Reliability and Maintainability in Perspective

Practical, contractual, commercial and software aspects

David J Smith
B.Sc.,C.Eng, F.I.E.E., F.I.Q.A.

Second Edition

Reliability and Maintainability in Perspective

Practical, contractual, commercial and software aspects

David J Smith
B.Sc.,C.Eng, F.I.E.E., F.I.Q.A

Second Edition

MACMILLAN

First edition 1981
Second edition 1985

Published by
Higher and Further Education Division
MACMILLAN PUBLISHERS LTD
Houndmills, Basingstoke, Hampshire RG21 2XS
and London
Companies and representatives
throughout the world

Printed in Hong Kong

British Library Cataloguing in Publication Data
Smith, David J.
Reliability and maintainability in perspective: practical, contractual, commercial & software aspects.
1. Electronic apparatus and appliances—Reliability 2. Maintainability (Engineering)
I. Title
621.381'042 TK7870

ISBN 0-333-39116-0
ISBN 0-333-39117-9 Pbk

Also by the same author

Reliability Engineering, Pitman, 1972
Maintainability Engineering, Pitman, 1973 (with A. H. Babb)
Statistics Workshop, Technis, 1974

Introduction to the Second Edition

It is the combination of Reliability and Maintainability which dictates the proportion of time that any equipment will be available for use. The two key parameters are Failure Rate and Down Time and they determine the user's failure costs in operating the product. For the manufacturer they will determine the cost of warranty and redesign, and also influence his prestige in the market place. A single defect can cost £50 in diagnosis and replacement if detected in the factory, while the same fault in the field will cost upwards of £200 to rectify. An hour of down time of a communications link can represent a lost revenue of at least £1000 whereas a spurious fire alarm on an oil production platform may cost 100 times that figure in lost production. This book emphasises the importance of setting realistic targets which lead to savings in excess of the design costs involved.

Reliability and Maintainability clauses in contracts for both system design and for off the shelf products are now commonplace. In the defence, telecommunications and aerospace fields these requirements have been specified for many years. More recently, contracts for equipment in the oil and gas industry have tended to stipulate reliability and repair requirements. Chapters 18 and 19 are devoted to contractual and legal topics.

Admittedly, defects can be 'inspected out', albeit at an unrealistic cost, but failure-free performance can result only from inherent reliability in design. It cannot be over-stated that satisfying such requirements is largely a matter of good engineering practice and the application of formal controls in design, manufacturing and service. The major part of this book deals with quantifying and achieving Reliability and ease of repair.

Computers have now entered every field and reliability is no exception. This book discusses the areas where computers can be used as reliability design aids. The increasing use of computer control in the form of microprocessors, now used in products from washing machines to petrol pumps, from telephone switching to motor vehicles, brings the possibility of failure due to the unforeseen behaviour of the software. Chapter 21 is devoted to the techniques used to minimise software-related failures.

The mathematical aspects of the subject, although important, do not themselves create more reliable or more easily maintained products. Too often the author has had to discourage efforts to refine reliability predictions and precisely define failure rates when an order of magnitude estimate would have sufficed. In all areas

of engineering the ability to recognise the degree of accuracy required is of the essence. Chapter 15 provides all the theory necessary for reliability prediction and the use of suitable approximations where appropriate.

Since we are dealing with engineering parameters a practical, cost-related, approach is essential. There is a cost to achieve any parameter as well as a cost associated with each failure. The aim is to select and to achieve levels of failure rate and repair time which keep the total of these costs at a minimum. Only in this way can reliability justify its place in the spectrum of activities.

A feature of this edition is the inclusion of a data bank (chapter 22) of failure rates for the full range of engineering and microelectronic components. In addition there are tables of human risks, human error rates and the percentage failure modes of components. The majority of the figures are expressed as ranges rather than single values.

The views and data expressed in this book are the result of the author's 20 years experience in industry and do not represent the opinions or data of any one organisation.

Acknowledgements

I would particularly like to thank the following friends and colleagues for their patient help and encouragement with this second edition.

My very good friend Len Nohre for his meticulous checking of the revised manuscript and for his many helpful suggestions.

My friend and colleague John Catchpole for checking the manuscript and for suggesting some useful additions.

Tony Fisher, of Field Fisher & Martineau, for his astute comments and help with revising the legal and contractual chapters.

Alex Babb, co-author of *Maintainability Engineering* (Pitman, 1973), for permission to quote freely from those pages.

George Knight with whom I have enjoyed numerous stimulating conversations on the subject.

My dear wife, Margaret, who has much to contend with.

I would also like to thank the Civil Aviation Authority and ITT Europe for permission to reproduce their failure report forms and the US Department of Defense for permission to quote from MIL Handbooks.

Contents

Part I

Understanding Terms, Parameters and Costs

Part I

Understanding Terms, Parameters and Costs

1 How Important are Reliability and Maintainability?

1.1 PAST AND PRESENT

Reference is often made in this type of literature to the spectacular reliability of many nineteenth-century engineering feats. Telford and Brunel indeed left a heritage of longstanding edifices such as the Menai and Clifton bridges. Fame is secured by their continued existence but history is remembered of the failures of their age. If, however, we concentrate on the success and seek to identify which characteristics of design or construction have given them a life span and freedom from failure far in excess of many twentieth-century products, then two important considerations arise.

Firstly it is necessary to examine the nature of the comparison. The reliability of a structure or assembly will be influenced by its complexity. The fewer sub-assemblies and the fewer types of material and component involved, then the greater is the likelihood of an inherently reliable product. The modern equipment and products which we so often condemn as unreliable are often comprised of thousands of piece parts, involving many different materials all of which interact within various tolerances. Telford and Brunel's structures, on the other hand, are less complex, comprising fewer types of material with relatively few well-proven modules.

Secondly we should consider the two most common methods of achieving reliability. They are:

DUPLICATION – The use of additional, redundant, parts whose individual failure does not cause the overall product to fail.

EXCESS STRENGTH – Deliberate design to withstand stresses higher than are anticipated. Small increases in strength for a given anticipated stress result in substantial decreases in failure rate. This applies equally to mechanical and electrical items.

Although effective, both are costly methods of achieving high reliability and long life. The next chapter will emphasise that reliability and maintainability are cost related and that the cost of any improvement in failure rate or repair time must be paid for by a reduction in operating or service costs or by increased revenue resulting from less down time.

The nineteenth-century engineers may have been less prone to material cost constraints, or to the difficulties of equipment complexity, compared with

today's designers and that may account for many of the successes of that age. No doubt many ventures did involve new materials and methods and had to be implemented under severe cost constraints. Perhaps they are the ones which have not survived to complete the comparison.

The purpose of the foregoing remarks is to point out that reliability is a 'built in' feature of any construction, be it mechanical, structural or electrical, and that it can be increased by design effort or by the addition of material. It is clear that the cost of such enhancement must be offset by at least the equivalent saving in maintenance in order to justify it. Maintainability is a related feature which determines repair times by a number of design features and maintenance methods and which must also be justified on a cost basis in the same way as reliability. Reliability and Maintainability together, at a given cost, dictate the proportion of time which the user will be able to use the equipment. The cost of ownership therefore will be that initial cost together with the cost of repair and the cost of lost usage resulting from the failures. It will be a recurring theme in this book that minimising the total is the basis of reliability and maintainability engineering. It should be borne in mind that achieving Reliability by the use of redundant techniques carries with it the penalty of additional maintenance at the subsystem level.

1.2 REASONS FOR INTEREST

The substantial increase in importance attached to this subject over the last two decades is due partly to the dramatic increase in maintenance costs and partly to the difficulties inherent in complex equipment involving rapidly changing technologies. The following headings highlight the major reasons for this interest.

COMPLEXITY – Gives rise to intrinsic failures. These are failures not resulting from the clearly definable failure of a component part. They result from a combination of drift conditions or from unforeseen characteristics of software. They are hence more difficult to diagnose and less likely to be foreseen by the designer.

Results in a much larger number of possible failure modes. The number of ways in which an equipment failure may be caused is much greater in complex equipment, thus making the task of prediction more prone to error.

MASS PRODUCTION – Requires a much higher degree of control over Material Procurement, Manufacture and Assembly, Engineering Changes and Concessions, etc. This type of production, with the division of labour involved, requires sophisticated systems of control and good Quality Assurance techniques in order to prevent manufacturing-related failures.

COST AND TOLERANCES – It is necessary to design to a production cost objective and (for commercial reasons) this is often a severe restriction. This leads to the calculation of tolerance and stress margins which will just meet the requirement. The probability of tolerance-related failures in the field is thus increased.

Testing is now expensive and complex. Electronic test equipment can cost up to £200 000 and test programming labour is costly. The temptation to prune testing costs is often the cause of later failures.

MAINTENANCE – Field diagnosis and repair costs are much greater than those incurred in the factory. As a result reductions in failure rate and in repair time justify a reasonable investment.

High complexity leads to the possibility of the maintenance activities themselves inducing failures as a result of faulty test equipment or human error.

1.3 ACTIVITIES INVOLVED

The achievement of reliability and maintainability results from activities in three main areas:

DESIGN – Reduction in complexity. Use of standard proven methods.

Duplication of modules to increase fault tolerance.

Derating. This is the practice of using components of a higher stress rating than the minimum requirement.

Prototype Testing sometimes called Qualification Testing.

Subsequent feedback of all failure information into the design.

MANUFACTURE – Control of Materials, Methods, Changes, etc.

Control of work standards (e.g. welding and the forming of electrical connections). This has a direct effect on failure rate.

FIELD SERVICE – Adequate Operating and Maintenance Instructions.

Use of Preventive Maintenance including the elimination of Dormant Faults.

Feedback of accurate failure information to design and manufacture (see chapter 11).

Replacement Strategy. This may involve replacing items after a specific time as a result of a known wearout characteristic.

The achievement of reliability and maintainability requirements involves, as can be seen from the above list, a wide spectrum of management and engineering activities. It should already be clear that they cannot be added after design and manufacture by enhanced inspection and test but must be inherent in the design. These parameters are part of the specification defining a product and can no more easily be added later than can power consumption, weight, signal to noise ratio or any other feature. In the event that this becomes necessary the cost is usually prohibitive. No amount of MTBF (Mean Time Between Failures) calculations or speculation, nor the use of more favourable figures, will ever enhance reliability. The quest for more detailed failure rate information and its application to reliability prediction is known as 'The Numbers Game'. It has its place in reliability and maintainability engineering but is no more or less than a tool to be used in a wider range of activities. Actual improvements are achieved only by