

# **System reliability**

## Concepts and applications



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

# SYSTEM RELIABILITY

*Concepts and Applications*



# SYSTEM RELIABILITY

*Concepts and Applications*

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

© VSSD  
1st Edition 1989-2006

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 a request to [hlf@vssd.nl](mailto:hlf@vssd.nl).

*All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.*

ISBN 978-90-71301-68-1 Ebook: ISBN 978-90-6562-226-6

NUR 992

*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 fuselage 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) and 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  
San Jose, California

Klaas B. Klaassen  
Jack C.L. van Peppen



# Contents

PREFACE	5
1 INTRODUCTION	11
1.1 Definitions	12
1.2 Need for reliability engineering	15
1.3 Statistical versus deterministic approach	16
1.4 Methods for increasing reliability	19
Problems	22
2 DETERMINISTIC RELIABILITY	23
2.1 Arrhenius' model	23
2.2 Failure mechanisms	26
2.3 Screening	29
Problems	30
3 STATISTICAL RELIABILITY	32
3.1 Nomenclature	32
3.2 Operational reliability quantities	34
3.2.1. Derived quantities	36
Problems	39
4 STATISTICAL FAILURE OF COMPONENTS	41
4.1 Failure distributions	41
4.1.1 Negative-exponential distribution	44
4.1.2 Normal distribution	48
4.1.3 Lognormal distribution	50
4.1.4 Weibull distribution	51
4.1.5 Gamma distribution	53
4.2 Life distribution measurements	57
4.2.1 Failure distribution from life tests	58
4.2.2 Confidence level of life tests	58
4.2.3 Accelerated life tests	61
Problems	62
5 RELIABILITY MODELS	63
5.1 Catastrophic failure model	63
5.2 Stress-strength model	68
5.3 Markov model	73
Problems	83

6 NON-MAINTAINED SYSTEMS	85
6.1 Introduction	85
6.2 Series systems	86
6.3 Redundancy	89
6.4 Parallel systems	92
6.4.1 Dependent failures	97
6.5 $m$ -out-of- $n$ systems	101
6.6 Majority voting systems	103
6.7 Mixed systems	106
6.8 Optimisation	107
6.9 Analysis methods	111
6.9.1 Network reduction method	111
6.9.2 Tie set and cut set method	112
6.9.3 Decomposition method	114
6.9.4 State-space method	115
Problems	119
7 MAINTAINED SYSTEMS	126
7.1 Introduction	127
7.2 Systems with preventive maintenance	129
7.2.1 Scheduled maintenance	129
7.2.2 Condition-based maintenance	132
7.3 Systems with corrective maintenance	135
7.3.1 Replacement	136
7.3.2 Repair	138
7.3.3 Repairable systems without redundancy	141
7.3.4 Repairable systems with redundancy	150
7.3.5 Shared-repair facilities	156
7.3.6 Inhomogeneous systems	159
7.4 Maintenance aspects	164
7.4.1 Maintenance strategies	165
7.4.2 Spare parts supplies	166
Problems	167
8 EVALUATION METHODS	172
8.1 Introduction	172
8.2 Causal evaluation	173
8.2.1 FMEC Analysis	174
8.3 Anti-causal evaluation	177
8.3.1 Fault tree analysis	178
8.4 Risk and safety	187
Problems	191
9 RELIABILITY OF COMPUTER SOFTWARE	196
9.1 Introduction	196
9.2 Writing reliable software	198

9.3 Reliability testing	200
9.4 Failure models for software	201
Problems	204
SOLUTIONS TO PROBLEMS	205
1 Introduction	205
2 Deterministic Reliability	206
3 Statistical Reliability	207
4 Statistically Failing System Components	209
5 Reliability Models	210
6 Non-Maintained Systems	212
7 Maintained Systems	223
8 Evaluation Methods	234
9 Reliability of Computer Software	242
APPENDIX	245
A.1 Applied Laplace Transforms	245
A.2 The Central Limit Theorem	245
A.3 Most Commonly Used Symbols	246
LITERATURE	247
INDEX	253

# 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  $100 \pm 5\%$ , 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.

<b>Name</b>	Instrumentation Amplifier	
<b>Manufacturer</b>	XXX Corporation	
<b>Model Number</b>	3456-B	
All specifications traceable to US Bureau of Standards		
<b>Function</b>	Voltage Amplification	
<b>Specifications</b>	Gain	$100 \pm 5\%$
	Frequency Range ( $-3$ dB)	DC $-2$ MHz
	Noise (referred to input)	$< 1.5$ nV/ $\sqrt{\text{Hz}}$
	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
<b>Environment</b>	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 <sup>2</sup>
	Line Voltage Range	$120$ V $+5\%$ , $-10\%$
Line Frequency Range	$48$ Hz to $440$ Hz	
<b>Reliability</b>	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 than 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.

For that reason we introduce a more general concept: *Availability*. For non-maintained systems the availability is equal to the reliability. We shall discuss the availability of a maintained system in more detail in Chapter 7, where we deal with maintained systems.

Reliability engineering can now be defined as the whole of mathematical, organisational, and other applied scientific technologies, methods, and strategies to achieve a reliable product and determine its degree of reliability.

## 1.2 Need for reliability engineering

The necessity to practise reliability engineering is obvious from the relation between the elements of the reliability definition given in the previous section. The size of the system, the intricacy of the specified functions, the length of the useful interval of the life variable, and the degree of hostility of the system's environment all influence the reliability.

It will be clear that the tendency to larger systems, i.e. systems with larger numbers of components, would decrease the reliability if the development of more reliable system components and structures does not keep in step. There are many such systems with a large *quantitative complexity*, such as energy distribution networks, telecommunication systems, digital computer networks, and space probes.

In addition, there is a tendency towards the use of more complex system functions, that is, more functions to be performed by a single system, the functions are more involved (which is expressed in more specified properties), and the allowed tolerances become smaller. This increase in *qualitative complexity* also causes the reliability to drop if no adequate countermeasures are taken. We may think of: Multi-function measuring equipment with a higher, required accuracy, automatic landing systems for airplanes, process control equipment, and so on.

Further, the correct functioning of a system over a longer interval of the life variable is increasingly important as we become more dependent on such systems (energy generation systems, pacemakers and the like). These so-called critical systems require a high reliability, often over long periods (e.g. 25 years for telecommunication systems). A source of concern in pacemakers, for instance, is the energy source, since circuit failures in pacemakers occur with a probability of less than  $140 \cdot 10^{-9}$  per hour. In Figure 1.1 the reliability of a number of different energy sources for pacemakers is shown.

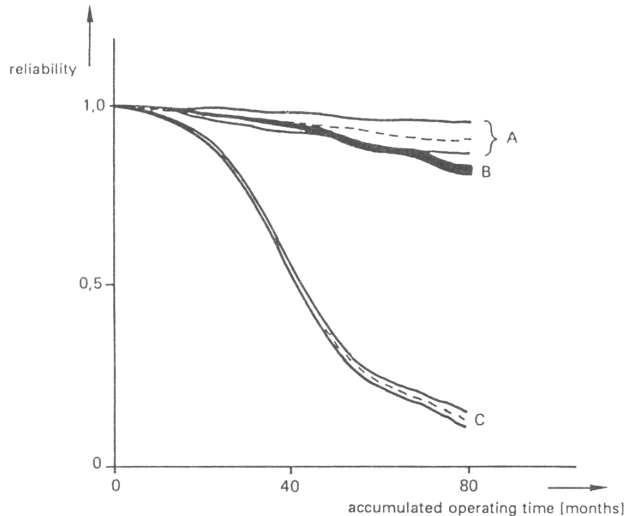
Besides this, our technical systems are more and more put to use in hostile environments; they have to be suitable for a wider variety of environments. Just think of applications in the process industry (heat, humidity, chemical substances), mobile applications in aircraft, ships, and vehicles (mechanical vibrations, shocks, badly defined power supply voltages, high electromagnetic interference level).

All in all, these are sufficient reasons for reliability engineering to be so much in the limelight these days. Add to that the emphasis on reliability in situations where no maintenance is possible, because of an isolated location (unmanned arctic weather stations, remote space probes, underwater amplification stations in transatlantic cables, etc.). Even if maintenance were possible, it is often better (more cost-effective) to increase the initial reliability of a system because of the high costs associated with that system being down for repairs. Despite the higher initial costs, the life cycle cost may turn out to be lower. This is



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.

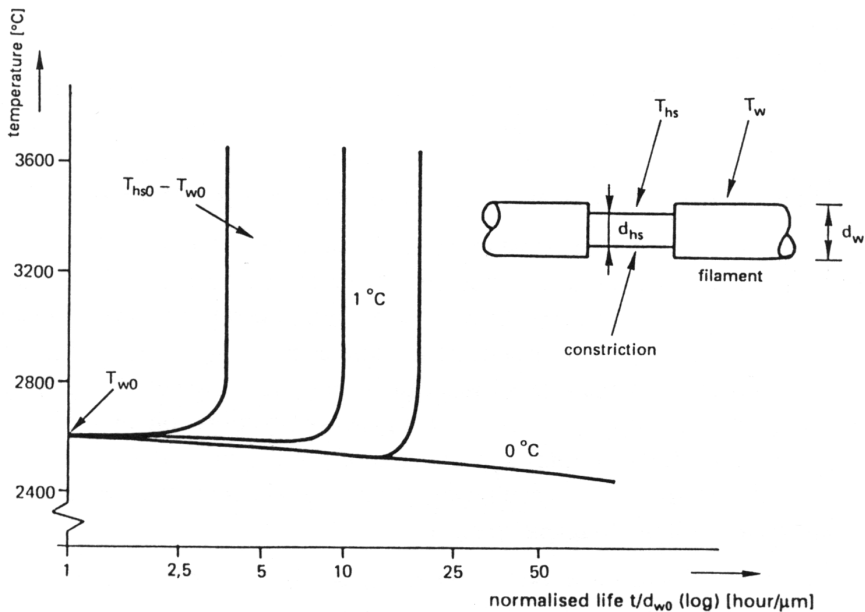
For the above reasons, an alternative to the statistical approach to the reliability problem, the deterministic approach, is also important. The deterministic approach entails the study of physical deterioration processes leading to failure in components. Important is what starts these processes, which 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.

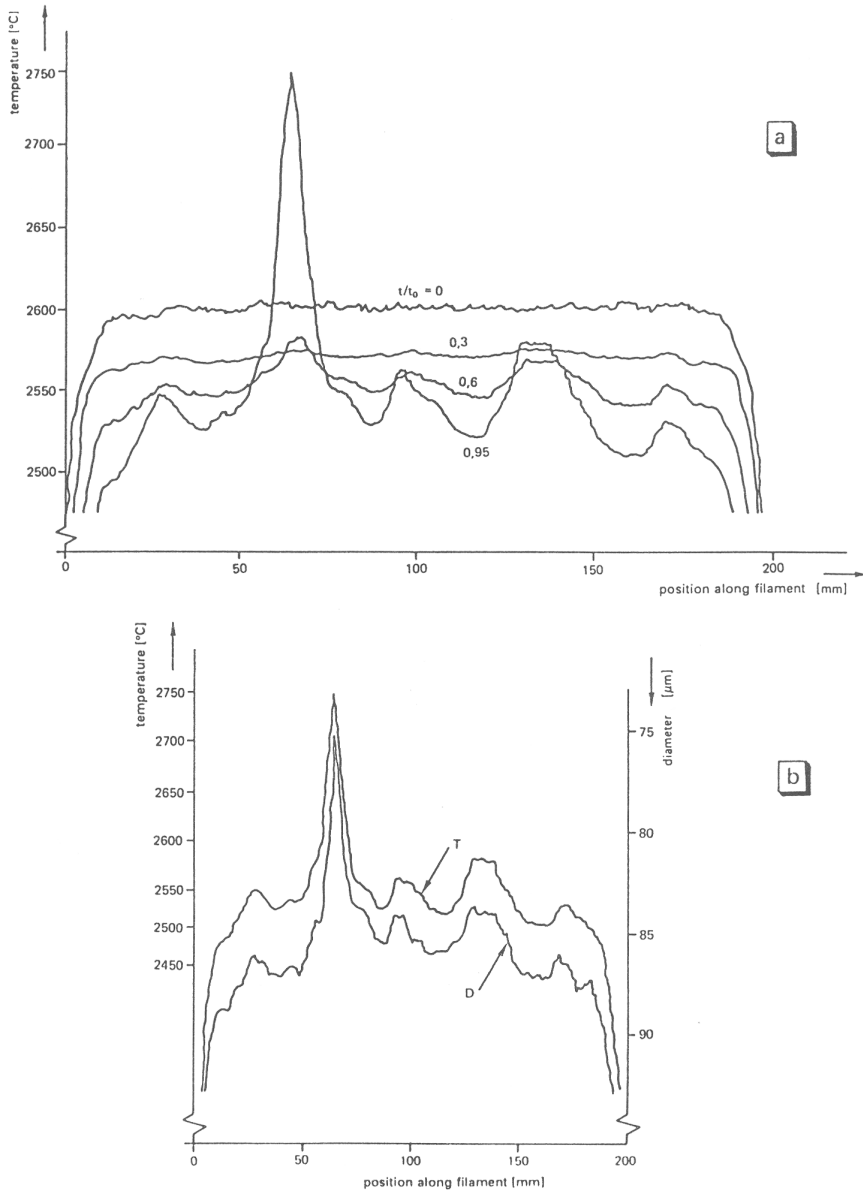
One cannot limit oneself to the statistical or the deterministic approach alone. Both are one-sided: The statistician is not interested in the cause of the failure, the physicist is only interested in the 'typical' failure mechanisms.

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.

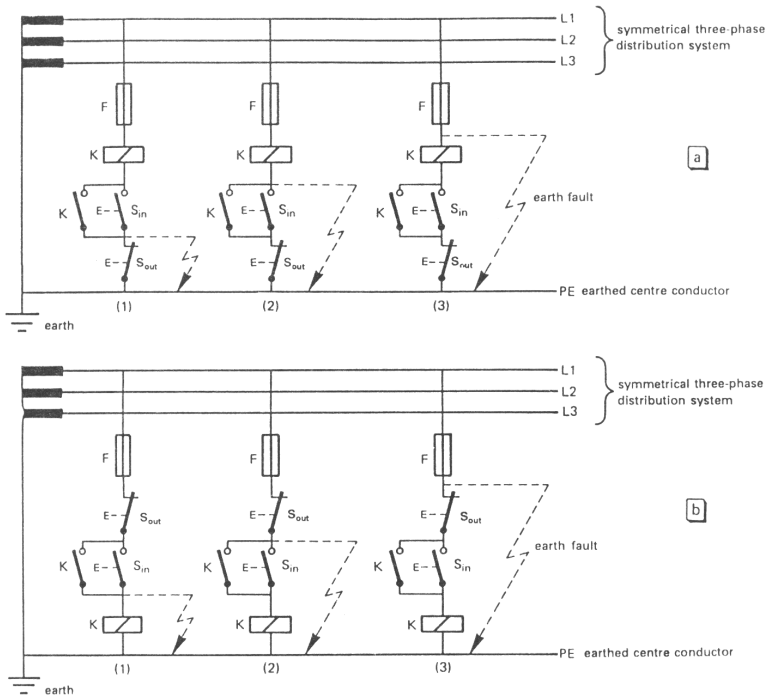
- The introduction of reliability in as early a phase of the system design as possible as one of the aims of that design. Figure 1.4 shows an example of how important a well-considered design is in this respect. This early introduction is necessary because, if the reliability is only introduced in a 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  $t/t_0 = 0.95$ .



**Figure 1.4** Design errors in a earth symmetrical three-phase distribution system. In spite of short circuits to earth, the relay  $K$  must be able to be switched off, or (because the fuse  $F$  melts) must switch off. Earth faults may never switch on  $K$ .  $S_{on}$  is a normally open push contact for switching on,  $S_{off}$  a normally closed push contact for switching off.

a) Wrong design. Before switching on, earth fault 2 can switch on  $K$  without a command. After switching on, earth faults 1 and 2 cause  $K$  to be unable to be switched off.

b) Good design. Both, before and after switching on, earth faults cannot lead to an undesired switching on or a refusal to switch off.

- The application of derating. Derating is the reduction of the operational and the environmental stress to which the components of a system are exposed. The components here are operated well below their maximum ratings by using more components to share the load or by utilising other stress derating measures. As long as the stress probability density function encountered in practical use and the strength probability density function of a component coming from the manufacturing line still overlap, derating will give an improvement. We will return to this matter in Section 5.2.
- The thorough testing of the system prototypes for unreliability and the interim inspection of the systems for flaws during production.
- The introduction of a burn-in period to trace early failures by running the system for a period of time, possibly under increased stress. This will be treated further in Section 2.3.
- The conduction of life tests resulting in failure-rate data which can be used to adjust the initial design. More failure-rate data are obtained from the field in a later phase and should be reported back to the designer. These actual data are used for validity studies of the life tests which have been conducted and for use in later designs or design updates.

- The use of redundancy. Incorporating redundancy into a system is providing alternative means for the realisation of the required system functions when the primary means have failed. To avoid dependent errors, the redundant (sub)systems should preferably realise the required function in a different way than the primary (sub)systems. They should consist of different components and be made by different manufacturers. If the reliability of the primary (sub)systems is higher, the redundant system connected in parallel has a greater effect, i.e. the reliability of the combination is increased to a greater extent. Because of this, redundancy should be used in the system at a hierarchical level that is as low as possible, so preferably at component level (see Section 6.3).
- The introduction of preventive maintenance where this is possible. Preventive maintenance aims to avoid system breakdown. Because preventive maintenance is usually conducted according to a predetermined plan, the costs are lower than those of corrective maintenance (repairs). Also, the costs resulting from an unscheduled stop of the system due to a sudden breakdown are reduced. However, preventive maintenance is not useful in all systems. Moreover, some corrective maintenance will always be necessary (see Chapter 7).
- The establishment of an organisational structure aimed at designing, developing, producing, and maintaining a reliable product. The principal management aspects involved here are organisation, training, logistics and coordination of manpower and means, etc.

## Problems

- 1.1. What are the essential elements in the reliability definition?
- 1.2. Why will a uniform filament of a light bulb with power supplied by a constant voltage source never fail?
- 1.3. What is your conclusion for a uniform filament in an incandescent lamp whose power is supplied by a constant current source?
- 1.4. Why is the allowed temperature range in Table 1.1 lower under operational conditions than under storage conditions?
- 1.5. What is meant by 'deterministic reliability engineering'?
- 1.6. Explain why a well thought through organisation is indispensable to realise a reliable product.
- 1.7. What kinds of environmental elements might have an influence on the ageing process of electronic integrated circuits?