



DPC: 20/30404282 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 17 July 2020

Origin: European

Latest date for receipt of comments: 09 September 2020

Project No. 2019/03141

Responsible committee: DS/1 Dependability

Interested committees:

Title: Draft BS EN IEC 60300-3-4: Dependability management. Part 3-4: Application guide - Guide to the specification of dependability requirements.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 09 September 2020

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Responsible Committee Secretary: Miss Jacinta Hampton (BSI)
Direct tel:
E-mail: jacinta.hampton@bsigroup.com

Full document details: 20/30404282 DC

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



56/1891/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER:
IEC 60300-3-4 ED3

DATE OF CIRCULATION:
2020-07-17

CLOSING DATE FOR VOTING:
2020-10-09

SUPERSEDES DOCUMENTS:
56/1726/CD, 56/1737A/CC

IEC TC 56 : DEPENDABILITY	
SECRETARIAT: United Kingdom	SECRETARY: Mr Amit Patel
OF INTEREST TO THE FOLLOWING COMMITTEES:	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	
☒ SUBMITTED FOR CENELEC PARALLEL VOTING Attention IEC-CENELEC parallel voting The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

Dependability management - Part 3-4: Application guide - Guide to the specification of dependability requirements

PROPOSED STABILITY DATE: 2023

NOTE FROM TC/SC OFFICERS:

CONTENTS

1		
2	FOREWORD	3
3	INTRODUCTION	5
4	1 Scope	7
5	2 Normative references	7
6	3 Terms and definitions	7
7	4 Specifying dependability	9
8	4.1 Description of dependability specification	9
9	4.2 Principles	11
10	4.3 Benefits	13
11	5 Derivation of dependability requirements	14
12	5.1 General	14
13	5.2 Define stakeholder needs and expectations	16
14	5.3 Develop supporting documentation	17
15	5.4 Derive dependability requirements	18
16	5.5 Justify the measures within the dependability requirements	30
17	5.6 Complete dependability requirements specification	30
18	5.7 Review dependability specification	30
19	Annex A (informative) Discussion on useful life	31
20	A.1 General	31
21	A.2 Factors that determine useful life	31
22	A.3 Specification of useful life of non-repairable items (components)	32
23	Annex B (informative) Process for prioritising dependability attributes	34
24	Annex C (informative) Development of a dependability specification for a home	
25	security system	36
26	Annex D (informative) Influencing factors for dependability specification	43
27		
28	Figure 1 – High level process for derivation of dependability requirements in the	
29	specification	15
30	Figure 2 – What are we trying to achieve	16
31	Figure 3 – Dependability attributes applicable to different specification scenarios	20
32	Figure 4 – What do we need to manage?	21
33	Figure 5 – What constraints are there?	22
34	Figure 6 – Assurance considerations	22
35	Figure 7 – Reliability requirements	26
36	Figure 8 – Maintainability requirements	27
37	Figure 9 – Supportability requirements	28
38	Figure 10 – Availability requirements	29
39	Figure B.1 – Process for prioritising attributes	35
40	Figure C.1 – System configuration for normal mode of operation	40
41	Figure C.2 – System configuration for panic mode of operation	40
42	Figure C.3 – System configuration for security service mode of operation	41
43		
44	Table D.1 – Examples of influencing factors under each influencing condition	47
45	Table D.2 - Relationship of system properties with influencing conditions	48
46		

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT -

**Part 3-4: Application guide -
Specification of dependability requirements**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60300-3-4 has been prepared by IEC technical committee 56: Dependability.

This third edition cancels and replaces the second edition published in 2007. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

The content of IEC 62347, including the relevant annexes, has been included in this standard and IEC 62347 has been withdrawn. IEC 62347 dealt with the definitions of systems and their constituent elements and how to define these so that the dependability requirements of each element could be specified using IEC 60300-3-4. The premise of IEC 62347 was to identify system requirements by functions from a system engineering perspective. It provided a process for transforming the purchaser's view on system applications into a technical view for engineering the system. IEC 62347 emphasised architectural and functional design for realisation of functions with appropriate selection of hardware, software and human elements to achieve the system dependability requirements relevant to the purchaser's needs.

104 The text of this International Standard is based on the following documents:

• FDIS	• Report on voting
• XX/XX/FDIS	• XX/XX/RVD

105

106 Full information on the voting for the approval of this International Standard can be found in the
107 report on voting indicated in the above table.

108 This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

109 The committee has decided that the contents of this document will remain unchanged until the
110 stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to
111 the specific document. At this date, the document will be

- 112 – reconfirmed,
- 113 – withdrawn,
- 114 – replaced by a revised edition, or
- 115 – amended.

116

117 The National Committees are requested to note that for this document the stability date
118 is 20XX

119 THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED
120 AT THE PUBLICATION STAGE.

121

122

INTRODUCTION

Dependability is the ability to perform as and when required. A dependable item is one where there is justifiable confidence (developed through analytical and risk-based approaches) that the item will operate as desired and satisfy agreed stakeholder needs and expectations.

Dependability has many attributes, but is usually characterised in terms of reliability, maintainability and supportability (including maintenance and support), which may be applied individually or combined into an availability performance measure. Dependability also includes the performance characteristics of durability, testability and restorability as well as security and integrity, particularly in relation to software-based systems.

Dependability is important in many items and products and therefore it needs to be defined and specified in the same way as other attributes such as functional performance, dimensions and mass. Whilst mainly addressing system and equipment level reliability, many of the techniques described in the different parts of IEC 60300 may also be applied to products or at the component level. The term item is used throughout this standard. The item may be an individual part, component, device, functional unit, off-the-shelf (OTS), equipment, subsystem, or system. The item may consist of hardware, software, people or any combination thereof (see IEC 60050 IEV 192). In order to refer to a specific kind of "item" terms like component, OTS, product or large open system are used.

Dependability attributes may be specified as either quantitative and / or qualitative measures. In order to assess the values of some of the dependability attributes achieved, statistical methods may be necessary.

The levels of reliability, maintainability, supportability and availability achieved by an item depend on the conditions under which it is realized, utilized, maintained and supported and also on the life profile of the system. When requirements for dependability are specified, it is also necessary to define the following:

- conditions under which the item is stored, transported, realized and utilized;
- life profile and expected useful life;
- maintenance principles;
- available support.

Dependability characteristics may be specified, along with other performance characteristics, in three different ways:

- 1) specifications written by the supplier;
- 2) specifications written by the purchaser;
- 3) specifications mutually agreed or written by the supplier and the purchaser.

This document is applicable to all three types of specification.

This document provides guidance on the appropriate choice of dependability attribute to be specified, general considerations for the creation of the dependability specification as well as dependability measurement and evaluation.

This document is one of the six 'top level' interrelated dependability standards that provide managers and technical personnel with guidance on how to effectively plan and implement dependability activities throughout the life cycle. As such, this document should be used in conjunction with:

- IEC 60300-1 to recognize the importance of dependability, how to integrate dependability activities into existing management systems and life cycle processes and how to derive management activities to achieve and improve dependability outcomes;

- 168 • IEC 60300-3-1, IEC 60300-3-10, IEC 60300-3-14 and IEC 60300-3-17 to apply analysis and
169 assurance techniques for reliability, maintainability (and maintenance), supportability (and
170 support) and availability.

171

DEPENDABILITY MANAGEMENT -

Part 3-4: Application guide - Specification of dependability requirements

1 Scope

This document gives guidance on specifying required dependability requirements and collating these requirements in a specification, together with the means of assuring the achievement of those requirements.

The guidance provided includes:

- specifying quantitative and qualitative reliability, maintainability, supportability and availability requirements;
- advising purchasers on how to ensure that the requirements will be fulfilled by suppliers;
- advising suppliers to help them meet the purchaser's requirements.

Other obligations, such as legislation and governmental regulation may also place requirements on items and these should be applied in addition to any requirements derived in accordance with this standard.

Whilst mainly addressing system and equipment level dependability, many of the techniques described in the different parts of IEC 60300 can also be applied to products or at the component level. The term item is used throughout this standard.

NOTE 1 This guide does not directly consider safety and environment specifications although much of the guidance in this standard could also be applied to them.

NOTE 2 This guide does not consider the specification of the dependability of a service, including those provided through Public-Private Partnership procurements.

NOTE 3 The guidance in this document may be applied to some aspects of the specification of requirements relating to software but specific guidance may be found in IEC 62628 and the different parts of IEC 61508.

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) applies.

IEC 60050-192, International Electrotechnical Vocabulary (IEV) - Chapter 192: Dependability and quality of service.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-192 apply.

NOTE Definitions of "dependability", "availability", "reliability", "maintainability", "supportability", "failure", "fault", "item", "time to failure", "operating time between failures", "verification" and "validation" are given in IEC 60050-192.

3.1

item

subject being considered

213 NOTE 1 The item may be an individual part, component, device, functional unit, equipment, subsystem, or system.

214 NOTE 2 The item may consist of hardware, software, people or any combination thereof.

215 NOTE 3 The item is often comprised of elements that may each be individually considered. See sub item (192-01-
216 02) and indenture level (192-01-05).

217 NOTE 4 IEC 60050-191:1990 (now withdrawn; replaced by IEC 60050-192:2015) identified the term “entity” as an
218 English synonym, which is not true for all applications.

219 NOTE 5 The definition for item in IEC 60050-191:1990 (now withdrawn; replaced by IEC 60050-192:2015) is a
220 description rather than a definition. This new definition provides meaningful substitution throughout this document.
221 The words of the former definition form new note 1.

222 **3.2** 223 **off-the-shelf** 224 **OTS**

225 non-developmental item of supply that is both commercial and sold in substantial quantities in
226 the commercial marketplace

227 NOTE 1 Sometimes referred to as COTS (commercial off-the-shelf) or MOTS (modified off-the-shelf).

228 **3.3**

229 **useful life** <of an item>
230 time interval from first use until user requirements are no longer met due to performance and /
231 or economic factors

232 NOTE 1 The applicable time interval is dependent on the nature and application of the asset and can be elapsed
233 time, operating hours, number of cycles, etc.

234 NOTE 2 Performance factors to be considered for useful life include a decrease in item performance below
235 acceptable limits which cannot be rectified, a change in performance or service requirements, increase in failure
236 probability or decrease in availability.

237 NOTE 3 Economic factors to be considered for useful life include excessive maintenance costs, increases in
238 operating costs and emergence of more cost-effective solutions.

239 NOTE 4 In some cases, the useful life of an item is more than that required by an organization in which case it will
240 have residual value and could be repurposed.

241 NOTE 5 In this context, “first use” excludes testing activities prior to hand-over of the item to the end-user.

242 NOTE 6 For non-repairable items (components) the useful life ends when the item fails. In that case the life of the
243 component can be specified as the time when a stated percentage of the components have failed. This is often stated
244 as a L.10 or B.10 value for 10% accumulated failures (see IEC 61649)

245 NOTE 7 For consumer products and other products produced in large volumes, where only a small percentage of the
246 products fail the L.10 or B.10 value can be used as an approximation.

247 **3.4**

248 **B10** <of a nonrepairable item>
249 time at which 10% of a nonrepairable item (e.g. component) have failed.

250 NOTE 1 B10 is in some cases called L10.

251 NOTE 2 The value of 10% can be changed to any specified percentage for example B1 for 1% failed or B50 for 50%
252 failed.

253 NOTE 3 The B10 can be measured in elapsed time, operating hours, number of cycles, number of demands or other
254 time-related measures.

4 Specifying dependability

4.1 Description of dependability specification

4.1.1 What is dependability?

Dependability is the ability to perform as and when required. A dependable item is one where there is justifiable confidence (developed through analytical and risk-based approaches) that the item will operate as desired and satisfy agreed stakeholder needs and expectations.

Dependability has a strong impact on the user's perception of the value of an item developed or provided by an organization and poor dependability will affect an organization's reputation.

Dependability is specified and verified using a set of measurable or demonstrable attributes. Where practicable these are quantified to provide assurance that requirements are met and to unambiguously demonstrate improvements. Dependability is usually characterised in terms of reliability, maintainability and supportability (including maintenance and support) or as an availability performance measure.

- Reliability relates to the ability to perform as required for a given interval (time, operating cycles, distance etc.), under given conditions, without the need for repair or restoration.
- Maintainability relates to the ease and speed with which an item can be retained in, or restored to, a state to perform as required. For software, maintainability also includes the ease with which it can be modified without major reverse engineering or redesign to deal with faults or with changing needs.
- Supportability is the ability to be supported to sustain the required operational capability with a defined operational profile and given logistic and maintenance resources. It affects the system's ability to evolve during its life, adapting to changes
- Availability is the ability to be in a state to perform. It is the ratio of operating time to total time. As reliability, maintainability and supportability are major contributors of up time and down time, availability is impacted by the trade-offs between these attributes.

Dependability is also related to other attributes of life cycle processes such as design, manufacturing, installation, and ongoing operation and support activity. The dependability specification therefore should be part of the total item specification and the interaction between dependability requirements and functional requirements recognized and taken into account.

4.1.2 What is a requirement?

A dependability requirement is a statement of a single aspect of a dependability attribute which meets a stakeholder's needs or expectations and for which evidence or assurance of compliance can be provided. Multiple requirements may be necessary to fully define how the stakeholder's needs and expectations are to be met for each dependability attribute.

Requirements are that part of the specification that the purchaser considers is essential and for which the supplier has to provide evidence or assurance. This evidence may be supplied before the item is utilized as part of the deliverables or once the item is utilized through the application of incentives (or penalties) for meeting (or not meeting) the requirements.

Dependability performance measures are the different ways in which each of the dependability attributes can be expressed within a requirement. See 5.4.3 for further details.

4.1.3 What is dependability specification?

The requirements for an item will be collated into a specification which will also include the context within which the requirements are valid and any supporting information. Supporting information includes item usage, operational environment and the conditions of use of the item (see 5.3 for further information). Changes in item usage are a factor that affects dependability. Intended use is thus an essential part of the supporting information in the dependability

specification and changes have to be monitored and managed as part of the dependability life cycle.

For mass produced industrial items and for consumer items the specification is written jointly by the management of the supplier and the project team of the supplier.

4.1.4 Which attributes to specify?

The way that dependability requirements are specified will depend on the type and nature of the item, e.g. whether the item is repairable or non-repairable or a single use device. For example, non-repairable and single use items generally require no maintenance actions so only reliability requirements need to be specified. Examples of non-repairable items include sealed items and items where the cost of repair outweighs the cost of replacement, such as many consumer goods, and items at remote locations, such as deep-sea systems and satellites, where maintenance skills and spare parts are not available when needed. Single use devices include explosives, passenger air-bags and safety helmets.

Many complex items, however, are repairable and maintainability is important. Maintainability requirements should be specified for items if the maintenance costs contribute significantly to life cycle cost or if maintenance is important for the purchaser or user. Preventive and corrective maintenance requirements may be specified, if applicable.

Supportability is the combined result of required maintenance support and the logistics required to provide that level of maintenance support. The level of supportability is very often influenced by the conditions of use and factors that change through the life cycle. Therefore the supportability and / or support requirements can be important in a specification.

Availability requirements are generally specified for items where down time could cause economic or other loss through increased operating costs, personnel injury or loss of service, for example, production plants, medical equipment, safety equipment and military systems. Availability can be determined from the item configuration, its subsystems and their reliability, maintainability and supportability in the context of the operational and support arrangements. Availability may also be expressed as service levels to be provided to an operator or end-user stakeholders.

Although safety and environment specifications are not considered directly in this guidance, much of the guidance in this standard could also be applied to safety and environmental specifications. Therefore, if there are dependability requirements related to safety and environment, the appropriate safety and environment requirements should be included in or referenced from the dependability specification.

4.1.5 Contracting for dependability

The purpose of any specification is to provide a basis for development or purchase of an item. 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 dependability.

The benefits of the different contract types are as follows.

- Penalties for poor performance will encourage the supplier to give dependability its full attention and can lead to higher levels of dependability than would otherwise be achieved.
- Incentives for passing demonstration testing focus the supplier on demonstrating the reliability. However demonstration testing can be costly and time-consuming and might only reveal, just before delivery, that the item does not meet its dependability requirements.
- Requiring the supplier to provide maintenance will encourage the supplier to mitigate the risk that the item achieves poor availability as the supplier may then experience

consequential losses as a result of item unreliability. However this requires a much longer contract, e.g. a fixed cost maintenance agreement, with its associated difficulties.

The way in which the specification is written depends on the circumstances. There are three main types:

- specifications written by the supplier;

These are mainly used for mass produced items that need to have certain dependability characteristics, in order to be accepted by the market place. They are therefore used between the management of the supplier and the supplier's product development team. The specifications are mainly used for standard items like industrial products, consumer products or components

- specifications written by the purchaser;

These specifications are mainly used when a purchaser seek an item for a specific purpose like components or OTS. They are also used when a purchaser issues an invitation for tenders.

- specifications mutually agreed or written by the supplier and the purchaser;

These specifications are mainly used for customer specified items which is usually unique items or items produced in small numbers. Often the process will start with an invitation for tenders from the purchaser followed by an offer (tender) from a supplier. A contract is negotiated including the final specification written by the supplier and the purchaser'.

The content of the specification will vary according to its type. Subclause 5.3 lists the different types of supporting documentation which needs to be tailored to the exact nature of the specification.

4.2 Principles

4.2.1 General

The development of dependability requirements and the creation of the dependability specification are founded on a set of principles. These principles should influence an organisation's intent as well as its approach to design for, and delivery of, dependability of an item. Maximum benefit will be obtained from the dependability specification if all of these principles are applied.

4.2.2 Systems approach

In general, a system for which dependability is to be specified can include equipment (both hardware and software), the people who manage, operate and maintain it, data, processes and procedures, facilities, materials and naturally occurring entities.

Requirements can be defined for:

- the system as a whole;
- any component or sub-system
- a separate entity (e.g. a product or asset);
- a collection of functions (e.g. a service or set of services).

In general, the dependability of an item is affected by its conditions of use, the people who use it and by the environment in which it operates. In consequence, dependability requirements should be specified considering not just the item itself but the broader system in which it is used as well as interfaces with other systems. This includes the people who use it and how it is utilised. Conditions of use should be monitored and changes managed as part of achieving dependability through the life cycle.

4.2.3 Requirements and goals

It is important to distinguish between formal requirements described in a specification, and stakeholder goals, as the method of acceptance is different.

A requirement is an essential element of the purchaser's needs and expectations and it must be possible to provide evidence or assurance of compliance with the requirement. A goal is not a requirement but is the purchaser's desires or aims and evidence of the degree to which the goal has been fulfilled either need not or cannot be provided.

For high availability or reliability systems, it may not be practicable or cost effective to provide formal evidence that the high level of availability or reliability has been achieved. The purchaser will need to clearly identify both the high availability and reliability goals, for which evidence cannot be provided, but also define demonstrable requirements for which evidence can be provided. This evidence can include control of the design and manufacturing process for example using ISO9001 certification, formal planning (IEC 61508 and ISO 26262), status reviews (see IEC 62960) or maturity matrix (see IEC 60300-1 Annex C).

4.2.4 Assuring achievement of requirements

There are two elements to any specification; the dependability requirements and the means by which the supplier has to demonstrate or assure the achievement of the requirements to the purchaser. This means that the supplier has to provide sufficient evidence to the purchaser that the item meets its requirements to give the purchaser the confidence needed to pay the agreed price. Generally, the additional evidence is required to provide assurance that the higher reliability items have met their requirements. This is one factor in the higher cost of higher reliability items but, without these activities, the supplier will have limited confidence that the item will meet its requirements. IEC 60300-3-1, IEC 60300-3-10, IEC 60300-3-14 and IEC 60300-3-17 discuss dependability evaluation and measurement in more detail for reliability, maintainability (and maintenance), supportability (and support) and availability respectively.

Assurance covers a number of activities designed to provide the evidence that an item is meeting its dependability requirements. These activities may provide the necessary evidence through different techniques, which have the same or similar overall aim but use different methods to achieve it. The choice of technique is dependent upon a number of factors and is discussed in IEC 60300-3-1, IEC 60300-3-10, IEC 60300-3-14 and IEC 60300-3-17.

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 item 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 item, then formal reliability or availability demonstration testing might be necessary. Rare events can seldom be proven to be absent by testing so assurance may need to be via a well reasoned argument. A Dependability case (see IEC 62741) provides one method of presenting such an argument.

4.2.5 Cost implications

All items exhibit some level of reliability, whatever the frequency of failure or the required level of maintenance. However, if an item fails too often it might not be available to perform when required or it might require high levels of corrective maintenance. In addition, items 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 items with high levels of reliability can be costly and may also require high levels of preventive maintenance to achieve the desired level of reliability. As such it may not be possible to produce such an item at an economical price. There is therefore a balance to be struck between low reliability items that cost a lot to maintain and high reliability items that may be expensive to design and construct.

An investment in dependability design and construction can therefore repay itself in terms of the combined development, realization and operating costs for the item.

describes Life Cycle Costing and the relationships between dependability and cost. Items produced by those organizations that do not actively manage dependability generally achieve levels of reliability much below the minimum life cycle cost point causing project delays, cost overruns and low levels of availability.

4.2.6 Dependability management

This document deals with the specification of dependability, through the setting of requirements for one or more of the dependability attributes. These attributes are characteristics of the item that can be assured. However, other factors can significantly reduce the achieved levels of these attributes below the intrinsic levels. The most significant are potentially the quality of manufacture and maintenance of the system that can introduce new faults into the item. It is therefore essential that dependability is actively managed throughout the system life cycle. This includes both during the procurement process and during use, with the management activities differing for each. If dependability is not managed correctly, there is a higher likelihood that reliability, maintainability, supportability or availability requirements will not be achieved.

Dependability management provides a systematic approach for addressing dependability and related issues from an organizational and business perspective. Dependability is often driven by technology and requires the integration of innovation with legacy products. Achieving dependability throughout the life cycle process can be influenced by market dynamics, global economics and resource distributions, changing customer needs, and a competitive environment. Strategies need to adapt to anticipated changes to sustain viability in business operations. Dependability management focuses on the needs of stakeholders in optimizing dependability to enhance organizational objectives and return-on-investments.

IEC 60300-1 establishes a framework for dependability management. It provides guidance on dependability management of products, systems, processes or services involving hardware, software and human aspects or any integrated combinations of these elements. It presents guidance on planning and implementation of dependability activities and technical processes throughout the life cycle taking into account other requirements such as those relating to safety and the environment. It also gives guidelines for managers and their technical personnel to assist them to optimize dependability.

4.2.7 Life profile and expected useful life

The length of time that an item is able to meet requirements for users and organizations is an important aspect of dependability. There are different aspects involved in determining useful life that can be characterized as performance, and economic (see Annex A). It also depends on whether the item is repairable or non-repairable.

The determination of useful life may be included as a part of a dependability specification. Understanding the useful life of items could assist in the decision as to which item to acquire as the most appropriate solution for an application. Expected useful life in some cases may also be required by a legal directive in certain markets. Knowledge of an item's useful life is important for estimating its life cycle cost (IEC 60300-3-3).

4.3 Benefits

Specifying dependability provides benefits by:

- defining, documenting and providing evidence, based on data and evaluation, that agreed stakeholder needs and expectations for dependable performance are met;
- managing changes in stakeholder needs and expectations, including changes in requirements themselves;
- improved knowledge of dependability requirements;
- enabling trade-offs between reliability, maintainability and supportability to be determined during design and acquisition of items;

- providing justification that dependability requirements are applicable, achievable and assurable;
- providing verification of contract requirements.

5 Derivation of dependability requirements

5.1 General

All reliability, maintainability, supportability and availability requirements should be expressed quantitatively wherever possible, but it might also be appropriate to specify qualitative requirements in the specification. Quantitative requirements are only appropriate when the requirement being specified can be measured during the assurance process.

As items and their usage are very different across different organisations, it is not possible to write a standardised approach that articulates how to develop dependability requirements. Instead, this clause provides a high-level process to determine what information is required, the decisions that could be made and what the output of the decision making process might be. It is also not possible to provide a fully comprehensive set of decisions which affect the development of dependability requirements for all situations, so the user of this document will need to tailor the approach described to their situation. The users should particularly consider what is within their control in making decisions using the process described.

Figure 1 describes the approach to developing dependability requirements.