Reliability of systems, equipment and components —

Part 4: Guide to the specification of dependability requirements

ICS 03.120.10; 21.020; 29.020

British Standards

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

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

Amendments issued since publication

Amd. No.	Date	Comments

Contents

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 It supersedes BS 5760-4:1986 and BS 5760-20:1997, which are both withdrawn.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that they align with current relevant standards, and all cross-references have been updated, removing those that are no longer current.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.

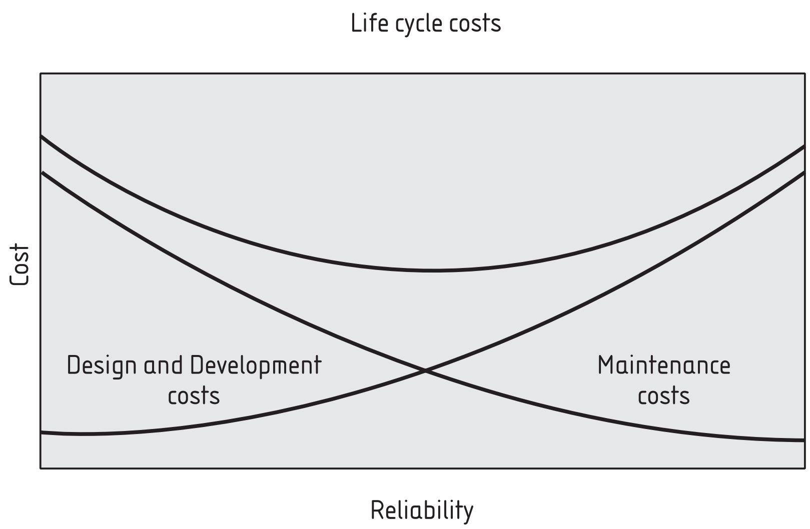

Figure 1 — Relationship between cost and reliability

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.

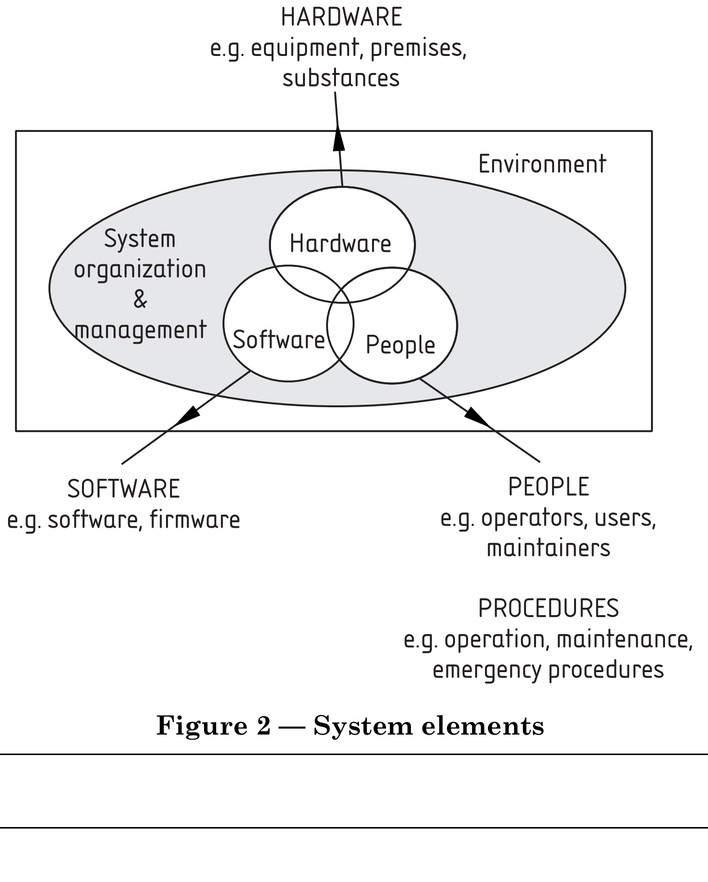

Figure 2 — System elements

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).

The definition of assurance states that assurance has to be planned and systematic. This requires the supplier to state the assurance activities in advance and to obtain agreement from the purchaser, usually through the contract.

For a long timescale procurement, activities might be planned many years before completion and, depending upon the contractual terms, the purchaser might have little control over the assurance until the end of the project. One way to reduce both the purchaser's and supplier's project risk that the system will not be able to provide the level of assurance required is the through the provision of progressive assurance. This means that assurance activities are planned throughout the life cycle and the results provided to the purchaser at project milestones. In this way the purchaser builds up confidence in the system throughout the project and there is a much-reduced risk that the level of assurance will be inadequate.

One model that is used for the supplier to provide assurance to the purchaser is the Reliability and Maintainability Case (usually known as the R&M Case). The R&M Case provides a reasoned, auditable argument that the system has met its requirements, is summarized at project milestones in the R&M Case Report and is similar in concept to a Safety Case, which is widely used in the safety industry. The R&M Case is usually used to provide progressive assurance and will be issued at a number of project milestones. UK Defence Standard 00-42 Part 3 [1] contains further guidance on the application of the R&M Case philosophy.

4.4.2 ***Assurance activities***

Assurance covers a number of activities designed to provide the evidence that a system is meeting its dependability requirements. These activities may be achieved through different techniques, which have the same or similar overall aim but use different methods to achieve it. An example would be that the performance of dependability analysis is an activity that provides an estimate of the likely reliability or availability that may be achieved by the system. This activity could make use of techniques such as fault tree analysis (FTA), failure mode and effects analysis (FMEA), etc. with the choice of technique depending upon a number of factors.

Where the purchaser requires assurance to be provided, the supplier has to determine the purpose of the activity and its contribution to assurance. For example, a specification should not require an FTA to be performed but should call up analysis to determine the combinations of events that could lead to system failure, as a reliability block diagram (RBD) could be an equally valid technique to achieve the same aim. The choice of technique to complete an activity should be at the discretion of the supplier, but considering such factors as the experience of the analyst, the time available and the data and information requirements. For example, an RBD performed by a knowledgeable analyst would be preferable to a badly completed FTA from an inexperienced analyst.

Assurance activities include:

a) testing and demonstration:
   1) performance in previous usage, for identical or similar items in identical or similar applications;
   2) dedicated dependability testing, including:
      i) reliability demonstration tests, including fixed time tests and sequential tests;
      ii) availability demonstration tests;
   3) other development testing (e.g. performance, fatigue life, software);

b) analysis:
   1) compliance with standards, regulations and guidelines;
   2) expert review/best practice/certification;
   3) design calculations (e.g. finite element analysis for stress, fatigue);
   4) simulation (e.g. of system performance);
   5) dedicated dependability analysis.

Further details of the dependability assurance techniques that can be found in other parts of BS 5760 and IEC standards are given in Annex A.

These assurance activities are not all appropriate at all life cycle phases. Testing cannot be carried out until the system has been designed and a prototype built. Similarly, analysis activities are more appropriate during the design stages to allow the exploration of the effects of different options upon the estimated dependability.

It should be noted that all assurance provided during development is a prediction of the likely dependability performance. The environment and usage of the system therefore have to be as close to that expected in-service as possible, to ensure that the estimated dependability is as accurate as possible.

4.5 Contracting for dependability

The purpose of any specification is to provide a basis for a purchaser to purchase the system from a supplier. It will usually form part of the contract between the purchaser and supplier and therefore it is essential that the specification is written in such a way that it can be used for contracting. Contracting for dependability can take many forms, from milestone payments dependent upon the successful completion of a demonstration test to the use of penalty clauses and incentives for in-service achieved reliability.

When writing dependability clauses for contracts, great care has to be taken that the clauses are meaningful and can be contracted for. For example, a clause in a contract for a surface to air missile called up a requirement for 99.5 % reliability. The contract also required a full reliability demonstration test at 80 % confidence levels. This would have necessitated a minimum of 322 missile firings, or in excess of six times the expected purchase of 50 missiles. Since the missile was designed to be a one-shot device, this was clearly a nonsensical specification and the purchaser had to find alternative methods of achieving the assurance required, through the use of lower reliability targets for which assurance could be provided, analysis, simulation and subsystem testing.

The choice of which assurance activities to call up in a contract is dependent upon the level of project risk that the purchaser is willing to accept. If the purchaser is willing to take the risk that the system might fail but be maintained by the supplier, then the use of penalties for poor performance and incentives for exceeding the requirements might be the best method. If, however, the purchaser is not willing to risk unavailability of the system, then formal reliability or availability demonstration testing might be necessary.

The benefits of each type of approach are as follows.

a) Penalties for poor performance will encourage the supplier to give dependability its full attention and can lead to higher levels than otherwise.

b) Demonstration testing is costly and time-consuming and might only reveal, just before the in-service date, that the system does not meet its dependability requirements.

c) Requiring the supplier to provide maintenance requires a much longer contract, with its associated difficulties but the supplier takes the risk that the system achieves poor reliability.

If a dependability specification is to be used as the basis for contracting, it is essential that the specification is fully defined, so as to prevent disagreements once the contract is used. Examples of the types of elements that have to be included in a specification that is used for contracting are as follows.

— The precise and clearly defined criteria by which reliability, maintainability or availability are to be judged.

— The definition of failure, i.e. total failure of the system to provide any functions, failure to provide essential functions, partial failure or any component failure. In addition, it is important to define exactly what constitutes a system fault, if necessary, by reference to a detailed performance specification.

— Accept/reject criteria for any testing provided as part of assurance.

— Acceptable data sources to be used in any analytical techniques.

— The system under consideration, for example the system, equipment or assembly to which the requirements apply.

4.6 Types of specification

The nature of the system being procured has a fundamental effect upon the manner in which the specification is written. There are three main types.

— Specifications produced by the supplier:

these are mainly used for systems that need to have certain dependability characteristics, for example 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.

Bespoke systems are where the purchaser specifies what is required and the supplier designs, develops and produces a system solely to meet that specification. If, however, the supplier states what is available and the purchaser chooses what best meets their requirements, this is known as commercial off the shelf (COTS). In this case, there are no changes to the standard commercially available system. In practice, most major procurements will be a combination of both bespoke and off the shelf elements and the specification will be mutually agreed between the purchaser and supplier.

Examples of a bespoke system would be a military purchase of a main battle tank (where each subsystem is used only on military vehicles), nuclear power stations and the London Eye. Examples of COTS systems include domestic washing machines and office IT systems.

For a bespoke system, the purchaser will specify the level and types of assurance that the supplier has to provide to demonstrate that the requirements have been met. This assurance will include testing and analytical evidence but, as the system is being built solely for the purchaser, cannot include evidence from the use of the system in the in-service environment, except after purchase. The supplier then includes the cost of that assurance in the quoted price for the system and the purchaser can determine the assurance required, in accordance with the business risks they are prepared to take. However, the purchaser will know that the system is being designed and developed to meet the requirements.

For a COTS system, the supplier states what is available and may provide standard assurance that the system meets certain levels of performance, which may include in-service data from previous applications. However, there is limited opportunity to provide assurance and many suppliers will be unwilling to provide in-service data that they consider commercially sensitive.

As a result of the reduced development effort and level of assurance activities, the costs of COTS systems are much less than that of bespoke systems. It is for this reason that many purchasers are now stating that they want to meet their requirements through the use of COTS systems, accepting that such a system may not meet the requirements exactly.

For small levels of modification, the type of procurement is often known as modified off the shelf (MOTS). However, if the purchaser requires any changes to the off-the-shelf system, then it cannot be considered a COTS system, as the changes might have a significant effect upon the achieved dependability. The purchaser, therefore, has to take care that a COTS system really is the same as the commercial system and that the assurance provided is adequate. If any changes are requested, the effect of these changes upon the dependability performance has to be considered in detail and additional assurance requested by the purchaser, if necessary.

4.7 Derivation of dependability specifications

All reliability, maintainability and availability requirements should be expressed quantitatively wherever possible, but it might also be appropriate to specify qualitative requirements in the specifications. Quantitative requirements are only appropriate when the requirement being specified can be measured during the assurance process. If the requirement cannot be measured during the assurance process then it is a target, and qualitative requirements will provide the basis for assurance.

Requirements also have to be achievable. All purchasers would like 100 % reliability from their systems but this is not achievable and neither is very high reliability, except at significant cost. The purchaser therefore has to assess what levels of the different dependability parameters are reasonable, based upon factors such as the achievement of previous similar systems, the operational need and consideration of whether an improvement can be expected. Current systems are becoming increasingly complex to meet operational needs and many have reached the limit of cost-effective reliability performance.

Data on past achievement is available from a number of sources, including:

a) supplier's own maintenance and servicing records;

b) generic data bases and data books;

c) manufacturer's data for subsystems and components.

When specifying all dependability parameters, it is important to state the following:

— the intended function of the system;

— how the system will be installed and used;

— the definition of fault, i.e. what constitutes a fault in this particular system in the intended application;

— the obligations and responsibilities of purchaser, supplier and any third parties;

— the various operating and environmental conditions under which the system is used including, where applicable, the relative amount of time spent in each condition;

— the methods intended to be applied for assurance of compliance with the requirements;

— the qualifications and responsibilities of the personnel responsible for operating and maintaining the equipment;

— the maintenance policy to be applied and the associated procedures and support arrangements.

5 Requirements for dependability management

This standard deals with the specification of dependability, through specification of one or more of availability performance, reliability performance, maintainability and maintenance support. These parameters are intrinsic characteristics of the system and assurance activities can demonstrate the likely levels of achievement. However, other factors can significantly reduce the achieved levels of these parameters below the intrinsic levels. The most significant is potentially the quality of manufacture and maintenance of the system that can introduce new faults into the system. It is, therefore, essential that dependability be actively managed throughout the system life cycle. This includes both during the procurement process and during use and the management activities required will be different for each. Poor management of dependability in either the procurement process or during use has a greater potential to reduce reliability or availability performance than a poor design or the use of sub-standard components.

BS 5750-14 and BS 5760-1 cover the management of dependability in detail and contain full details of activities and techniques for dependability management. These standards include details of the dependability life cycle. A product life cycle consists of the following phases:

— concept and definition;

— design and development;

— manufacturing;

— installation;

— operation and maintenance;

— disposal.

The life cycle of the system can have a significant effect upon the achieved dependability of the system. For example, poor handling and extended periods of storage can significantly reduce the reliability performance of a system. In addition, the dependability performance can differ through life, with most systems exhibiting increasing failure rate with life due to component or subsystem wear-out. This change in dependability performance with usage means that, for many systems, the constant failure rate assumption is not valid and different distributions, which require more complex mathematical expressions for estimating reliability performance, have to be used. BS EN 61703 gives further guidance.

A further factor that affects reliability performance is changes in system usage. For example, a vehicle that normally runs on the road will almost certainly fail more often when used off-road due to the different stresses and loads placed on the vehicle. Thus the system mission or usage is an essential part of the dependability specification and changes have to be monitored and managed as part of the dependability life cycle.

6 Availability

6.1 General

6.1.1 *Choice of dependability characteristic*

For some systems, particularly complex systems, it is necessary to consider redundancy and maintenance together. In such systems, it might be appropriate at the system level to specify availability requirements rather than separate reliability and maintainability requirements. It is important that the purchaser defines which of the availability definitions is being specified or there is a risk that the required level of availability performance will not be achieved. Requirements for the steady state availability are the most commonly used, although instantaneous or mean availability may also be appropriate.

Examples of industries where availability performance may be the prime dependability characteristic of interest include the rail industry, where the train operators require a percentage of the trains to be available for use during peak periods, and the telecommunications industry, where the operator requires a certain number of communication channels to be available and the diverse routeings available mean that some routes might be unavailable while the system maintains an overall availability.

Steady state availability is "the mean of the instantaneous availability under steady state conditions over a given time interval." For this definition of availability to be relevant, steady-state conditions have to exist but, if they do, the mathematics is simplified and it is therefore sometimes specified when not appropriate.

NOTE Under certain conditions, for instance constant failure rate and constant repair rate, the steady state availability may be expressed by the ratio of the mean up time to the sum of the mean up time and mean down time. Under these conditions, asymptotic and steady state availability are identical and are often simply referred to as "availability".

Instantaneous availability is the "probability that an item is in a state to perform a required function under given conditions at a given instant of time, assuming that the required external resources are provided." At any instant, this will be either 0 or 1, i.e. the system either will be available or unavailable and is unlikely to be specified in a dependability specification.

Mean availability is the "mean of the instantaneous availability over a given time interval (t_1, t_2)". This parameter is more useful for specification and is of interest in industries where the availability over different time intervals may change, perhaps due to different operating conditions.

Other definitions of availability also exist, such as operational availability (where logistic delays are included) and asymptotic availability (see BS 4778-3.2).

6.1.2 *Relationship between availability, reliability and maintainability*

Availability, reliability and maintainability are not independent parameters. As stated in **6.1.1**, for steady state availability with constant failure rate and constant repair rate the three parameters are linked as follows:

$$\text{Steady State Availability} = \frac{(\text{MTTF})}{(\text{MTTF}) + (\text{MDT})}$$

where

MTTF = mean time to failure;

MDT = mean down time.

All three parameters should not be specified as this will constrain the system performance. However, it is usual to specify two of the three parameters in order to ensure that the balance between up-time and down time is operationally acceptable. The same availability may be achieved through high levels of MTTF with long down times or alternatively lower MTTF but short down times. For example, personal computer operating systems can fail regularly but only take seconds to reboot and restart, giving an overall high availability. This is frustrating for the user but might be more acceptable than the same availability from a computer that only fails infrequently but then is not available for use for some days following failure. However, for telecommunications networks achieving availability through lower reliability with short down times might be unacceptable because they are not available for sufficient times for data to be transmitted.

6.2 Availability specifications

6.2.1 *Quantitative requirements*

Any availability specification has to define exactly what is meant by availability, i.e. which type of availability is being specified, and what times are included in down time, are logistic delays included or to what extent?

Requirements for availability can be expressed as a decimal fraction or as a percentage, for example, mean up time as a percentage of observation time. Availability requirements cover both the occurrence of failures and down time. If mean availability is being specified, the time period over which it is measured also has to be specified, together with other relevant time information. For example, if the mean availability for trains is being specified, this will include the mean availability measured over each hour between the hours of (say) 7 am and 10 am and 5 pm and 8 pm from Monday to Friday.

When specifying quantitative availability requirements, it is usual to accumulate the down times occurring over a certain time period (for example, a month or a year). If part of the system down time is excluded from the responsibility of the supplier (for example, logistic or administrative delay), this should be noted in the specification together with a statement of the values of the times concerned. Figure 191-10 in BS 4778-3.2:1991 gives guidance on the various maintenance times. Alternatively, an intrinsic availability may be specified, that is calculated by excluding such maintenance times.

6.2.2 *Qualitative requirements*

Quantitative availability specifications should be used if at all possible. Qualitative availability requirements should be specified only if the quantitative requirement does not specify the availability performance of the item with sufficient precision, for example, if downtime under certain operating conditions is more critical. However, the type of availability and the times included in downtime still have to be defined in the specification.

6.3 Availability assurance

6.3.1 *General*

The specification or contract should include the need for assurance of the required availability performance. Availability assurance is often provided through a combination of reliability and maintainability assurance, rather than directly.

6.3.2 *Assurance by testing*

Where assurance is to be carried out by testing, the standardized compliance test procedures for steady state availability given in BS 5760-10.3 may be applied. It should be noted, however, that for very high availability requirements (for example, >0.999 9), it is very difficult to establish a meaningful test plan. Evaluation and assurance of subsystem performance can assist in this activity. This can be achieved by using observations at system and subsystem level in a system availability model. In any case, the feasibility of the methods applied to assure high availability requirements needs to be proven.

For in-service or performance testing, a detailed field data collection program should be agreed in advance (see BS 5760-11), including down time due to hardware failures, software failures, maintenance procedures and other reasons. The performance of the test then has to be monitored and analysed as it progresses to provide the necessary assurance.

Furthermore, if more than one item of the same type of system is used during the test, the number of items and the period of observation should be taken into account. A procedure should be specified such that, in the event of non-compliance, an improvement is agreed and introduced and testing is continued. Care should be taken that the use of more than one item is statistically valid, as 100 hours of one item is only equivalent to one hour of 100 items if a number of factors taken into account and assumptions are true. These include the assumption of constant failure rate, the occurrence of early life or wear out failures and the degree of confidence that the samples used are representative of the system.

6.3.3 ***Assurance by analysis***

If assurance is to be carried out by analysis methods, the standardized prediction techniques given in BS 5760-2 and BS 5760-12 with detailed analysis methodology as specified in BS 5760-2 and BS IEC 60300-3-1 may be applied.

Generally, data for calculation should be based on recognized sources of data, results obtained from operational experience on similar equipments in the field, laboratory tests or from software/hardware integration. The data should be agreed between the supplier and the purchaser and the data source should be recorded.

7 Reliability

7.1 General

For some systems, it is necessary to consider directly the reliability of the system. In such systems, it might be appropriate at system level to specify separate reliability and maintainability requirements. Reliability is, by definition, the ability of a system to perform a required function under given conditions for a given time interval, that is without failure. It is most correctly described by a probability that the system can complete its required mission. However, many specifications will define the required reliability through the use of alternative parameters, such as mean time to failure or mean operating time between failure.

Examples of industries where reliability performance can be the prime dependability characteristic of interest include the aerospace industry, where once an aircraft has taken off it is essential that it completes the flight without failure, and the automotive industry, where the driver needs to reach the destination and can maintain the vehicle once at the destination.

Examples of where time to/between failure can be the required reliability parameter include electric light bulbs that are designed to a life. Other examples include process machinery, where the system is continuously operating and the time to failure is of importance to plan maintenance activities.

Care has to be taken by the purchaser that the appropriate reliability performance measure is specified and that the statistical implications of the specification are understood. For example, if a 99 % reliability over one year is specified, this can seem sensible. However, this equates to a MTBF of 871 613 h (or 99.499 years), if the failure rate is constant, which is high.

7.2 Reliability specification

7.2.1 ***Quantitative requirements***

Reliability performance requirements should be quantitative and should be specified before design of the system begins.

One early consideration is the failure mechanisms likely to be experienced by the system, as this will determine which of the reliability measures is appropriate and relevant. For example, motor vehicle engines fail according to how far they are driven rather than age since new, so that miles driven is the appropriate unit. They also wear-out so that the constant failure rate assumption is not valid. Electric light bulbs fail relative to the number of times they are switched on and off, and to a lesser extent the number of hours they are lit, so operations or operational hours are the appropriate units and the system is designed for a defined operational life. The inclusion, or not, of redundant elements is another factor that affects the choice of reliability measure.

For every system, it is necessary to select and define each reliability characteristic that is required and to specify a quantitative requirement for each characteristic. When specifying quantitative requirements for an item, it is important to state the following:

— the system's application;

— the definition of a fault, i.e. what constitutes a fault in the particular system in the intended application;

NOTE A fault may be defined in various ways according to the consequences, for example, the loss of a service, or the need for repair.

— the operating conditions;

— the environmental conditions;

— the methods intended to be applied for the assurance of compliance with the requirements.

Without such statements, the specification of a reliability performance measure such as MTTF, MTBF and R(t) would be meaningless.

When selecting the value of the reliability performance measure to be specified, the following factors should be taken into account:

— limits imposed by the technological state of the art and the nature and complexity of the system (equipment or system);

— the experience of the user in operating and maintaining the particular type of equipment;

— the feasibility of verifying the specified requirement;

— the reliability level of units, components, etc., from which the item can be manufactured;

— the cost of design, production and assurance of the item with a specified level of reliability.

If, during the development of a project, it becomes evident that the underlying assumptions are not valid, the reliability performance requirements might have to be reconsidered and changed. If the specification is to be changed, this should only be done with the agreement of all the parties concerned.

The quantitative requirements should be clearly specified in a form against which it will be possible to compare the results subsequently obtained.

Where assurance of conformity to the quantitative requirements is to be done through testing, the confidence level required should be specified, or the actual test plan to be used should be specified. If a test plan is specified, the specification should include the test duration and the acceptance/rejection criteria. A number of different types of reliability demonstration test exist and, all other things being equal, sequential probability ratio tests (see BS 5760-10.5) should be used in preference to fixed time or sample tests (see BS IEC 61124) as the former are more efficient.

If the specified reliability performance measure is known, or is likely to vary with time, the dependency should be specified by, for example, specifying a mean failure intensity over the first months of use. See BS IEC 60300-3-5 for information on statistical distributions.

7.2.2 *Qualitative requirements*

Qualitative reliability requirements may be expressed in terms of either or both of the following:

a) design criteria for the system;

b) reliability improvement activities to be applied during the system life cycle phases.

Design criteria for a system, such as the physical, performance and operational requirements, usually stand alone, but might also be complementary to quantitative reliability requirements. Such criteria can indirectly impose reliability requirements for the system itself and for the way the system is installed and its performance is monitored. Some examples are as follows:

— single fault criterion, i.e. the system has to be such that no single fault can lead to a critical state of the system;

— accumulating fault criterion, i.e. the system has to be such that no undetected fault, when combined with additional faults, can cause system failure;

— path separation, i.e. redundant subsystems have to be kept independent by using separate paths for cables, pipes, etc., for signalling channels, power supply and other supporting supplies;

— monitoring of critical functions, i.e. provision has to be made for automatic or manual checking of critical functions either continuously or at intervals, in order to maintain a specified level of reliability performance.

In addition to specifying quantitative reliability performance requirements, it might often be advisable to specify a sequence of reliability (and maintainability) improvement activities to be implemented during system life-cycle phases. Such qualitative requirements may be applied to hardware, software and support. These activities are particularly important if the quantitative requirements do not specify with sufficient precision the reliability performance of the system. They should be mutually agreed between purchaser and supplier, both technically and in terms of time schedule and cost. Such qualitative requirements should be formalized in and managed through a reliability programme plan (or dependability plan), as specified in BS 5760-1.

The reliability programme plan should be tailored according to the nature of the system and the requirements specified, and typically includes the following:

— the types of analysis methods to be applied;

— a reliability growth programme, if necessary;

— statements about how to verify conformity to the requirements (see BS IEC 60300-3-5) or any other qualitative or quantitative measure to be used for expressing the degree of conformity to the requirements;

— criteria for component selection and arrangements for quality assurance;

— worst case analysis.

7.3 Reliability assurance

7.3.1 *General*

The specification should state the methods to be used to provide assurance that the specified requirements have been met.

Reliability assurance may be done either by analysis during the design and before production, by laboratory tests or field tests after production or by field performance evaluation after delivery. In addition, assurance may be gained from other activities during the development process. Examples include design analysis (such as stress analysis), performance testing, software testing and operational simulations. Evidence may be collected from all sources to provide assurance and will complement dedicated reliability assurance activities.

7.3.2 *Assurance by testing*

Preferred methods of assurance by testing include:

a) the collection and analysis of failure data from systems in the field, i.e. in actual use;

b) testing systems in use or in the laboratory, using compliance or determination tests as described in BS 5760-10.5.

Precise criteria should be specified to enable all failures in hardware and software, etc. to be classified into relevant or non-relevant categories.

This classification is the basis of the acceptance/rejection criteria and it is essential that it should be clearly and precisely specified before the tests start.

Assurance procedures are normally selected by agreement between the purchaser and supplier from either field tests or laboratory tests, as follows.

— Tests in actual usage are often preferred, but their validity requires sufficient data collection. They may, however, be too late in the procurement process if high levels of assurance are required. See BS IEC 60300-3-5 and BS 5760-11 for the requirements to be stated.

— Laboratory tests should be conducted as described in BS IEC 60300-3-5. When specifying laboratory tests, it is important to consider the associated factors such as cost and time.

The assurance of reliability performance measures for repairable and non-repairable systems have each to be considered separately.

If success ratio is used as the reliability performance measure, the test should be carried out in accordance with BS 5760-10.5.

If reliability performance requirements are based on a constant failure rate or failure intensity assumption, an appropriate test plan in accordance with BS IEC 61124 should be selected. Tests for validation of this assumption can be found in BS IEC 60605-6 and have to be performed as the results of a test may be nullified if the assumption is incorrectly used.

7.3.3 *Assurance by analysis*

Reliability assurance of a system can be made prior to delivery by calculation based on reliability analysis. In some instances (for example systems having very high reliability), this can be the only practicable approach. Analysis can be used long before reliability validation during in-service operation or by laboratory testing is possible. Such a method can only determine by analysis whether the system to be delivered fulfils corresponding requirements laid down in the system specification; it does not measure the realized reliability directly.

Examples of analytical techniques for reliability assurance of an item such as a system with hardware and software include reliability block diagrams, fault trees, state diagrams and fault mode and effect analysis. See Annex A for standards that give guidance on various analysis tools.

The hardware element of a system should be analysed to establish that the failure rates of each of its subsystems, parts and electronic or other components take into account the expected usage and operational stress and that their derivation is appropriate and justifiable. Electrical, thermal or other measurements can be necessary for this purpose.

The software in the system should be similarly analysed to identify possible software fault modes and evaluate qualitatively their impact on the reliability performance of the system.

Data for such calculations can be based, for example, on results obtained from operational experience with similar equipment in the field, from laboratory tests, from software/hardware integration or from recognized data sources. If the purchaser intends to specify the use of a certain database (for example, a particular failure rate data bank), this should be agreed between the supplier and the purchaser. Specifying the use of a certain database, however, does not relieve the supplier of his obligation to achieve the required reliability performance. In all cases, the data source should be identified and recorded.

BS 5760-12 gives guidance on the presentation of reliability, maintainability and availability predictions.

8 Maintainability

8.1 General

Maintainability is not often the primary dependability parameter, but can be so in software projects or projects such as mid-life updates to correct low levels of achieved availability or systems at remote locations that are difficult to maintain. However, it will be a secondary parameter for many systems and, if specified incorrectly, can have a significant effect upon the achieved dependability, especially in systems containing redundancy.

8.2 Maintainability specification

BS 6548-1 contains full details of specifying and contracting for maintainability. It might be necessary for a specification to specify requirements for corrective and preventive maintenance separately as the maintenance support required can be very different.

Maintainability requirements may be quantitative or qualitative. Where quantitative requirements are specified, it is important to specify how long an item is expected to be in a non-operating state due to maintenance or maintenance support. This time has to be specified in terms of appropriate measures such as mean or x % repair time, or mean or y % logistic delay. Where qualitative requirements are specified, it is necessary to specify the degree to which an item has to conform to specific conditions and constraints related to maintenance.

A complete specification of maintainability performance requirements should cover four broad areas:

a) the maintainability performance to be achieved by the design of the item;

b) the constraints that will be placed on the use of the item which will affect maintenance;

c) the maintainability programme requirements to be accomplished by the supplier to assure that the delivered item has the required maintainability characteristics;

d) the provision of maintenance support planning.

When specifying maintainability requirements, it is important to state the following:

— the various operating and environmental conditions under which the equipment is used;

— the qualifications and responsibilities of the personnel responsible for operating and maintaining the equipment;

— the maintenance policy to be applied and the associated procedures and support arrangements;

— the spare parts to be provided and how they are estimated and managed.

The maintainability performance specification should detail the requirements and the method to be followed to achieve them. It should also include precise definitions of terms used in the specification with references to standard vocabularies as appropriate.

Maintainability requirements may be specified in the specification either as targets or as definite requirements that are to be verified in accordance with prescribed procedures. Targets or requirements may be specified in either quantitative or qualitative terms.

A maintainability performance specification typically covers the various aspects of maintainability achievement at the operational level. However, since maintainability performance as a system characteristic affects maintenance support costs and can also affect maintenance times at different maintenance levels, requirements should be included in the specification covering achievements at all levels affected by the maintenance policy.

More detailed guidance on maintainability performance requirements in specifications and contracts, is provided in BS 6548-1:1984, Section 2, Clause **6**.

8.3 Maintainability assurance

Much of the assurance of maintainability may be provided through other development testing or analysis. For example, reliability testing will provide data on the maintainability of the system, provided that the relevant data is collected. Therefore, all development trials and analyses should be examined to see if they could provide meaningful maintainability data, and such input built into the trial plan from the earliest opportunity.

Assurance of maintainability performance is the process of determining that the requirements in the specification have been met. The methods and procedures for assurance should be specified with the maintainability requirements. Methods of assurance may range from the submission by the supplier of appropriate data or information to a requirement to perform a special maintainability demonstration.

Maintainability assurance should be regarded as a continuous process. Maintainability related data should be generated, collected and evaluated as they become available in the course of project development, and the results should be compared constantly with specified maintainability requirements.

Several methods of verifying maintainability performance are described in BS 6548-3. They include the following:

— analysis and review of maintainability characteristics;

— special studies;

— demonstration tests (see BS 6548-6);

— review of operational experience.

The specification may give guidance on, or may specify which of the above methods is to be applied.

Further information on maintainability assurance is given in BS 6548-3:1992, Section **6**. Information concerning diagnostic testing is given in BS 6548-5 and statistical methods in maintainability evaluation in BS 6548-6.

9 Maintenance support

9.1 General

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

Maintenance support can be supplied fully or partly by the supplier or the purchaser of the system, depending upon the nature of the contract. The specification will therefore vary depending upon the source of maintenance support.

To the extent that the maintenance support is supplied by the supplier it should be specified as part of the delivery. Maintenance support by the purchaser (including the user) will be part of the specified conditions of operation of the equipment, a prerequisite for the stated reliability, availability and maintainability values.

9.2 Maintenance support specification

9.2.1 *Quantitative requirements*

Maintenance support requirements should, where possible, be specified in a quantitative way. Examples of such quantitative specifications are guaranteed response times, mean administrative delay, mean logistic delay and spare shortage probability and delay. Further information can be found in BS 6548-1 and BS 6548-6.

When specifying maintenance support requirements, it is important to state the following:

— the various operating and environmental conditions under which the equipment is used;

— the obligations and responsibilities of purchaser, supplier and third parties;

— the maintenance policy to be applied and the associated procedures and support arrangements;

— the qualifications and responsibilities of the personnel responsible for operating and maintaining the equipment.

The maintenance support specifications should be specified before design of the system begins and be updated before delivery of the equipment.

9.2.2 *Qualitative requirements*

Where maintenance support requirements cannot be specified quantitatively, qualitative requirements should be used as a supplement. However, as with all dependability characteristics, both quantitative and qualitative requirements may be specified. This can for example be specifications of the required training level and workmanship, standard of maintenance personnel or requirements for workshop facilities and tools to be available.

Further information can be found in BS 6548-1.

9.3 Maintenance support assurance

Assurance methods for maintenance support will be related closely to maintainability assurance and it is unlikely that they could be separated, as maintainability performance will depend upon the maintenance support available and no further information will be available. Other assurance will be qualitative evidence that the support is available and effective.

Annex A (informative)
Reference standards for assurance techniques

A.1 Techniques for dependability testing

Table A.1 shows reference standards for dependability assurance through testing.

Table A.1 — Techniques for dependability assurance through testing

Standard identifier	Standard title	Testing technique covered
BS 5760-10.3:1993	Reliability of systems, equipment and components. Guide to reliability testing. Compliance test procedures for steady-state availability	Availability demonstration
BS IEC 61124:1997	Reliability testing. Compliance tests for constant failure rate and constant failure intensity	Compliance test plans – constant failure rate
BS 5760-10.5:1993	Reliability of systems, equipment and components. Guide to reliability testing. Compliance test plans for success ratio	Compliance test plans – success ratio
BS 5760-11:1994	Reliability of systems, equipment and components. Collection of reliability, availability, maintainability and maintenance support data from the field	Dependability data collection
BS IEC 61710:2000	Power law model. Goodness-of-fit tests and estimation methods	Goodness of fit tests – power law model
BS IEC 61649:1997	Procedures for goodness-of-fit tests, confidence intervals and lower confidence limits for Weibull distributed data	Goodness of fit tests – Weibull distribution
BS 6548-3:1992	Maintainability of equipment. Guide to maintainability, verification and the collection, analysis and presentation of maintainability data	Maintainability data analysis
BS 6548-5:1995	Maintainability of equipment. Guide to diagnostic testing	Maintainability testing
BS 5760-6:1991	Reliability of systems, equipment and components. Guide to programmes for reliability growth	Reliability growth programmes
BS 5760-17:1995	Reliability of systems, equipment and components. Reliability growth. Statistical test and estimation methods	Reliability growth test and estimation methods
BS 5760-10.2:1995	Reliability of systems, equipment and components. Guide to reliability testing. Design of test cycles	Reliability testing – design of test cycles
BS EN 61709:2000	Electronic components. Reliability. Reference conditions for failure rates and stress models for conversion	Reliability testing – statistics
BS IEC 60300-3-5:2001	Dependability management. Application guide. Reliability test conditions and statistical test principles	Reliability testing – statistics
BS IEC 60605-4:2001	Equipment reliability testing. Statistical procedures for exponential distribution. Point estimates, confidence intervals, prediction intervals and tolerance intervals	Reliability testing – statistics
BS IEC 60605-6:1997	Equipment reliability testing. Tests for the validity of the constant failure rate or constant failure intensity assumptions	Reliability testing – statistics

Table A.1 — Techniques for dependability assurance through testing *(continued)*

Standard identifier	Standard title	Testing technique covered
BS IEC 61650:1997	Reliability data analysis techniques. Procedures for comparison of two constant failure rates and two constant failure (event) intensities	Reliability testing – statistics
BS 5760-13.1:1993	Reliability of systems, equipment and components. Guide to reliability test conditions for consumer equipment. Conditions providing a low degree of simulation for indoor portable equipment	Reliability testing for consumer equipment
BS 5760-13.2:1993	Reliability of systems, equipment and components. Guide to reliability test conditions for consumer equipment. Conditions providing a high degree of simulation for equipment for stationary use in weatherprotected locations	Reliability testing for consumer equipment
BS 5760-13.3:1993	Reliability of systems, equipment and components. Guide to reliability test conditions for consumer equipment. Conditions providing a low degree of simulation for equipment for stationary use in partially weatherprotected locations	Reliability testing for consumer equipment
BS 5760-13.4:1993	Reliability of systems, equipment and components. Guide to reliability test conditions for consumer equipment. Conditions providing a low degree of simulation for equipment for portable and non-stationary use	Reliability testing for consumer equipment
BS 5760-13.5:1996	Reliability of systems, equipment and components. Guide to reliability test conditions for consumer equipment. Ground mobile equipment. Low degree of simulation	Reliability testing for consumer equipment
BS 5760-13.6:1997	Reliability of systems, equipment and components. Guide to reliability test conditions for consumer equipment. Outdoor transportable equipment. Low degree of simulation	Reliability testing for consumer equipment
BS IEC 61163-2:1998	Reliability stress screening. Electronic components	Stress screening – electronic components
BS IEC 60300-3-7:1999	Dependability management. Application guide. Application guide. Reliability stress screening of electronic hardware	Stress screening – electronic hardware
BS 5760-16.1:1996	Reliability of systems, equipment and components. Guide to stress screening. Repairable items manufactured in lots	Stress screening – repairable items

A.2 Techniques for dependability analysis

Table A.2 shows reference standards for dependability assurance through analysis.

Table A.2 — Techniques for dependability assurance through analysis

Standard identifier	Standard title	Analysis technique covered
BS 5760-2:1994	Reliability of systems, equipment and components. Guide to the assessment of reliability	Overview of analysis techniques
BS 5760-5:1991	Reliability of systems, equipment and components. Guide to failure modes, effects and criticality analysis (FMEA and FMECA)	FMEA and FMECA
BS 5760-7:1991	Reliability of systems, equipment and components. Guide to fault tree analysis	Fault tree analysis
BS 5760-8:1998	Reliability of systems, equipment and components. Guide to assessment of reliability of systems containing software	Software
BS 5760-12:1993	Reliability of systems, equipment and components. Guide to the presentation of reliability, maintainability and availability predictions	Dependability predictions
BS 5760-14:1993	Reliability of systems, equipment and components. Guide to formal design review	Formal design review
BS 5760-15:1995	Reliability of systems, equipment and components. Guide to the application of Markov techniques	Markov techniques
BS EN 61078:1994	Reliability of systems, equipment and components. Guide to the block diagram technique	Reliability block diagrams
BS EN 61703:2002	Mathematical expressions for reliability, availability, maintainability and maintenance support terms	Mathematical expressions
BS 6548-6:1995	Maintainability of equipment. Guide to statistical methods in maintainability evaluation	Maintainability statistics
BS 6548-2:1992	Maintainability of equipment. Guide to maintainability studies during the design phase	Maintainability analysis
BS EN 61703:2002	Mathematical expressions for reliability, availability, maintainability and maintenance support terms	Dependability mathematics

Bibliography

Standards publications

BS 4778-3.2:1991, *Quality vocabulary — Part 3: Availability, reliability and maintainability terms — Section 3.2: Glossary of international terms.* (IEC 60050-191:1990).

BS 5750-14:1993, *Quality systems — Part 14: Guide to dependability programme management.* (EN 60300-1:1993, ISO 9000-4:1993, IEC 60300-1:1993).

BS 5760-1:1996, *Reliability of systems, equipment and components — Part 1: Dependability programme elements and tasks.* (EN 60300-2:1996, IEC 60300-2:1995).

BS 5760-2:1994, *Reliability of systems, equipment and components — Part 2: Guide to the assessment of reliability.*

BS 5760-5:1991, *Reliability of systems, equipment and components — Part 5: Guide to failure modes, effects and criticality analysis (FMEA and FMECA).*

BS 5760-6:1991, *Reliability of systems, equipment and components — Part 6: Guide to programmes for reliability growth.* (IEC 61014:1989).

BS 5760-7:1991, *Reliability of systems, equipment and components — Part 7: Guide to fault tree analysis.* (IEC 61025:1990).

BS 5760-8:1998, *Reliability of systems, equipment and components — Part 8: Guide to assessment of reliability of systems containing software.*

BS 5760-10.2:1995, *Reliability of systems, equipment and components — Part 10: Guide to reliability testing — Section 10.2: Design of test cycles.* (IEC 60605-2:1994).

BS 5760-10.3:1993, *Reliability of systems, equipment and components — Part 10: Guide to reliability testing — Section 10.3: Compliance test procedures for steady-state availability.* (IEC 61070:1991).

BS 5760-10.5:1993, *Reliability of systems, equipment and components — Part 10: Guide to reliability testing — Section 10.5: Compliance test plans for success ratio.* (IEC 61123:1991).

BS 5760-11:1994, *Reliability of systems, equipment and components — Part 11: Collection of reliability, availability, maintainability and maintenance support data from the field.* (IEC 60300-3-2:1993).

BS 5760-12:1993, *Reliability of systems, equipment and components — Part 12: Guide to the presentation of reliability, maintainability and availability predictions.* (IEC 60863:1986).

BS 5760-13.1:1993, *Reliability of systems, equipment and components — Part 13: Guide to reliability test conditions for consumer equipment — Section 13.1: Conditions providing a low degree of simulation for indoor portable equipment.* (IEC 60605-3-1:1986).

BS 5760-13.2:1993, *Reliability of systems, equipment and components — Part 13: Guide to reliability test conditions for consumer equipment — Section 13.2: Conditions providing a high degree of simulation for equipment for stationary use in weatherprotected locations.* (IEC 60605-3-2:1986).

BS 5760-13.3:1993, *Reliability of systems, equipment and components — Part 13: Guide to reliability test conditions for consumer equipment — Section 13.3: Conditions providing a low degree of simulation for equipment for stationary use in partially weatherprotected locations.* (IEC 60605-3-3:1992).

BS 5760-13.4:1993, *Reliability of systems, equipment and components — Part 13: Guide to reliability test conditions for consumer equipment — Section 13.4: Conditions providing a low degree of simulation for equipment for portable and non-stationary use.* (IEC 60605-3-4:1992).

BS 5760-13.5:1996, *Reliability of systems, equipment and components — Part 13: Guide to reliability test conditions for consumer equipment — Section 13.5: Ground mobile equipment — Low degree of simulation.* (IEC 60605-3-5:1996).

BS 5760-13.6:1997, *Reliability of systems, equipment and components — Part 13: Guide to reliability test conditions for consumer equipment — Section 13.6: Outdoor transportable equipment — Low degree of simulation.* (IEC 60605-3-6:1996).

BS 5760-14:1993, *Reliability of systems, equipment and components — Part 14: Guide to formal design review.* (IEC 61160:1992).

BS 5760-15:1995, *Reliability of systems, equipment and components — Part 15: Guide to the application of Markov techniques.* (IEC 61165:1995).

BS 5760-16.1:1996, *Reliability of systems, equipment and components — Part 16: Guide to stress screening — Section 16.1: Repairable items manufactured in lots.* (IEC 61163-1:1995).

BS 5760-17:1995, *Reliability of systems, equipment and components — Part 17: Reliability growth — Statistical test and estimation methods.* (IEC 61164:1995).

BS 6079-3:2000, *Project management — Part 3: Guide to the management of business related project risk.*

BS 6548-1:1984, *Maintainability of equipment — Part 1: Guide to specifying and contracting for maintainability.* (IEC 60706-1:1982).

BS 6548-2:1992, *Maintainability of equipment — Part 2: Guide to maintainability studies during the design phase.* (IEC 60706-2:1990).

BS 6548-3:1992, *Maintainability of equipment — Part 3: Guide to maintainability, verification and the collection, analysis and presentation of maintainability data.* (IEC 60706-3:1987).

BS 6548-5:1995, *Maintainability of equipment — Part 5: Guide to diagnostic testing.* (IEC 60706-5:1994)

BS 6548-6:1995, *Maintainability of equipment — Part 6: Guide to statistical methods in maintainability evaluation.* (IEC 60706-6:1994).

BS CECC 00804:1996, *Harmonized system of quality assessment for electronic components — Interpretation of "EN ISO 9000:1994" — Reliability aspects for electronic components.*

BS EN 61078:1994, *Reliability of systems, equipment and components — Guide to the block diagram technique.* (BS 5760-9:1992, IEC 61078:1991).

BS EN 61319:1996, *Interconnections of satellite receiving equipment.* (IEC 61319:1995).

BS EN 61508-3:2002, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements.* (BS IEC 61508-3:1998).

BS EN 61508-4:2002, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations.*

BS EN 61703:2002, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms.*

BS EN 61709:2000, *Electronic components — Reliability — Reference conditions for failure rates and stress models for conversion.* (IEC 61709:1996).

BS IEC 60300-3-1:2003, *Dependability management — Part 3-1: Application guide — Analysis techniques for dependability — Guide on methodology.*

BS IEC 60300-3-5:2001, *Dependability management — Part 3-5: Application guide —Reliability test conditions and statistical test principles.*

BS IEC 60300-3-7:1999, *Dependability management — Part 3-7: Application guide. Application guide — Reliability stress screening of electronic hardware.*

BS IEC 60605-4:2001, *Equipment reliability testing — Part 4: Statistical procedures for exponential distribution — Point estimates, confidence intervals, prediction intervals and tolerance intervals.*

BS IEC 60605-6:1997, *Equipment reliability testing — Part 6: Tests for the validity of the constant failure rate or constant failure intensity assumptions.*

BS IEC 61124:1997, *Reliability testing — Compliance tests for constant failure rate and constant failure intensity.*

BS IEC 61163-2:1998, *Reliability stress screening — Part 2: Electronic components.*

BS IEC 61649:1997, *Procedures for goodness-of-fit tests, confidence intervals and lower confidence limits for Weibull distributed data.*

BS IEC 61650:1997, *Reliability data analysis techniques — Procedures for comparison of two constant failure rates and two constant failure (event) intensities.*

BS IEC 61710:2000, *Power law model — Goodness-of-fit tests and estimation methods.*

BS IEC 62198:2001, *Project risk management — Application guidelines.*

BS ISO 3534-1:1993, *Statistics — Vocabulary and symbols — Part 1: Probability and general statistical terms.*

Other publications

[1] Def Stan 00-42 (Part 3) Issue 1. *Reliability & Maintainability (R&M) Assurance Guidance.* R&M Case. DStan, Glasgow: 1999.

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.
Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001.
Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre.
Tel: +44 (0)20 8996 7111. Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.
Tel: +44 (0)20 8996 7002. Fax: +44 (0)20 8996 7001.
Email: membership@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsi-global.com.

Copyright

Details and advice can be obtained from the Copyright & Licensing Manager.
Tel: +44 (0)20 8996 7070. Fax: +44 (0)20 8996 7553.
Email: copyright@bsi-global.com.

BSI
389 Chiswick High Road
London
W4 4AL