1

Introduction

1.1 What is Reliability?

Nowadays, nearly all of us depend on a wide range of technical products and services in our everyday life. We expect our electrical appliances, cars, computers, mobile phones, and so on, to function when we need them, and to be reliable for a rather long time. We expect services, such as electricity, computer networks, and transport, to be supplied without disruptions or delays. When a product, machinery, or service fails, the consequences may sometimes be catastrophic. More often, product flaws and service outages lead to customer dissatisfaction and expenses for the supplier through warranty costs and product recalls. For many suppliers, reliability has become *a matter of survival*.

There is no generally accepted definition of the *reliability* of a technical product. The definition and interpretation of the term vary from industry to industry and from user to user. For the purpose of this book, we choose a rather wide definition of the reliability of a technical item.

Definition 1.1 (Reliability)
The ability of an item to perform as required in a stated operating context and for a stated period of time. □

The term *item* is used to designate any technical system, subsystem, or component. The items studied in this book are built of hardware parts, and to an increasing degree, of software. When relevant, the user interface is part of the item, but operators and other humans are not part of the items studied here.

The reliability concept is illustrated in Figure 1.1. The *required performance* is determined by laws and regulations, standards, customer requirements and expectations, and supplier requirements, and is usually stated in a *specification document*, where delimitations of the operating context are stated. As long as

System Reliability Theory: Models, Statistical Methods, and Applications, Third Edition.
Marvin Rausand, Anne Barros, and Arnljot Høyland.

Companion Website: www.wiley.com/go/SystemReliabilityTheory3e

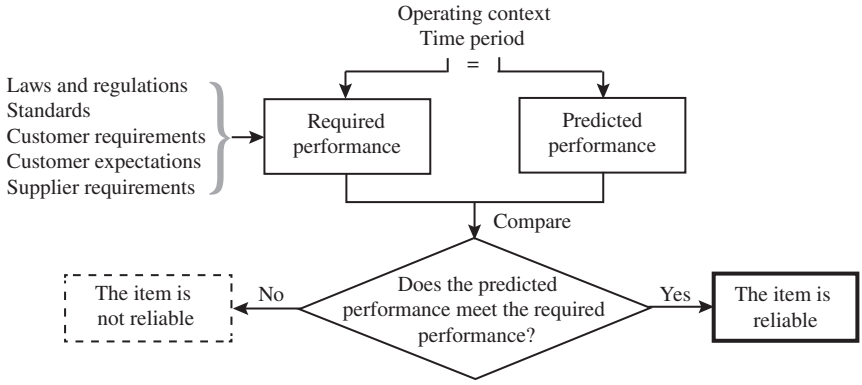


Figure 1.1 The reliability concept.

the predicted performance at least fulfills the required performance, the item is reliable – when it is used in the same operating context and for the period of time stated in the required performance.

By *operating context*, we mean the environmental conditions the item is used in, the usage patterns, and the loads it is subjected to, and how the item is serviced and maintained.

Definition 1.1 is not new and is not created by us. Several authors and organizations have used this, or a very similar definition of reliability, at least since the 1980s. A more thorough discussion of reliability and related concepts is given in Section 1.3.

1.1.1 Service Reliability

A *service* is provided by a person, an organization, or a technical item to a person or a technical item. The entity providing the service is called a *service provider*, and the entity receiving the service is called a *customer*. Services can be provided on a (i) continuous basis (e.g. electric power, computer networks), (ii) according to a timetable (e.g. bus, rail, and air transport), or (iii) on demand (e.g. payment by debit cards).

Many services are provided by a single service provider to a high number of customers. A customer considers the service to be reliable when she receives the service (e.g. electric power) with sufficient quality without outages. We define service reliability as follows:

Definition 1.2 (Service reliability)
The ability of the service to meet its supply function with the required quality under stated conditions for a specified period of time. □

Several quantitative service reliability metrics have been defined, but they vary between the different types of services.

1.1.2 Past and Future Reliability

In our daily language, the term "reliability" is used to describe both past and future behavior. We may, for example, say that (i) "my previous car was very reliable" and (ii) "I believe that my new car will be very reliable." These two statements are quite different. The first statement is based on experience with the car over a certain period, whereas the second statement is a *prediction* of what will happen in the future. We distinguish them by using two different terms.

Reliability (single word) is always used to describe the *future* performance of an item. Because we cannot predict the future with certainty, we need to use probabilistic statements when assessing the reliability.

Achieved reliability is used to describe the item's *past* performance, which is assumed to be known to the analyst. No probabilistic statements are therefore involved. The achieved reliability is also called *observed reliability*.

The focus of this book is on reliability and the future performance. The achieved reliability is most relevant in Chapter 14, where analysis of observed failure data is discussed.

1.2 The Importance of Reliability

Several producers of technical items have struggled and even collapsed because of item flaws and failures. To build a reputation for reliability is a long-term project, but it may take a short time to lose this reputation. The main drivers for high reliability are listed in Figure 1.2. Over the years, the reliability has improved for

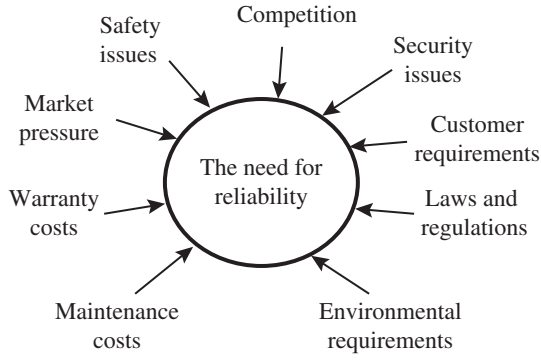


Figure 1.2 Main drivers for high reliability.

almost all types of items, but at the same time, customers expect a higher and higher reliability of the new items they buy. Current customers further expect that possible failures in the warranty period are rectified without any cost to the customer. To be attractive in the market, the suppliers have to offer a longer and longer warranty period.

If items have flaws that affect safety, safety regulations may require all the flawed items to be recalled for repair or modification. Such recalls are rather frequent in the car industry, but are also common in many other industries. In addition to excessive warranty costs and item recalls, flawed items lead to dissatisfied and nonreturning customers.

1.2.1 Related Applications

Reliability considerations and reliability studies are important inputs to a number of related applications. Several of these applications have adopted the basic terminology from reliability. Among the relevant applications are:

Risk analysis. The main steps of a *quantitative risk analysis* (QRA) are: (i) identification and description of potential *initiating events* that may lead to unwanted consequences, (ii) identification of the main causes of each initiating event and quantification of the frequency of the initiating events, and (iii) identification of the potential consequences of the initiating events and quantification of the probabilities of each consequence. The three steps are shown in the *bow-tie model* in Figure 1.3, where the main methods are indicated. The methods that are covered in this book are marked with an $*$.

Maintenance planning. Maintenance and reliability are closely interlinked. High-quality maintenance improves the operational reliability and high reliability gives few failures and low maintenance cost. The close link is also visible in the popular approach *reliability-centered maintenance* (RCM), which is discussed in Chapter 9.

Quality. Quality management is increasingly focused, stimulated by the ISO 9000 series of standards. The concepts of quality and reliability are closely connected. Reliability may in some respects be considered to be a quality characteristic.

Life cycle costing. The life cycle cost (LCC) may be split into three types: (i) capital expenditure (CAPEX), (ii) operational expenditure (OPEX), and (iii) risk expenditure (RISKEX). The main links to reliability are with types (ii) and (iii). The OPEX is influenced by how regular the function/service is and the cost of maintenance. The RISKEX covers the cost related to accidents, system failures, and insurance. LCC is also called *total ownership cost*.

Production assurance. Failures in a production system lead to downtime and reduced production. To assure a regular production, the production system

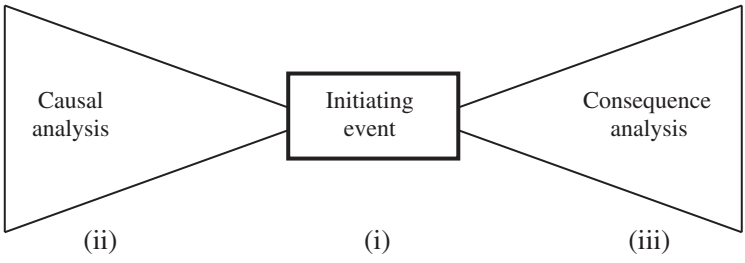
must have a high reliability. Production assurance is treated in the international standard ISO 20815 and discussed in Chapter 6.

Warranty planning. A warranty is a formal commitment to deliver reliable items. If failures and malfunctions are detected during a specified *warranty period*, the supplier has to repair and/or compensate the failure. Unreliable items may incur a high cost for the supplier.

Systems engineering. Reliability is one of the most important quality attributes of many technical systems. Reliability assurance is therefore an important topic during the systems engineering process. This is especially the case within the nuclear power, the aviation, the aerospace, the car, and the process industries.

Environmental protection. Reliability studies are used to improve the design and operational availability of many types of environmental protection systems. Many industries have realized that a main part of the pollution from their plants is caused by production irregularities and that consequently the reliability of the plant is an important factor in order to reduce pollution. Environmental risk analyses are carried out according to the procedure shown in Figure 1.3.

Technology qualification. Many customers require the producer of technical items to verify that the item satisfies the agreed requirements. The verification is carried out by following a *technology qualification program* (TQP) based on



Methods		
– Fault tree analysis*	– Checklists	– Event tree analysis*
– Reliability block diagrams*	– Preliminary hazard analysis	– Consequence models
– Bayesian networks*	– FMECA*	– Reliability assessment*
– FMECA*	– HAZOP	– Evacuation models
		– Simulation
– Reliability data sources*	– Event data sources	

Figure 1.3 Main steps of risk analysis, with main methods. The methods covered in this book are marked with ∗.

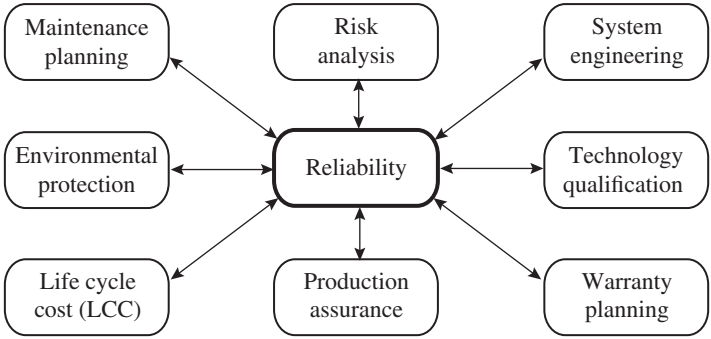


Figure 1.4 Reliability as basis of other applications.

analysis and testing. This is especially the case within the aerospace, defense, and petroleum industries (e.g. see DNV-RP-A203 2011).

Applications related to reliability are illustrated in Figure 1.4.

1.3 Basic Reliability Concepts

The main concept of this book is *reliability* as defined in Definition 1.1. The aim of this section is to discuss and clarify this definition and to define related terms, such as maintainability and maintenance, availability, quality, and dependability.

It is important that all main words 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."

1.3.1 Reliability

Definition 1.1 says that reliability expresses "the ability of an item to perform as required in a stated operating context and for a stated period of time." We start by clarifying the main words in this definition.

(1) Reliability is defined by using the word *ability*, which is not directly measurable. A quantitative evaluation of the item's ability to perform must therefore be based on one or more metrics, called *reliability metrics*. Several probabilistic reliability metrics are defined and discussed in Section 1.4.
(2) Some authors use the word *capability* instead of *ability* in the definition of reliability and claim that the term "capability" is more embracing, covering both ability and capacity. Most dictionaries list ability and capability as synonyms. We prefer the word "ability" because this is the word most commonly used.

(3) The statement *perform as required* means that the item must be able to perform one or more specified functions according to the performance criteria for these function(s). Functions and performance criteria are discussed in Section 2.5.
(4) Many items can perform a high number of functions. To assess the reliability (e.g. of a car), we must specify the required function(s) that are considered.
(5) To be reliable, the item 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 operating context.
(6) The stated period of time may be a delimited time period, such as a mission time, the time of ownership, and several more.
(7) The time may be measured by many different time concepts, such as calendar time, time in operation, number of work cycles, and so on. For vehicles, the time is often measured as the number of kilometers driven. For items that are not operated continuously in the same mode, a more complicated time concept may be needed.

Inherent and Actual Reliability

It may be useful to qualify the reliability of an item by adding a word, such as inherent or actual. The inherent reliability is defined as follows:

Definition 1.3 (Inherent reliability)
The reliability of the item as designed and manufactured, which excludes effects of operation, environment, and support conditions other than those assumed and stated in the item requirements and specification. □

The inherent reliability is therefore the reliability of a brand new item that will be used and maintained exactly according to the conditions described in the item specification document or implicitly assumed. The inherent reliability is sometimes called *built reliability* or *built-in reliability* of the item.

The design and development team always attempts to adapt the item to the actual operating context, but it is difficult, if not impossible, to account for all the aspects in practical use. The actual reliability may consequently be different from the inherent reliability that was determined before the item was put into use. The actual reliability of an item is defined as follows:

Definition 1.4 (Actual reliability)
The reliability of the item in an actual operating context. □

The actual reliability is sometimes called *operational reliability* or *functional reliability*.

Software Reliability
Software reliability is different from hardware reliability. Hardware items generally deteriorate due to wear or other mechanisms and failures occur as a random process. Software, on the other hand, does not deteriorate and faults or *bugs* remain dormant and undetected until the software is modified or a specific condition or trigger activates the bug – leading to item failure. Software bugs are manifestations of mistakes done in specification, design, and/or implementation. Reliability analysis of a software program is done by checking the code syntax according to specific rules and by testing (debugging) the software for a variety of input data. This process is not discussed further in this book. Interested readers may consult ISO 25010.

1.3.2 Maintainability and Maintenance

Many items have to be maintained to perform as required. Two different concepts are important, maintainability, and maintenance. *Maintainability* is a design feature of the item and indicates how easy it is to get access to the parts that are to be maintained and how fast a specific maintenance task can be done. *Maintenance* describes the actual work that is done to maintain an item. Maintainability is defined as follows:

Definition 1.5 (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 as required, when maintenance is performed under stated conditions and using prescribed procedures and resources. □

Maintainability is further discussed in Chapter 9. Maintenance is defined as follows:

Definition 1.6 (Maintenance)
The combination of all technical and management actions during the life cycle of an item intended to retain the item in, or restore it to, a state in which it can perform as required (IEV 192-06-01). □

Hardware maintenance is discussed in more detail in Chapters 9 and 12. Software maintenance is not treated in this book.

1.3.3 Availability

Availability measures the degree to which an item is able to operate at some future time t or during a future time interval (t_1, t_2), and is in this book regarded

as a reliability metric. The availability of an item depends on the reliability, recoverability, and maintainability of the item, and also on the maintenance support performance. Recoverability is the item's ability to recover from a failure, without repair. Maintenance support is the resources that are available for maintenance, such as workshops, qualified personnel, and tools. Availability is discussed in Chapters 6, 11, and 13.

1.3.4 Quality

The term "quality" is closely related to reliability and is defined as follows:

Definition 1.7 (Quality)
The totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs. □

Quality is sometimes defined as *conformity to specifications* and a quality defect is referred to as a nonconformity. According to common usage, quality denotes the conformity of the item to its specification as manufactured, whereas reliability denotes its ability to continue to comply with its specification over its useful life. With this interpretation, reliability may be considered as an extension of quality into the time domain.

1.3.5 Dependability

Dependability is a more recent concept that embraces the concepts of reliability, maintainability, and availability, and in some cases also safety and security. Dependability has, especially, become known through the important series of standards IEC 60300 "Dependability management." The IEV defines dependability as follows:

Definition 1.8 (Dependability)
The ability (of an item) to perform as and when required (IEV 192-01-01). □

Another commonly used definition is "Trustworthiness of a system such that reliance can justifiably be placed on the service it delivers" (Laprie 1992).

Remark 1.1 (Translating the word "dependability")
Many languages, such as Norwegian and Chinese, do not have words that can distinguish reliability and dependability, and reliability and dependability are therefore translated to the same word. □

1.3.6 Safety and Security

General safety is outside the scope of this book, and we deal only with the safety aspects of a specified technical item and define safety as follows:

Definition 1.9 (Safety)
Freedom from unacceptable risk caused by the technical item. □

This definition is a rephrasing of definition IEV 351-57-05. The concept *safety* is mainly used related to random hazards, whereas the concept *security* is used related to deliberate hostile actions. We define security as:

Definition 1.10 (Security)
Dependability with respect to prevention of deliberate hostile actions. □

The deliberate hostile action can be a physical attack (e.g. arson, sabotage, and theft) or a cyberattack. The generic categories of attacks are called *threats* and the entity using a threat is called a *threat actor*, a *threat agent*, or an *adversary*. Arson is therefore a threat, and an arsonist is a threat actor. The threat actor may be a disgruntled employee, a single criminal, a competitor, a group, or even a country. When a threat actor attacks, he seeks to exploit some weaknesses of the item. Such a weakness is called a *vulnerability* of the item.

Remark 1.2 (Natural threats)
The word "threat" is also used for natural events, such as avalanche, earthquake, flooding, landslide, lightning, tsunami, and volcano eruption. We may, for example, say that earthquake is a threat to our item. Threat actors are not involved for this type of threats. □

1.3.7 RAM and RAMS

RAM, as an acronym for reliability, availability, and maintainability, is often used, for example, in the annual RAM Symposium.[1] RAM is sometimes extended to RAMS where S is added to denote safety and/or security. The RAMS acronym is, for example, used in the railway standard IEC 62278.

Remark 1.3 (Broad interpretation of reliability)
In this book, the term "reliability" is used quite broadly, rather similar to RAM as defined above. The same interpretation is used by Birolini (2014). □

1 RAM Symposium: www.rams.org.

1.4 Reliability Metrics

Throughout this book, it is assumed that the time-to-failure and the repair time of an item are *random variables* with *probability distributions* that describe the future behavior of the item. The future behavior may be evaluated based on one or more *reliability metrics*. A reliability metric is a "quantity" that is derived from the reliability model and is, as such, not directly measurable. When performance data become available, we may estimate or predict quantitative values for each reliability metric.

A single reliability metric is not able to tell the whole truth. Sometimes, we need to use several reliability metrics to get a sufficiently clear picture of how reliable an item is.

1.4.1 Reliability Metrics for a Technical Item

Common reliability metrics for an item include

(1) The mean time-to-failure (MTTF)
(2) The number of failures per time unit (*failure frequency*)
(3) The probability that the item does not fail in a time interval $(0, t]$ (*survivor probability*)
(4) The probability that the item is able to function at time t (*availability at time t*)

These and several other reliability metrics are given a mathematical precise definition in Chapter 5, and are discussed and exemplified in all the subsequent chapters.

Example 1.1 (Average availability and downtime)
Consider the electricity supply, which is supposed to be available at any time. The achieved average availability A_{av} of the supply is quantified as

$$A_{\text{av}} = \frac{\text{Uptime}}{\text{Total time}} = 1 - \frac{\text{Downtime}}{\text{Total time}}$$

If we consider a period of one year, the *total time* is approximately 8760 hours. The *downtime* is the time, during the specified time period, the service is not available. The relationship between the average availability and the length of the downtime is illustrated in Table 1.1. □

Table 1.1 Availability and downtime.

90	36.5 d
99	3.65 d
99.9	8.76 h
99.99	52 min
99.999	5 min

1.4.2 Reliability Metrics for a Service

A wide range of service reliability metrics have been defined, but these vary significantly between the application areas. The most detailed metrics are available for electric power supply (e.g. see IEEE Std. 1366 2012).

Example 1.2 (Airline reliability and availability)
Airline passengers are mainly concerned about whether the journey will be safe and whether the aircraft will take off and land on the scheduled times. The second concern is, by airlines, expressed by the *dispatch reliability*, which is defined as the probability that a scheduled departure takes place within a specified time after the scheduled departure time. Many airlines use a 15-minutes margin between actual and scheduled departure time for a flight to be considered as having departed on time. The achieved dispatch reliability indicator for a (past) period is reported as the percentage of all departures that departed on time.

$$\text{Dispatch reliability} = \frac{\text{No. of departures on time}}{\text{No. of departures + cancelations}}$$

For technical items, the airlines are mainly using the reliability metrics listed in Section 1.4.1 □

1.5 Approaches to Reliability Analysis

Three main branches of reliability can be distinguished:

- Hardware reliability
- Software reliability
- Human reliability

The present book is concerned with hardware items (existing or in design) that may or may not have embedded software. Within hardware reliability, two different approaches may be used: the *physical approach* and/or the *systems approach*.

1.5.1 The Physical Approach to Reliability

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 shown in Figure 1.5. A failure will occur as soon as the load is higher than the strength. The survival probability R of the item is defined as the probability that the strength is greater than the load,

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

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

The load may vary with time and be modeled as a time-dependent variable $L(t)$. The item may deteriorate with time, due to failure mechanisms, such as, 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 shown in Figure 1.6. 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 survivor probability $R(t)$ of the item may be defined as

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

The physical approach is mainly used for reliability analyses of structural elements, such as beams and bridges. The approach is therefore often called *structural reliability analysis* (Melchers 1999). A structural element, such as 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 $\boldsymbol{L}(t)$. In the same way, the strength will also depend on the direction and has to be modeled as a vector $\boldsymbol{S}(t)$. The models and the analysis therefore become complicated. The physical approach is not pursued further in this book.

1.5.2 Systems Approach to Reliability

By the systems approach, all our information about the operational loads and the strength of an item is incorporated in its probability distribution function

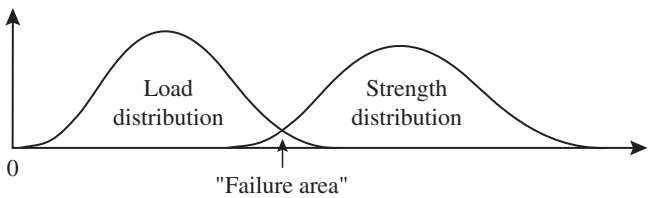


Figure 1.5 Load and the strength distributions at a specified time t.

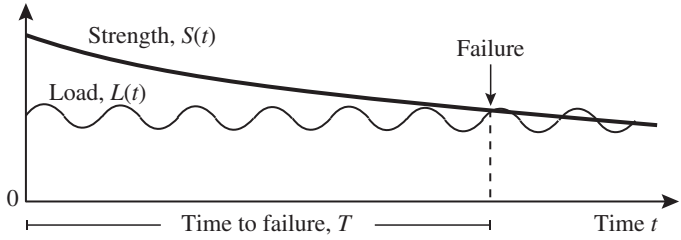


Figure 1.6 Possible realization of the load and the strength of an item.

$F(t)$ of the *time-to-failure* T. No explicit modeling of the loads and the strength is carried out. Reliability metrics, such as the *survivor probability* and the *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*.

Quantitative results are based on information about the reliability of the components. Such information comes from statistical data on past experience with the same or similar components, laboratory testing, or from expert judgments. This approach has similarities to actuarial assessments, and the systems approach to reliability is, therefore, sometimes referred to as an *actuarial approach*. This book is concerned with the systems approach to reliability.

System Models

In reliability studies of technical systems, we always have to work with models of the systems. These models may be graphical (networks of different types) or mathematical. A mathematical model is necessary in order to be able to bring in data and use mathematical and statistical methods to estimate reliability parameters. For such models, two conflicting interests always apply:

(1) The model should be sufficiently simple to be handled by available mathematical and statistical methods.
(2) The model should be sufficiently "realistic" such that the deducted results are of practical relevance.

We should always bear in mind that we are working with an idealized, simplified model of the system. Furthermore, the results we derive are, strictly speaking, valid only for the model, and are accordingly only "correct" to the extent that the model is realistic.

The modeling situation is illustrated in Figure 1.7. Before we start developing a model, we should clearly understand what type of decision the results from

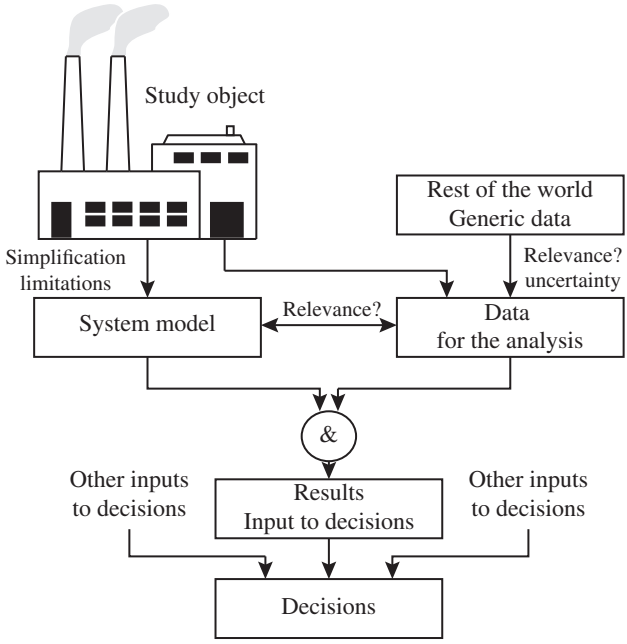


Figure 1.7 The system reliability analysis process.

our analysis should provide input to, and also the required format of the input to the decision. To estimate the system reliability from a model, we need input data. The data will usually come from generic data sources, as discussed in Chapter 16. The generic data may not be fully relevant for our system and may have to be adjusted by expert judgment. This is especially the case when we are introducing new technology. Some data may also come from the specific system. When establishing the system model, we have to consider the type, amount, and quality of the available input data. It has limited value to establish a very detailed model of the system if we cannot find the required input data.

1.6 Reliability Engineering

Engineering deals with the design, building, and use of technical items. *Reliability engineering* is an engineering discipline that provides support to the engineering process. To be successful, reliability engineering must be integrated in the engineering process and the reliability engineer(s) must take full part in the engineering team.

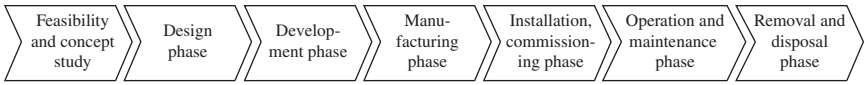


Figure 1.8 The phases of a system development project (example).

An item development project is split into a number of phases. The number and the title of these phases vary from industry to industry and also between companies in the same industry. A typical set of phases is shown in Figure 1.8.

The phases in Figure 1.8 are arranged as a time axis, but iterations are usually required, for example, to make a redesign after a defect has been revealed in a later phase. Each phase is usually divided into stages, and many manufacturers have procedures describing in detail which reliability analyses to carry out in each stage together with procedures for the data flow.

Reliability engineering has its most important role in the three first phases in Figure 1.8, but should be integrated in all phases.

1.6.1 Roles of the Reliability Engineer

The objective of reliability engineering is to identify, analyze, and mitigate failures and operational problems during all phases of an item's life cycle. The reliability engineer has an important role in all these phases. Below, the roles of the reliability engineer are listed briefly in the design and development phases and in the operational phase.

Roles in Design and Development

A reliability engineer has her most important role in the specification, design, and development phases of a new item. In these phases, the reliability engineer helps the development team to

(1) Identify potential failures of suggested component and module concepts such that failures may be designed out.
(2) Quantify the reliability of suggested system concepts.
(3) Provide input to decisions about modularization, stacking, and system layout.
(4) Make tradeoffs between factors such as cost, functions, performance, reliability, time to market, safety, and security.
(5) Identify weaknesses of the system design such that they can be corrected before the system goes to manufacturing or to the customers.
(6) Clarify benefits and drawbacks related to redundancy of components and modules.
(7) Identify causes and effects of possible failure modes.

(8) Compare the LCC of design alternatives.
(9) Evaluate the cost of suggested warranty policies.
(10) Calculate the reliability of system options as input to choice between these.
(11) Plan and perform reliability acceptance or qualification testing (e.g. in a TQP framework).

Roles in Normal Operation

The main role of the reliability engineer in normal operation is to track items causing abnormally high maintenance cost and production losses or service outages, then find ways to reduce these losses or high costs. The role of a reliability engineer may vary from company to company, but the overall goal is always the same: reduce maintenance costs as much as possible without interrupting system operation.

Another main role of the reliability engineer in this phase is to collect, analyze, and present reliability data. This topic is treated in detail in Chapter 14.

Reliability has to be designed and manufactured into an item. It is too late and too costly to wait until the item is produced. Reliability considerations must be integrated into all steps of the development process. This book presents the main theory and many of the required methods and tools for reliability engineering, but reliability engineering also requires a number of methods that are outside the scope of this book. When to carry out an analysis, which data are available at this stage, and how to update and use the results are central questions in reliability engineering that are not covered in this book.

1.6.2 Timing of Reliability Studies

Reliability studies are carried out to provide input to *decision-making* related to an item. The objectives and the scope of the reliability study are dependent on the type of decision to be made. Before starting a reliability study, it is essential to have a clear understanding of the decision and the data needed as input to the decision-making. A reliability study to provide input to decisions on warranties may, for example, be quite different from a reliability study to provide input to decisions on safety barriers in a risk assessment.

It is very important that the reliability studies are planned and executed such that the required results are available before the decision-making takes place!

1.7 Objectives, Scope, and Delimitations of the Book

The overall objective of this book is to give a thorough introduction to component and system reliability analysis by the system reliability approach. More detailed objectives are

(1) To present and discuss the terminology and the main models used in system reliability studies.
(2) To present the main analytical methods used in reliability engineering and management.
(3) To present and discuss basic theory of maintenance and preventive maintenance modeling and illustrate how these can be applied.
(4) To present the main theory and a selection of methods for reliability data analysis, which is also called *survival analysis*.
(5) To give an introduction to Bayesian probability and Bayesian data analysis.

The book does not specifically deal with how to engineer and manage a reliable system. The main topics of the book are connected to how to define and quantify reliability metrics and to predict the reliability of a system. Our aim is that the book will be a valuable source as follows:

(a) A textbook for system reliability courses at university level.
(b) A handbook for reliability engineers in industry and consulting companies.
(c) A reference book for scientists and engineers in related disciplines.

The following delimitations apply:

- The study object is built of hardware parts based on mechanical, electrical, or electronic technology, and may or may not have embedded software and communication to/from the outside. In most cases, the study object has a human/operator interface. Operators and third-party personnel are outside the scope of the book. This means that human reliability, as such, is not covered. The prime focus of the book is on hardware items.
- The reliability of purely software items is outside the scope of this book.
- Structural reliability issues are not covered in this book.
- The focus of the book is on components and rather simple systems. The theory and methods presented may also be useful for analyzing complex systems, but we have to realize that they may not be sufficient.
- Failures caused by deliberate hostile actions is covered rather rudimentarily.
- In the main part of the book, we assume that each item can have only two states, functioning or failed. Multistate reliability is not covered properly.
- A general introduction to maintenance is not provided. The presentation is delimited to aspects of maintenance that are directly relevant for system reliability.
- The book provides a thorough introduction to system reliability analysis, but does not cover reliability engineering and reliability management in a sufficient way.

1.8 Trends and Challenges

System reliability has been around since the 1940s. The relevance of reliability has increased steadily and we clearly see trends and challenges that will increase the relevance in the years to come. In this section, we briefly mention some of these trends and challenges. An overall trend is that customers expect new items to be BETTER, FASTER, and CHEAPER than the items they replace. More specific challenges include

(1) Items get more and more complicated with a lot of embedded software. Hardware functions are replaced with software-based functions. Because the software-based functions are relatively cheap, many items are loaded with "nice-to-have" function that may also fail.
(2) Most producers meet fierce international competition. To survive, this requires reduced development costs, shorter time to market, and less time spent on analyses and testing. New items have to be sufficiently reliable in the first concept version.
(3) Customers require more and more of the items they purchase, related to functions, quality, and reliability. The requirements are often changing rapidly. Factors influencing item requirements are shown in Figure 1.9.
(4) There is an increasing focus on safety and environmental friendliness and an increasing risk of item call-back if the items should have safety-related defects.
(5) New items are increasingly made up of elements from a variety of subcontractors from many different countries, making it difficult for the main producer to verify the item reliability.

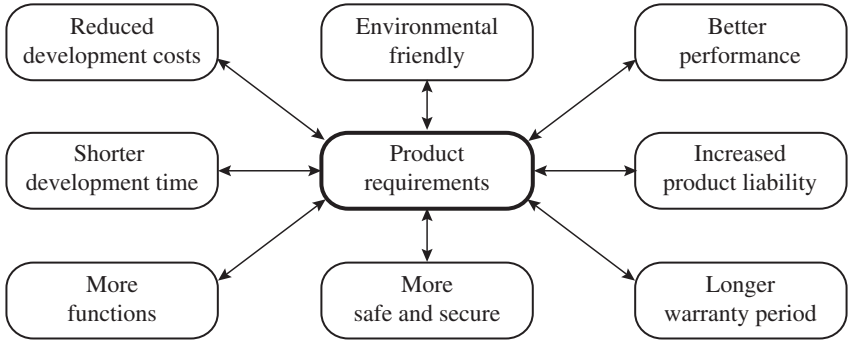


Figure 1.9 Factors that influence item requirements.

(6) For some items, high-speed operation reduces the tolerance of deviations and increases the consequences of failures, should they happen.
(7) There is an increasing focus on warranty. Companies have disappeared because of excessive warranty costs.
(8) An increasing number of items are now connected to a cybernetwork and are vulnerable to cyberattacks. Current challenges are related to the rapid developments of smart homes, smart cities, smart transport systems, the Internet of Things (IoT), cyber-physical systems, systems of systems, and Industry 4.0. Within few years, we expect to see many more new initiatives of similar nature. This will make reliability analyses even more challenging.

1.9 Standards and Guidelines

A range of standards and guidelines stating requirements to reliability and safety have been issued. Any reliability engineer needs to be familiar with the standards and guidelines that are applicable within her subject areas.

1.10 History of System Reliability

This section highlights some achievements in the history of system reliability starting from the 1930s. We realize that our presentation is biased because we put too much focus on activities in Europe and in the United States. In addition, we have included mainly events and books that have influenced our own learning and understanding of system reliability. The development of reliability theory has been strongly influenced by a series of accidents and catastrophic failures. Some of these are mentioned, but you may find that we have missed many important accidents.

Some of the achievements mentioned in this section may be difficult to comprehend fully at this stage, and it may therefore be wise to postpone the reading of this section until you have delved deeper into the subject.

1930s

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, but such methods were not used to any great extent until the beginning of World War II. Products that were composed of a large number of parts often failed, despite the fact that they were made of individual high-quality components.

An important achievement was made in the 1930s by the Swedish professor *Waloddi Weibull* (1887–1979) during his studies of the strength of materials. In Weibull (1939), he laid the basis for one of the most important probability distributions in reliability theory, the *Weibull distribution* (Weibull 1951).

1940s

It is often claimed that the first quantitative system reliability assessment can be attributed to *Robert Lusser* (1899–1969). He was a German engineer and aircraft designer who took part in several well-known Messerschmitt and Heinkel designs during World War II. During the war, a group in Germany was working under Wernher von Braun developing the V-1 missile, but the 10 first 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 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* saying that the reliability of series system is equal to the product of the reliabilities of the individual components that make up the system. If the system comprises a large number of components, the system reliability may therefore be low, even though the individual components have high reliabilities. A young mathematician, *Erich Pieruschka*, assisted Wernher von Braun and may have been as important as Lusser in developing Lusser's law. Some authors prefer to refer to Pieruschka's law instead of Lusser's law.

An important contribution to the subsequent reliability theory was made by the Russian mathematician *Boris V. Gnedenko* (1912–1995) in his 1943 paper "On the limiting distribution of the maximum term in a random series."[2] In this paper, Gnedenko provided rigorous proofs and formulated three classes of limit distributions, one of which was the Weibull distribution. Gnedenko was not the first to define the three limit distribution classes, but the first to provide proofs. The classes had earlier been defined by Fisher and Tippett (1928). The extreme value theorem proved by Gnedenko is often referred to as the Fisher–Tippett–Gnedenko theorem.

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-

2 For a discussion of Gnedenko's contribution, see Smith (1992).

increasing number of components (e.g. television sets and electronic computers). With automation, the need for complicated control and safety systems also became steadily more pressing.

Several attempts to test and quantify the reliability of electronic components began in the 1940s during World War II. The war activities clearly revealed that electron (vacuum) tubes were the most failure-prone components in electronic systems (Denson 1998). Several groups tried to identify ways to improve the reliability of electronic systems, and it was suggested that the reliability of the components needed to be verified by testing before full-scale production.

In 1945, *Milton A. Miner* formulated the important Miner's rule for fatigue failures (Miner 1945). A similar rule was suggested by the Swedish engineer *Nils Arvid Palmgren* (1890–1971) already in 1924 while studying the life length of roller bearings. The rule is therefore also called the Palmgren–Miner's rule and the Miner–Palmgren's rule.

In 1949, the Institute of Electrical and Electronic Engineers (IEEE) formed a professional group on quality control as part of its Institute of Radio Engineers. The group got more and more focused on reliability issues and changed name several times. In 1979, the group got its current name, *IEEE Reliability Society*.

The first guideline on failure modes and effects analysis (FMEA) was issued in 1949 (MIL-P-1629 1949). This guideline was later developed into the military standard MIL-STD-1629A.

1950s

The Advisory Group on Reliability of Electronic Equipment (AGREE) was established in 1950 to survey the field and identify and promote actions that could provide more reliable electronic equipment. A big step forward was made by the report AGREE (1957).

The 1950s saw much pioneering work in the reliability discipline. The Weibull distribution was properly defined (Weibull 1951) and soon became popular and several US military handbooks were issued. The statistical branch of reliability theory was strongly enhanced by the paper "Life testing" (Epstein and Sobel 1953) and some years later by the Kaplan–Meier estimate (Kaplan and Meier 1958).

The UK Atomic Energy Authority (UKAEA) was formed in 1954. It soon got involved in performing safety and reliability assessments for outside bodies, due to its competence in such work in the nuclear field.

In the middle of the 1950s, Bell Telephone Laboratories started to develop the *fault tree* approach describing the possible causes of an undesired event, using Boolean algebra.

1960s

Reliability theory was significantly enhanced during the 1960s and several important books were published, among which are Bazovsky (1961), Lloyd and Lipow (1962), Barlow and Proschan (1965), and Shooman (1968).

In 1960, the first edition of the US military handbook MIL-HDBK-217F was released, outlining an approach for reliability prediction of electronic equipment.

In 1962, the Bell Telephone Laboratories published a report on the safety of the launch control system for the Minuteman intercontinental ballistic missile using *fault tree analysis*. This report is considered to be the birth of fault tree analysis. The same year, *David R. Cox* published his seminal book on renewal theory (Cox 1962).

In 1964, the "Reliability Engineering" handbook was published by Aeronautical Radio, Incorporated (ARINC). This book (ARINC 1964) was one of the first books describing engineering aspects of reliability theory. Another book on reliability engineering was Ireson (1966).

In 1968, the Air Transport Association (ATA) issued a document titled "Maintenance Evaluation and Program Development." This document gave rise to the approach "maintenance steering group" (MSG). The first version, called MSG-1, was used to ensure the safety of the new Boeing 747-100 aircraft. The MSG-1 process used failure modes, effects, and criticality analysis (FMECA) and a decision logic to develop scheduled maintenance. MSG-1 was later developed into MSG-2 and MSG-3, which is the current version.

The Reliability Analysis Center (RAC) was established in 1968 as a technical information center for the US Department of Defense, and soon played a very important role in the development of reliability theory and practice. The RAC journal was widely distributed, presenting updated information about new developments.

The military standard "Reliability program for systems and equipment" was published in 1969 (MIL-STD-785A 1969).

One of the most influential researchers on reliability theory in the 1960s was *Zygmunt Wilhelm Birnbaum* (1903–2000). He introduced a new importance metric of component reliability (Birnbaum 1969), made a probabilistic version of Miner's rule for fatigue life (Birnbaum and Saunders 1968), and made many other significant contributions.

1970s

A most important event for reliability in the 1970s was the release of the report from the *Reactor Safety Study* in 1975 (NUREG-75/014). The study was made by a

group of experts lead by professor *Norman Rasmussen* of MIT. A high number of important methods were developed as part of – or inspired by – the Reactor Safety Study.

The US Nuclear Regulatory Commission (NRC) was established the same year (in 1975) and soon started to issue NRC Regulations, called NUREG.

The nuclear accident at Three Mile Island (TMI) near Harrisburg, PA occurred in 1979. In light of the recent Reactor Safety Study, it had a great impact of the development of system reliability theory.

In the early 1970s, several important results on network reliability were developed in Russia (e.g. see Lomonosov and Polesskii 1971). Many new books on system reliability were published. Among these are Green and Bourne (1972), Barlow and Proschan (1975), and Kapur and Lamberson (1977).

Analysis of reliability and lifetime data grew more important and the new book Mann et al. (1974) provided help on theory and methods. An even more important publication in this area was *David R. Cox*'s paper "Regression models and life tables (with discussions)" (Cox 1972).

Based on the ideas of the MSG-approach (see 1960s), a new maintenance planning approach called "reliability-centered maintenance" (RCM) was introduced in 1978 (Nowlan and Heap 1978). The RCM approach was initially developed for the defense industry, but is today used in many other applications and a high number of standards and guidelines have been issued.

In Norway, the first major accident in the offshore oil and gas industry occurred in 1977, the Bravo blowout in the Ekofisk field in the North Sea. This was a shock for the Norwegian industry and the government. As a consequence of this accident, a large research program, called "Safety Offshore" was launched by the Norwegian Research Council. A high number of safety and reliability projects were sponsored by the oil and gas industry. The first author of this book started lecturing a course in system reliability at the Norwegian University of Science and Technology (NTNU) in 1978.

The UKAEA Safety and Reliability Directorate (SRD), established in 1977, became a very active unit with a strong influence on the development of reliability theory, especially in Europe.

1980s

The 1980s started with a new journal *Reliability Engineering*, which had a great influence on the further development of reliability theory. The first editor of the journal was *Frank R. Farmer* (1914–2001), who made significant contributions in

both risk and reliability theory. The title of the journal was later changed to *Reliability Engineering and System Safety*.

The Offshore Reliability Data (OREDA) project was initiated in 1981 and the first OREDA handbook was published in 1984. The same year another important reliability data handbook, IEEE Std. 500 (1984) also entered the market.

Reliability data analysis became more important, and several books on this topic were published in the early 1980s, the most influential may be Kalbfleisch and Prentice (1980), Lawless (1982), Nelson (1982), and Cox and Oakes (1984).

Fault tree analysis got more standardized through the *Fault Tree Handbook* that was published by the US NRC in 1981 (NUREG-0492). Bayesian probability entered into the field of reliability promoted by the book Martz and Waller (1982).

To strengthen the US semiconductor industry, the organization SEMATECH was established in 1987. SEMATECH prepared and made available a range of high-quality reliability guidelines that were studied far beyond the semiconductor industry.

Several universities established education programs in safety and reliability during the 1980s. Most notable were perhaps the programs provided by the Center of Risk and Reliability at the University of Maryland and the NTNU.

Several catastrophic accidents occurred in the 1980s and clearly showed the importance of risk and reliability. Among these were the capsizing of the Alexander Kielland offshore platform in 1980, the gas disaster in Bhopal, India in 1984, the fire and chemical spill at the Sandoz warehouse in Basel, Switzerland in 1986, the Challenger space shuttle accident in 1986, and the explosion on the offshore platform Piper Alpha in 1988. Several of these accidents prompted changes in legislation, new requirements to risk and reliability analyses, and initiated a range of research projects.

After 1990

The developments mentioned above continued and were strengthened in the years after 1990. The topic of system reliability got more and more popular and a range of new journals, new books, new education programs, new computer programs, new organizations, and a variety of reliability conferences emerged. The first edition of the current book was published in 1994, based on experience from reliability courses at NTNU.

The industry started to integrate reliability in their system development processes, often as part of a systems engineering framework. The topics of

reliability qualification and technology readiness became more and more important and requirements were integrated in contracts of specialized products.

The first edition of the important standard IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems" came in 1997 and required producers and users of safety-instrumented systems (SIS) to perform detailed reliability assessments.

During this period, more and more software has been introduced in almost all types of systems. Software quality and reliability are now an important part of most system reliability assessments. More recently, security aspects have also entered the scene.

The current survey has highlighted some few fragments of the history of system reliability. A more thorough treatment of the history is given by Coppola (1984), Denson (1998), and Knight (1991) and National Research Council (2015, Annex D). A lot of valuable information may also be found by searching the Internet.

1.11 Problems

1.1 Discuss the main similarities and differences between the concepts of quality and reliability.

1.2 List some of the services you make use of in your daily life. Which factors do you consider relevant in order to describe the reliability of each of these services?

1.3 Section 1.2 lists several application areas that are related to, and use terminology from reliability theory. Can you suggest some more application areas?

1.4 Discuss the main differences between hardware reliability and software reliability. Do you consider the term "software quality" to be more or less relevant than "software reliability"?

1.5 A *stakeholder* may be defined as a "person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity." Choose a specific item/system (e.g. a dangerous installation) and list the main stakeholders of a system reliability analysis of this item/system.

1.6 Evaluate the maintainability of a modern mobile phone. Can you suggest any design changes of the phone that will improve its maintainability?

1.7 List some technical items for which you consider it beneficial to use the physical (i.e. load-strength) approach to reliability analysis.

References

AGREE (1957). Reliability of Military Electronic Equipment. *Tech. Rep*. Washington, DC: Advisory Group on Reliability of Electronic Equipment, U.S. Department of Defense.

ARINC (1964). *Reliability Engineering*. Englewood Cliffs, NJ: Prentice-Hall.

Barlow, R.E. and Proschan, F. (1965). *Mathematical Theory of Reliability*. New York: Wiley.

Barlow, R.E. and Proschan, F. (1975). *Statistical Theory of Reliability and Life Testing, Probability Models*. New York: Holt, Rinehart, and Winston.

Bazovsky, I. (1961). *Reliability Theory and Practice*. Englewood Cliffs, NJ: Prentice-Hall.

Birnbaum, Z.W. (1969). On the importance of different components in a multicomponent system. In: *Multivariate Analysis II* (ed. P.R. Krishnaiah), 581–592. New York: Academic Press.

Birnbaum, Z.W. and Saunders, S.C. (1968). A probabilistic interpretation of Miner's rule. *SIAM Journal of Applied Mathematics* 16: 637–652.

Birolini, A. (2014). *Reliability Engineering: Theory and Practice*, 7e. Heidelberg: Springer.

Coppola, A. (1984). Reliability engineering of electronic equipment: a historic perspective. *IEEE Transactions on Reliability* 33: 29–35.

Cox, D.R. (1962). *Renewal Theory*, In: *Methuen's Monographs on applied probability and statistics*. Methuen, London: Methuen & Co.

Cox, D.R. (1972). Regression models and life tables (with discussion). *Journal of the Royal Statistical Society* B 21: 411–421.

Cox, D.R. and Oakes, D. (1984). *Analysis of Survival Data*. London: Chapman and Hall.

Denson, W. (1998). The history of reliability prediction. *IEEE Transactions on Reliability* 47 (3): 321–328.

DNV-RP-A203 (2011). Qualification procedures for new technology, *Recommended practice*, DNV GL. Høvik, Norway.

Epstein, B. and Sobel, M. (1953). Life testing. *Journal of the American Statistical Association* 48 (263): 486–502.

Fisher, R.A. and Tippett, L.H.C. (1928). Limiting forms of the frequency distributions of the largest or smallest of a sample. *Proceedings of the Cambridge Philosophical Society* 24: 180–190.

Green, A.E. and Bourne, A.J. (1972). *Reliability Technology*. Chichester: Wiley.

IEC 62278 (2002). *Railway applications – specification and demonstration of reliability, availability, maintainability and safety (RAMS)*, *International standard*. Geneva: International Electrotechnical Commission.

IEEE Std. 500 (1984). *IEEE guide for the collection and presentation of electrical, electronic, sensing component, and mechanical equipment reliability data for nuclear power generating stations, Standard*. New York: Institute of Electrical and Electronics Engineers.

IEEE Std. 1366 (2012). *IEEE guide for electric power distribution reliability indices*, *Standard*. New York: Institute of Electrical and Electronics Engineers.

Ireson, W.G (ed.) (1966). *Reliability Handbook*. New York: McGraw-Hill.

ISO 20815 (2018). *Petroleum, petrochemical, and natural gas industries: production assurance and reliability management*, *International standard*. Geneva: International Organization for Standardization.

ISO 25010 (2011). *Systems and software engineering – systems and software quality requirements and evaluation (SQuaRE) – system and software quality models*, *International standard*. Geneva: International Organization for Standardization.

ISO 9000 (2015). *Quality management systems – fundamentals and vocabulary*, *Standard ISO9000*. Geneva: International Organization for Standardization.

Kalbfleisch, J.D. and Prentice, R.L. (1980). *The Statistical Analysis of Failure Time Data*. Hoboken, NJ: Wiley.

Kaplan, S. (1990). Bayes is for eagles. *IEEE Transactions on Reliability* 39: 130–131.

Kaplan, E.L. and Meier, P. (1958). Nonparametric estimation from incomplete observations. *Journal of the American Statistical Association* 53 (282): 457–481.

Kapur, K.C. and Lamberson, L.R. (1977). *Reliability in Engineering Design*. Hoboken, NJ: Wiley.

Knight, C.R. (1991). Four decades of reliability progress. In: *Annual Reliability and Maintainability Symposium*. Orlando, FL: IEEE, 29-31 January 1991. DOI: 10.1109/ARMS.1991.154429, 156–160.

Laprie, J.C. (1992). *Dependability: Basic Concepts and Terminology*. Berlin: Springer.

Lawless, J.F. (1982). *Statistical Models and Methods for Lifetime Data*. Hoboken, NJ: Wiley.

Lloyd, D.K. and Lipow, M. (1962). *Reliability: Management, Methods, and Mathematics*. Englewood Cliffs, NJ: Prentice-Hall.

Lomonosov, M.V. and Polesskii, V.P. (1971). A lower bound for network reliability. *Problems of Information Transmission* 7 (4): 118–123.

Mann, N.R., Schafer, R.E., and Singpurwalla, N.D. (1974). *Methods for Statistical Analysis of Reliability and Lifetime Data*. Hoboken, NJ: Wiley.

Martz, H.F. and Waller, R.A. (1982). *Bayesian Reliability Analysis*. New York: Wiley.

Melchers, R.E. (1999). *Structural Reliability Analysis and Prediction*, 2e. Hoboken, NJ: Wiley.

MIL-HDBK-217F (1995). Reliability prediction of electronic equipment, *Military handbook*. Washington, DC: U.S. Department of Defense.

MIL-P-1629 (1949). Procedures for performing a failure modes, effects, and criticality analysis, *Military procedure*. Washington, DC: U.S. Department of Defense.

MIL-STD-785A (1969). Reliability program for systems and equipment development and production, *Military standard*. Washington, DC: U.S. Department of Defense.

MIL-STD-1629A (1980). Procedures for performing a failure mode, effects, and criticality analysis, *Military standard*. Washington, DC: U.S. Department of Defense.

Miner, M.A. (1945). Cumulative damage in fatigue. *Journal of Applied Mechanics* 12: A159–A164.

National Research Council (2015). *Reliability Growth: Enhancing Defense System Reliability*. Washington, DC: The National Academies Press.

Nelson, W. (1982). *Applied Life Data Analysis*. New York: Wiley.

Nowlan, F.S. and Heap, H.F. (1978). Reliability-Centered Maintenance. *Tech. Rep. A066-579*. San Francisco, CA: United Airlines.

NUREG-0492 (1981). Fault tree handbook, *Handbook NUREG-0492*. Washington, DC: U.S. Nuclear Regulatory Commission.

NUREG-75/014 (1975). Reactor Safety: An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants. *Report NUREG-75/014*. Washington, DC: U.S. Nuclear Regulatory Commission.

Shooman, M.L. (1968). *Probabilistic Reliability: An Engineering Approach*. New York: McGraw-Hill.

Smith, R.L. (1992). Introduction to Gnedenko (1943) on the limiting distribution of the maximum term in a random series. In: *Breakthroughs in Statistics* (ed. S. Kotz and N.L. Johnson). New York: Springer, 185–194.

Weibull, W. (1939). A Statistical Theory of the Strength of Materials. *Report 151*. Stockholm, Sweden: Royal Swedish Institute for Engineering Research.

Weibull, W. (1951). A statistical distribution function of wide applicability. *Journal of Applied Mechanics* 18: 293–297.