SYSTEM RELIABILITY THEORY

Models, Statistical Methods, and Applications

SECOND EDITION

Marvin Rausand
École des Mines de Nantes
Departement Productique et Automatique
Nantes Cedex 3 France

Arnljot Høyland

A JOHN WILEY & SONS, INC., PUBLICATION

This Page Intentionally Left Blank

SYSTEM RELIABILITY THEORY

Second Edition

WILEY SERIES IN PROBABILITY AND STATISTICS

Established by WALTER A. SHEWHART and SAMUEL S. WILKS

A complete list of the titles in this series appears at the end of this volume.

SYSTEM RELIABILITY THEORY

Models, Statistical Methods, and Applications

SECOND EDITION

Marvin Rausand
École des Mines de Nantes
Departement Productique et Automatique
Nantes Cedex 3 France

Arnljot Høyland

A JOHN WILEY & SONS, INC., PUBLICATION

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Rausand, Marvin.
System reliability theory : models, statistical methods, and applications / Marvin Rausand, Arnljot Høyland. — 2nd ed.
p. cm. — (Wiley series in probability and mathematics. Applied probability and statistics)
Høyland's name appears first on the eariler edition.
Includes bibliographical references and index.
ISBN 0-471-47133-X (acid-free paper)
1. Reliability (Engineering)—Statistical methods. I. Høyland, Arnljot, 1924– II. Title. III. Series.

TA169.H68 2004
620'.00452—dc22 2003057631

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

The second edition is dedicated to the memory of
Professor Arnljot Høyland (1924–2002)

This Page Intentionally Left Blank

Contents

This Page Intentionally Left Blank

Preface to the Second Edition

The second edition of *System Reliability Theory* is a major upgrade compared to the first edition. Two new chapters have been added, and most of the original chapters have been significantly revised. Most of the text has been rewritten, and all the figures have been redrawn. The new chapters are:

Chapter 9, Reliability of Maintained Systems, where reliability assessment of repairable systems is discussed, together with models and methods for optimization of age-based and condition-based replacement policies. A description of reliability centered maintenance (RCM) and total productive maintenance (TPM) is also given.

Chapter 10, Reliability of Safety Systems, where reliability assessment of periodically tested safety-critical systems is discussed. The terminology from the international standard IEC61508 is used, and an approach to document compliance with this standard is outlined.

New material has been included in all the original chapters, with the greatest number of additions in Chapters 3, 5, and 7. Various approaches to functional modelling and analysis are included in Chapter 3, Qualitative System Analysis, as a basis for failure analysis. Chapter 3 is very fundamental and it may be beneficial to read this chapter before reading Chapter 2.

The second edition has more focus on practical application of reliability theory than the first edition. This is mainly shown by the two new chapters and by the high number of new worked examples that are based on real industry problems and real data.

A glossary of the main terms used in the book has been included at the end of the book, together with a list of acronyms and abbreviations.

The revision of the book is based on experience from using the book in various courses in reliability and life data analysis at the Norwegian University of Science and Technology (NTNU) in Trondheim, continuing education courses arranged for industry both in Norway and abroad. Many instructors who have used the first edition have sent very useful comments and suggestions. Feedback has also been received from people working in industry and consulting companies who have used the book as a reference in practical reliability studies. These comments have led to improvements in the second edition.

Audience and Assumed Knowledge. The book has primarily been written as a textbook for university courses at senior undergraduate and graduate level. The

book is also intended as a reference book for practicing engineers in industry and consulting companies, and for engineers who which to do self-study.

The reader should have some knowledge of calculus and of elementary probability theory and statistics. We have tried to avoid heavy mathematical formalism, especially in the first six chapters of the book. Several worked examples are included to illustrate the use of the various methods.

A number of problems are included at the end of almost all the chapters. The problems give the readers a chance to test their knowledge and to verify that they have understood the material. We have tried to arrange the problems such that the easiest problems come first. Some problems are rather complex and cover extensions of the theory presented in the chapter.

Use as a Textbook. The second edition should be applicable as a text for several types of courses, both at senior undergraduate as well as graduate level. Some suggested courses are listed in Table P.1. Each course in Table P.1 is a one-semester course with two to three lectures per week. Several alternatives to these courses may be defined based on the desired focus of the course and the background of the students. It should be possible to cover the whole book in a two-semester course with three to four lectures per week. Examples of detailed course programs at NTNU may be found on the associated web site.

Solutions to the problems are not provided as part of the book. A solutions manual, which contains full worked-out solutions to selected problems is, however, available to instructors and self-learning practicing engineers. A free copy can be obtained by contacting the author (marvin.rausand@ipk.ntnu.no).

Associated web site. The first edition contained detailed references to computer programs for the various methods and approaches. These have been removed from the second edition and included in a web site that is associated to the book (see end

Table P.1. Suggested Courses Based on the Book

	Chapters													
Course	1	2	3	4	5	6	7	8	9	10	11	12	13	14
System reliability theory (undergraduate course)	x	(x)	x	x	(x)			(x)	(x)				(x)	x
System reliability theory (graduate course)	x	x	(x)	x	x	x		x		(x)			x	x
Reliability of safety systems	x	(x)	x	x	(x)	x		(x)		x				x
Reliability and maintenance modelling	x	x	x	x			x	(x)	x	(x)				x
Analysis of life data	x	x	(x)				x				x	x	x	x

(x) means that this chapter may be an option or that only part of the chapter is required.

of Chapter 1). The reason for this is that such references will be outdated rather fast and are easier maintained on a web site. The intention is to keep this web site as up-to-date as possible, including additional information and links to other sites that are potentially useful to instructors, students, and other users of the book.

MARVIN RAUSAND

This Page Intentionally Left Blank

Preface to the First Edition

The main purpose of this book is to present a comprehensive introduction to system reliability theory. We have structured our presentation such that the book may be used as a text in introductory as well as graduate level courses. For this purpose we treat simple situations first. Then we proceed to more complicated situations requiringadvanced analytical tools.

At the same time the book has been developed as a reference and handbook for industrial statisticians and reliability engineers.

The reader ought to have some knowledge of calculus and of elementary probability theory and statistics.

In the first five chapters we confine ourselves to situations where the state variables of components and systems are binary and independent. Failure models, qualitative system analysis, and reliability importance are discussed. These chapters constitute an elementary, though comprehensive introduction to reliability theory. They may be covered in a one-semester course with three weekly lectures over fourteen weeks.

The remaining part of the book is somewhat more advanced and may serve as a text for a graduate course. In Chapter 6 situations where the components and systems may be in two or more states are discussed. This situation is modeled by Markov processes. Renewal theory is treated in Chapter 7, and dependent failures in Chapter 8. A rather broad introduction to life data analysis is given in Chapter 9, accelerated life testing in Chapter 10, and Bayesian reliability analysis in Chapter 11. The book concludes with information about reliability data sources in Chapter 12.

The book contains a large number of worked examples, and each chapter ends with a selection of problems, providing exercises and additional applications.

A forerunner of this book, written in Norwegian by professor Arne T. Holen and the present authors, appeared in 1983 as an elementary introduction to reliability analysis. It was published by TAPIR and reprinted in 1988. However, we have rewritten all the chapters of the earlier book and added new material as well as several new chapters. The present book contains approximately twice as many pages as its forerunner and can be considered as a completely new book.

We have already tried much of the material in the present book in courses on reliability and risk analysis at the university level in Norway and Sweden, including continuing education courses for engineers working in industry. The feedback from participants in these courses has significantly improved the quality of the book.

We are grateful to Bjarne Stolpnessæter for drawing most of the figures, and to Anne Kajander for typing a first draft of the manuscript. We are further grateful for economic support by Conoco Norway. Permission from various publishers to reproduce tables and figures is also appreciated.

ARNLJOT HØYLAND AND MARVIN RAUSAND

Trondheim, 1993

Acknowledgments

First of all I would like to express my deepest thanks to Professor Arnljot Høyland. Professor Høyland died in December 2002, 78 years old, and could not participate in writing this second edition. I hope that he would have approved and appreciated the changes and additions I have made.

The second edition was written during my sabbatical year at École des Mines de Nantes (EMN) in France. I am very grateful to Pierre Dejax, Philippe Castagliola, and their colleagues at EMN, who helped me in various ways and made my stay a very positive experience. Special thanks go to Bruno Castanier, EMN, who helped me in all possible ways, and also co-authored a section in Chapter 9 of this second edition. Per Hokstad at SINTEF read drafts to several chapters and gave a lot of constructive comments. Also thanks to Bo Lindqvist, Jørn Vatn, and Knut Øien at NTNU, Tørris Digernes at Aker Kværner, Leif T. Sunde at FMC Kongsberg Subsea, Enrico Zio at Politecnico di Milano, and several anonymous referees for many helpful comments.

Special thanks go to my family for putting up with me during the preparation of this edition.

M.R.

This Page Intentionally Left Blank

1

Introduction

1.1 A BRIEF HISTORY

Reliability, as a human attribute, has been praised for a very long time. For technical systems, however, the reliability concept has not been applied for more than some 60 years. It emerged with a technological meaning just after World War I and was then used in connection with comparing operational safety of one-, two-, and four-engine airplanes. The reliability was measured as the number of accidents per hour of flight time.

At the beginning of the 1930s, Walter Shewhart, Harold F. Dodge, and Harry G. Romig laid down the theoretical basis for utilizing statistical methods in quality control of industrial products. Such methods were, however, not brought into use to any great extent until the beginning of World War II. Products that were composed of a large number of parts often did not function, despite the fact that they were made up of individual high-quality components.

During World War II a group in Germany was working under Wernher von Braun developing the V-1 missile. After the war, it was reported that the first 10 V-1 missiles were all fiascos. In spite of attempts to provide high-quality parts and careful attention to details, all the first missiles either exploded on the launching pad or landed "too soon" (in the English Channel). Robert Lusser, a mathematician, was called in as a consultant. His task was to analyze the missile system, and he quickly derived the *product probability law of series components*. This theorem concerns systems functioning only if all the components are functioning and is valid under special assumptions. It says that the reliability of such a system is equal to the product of the reliabilities of the individual components which make up the system. If the system

comprises a large number of components, the system reliability may therefore be rather low, even though the individual components have high reliabilities.

In the United States, attempts were made to compensate a low system reliability by improving the quality of the individual components. Better raw materials and better designs for the products were demanded. A higher system reliability was obtained, but extensive systematic analysis of the problem was probably not carried out at that time.

After World War II, the development continued throughout the world as increasingly more complicated products were produced, composed of an ever-increasing number of components (television sets, electronic computers, etc.). With automation, the need for complicated control and safety systems also became steadily more pressing.

Toward the end of the 1950s and the beginning of the 1960s, interest in the United States was concentrated on intercontinental ballistic missiles and space research, especially connected to the Mercury and Gemini programs. In the race with the Russians to be the first nation to put men on the moon, it was very important that the launching of a manned spacecraft be a success. An association for engineers working with reliability questions was soon established. The first journal on the subject, IEEE Transactions on reliability came out in 1963, and a number of textbooks on the subject were published in the 1960s.

In the 1970s interest increased, in the United States as well as in other parts of the world, in risk and safety aspects connected to the building and operation of nuclear power plants. In the United States, a large research commission, led by Professor Norman Rasmussen was set up to analyze the problem. The multimillion dollar project resulted in the so-called Rasmussen report, WASH-1400 (NUREG-75/014). Despite its weaknesses, this report represents the first serious safety analysis of so complicated a system as a nuclear power plant.

Similar work has also been carried out in Europe and Asia. In the majority of industries a lot of effort is presently put on the analysis of risk and reliability problems. The same is true in Norway, particularly within the offshore oil industry. The offshore oil and gas development in the North Sea is presently progressing into deeper and more hostile waters, and an increasing number of remotely operated subsea production systems are put into operation. The importance of the reliability of subsea systems is in many respects parallel to the reliability of spacecrafts. A low reliability cannot be compensated by extensive maintenance.

A more detailed history of reliability technology is presented, for example, by Knight (1991), and Villemeur (1988).

1.2 DIFFERENT APPROACHES TO RELIABILITY ANALYSIS

We can distinguish between three main branches of reliability:

- Hardware reliability
- Software reliability

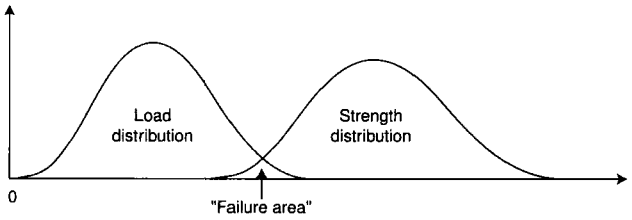

Fig. 1.1 Load and the strength distributions.

- Human reliability

The present textbook is concerned with the first of these branches: the reliability of technical components and systems. Many technical systems will also involve software and humans in many different roles, like designers, operators, and maintenance personnel. The interactions between the technical system, software, and humans are very important, but not a focused topic in this book. Within hardware reliability we may use two different approaches:

- The physical approach
- The actuarial approach

In the *physical approach* the strength of a technical item is modeled as a random variable S. The item is exposed to a load L that is also modeled as a random variable. The distributions of the strength and the load at a specific time t are illustrated in Fig. 1.1. A failure will occur as soon as the load is higher than the strength. The reliability R of the item is defined as the probability that the strength is greater than the load,

$$R = \Pr(S > L)$$

where $\Pr(A)$ denotes the probability of event A.

The load will usually vary with time and may be modeled as a time-dependent variable $L(t)$. The item will deteriorate with time, due to failure mechanisms like corrosion, erosion, and fatigue. The strength of the item will therefore also be a function of time, $S(t)$. A possible realization of $S(t)$ and $L(t)$ is illustrated in Fig. 1.2. The time to failure T of the item is the (shortest) time until $S(t) < L(t)$,

$$T = \min\{t;\, S(t) < L(t)\}$$

and the reliability $R(t)$ of the item may be defined as

$$R(t) = \Pr(T > t)$$

The physical approach is mainly used for reliability analyses of structural elements, like beams and bridges. The approach is therefore often called *structural reliability*

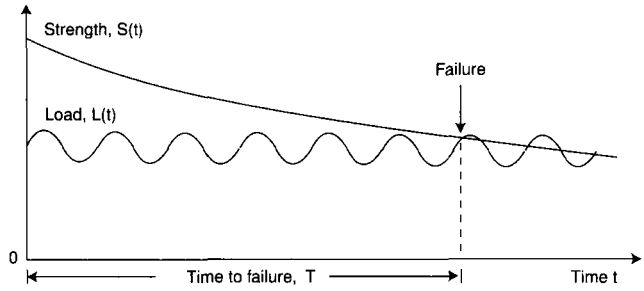

Fig. 1.2 Possible realization of the load and the strength of an item.

analysis (Melchers 1999). A structural element, like a leg on an offshore platform, may be exposed to loads from waves, current, and wind. The loads may come from different directions, and the load must therefore be modeled as a vector $\mathbf{L}(t)$. In the same way, the strength will also depend on the direction and has to be modeled as a vector $\mathbf{S}(t)$. The models and the analysis may therefore become rather complex.

In the *actuarial approach*, we describe all our information about the operating loads and the strength of the component in the probability distribution function $F(t)$ of the time to failure T. No explicit modeling of the loads and the strength is carried out. Reliability characteristics like *failure rate* and *mean time to failure* are deduced directly from the probability distribution function $F(t)$. Various approaches can be used to model the reliability of systems of several components and to include maintenance and replacement of components. When several components are combined into a system, the analysis is called a *system reliability analysis*.

1.3 SCOPE OF THE TEXT

This book provides a thorough introduction to component and system reliability analysis by the actuarial approach. When we talk about reliability and reliability studies, it is tacitly understood that we follow the actuarial approach.

The main objectives of the book are:

1. To present and discuss the terminology and the main models used in reliability studies.

2. To present the analytical methods that are fundamental within reliability engineering and analysis of reliability data.

The methods described in the book are applicable during any phase of a system's lifetime. They have, however, their greatest value during the design phase. During this phase reliability engineering can have the greatest effect for enhancing the system's safety, quality, and operational availability.

Some of the methods described in the book may also be applied during the operational phase of the system. During this phase, the methods will aid in the evaluation of the system and in improving the maintenance and the operating procedures.

The book does not specifically deal with how to build a reliable system. The main topics of the book are connected to how to evaluate, measure, and predict the reliability of a system.

1.4 BASIC CONCEPTS

The main concept of this book is *reliability*. During the preceding sections the concept of reliability has been used without a precise definition. It is, however, very important that all main concepts are defined in an unambiguous way. We fully agree with Kaplan (1990) who states: "When the words are used sloppily, concepts become fuzzy, thinking is muddled, communication is ambiguous, and decisions and actions are suboptimal, to say the least."

A precise definition of reliability and some associated concepts like quality, availability, safety, security, and dependability are given below. All of these concepts are more or less interconnected, and there is a considerable controversy concerning which is the broadest and most general concept. Further concepts are defined in the Glossary at the end of the book.

Until the 1960s reliability was defined as "the probability that an item will perform a required function under stated conditions for a stated period of time." Some authors still prefer this definition, for example, Smith (1997) and Lakner and Anderson (1985). We will, however, in this book use the more general definition of reliability given in standards like ISO 8402 and British Standard BS 4778:

Reliability
The ability of an item to perform a required function, under given environmental and operational conditions and for a stated period of time (ISO 8402).

- The term "item" is used here to denote any component, subsystem, or system that can be considered as an entity.
- A required function may be a single function or a combination of functions that is necessary to provide a specified service.
- All technical items (components, subsystems, systems) are designed to perform one or more (required) functions. Some of these functions are active and some functions are passive. Containment of fluid in a pipeline is an example of a passive function. Complex systems (e.g., an automobile) usually have a wide range of required functions. To assess the reliability (e.g., of an automobile), we must first specify the required function(s) we are considering.
- For a hardware item to be reliable, it must do more than meet an initial factory performance or quality specification—it must operate satisfactorily for a specified period of time in the actual application for which it is intended.

Remark: The North American Electric Reliability Council (NERC) has introduced a more comprehensive definition of the reliability of an electric system. NERC defines the reliability of an electric systems in terms of two basic functional aspects:

1. *Adequacy*. The ability of the electric system to supply the aggregate electrical demand and energy requirements of customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements.

2. *Security*. The ability of the electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system elements. □

Quality
The totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs (ISO 8402).

- Quality is also sometimes defined as conformance to specifications (e.g., see Smith 1997).

- The quality of a product is characterized not only by its conformity to specifications at the time it is supplied to the user, but also by its ability to meet these specifications over its entire lifetime.

However, according to common usage, quality denotes the conformity of the product to its specification as manufactured, while reliability denotes its ability to continue to comply with its specification over its useful life. *Reliability is therefore an extension of quality into the time domain.*

Remark: In common language we often talk about the *reliability and quality* of a product. Some automobile journals publish regular surveys of reliability and quality problems of the various cars. Under reliability problems they list problems related to the essential functions of the car. A reliability problem is present when the car cannot be used for transport. Quality problems are secondary problems that may be considered a nuisance. □

Availability
The ability of an item (under combined aspects of its reliability, maintainability and maintenance support) to perform its required function at a stated instant of time or over a stated period of time (BS 4778).

- We may distinguish between the availability $A(t)$ at time t and the average availability A_{av}. The availability at time t is

$$A(t) = \Pr(\text{item is functioning at time } t)$$

The term "functioning" means here that the item is either in active operation or that it is able to operate if required.

The average availability A_{av} denotes the mean proportion of time the item is functioning. If we have an item that is repaired to an "as good as new" condition

every time it fails, the average availability is

$$A_{av} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \tag{1.1}$$

where MTTF (mean time to failure) denotes the mean functioning time of the item, and MTTR (mean time to repair) denotes the mean downtime after a failure. Sometimes MDT (mean downtime) is used instead of MTTR to make it clear that it is the total mean downtime that should be used in (1.1) and not only the mean active repair time.

- When considering a production system, the average availability of the production (i.e., the mean proportion of time the system is producing) is sometimes called the *production regularity*.

Maintainability
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 (BS4778).

- "Maintainability" is a main factor determining the availability of the item.
- RAM is often used as an acronym for reliability, availability, and maintainability. We also use the notions RAM studies and RAM engineering.

Safety
Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property (MIL-STD-882D).

- This definition has caused considerable controversy. A number of alternative definitions have therefore been proposed. The main controversy is connected to the term "freedom from." Most activities involve some sort of risk and are never totally *free* from risk. In most of the alternative definitions safety is defined as an *acceptable level of risk.*
- The concept *safety* is mainly used related to random hazards, while the concept *security* is used related to deliberate actions.

Security
Dependability with respect to prevention of deliberate hostile actions.

- Security is often used in relation to information and computer systems. In this context, security may be defined as "dependability with respect to prevention of unauthorized access to and/or handling of information" (Laprie 1992).
- The security of critical infrastructures is thoroughly discussed in CCIP (1997)

Dependability
The collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance (IEC60300).

- A slightly different definition is given by Laprie (1992). He defines dependability to be: "Trustworthiness of a system such that reliance can justifiably be placed on the service it delivers." In comments to this definition, Laprie (1992) claims that dependability is a global concept which subsumes the attributes of reliability, availability, safety, and security. This is also in accordance with the definition used by Villemeur (1988).

- If safety and security are included in the definition of dependability as influencing factors, dependability will be identical to the RAMS concept (RAMS is an acronym for reliability, availability, maintainability, and safety).

- According to Laprie (1992) the definition of dependability is synonymous to the definition of reliability. Some authors, however, prefer to use the concept of dependability instead of reliability. This is also reflected in the important series of standards IEC 60300 "Dependability Management."

In this book we will use reliability as a global, or general, concept with the same main attributes as listed under the definition of dependability.

The reliability may be measured in different ways depending on the particular situation, for example as:

1. Mean time to failure (MTTF)

2. Number of failures per time unit (*failure rate*)

3. The probability that the item does not fail in a time interval $(0, t]$ (*survival probability*)

4. The probability that the item is able to function at time t (*availability at time t*)

If the item is not repaired after failure, 3 and 4 coincide. All these measures are given a mathematically precise definition in Chapter 2 with concepts from probability theory.

1.5 APPLICATION AREAS

The main objective of a reliability study should always be to provide information as a basis for decisions. Before a reliability study is initiated, the decision maker should clarify the decision problem, and then the objectives and the boundary conditions and limitations for the study should be specified such that the relevant information needed as input to the decision is at hand, in the right format, and on time.

Reliability technology has a potentially wide range of application areas. Some of these areas are listed below to illustrate the wide scope of application of reliability technology.

1. *Risk analysis.* The main steps of a quantitative risk analysis (QRA) are, as illustrated in Fig. 1.3: