$\frac{U_{no\_ccf}(\rho=1)}{U_{no\_ccf}(\rho=0)}=2.0$	$\frac{U_{ccf}(\rho=1)}{U_{ccf}(\rho=0)}=1.3$	

U unavailability; ρ correlation

mean is three orders of magnitude larger than the impact of correlations, as shown in Table 14.10.

The result of the case study suggests that, when CCFs are present and modeled, the correlations among epistemic parameters will affect principally the confidence bounds while leaving the mean unavailability to a larger degree unaffected. Accounting for correlation among the parameters will broaden the confidence bounds. It may also increase the mean unavailability slightly, whereby the effect is negligible when CCFs are modeled.

It is worth noting that when basic events are modeled with failure parameters as uncertain input parameters in a PSA software tool, in this case Risk Spectrum, the propagation of uncertainties generates values of the failure parameters and uses the same value in all basic events that refer to this failure parameter. This implements fully correlated identical basic events. However, defining the uncertainty distribution at the basic event level instead of using failure parameters defined for the identical components results in independent samples for identical basic events (correlation = 0.0). Consequently (at least in Risk Spectrum), if uncertainties are properly specified for identical components at the parameter level and CCF is modeled, the maximum effect of correlated parameters for identical components is accounted for.

Summary on Uncertainty Analysis with Correlated Basic Events

Dependencies exist inherently in engineering systems among the constituting elements due to several reasons. A comparison has been made between common cause failures, which introduce dependencies of aleatory variables, and correlations among epistemic variables. The impact of common cause failures over the system measure is generally much larger than the impact from the correlations of the failure rates.

However, assigning the level of correlation among the dependent epistemic parameters is still an open issue. In particular, there is an overlap among the causes cited for correlation and those cited for common cause failure modeling. This raises the issue of double-counting, with the exception of systems for which common cause failures are not usually modeled (identical components used in non-redundant systems). Uncertainty propagation methods in PSA available in the literature for correlated basic events are analytical and restricted to small applications. Uncertainty analysis in PSA with correlated basic events with Nataf Transformation in Monte Carlo simulation is explored. With the help of case studies it is suggested that the correlation among the basic events should be considered while conducting uncertainty analysis in PSA of complex systems, so as to prevent underestimating the uncertainty bounds.

14.2 Uncertainty Importance Measures

Reliability studies are useful for decision making towards safe, economical and efficient design and operation of complex engineering systems. Uncertainties are present in any reliability calculations due to randomness in the failure/repair phenomena and given the limitation in assessing the component parameters. Uncertainties at the component level are propagated to find uncertainty at the system level reliability. It is very important to identify all the uncertainties and treat them effectively to make reliability studies more useful for decision making. Conventional probabilistic approaches adopt probability distributions to characterize uncertainty where as fuzzy reliability models adopt membership functions to characterize uncertainty. Both the approaches are widely used in uncertainty propagation for reliability studies [27–58].

One of the major objectives in performing parameter uncertainty propagation is to rank the parameters with respect to their contribution to the uncertainty in the model prediction. The most obvious reason for this being that such a ranking makes it possible to allocate resources efficiently in case the reduction in the calculated uncertainties in the output prove necessary in order to reach an acceptable degree of confidence in the results.However, identification of critical parameters based on their uncertainty contribution at the system level is very important for effective management of uncertainty. The process of identifying components from uncertainty contribution point of view is called uncertainty importance measures. It is different from functional importance, which denotes the criticality of the component in the successful/failure operation of whole system. The methods required for this kind of ranking will depend upon the type of uncertainty propagation method used. In the probabilistic framework, there are several methods available in the literature for uncertainty importance measures such as non parametric methods and variance based methods [59–64]. They are useful in identifying the critical uncertain parameters and further with more information reducing the uncertainty. In fuzzy reliability framework, importance measures from functional (or structural) point of view are available in the literature and work on fuzzy uncertainty importance measure is attempted by Utkin [65, 66]. A new approach is discussed in the fuzzy framework where uncertain parameters are ranked based on their contribution of uncertainty of system reliability. It is compared with probabilistic methods (Pearson correlation coefficient and variance based methods) with the help of a case study on reactor protection system.

14.2.1 Probabilistic Approach to Ranking Uncertain Parameters in System Reliability Models

The expression of the system reliability (or availability), Y, as a function of the component reliabilities (X_i) is written as:

$$Y = f(X_1, X_2 \ldots X_n) \tag{14.4}$$

This relation can be obtained from fault tree analysis technique which denotes system failure logic with various failure combinations of one or more components. Due to scarcity or lack of data, it is not possible to exactly give a fixed value to the reliability of each of the components. In case of probabilistic approach, reliability of components is treated as a random variable represented by a probability distribution. Uncertainty in system reliability is obtained by propagating component uncertainties through Monte-Carlo simulation. But it is equally important to identify which component is contributing more uncertainty to system reliability as this information is required for effective management of uncertainty. This helps in identifying the components for which more information should be collected so that the uncertainty in the calculated system reliability can be reduced. In the probabilistic framework, various methods used for uncertainty importance measures are just briefed here.

14.2.1.1 Correlation Coefficient Method

One fairly simple and straightforward method of ranking uncertain parameters is to calculate the sample. Correlation coefficient of the model prediction and each of the uncertain parameters, using the sample of output values and the corresponding sample of values for each input. Consider ‘m’ samples from the output and a single input, denoted as y_j, x_j for j = 1–m. The sample (or Pearson) correlation coefficient is computed from the following equation (Abrahamsson [67] and Borgonovo [64]):

$$r_{XY} = \frac{\sum_{j=1}^{m} (x_j - \bar{x})(y_j - \bar{y})}{\sqrt{\sum_{j=1}^{m} (x_j - \bar{x})^2 \times \sum_{j=1}^{m} (y_j - \bar{y})^2}} \tag{14.5}$$

The correlation coefficient provides an estimate of the degree of linear relationship between the sample values of the model output and the input parameter.

This is done for every input parameter, providing a measure of how much each input contributes to the output uncertainty. The sign of the coefficient tells us the direction of the relationship, and the absolute value of the coefficient indicates the strength of the relationship (where −1 indicates a completely negative linear relation and +1 a completely positive linear relation).

14.2.1.2 Variance Based Method

Variance based techniques explain V_Y, i.e. the variance of Y, in terms of variances of the individual parameters or parameter groups. They identify the parameters that contribute to over all uncertainty in Y the most, as follows. V_Y can be written in terms of individual parameter and parameter group contribution as Iman [62]:

$$V_Y = \sum_i V_i + \sum_{i<j} V_{ij} + \sum_{i<j<m} V_{ijm} + \ldots + V_{12\ldots n} \tag{14.6}$$

where n is the number of parameters, X_i denotes the *i*th parameter, $E(Y|X_i = x_i^*)$ denotes the expectation of Y conditional on X_i having a fixed value x_i^*. $V_i = V(E(Y|X_i = x_i^*))$ stands for the variance over all possible values of x_i, and analogous definitions hold for the higher order terms.

First order global sensitivity indexes can be introduced using Eq. (14.31) as [61]:

$$S(x_i) = V_i/V_Y \tag{14.7}$$

Parameters that have a higher contribution to the variance will have higher conditional variances V_i, and therefore will have higher $S(x_i)$ is then taken as the uncertainty importance measure of the individual parameter x_i.

14.2.2 Method Based on Fuzzy Set Theory

In fuzzy set theory based uncertainty analysis, component reliability is treated as a fuzzy number and the variability is characterized by the Membership Function (MF). The membership function is usually assumed to be a triangular function and is treated as a possibility distribution. Having the model output expression (Y) from fault tree analysis and membership function information for parameters (X_i), fuzzy arithmetic based on α-cut method for fault trees [31] can be used to find membership function for model output, system reliability. Several authors worked extensively in applying fuzzy set theory to system reliability analysis in assessing uncertainty in reliability models. However, one of the major objectives in performing parameter uncertainty propagation is to rank the parameters with respect to their contribution to the uncertainty in the model output. Many measures are available in probabilistic approaches which are explained in the previous section. In the context of fuzzy reliability models, an algorithm is explained here for characterizing uncertainty importance measures which is shown in Fig. 14.5. This fuzzy uncertainty importance measure plays an important role in the reduction of uncertainty, for it is used to identify those sources of uncertainty having greatest impact on system reliability.

Fuzzy uncertainty importance measure is introduced as [68]:

$$FUIM_i = \frac{Y_i^R}{Y_i^L} \tag{14.8}$$

where Y_i^R is system model output, system unavailability (for repairable engineering systems unavailability is appropriate measure of reliability) with *i*th component parameter value at the most pessimistic value (for α = 0, upper value) and remaining components are as per the given membership functions. Y_i^L is unavailability with *i*th component parameter value at the most optimistic value (for α = 0, lower value) and remaining components are as per the given membership functions. Parameters that have higher value of above measure will contribute more uncertainty to the system unavailability.

$$x_0 = \frac{\int_{-\infty}^{+\infty} xf(x)dx}{\int_{-\infty}^{+\infty} f(x)dx} = \frac{\int_a^b xf^L(x)dx + \int_b^c xf^R(x)}{\int_a^b f^L(x)dx + \int_b^c f^R(x)} \tag{14.9}$$

$$y_0 = \frac{\int_0^1 y(g^R(y) - g^L(y))dy}{\int_0^1 (g^R(y) - g^L(y))dy} \tag{14.10}$$

$$D_i = \sqrt{x_0^2 + y_0^2} \tag{14.11}$$

But $\mathrm{FUIM_i}$ is a fuzzy set and based on this it is difficult to rank the components as per their shape of membership function. Hence ranking of fuzzy numbers is required to compare the fuzzy uncertainty importance measures. Method proposed based on the centroid calculation and distance between origin and centroid is adopted here as it is more efficient than other methods [69, 70]. Centroid for a triangular fuzzy number can be calculated using Eqs. (14.9) and (14.10). The distance between centroid and origin denoted with $\mathrm{D_i}$, provides a measure of uncertainty importance as shown in Eq. (14.11). $\mathrm{D_i}$ has to be calculated for all the components of the system. Component having highest value of $\mathrm{D_i}$ is the most critical uncertain parameter. Now components will be ranked based on the value of $\mathrm{D_i}$ in the decreasing order as it is a crisp value.

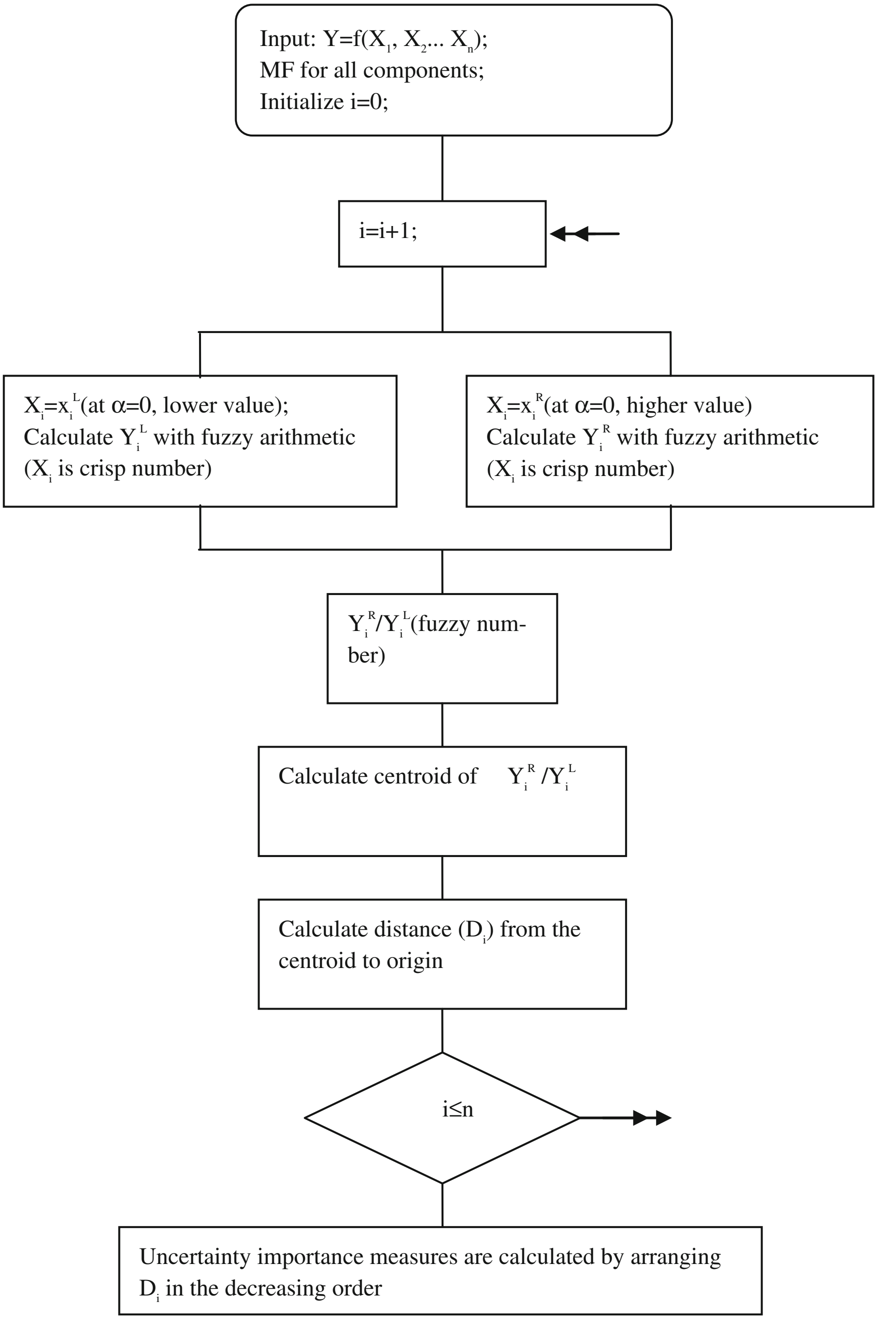

Input: $Y=f(X_1, X_2... X_n)$;
MF for all components;
Initialize i=0;
i=i+1;
$X_i=x_i^L$(at α=0, lower value);
Calculate Y_i^L with fuzzy arithmetic
(X_i is crisp number)
$X_i=x_i^R$(at α=0, higher value)
Calculate Y_i^R with fuzzy arithmetic
(X_i is crisp number)
Y_i^R/Y_i^L(fuzzy number)
Calculate centroid of Y_i^R/Y_i^L
Calculate distance (D_i) from the centroid to origin
i≤n
Uncertainty importance measures are calculated by arranging D_i in the decreasing order

Fig. 14.5 Algorithm for calculation of fuzzy uncertainty importance measures

14.2.3 Application to a Practical System

This section applies the algorithm discussed in the previous section to a practical system, reactor protection system [71]. Simplified fault tree for reactor protection system is shown in Fig. 14.6. The expression for the top event (failure probability or unavailability of the system) of the fault tree is the sum of minimal cut-sets as expressed in Eq. (14.12). All basic events of fault tree (components of system) are assumed to be mutually independent and log-normally distributed in probabilistic calculations and triangular membership functions in fuzzy framework with the same median and tail values (90 % confidence bounds) as that of probability distribution. The component data is shown in Table 14.11.

$$\begin{aligned} Y &= f(X_1, X_2 \ldots X_n) \\ &= X_1 + X_7X_8 + X_9X_6 + X_3X_5 + X_8X_5 + X_3X_9 + X_8X_9 \\ &\quad + X_3X_4 + X_2X_5 + X_8X_4 + X_2X_9 + X_2X_4 \end{aligned} \tag{14.12}$$

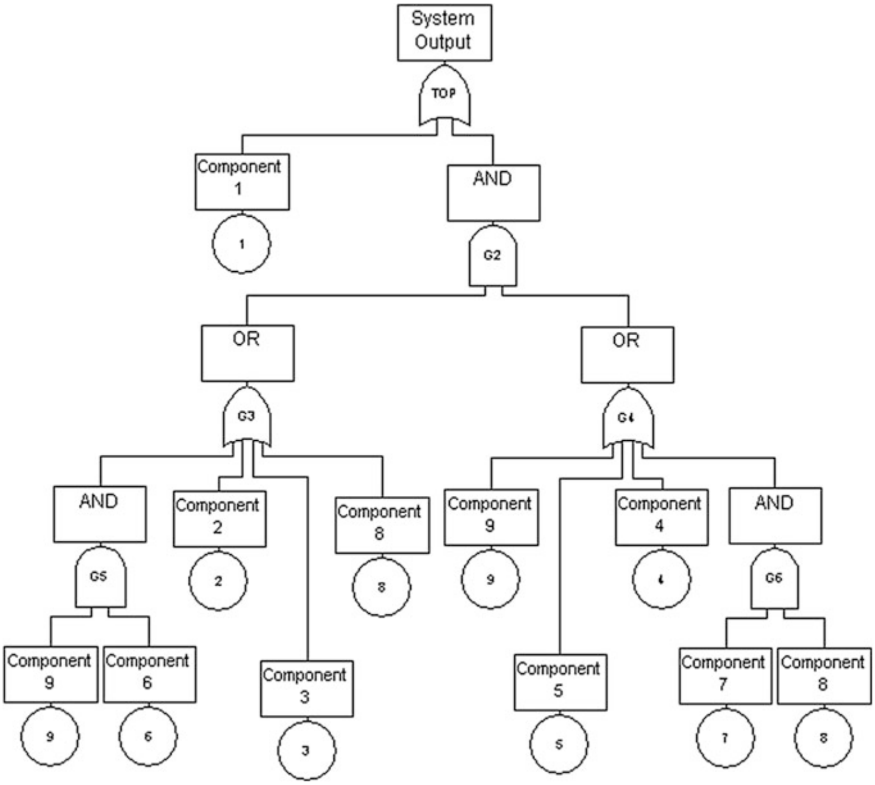


Fig. 14.6 Simplified fault tree for the reactor protection system

Table 14.11 Component data

Component	Probabilistic approach (lognormal)		Fuzzy approach (triangular)		
	Median probability	90 % error factor	Low	Median	High
1	1.7e-5	10	1.70E-06	1.70E-05	1.70E-04
2	3.6e-4	3	1.20E-04	3.60E-04	1.08E-03
3	1.0e-3	3	3.33E-04	1.00E-03	3.00E-03
4	3.6e-4	3	1.20E-04	3.60E-04	1.08E-03
5	1.0e-3	3	3.33E-04	1.00E-03	3.00E-03
6	6.1e-3	4	1.53E-03	6.10E-03	0.0244
7	6.1e-3	4	1.53E-03	6.10E-03	0.0244
8	9.7e-4	10	9.70E-05	9.70E-04	9.70E-03
9	9.7e-4	10	9.70E-05	9.70E-04	9.70E-03

In the probabilistic framework, two techniques as explained in previous section are adopted here. In the first method, Monte Carlo simulation with 10^6 iterations have been carried out which gave 10^6 sample of inputs (x_1, x_2 … x_9) and associated system output (y_i), where 'i' denotes iteration number. Pearson correlation coefficient has been calculated with the Eq. (14.5) for each component. This coefficient provides a measure of how much each input contributes to the output uncertainty, larger the value higher the contribution. They are shown in Table 14.12 and ranked in the decreasing order.

In the second method also, simulation has been carried out for 10^6 iterations and calculated variance V_Y from the sample of y_i. As per Eq. (14.6), V_i has to be calculated for each component. This has been done by carrying out simulation again keeping *i*th component at the fixed value (median) and allowing uncertainty in the remaining components. Expected value (mean) of Y_j is calculated from the simulation for a fixed value of X_i. The simulations are repeated ($j = 10^5$) for various

Table 14.12 Comparison of results for uncertainty importance measures

Component	Correlation coefficient		Variance based method		Proposed method	
	r_{XiY}	Rank	V_i/V_Y	Rank	D_i	Rank
1	0.621	1	0.4128	1	22.87	1
2	0.011	8/9	0.0011	8/9	9.703	8/9
3	0.024	6/7	0.0019	6/7	9.99	6/7
4	0.011	8/9	0.0011	8/9	9.703	8/9
5	0.024	6/7	0.0019	6/7	9.99	6/7
6	0.129	4/5	0.0271	4/5	11.41	4/5
7	0.129	4/5	0.0271	4/5	11.41	4/5
8	0.436	2/3	0.205	2/3	14.118	2/3
9	0.436	2/3	0.205	2/3	14.118	2/3

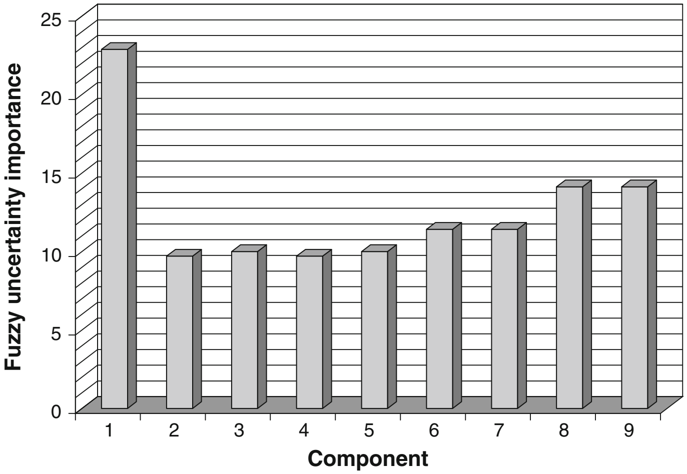


Fig. 14.7 Fuzzy uncertainty importance measure

values of X_i as per its PDF. V_i is obtained by calculating variance from the newly generated sample of Y_j. This procedure has been repeated for all the components and calculated first order global sensitivity index (Eq. 14.32). Larger the value of the index, higher will be the uncertainty contribution. Ranks are given to the component in the decreasing order of values of the index as shown in Table 14.12.

In the fuzzy framework, the algorithm explained in Sect. 14.2.3 has been applied and compared with the probabilistic methods. D_i has to be calculated for each component, which gives uncertainty importance measure. For components having higher value of D_i, uncertainty contribution will be larger. Ranks have been obtained based on the calculated D_i values of all components. They are shown graphically in Fig. 14.7. Ranking based on the proposed approach is exactly matching (see Table 14.12) with the conventional probabilistic approaches. The proposed method is very simple and also computational effort required is less compared with the probabilistic methods. Thus, in the fuzzy reliability models, the algorithm is able to rank the components based on their uncertainty contribution.

In addition, component importance measuresalso can be obtained from the same algorithm with small modification. In the calculation of Y_i^R, keep $X_i = 1$and for Y_i^L, keep $X_i = 0$.With this modification, obtained measure denotes importance of the component from the functional point of view. The results for the same system are shown in Table 14.13. Using ISOGRAPH commercial software [72], probabilistic based importance measures (Birnbaum importance) have been obtained (see Table 14.13). The ranking for 1, 6, 7, 8, 9 are same in both the cases. However, probabilistic approach is giving one rank for 2, 3, 4, 5 where as the proposed method is able marginally distinguishing 2, 4 from 3, 5. Fuzzy based approach looks more sensible when there is close importance between the components. Fuzzy functional importance is graphically shown in Fig. 14.8.

Table 14.13 Comparison of results for component importance measures

Component	Birnbaum importance (probabilistic)		Proposed method (fuzzy)	
	Value of measure	Rank	Value of measure	Rank
1	1	1	81780	1
2	2.33e-3	4/5/6/7	244.119	6/7
3	2.33e-3	4/5/6/7	254.265	4/5
4	2.33e-3	4/5/6/7	244.119	6/7
5	2.33e-3	4/5/6/7	254.265	4/5
6	9.7e-4	8/9	177.041	8/9
7	9.7e-4	8/9	177.041	8/9
8	8.4e-3	2/3	822.75	2/3
9	8.4e-3	2/3	822.75	2/3

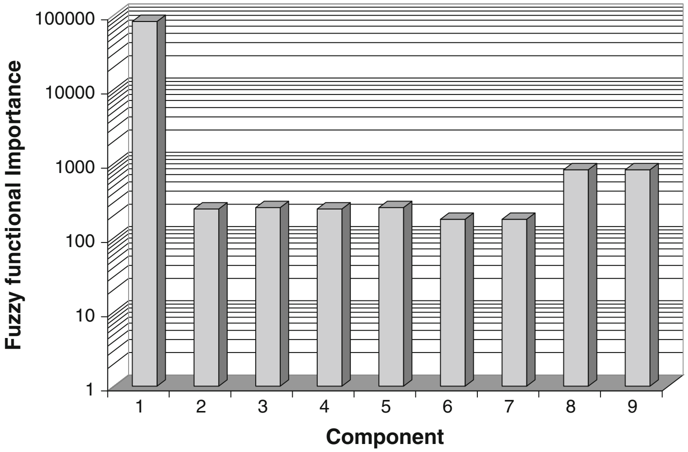


Fig. 14.8 Fuzzy functional importance measure

14.3 Treatment of Aleatory and Epistemic Uncertainties

The problem of acknowledging and treating uncertainty is vital for practical usability of reliability analysis results. The randomness in the failure/repair phenomena is classified under aleatory uncertainty and epistemic uncertainty is present in assessing the parameters of the failure/repair probability density functions. The distinction of uncertainties is useful for taking the reliability/risk informed decisions with confidence and also for effective management of uncertainty. It is required to treat both types of uncertainties to make the uncertainty analysis useful in decision making. Knowing the sources of uncertainty involved in the analysis plays an important role in handling it. If one knows why there are uncertainties and what kinds of uncertainties are involved, one has a better chance of finding the right methods for reducing them [13, 73–76].

14.3.1 Epistemic and Aleatory Uncertainty in Reliability Calculations

The inherent variability of failure and repair times of equipment imposes the use of probabilistic models; as such phenomena cannot be dealt with deterministic approaches. This variability is sometimes referred as 'randomness' or 'stochastic uncertainty', commonly known as 'aleatory uncertainty', which cannot be reduced. However, both deterministic and probabilistic approaches are built on a number of model assumptions and model parameters that are based on what is currentlyknown about the physics of the relevant processes and the behavior of systemsunder given conditions. There is uncertainty associated with these conditions,which depends upon state of knowledge, is referred as 'epistemic uncertainty' or 'subjective uncertainty'. It is important that the uncertainties in inherent variabilityof physical processes (i.e., aleatory uncertainty) and the uncertainties in knowledgeof these processes (i.e., epistemic uncertainty) are properly accounted for. The impact of these uncertainties must be addressed if the analysis is to serve as a tool in the decision making process.

Figure 14.9shows the two reliability curves with the two values of the failure rate.These curves are, of course, aleatory, since they deal with the observable quantity "time." The probability at time t is shown for each curve. Thus, for a given time t, the Fig. 14.9 shows clearly that there are two possible values of the reliability, eachwith its own probability. In this simple example, it is assumed that only

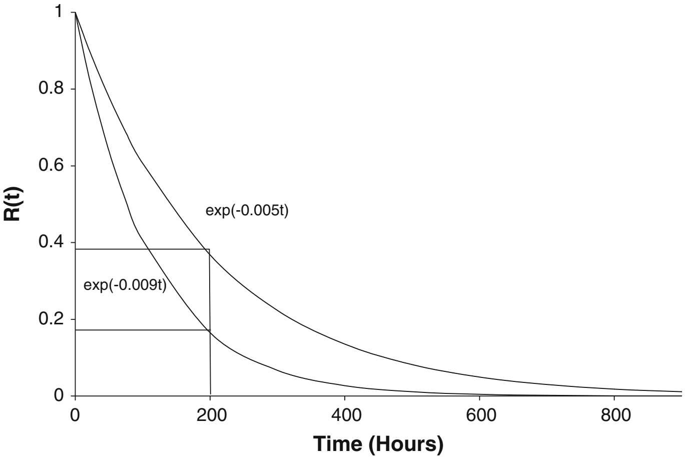


Fig. 14.9 Aleatory reliability curves with epistemic uncertainty

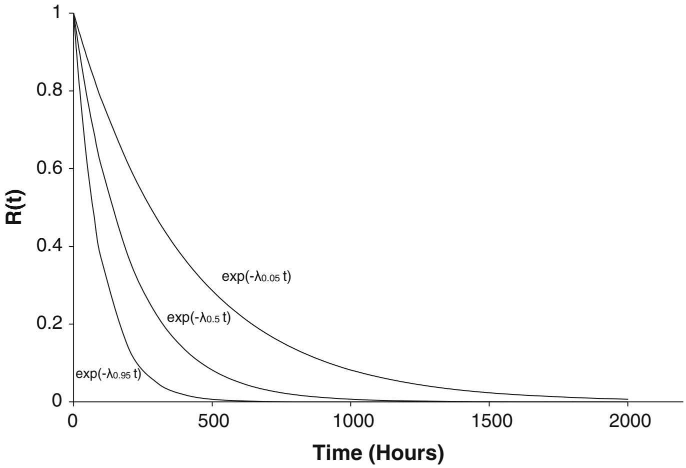


Fig. 14.10 Aleatory curves with continuous epistemic distribution

two valuesof the failure rate are possible. In real applications, the epistemic uncertainty epistemic uncertainty about λ is usually expressed using a continuous pdf π(λ). Then, it is customary to displaya family of curves for various percentiles of λ. Figure 14.10 shows three curveswith λ being equal to the 5th, 50th, and 95th percentiles of π(λ).

14.3.2 Need to Separate Epistemic and Aleatory Uncertainties

The first, and most important, reason for keeping epistemic and aleatory uncertainties separate is that it is mathematically more correct [76]. Mixing both the uncertainties means that one can not see how much of the total uncertainty comes from epistemic and aleatory uncertainties. If one knows that a large part of the total uncertainty is due to epistemic uncertainty (as shown in Fig. 14.11) then by collecting further information and thereby reducing total uncertainty one would be able to improve the estimate of the future. On the other hand, if the total uncertainty was nearly all due to variability (as shown in Fig. 14.12), it is a waste of time to collect more information and the only way to reduce the total uncertainty would be to change the physical system. In general, the separation of uncertainty allows understanding what steps can be taken to reduce the total uncertainty of the model, and allows gauging the value of more information or of some potential change to the system one can make. Vose [76] explained that a much larger problem than mixing epistemic and aleatory distributions together can occur when an aleatory distribution is used as if it were epistemic distribution. Separating uncertainties very

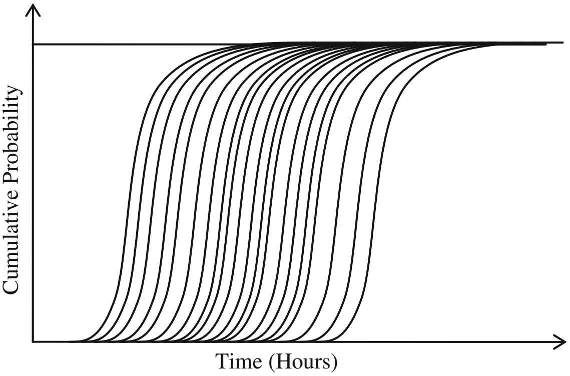


Fig. 14.11 Epistemic uncertainty domination

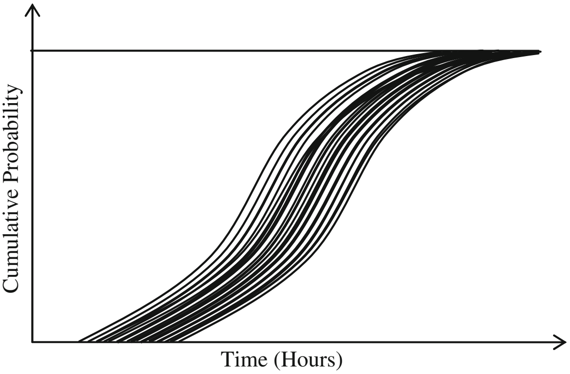


Fig. 14.12 Aleatory uncertainty domination

deliberately gives the discipline and understanding to avoid the much larger errors that this mistake will produce. Now, having understood how useful it is to separate uncertainties, one must see whether the effort is worth the extra information that can be gained as applicable to specific problems under consideration. This is because the separation of uncertainties is time consuming and cumbersome task.

14.3.3 Methodology for Uncertainty Analysis in Reliability Assessment Based on Monte Carlo Simulation

Level-1 PSA studies of NPP focus on evaluation of core damage frequency considering failure and maintenance characteristics of various process and safety systems in NPP. Availability is more commonly used to represent a maintainable system which is a function of reliability and maintainability. Reliability is a function of time to failure and maintainability is a function of time to repair. Hence, availability is the function of two random variables, viz., time to failure and time to repair. The fault tree approach is used which estimates the average unavailability based on failure rates, repair rates and demand failure probabilities (stand by failure rate) assuming all random variables (time to failure and time to repair of all components in the system) are following exponential distribution. However, randomness in unavailability is not quantified and also unavailability is approximated when there is a complex scenario, for example, stand-by tested maintenance policy. Availability modeling by stochastic simulation can quantify the aleatory uncertainty and also unnecessary assumptions can be eliminated in complex scenario. The second source of uncertainty in PSA is from parameters of PDF of failures and repairs. In case of exponential PDF, the parameter is known as failure rate/repair rate. Due to limitation in exactly assessing these parameters of the PDF, uncertainty is present in it. This type of uncertainty falls in epistemic classification as it can be reduced with more information. Having identified various uncertain parameters in the model, methodology is explained here based on two-phase Monte Carlo simulation to quantify and separate both kinds of uncertainty (see Fig. 14.13) [77].

14.3.3.1 Methodology

1. Information regarding PDF of Time to Failure (TTF, operating), time to failure (stand-by), and Time to Repair (TTR) of all components in the model are collected. The uncertainty in the parameters of PDF (epistemic uncertainty) is also generally characterized by a probability distribution. The current practice is assigning a lognormal distribution to epistemic uncertainty with a median and error factor (for most of the components IAEA TECDOC 478 gives error factor or 5 and 95 % values). The same is integrated further with new information (operating experience) if available to get improved estimate.
2. Distributions for PDF parameters of components are first sampled by any sampling approach, like crude or Latin-hypercube sampling approach. This action takes place in first loop of two loop sampling as depicted in Fig. 14.13. The first loop or outer loop focuses on epistemic uncertainty and the second loop or inner loop focuses on aleatory uncertainty.
3. Epistemic variables are treated as constants inside the second loop, i.e., the sampled values from step 2 are passed on to second loop. Now in the second loop, stochastic simulation has to be carried out. In addition to failure/repair characteristics, maintenance policies of all components have to be collected from the system technical specifications record. Information such as interval and duration of surveillance test and preventive maintenance actions are obtained in this step. System failure logic is obtained from qualitative FTA or RBD in the form of minimal cut-sets (combination of minimum number of component failures leading to system failures)
4. Generation of component state profiles Components are simulated for a specified mission time for depicting the duration of available (up) and unavailable (down) states. If component is repairable as is the case for most of practical systems, up and down states will come alternatively. Down state can be due to

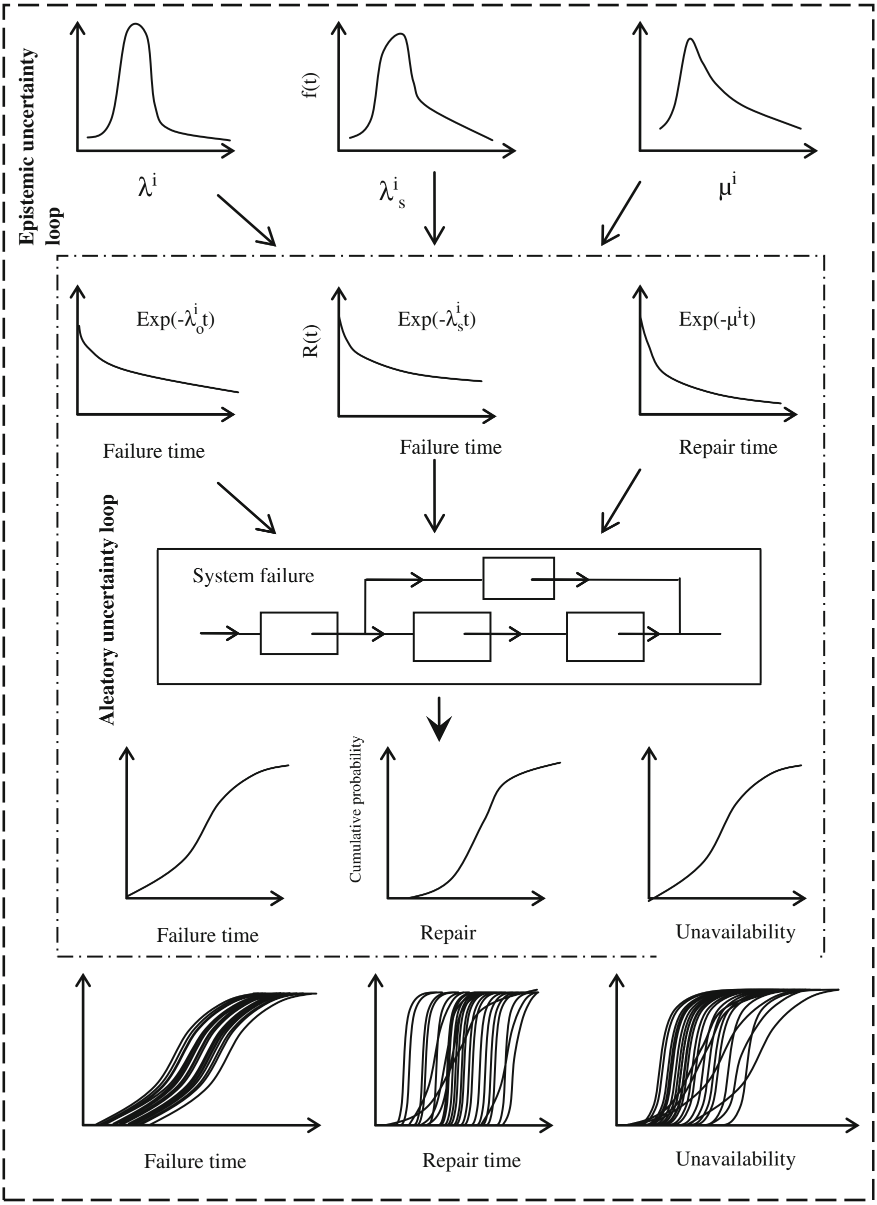


Fig. 14.13 A methodology for uncertainty analysis in level-1 PSA

failure or scheduled maintenance activity. Duration of the state is random for up state and also for down state if it is unscheduled repair, where as scheduled maintenance activity may be a fixed value.

4.1 *Active Components* Active component is the one which is in working condition during normal operation of the system. Active components can be either in success state or failure state. Based on the PDF of failure of component, time to failure is obtained from the random variant calculations. The failure is followed by repair whose time depends on the PDF of repair time. This sequence is continued until it reaches the predetermined system mission time.

4.2 *Standby/Dormant Components* These components are required on demand due to the failure of active components. When there is no demand, it will be in standby state or may be in failed state due to on-shelf failure. It can also be unavailable due to test or maintenance state as per the scheduled activity when there is a demand. This makes the component to have multi states and such stochastic behaviour need to be modelled to exactly suit the practical scenario. Down times due to the scheduled test and maintenance policies are first accommodated in the component state profiles. In certain cases test override probability has to be taken to account for its availability during testing. As the failures occurred during standby period can not be revealed till its testing, time from failure till identification has to be taken as down time. It is followed by imposing the standby down times obtained from the standby time to failure PDF and time to repair PDF. Apart from the availability on demand, it is also required to check whether the standby component is successfully meeting its mission. This is incorporated by obtaining the time to failure based on the operating failure PDF and is checked with the mission time, which is the down time of active component.

5. Generation of system state profile System state profile is developed by integrating components state profiles with the system failure logic. Failure logic of complex systems is generally derived from fault tree analysis, which is logical and graphical description of various combinations of failure events. Fault tree analysis represents failure logic of the system with the sum of minimal cut-sets. In other words, system logic is denoted with series configuration of parallel subsystems. Each minimal cut-set represents this subsystem which will have certain basic components in parallel.

5.1 State profile for each minimal cut-set is generated based on component state profiles obtained from steps 4.1 or 4.2. Down state is identified by calculating the duration that all the components in the cut-set under consideration are simultaneously unavailable as it is equivalent to a parallel configuration. MCS state is in up state in the remaining duration of the mission. Thus, state profile for MCS is also in up and down states alternatively through out its mission.

5.2 System states are generated from state profiles of MCS which are obtained from step 5.1. As system is in series configuration of all MCS, down state of every MCS imposes the same down state on the system. Thus all down states of all MCS are reflected in system state profile and the remaining time of the mission is in the up state.

6. Steps 4 and 5 are repeated for sufficient number of iterations and required measures of reliability such as PDF of TTF and TTR of system, availability, etc. are obtained from the simulation results. This is one time execution of inner loop and the uncertainty from randomness in reliability measures are obtained in this step.
7. Check for the number of times first loop has to be executed, if it is less than the predetermined number of iterations then go to step 2 where sampling is done again for epistemic parameters and subsequently entering second loop.
8. After sufficient number of iterations of the outer loop, the summarized results for failure time, repair time and unavailability looks like family of curves. Each cumulative probability curve of these reliability measure denotes the uncertainty due to randomness in failures and repairs, where as the spread is due to epistemic uncertainty in the parameters of PDFs.

14.4 Dempster-Shafer Theory

Basic building block of Dempster-Shafer theory is mass function *m*, which is also called as Basic Belief Assignment (bba) or Basic Probability assignment (bpa). It can be said as an analogue of probability, a weight associated to an elementary event. But, generally speaking, the term "basic probability assignment" does not refer to probability in the classical sense. The value of the bba for a given set A (represented as *m*(*A*)), expresses the proportion of all relevant and available evidence that supports the claim that a particular element of Ω (the universal set) belongs to the set A but to no particular subset of A. The value of *m*(*A*) pertains only to the set A and makes no additional claims about any subsets of A. Any further evidence on the subsets of A would be represented by another bba, *m* (*B*) would the bba for the subset *B*.

Consider example of decision problem with *n* possible elements or states of nature, which are mutually exclusive and totally exhaustive sets, represented by {a_1, a_2, a_3,…a_n}. Under the probability framework we assign probabilities to each state of nature and these probabilities must add to one. Under the belief function framework, basic belief masses or m-values are assigned not only to each state of nature but also to all possible combinations of these states of nature. For example in tossing of coin problem belief masses are assigned not only to head and tail but also to combined head and tail (though they can not occur at the same time).

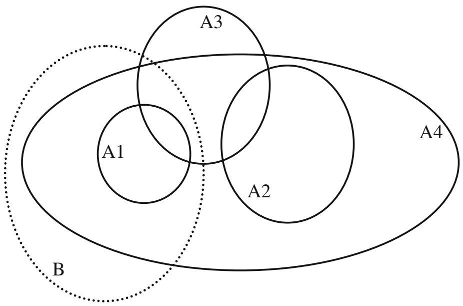


Fig. 14.14 Example problem

$$m(H) + m(T) + m(T, H) = 1$$

so that

$$m(T) + m(H) \neq 1$$

From the basic belief assignment, the upper and lower bounds of an interval can be defined. This interval contains the precise probability of a set of interest (in the classical sense) and is bounded by two non-additive continuous measures called Belief and Plausibility.

Example 4 If $F = \{A1, A2, A3, A4\}$ with $m(A_1) = 0.1$, $m(A_2) = 0.3$, $m(A_3) = 0.2$, $m(A_4) = 0.4$, then calculate belief and plausibility of B?

Solution Belief and Plausibility of the set B (Fig. 14.14) can be calculated as follows,

$$Bel(B) = \sum_{A_j/A_j \in B} m(A_j)$$

In this example, A_4 is fully contained in B and therefore

$$Bel(B) = m(A_1) = 0.1$$
$$Pls(B) = \sum_{A_j/A_j \cap B \neq \phi} m(A_j) = \text{Sum of all the sets which intersect with set}\, B$$

In this example, the sets A_1, A_3, A_4 intersect with B, the set A_2 and B does not intersect. Therefore $Pls(B)$ is sum of bbas of A_1, A_3 and A_4 only.

$$Pls(B) = m(A_1) + m(A_3) + m(A_4) = 0.1 + 0.2 + 0.4 = 0.7$$

Table 14.14 Basic belief assignment, belief and plausibility for example problem

Hypothesis	bba	Belief	Plausibility
Null	0	0	0
A	0.2	0.2	0.39
B	0.3	0.3	0.52
C	0.04	0.25	0.46
A or B	0.03	0.54	0.75
A or C	0.06	0.48	0.7
B or C	0.12	0.61	0.8
Any	0.1	1.0	1.0

Example 5 A person is suffering from any of the disease A, B or C and basic belief assignments for the possible sets are given in Table 14.14. Quantify the uncertainty about the disease.

Solution

$$\begin{aligned} Bel(\mathrm{A}) &= \text{sum of basic belief assignments of subsets of A } = \mathrm{m(A)} = 0.2 \\ \mathrm{Pls(A)} &= \text{sum of basic belief assignments of sets containing A} \end{aligned}$$

A can be present in a set containing A alone, a set containing A and B, a set containing A and C and set containing A, B and C. Therefore

$$\begin{aligned} \mathrm{Pls(A)} &= \mathrm{m(A)} + \mathrm{m(A,B)} + \mathrm{m(A,C)} + \mathrm{m(A+B+C)} \\ &= 0.2 + 0.04 + 0.03 + 0.12 = 0.39 \end{aligned}$$

Belief and plausibility for all hypotheses is shown in Table 14.14.

A belief measure (or a plausibility measure) becomes a *probability measure* when all focal elements are *singletons* or the evidences are disjoint. In this case, we have,

$$Bel(a) = prob(a) = Pl(a)$$

Dempster Shafer structure is useful tool in risk analysis including epistemic uncertainty. As epistemic uncertainty arises due to lack of knowledge and measurement uncertainty the question raised is how to assign basic belief assignment to particular uncertain variable. In turn there are five ways to do this:

1. Direct assumption
2. Modeling
3. Appeal to robust Bayes methods
4. Constraint propagation
5. Observation of measurements

14.4.1 Belief and Plausibility Function of Real Numbers

For a finite Dempster-Shafer structure with basic belief assignment m and n focal elements a_i having masses p_i. The upper bound for its distribution function is Pls(g(z)) is the set of all real numbers less than or equal to z. Where g(z) is the set of all real numbers less than or equal to z, $g(z) = \{x : x \in R,\ x \leq z\}$. Thus the function is

$$Pls(g(z)) = \sum_{\substack{i \\ a_i \cap g(z) \neq \phi}} m(a_i) \tag{14.13}$$

Associated lower bound on the distribution function is

$$Bel(g(z)) = \sum_{\substack{i \\ a_i \subset g(z)}} m(a_i) \tag{14.14}$$

Both of above functions are non-decreasing functions from the reals into [0,1].

For real numbers masses are assigned for elements having closed intervals and these intervals and masses are called as Dempster structure. It is collection of pairs consisting intervals and a mass. $\{([x_1,y_1], m_1), ([x_2,y_2], m_2), ([x_3,y_3], m_3), \ldots ([x_n,y_n], m_n)\}$, where $x_i \leq y_i$ for all i, $\sum m_i = 1$, and $y_i \neq y_j$ whenever $x_i = x_j$.

Example 6 Consider a uncertain variable x having Dempster Shafer structure {([0,6],1/15), ([3, 13], 1/15) ([6, 16], 1/15) ([10, 18], 1/15) ([11, 19], 2/15) ([12, 20], 1/15) ([14, 20], 1/15) ([16, 22], 1/15) ([17, 23], 1/15) ([19, 23], 1/15) ([23, 27], 1/15),([27, 29], 1/15), ([31, 33], 1/15), ([37, 39], 1/15),}. 1/15 is a belief mass associated with variable x lying between 0 and 6. Similarly various belief mass have been associated with variable x lying between the ranges. This Dempster structure is shown in Fig. 14.15.

Solution Plausibility and Belief for the variable x is calculated using Eqs. 14.13 and 14.14 respectively and is shown in Fig. 14.16.

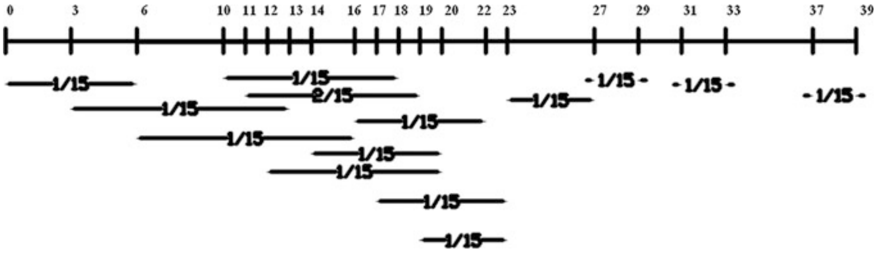


Fig. 14.15 Dempster Shafer structure

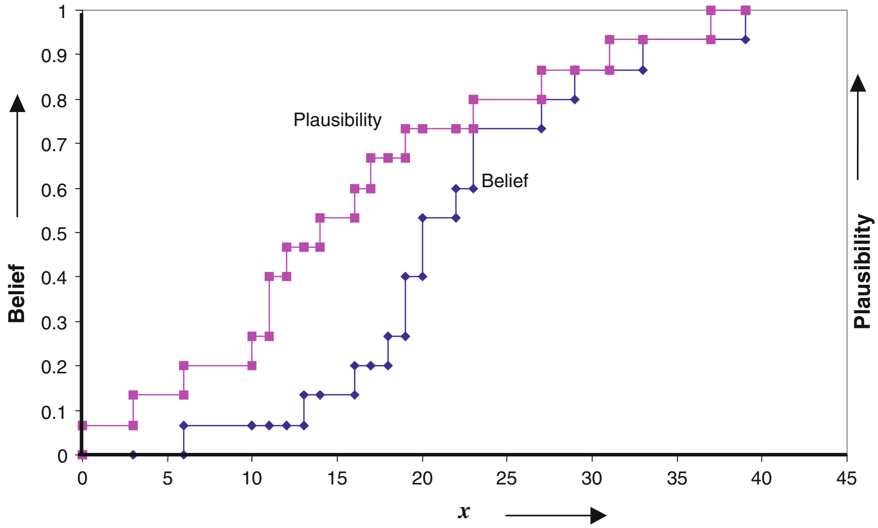


Fig. 14.16 Belief and plausibility for variable *x*

14.4.2 Dempster's Rule of Combination

Two BBA structures, m_1 and m_2, given by two different evidence sources, can be fused by Dempster's rule of combining in order to make a new BBA structure,

$$m(C) = \frac{\sum_{\substack{i,j \\ A_i \cap B_j = C}} m_1(A_i) m_2(B_j)}{1 - K} \tag{14.15}$$

where $K = \sum_{\substack{i,j \\ A_i \cap B_j = \phi}} m_1(A_i) m_2(B_j)$

K represents basic probability associated with conflict.

Example 7 From expert 1, for variable *a*, Dempster Shafer structure is {([0.6,1],0.3), ([1, 2], 0.6), ([2, 3], 0.1)} Let $A_1 = [0.6,1]$, $A_2 = [1, 2]$ and $A_3 = [2, 3]$ so that $m_1(A_1) = 0.3$, $m_1(A_2) = 0.6$ and $m_1(A_3) = 0.1$. Similarly, from expert 2, for the same variable *a*, Dempster structure {([0.6,3], 0.6), ([1, 2], 0.4)} Let $B_1 = [0.6,3]$ and $B_2 = [1, 2]$ so that $m_2(B_1) = 0.6$ and $m_2(B_2) = 0.4$.

Solution Since above two evidences comes from two different sources, Dempster's rule (Eq. 14.15) is used to combine them. The calculation using Dempster's rule is summarized in Table 14.15.

Table 14.15 Example—Combining evidences using Dempster's rule

Expert 1			Interval	bpa = m	Interval	bpa = m	Interval	bpa = m
			[0.6,1]	0.3	[1, 2]	0.6	[2, 3]	0.1
Expert 2	Interval	bpa = m						
	[0.6,3]	0.6	[0.6,1]	0.18	[1, 2]	0.36	[2, 3]	0.06
	[1, 2]	0.4	–	0.12	[1, 2]	0.24	–	0.04

We have to form power set C, such that its subsets are intersections of subset of A and subset of B.

Let C = {C_1,C_2,C_3} and C1 = [0.6,1] C_2 = [1, 2] C_3 = [2, 3]

Here value K (probability mass associated with conflict) is equal sum of product of bpas from two different sources, which are not intersecting. In above example A_1 is not intersecting with. Similarly A_3 is not intersecting with B_2.

$$\begin{aligned} K &= m_1(A_1)m_2(B_2) + m_1(A_3)m_2(B_2) \\ &= 0.330.4 + 0.130.4 = 0.12 + 0.04 = 0.16 \end{aligned}$$

Now using Eq. (14.15)

$$\begin{aligned} m(C_1) &= \frac{m_1(A_1)\,m_2(B_1)}{1-K} = \frac{0.3 \times 0.6}{1-K} = \frac{0.18}{1-0.16} = 0.2143 \\ m(C_2) &= \frac{m_1(A_2)\,m_2(B_1) + m_1(A_2)\,m_2(B_2)}{1-K} = \frac{0.6 \times 0.6 + 0.6 \times 0.4}{1-0.16} = 0.7143 \\ m(C_3) &= \frac{m_1(A_3)\,m_2(B_1)}{1-K} = \frac{0.1 \times 0.6}{1-K} = \frac{0.06}{1-0.16} = 0.0.07143 \end{aligned}$$

Combined Dempster's structure is {([0.6,1], 0.2143), ([1, 2], 0.7143), ([2, 3], 0.07143)}.

Dempster's rule of combination is very useful in calculating the belief and plausibility values when we have opinions from more than one expert.

14.4.3 Sampling Technique for the Evidence Theory

Sampling technique used in probabilistic method can also be used in the uncertainty quantification of system output using evidence theory [78, 79]. In this technique initially uniformly distributed random numbers are generated. Uncertain variables of given uncertainty are generated by equating these numbers to belief function and plausibility function. Two numbers are generated in this process, one is corresponding to belief function and other is corresponding to plausibility function (Fig. 14.17). This procedure is repeated for all the uncertain variables present in the problem.

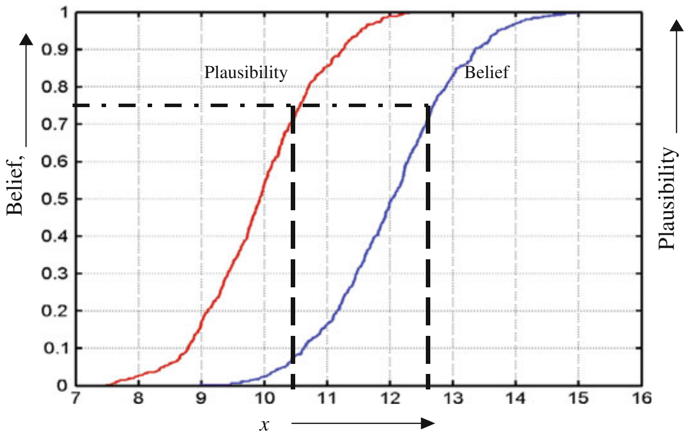


Fig. 14.17 Sampling technique in evidence theory

To generate uncertain variable x having belief function $Bel(x)$ and plausibility function $Pls(x)$

$$x_{max} = Bel^{-1}(u)$$
and
$$x_{min} = Pls^{-1}(u)$$

where u is uniformly distributed random variable generated in particular simulation.

If g is response function of uncertain variables x_1, x_2, x_3,…x_n

$$g = f(x_1, x_2, x_3, x_4 \ldots\ldots x_5).$$
$g_{\min}$ and $g_{\max}$ values for particular simulation are
$$g_{\min} = \min(f(x_1, x_2, x_3, x_4 \ldots\ldots x_5))\text{and}$$
$$g_{\max} = \max(f(x_1, x_2, x_3, x_4 \ldots\ldots x_5)).$$

Then belief of failure is

$$Bel(F) = n_1/N$$

and Plausibility of failure is

$$Pls(F) = n_2/N$$

Where n_1 is number of simulations for which is $g_{\min}$ is less than zero and n_2 is number of simulations for which $g_{\max}$ is lesser than zero and N is total number of simulations.

Example 8 A slab of thickness (L) 10 mm is insulated on one side at x = 0 and cooled by fluid having bulk temperature100 °C. The heat generated (Q_0) in the slab is equal to 8 × 10^7 W/m^3. Determine the probability of melting of slab.

Performance function is:

$$g = T_m - \left(\frac{Q_0 L^2}{2\,k} + \frac{Q_0 L}{h} + T_\infty \right) \tag{14.16}$$

Thermal conductivity '*k*', heat transfer coefficient '*h*' and melting temperature 'T_m' of material are considered as uncertain variable with basic belief assignment as shown in Fig. 14.18.

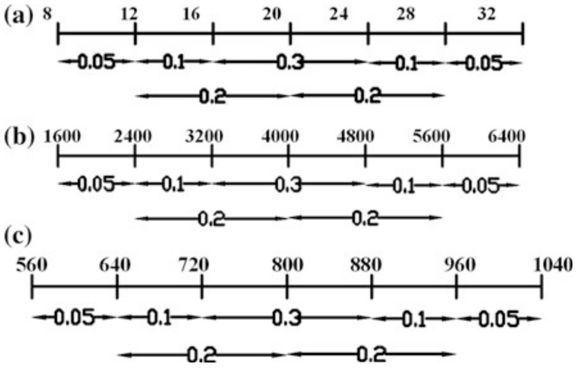


Fig. 14.18 Basic belief assignment **a** Conductivity **b** Heat transfer coefficient **c** Melting temperature

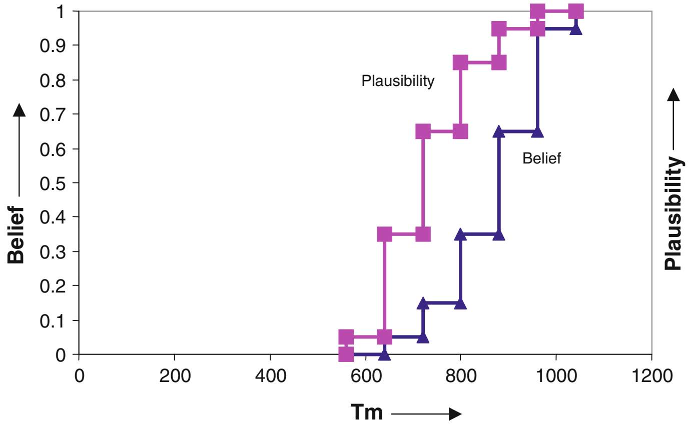


Fig. 14.19 Belief and plausibility for melting temperature

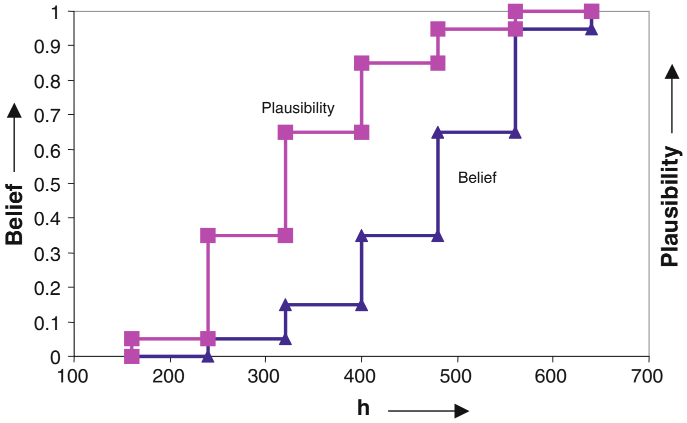


Fig. 14.20 Belief and plausibility for coefficient of heat transfer

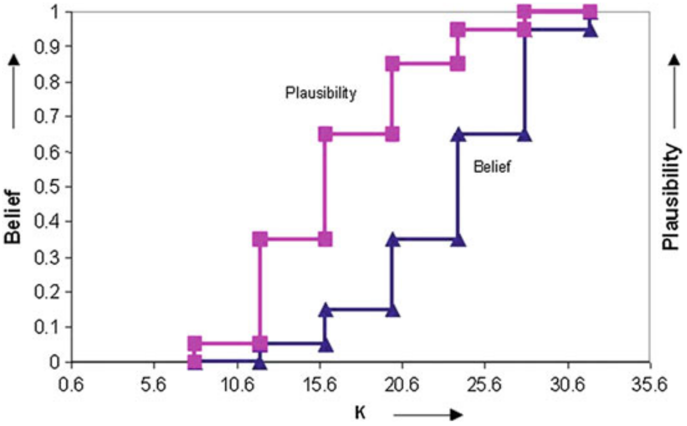


Fig. 14.21 Belief and plausibility for thermal conductivity

Solution Simulation technique is used for the calculation of belief of failure and plausibility of failure. The belief and plausibility of thermal conductivity, heat transfer, melting temperature, and performance function g are shown in Figs. 14.19, 14.20, 14.21 and 14.22.

14.5 Probability Bounds Approach

Probability bounds approach combines probability theory and interval arithmetic to produce probability boxes (p-boxes), structures that allow the comprehensive propagation of both aleatory uncertainty and epistemic uncertainty through

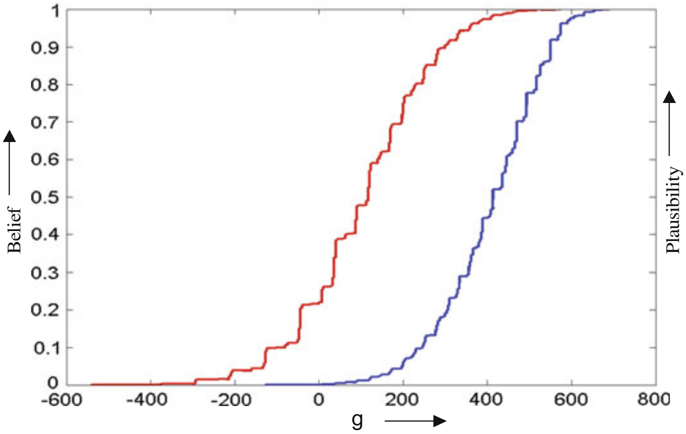


Fig. 14.22 Belief and plausibility of performance function (g), Belief of melting = 0.000866, Plausibility of melting = 0.215577, Number of simulations = 2000000

calculations in a rigorous way (Tucker and Ferson 2003 [55]; Morgan and Paredis 2006 [56]; Christopher Frey and Ranjit Bharvirkar 2002 [57]).

14.5.1 Computing with Probability Bounds

Williamson and Downs (1990) [58] provided explicit numerical methods for computing bounds on the result of addition, subtraction, multiplication and division of random variables when only bounds on the input distributions are given. These algorithms have been implemented in software [55] and have been extended to transformations such as logarithms and square roots, other convolutions such as minimum, maximum and powers, and other dependence assumptions.

As all the necessary mathematical operations can be performed using p-boxes, the input distributions used in a probabilistic risk assessment need *not* be particular, well-defined statistical distributions. Suppose that variables A and B have bounds (d_A, u_A) and (d_B, u_B) respectively, and that each of these four functions is evenly discretized into $m + 1$ elements. Assuming A and B are independent; the bounds on the sum $A + B$ have a discretization

$$d_{A+B}(i/m), u_{A+B}(i/m) \quad i \in \{0, 1, 2, \ldots, m\} \tag{14.17}$$

where $d(i/m)$ is approximated by the $(i + im + m)$th element of a numerical sorting of the $(m + 1)^2$ values

$$d_A(j/m) + d_B(k/m) \quad \forall j, k \in \{0, 1, 2, \ldots, m\} \tag{14.18}$$

and $u(i/m)$ is approximated by the $(i + im)$th element of a numerical sorting of the values

$$u_A(j/m) + u_B(k/m) \quad \forall j, k \in \{0, 1, 2, \ldots, m\} \tag{14.19}$$

The algorithm for subtraction is virtually the same except that the pluses between the *d*'s and the *u*'s are replaced by minuses. Multiplication and division use their respective operators too, so long as both variables are strictly positive. A more elaborate algorithm is required in the general case, although division is undefined whenever the divisor includes zero.

Example 9 Determine p-box resulting from multiplication of A and B which are second order random variables. Let A: Distribution is Lognormal with median [10, 20] and Error factor[1] [2, 3]; B: Distribution is Lognormal with median [40, 120] and Error factor [2, 3]

Solution The three graphs in Fig. 14.23 depict the modeling of a product of two variables using these algorithms. The quantity *A* depicted in the graph is modeled as a lognormal distribution whose median is in the interval [10, 20] and whose error factor is in the interval [2, 3]. The distribution is truncated at the 0.5th and 99.5th percentiles. B is also lognormal distribution with median in the interval [40, 120] and error factor [2, 3].

The lognormal probability distribution function (PDF) is given by

$$f(x) = \frac{1}{\sqrt{2\pi}(\sigma x)} e^{\left(-\frac{1}{2}\left[\frac{\ln x - \mu}{\sigma}\right]^2\right)}$$

Where μ and σ parameter of the distribution, given by

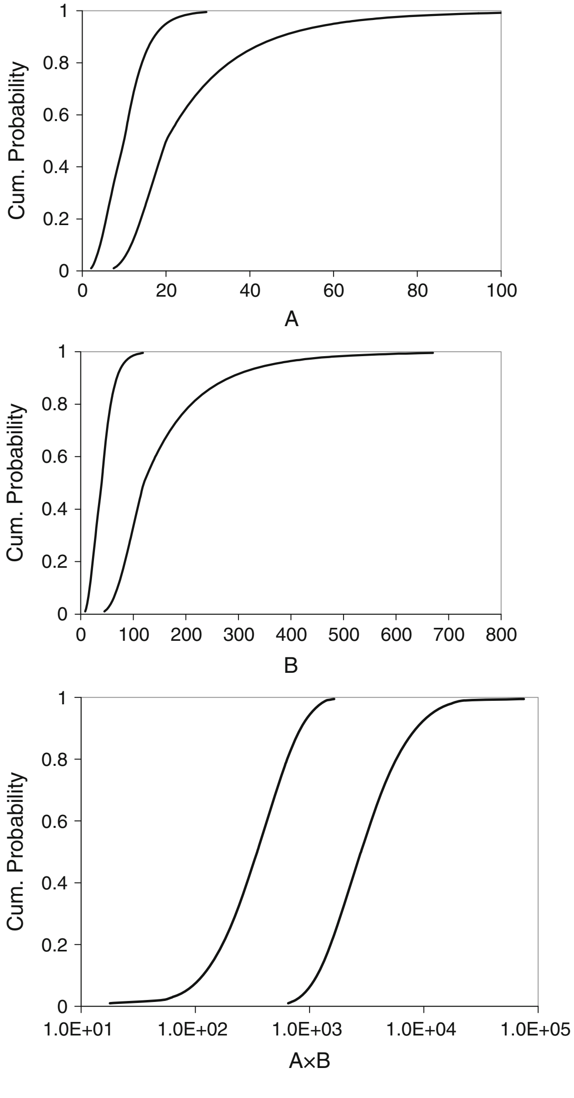
$$\mu = \ln(\text{Median}) \text{ and } \sigma = \ln(\text{Error factor})/1.645$$

The multiplication $A \times B$ of these two quantities, computed under the assumption that they are mutually independent, is depicted in the third graph of Fig. 14.23.

Figure 14.24 is a matrix containing a few of the calculations showing how this multiplication is computed. Each multiplicand is decomposed into a collection of intervals called focal elements. Each focal element is paired with a probability mass that depends on the discretization scheme employed. In this case, 100 discretization levels are used, so the focal elements are $[d(i/100), u(i/100)]$, where $i \in \{0, 1, 2, \ldots, 99\}$ and every probability mass is 1/100. The first line in each cell is an interval focal element and the second line is the probability mass associated with that focal

[1] Error factor is a parameter of lognormal distribution. Standard deviation of lognormal distribution is expressed as σ = ln(Error factor)/1.645.

Fig. 14.23 P-box for A, B and resulting p-box for A × B



element. The elements of *A* are arrayed along the top row of the matrix. The elements of *B* are in the first column. The cells inside the matrix form the Cartesian product, crossing each element from *A* with every element from *B*. The first line of a cell inside the matrix is determined by interval arithmetic on the corresponding focal elements from *A* and *B*. Because the model asserts that the quantity is the product of *A* and *B*, each of these interval operations is multiplication. The second line in each cell is the probability mass associated with the interval on the first line. The probability masses in the top row and first column are each 0.01; these are the masses that arose from the discretization of the continuous distributions. The masses inside the matrix are all 0.0001, which is the product (under independence)

A ↓ B →	[8.46, 45.02] 0.01	[10.1, 50.50] 0.01	....	[106.60, 567.44] 0.01	[118.421, 670.32] 0.01
[2.11, 7.5] 0.01	[17.85, 337.65] 0.0001	[21.31, 378.75] 0.0001		[224.92, 4255.8] 0.0001	[249.86, 5027.4] 0.0001
[2.53, 8.42] 0.01	[21.4, 379.06] 0.0001	[25.55,425.21] 0.0001		[269.69, 4777.84] 0.0001	[299.6, 5644.09] 0.0001
⋮			⋮		
[26.70, 94.57] 0.01	[225.88, 4257.54] 0.0001	[269.67, 4775.78] 0.0001	....	[2846.22, 53662.8] 0.0001	[3161.81, 63392.16] 0.0001
[29.60, 111.7] 0.01	[250.41, 5028.73] 0.0001	[298.96, 5640.85] 0.0001	....	[3155.36, 63383.05] 0.0001	[3505.23, 74874.74] 0.0001

Fig. 14.24 Matrix of interval focal elements (first line in each cell) and associated probability mass (second line in each cell) used to compute the sum of a p-box and a probability distribution

of 0.01 and 0.01. Because there are 100 focal elements in both *A* and *B*, there will be 10,000 focal elements in their product. Williamson [58] describes a condensation strategy that can reduce this number back to 100 in a way that conservatively captures uncertainty.

Detailed Information About Calculations

A is lognormal distribution whose parameters are available as intervals, median (10, 20) and Error factor (2, 3). The p-box for A has to be calculated by taking all the combinations such as (10; 2), (10; 3), (20; 2) and (20; 3) where first one is median followed by error factor. Figure 14.25a shows graphically the plot of all four distributions. The envelope over four distributions is the resulting p-box for A, as shown in Fig. 14.25b. Similarly p-box has to be constructed for B. Each multiplicand is decomposed into a collection of intervals called focal elements. In this case, 100 discretization levels are used, so the focal elements are [u*(i*/100), *d*(*i*/100)], where $i \in \{0, 1, 2, \ldots, 99\}$ and every probability mass is 1/100. F(x), cumulative distributive function will take values from 0, 0.01, 0.02, 0.03, …, 0.99, 1.0. For example, for a value of F(x) = 0.8, there will be a corresponding value of x for left distribution and also for right distribution. Thus A will be an interval [14.25, 35.1] at the CDF value of 0.8. Similarly, B will be an interval [57, 210.57] at the CDF value of 0.8 (Fig. 14.26).

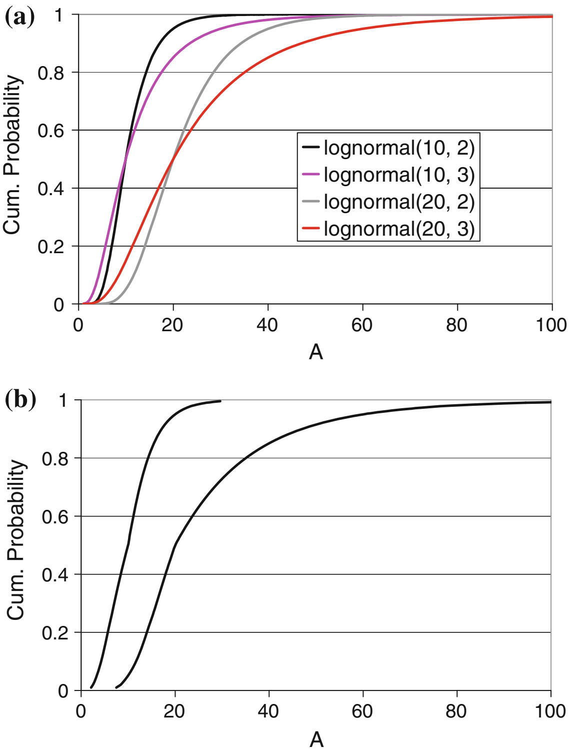


Fig. 14.25 **a** Combination of distributions—A **b** P-box for A

Now we have A[14.25, 35.1] and B[57, 210.57], the multiplication of two intervals is based on the laws of interval arithmetic.[2]

$$A \times B = [14.25 \times 57,\ 35.1 \times 210.57] = [812.25,\ 7391]$$

This calculation is for one Cartesian product. Because there are 100 focal elements in both *A* and *B*, there will be 10,000 focal elements in their product. They will be condensed and the final result will look like as shown in Fig. 14.23 and Table 14.16.

[2] Let A = [a_1, a_2] and B[b_1, b_2] are two interval numbers then C[c_1,c_2] = A[a_1, a_2] * B[b_1, b_2] can be defined as (* denotes any arithmetic operation)

$$C[c_1, c_2] = A[a_1,\ a_2] + B[b_1,\ b_2] = [a_1 +\ b_1,\ a_2 + b_2]$$
$$C[c_1, c_2] = A[a_1,\ a_2] - B[b_1,\ b_2] = [a_1 - b_2,\ a_2 - b_1]$$
$$\begin{aligned} C[c_1, c_2] &= A[a_1,\ a_2] \times B[b_1,\ b_2] \\ &= [\min(a_1 \times b_1,\ a_1 \times b_2,\ a_2 \times b_1,\ a_2 \times b_2),\ \max(a_1 \times b_1,\ a_1 \times b_2,\ a_2 \times b_1,\ a_2 \times b_2)] \end{aligned}.$$
$$C[c_1, c_2] = A[a_1,\ a_2]/B[b_1,\ b_2] = A[a_1,\ a_2] \times B[1/b_2, 1/b_1]$$

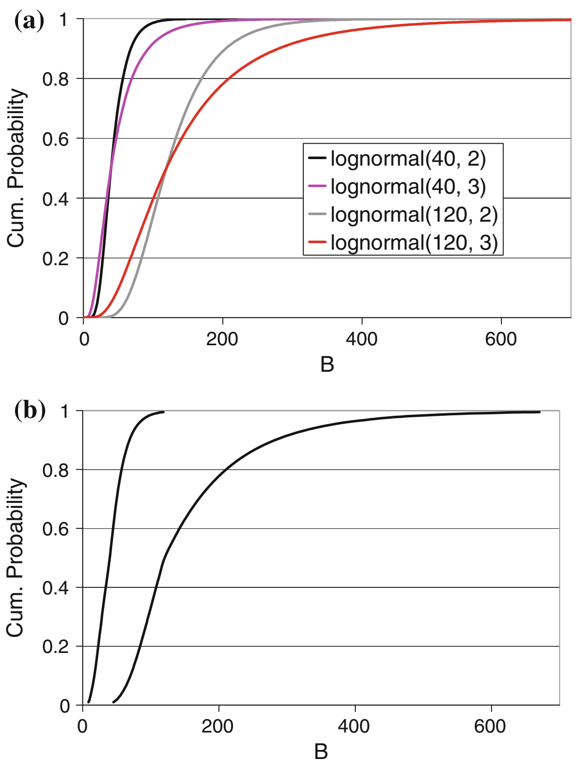


Fig. 14.26 **a** Combination of distributions—B **b** P-box for B

14.5.2 Two-Phase Monte Carlo Simulation

Treatment of epistemic and aleatory uncertainties in the simulation approach is carried out by sampling epistemic variables in the outer loop and aleatory variables in the inner loop. For a problem of second order random variable, the epistemic uncertainty in the parameters of the distributions is sampled first and later the randomness in the distribution is propagated. Unlike probability bounds approach where it can solve only problem of second order random variables, simulation approach can provide solution where epistemic and aleatory variables are completely separate also. For instance model uncertainty has to be kept separate from input parameters of the model. Thus two-phase Monte Carlo provides solution for two different problems of separating uncertainties. However, the computations will increase exponentially with the increase in the number of variables. The procedure for carrying out two-phase Monte Carlo simulation is explained below (see Fig. 14.27).

1. Information regarding PDF of elements in the model and the uncertainty in the parameters of PDF (epistemic uncertainty) (generally characterized by a probability distribution or an interval) is obtained.

Table 14.16 Final condensed values for A × B

$u_{A\times B}(i/m)$	$d_{A\times B}(i/m)$	CDF	$u_{A\times B}(i/m)$	$d_{A\times B}(i/m)$	CDF	$u_{A\times B}(i/m)$	$d_{A\times B}(i/m)$	CDF
1.79E+01	6.50E+02	0.01	2.48E+02	2.05E+03	0.34	4.96E+02	4.15E+03	0.68
5.07E+01	7.51E+02	0.02	2.54E+02	2.09E+03	0.35	5.05E+02	4.24E+03	0.69
6.34E+01	8.26E+02	0.03	2.60E+02	2.13E+03	0.36	5.15E+02	4.35E+03	0.7
7.39E+01	8.87E+02	0.04	2.66E+02	2.18E+03	0.37	5.25E+02	4.46E+03	0.71
8.26E+01	9.41E+02	0.05	2.71E+02	2.22E+03	0.38	5.36E+02	4.57E+03	0.72
9.01E+01	9.87E+02	0.06	2.77E+02	2.27E+03	0.39	5.48E+02	4.69E+03	0.73
9.73E+01	1.04E+03	0.07	2.83E+02	2.31E+03	0.4	5.59E+02	4.82E+03	0.74
1.04E+02	1.08E+03	0.08	2.89E+02	2.36E+03	0.41	5.70E+02	4.95E+03	0.75
1.10E+02	1.12E+03	0.09	2.95E+02	2.40E+03	0.42	5.83E+02	5.09E+03	0.76
1.17E+02	1.16E+03	0.1	3.01E+02	2.45E+03	0.43	5.96E+02	5.24E+03	0.77
1.22E+02	1.20E+03	0.11	3.08E+02	2.50E+03	0.44	6.09E+02	5.39E+03	0.78
1.28E+02	1.24E+03	0.12	3.14E+02	2.55E+03	0.45	6.23E+02	5.57E+03	0.79
1.34E+02	1.28E+03	0.13	3.21E+02	2.60E+03	0.46	6.37E+02	5.73E+03	0.8
1.40E+02	1.31E+03	0.14	3.27E+02	2.65E+03	0.47	6.52E+02	5.92E+03	0.81
1.45E+02	1.35E+03	0.15	3.33E+02	2.70E+03	0.48	6.69E+02	6.13E+03	0.82
1.51E+02	1.39E+03	0.16	3.40E+02	2.76E+03	0.49	6.85E+02	6.34E+03	0.83
1.56E+02	1.42E+03	0.17	3.47E+02	2.82E+03	0.5	7.03E+02	6.59E+03	0.84
1.62E+02	1.46E+03	0.18	3.55E+02	2.87E+03	0.51	7.22E+02	6.83E+03	0.85
1.67E+02	1.49E+03	0.19	3.62E+02	2.93E+03	0.52	7.41E+02	7.12E+03	0.86
1.72E+02	1.53E+03	0.2	3.69E+02	2.99E+03	0.53	7.62E+02	7.43E+03	0.87
1.78E+02	1.56E+03	0.21	3.76E+02	3.05E+03	0.54	7.86E+02	7.76E+03	0.88
1.83E+02	1.60E+03	0.22	3.91E+02	3.18E+03	0.56	8.09E+02	8.16E+03	0.89
1.88E+02	1.64E+03	0.23	3.99E+02	3.25E+03	0.57	8.38E+02	8.55E+03	0.9
1.94E+02	1.67E+03	0.24	4.07E+02	3.31E+03	0.58	8.67E+02	9.05E+03	0.91

(continued)

Table 14.16 (continued)

$u_{A\times B}(i/m)$	$d_{A\times B}(i/m)$	CDF	$u_{A\times B}(i/m)$	$d_{A\times B}(i/m)$	CDF	$u_{A\times B}(i/m)$	$d_{A\times B}(i/m)$	CDF
1.99E+02	1.71E+03	0.25	4.15E+02	3.38E+03	0.59	9.00E+02	9.62E+03	0.92
2.05E+02	1.74E+03	0.26	4.23E+02	3.46E+03	0.6	9.38E+02	1.02E+04	0.93
2.10E+02	1.78E+03	0.27	4.31E+02	3.54E+03	0.61	9.81E+02	1.10E+04	0.94
2.15E+02	1.82E+03	0.28	4.40E+02	3.61E+03	0.62	1.03E+03	1.19E+04	0.95
2.21E+02	1.86E+03	0.29	4.49E+02	3.69E+03	0.63	1.09E+03	1.32E+04	0.96
2.26E+02	1.90E+03	0.3	4.57E+02	3.77E+03	0.64	1.16E+03	1.48E+04	0.97
2.32E+02	1.93E+03	0.31	4.66E+02	3.86E+03	0.65	1.26E+03	1.74E+04	0.98
2.37E+02	1.97E+03	0.32	4.76E+02	3.95E+03	0.66	1.40E+03	2.25E+04	0.99
2.43E+02	2.01E+03	0.33	4.85E+02	4.04E+03	0.67	1.64E+03	7.49E+04	0.995

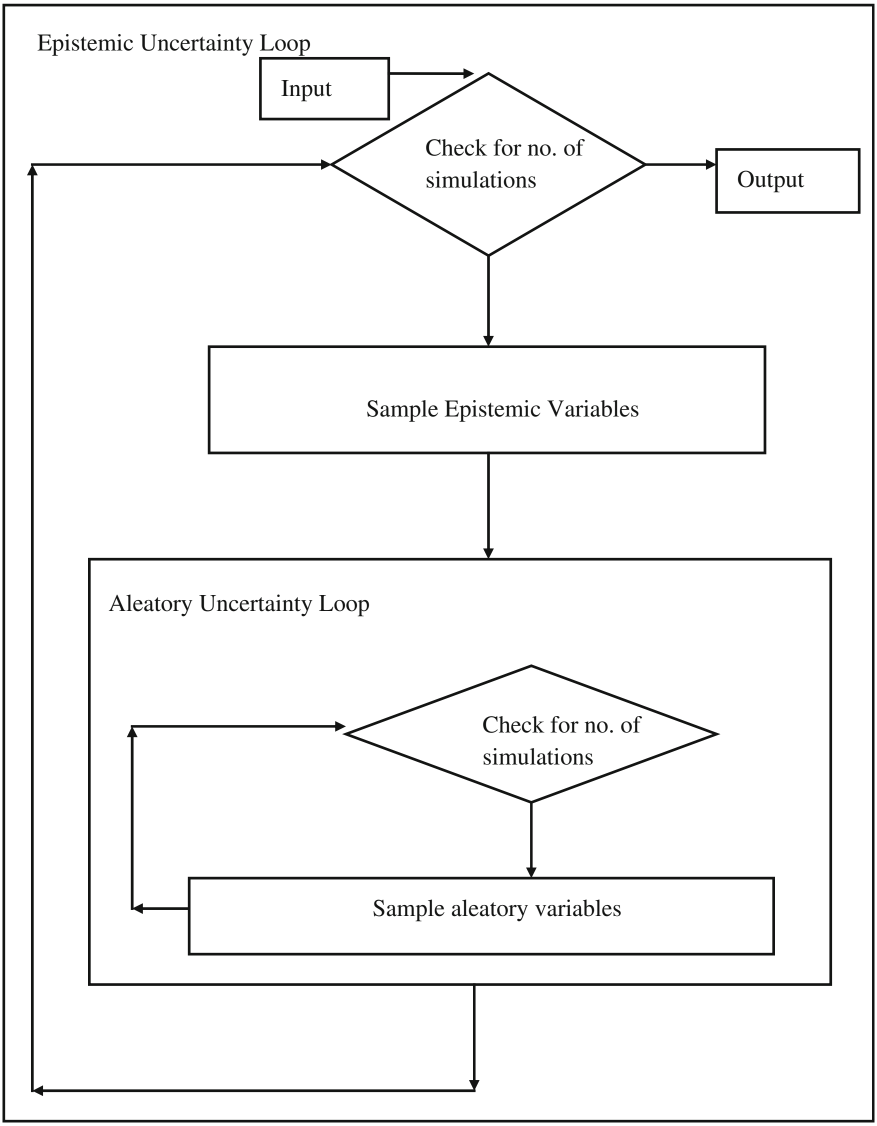

Epistemic Uncertainty Loop
Input
Check for no. of simulations
Output
Sample Epistemic Variables
Aleatory Uncertainty Loop
Check for no. of simulations
Sample aleatory variables

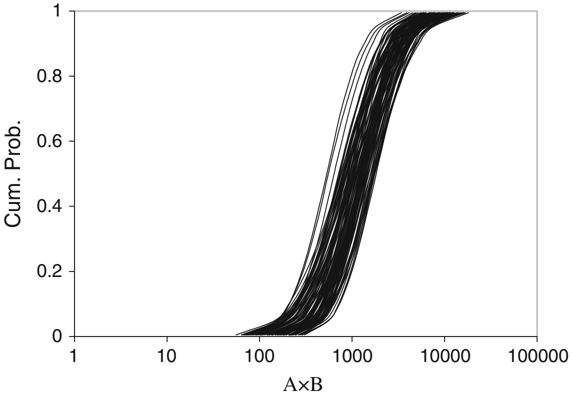
Fig. 14.27 Flowchart for two phase Monte Carlo approach

2. Distributions for PDF parameters of components are first sampled by any sampling approach, like crude or Latin-hypercube sampling approach. This action takes place in first loop of two loop sampling as depicted in Fig. 14.27. The first loop or outer loop focuses on epistemic uncertainty and the second loop or inner loop focuses on aleatory uncertainty.
3. Epistemic variables are treated as constants inside the second loop, i.e., the sampled values from step 2 are passed on to second loop. Now in the second loop, simulation is carried out by sampling aleatory variables.
4. Step 3 is repeated for sufficient number of iterations and required measures of uncertainty is obtained from the simulation results. This is one time execution of inner loop and the uncertainty from randomness are obtained in this step.
5. Check for the number of times first loop has to be executed, if it is less than the predetermined numbers of iterations then go to step 2 where sampling is done again for epistemic parameters and subsequently entering second loop.
6. After sufficient number of iterations of the outer loop, the summarized results looks like family of curves. Each cumulative probability curve of these denotes the uncertainty due to randomness, where as the spread is due to epistemic uncertainty in the parameters of PDFs.

For the example explained in the previous section on multiplication of two second order random variables (A × B), two-phase Monte Carlo simulation is applied with the same input information. In the present case 100 iterations in the outer loop and 10,000 iterations in the inner loop are performed in the two-phase Monte Carlo sampling procedure. The result obtained with 100 × 10,000 iterations with crude sampling is shown Fig. 14.28. The result is in good agreement with the result obtained from probability bounds approach.

In the large majority of cases, the focus is on the uncertainties regarding the numerical values of parameters of a given model (parameter uncertainty), rather on uncertainty regarding the validity of model it self. Since the model attempts to simulate reality, it is inevitable that there will be simplifying assumptions and

Fig. 14.28 A × B of A and B with two-phase Monte Carlo simulation



idealizations of rather complex processes and phenomena. There are uncertainties introduced by the relative inadequacy of the conceptual models, the mathematical models, and model assumptions. This uncertainty is called model uncertainty. Though model uncertainty is also knowledge-based uncertainty as the parameter uncertainty, it is required to keep different from the later in order to see its stand-alone impact. Two phase Monte Carlo methodologies can be applied to solve this problem. But, probability bounds is not suitable to solve this problem, it is useful only to solve second order random variable problem. The obtained result will be a collection of distributions representing model uncertainty, while the spread of distributions represents parameter uncertainty.

14.5.3 Uncertainty Propagation Considering Correlation Between Variables

In most of uncertainty studies, it is assumed that variables are statistically independent. But neglecting dependency between the variables may underestimate/overestimate the results which may mislead decision making. Hence, it is important to account for statistical dependencies between the variable if they exist [8]. There are essentially two obstacles that complicate the handling of dependencies. The first is the potential complexity of dependencies and the second is that empirical information is usually lacking.

There are several strategies a Monte Carlo analyst can use to account for knowledge and uncertainty about correlations and dependencies. These include assuming independence, functional modeling, simulating observed correlations, assuming perfect covariance, and assuming linear dependency. The probability bounds approach can also account for dependencies between variables in the same manner as the Monte Carlo approach. Additionally, probability bounds approach can be used to calculate bounds that allow for precisely specified copulas that fully characterize the statistical dependence [55].

In the domain of system reliability/availability assessment, Apostolakis [13] pointed out that there is correlation or coupling among the data of identical basic events such as the failure of two identical basic events such as the failure of two identical pumps, circuit breakers, etc. This correlation means that the data of identical basic events are entirely correlated and should be treated as a single random variable rather than statistically independent random variable in the uncertainty analysis. Using this premise, in case of Monte Carlo simulation approach same random variate should be used for identical basic events. In the present problem, MCPS, it has identical circuit breakers, rectifiers, batteries, inverters, switches and buses. Instead of 24 basic events as is the case with independent assumption calculations, now it is reduced to 7 random variables.

In case of probability bounds approach, Williamson and Downs [58] described numerical methods for computing bounds without using an assumption of independence between the variables. Bounds on the sum of A and B, for example, are

$$\begin{aligned} d(i/m) &= \min_{j=i}^{m}(d_A(j/m) + d_B((i-j+m)/m)) \\ u(i/m) &= \min_{j=0}^{i}(u_A(j/m) + u_B((i-j)/m)) \end{aligned} \tag{14.20}$$

where i varies between 0 and m (discretization levels). These bounds are guaranteed to enclose the true answer no matter what correlation or statistical dependency exists between A and B. Similar expression can be used for other arithmetic operations also.

14.6 Case Study to Compare Uncertainty Analysis Methods

All the different approaches available in the literature to propagate uncertainty are different from each other, in terms of characterizing the input parameter uncertainty and also in the kind of propagation from parameter level to model output level. Probabilistic approaches characterize the uncertainty in the parameter by a probability distribution. Interval approach represents with an interval having lower bound and upper bound. Fuzzy Set Theory based approach characterizes uncertainty by a fuzzy membership function. Different methods for uncertainty propagation available

Table 14.17 Comparison of methods for uncertainty propagation

S. no.	Method	Representation of uncertainty	Propagation to output
1.	Probabilistic methods		
	a. Analytical methods (Method of Moments)	Moments of the parameters (mean and variance)	Analytical
	b. Simulation (crude Monte-Carlo and Latin Hypercube sampling)	Probability distributions	Simulation
	c. Discrete Probability	Probability distributions	Analytical
2.	Interval Analysis	Intervals	Interval arithmetic
3.	Fuzzy set theory	Fuzzy membership function	Fuzzy arithmetic
4.	Dempster-Shafer theory	Dempster-Shafer structures, Possibility and Probability distributions	Combination of analytical and simulation
5.	Probability bounds	P-boxes	Cartesian product of intervals and probabilities

in the literature are summarized in Table 14.17. The first three approaches are fundamentally different from each other where as the last two methods are integration of the first three methods. However, the different approaches to dealing with uncertainty presented above have proved to possess different desirable and undesirable features, making them only contextually useful in different situations [80]. A comparative study is presented here on various uncertainty propagation methods available in the literature with a case study on the availability assessment of Main Control Power Supply (MCPS) system of NPP. Merits and demerits of each method are discussed.

14.6.1 Availability Assessment of MCPS Using Fault Tree Analysis

240 V AC MCPS is a very important support system in Nuclear Power Plant which provides uninterrupted A.C. power supply to safety related loads such as reactor regulation systems and safety system loads such as shut down systems. The schematic diagram of this system is shown in Fig. 14.2 [24].

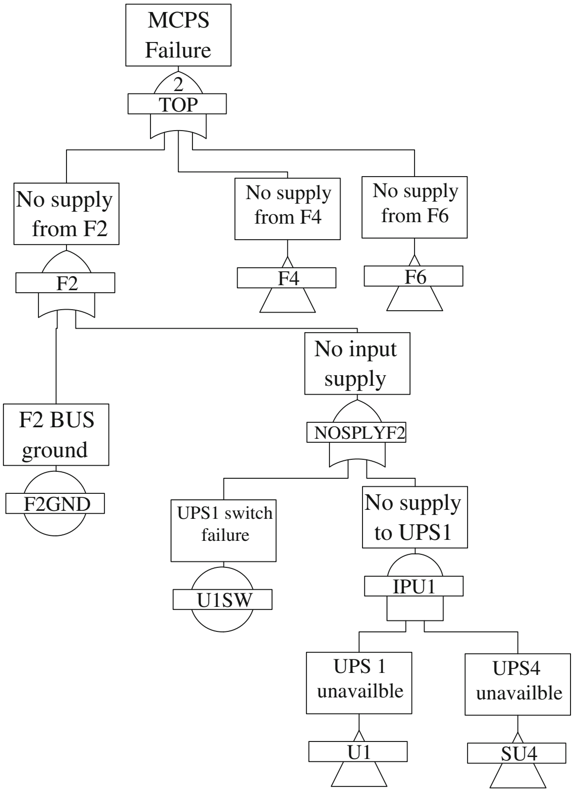


Fig. 14.29 Simplified fault tree of MCPS

There are four (Uninterrupted Power Supply) UPSs namely, UPS-1, UPS-2, UPS-3 and UPS-4; and four UPS batteries (BY) viz., BY-1, BY-2, BY-3 and BY-4. UPS-1, UPS-2 and UPS-3 are having in-built static switches for transferring the load to standby UPS which is UPS-4. Ch-A/D/Y (Bus F2) loads are fed from UPS-1, Ch-B/E/Z (Bus F6) loads are fed from UPS-2, Ch-C/F (Bus F4) loads are fed from UPS-3, and UPS-4 is standby UPS. Input supply to UPS-1 and UPS-3, and UPS-2 and UPS-4 is taken from division I and division II of class III respectively (Refer Fig. 14.2).

Unavailability model is obtained with the help of fault tree analysis technique. Failure criterion is unavailability of power supply at 2 out of 3 buses. Fault tree is developed and the minimal cut-sets and unavailability of the system are obtained using ISOGRAPH [72]. There are 24 components identified in the system and 219 minimal cut sets are obtained from the analysis. A simplified fault tree and the first 30 minimal cut sets of MCPS are shown in Fig. 14.29 and Table 14.18 respectively.

14.6.2 Uncertainty Propagation in MCPS with Different Methods

14.6.2.1 Interval Analysis

The uncertainty in the variables is specified as interval number in this approach. The intervals should represent the absolute bounds of the uncertain parameter that one wants to explore in the analysis. Table 14.19 gives the intervals chosen for the uncertain variables in unavailability expression of MCPS [80]. The system unavailability obtained after carrying out interval arithmetic is [1.44E-7, 1.17E-5].

Benefits Interval analysis is a straightforward, easily explainable simple method. Interval analysis can be used whatever the source of uncertainty. Interval analysis is very well suited for screening studies, due to inherent conservatism and simplicity.

Limitations As one is working with only the ranges of the inputs, these ranges can grow very quickly, making the results highly conservative in many real-life situations. To some extent, the approach is paradoxical, since it implies that one cannot know the exact value of a parameter, but the exact bounds may be known. The methodology compounds aleatory and epistemic uncertainty.

14.6.2.2 Fuzzy Arithmetic

The uncertainty in parameters are specified as triangular fuzzy numbers using the simple strategy of allowing alpha-level 0 be represented by the intervals specified above, and alpha-level 1 to be represented by the best estimate. It is characterized by three values as shown in Table 14.19 for all the unavailability of components

Table 14.18 List of minimal cut-set

S. no.	Cut set		S. no.	Cut set		
1	F2GND	F6GND	16	UPS1BATR	UPS3BATR	DIV1
2	F4GND	F6GND	17	UPS1INV	UPS2BATR	UPS2RECT
3	F2GND	F4GND	18	UPS2INV	UPS3BATR	DIV1
4	F2GND	U3SWOPN	19	UPS2INV	UPS3BATR	UPS3RECT
5	F4GND	U2SWOPN	20	UPS2INV	UPS1BATR	UPS1RECT
6	F6GND	U1SWOPN	21	UPS3INV	UPS1BATR	UPS1RECT
7	F4GND	U1SWOPN	22	UPS3INV	UPS2BATR	DIV2
8	F2GND	U2SWOPN	23	UPS3INV	UPS2BATR	UPS2RECT
9	F6GND	U3SWOPN	24	UPS1INV	UPS3BATR	DIV1
10	UPS3INV	UPS2INV	25	UPS1INV	UPS3BATR	UPS3RECT
11	UPS1INV	UPS3INV	26	UPS3INV	UPS1BATR	DIV1
12	UPS1INV	UPS2INV	27	UPS2INV	UPS1BATR	DIV1
13	U1SWOPN	U3SWOPN	28	UPS1INV	UPS2BATR	DIV2
14	U3SWOPN	U2SWOPN	29	F2GND	UPS3INV	UPS4INV
15	U1SWOPN	U2SWOPN	30	F6GND	UPS3INV	UPS4INV

Table 14.19 Unavailability of components as uncertain parameters

Component description	Interval	Fuzzy number
BUS F GROUND	[1.83E-04, 1.65E-03]	[1.83E-04, 5.50E-04, 1.65E-03]
UPS SWITCH OPEN	[3.33E-05, 3.00E-04]	[3.33E-05, 1.00E-04, 3.00E-04]
UPS INVERTER	[3.66E-05, 3.30E-04]	[3.66E-05, 1.10E-04, 3.30E-04]
UPS BATTERY	[8.33E-05, 7.50E-04]	[8.33E-05, 2.50E-04, 7.50E-04]
UPS RECTIFIER	[1.83E-04, 1.65E-03]	[1.83E-04, 5.50E-04, 1.65E-03]
CIRCUIT BREAKER	[3.00E-06, 2.70E-05]	[3.00E-06, 9.00E-06, 2.70E-05]
DIVISION	[1.83E-04, 1.65E-03]	[1.83E-04, 5.50E-04, 1.65E-03]

[27, 35]. The following expressions are used for calculating unavailability for different alpha cuts:

$$\begin{aligned} Unava. &= lower\,bound + (best\,estimate - lower\,bound]) \times,\ for\ left\,leg \\ Unava. &= upper\,bound + (best\,estimate - upper\,bound]) \times,\ for\ right\,leg \end{aligned} \tag{14.21}$$

Software has been developed for carrying out these analyses. If the model output expression is non-linear then optimized vertex method shall be used [38]. As the present output expression is simply the sum of products of component unavailabilities, simple alpha-cut method is sufficient. The resulting fuzzy number for MCPS unavailability is shown in Fig. 14.30. Not surprisingly, the range of resulting unavailability at alpha = 0 is the same as for interval analysis. At alpha-level 0,

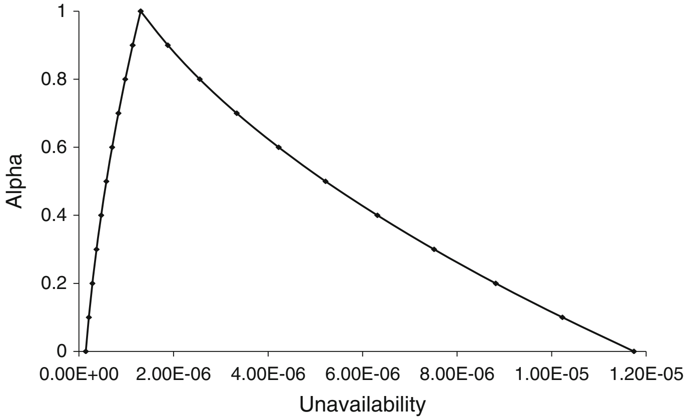


Fig. 14.30 Resulting fuzzy number for unavailability of MCPS

obviously the most conservative range is displayed, where as at alpha-level 1 the most optimistic estimation is presented. The intermediate alpha levels can only be interpreted as alpha increases, the level of conservatism decreases.

Benefits: Fuzzy arithmetic is the generalization of interval analysis and computations are easy to carry out. It does not require detailed empirical information like shape of distribution, dependencies and correlations. Fuzzy numbers are robust representation of uncertainty when empirical information is very sparse.

Limitations: Fuzzy arithmetic is inherently conservative as inputs are treated fully correlated. The meaning of alpha, the level of conservatism, is not clear and because of this it is not yet widely used in performance analysis. The level of conservatism with fuzzy arithmetic is in between interval analysis and Monte Carlo based methods. Repeated parameters may constitute a computational problem leading to unnecessarily conservative results.But fuzzy numbers handle certain types of uncertainty better than probabilistic methods and vice versa. Nevertheless, no methods are available with in fuzzy framework to keep different types of uncertainty separate in an analysis.

14.6.2.3 Monte Carlo Simulation

Probabilistic approaches characterize the uncertainty in the parameter by a probability distribution. The base resource document for failure data given by USNRC [81] and IAEA [82] suggests considering lognormal distribution for epistemic uncertainty in unavailability. With the more plant specific information available, Bayesian updating technique will be used to get better estimations by integrating new evidence with the prior distribution.

In the MCPS problem, lognormal distributions are considered with the median as the best estimate and error factor is considered as 3. Crude Monte Carlo sampling scheme was used for the sampling procedure. 50,000 iterations are used as convergence

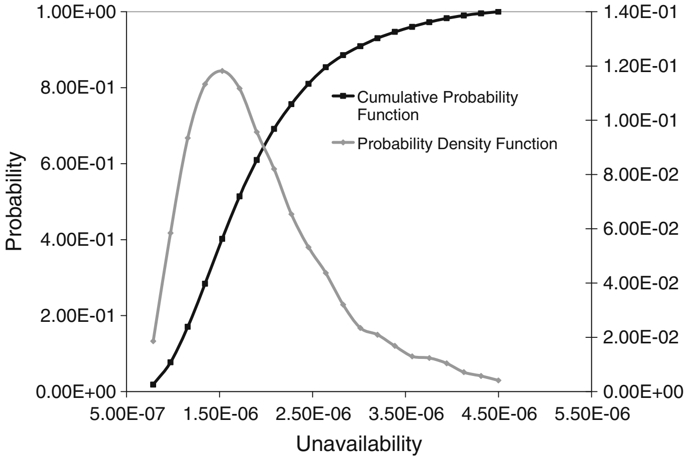


Fig. 14.31 Probability distribution for unavailability of MCPS

for simulation. Software has been written to carry out the simulations. The resulting probability distribution for unavailability of MCPS is shown in Fig. 14.31.

Benefits The sampling based methodologies are fairly simple to implement and user-friendly software is available for analysts. One can use information on correlation and dependencies between the variables to see what impact they have on the uncertainty in the final results even though such a study has not been attempted here.

Limitations More information is required, for example, information on distribution of variables and their correlations. This forces the analyst to make assumptions, for example, independent variables, which might lead to narrower distribution for the system characteristic than justified. It is not possible to separate aleatory and epistemic uncertainty with in the classical Monte Carlo approach.

14.6.2.4 Dempster-Shafer Theory

Former methods can handle either with model parameters having probability distributions or fuzzy membership functions. Uncertainty quantification based on Dempster-Shafer theory is explored here in the context of availability models where certain parameters of model are probability distributions and certain parameters of model are fuzzy membership functions and presented in this section.

In the MCPS problem using evidence theory, information used in fuzzy arithmetic (Table 14.19) for unavailability of UPS switches (3) and batteries (4) and information used in Monte Carlo simulation (Sect. 14.6.2.3) for remaining components (17) is considered here. Thus 7 fuzzy numbers and 17 probability distributions are there for propagation. Computer code has been developed to carry out the calculations. The resulting Belief and Plausibility distributions for Unavailability of MCPS which were calculated with 50,000 iterations are shown in Fig. 14.32.

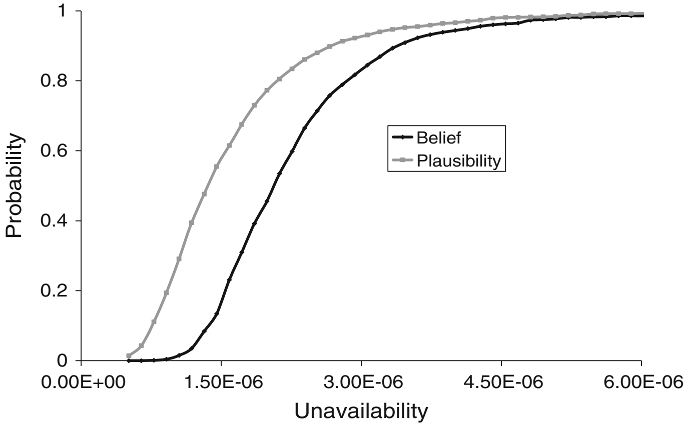


Fig. 14.32 Belief and plausibility distributions

Benefits: General theory which contents probability and possibility theories. This can handle uncertainty quantification of model which is having some parameters as probability distributions and some parameters as possibility distributions. It can give common framework for imprecision and variability modelling.

Limitations: One of the major difficulties in applying evidence theory to an engineering system is the computational cost. Unlike the probability density function or possibility distribution function (membership function of fuzzy variable), there is no explicit function of the given imprecise information in evidence theory. Since many possible discontinuous sets can be given for an uncertain variable instead of a smooth and continuous explicit function, intensive computational cost might be inevitable in quantifying uncertainty using evidence theory. However, with the incredible development in the computer technology for data processing at unprecedented levels, the computational cost is no longer a limitation.

14.6.2.5 Probability Bounds Analysis

Calculation in case of probability bounds involve following steps [83]:

- Convert component uncertainty information to p-boxes. It has to be done for all the components (24 in this case)
- Generation of p-box for each cut-set:
- Cut-set is the product of certain number of components (say ‘n’). This is done iteratively, for example if there are ‘n’ components in a cut-set, then there will be ‘n-1’ multiplication operations have to be carried out. First two elements in the cut-set are multiplied to generate a p-box, now this is multiplied with p-box of third element in the cut-set. This will go on till ‘n-1’ multiplications are achieved.

- From step (ii), p-box is obtained for each cut-set. Now, p-box addition has to be done to sum up all the cut-sets. If there are ‘N’ numbers of cut-sets, then there will be ‘N-1’ p-box additions have to be carried out. This step generates final p-box for the overall system unavailability.

Uncertainty in the parameters of the lognormal distribution are specified as intervals as shown in Table 14.20.

Figure 14.33 shows probability bounds for the system unavailability of MCPS compared with Monte Carlo simulation result.

With precise information about probability distribution of input variables of the model, uncertainty analysis with conventional Monte Carlo simulation approach is simple and straight forward to apply. But in scenarios such as (i) if the shape of the distribution is unknown or (ii) both the parameters of the distributions and shape

Table 14.20 Unavailability of components as uncertain parameters

Component description	Unavailability of component (lognormal distribution)	
	Mean	Standard deviation
BUS F GROUND	[6.01e-4, 1.37e-3]	[2.65e-4, 1.03e-3]
UPS SWITCH OPEN	[1.09e-4, 2.5e-4]	[4.81e-5, 1.87e-4]
UPS INVERTER	[1.2e-4, 2.75e-4]	[5.29e-5, 2.06e-4]
UPS BATTERY	[2.73e-4, 6.24e-4]	[1.2e-4, 4.68e-4]
UPS RECTIFIER	[6.01e-4, 1.37e-3]	[2.65e-4, 1.03e-3]
CIRCUIT BREAKER	[9.83e-6, 2.25e-5]	[4.33e-6, 1.68e-5]
DIVISION	[6.01e-4, 1.37e-3]	[2.65e-4, 1.03e-3]

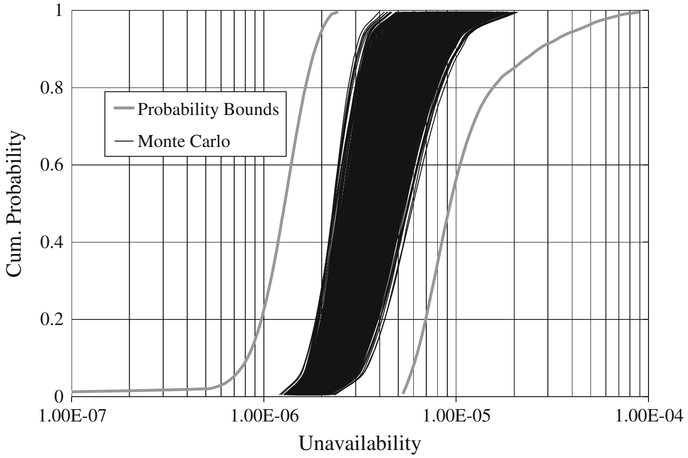


Fig. 14.33 Comparison of probability bounds result with Monte Carlo simulation

(but some constraints on distribution, for example: min, max, mean, variance are available) are uncertain, analysis with simulation is very difficult. No general method is available in the simulation approach to comprehensively solve such scenarios. Applying simulation approach in such situations to yield less conservative results with unjustified assumptions (such as assuming shape of distribution and parameters) may not be technically correct. Though a common strategy is to try a few parametric distributions, but the result would not be comprehensive. The level of effort necessary to perform such computations and interpret the results would be very high. In contrast, Probability bounds approach provides effective solution in these scenarios. P-box can be constructed to comprehensively enclose all possible distributions that satisfy known constraints which can be used to propagate this uncertainty through to the model result.

14.6.3 Observations from Case Study

The four methods, namely, interval arithmetic, fuzzy arithmetic, Monte Carlo simulation and Dempster-Shafer theory are different from each other, in terms of characterizing the input parameter uncertainty and also in kind of propagation from parameter level to model output level. All the four methods have different desirable and undesirable features making them more or less useful in different situations.

The uncertainty bound given by interval arithmetic and fuzzy arithmetic is [1.44E-7, 1.17E-5] whereas the same with Monte Carlo simulation (98% confidence limits) is [7.86E-7, 4.5E-6]. This shows that interval and fuzzy approaches are conservative compared with Monte Carlo method. The former methods are inherently conservative whereas the lattermethod can underestimate uncertainty in certain cases due to assumptions such as independent variables. Moreover, interpretation of uncertainty for intermediate alpha-cut values in fuzzy arithmetic is not as clear as with probabilistic approaches. However, resources required for doing interval and fuzzy arithmetic, for example, computational requirements and information of uncertainty at component level are less. Fuzzy arithmetic is less conservative than interval arithmetic as repeated parameters may constitute a computational problem, leading to unnecessary conservative results with interval arithmetic. When there is limited empirical information, one can make use of subjectively assigned distributions and carry out fuzzy arithmetic at less computational burden. But if one wants to use information on correlations and dependencies between variables and detailed information is there about uncertainties in parameters, then Monte Carlo simulation is suitable. Dempster-Shafer theory contents probability and possibility theories and can handle uncertainty quantification of model which is having some parameters as probability distributions and some parameters as possibility distributions. It can give common framework for imprecision and variability modelling. One of the major difficulties in applying Dempster-Shafer theory to an engineering system is the computational cost. Since many possible discontinuous sets can be given for an uncertain variable instead of a smooth and continuous explicit function, intensive computational cost might be inevitable in quantifying uncertainty using evidence theory.

Remarks In spite of several potential applications of reliability assessment for its system effectiveness, the uncertainties associated with parameters, models, phenomena and assumptions are limiting its usage. Knowing the sources of uncertainty involved in the analysis plays an important role in handling it. If one knows why there are uncertainties and what kinds of uncertainties are involved, one has a better chance of finding the right methods for reducing them. Problem of acknowledging and treating uncertainty is vital for quality and practical usability of the analysis results. Uncertainty propagation methods focus on how one can assess the impact of these uncertainties in the input parameters on the model output.

The different approaches available in the literature for propagation of uncertainty are discussed. They are different from each other, in terms of characterizing the input parameter uncertainty and also in propagation from parameter level to model output level. A case study on 240V AC MCPS of a typical Indian NPP has been carried out, in which different features of methods of uncertainty propagation surveyed are highlighted. However, the different approaches to dealing with uncertainty presented have proved to possess different desirable and undesirable features, making them more or less useful in different situations (Table 14.21). When there is limited empirical information, one can make use of subjectively assigned possibility distributions and carry out fuzzy arithmetic at less computational burden. But if one wants to use information on correlations and dependencies between variables and detailed information is there about uncertainties in parameters, then Monte Carlo simulation is suitable. In availability models where there are both probability and possibility distribution parameters, Dempster-Shafer theory based approach is found to be the only suitable for uncertainty propagation.

Table 14.21 Potential area of applications for different methods

Method	Potential areas of application
Interval and fuzzy	1. Limited information is available
Arithmetic	2. Large number of fault trees and event trees
Monte carlo simulation	1. Detailed information is available
	2. Correlations exist
Dempster-Shafer approach	Both probability and possibility distributions are present in the model
Probability bounds	Imprecise shape and parameters

References

1. Apostolakis G (1981) Pitfalls in risk calculations. Reliab Eng 2:135–145
2. Ferson S, Hajagos JG (2006) Varying correlation coefficients can underestimate uncertainty in probabilistic models. Reliab Eng Syst Safety 91:1461–1467
3. Jin T, Coit DW (2001) Variance of system-reliability estimates with arbitrarily repeated components. IEEE Trans Reliab 50(4):409–413
4. Xu C, Gertner GZ (2008) Uncertainty and sensitivity analysis for models with correlated parameters. Reliab Eng Syst Safety 93:1563–1573
5. Dezfuli H, Modarres M (1985) Uncertainty analysis of reactor safety systems with statistically correlated failure data. Reliab Eng 11:47–64
6. Zhang Q (1989) A general method dealing with correlations in uncertainty propagation in fault trees. Reliab Eng Syst Safety 26(3):231–247
7. Zhang Q (1993) A method dealing with correlations in uncertainty propagation by using traditional correlation coefficients. Reliab Eng Syst Safety 41(2):107–114
8. Kafrawy KF, Rushdi AM (1990) Uncertainty analysis of fault tree with statistically correlated failure data. Microelectron Reliab 30:157–175
9. Ferson S, Hajagos JG (2004) Arithmetic with uncertain numbers: rigorous and (often) best possible answers. Reliab Eng Syst Safety 85:135–152
10. Karanki DR, Kushwaha HS, Verma AK, Ajit S (2009) Uncertainty Analysis based on probability bounds (p-box) approach in probabilistic safety assessment. Risk Anal: Int J 29 (5):662–675
11. Helton JC (1994) Treatment of uncertainty in performance assessment for complex systems. Risk Anal 14(4):483–511
12. Cornell MEP (1996) Uncertainties in risk analysis: Six levels of treatment. Reliab Eng Syst Safety 54:95–111
13. Apostolakis G (1999) The distinction between aleatory and epistemic uncertainties is important: an example from the inclusion of aging effects into PSA. In: Proceedings of PSA '99, international topical meeting on probabilistic safety assessment, American Nuclear Society, La Grange Park, IL, Washington, DC, August 22–26: 135–142
14. Durga Rao K, Kushwaha HS, Verma AK, Ajit S (2007) Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies. Reliab Eng Syst Safety 92:947–956
15. USNRC (1993) Procedure for analysis of common-cause failures in probabilistic safety analysis. NUREG/CR-5801 (SAND91-7087)
16. USNRC (2007) Common-cause failure database and analysis system: event data collection, Classification, and coding, NUREG/CR-6268
17. Jackson PS, Hockenbury RW, Yeater ML (1981) Uncertainty analysis of system reliability and availability assessment. Nucl Eng Des 68:5–29
18. IAEA, Procedure for conducting probabilistic safety assessment of nuclear power plants (level 1), International Atomic Energy Agency, Vienna, Safety Series No. 50-P-4, 1992
19. Kiureghian AD, Asce M, Lin PL (1986) Structural reliability under incomplete probability information. J Eng Mech 112(1):85–103
20. Karanki DR, Dang VN (2010) Quantification of Uncertainty in Fault Tree Analysis with Correlated Basic Events", ESREL 2010, Rhodes, Greece, Taylor & Francis Group, London, ISBN 978-0-415-60427-7, pp 1619–1628
21. Billinton R, Allan RN (1992) Reliability evaluation of engineering systems. Plenum Press, New York
22. Helton JC, Davis FJ (2003) Latin hypercube sampling and the propagation of uncertainty in analyses of complex systems. Reliab Eng Syst Safety 81(1):23–69
23. Liu P-L, Kiureghian AD (1986) Multivariate distribution models with marginal and covariances. Probab Eng Mech 1(2):104–112

24. Thamatampalli S, Karanki DR (2003) Reliability analysis of main control power supply system of TAPP 3&4. BARC Internal Report, Mumbai
25. Risk Spectrum PSA professional version 2.10, RELCON Scandpower AB, Sweden
26. Vaurio JK (2007) Consistent mapping of common cause failure rates and alpha factors. Reliab Eng Syst Safety 92(5):628–645
27. Tanaka H, Fan LT, Lai FS, Toguchi K (1983) Fault tree analysis by fuzzy probability. IEEE Trans Reliab 32:453–457
28. Modarres M (1985) Statistical uncertainty analysis in reactor risk estimation. Nucl Eng Des 85:385–399
29. Wu JS, Apostolakis GE, Okrent D (1990) Uncertainties in system analysis: probabilistic Vs non probabilistic theories. Reliab Eng Syst Safety 30:163–181
30. Helton JC (1993) Uncertainty and sensitivity analysis techniques for use in performance assessment for radioactive waste disposal. Reliab Eng Syst Safety 42:327–367
31. Soman KP, Misra KB (1993) Fuzzy fault tree analysis using resolution identity. J Fuzzy Math 1:193–212
32. Suresh PV, Babar AK, Venkatraj V (1996) Uncertainty in fault tree analysis: a fuzzy approach. Fuzzy Sets Syst 83:135–141
33. Karanki DR, Saraf RK, Kushwaha HS (2003) Uncertainty in reliability analy-sis of MCPS of TAPP 3 & 4, ICQRIT 2003, New Delhi
34. Ferson S, Hajago JG (2004) Arithmetic with uncertain numbers: rigorous and often best possible answers. Reliab Eng Syst Safety 85:135–152
35. Regan HM, Ferson S, Berleant D (2004) Equivalence of methods for uncer-tainty propagation of real valued random variables. Int J Approximate Reasoning 36:1–30
36. Karanki DR, et al (2004) A Study on uncertainty analysis of safety systems of advanced heavy water reactor using fuzzy set theory, PSAM7 – ESREL 2004, Berlin, Germany, 2283– 2288
37. Antonio CFG, Nelson FFE (1999) FuzzyFTA: A fuzzy fault tree analysis for uncertainty analysis. Ann Nucl Energy 26:523–532
38. Smith SA, Krishnamurthy T, Mason BH (2002) Optimized vertex method and hybrid reliability. American Institute of Aeronautics and Astronautics, Inc., 1465
39. Frantzich H (1988) Uncertainty and risk analysis in fire safety engineering. Doctoral dissertation, Department of Fire Safety Engineering, Lund University, Lund
40. Marquez AC, Heguedas AS, Iung B (2005) Monte Carlo-based assessment of system availability. Reliab Eng Syst Safety 88:273–289
41. Bae HR, Grandhi RV, Canfield RA (2003) Uncertainty quantification of structural response using Evidence Theory. AIAA J 41(10):2062–2068
42. Hofer E, Kloos M, Hausmann BK, Peschke J, Woltereck M (2002) An approximate epistemic uncertianty analysis approach in the presence of epistemic and aleatory uncertainties. Reliab Eng Syst Safety 77:229–238
43. Bae H, Grandhi RV, Canfield RA (2004) Epistemic uncertainty quantification techniques including evidence theory for large scale structures. Comput Struct 82:1101–1112
44. Daniel B, Jianzhong Z (2004) Representation and problem solving with Distribution Envelope Determination (DEnv). Reliab Eng Syst Safety 85(1–3):153–168
45. Winkler RL (1996) Uncertainty in probabilistic risk assessment. Reliab Eng Syst Safety 34:127–132
46. Ahmed DR, Metcalf Pegram JW (1981) Uncertainty propagation in probabilistic risk assessment: A comparative study. Nucl Eng Des 68:1–3
47. Keey RB, Smith CH (1985) The propagation of uncertainties in failure events". Reliab Eng 10:105–127
48. Zhang Q (1990) A new approximate method for uncertainty propagation in system reliability analysis. Reliab Eng Syst Safety 29:261–275
49. Mon DL, Cheng CH (1994) Fuzzy system reliability analysis for components with different membership functions. Fuzzy Sets Syst 64:145–157
50. Helton JC (1994) Treatment of uncertainty in performance assessment for complex systems. Risk Analysis 483–511

51. Bae H, Grandhi RV, Canfield RA (2004) An approximation approach for uncertainty quantification using evidence theory. Reliab Eng Syst Safety 86:215–225
52. Misra KB, Weber GG (1989) A new method for fuzzy fault tree analysis. Micr Rel 29(2):195–216
53. Parry GW (1996) The characterization of uncertainty in probabilistic risk as-sessments of complex systems. Reliab Eng Syst Safety 54:119–126
54. Cornell MEP (54) Uncertainties in risk analysis: Six levels of treatment. Reliability Engineering and System Safety 54:95–111
55. Tucker WT, Ferson S (2003) Probability bounds analysis in environmental risk assessments. Appl Biomath
56. Bruns M, Christiaan J, Paredis J (2006) Numerical methods for propagating imprecise uncertainty, Proceedings of IDETC 2006: ASME Design Engineer-ing and Technical Conferences and Design Automation Conference, September 10–13, 2006, Philadelphia, PA, USA
57. Frey HC, Bharvirkar R (2002) Quantification of variability and uncertainty: A case study of power plant hazardous air pollutant emissions, Chapter 10 in Human and Ecological Risk Analysis, D. Paustenbach, Ed., John Wiley and Sons: New York, 2002. pp 587–617
58. Williamson RC, Downs T (1990) Probabilistic arithmetic I: numerical meth-ods for calculating convolutions and dependency bounds. Int J Approximate Reasoning 4:89–158
59. Saltelli A, Marivoet J (1990) Non-parameter statistics in sensitivity analysis for model out-put: A comparison of selected techniques. Reliab Eng Syst Safety 28:229–253
60. Borgonovo E (2006) Measuring uncertainty importance: Investigation and comparison of alternative approaches. Risk Anal 26:1349–1361
61. Iman RL, Conover WJ (1987) A measure of top down correlation. Technometrics 29(3): 351–357
62. Iman RL, Hora SC (1990) A robust measure of uncertainty importance for use in fault tree system analysis. Risk Anal 10(3):401–406
63. Homma T, Saltelli A (1996) Importance measures in global analysis of nonlinear models. Reliab Eng Syst Safety 52:1–17
64. Borgonovo E, Apostolakis GE, Tarantola S, Saltelli A (2003) Comparison of global sensitivity analysis techniques and importance measures in PSA. Reliab Eng Syst Safety 79:175–185
65. Utkin LV (1993) Uncertainty importance of system components by fuzzy and interval probability. Microelectron Reliab 33(9):1357–1364
66. Utkin LV (1993) Uncertainty importance of multistate system components. Microelectron Reliab 33(13):2021–2029
67. Abrahamsson M (2002) Uncertainty in quantitative risk analysis. Report 1024, Lund University
68. Rao KD, Kushwaha HS, Verma AK, Srividya A (2009) A new uncertainty importance measure in fuzzy reliability analysis. Int J Performab Eng 5(3):219–226
69. Cheng CH (1998) A new approach for ranking fuzzy numbers by distance method. Fuzzy Sets Syst 95:307–317
70. Ying W, Jian Y, Dong X, Kwai C (2006) On the centroids of fuzzy numbers. Fuzzy Sets Syst 157:919–926
71. Zhi P, Tai Ya (1988) Variance importance of system components by Monte-Carlo. IEEE Trans Reliab 37(4):421–423
72. ISOGRAPH, FaultTree + 10.1, Commercial software for fault tree analysis, UK
73. Hora SC (1996) Aleatory and epistemic uncertainty in probability elicitation with an example from hazardous waste management. Reliab Eng Syst Safety 54:217–223
74. Ferson S et al (2004) Summary from the epistemic uncertainty workshop: Consensus amid diversity. Reliab Eng Syst Safety 85:355–369
75. Stephen CH (1996) Aleatory and epistemic uncertainty in probability elicitation with an example from hazardous waste management. Reliab Eng Syst Safety 54:217–223
76. Vose D (2000) Risk analysis-A quantitative guide. Wiley, New York

77. Durga Rao K, Kushwaha HS, Verma AK, Srividya A (2007) Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies. Reliab Eng Syst Safety 92(7):947–956
78. Jadhav PA (2007) Belief and plausibility analysis: Steady state heat conduction applications. DAE BRNS Theme Meeting on Methodology for Quantification and Propagation of Uncertainty in Safety Assessment of NPP and Fuel Cycle Facilities: 108–131
79. Kushwaha HS (2009) Uncertainty modeling and analysis. Bhabha Atomic Research Centre, Mumbai
80. Durga Rao K, Kushwaha HS, Verma AK, Srividya A (2008) Epistemic uncertainty propaga-tion in reliability assessment of complex systems. Int J Performab Eng 4(1):71–84
81. USNRC (1975) Reactor safety study. WASH-1400, NUREG-75/014, United States Nuclear Regulatory Commission
82. IAEA (1988) Component reliability data for use in probabilistic safety assessment. IAEA TECDOC 478, International Atomic Energy Agency, Vienna
83. Karanki DR, Kushwaha HS, Verma AK, Srividya A (2009) Uncertainty analysis based on probability bounds (p-box) approach in probabilistic safety assessment. Risk Anal 29(5): 662–675

Appendix

Distribution Tables

See Tables A.1, A.2, A.3 and A.4

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

Table A.1 Cumulative areas under standard normal distribution

Z	0	1	2	3	4	5	6	7	8
−3.0	0.0013	0.0010	0.0007	0.0005	0.0003	0.0002	0.0002	0.0001	0.0001
−2.9	0.0019	0.0018	0.0017	0.0017	0.0016	0.0016	0.0015	0.0015	0.0014
−2.8	0.0026	0.0025	0.0024	0.0023	0.0023	0.0022	0.0021	0.0021	0.0020
−2.7	0.0035	0.0034	0.0033	0.0032	0.0031	0.0030	0.0029	0.0028	0.0027
−2.6	0.0047	0.0045	0.0044	0.0043	0.0041	0.0040	0.0039	0.0038	0.0037
−2.5	0.0062	0.0060	0.0059	0.0057	0.0055	0.0054	0.0052	0.0051	0.0049
−2.4	0.0082	0.0080	0.0078	0.0075	0.0073	0.0071	0.0069	0.0068	0.0066
−2.3	0.0107	0.0104	0.0102	0.0099	0.0096	0.0094	0.0091	0.0089	0.0087
−2.2	0.0139	0.0136	0.0132	0.0129	0.0126	0.0122	0.0119	0.0116	0.0113
−2.1	0.0179	0.0174	0.0170	0.0166	0.0162	0.0158	0.0154	0.0150	0.0146
−2.0	0.0228	0.0222	0.0217	0.0212	0.0207	0.0202	0.0197	0.0192	0.0188
−1.9	0.0287	0.0281	0.0274	0.0268	0.0262	0.0256	0.0250	0.0244	0.0238
−1.8	0.0359	0.0352	0.0344	0.0336	0.0329	0.0322	0.0314	0.0307	0.0300
−1.7	0.0446	0.0436	0.0427	0.0418	0.0409	0.0401	0.0392	0.0384	0.0375
−1.6	0.0548	0.0537	0.0526	0.0516	0.0505	0.0495	0.0485	0.0475	0.0465
−1.5	0.0668	0.0655	0.0643	0.0630	0.0618	0.0606	0.0594	0.0582	0.0570
−1.4	0.0808	0.0793	0.0778	0.0764	0.0749	0.0735	0.0722	0.0708	0.0694
−1.3	0.0968	0.0951	0.0934	0.0918	0.0901	0.0885	0.0869	0.0853	0.0838
−1.2	0.1151	0.1131	0.1112	0.1093	0.1075	0.1056	0.1038	0.1020	0.1003
−1.1	0.1357	0.1335	0.1314	0.1292	0.1271	0.1251	0.1230	0.1210	0.1190
−1.0	0.1587	0.1562	0.1539	0.1515	0.1492	0.1469	0.1446	0.1423	0.1401
−0.9	0.1841	0.1814	0.1788	0.1762	0.1736	0.1711	0.1685	0.1660	0.1635
−0.8	0.2119	0.2090	0.2061	0.2033	0.2005	0.1977	0.1949	0.1922	0.1894
−0.7	0.2420	0.2389	0.2358	0.2327	0.2297	0.2266	0.2236	0.2206	0.2177

(continued)

Table A.1 (continued)

Z	0	1	2	3	4	5	6	7	8
−0.6	0.2743	0.2709	0.2676	0.2643	0.2611	0.2578	0.2546	0.2514	0.2483
−0.5	0.3085	0.3050	0.3015	0.2981	0.2946	0.2912	0.2877	0.2843	0.2810
−0.4	0.3446	0.3409	0.3372	0.3336	0.3300	0.3264	0.3228	0.3192	0.3156
−0.3	0.3821	0.3783	0.3745	0.3707	0.3669	0.3632	0.3594	0.3557	0.3520
−0.2	0.4207	0.4168	0.4129	0.4090	0.4052	0.4013	0.3974	0.3936	0.3897
−0.1	0.4602	0.4562	0.4522	0.4483	0.4443	0.4404	0.4364	0.4325	0.4286
−0.0	0.5000	0.4960	0.4920	0.4880	0.4840	0.4801	0.4761	0.4721	0.4681
0.0	0.5000	0.5040	0.5080	0.5120	0.5160	0.5199	0.5239	0.5279	0.5319
0.1	0.5398	0.5438	0.5478	0.5517	0.5557	0.5596	0.5636	0.5675	0.5714
0.2	0.5793	0.5832	0.5871	0.5910	0.5948	0.5987	0.6026	0.6064	0.6103
0.3	0.6179	0.6217	0.6255	0.6293	0.6331	0.6368	0.6406	0.6443	0.6480
0.4	0.6554	0.6591	0.6628	0.6664	0.6700	0.6736	0.6772	0.6808	0.6844
0.5	0.6915	0.6950	0.6985	0.7019	0.7054	0.7088	0.7123	0.7157	0.7190
0.6	0.7257	0.7291	0.7324	0.7357	0.7389	0.7422	0.7454	0.7486	0.7517
0.7	0.7580	0.7611	0.7642	0.7673	0.7703	0.7734	0.7764	0.7794	0.7823
0.8	0.7881	0.7910	0.7939	0.7967	0.7995	0.8023	0.8051	0.8078	0.8106
0.9	0.8159	0.8186	0.8212	0.8238	0.8264	0.8289	0.8315	0.8340	0.8365
1.0	0.8413	0.8438	0.8461	0.8485	0.8508	0.8531	0.8554	0.8577	0.8599
1.1	0.8643	0.8665	0.8686	0.8708	0.8729	0.8749	0.8770	0.8790	0.8810
1.2	0.8849	0.8869	0.8888	0.8907	0.8925	0.8944	0.8962	0.8980	0.8997
1.3	0.9032	0.9049	0.9066	0.9082	0.9099	0.9115	0.9131	0.9147	0.9162
1.4	0.9192	0.9207	0.9222	0.9236	0.9251	0.9265	0.9278	0.9292	0.9306
1.5	0.9332	0.9345	0.9357	0.9370	0.9382	0.9394	0.9406	0.9418	0.9430
1.6	0.9452	0.9463	0.9474	0.9484	0.9495	0.9505	0.9515	0.9525	0.9535

(continued)

Table A.1 (continued)

Z	0	1	2	3	4	5	6	7	8
1.7	0.9554	0.9564	0.9573	0.9582	0.9591	0.9599	0.9608	0.9616	0.9625
1.8	0.9641	0.9648	0.9656	0.9664	0.9671	0.9678	0.9686	0.9693	0.9700
1.9	0.9713	0.9719	0.9726	0.9732	0.9738	0.9744	0.9750	0.9756	0.9762
2.0	0.9772	0.9778	0.9783	0.9788	0.9793	0.9798	0.9803	0.9808	0.9812
2.1	0.9821	0.9826	0.9830	0.9834	0.9838	0.9842	0.9846	0.9850	0.9854
2.2	0.9861	0.9864	0.9868	0.9871	0.9874	0.9878	0.9881	0.9884	0.9887
2.3	0.9893	0.9896	0.9898	0.9901	0.9904	0.9906	0.9909	0.9911	0.9913
2.4	0.9918	0.9920	0.9922	0.9925	0.9927	0.9929	0.9931	0.9932	0.9934
2.5	0.9938	0.9940	0.9941	0.9943	0.9945	0.9946	0.9948	0.9949	0.9951
2.6	0.9953	0.9955	0.9956	0.9957	0.9959	0.9960	0.9961	0.9962	0.9963
2.7	0.9965	0.9966	0.9967	0.9968	0.9969	0.9970	0.9971	0.9972	0.9973
2.8	0.9974	0.9975	0.9976	0.9977	0.9977	0.9978	0.9979	0.9979	0.9980
2.9	0.9981	0.9982	0.9982	0.9983	0.9984	0.9984	0.9985	0.9985	0.9986
3.0	0.9987	0.9990	0.9993	0.9995	0.9997	0.9998	0.9998	0.9999	0.9999

Table A.2 Quantiles for Student's t distribution

d.c. (v)	Level of significance (α)						
	0.20	0.10	0.05	0.02	0.01	0.005	0.001
1	3.08	6.31	12.71	31.82	63.66	127.32	635.62
2	1.89	2.92	4.30	6.97	9.93	14.09	31.60
3	1.64	2.35	3.18	4.54	5.84	7.45	12.94
4	1.53	2.13	2.78	3.75	4.60	5.60	8.61
5	1.48	2.02	2.57	3.37	4.03	4.77	6.86
6	1.44	1.94	2.45	3.14	3.71	4.32	5.96
7	1.42	1.90	2.37	3.00	3.50	4.03	5.41
8	1.40	1.86	2.31	2.90	3.36	3.83	5.04
9	1.38	1.83	2.26	2.82	3.25	3.69	4.78
10	1.37	1.81	2.23	2.76	3.17	3.58	4.59
11	1.36	1.80	2.20	2.72	3.11	3.50	4.44
12	1.36	1.78	2.18	2.68	3.06	3.43	4.32
13	1.35	1.77	2.16	2.65	3.01	3.37	4.22
14	1.34	1.76	2.15	2.62	2.98	3.33	4.14
15	1.34	1.75	2.13	2.60	2.95	3.29	4.07
16	1.34	1.75	2.12	2.58	2.92	3.25	4.02
17	1.33	1.74	2.11	2.57	2.90	3.22	3.97
18	1.33	1.73	2.10	2.55	2.88	3.20	3.92
19	1.33	1.73	2.09	2.54	2.86	3.17	3.88
20	1.33	1.73	2.09	2.53	2.85	3.15	3.85
21	1.32	1.72	2.08	2.52	2.83	3.14	3.82
22	1.32	1.72	2.07	2.51	2.82	3.12	3.79
23	1.32	1.71	2.07	2.50	2.81	3.10	3.77
24	1.32	1.71	2.06	2.49	2.80	3.09	3.75
25	1.32	1.71	2.06	2.48	2.79	3.08	3.73
26	1.32	1.71	2.06	2.48	2.78	3.07	3.71
27	1.31	1.70	2.05	2.47	2.77	3.06	3.69
28	1.31	1.70	2.05	2.47	2.76	3.05	3.67
29	1.31	1.70	2.04	2.46	2.76	3.04	3.66
30	1.31	1.70	2.04	2.46	2.75	3.03	3.65
40	1.30	1.68	2.02	2.42	2.70	2.97	3.55
60	1.30	1.67	2.00	2.39	2.66	2.91	3.46
120	1.29	1.66	1.98	2.36	2.62	2.86	3.37
Infinity	1.28	1.64	1.96	2.33	2.58	2.81	3.29

Table A.3 Quantiles for the Chi-Square distribution

d. f. (v)	Level of significance (α)							
	0.99	0.98	0.95	0.90	0.80	0.70	0.50	0.30
1	0.00016	0.0006	0.0039	0.016	0.064	0.148	0.455	1.07
2	0.020	0.040	0.103	0.211	0.446	0.713	1.386	2.41
3	0.115	0.185	0.352	0.584	1.005	1.424	2.366	3.66
4	0.30	0.43	0.71	1.06	1.65	2.19	3.36	4.9
5	0.55	0.75	1.14	1.61	2.34	3.00	4.35	6.1
6	0.87	1.13	1.63	2.20	3.07	3.83	5.35	7.2
7	1.24	1.56	2.17	2.83	3.82	4.61	6.35	8.4
8	1.65	2.03	2.73	3.49	4.59	5.53	7.34	9.5
9	2.09	2.53	3.32	4.17	5.38	6.39	8.34	10.7
10	2.56	3.06	3.94	4.86	6.18	7.27	9.34	11.8
11	3.1	3.6	4.6	5.6	7.0	8.1	10.3	12.9
12	3.6	4.2	5.2	6.3	7.8	9.0	11.3	14.0
13	4.1	4.8	5.9	7.0	8.6	9.9	12.3	15.1
14	4.7	5.4	6.6	7.8	9.5	10.8	13.3	16.2
15	5.2	6.0	7.3	8.5	10.3	11.7	14.3	17.3
16	5.8	6.6	8.0	9.3	11.2	12.6	15.3	18.4
17	6.4	7.3	8.7	10.1	12.0	13.5	16.3	19.5
18	7.0	7.9	9.4	10.9	12.9	14.4	17.3	20.6
19	7.6	8.6	10.1	11.7	13.7	15.4	18.3	21.7
20	8.3	9.2	10.9	12.4	14.6	16.3	19.3	22.8
21	8.9	9.9	11.6	13.2	15.4	17.2	20.3	23.9
22	9.5	10.6	12.3	14.0	16.3	18.1	21.3	24.9
23	10.2	11.3	13.1	14.8	17.2	19.0	22.3	26.0
24	10.9	12.0	13.8	15.7	18.1	19.9	23.3	27.1
25	11.5	12.7	14.6	16.5	18.9	20.9	24.3	28.2
26	12.2	13.4	15.4	17.3	19.8	21.8	25.3	29.3
27	12.9	14.1	16.2	18.1	20.7	22.7	26.3	30.3
28	13.6	14.8	16.9	18.9	21.6	23.6	27.3	31.4
29	14.3	15.6	17.7	19.8	22.4	24.6	28.3	32.5
30	15.0	16.3	18.5	20.6	23.4	25.5	29.3	33.5
1	1.64	2.7	3.8	5.4	6.6	7.9	9.5	10.8
2	3.22	4.6	6.0	7.8	9.2	10.6	12.4	13.8
3	4.64	6.3	7.8	9.8	11.3	12.8	14.8	16.3
4	6.0	7.8	9.5	11.7	13.3	14.9	16.9	18.5
5	7.3	9.2	11.1	13.4	15.1	16.3	18.9	20.5
6	8.6	10.6	12.6	15.0	16.8	18.6	20.7	22.5
7	9.8	12.0	14.1	16.6	18.5	20.3	22.6	24.3
8	11.0	13.4	15.5	18.2	20.1	21.9	24.3	26.1
9	12.2	14.7	16.9	19.7	21.7	23.6	26.1	27.9

(continued)

Table A.3 (continued)

d. f. (v)	Level of significance (α)							
	0.99	0.98	0.95	0.90	0.80	0.70	0.50	0.30
10	13.4	16.0	18.3	21.2	23.2	25.2	27.7	29.6
11	14.6	17.3	19.7	22.6	24.7	26.8	29.4	31.3
12	15.8	18.5	21.0	24.1	26.2	28.3	31.0	32.9
13	17.0	19.8	22.4	25.5	27.7	29.8	32.5	34.5
14	18.2	21.1	23.7	26.9	29.1	31.3	34.0	36.1
15	19.3	22.3	25.0	28.3	30.6	32.8	35.5	37.7
16	20.5	23.5	26.3	29.6	32.0	34.3	37.0	39.2
17	21.6	24.8	27.6	31.0	33.4	35.7	38.5	40.8
18	22.8	26.0	28.9	32.3	34.8	37.2	40.0	42.3
19	23.9	27.2	30.1	33.7	36.2	38.6	41.5	43.8
20	25.0	28.4	31.4	35.0	37.6	40.0	43.0	45.3
21	26.2	29.6	32.7	36.3	38.9	41.4	44.5	46.8
22	27.3	30.8	33.9	37.7	40.2	42.8	46.0	48.3
23	28.4	32.0	35.2	39.0	41.6	44.2	47.5	49.7
24	29.6	33.2	36.4	40.3	43.0	45.5	48.5	51.2
25	30.7	34.4	37.7	41.6	44.3	46.9	50.0	52.6
26	31.8	35.6	38.9	42.9	45.6	48.3	51.5	54.1
27	32.9	36.7	40.1	44.1	47.0	49.6	53.0	55.5
28	34.0	37.9	41.3	45.4	48.3	51.0	54.5	56.9
29	35.1	39.1	42.6	46.7	49.6	52.3	56.0	58.3
30	36.3	40.3	43.8	48.0	50.9	53.7	57.5	59.7

Table A.4 Quantiles for the F distribution, F 0.90

	v_1											
v_2	1	2	3	4	5	6	7	8	9	12	24	∞
1	39.86	49.50	53.5	55.8	57.2	58.2	58.9	59.4	59.8	60.7	62.0	63.33
2	8.53	9.00	9.16	9.24	9.29	9.33	9.35	9.37	9.38	9.41	9.45	9.49
3	5.54	5.46	5.39	5.34	5.31	5.28	5.27	5.25	5.24	5.22	5.18	5.13
4	4.54	4.32	4.19	4.11	4.05	4.01	3.98	3.95	3.94	3.90	3.83	3.76
5	4.06	3.78	3.62	3.52	3.45	3.40	3.37	3.34	3.32	3.27	3.19	3.10
6	3.78	3.46	3.29	3.18	3.11	3.05	3.01	2.98	2.96	2.90	2.82	2.72
7	3.59	3.26	3.07	2.96	2.88	2.83	2.78	2.75	2.72	2.67	2.58	2.47
8	3.46	3.11	2.92	2.81	2.73	2.67	2.62	2.59	2.56	2.50	2.40	2.29
9	3.36	3.01	2.81	2.69	2.61	2.55	2.51	2.47	2.44	2.38	2.28	2.16
10	3.29	2.92	2.73	2.61	2.52	2.46	2.41	2.38	2.35	2.28	2.18	2.06
11	3.23	2.86	2.66	2.54	2.45	2.39	2.34	2.30	2.27	2.21	2.10	1.97
12	3.18	2.81	2.61	2.48	2.39	2.33	2.28	2.24	2.21	2.15	2.04	1.90
13	3.14	2.76	2.56	2.43	2.35	2.28	2.23	2.20	2.16	2.10	1.98	1.85
14	3.10	2.73	2.52	2.39	2.31	2.24	2.19	2.15	2.12	2.05	1.94	1.80
15	3.07	2.70	2.49	2.36	2.27	2.21	2.16	2.12	2.09	2.02	1.90	1.76
16	3.05	2.67	2.46	2.33	2.24	2.18	2.13	2.09	2.06	1.99	1.87	1.72
17	3.03	2.64	2.44	2.31	2.22	2.15	2.10	2.06	2.03	1.96	1.84	1.69
18	3.01	2.62	2.42	2.29	2.20	2.13	2.08	2.04	2.01	1.93	1.81	1.66
19	2.99	2.61	2.40	2.27	2.18	2.11	2.06	2.02	1.98	1.91	1.79	1.63
20	2.97	2.59	2.38	2.25	2.16	2.09	2.04	2.00	1.96	1.89	1.77	1.61
21	2.96	2.57	2.36	2.23	2.14	2.08	2.02	1.98	1.95	1.87	1.75	1.59
22	2.95	2.56	2.35	2.22	2.13	2.06	2.01	1.97	1.93	1.86	1.73	1.57
23	2.94	2.55	2.34	2.21	2.11	2.05	1.99	1.95	1.92	1.84	1.72	1.55

(continued)

Table A.4 (continued)

	v_1											
v_2	1	2	3	4	5	6	7	8	9	12	24	∞
24	2.93	2.54	2.33	2.19	2.10	2.04	1.98	1.94	1. 91	1.83	1.70	1.53
25	2.92	2.53	2.32	2.18	2.09	2.02	1. 97	1. 93	1.89	1.82	1.69	1.52
26	2.91	2.52	2.31	2.17	2.08	2.01	1.96	1.92	1.88	1.81	1.68	1.50
27	2.90	2.51	2.30	2.17	2.07	2.00	1.95	1. 91	1.87	1.80	1.67	1.49
28	2.89	2.50	2.29	2.16	2.06	2.00	1.94	1.90	1.87	1.79	1.66	1.48
29	2.89	2.50	2.28	2.15	2.06	1.99	1. 93	1.89	1.86	1.78	1.65	1.47
30	2.88	2.49	2.28	2.14	2.05	1.98	1. 93	1. 88	1.85	1.77	1.64	1.46
40	2.84	2.44	2.23	2.09	2.00	1.93	1.87	1.83	1.79	1.71	1.57	1.38
60	2.79	2.39	2.18	2.04	1.95	1.87	1.82	1.77	1.74	1.66	1.51	1.29
120	2.75	2.35	2.13	1.99	1.90	1.82	1.77	1.72	1.68	1.60	1.45	1.19
>	2.71	2.30	2.08	1.94	1.85	1.77	1.72	1.67	1.63	1.55	1.38	1.00
1	161.4	199.5	215.7	224.6	230.2	234.0	236.8	238.9	240.5	243.9	249.1	254.3
2	18.51	19.00	19.16	19.25	19.30	19.33	19.35	19.37	19.38	19.41	19.45	19.50
3	10.13	9.55	9.28	9.12	9.01	8.94	8.89	8.85	8.81	8.74	8.64	8.53
4	7.71	6.94	6.59	6.39	6.26	6.16	6.09	6.04	6.00	5.91	5.77	5.63
5	6.61	5.79	5.41	5.19	5.05	4.95	4.88	4.82	4.77	4.68	4.53	4.36
6	5.99	5.14	4.76	4.53	4.39	4.28	4.21	4.15	4.10	4.00	3.84	3.67
7	5.59	4.74	4.35	4.12	3.97	3.87	3.79	3.73	3.68	3.57	3.41	3.23
8	5.32	4.46	4.07	3.84	3.68	3.85	3.50	3.44	3.39	3.28	3.12	2.93
9	5.12	4.26	3.86	3.63	3.48	3.37	3.29	3.23	3.18	3.07	2.90	2.71
10	4.96	4.10	3.71	3.48	3.33	3.22	3.14	3.07	3.02	2.91	2.74	2.54
11	4.84	3.98	3.59	3.36	3.20	3.09	3.01	2.95	2.90	2.79	2.61	2.40
12	4.75	3.89	3.49	3.26	3.11	3.00	2.91	2.85	2.80	2.69	2.51	2.30

(continued)

Table A.4 (continued)

	v_1											
v_2	1	2	3	4	5	6	7	8	9	12	24	∞
13	4.67	3.81	3.41	3.18	3.03	2.92	2.83	2.77	2.71	2.60	2.42	2.21
14	4.60	3.74	3.34	3.11	2.96	2.85	2.76	2.70	2.65	2.53	2.35	2.13
15	4.54	3.68	3.29	3.06	2.90	2.79	2.71	2.64	2.59	2.48	2.29	2.07
16	4.49	3.63	3.24	3.01	2.85	2.74	2.66	2.59	2.54	2.42	2.24	2.01
17	4.45	3.59	3.20	2.96	2.81	2.70	2.61	2.55	2.49	2.38	2.19	1.96
18	4.41	3.55	3.16	2.93	2.77	2.66	2.58	2.51	2.46	2.34	2.15	1.92
19	4.38	3.52	3.13	2.90	2.74	2.63	2.54	2.48	2.42	2.31	2.11	1.88
20	4.35	3.49	3.10	2.87	2.71	2.60	2.51	2.45	2.39	2.28	2.08	1.84
21	4.32	3.47	3.07	2.84	2.68	2.57	2.49	2.42	2.37	2.25	2.05	1.81
22	4.30	3.44	3.05	2.82	2.66	2.55	2.46	2.40	2.34	2.23	2.03	1.78
23	4.28	3.42	3.03	2.80	2.64	2.53	2.44	2.37	2.32	2.20	2.01	1. 76
24	4.26	3.40	3.01	2.78	2.62	2.51	2.42	2.36	2.30	2.18	1.98	1.73
25	4.24	3.39	2.99	2.76	2.60	2.49	2.40	2.34	2.28	2.16	1.96	1.71
26	4.23	3.37	2.98	2.74	2.59	2.47	2.39	2.32	2.27	2.15	1. 95	1.69
27	4.21	3.35	2.96	2.73	2.57	2.46	2.37	2.31	2.25	2.13	1.93	1.67
28	4.20	3.34	2.95	2.71	2.56	2.45	2.36	2.29	2.24	1.12	1.91	1.65
29	4.18	3.33	2.93	2.70	2.55	2.43	2.35	2.28	2.22	2.10	1.90	1.64
30	4.17	3.32	2.92	2.69	2.53	2.42	2.33	2.27	2.21	2.09	1.89	1.62
40	4.08	3.23	2.84	2.61	2.45	2.34	2.25	2.18	2.12	2.00	1.79	1.51
60	4.00	3.15	2.76	2.53	2.37	2.25	2.17	2.10	2.04	1. 92	1.70	1.39
120	3.92	3.07	2.68	2.45	2.29	2.17	2.09	2.02	1. 96	1. 83	1. 61	1.25
>	3.84	3.00	2.60	2.37	2.21	2.10	2.01	1.94	1.88	1.75	1.52	1.00
1	4052	4999	5403	5625	5764	5859	5928	5982	6022	6106	6235	6366

(continued)

Table A.4 (continued)

	v_1											
v_2	1	2	3	4	5	6	7	8	9	12	24	∞
2	98.50	99.00	99.1	99.25	99.30	99.33	99.36	99.37	99.39	99.42	99.46	99.50
3	34.12	30.82	29.4	28.71	28.24	27.91	27.67	27.49	27.35	27.05	26.60	26.13
4	21.20	18.00	16.7	15.98	15.52	15.21	14.98	14.80	14.66	14.37	13.93	13.46
5	16.26	13.27	12.0	11.39	10.97	10.67	10.46	10.29	10.16	9.89	9.47	9.02
6	13.75	10.92	9.78	9.15	8.75	8.47	8.26	8.10	7.98	7.72	7.31	6.88
7	12.25	9.55	8.45	7.85	7.46	7.19	6.99	6.84	6.72	6.47	6.07	5.65
8	11.26	8.65	7.59	7.01	6.63	6.37	6.18	6.03	5.91	5.67	5.28	4.86
9	10.56	8.02	6.99	6.42	6.06	5.80	5.61	5.47	5.35	5.11	4.73	4.31
10	10.04	7.56	6.55	5.99	5.64	5.39	5.20	5.06	4.94	4.71	4.33	3.91
11	9.65	7.21	6.22	5.67	5.32	5.07	4.89	4.74	4.63	4.40	4.02	3.60
12	9.33	6.93	5.95	5.41	5.06	4.82	4.64	4.50	4.39	4.16	3.78	3.36
13	9.07	6.70	5.74	5.21	4.86	4.62	4.44	4.30	4.19	3.96	3.59	3.17
14	8.86	6.51	5.56	5.04	4.69	4.46	4.28	4.14	4.03	3.80	3.43	3.00
15	8.68	6.36	5.42	4.89	4.56	4.32	4.14	4.00	3.89	3.67	3.29	2.87
16	8.53	6.23	5.29	4.77	4.44	4.20	4.03	3.89	3.78	3.55	3.18	2.75
17	8.40	6.11	5.18	4.67	4.34	4.10	3.93	3.79	3.68	3.46	3.08	2.65
18	8.29	6.01	5.09	4.58	4.25	4.01	3.84	3.71	3.60	3.37	3.00	2.57
19	8.18	5.93	5.01	4.50	4.17	3.94	3.77	3.63	3.52	3.30	2.92	2.49
20	8.10	5.85	4.94	4.43	4.10	3.87	3.70	3.56	3.46	3.23	2.86	2.42
21	8.02	5.78	4.87	4.37	4.04	3.81	3.64	3.51	3.40	3.17	2.80	2.36
22	7.95	5.72	4.82	4.31	3.99	3.76	3.59	3.45	3.35	3.12	2.75	2.31
23	7.88	5.66	4.76	4.26	3.94	3.71	3.54	3.41	3.30	3.07	2.70	2.26
24	7.82	5.61	4.72	4.22	3.90	3.67	3.50	3.36	3.26	3.03	2.66	2.21

(continued)

Table A.4 (continued)

	v_1											
v_2	1	2	3	4	5	6	7	8	9	12	24	∞
25	7.77	5.57	4.68	4.18	3.85	3.63	3.46	3.32	3.22	2.99	2.62	2.17
26	7.72	5.53	4.64	4.14	3.82	3.59	3.42	3.29	3.18	2.96	2.58	2.13
27	7.68	5.49	4.60	4.11	3.78	3.56	3.39	3.26	3.15	2.93	2.55	2.10
28	7.64	5.45	4.57	4.07	3.75	3.53	3.36	3.23	3.12	2.90	2.52	2.06
29	7.60	5.42	4.54	4.04	3.73	3.50	3.33	3.20	3.09	2.87	2.49	2.03
30	7.56	5.39	4.51	4.02	3.70	3.47	3.30	3.17	3.07	2.84	2.47	2.01
40	7.31	5.18	4.31	3.83	3.51	3.29	3.12	2.99	2.89	2.66	2.29	1.80
60	7.08	4.98	4.13	3.65	3.34	3.12	2.95	2.82	2.72	2.50	2.12	1.60
120	6.85	4.79	3.95	3.48	3.17	2.96	2.79	2.66	2.56	2.34	1.95	1.38
>	6.63	4.61	3.78	3.32	3.02	2.80	2.64	2.51	2.41	2.18	1.79	1.00

Index

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