

Reliability of systems, equipment and components —

Part 4: Guide to the specification of dependability requirements

ICS 03.120.10; 21.020; 29.020

Committees responsible for this British Standard

The preparation of this British Standard was entrusted to Technical Committee, DS/1, Dependability and terotechnology, upon which the following bodies were represented:

- AIRMIC
- Association for Project Management
- Association of Consulting Engineers
- BSS — British Standards Society
- BT Plc — British Telecommunications Plc
- British Railways Board
- Chartered Institution of Building Services
- City University
- Civil Aviation Authority
- Consumer Policy Committee of BSI
- Cranfield University
- Defence Manufacturers Association
- GAMBICA
- HSE — Health and Safety Executive
- IEE — Institution of Electrical Engineers
- Institute of Logistics
- Institute of Quality Assurance
- Institute of Risk Management
- Institute of Value Management
- Institution of Chemical Engineers
- Institution of Mechanical Engineers
- Intellect
- London Underground Ltd.
- MOD — UK Defence Standardization
- Strategic Rail Authority
- Safety and Reliability Society
- Society of Motor Manufacturers and Traders Limited
- Society of Environmental Engineers
- United Kingdom CALS Industry Council
- West Midlands Enterprise Board

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 29 July 2003

© BSI 29 July 2003

Amendments issued since publication

Amd. No.	Date	Comments

First published September 1986

The following BSI references relate to the work on this British Standard:
Committee reference DS/1
Draft for comment 03/101534 DC

ISBN 0 580 42266 6

Contents

	Page
Committees responsible	Inside front cover
Foreword	ii
Introduction	1
1 Scope	1
2 Normative references	2
3 Terms and definitions	2
4 General considerations for dependability specifications	3
5 Requirements for dependability management	9
6 Availability	10
7 Reliability	12
8 Maintainability	15
9 Maintenance support	16
Annex A (informative) Reference standards for assurance techniques	18
Bibliography	21
Figure 1 — Relationship between cost and reliability	3
Figure 2 — System elements	4
Table A.1 — Techniques for dependability assurance through testing	18
Table A.2 — Techniques for dependability assurance through analysis	20

Foreword

This part of BS 5760 was prepared by Technical Committee DS/1. It supersedes BS 5760-4:1986 and BS 5760-20:1997, which are both withdrawn.

BS 5760-4 was originally published in 1986, and confirmed in 1993, and BS 5760-20:1997, a dual-numbered IEC standard, was published to compliment it. In producing this latest version, the technical content of its predecessors has been combined, thoroughly updated, and re-structured to conform to the requirements of BS 0-3:1997. Terms and definitions have been checked to ensure that they align with current relevant standards, and all cross-references have been updated, removing those that are no longer current.

This British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This documents comprises a front cover, an inside front cover, pages i and ii, pages 1 to 23 and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

Introduction

In many systems, reliability, maintainability and availability are essential performance characteristics. These characteristics, together with maintenance support performance, are known collectively as dependability.

In systems where any of the dependability characteristics are important, it is necessary that these characteristics should be defined and specified in the same way as other system characteristics such as technical performance, dimensions and mass.

The levels of reliability, maintainability, availability and maintenance support performance achieved by a system depend on the conditions under which the system is used. When requirements for dependability characteristics are specified, it is necessary to define the conditions of storage, transportation, installation and use that will be applied to the system. It may be important to take account not only of the conditions under which the system will operate, but also of the maintenance policy and organization for maintenance support of the system.

In order to assess the values of the dependability characteristics achieved, it is necessary to use statistical methods.

Dependability characteristics may be specified, like other performance characteristics, in three types of specifications.

- Specifications produced by the supplier:

these are mainly used for systems that need to have certain dependability characteristics, e.g. reliability, in order to be accepted in the market place.

- Specifications produced by the purchaser:

these are mainly used for standard systems that have to meet certain dependability characteristics in order to satisfy the purchaser's needs.

- Specifications mutually agreed or produced by the supplier and the purchaser:

these are normally used in the case of custom-made systems or alterations to an existing design.

This standard is applicable to all three types of specification.

1 Scope

This part of BS 5760 gives guidance on specifying the required dependability characteristics in system specifications, together with specifications of procedures and criteria for assurance.

The guidance provided includes the following:

- advice on specifying quantitative and qualitative availability, reliability, maintainability and maintenance support requirements;

- advice to purchasers of a system to help them to ensure that the specified requirements will be fulfilled by suppliers;

- advice to suppliers to help them to meet purchaser requirements.

NOTE 1 Whilst mainly addressing system and equipment level reliability, many of the techniques described in the different parts of BS 5760 may also be applied at the component level. Further guidance on component reliability is given in BS CECC 00804:1996.

NOTE 2 This standard does not give guidance on the management of dependability programmes or on the various activities necessary to fulfil stated availability, reliability, maintainability and maintenance support requirements. For this general guidance, see other standards (see Annex A).

NOTE 3 Safety specifications are not considered in this guide.

NOTE 4 Guidance for the inclusion of reliability clauses in specifications for components (or parts) for electronic equipment is given in BS EN 61319.

NOTE 5 Specifications for the dependability of a service are not considered in this guide. This includes the provision of a service such as those provided through Public-Private Partnership procurements.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the reference cited applies. For undated references, the latest edition of the referenced document (including any amendments).

BS 4778-3.2, *Quality vocabulary — Part 3: Availability, reliability and maintainability terms — Section 3.2: Glossary of international terms*. (IEC 60050-191)

3 Terms and definitions

For the purposes of this part of BS 5760, the terms and definitions given in BS 4778-3.2 and the following apply.

NOTE Definitions of “dependability”, “availability (performance)”, “reliability (performance)”, “maintainability (performance)”, “maintenance support”, “failure”, “fault”, “(reliability and maintainability) assurance”, “item”, “time to failure”, and “operating time between failure” are given in BS 4332-3.2.

3.1 verification

confirmation by examination and provision of objective evidence that the requirements have been fulfilled

NOTE 1 Adapted from BS EN 61508-3:2002, **3.8.1**, by excluding some of the notes.

NOTE 2 In the context of this standard, verification is the activity of demonstrating for each phase of the relevant life cycle, by analysis and/or tests, that, for the specific inputs, the deliverables meet in all respects the objectives and requirements set for the specific phase.

NOTE 3 Example verification activities include:

- reviews on outputs (documents from all phases of the life cycle) to ensure compliance with the objectives and requirements of the phase, taking into account the specific inputs to that phase;
- design reviews;
- tests performed on the designed systems to ensure that they perform according to their specification;
- integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together.

3.2 validation

confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

NOTE 1 Adapted from BS EN 61508-3:2002, **3.8.2**, by excluding some of the notes.

NOTE 2 Validation is the activity of demonstrating that the system under consideration, before or after installation, meets in all respects the requirements specification for that system. Therefore, for example, software validation means confirming by examination and provision of objective evidence that the software satisfies the software requirements specification.

3.3 confidence level

value of $(1 - \alpha)$ of the probability associated with a confidence interval or a statistical coverage interval

NOTE 1 $(1 - \alpha)$ is often expressed as a percentage.

NOTE 2 See also BS IEC 60605-4:2001 for a discussion on confidence intervals and their use.

NOTE 3 See BS ISO 3534-1:1993.

3.4 system

set of elements which interact according to a design, where an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software and human interaction

NOTE 1 A person can be part of a system.

NOTE 2 This definition is taken from BS EN 61508-4:2002, **3.3.1**.

4 General considerations for dependability specifications

4.1 The need for dependability

All systems exhibit some level of dependability, however often they might fail or require maintenance. However, if a system fails too often it might not be available to perform when required or it might cost too much to maintain. In addition, systems that fail repeatedly will get a bad reputation with the user and are unlikely to be bought again once a replacement is required. On the other hand, designing and manufacturing systems with high levels of reliability is costly and it may not be possible to produce such a system at an economical price. There is, therefore, a balance to be struck between low reliability systems that cost a lot to maintain and high reliability systems that are expensive to design and construct. This is demonstrated by Figure 1, which shows the costs of design and operation for systems of different reliability.

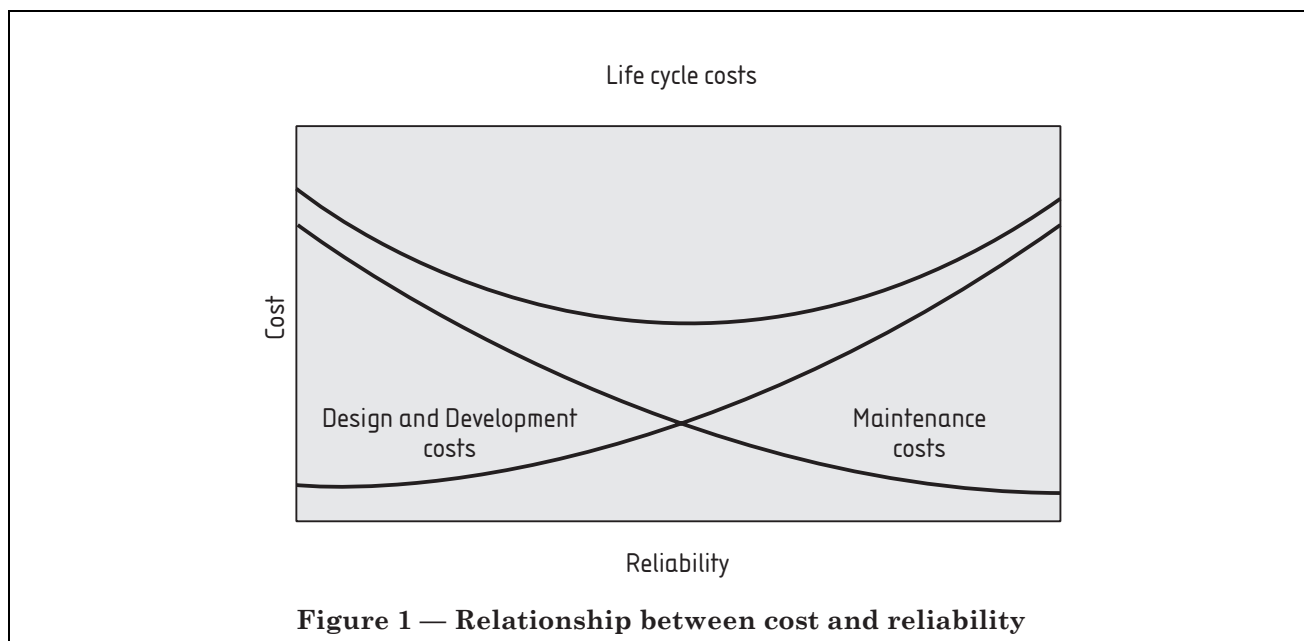


Figure 1 shows that there is an optimum level of reliability for which the costs over the lifetime of the system are minimized. It is probably true that systems produced by those organizations that do not actively manage dependability achieve levels of reliability much below this optimum point. An investment in dependability design and construction can therefore repay itself in terms of the combined development, construction and operating costs for the system.

Dependability includes a number of attributes that are specified differently. Within this standard, dependability has been considered under four headings, as follows:

- availability (A);
- reliability [$R(t)$], plus mean time to failure (MTTF) or mean time between failure (MTBF);
- maintainability, plus mean down time (MDT) and mean time to restore (MTTR);
- maintenance support.

The dependability characteristics selected for specification should be related to the type of system and the intended application. For example, only reliability requirements need to be specified if no maintenance actions are intended.

Maintainability performance requirements should be specified for equipment if the maintenance costs contribute significantly to life-cycle cost or if maintenance is important for the user. Preventive maintenance requirements may be specified, if applicable.

Availability performance requirements are generally specified for systems where down time could cause economic loss, through increased operating costs, or personnel injury, for example, large systems, production plants, medical equipment and safety equipment. Availability performance can be calculated from the system configuration, its subsystems and their reliability performance and maintainability performance requirements, if stated, and by taking into account the maintenance support performance.

The dependability specification should draw attention to the various factors likely to affect the cost of reliability and maintainability assurance. This includes the expected lifetime and disposal or recycling of the system.

NOTE The level of maintenance support is very often determined by the conditions of use and is not an intrinsic requirement of the system itself.

Clause 6, 7, 8 and 9 contain further information on when each of the dependability characteristics would be the most appropriate.

The levels of dependability performance achieved by a system are strongly influenced by the conditions in which it is designed, developed, installed and operated. Dependability is therefore related to other attributes such as quality and the design and manufacturing process. The dependability specification therefore should be part of the total system specification and the interaction between the different attributes recognized and taken into account.

4.2 Requirements and targets or goals

It is important to distinguish between requirements in a specification and targets or goals, as the contractual basis is different.

A requirement is part of the specification that the purchaser considers is essential that the system meets and for which the supplier has to provide assurance. A target or goal is not a requirement but is desirable and assurance either need not or cannot be provided.

For high availability or reliability systems, it might not be practicable to provide formal assurance of the high level of availability or reliability desired. The purchaser will need to provide both the high availability and reliability targets, for which assurance cannot be provided, and lower requirements for which assurance can be provided and make it clear which is which.

4.3 Systems

The specification of dependability should be at the system level. A system includes the equipment (both hardware and software) as well as the humans who operate and maintain the system and the procedures by which they operate and maintain it. The system also includes the environment in which the system operates, as shown in Figure 2.

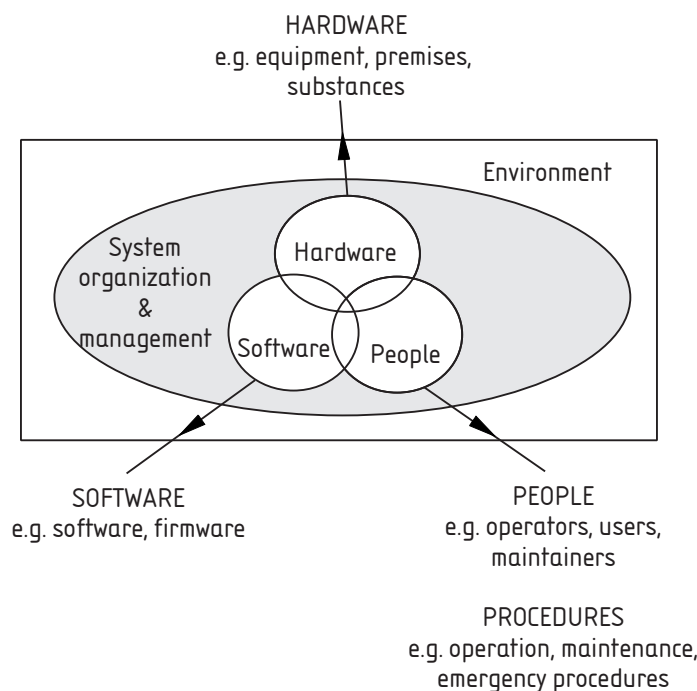


Figure 2 — System elements

All elements of a system have to be included in a dependability specification as a change in any one can have a significant effect upon the achieved dependability of the system. For example, different operators of a system can abuse it and lead to more failures and therefore achieve lower reliability.

Systems occur at many levels and any system may itself be made up of other systems, often referred to as a system of systems. For example, a motor car is a system that includes the motor vehicle, the driver and the driving procedures. The motor vehicle is made up of subsystems that are themselves systems, for example the engine or gearbox, where the human input to the gearbox involves the operation of the gearlever. The subsystems are made up of components, equipment and items that can themselves be considered as systems and analysed accordingly, i.e. considering the interaction of the people who use them and how they do so.

The purchaser might set dependability specifications only at the highest level of system or might decide that it is important that the one of the subsystems does not dominate the achieved reliability, and therefore also set specifications at lower levels. These lower level specifications have to be consistent with the top-level specification and they have to be measurable and achievable, or they will be targets and not requirements. For example, the contribution of the subsystem to the overall system dependability has to be estimated before the requirements can be apportioned to the subsystems. In a simple series system, i.e. one without redundancy, the system failure rate is the sum of the subsystem failure rates (assumed constant with time). BS 5760-2 and BS EN 61703 give further guidance on the analysis of system dependability.

The type and nature of a system will affect the dependability specification. These include repairable and non-repairable systems and one-shot devices. Repairable systems cover those where failures can be repaired and the system returned to a good-as-new state. Examples of non-repairable systems include sealed items, those where the cost of repair outweighs the cost of replacement, such as many consumer goods, and those at remote locations where the skills and spares are not available for the time at risk. One-shot devices include explosives, passenger air-bags and safety helmets.

Non-repairable systems have to be replaced rather than repaired and the maintainability and maintenance support requirements will be fundamentally different. Also, MTBF will not be a relevant parameter for one-shot devices, where the correct parameter would be reliability for the probability that the system works when required and MTTF for premature activation. The purchaser has to ensure that they identify the nature of the system and the effect that this can have upon the dependability requirements before the specification is written.

4.4 Assurance

4.4.1 *Concept of assurance*

There are two elements to any specification; the performance requirements and the means by which the supplier is to demonstrate the achievement of the requirements to the purchaser, usually known as assurance. The definition of assurance is given as “the implementation of adequate planned and systematic actions necessary to provide confidence that an item will satisfy given reliability performance and maintainability performance requirements”. In reality this means that the supplier has to provide sufficient evidence to the purchaser that the system meets its requirements to give the purchaser the confidence needed to pay the agreed cost. Additional assurance costs money and is one element in the higher cost of higher reliability systems (see Figure 1) but, without assurance activities, there is the possibility that the system will not meet its requirements.

There are two main elements to assurance; verification and validation. These are used particularly in the software industry as part of the software development process or “v-model” (see BS EN 61508-3). Verification is the process of providing assurance that the system, at any life cycle phase meets its requirements from the previous phase(s). Validation is the process of providing assurance that the system meets the actual requirements, which might not always be reflected in the written specification. Both are essential elements of assurance.

The level of assurance required by the purchaser depends upon the level of business or project risk that the purchaser is willing to accept. If the purchaser is willing to maintain a system when it fails in use, then they could be willing to accept a lower level of assurance than if they want to produce a high-reliability system that rarely fails. However, higher levels of assurance cost money to provide and the purchaser has to take a balanced decision on the risks that they are willing to accept when specifying assurance requirements (see BS IEC 62198:2001 and BS 6079-3:2000 for further information on project risk management).