SYSTEM RELIABILITY

Concepts and Applications

Klaas B. Klaassen and
Jack C.L. van Peppen

VSSD

© VSSD
1st Edition 1988-2006

Published by:
VSSD
Leeghwaterstraat 42, 2628 CA Delft, The Netherlands
tel. +31 15 27 82124, telefax +31 15 27 87585, e-mail: hlf@vssd.nl
internet: http://www.vssd.nl/hlf
URL on this book: **http://www.vssd.nl/hlf/e003.htm**
A collection of digital pictures, printed in the book, can be made available for lecturers who adopt this book. Please send an e-mail to hlf@vssd.nl.

ISBN-10 90-71301-68-0 ISBN-13 978907130168
NUR XXX
Key word: system reliability

Preface

The mind-boggling rate of industrial expansion of the past few decades has produced innumerable technical devices and systems on which we rely in our daily life for modern convenience, safety, and sometimes even preservation of human lives. These modern artifacts cover a broad spectrum ranging from a relatively simple electronic watch to very complex transportation systems such as airplanes or spacecraft. Often, one is not even aware of the use of particular systems (part of our electrical energy is generated by nuclear reactors) until one is most unpleasantly reminded (Chernobyl disaster).

It is a proven fact that all these technical systems are *producible*, in other words: One can at least make them work at the time of first use. A higher order requirement, however, is that they remain serviceable throughout their expected useful life; i.e. that they are *reliable*. The consequences of an unreliable functioning of these systems may vary from inconvenience, extra costs, environmental damage, to even death. Such inability to perform reliably may not only arise from the product itself (usually manifested in hardware or software failures), but also from human errors. Take for instance the (pilot) error where an aircraft is put down on the runway extremely hard. As the cover picture shows, this can result in a cracked fusilage and the dragging of the entire tail section over the runway until the aircraft comes to a complete stop (Eastern Airlines, Florida, Dec. 28, 1987).

Only recently has the reliability aspect of our industrial activity been increasingly emphasised. The U.S. automobile industry, after having lost out almost completely to the Japanese and their more reliable cars, has only lately improved the reliability of its products drastically. Of course, producibility, yield, and quality are of eminent importance for an industrial product, but a healthy reliability over the entire planned life span of the product is at least of equal importance. The hesitation of many manufacturers in accepting a high reliability as one of the product design goals can be explained by the extra cost associated with the reliability program and by the intangible nature of product reliability to the customer. The customer (at least initially) does not know that one system is more reliable than another, and also does not know that the price difference between the two is more than warranted if one takes into account the later savings on "inconveniences" such as repair costs, aggravation, loss of production, accidents, environmental damage, etc.. Judging from the large number of unreliable systems around today, not everybody recognizes the principle underlying reliability engineering: "*Invest now, save later*".

A secondary cause for the hesitation to regard reliability as an important product specification is the lack of training product design engineers receive in this field. To fill this gap for graduating engineers, Dr. K.B. Klaassen started a lecture series on Reliability Engineering at the Electrical Engineering Department of the Delft University of Technology in the Netherlands. Due to the great student interest in this topic (judging from the large enrollment figures), good lecture notes became a necessity. These notes found such a receptive audience outside the University that it was decided to publish them in the form of a book, first in the Dutch language and later, when the authors had joined IBM's Almaden Research Center in San Jose, California, also in English.

This book is composed of nine chapters. At the end of each chapter the reader finds a number of problems designed to rehearse the subject matter of that specific chapter. To aid in solving the problem, the end of the book provides not only answers to these exercises, but also a detailed explanation of the solutions. Throughout the text of the book, practical examples are provided, taken from the various applications of reliability engineering such as: electronics, control engineering, avionics, power engineering etc.

Chapter 1 discusses the definition of reliability and the various associated aspects. It reviews the reasons for reliability improvement, dwells briefly on the probabilistic versus deterministic approach to reliability engineering, and gives the most important ways in which the reliability of a system may be increased.

Chapter 2 is devoted to the deterministic approach to reliability engineering, which is often indicated as the "physics of failure" approach. It deals with several degradation models, gives examples of important physical failure mechanisms, and explains the use of screening techniques for removing the potentially weak components.

From Chapter 3 on, the book focuses on probabilistic reliability engineering. *Chapter 3* covers the nomenclature, definitions and, mathematical relationships of all essential probabilistic reliability, availability, and maintainability parameters.

Chapter 4 deals with all frequently encountered failure probability distributions. It also covers reliability testing, confidence levels, and accelerated testing.

Chapter 5 is dedicated to probabilistic reliability models, in particular the catastrophic failure model, the stress-strength model, and the Markov model.

Chapter 6 discusses the effect of system structure on the reliability of non-maintained systems. It deals with series, parallel, m-out-of-n, and majority voting systems. This chapter also acquaints the reader with various techniques for reliability analysis and reliability optimization.

Chapter 7 deals with maintained systems. It introduces various forms of maintenance and their effect on the system's availability. The effect of redundancy combined with maintenance is also discussed. The chapter closes with a look at the problem of spare-parts provisioning.

Chapter 8 deals with system evaluation techniques such as Fault Tree Analysis (FTA) ans Failure Mode Effect and Criticality Analysis (FMECA). It also introduces the concepts of risk and safety.

Finally, *Chapter 9* is dedicated to software reliability. It discusses how to write reliable programs, how to test software for reliability, and gives an effective software failure model.

Acknowledgements

The authors wish to express their gratitude to the many students of the Delft University whose comments made this a better book. In addition, they wish to acknowledge the efforts of Mr. J.C. van Dijk in coordinating the drafts of this book between San Jose and Delft. They thank Mr. G. van Berkel for making most illustrations, and Mr. J.D. Schipper for his assistance with the first editions of the lecture notes. Last but not least, they thank Dr. A. Bossche for his remarks and suggestions to improve the didactic quality of this book.

Spring 1989	Klaas B. Klaassen
San Jose, California	Jack C.L. van Peppen

Contents

1 Introduction

The field of reliability engineering covers a large and extremely varied area of applied science; for that reason it is impossible to do justice to the many aspects of reliability engineering in one book. The total province of reliability engineering can be divided roughly as follows:

- *Reliability theory:* The mathematical approach of solving reliability problems by statistical and stochastic means, for example: Estimation theory, renewal theory, queueing theory, logistics, etc.
- *Measuring, testing and certifying reliability:* Measuring the achieved reliability of a product on the basis of experiments (tests), performed on only part of the products (sample), during a relatively short time (accelerated tests) which are discontinued before the entire sample has failed (truncated tests) and determining the statistical confidence of these measurements.
- *Reliability analysis:* Collection of failure data, reduction and archiving of these data for use in future designs. The occurring failures can be analysed physically (physics of failure), but also statistically (statistical failure analysis). The information gathered about causes of failure, failure mechanisms, and ways in which components fail is then used in the design phase to avoid such failures in the future.
- *Design for reliability:* Increasing the inherent reliability of a product by such means as: Using special, highly reliable components (hi-rel components), decreasing the loading level of the components (derating), reviewing the designs at certain intervals (design reviews), adapting the product to user and environment (human engineering, fail-safe methods), making a product well maintainable (modular design, standardisation), and using extra parallel components (hardware redundancy) or extra parallel calculations or operations (software redundancy).
- *Management and organisation:* Creating and maintaining an (industrial) organisation suited for the design, development, production, and maintenance of reliable products. The development of the necessary administrative and logistic support. Furthermore, training programmes, inspection, test and maintenance procedures, as well as cost-benefit analyses of the applied reliability measures are usually included in this category.

Of the above subjects, the management aspect will not be discussed in this book. The theory of reliability will be treated and elucidated by means of a number of examples from areas such as energy technology, avionics, electronics, control engineering, computer technology, and everyday life. Further, a number of topics from the reliability analysis area will be discussed. A number of design techniques will be evaluated. The importance of the choice of proper maintenance techniques will also be treated.

N.B.: The concept '*reliability*' is often confused with another concept: '*quality*'. The quality of a component, product or service (generally speaking a 'system') is determined by the degree to which the properties of that system are within predetermined and specified tolerances. If there are no specifications with regard to the expected life in a system specification, and hence the quality only pertains to the state of the system at the time of delivery by the producer to the consumer, the fraction of the total number of systems that meets the specification is expressing the *conformity* of that system. If there are also specifications with regard to the life of a system, and therefore the properties of the supplied system are also of recognised importance after the time of delivery, the fraction of the total number of supplied products that still functions in accordance with the specifications at a time t after the time of delivery t_0 is expressing the *reliability* of that system.

The following section defines exactly what is understood by the reliability of a system.

1.1 Definitions

In this book the *reliability* of a system shall be the *probability* that this *system* uninterruptedly performs certain (accurately) *specified functions* during a stated interval of a *life variable*, on the condition that the system is used within a certain *specified environment*. This general definition contains six elements which will be explained briefly below:

- *Reliability*: This is a statistical probability which is usually denoted as $R(t)$. It is often confused with the concept 'quality'. Both concepts originated in the area of quality control, from which reliability engineering later emerged as a separate field of specialisation.
- *Probability*: One should distinguish predicted, or *a priori* reliability, which is defined as a sheer likelihood, and proved, or *a posteriori* reliability, which is a retrospective certainty, and is defined as the fraction of surviving systems. For a future design one can only predict; afterwards, in a case history for example, one has certainty.
- *System*: A system encompasses a collection of elements (components, units, modules) between which there is a mutual interaction (interconnection) which can be separated from the environment of that system (system boundaries). The mutual interaction between the elements of a system realises the system function, which can, in general, be divided into a number of specified attributes or properties.

  The designation 'system' does not only imply technical systems such as equipment, installations, and machines, but also non-technical systems such as biological organisms, organisations, and services. For convenience we will restrict our examples to technical systems
- *Specified function*: The purpose of a certain system is reflected by the system functions, which in turn consist of one or more specified properties or attributes. In systems with signals continually varying between certain limits (analog systems) a system function (for example amplification) can be separated into a number of properties (e.g. voltage amplification 100, bandwidth 2 MHz) which are subjected to tolerances (voltage amplification 100 ± 5%, bandwidth > 2 MHz). In Table 1.1 the specifications of an

analog measurement instrument are given. If one or more specified properties exceed the tolerance intervals the system is no longer reliable; it has failed. In the case of analog systems (here the amplifier) the system may still be able to function, but outside the tolerances. In systems operating with binary signals (digital systems) one usually sees that a certain function (for example, access to a background memory) or a property of it (the ability to store information) ceases completely, i.e. can no longer be used, after a failure has occurred. Therefore, the temptation to continue using a failed system is not as strong here.

Name	Instrumentation Amplifier	
Manufacturer	XXX Corporation	
Model Number	3456-B	
All specifications traceable to US Bureau of Standards		
Function	Voltage Amplification	
Specifications	Gain	$100 \pm 5\%$
	Frequency Range (–3 dB)	DC –2 MHz
	Noise (referred to input)	< 1.5 nV/$\sqrt{}$Hz
	Input Impedance	> 1 Mohm
	Output Impedance	< 0.1 ohm
	Nonlinearity (input < 1 V)	$< 10^{-3}$
	Max. Output Current	> 100 mA (short circuit protected)
	Required Line Power	< 42 VA
Environment	Temperature Range	
	Operational	0 °C to 50 °C
	Storage	–40 °C to 75 °C
	Humidity Range	$< 95\%$,no condensation
	Altitude	
	Operational	< 4.5 km
	Mechanical Shocks	< 50 m/s^2
	Line Voltage Range	120 V +5%,–10%
	Line Frequency Range	48 Hz to 440 Hz
Reliability	Mean time to failure (no maintenance)	5 years

Table 1.1 *An example of a system (instrumentation amplifier) with a certain function (voltage amplification) which is specified. The environment in which the instrument should be used is also specified. The reliability specification is given as the expected average life.*

- *Life variable*: The elapsed time in almost all cases will be the life variable. This may be calendar time, but also accumulated user time (operation time). The time that the system is not in use must be accounted for, however, if it contributes to a shortening of the system's life. The total time is then $t = t_o + at_{oo}$, in which t_o is the operation time and t_{oo} the time that the system is not in use. The coefficient 'a' which indicates the severity of 'non use' is almost always smaller than 1. However, there are cases in which systems out of operation have, per unit of time, a greater mortality then when in operation. Just think of electrolytic capacitors, effects of condensation in systems that are not in use, and think also of people with a task too light or no task at all who more often make mistakes from plain boredom. Besides time, the life variable may also be the number of times a system is switched on and off (relay), the number of load changes (fatigue fractures in airplane wings, landing-gears, jet turbine blades, etc.), or it may be the distance travelled (cars).

- *Specified environment*: Every system is placed in a certain environment. All elements that are not part of the system belong to this environment, thus most of the time also the user and the rest of the installation of which the system in question is a part. If a system is put in the wrong environment (i.e. outside the specified environment parameter ranges), either on purpose or inadvertently, the system may fail or age more quickly. Examples are an environment that is too hot or too wet, a supply voltage that is too high, input signals that are too large, or a load that is too great or too small (applying full throttle while the car's gear is in neutral). This so-called *misuse* of a system outside the specified environment cannot be accurately forecast by the designer and must therefore be excluded in the reliability definition.
  N.B.: In practice most systems fail due to misuse, either by the user or by the designer who wrongly applies the components in the system; so most systems fail because of human error.

In the above, the definition of reliability has been explained in detail. It turns out that no statement about the reliability of the system can be made without an explicit, clearly formulated description of the *system* under observation, the *system functions*, and the *allowed environment*. For example, what is the reliability of a human being? Is a human outside the specifications if he or she has a headache?

In technical systems, but also in services and the like, it is therefore of major importance to describe these matters as exactly as possible, also with regard to later legal and financial consequences (legal liability for and warranty on products etc.).

We shall later see that it is important to distinguish between systems that are maintained and systems that are not. By *maintenance* we understand any human intervention which keeps the system operational or returns it to an operational state. If a system is maintainable but *de facto* is not maintained due to neglect, for instance, that system belongs actually to the second above-mentioned group of systems without maintenance. Rather than use the term 'maintainable', which indicates a degree of freedom, we shall use the term 'maintained'. We shall therefore call the two categories mentioned above 'maintained' and 'non-maintained' systems.

The concept reliability only pertains to non-maintained systems, since in the considered interval of the life variable the system has to function correctly without interruption, so no failures may occur. Repairs are not allowed here.

called the ‘invest now, save later’ principle of reliability.

Also the socio-ethical aspects of products with a reliability that is too low cannot be underestimated. These low-reliability disposable products lead to a waste of labour, energy, and raw materials that are becoming more and more scarce.

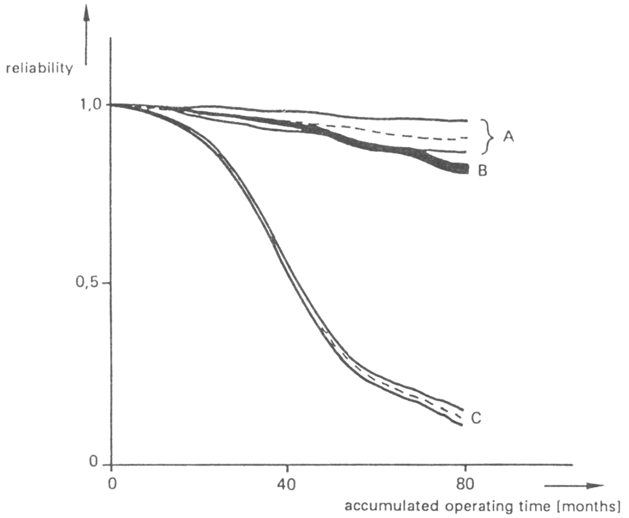

Figure 1.1 *The reliability of various energy sources for pacemakers.*
a) nuclear batteries (140 elements);
b) lithium batteries (5600 elements);
c) mercury-zinc batteries (2000 elements).

1.3 Statistical versus deterministic approach

As we have seen in Section 1.1 one has to distinguish between *a priori*, or predicted reliability, and *a posteriori*, or proven reliability.

In the statistical, predicting approach of the reliability problem the designer will try to make a judgement about the expected reliability of a future system on the basis of information about the field behaviour of previously produced components and on the basis of the results of (artificially accelerated) reliability measurements of current components. Taking this approach can give rise to a number of problems.

With today’s fast development of technology, future products will hardly contain components of which the reliability history is known. So, in general, we do not have access to statistical data for the calculation of system reliability. Even if we do use components developed in the past, with a known reliability history, the components to be used will fairly certainly have been manufactured at another time. Usually the production process has been adjusted in the meantime. From investigations it has become clear that these, at first sight, small adjustments may have great consequences for the reliability. The components produced later no longer fulfill the previously proven reliability (non-homogeneity in time of the production line).

An alternative would be to measure the reliability of components by accelerating the ageing process. Here too, a number of problems may occur.

How large is the applied acceleration factor exactly? Are the component parameters which are stressed to produce accelerated ageing really representative of the actual ageing of the components in the field, i.e. during practical use? Are perhaps other failure mechanisms also triggered which would result in too low a predicted reliability? Are certain failure mechanisms occurring during practical use not excited at all, in the test or are they excited with an acceleration factor which deviates from the intended acceleration?
Another problem is that we usually are not able to measure 100% of the components; for example because the components surviving the test have a considerably shortened remaining life expectancy. We will therefore have to make our judgement based on a sample out of the total population of components. If the production is not sufficiently homogeneous, a small sample will result in an inaccurate assessment of the reliability of the entire collection (take for instance the production non-homogeneity within one batch or between batches).
All in all, the conclusion is that the statisticians hand us very fine algorithms for sampling and testing, which find widespread use in reliability engineering, but we have to work with an appalling lack of information. In practice one often has to make do with many best judgement estimates. The confidence level of the final results is then so low that one achieves little more than a rather uncertain assessment of the expected reliability of a future system. In this respect, it should be noted that the statistical methodology (when using estimated reliability data for many components) gives a far better estimate for the *ratio* of the reliabilities when we are comparing different design alternatives.

For the above reasons, an alternative to the statistical approach to the reliability problem, the deterministic approach, is also important. The deterministic approach entails the study of physical deterioration processes leading to failure in components. Important is what starts these processes, which environment accelerates them, how they lead to breakdown of a component, and how these processes can be stopped or slowed down. Based on the know-how of the (dominant) deterioration process (evaporation of a filament in an incandescent lamp, for example) and the rate of the degeneration (depending on the temperature of the filament) one can make a prediction about the life (*in casu* the number of burning-hours until the filament opens up).

As an example of the deterministic approach to a reliability problem, we shall briefly discuss a study of failure mechanisms in light bulbs.
Light bulbs are made for a certain mains voltage V (for example $V = V_{rms} = 220$ volt), so that the dissipated power P ($P = V^2/R_{hot}$) has a certain value (e.g. $P = 100$ watt). This determines, among other things, the length and cross sectional area of the tungsten filament. Usually the filament is spiralled (sometimes even twice) to increase the heat production (temperature increase per watt) and thus the light production (lumen/watt). After switching on, the filament reaches in ca. 10–20 ms a final temperature of about 2500 to 2600 °C (4500 to 4700 °F). The accompanying rapid expansion (and contraction when switching off) may result in thermal fatigue of the filament. The life variable of this failure mechanism is clearly the number of on-off cycles of the lamp. If the filament is left on, the dominant failure mechanism is the evaporation of the filament. Here the life variable is the number of burning-hours. However, one is faced with a paradox here: *a uniformly evaporating filament, supplied with a constant voltage, cannot fail by evaporation!* This is because the

filament's resistance will increase more and more as the filament evaporates, thereby reducing the dissipated power and consequently the filament's temperature. In turn, this lower temperature will slow down the evaporation process more and more. The lamp's real cause of failure is a local, greatly increased evaporation, for example at the location of a crack in the filament or at a narrow site caused by the surface roughness of the drawn filament. At this site the cross section is smaller and the dissipation, and therefore also the temperature, is higher. This causes the evaporation to be much faster here. In Figure 1.2 it is shown how the life t decreases accordingly as the temperature T_{hs} of a hot spot rises higher above the temperature T_w of the rest of the filament.

N.B.: Small differences in the diameter and thus in the temperature have large consequences! Therefore, we have to conclude that the quality control of the filament during production is of decisive importance for the later life of the lamp.

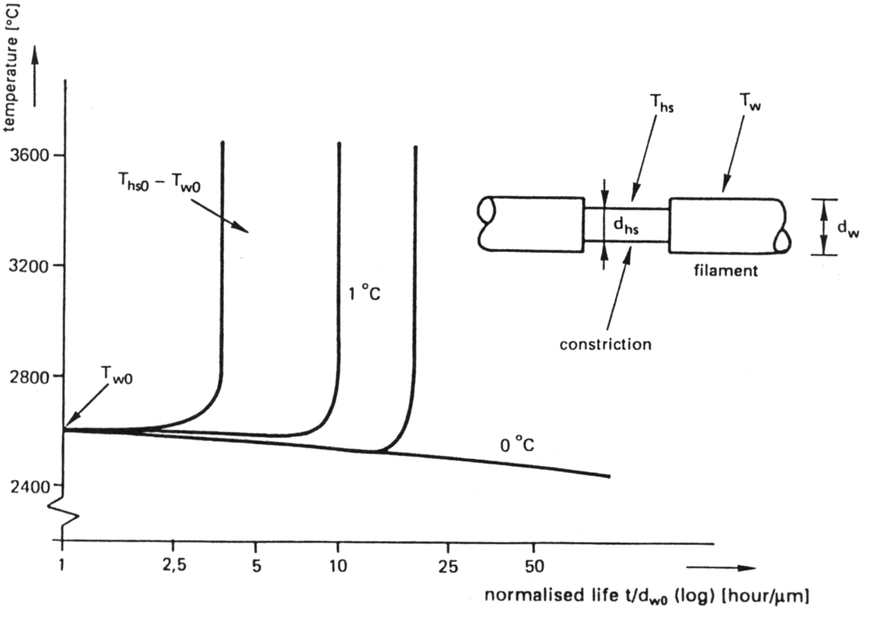

Figure 1.2 *Normalised life t/d_{w0} of a filament of a light bulb as a result of an initial hot spot caused by a constriction. The initial diameter of the filament is d_{w0}, the initial hot spot temperature is T_{hs0}, the initial filament temperature is T_{w0}. A minor difference in temperature has great consequences!*

Figure 1.3a shows the temperature profile along a filament that is left on continuously. It shows four instances, viz. 0, 30, 60 and 95 % of the life t_0 of the filament. We clearly see the development of a hot spot. Finally, Figure 1.3b indicates how the temperature profile (designated *T*) correlates with the measured diameter profile of the filament (designated *D*). Concludingly, the following remark. Many light bulbs die prematurely from yet another cause: Mains voltage spikes. After all, a mains voltage above nominal is an accelerating factor for both above-mentioned failure mechanisms. It does not introduce a new failure process; it just accelerates existing failure processes.

The information often neglected in accelerated testing conducted on a purely statistical basis, is the failure mechanism of the defective components. This failure mechanism will probably also be present in the other components, but has not caused a failure within the duration of the test under the applied test conditions. In the field this may be different.
The questions arising if one would only follow the deterministic approach (i.e. the physics of failure approach) are, among others: Can statistical fluctuations in the production process cause some components to fail, for example, by a failure mechanism which is not probable in most components? Small cracks, for example, may be created in the filament of some light bulbs by fluctuations in the drawing process, where an ordinary filament has a life which is limited by the surface roughness of the filament.
Another question is whether many of these physics of failure studies are not aimed too much at the 'typical' component. The entire production process, which also produces 'atypical' specimens, gets too little attention. Precisely these atypical specimens may later dominate the failure behaviour of the total population.

One cannot limit oneself to the statistical or the deterministic approach alone. Both are one-sided: The statistician is not interested in the cause of the failure, the physicist is only interested in the 'typical' failure mechanisms.
This is the reason to use both approaches in mutual harmony to obtain accurate life expectancy information and a reliable product.

1.4 Methods for increasing reliability

There are several ways in which the inherent reliability of a system can be assured. The inherent reliability is the reliability intrinsic to the system that will indeed be realised in the field provided the system is not misused. In this section the most important measures that can be taken to secure a high inherent reliability will be discussed briefly below. Many of them will later be treated in more detail.

- The introduction of reliability in as early a phase of the system design as possible as one of the aims of that design. Figure 1.4 shows an example of how important a well-considered design is in this respect. This early introduction is necessary because, if the reliability is only introduced in a late phase where the design is final or nearly final, the only thing a designer can do is to resort to the use of reliable (and therefore expensive) components, or he can apply redundancy at the system level (which is very ineffective), or he can improve only the weakest link in the chain. These are all methods that are not very cost effective. We will return to this later.
- The choice of those technical means and technologies that can easily realise the required system functions without necessitating a *tour de force*. After the choice of a proper technology or a proper combination of technologies, one should be able to design the system with configuration necessitating the minimal quantitative and qualitative complexity. The aim of the design should be that the system functions are determined by only a few, reliable components and the design must be tolerant of variations with time in the properties of the other, less critical components.

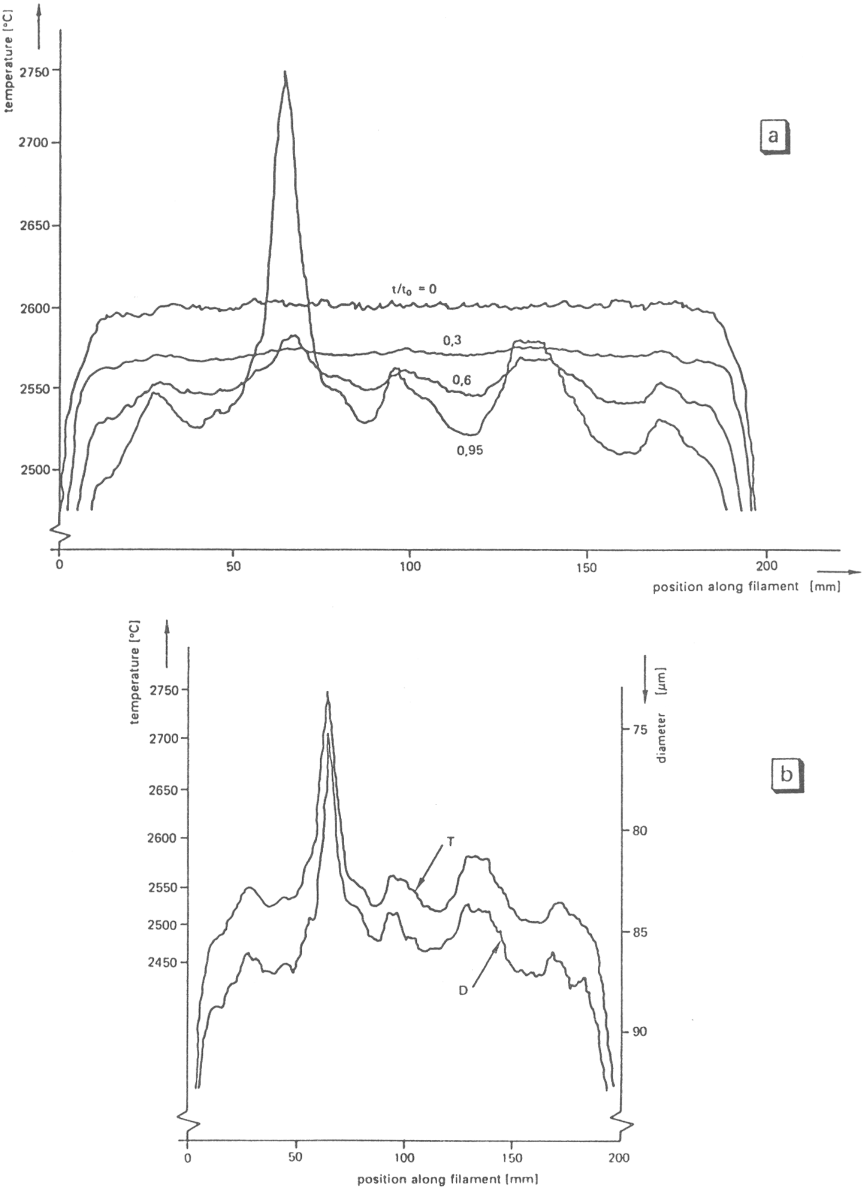

Figure 1.3 *Temperature variation along a filament of an incandescent lamp.*

a) Temperature profile at four different instants t/t_0 in the life $(0, t_0)$ of a filament.

b) Correlation between the temperature profile (indicated by T) and the profile of the filament diameter (indicated by D) for the instant $t/t_0 = 0.95$.

2 Deterministic Reliability

As we have already seen, the deterministic approach to reliability is especially interested in the physical process that leads to failure. This process is called the *failure mechanism*. Eventually, it leads to the situation where a component does not function at all or where it functions outside the specified tolerances. The consequences of a failure mechanism that has led to the component exceeding its specified limits can be observed externally. The observed failure is called the *failure mode* of that component. A failure mechanism is usually activated and accelerated by a certain environmental quantity or combination of environmental quantities. Such quantities are called *stress quantities*. If we use the example with the light bulb from Section 1.3, one of the *failure mechanisms* is an increasing local evaporation caused by the creation of hot spots along the filament due to cracks or surface roughness. The externally observable *failure mode* is an open filament. So the light bulb fails in the open mode. A *stress quantity* for this failure mechanism is the applied voltage (mains voltage). The stress as a result of a slightly increased supply voltage is large: The mains voltage has only to be increased very little above the nominal value for a much shorter life.

2.1 Arrhenius' model

One of the most common and important stress quantities is the increase of a component's *temperature*. The temperature of a component is determined by the temperature of the environment (external stress) and the power dissipation in the component, which in combination with the heat resistance to ambient (*environment*) makes the internal temperature rise above the ambient temperature (*internal stress*). A temperature increase accelerates all sorts of physicochemical processes. It is often assumed that the failure process behaves as a chemical process with a certain reaction rate Q for which the following equation holds:

$$Q(T) = Q_0 \, e^{-E_A/kT},$$

here Q_0 is a constant, E_A the *activation energy* in electron-volt, k is Boltzmann's constant ($k = 8.6\times10^{-5}$ eV/K) and T the absolute temperature. This expression was determined experimentally by Arrhenius in 1880.

If it is assumed that the drift in the properties (parameters) of the component as a function of time t is proportional to:

$$t^n Q(T),$$

in which linear drift in time is a special case: $n = 1$, we can compare failure rates at two

3
Statistical Reliability

Statistical reliability engineering is too broad a subject to be completely covered in one book. In the choice we had to make, it was, for example, decided not to treat the measurement of reliability and its related topics such as: Statistical sampling methods and strategies, estimation theory, decision theory, and statistical data analysis. In this book only those subjects that lead to a direct insight into stochastic failure processes, reliable system configurations, calculation methods, reliability models, and maintenance strategies will be treated.

3.1 Nomenclature

The useful life of a system is assumed to end when the first failure occurs. We shall therefore define *failure* as the end of the ability of a system to realise the function required from that system.

- *Implicit restrictions*. It is assumed, in accordance with the reliability definition given in Section 1.1, that the system failure is not (also) caused by *misuse*. So the system is always used within the specified environment. It is further assumed that the failure is not *intermittent*, i.e. a failure does not correct itself without human intervention. Once failed, the system remains broken until repaired. In addition, it is assumed that the system *either functions correctly or is broken*; a state in between the two is not possible. Lastly, it is assumed that the *life variable* is the time t after delivery of the system by the manufacturer to the user. In Figure 3.1 it is indicated that a system with continuously variable parameters (for example, an analog electronic system) can show failures in two ways. The respective parameter x (the amplification) has a nominal value of x_0 and an allowed tolerance interval of ± 1%. A *degradation failure* is a failure where this tolerance interval is gradually exceeded, whereas a *catastrophic failure* is a failure where the function (amplification) suddenly falls away completely. In this book we shall not treat calculation methods specifically suitable for degeneration failures. The parameter drift in time viewed as a statistical process can often not be described analytically and one has to resort to 'Monte Carlo' simulations. These are statistical model experiments performed on a computer. Here we shall not digress on such special approaches to degeneration failures. So we hold the viewpoint: outside the tolerances means failed, within the tolerances means functioning correctly. Further, we assume that a system with degeneration failures breaks down at the first moment the tolerances are exceeded and remains broken, even if the parameter drifts back to within the tolerances.

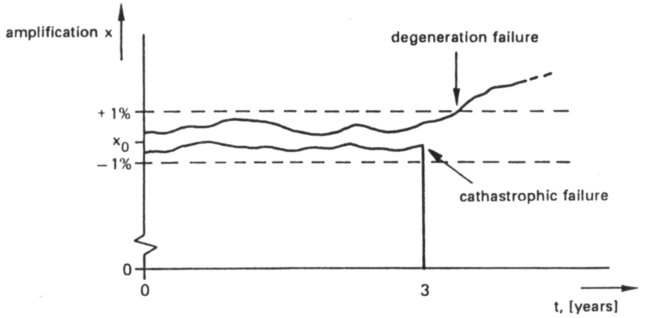

Figure 3.1 *Two different failures in an analog electronic amplifier; a total or catastrophic failure, for example caused by a short circuit which terminates the amplification function completely and a gradual and partial failure, for example caused by drift of the amplifier gain.*

- *Distinct time intervals*
  The useful life of a system is the time that elapses after delivery to the customer and before the system is finally discarded. This useful life span can be divided into a number of time intervals that are meaningful with regard to the operational quantities to be defined in the next section. For the most general system, that is a system which is also maintained, the time intervals are shown in Figure 3.2.

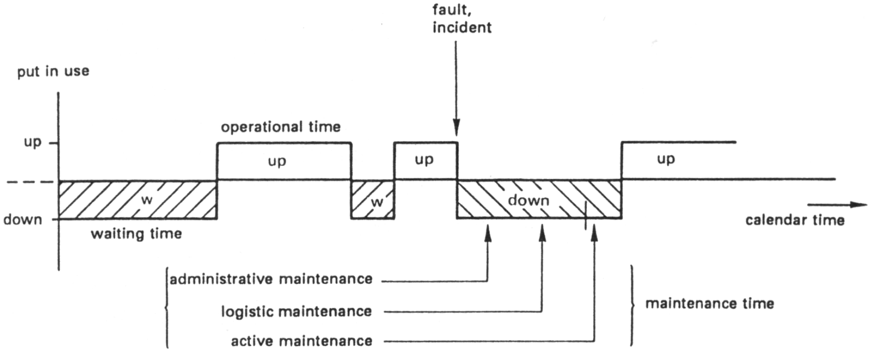

Figure 3.2 *Main subdivision of the calendar time of a maintained system.*

Two cases are to be distinguished here.

• The system is in use or ‘up’.

During the so-called *up-time* the system functions correctly. During this time, the owner will utilise the system to the full (example: The activity of actually driving a car) or he will keep it ready for direct use (the car is idling while waiting at a traffic light).

•The system is not in use.

This time can be divided into two classes, depending on whether a system is down on purpose (car parked in front of the house) or unintentionally (car not available because of required maintenance). The first time is called *stand-by* or *waiting time*, the second time *maintenance* or *down time*. The maintenance time can be used for preventive maintenance (changing oil, lubrication, checking the pressure in the tyres), but also for corrective maintenance (fixing a failed ignition). The maintenance time can usually be divided into three classes.

5 Reliability Models

This chapter will discuss a number of frequently used reliability models. A reliability model is determined by a number of premises about the failure of system components. Taken together, these premises form the model on which the reliability computation is based.

In Section 3.1 we have already mentioned a number of premises. This was necessary, because otherwise concepts such as $R(t), F(t), f(t)$ and $z(t)$ could not be defined without ambiguity. These premises are:

1. A component is correct or has failed; for degeneration failures the component is faulty from the first time it exceeds the tolerances.
2. Once failed, a component remains defective (until maintenance is completed); no intermittent failures occur.
3. The life variable is the calendar time (see Section 1.1).

The reliability models that will be discussed in this chapter also include other assumptions, still to be introduced, in addition to those above.

N.B.: One can also do without the above-mentioned assumptions, but the theory will become complex. Just think of omitting (2) which has the result that the $R(t)$ function will no longer be a single-valued function. The reliability function would increase if the likelihood increases that more components will function again.

In addition to reliability models we also come across other models in reliability engineering. Examples are *schematic models* (wiring diagrams, component layouts, and the like) and *functional models*. A schematic model contains the highest useful degree of detail with the component parts, parameter values and other useful data (see Figure 5.1). A functional model is, in fact, a drawing indicating how a system is built up from subsystems. In such a functional model the information and energy flows are clearly reflected (see Figure 5.2).

5.1 Catastrophic failure model

The catastrophic failure model is the simplest failure model, in which, besides the above-mentioned premises, it is also assumed that if a component fails it does not matter how it fails. So it is, in fact, assumed that the component has only one single distinguishable failure mode (*single mode failure*). Representing failures by means of a model now becomes very simple. As indicated in Figure 5.3, the component (or the relevant part of the system) may be replaced by a black box in which there is a hypothetical switch.

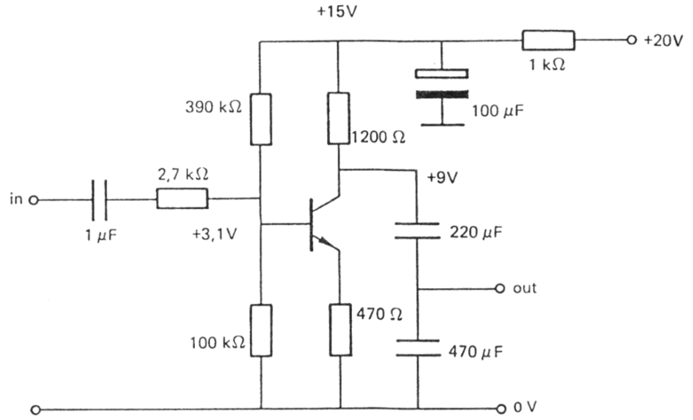

Figure 5.1 *Example of a schematic model of part of an electronic circuit, usually called 'schematic' for short.*

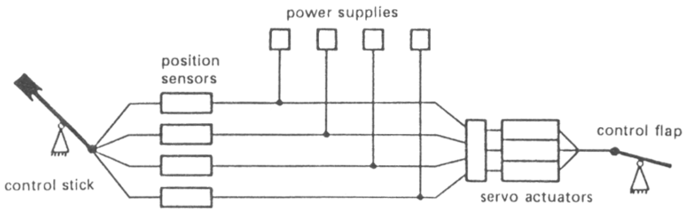

Figure 5.2 *Functional model of a 'fly-by-wire' system as used in modern airplanes (fourfold redundant power supplies, sensors and cabling).*

If the component is functioning correctly this switch is closed and the *state* of the component is defined as '1'. The state is '0' if the component has failed; the switch is then open. In the corresponding reliability model there must always be at least one path of closed switches in oder for the system to function. Compare Figures 5.3b and 5.3c. The state of a system is therefore fully determined by the state of its component parts. One can now simply draw up a *truth table* with the state of the components as binary input variables and the state of the system as the binary output variable. The structure of the reliability model determines the relationship between these variables, which can be described by Boolean algebra. Based on this is a particular calculation method for the reliability of systems, which will discussed in Section 6.9.2.

To demonstrate the limitations of catastrophic failure models we use Figure 5.3c for reference. For the RC-member depicted a certain nominal value for R and C will be specified, together with certain tolerance limits if it is to function correctly as a filter. It is assumed that the resistor exhibits the failure 'open' if it exceeds the upper tolerance limit, while it shows the failure 'short-circuited' if the lower tolerance limit is exceeded. Subsequently, we assume that both failure modes, as far as the reliability is concerned, do not need to be distinguished. We therefore label them jointly as: 'Broken resistor' with a failure probability P_r. For the capacitor the same assumptions are made. We see that a catastrophic failure model contains no information as to how a component fails. It is not always possible to lump together the transgression of a component parameter beyond an upper and a lower tolerance limit. This can be easily seen from Figure 5.4. The two