



BSI Standards Publication

Dependability management

Part 1: Managing dependability

National foreword

This British Standard is the UK implementation of EN IEC 60300-1:2024. It is identical to IEC 60300-1:2024. It supersedes BS EN 60300-1:2014, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 12973 1

ICS 03.100.40; 03.120.01; 21.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2024.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English Version

Dependability management - Part 1: Managing dependability
(IEC 60300-1:2024)

Gestion de la sûreté de fonctionnement - Partie 1: Gérer la
sûreté de fonctionnement
(IEC 60300-1:2024)

Zuverlässigkeitsmanagement - Teil 1: Management von
Zuverlässigkeit
(IEC 60300-1:2024)

This European Standard was approved by CENELEC on 2024-07-16. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 56/2031/FDIS, future edition 4 of IEC 60300-1, prepared by IEC/TC 56 "Dependability" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 60300-1:2024.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2025-04-16
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2027-07-16

This document supersedes EN 60300-1:2014 and all of its amendments and corrigenda (if any).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Standard IEC 60300-1:2024 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standard indicated:

IEC 31010	NOTE Approved as EN IEC 31010
IEC 60300-3-1	NOTE Approved as EN 60300-3-1
IEC 60300-3-2	NOTE Approved as EN 60300-3-2
IEC 60300-3-3	NOTE Approved as EN 60300-3-3
IEC 60300-3-4	NOTE Approved as EN IEC 60300-3-4
IEC 60300-3-11	NOTE Approved as EN 60300-3-11
IEC 60300-3-12	NOTE Approved as EN 60300-3-12
IEC 60300-3-14	NOTE Approved as EN 60300-3-14
IEC 60300-3-16	NOTE Approved as EN 60300-3-16
IEC 60706-2	NOTE Approved as EN 60706-2
IEC 60706-3	NOTE Approved as EN 60706-3
IEC 60706-5	NOTE Approved as EN 60706-5
IEC 60812	NOTE Approved as EN IEC 60812
IEC 61014	NOTE Approved as EN 61014

IEC 61025	NOTE Approved as EN 61025
IEC 61078	NOTE Approved as EN 61078
IEC 61123	NOTE Approved as EN IEC 61123
IEC 61124	NOTE Approved as EN IEC 61124
IEC 61163-1	NOTE Approved as EN 61163-1
IEC 61163-2	NOTE Approved as EN IEC 61163-2
IEC 61165	NOTE Approved as EN 61165
IEC 61649	NOTE Approved as EN 61649
IEC 61703	NOTE Approved as EN 61703
IEC 61709	NOTE Approved as EN 61709
IEC 61710	NOTE Approved as EN 61710
IEC 61709	NOTE Approved as EN 61709
IEC 61710	NOTE Approved as EN 61710
IEC 61882	NOTE Approved as EN 61882
IEC 61907	NOTE Approved as EN 61907
IEC 62198	NOTE Approved as EN 62198
IEC 62308	NOTE Approved as EN 62308
IEC 62309	NOTE Approved as EN 62309
IEC 62402	NOTE Approved as EN IEC 62402
IEC 62502	NOTE Approved as EN 62502
IEC 62506	NOTE Approved as EN IEC 62506
IEC 62508	NOTE Approved as EN 62508
IEC 62550	NOTE Approved as EN 62550
IEC 62551	NOTE Approved as EN 62551
IEC 62628	NOTE Approved as EN 62628
IEC 62673	NOTE Approved as EN 62673
IEC 62740	NOTE Approved as EN 62740
IEC 62741:2015	NOTE Approved as EN 62741:2015 (not modified)
IEC 62853	NOTE Approved as EN IEC 62853
IEC 62960	NOTE Approved as EN IEC 62960
IEC 80001-1	NOTE Approved as EN IEC 80001-1
ISO 9001	NOTE Approved as EN ISO 9001
ISO 9241-210:2019	NOTE Approved as EN ISO 9241-210:2019 (not modified)
ISO 20815	NOTE Approved as EN ISO 20815

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cencenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60050-192	2015	International electrotechnical vocabulary -- Part 192: Dependability	--	-

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	8
2 Normative references	8
3 Terms, definitions, and abbreviated terms	8
3.1 Terms and definitions.....	9
3.2 Abbreviated terms.....	14
4 Key concepts and application of this document.....	14
4.1 Overview.....	14
4.2 Principles of dependability management	14
4.3 Benefits of managing dependability.....	15
4.4 Attributes of dependability.....	16
4.5 Relationship between an organization's management system and dependability	18
4.6 Technical programmes for dependability	19
4.7 Life cycle concept	20
4.8 Dependability activity concept.....	21
5 Integrating dependability into an organization's management system	21
5.1 Overview.....	21
5.2 Understanding the organization and its context	22
5.3 Leadership.....	22
5.4 Planning	23
5.5 Support.....	23
5.6 Documented information	24
5.7 Operation.....	25
5.8 Performance evaluation and improvement.....	25
6 Programme design	26
6.1 General.....	26
6.2 Coordination and integration	26
6.3 Trade-offs	27
6.4 Tailoring a technical programme of dependability activities	27
6.5 Key success factors	28
7 Programme management activities	28
7.1 Overview.....	28
7.2 Plan dependability activities	29
7.2.1 Purpose	29
7.2.2 Outcomes	29
7.2.3 Tasks	29
7.3 Implement the plan	31
7.3.1 Purpose.....	31
7.3.2 Outcomes	31
7.3.3 Tasks	31
7.4 Review and improve.....	32
7.4.1 Purpose.....	32
7.4.2 Outcomes	32
7.4.3 Tasks	32

7.5	Providing assurance	33
7.5.1	Purpose	33
7.5.2	Outcomes	33
7.5.3	Tasks	33
7.6	Achieving accountability	34
7.6.1	Purpose	34
7.6.2	Outcomes	34
7.6.3	Tasks	34
8	Technical dependability activities	35
8.1	Overview	35
8.2	Stakeholder engagement, consensus building and communication	35
8.2.1	Purpose	35
8.2.2	Outcomes	36
8.2.3	Tasks	36
8.3	Managing opportunities, threats and risks	37
8.3.1	Purpose	37
8.3.2	Outcomes	37
8.3.3	Tasks	38
8.4	Dependability analysis	38
8.4.1	Purpose	38
8.4.2	Outcomes	39
8.4.3	Tasks	39
8.5	Dependability assessment	40
8.5.1	Purpose	40
8.5.2	Outcomes	40
8.5.3	Tasks	41
8.6	Maintenance, support and improvement	41
8.6.1	Purpose	41
8.6.2	Outcomes	42
8.6.3	Tasks	42
Annex A (informative)	IEC standards related to dependability	44
Annex B (informative)	Life cycle models	47
B.1	Generic life cycle	47
B.2	Alternative life cycle models	48
B.2.1	Life cycle model with multiple progressions	48
B.2.2	Managing change through the life cycle	48
B.2.3	Hardware	49
B.2.4	Software (see Figure B.5)	49
B.2.5	Services	50
B.2.6	Open systems	50
Annex C (informative)	Stakeholders	51
C.1	General	51
C.2	Users of systems, products and services	51
C.3	Managers	51
C.4	The workforce	51
C.5	Specialists	52
C.6	Others	52
C.7	Stakeholders through the life cycle	52

C.7.1	Concept – Specification	52
C.7.2	Development	52
C.7.3	Realization (including manufacture, transport acquisition and installation).....	52
C.7.4	Operation or use of items	53
C.7.5	Maintenance	53
C.7.6	Obsolescence, retirement and re-use	53
Annex D (informative)	Dependability maturity assessment	54
Annex E (informative)	Dependability through the life cycle	57
Annex F (informative)	Comparison of approach of ISO/IEC/IEEE 15288 with that of IEC 60300-1	60
F.1	Overview.....	60
F.2	Concept of system life cycle processes	60
Annex G (informative)	Testing.....	64
G.1	General.....	64
G.2	Purpose and objectives of tests	64
G.3	Test conditions	64
G.4	Types of test.....	65
G.5	Data quality and quantity	66
Bibliography		68
Figure 1 – Dependability and security attributes.....		18
Figure 2 – Relationship between management system standards and dependability standards.....		19
Figure 3 – Integration of dependability into a management system		22
Figure B.1 – Generic life cycle model.....		47
Figure B.2 – Life cycle model with some of the possible progressions.....		48
Figure B.3 – Managing change through the life cycle		49
Figure B.4 – Example of hardware life cycle model		49
Figure B.5 – Example of software life cycle model		50
Figure B.6 – Example of service life cycle model		50
Figure B.7 – Simplified life cycle model for an open system		50
Figure F.1 – System life cycle processes according to ISO/IEC/IEEE 15288		61
Figure G.1 – Verification and validation methods or practices		65
Table A.1 – Classification of dependability standards by topic and life cycle stage.....		44
Table B.1 – Stages of generic model, their purpose and outputs		47
Table D.1 – Example of dependability maturity matrix		54
Table E.1 – Examples of dependability focus relevant to each life cycle stage		57
Table F.1 – Comparison of approach of ISO/IEC/IEEE 15288 and IEC 60300-1		62

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –**Part 1: Managing dependability****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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 60300-1 has been prepared by IEC technical committee 56: Dependability. It is an International Standard.

This fourth edition cancels and replaces the third edition published in 2014. This edition constitutes a technical revision.

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

- a) more guidance on integration of dependability activities into an existing management system;
- b) greater detail on the activities required to establish and implement a programme of dependability activities;
- c) changes to provide consistency with other dependability standards.

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

Draft	Report on voting
56/2031/FDIS	56/2044/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all parts in the IEC 60300 series, published under the general title *Dependability management*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Dependability is the ability to perform as and when required. A dependable item is one where there is justified confidence that it operates as desired and satisfies agreed stakeholder needs and expectations. Dependability has many attributes but is usually characterised in terms of reliability, maintainability and supportability, and the resulting availability. In some cases, attributes such as resilience, recoverability, durability, integrity, safety, security, and trustworthiness are included in, or overlap with, dependability.

The specification and verification of dependability attributes provide stakeholders with assurance that requirements will be met into the future and quality will be maintained over time. The dependability of a system, product or service influences the business strategies associated with its design, acquisition and use, and costs over its life cycle. The dependability of an organization's systems, products and services has a strong impact on the perception of the value and trustworthiness of the organization.

Dependability is managed as a key element of an organization's wider management system, particularly aspects relating to assets, quality and finance.

This document highlights the importance and benefits of managing dependability. It gives guidance on dependability activities and their integration into an existing management system and life cycle processes so that an efficient, effective and economical approach is achieved.

Dependability activities bring benefits whenever they are performed but greater benefit is achieved the sooner in the life cycle they are implemented.

This document is applicable to a broad range of industry sectors and organizations of any size. It applies to systems of systems, large unique systems, mass produced industrial and consumer products, software applications, components and services. These categories are not mutually exclusive. For example, many products and components are in themselves complex systems.

The document will be useful for:

- managers and technical personnel;
- those involved in deciding how their systems, products and services can be made dependable;
- organizations such as regulators who evaluate the dependability of systems, products and services;
- those (e.g. users or the public) who need justified confidence in systems, product and services that might affect them;
- developers of other dependability related standards.

This document is one of a suite of "top level" interrelated IEC dependability standards that provide managers and technical personnel with guidance on how to effectively plan and implement dependability activities. Other documents in the suite are:

- IEC 60300-3-4 which provides guidance on writing dependability requirements in specifications, and on the means of assuring the achievement of those requirements;
- IEC 60300-3-10 and IEC 60300-3-14 which provide guidance on how to identify and apply appropriate analysis and assurance techniques for maintainability (and maintenance) and supportability (and support) respectively;
- standards to cover reliability and availability, which are planned.

DEPENDABILITY MANAGEMENT –

Part 1: Managing dependability

1 Scope

This document provides guidance on:

- the meaning and significance of dependability from a business, technical and financial perspective;
- achieving dependability through suitable adaptation of organizational management systems such as those described in ISO 9001 (quality management) and ISO 55001 (asset management);
- the activities that are integrated into management systems and life cycle processes in order to achieve dependable systems, products and services;
- planning and implementing dependability activities throughout the life cycle to achieve and assure required outcomes, taking into account factors such as costs, safety, the environment, customer goodwill, brand and reputation.

This document is applicable to any type of system, both new and existing, to mass produced industrial or consumer products, to components and to services. This document addresses all elements of systems, products and services including hardware, software, data, processes, procedures, facilities, materials, and personnel required for operations and support.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050-192:2015, *International Electrotechnical Vocabulary (IEV) – Part 192: Dependability* (available at www.electropedia.org)

3 Terms, definitions, and abbreviated terms

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1 Terms and definitions

3.1.1

accountability

state of being answerable for decisions and activities to the organization's governing bodies, legal authorities and, more broadly, its stakeholders and society in general

Note 1 to entry: Accountability involves an obligation on management, the organization and individuals to be answerable for the impact of their decisions and activities on stakeholders, society and the environment. Accountability thus implies answerability to those affected and to society in general.

Note 2 to entry: Accountability implies that individuals, organizations and the community are responsible for their actions and can be required to justify them to others.

[SOURCE: ISO 26000:2010, 2.1, modified – "and society in general" has been added to the definition and notes to entry have been added.]

3.1.2

adaptability

ability to adjust to changed conditions or to be modified for a particular purpose or for a changed environment

3.1.3

assurance

grounds for justified confidence that a claim has been or will be achieved

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.1.1]

3.1.4

availability

ability to be in a state to perform as required under given conditions

Note 1 to entry: Availability depends upon the combined attributes of the reliability, maintainability, supportability and on the maintenance and support provided.

Note 2 to entry: Availability can also be affected by delays before it is recognised that maintenance or support are needed, for example fault detection time (192-06-18) and administrative delay (192-07-12).

Note 3 to entry: Given conditions include aspects that affect availability such as mode of operation, stress levels, environmental conditions and maintenance defined in the life profile.

Note 4 to entry: Availability may be quantified using measures defined in IEC 60050-192:2015, 192-08, *Availability related measures*.

[SOURCE: IEC 60050-192:2015, 192-01-23, modified – in the definition "of an item" has been deleted, "under given conditions" has been added, Note 1 to entry has been modified, and Notes 2 and 3 to entry have been added.]

3.1.5

business process

partially ordered set of inter-related enterprise activities that can be executed to achieve some desired end-result in pursuit of a given objective of an organization

Note 1 to entry: Business is interpreted broadly to mean those activities that are core to the purposes of the organization's existence whether the organization is public, private, for profit or not for profit.

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.445, modified – Note 1 to entry has been added.]

3.1.6

dependability

ability to perform as and when required

Note 1 to entry: A dependable item or service is one where there is justified confidence that it operates as desired and satisfies agreed stakeholder expectations.

Note 2 to entry: In most cases, the term dependability is used as an umbrella term to express its core attributes of reliability, maintainability, and supportability and the resulting availability. In some cases, attributes such as resilience, recoverability, durability, integrity, safety, security and trustworthiness are included in or overlap with dependability.

Note 3 to entry: In order to express the ability to perform, requirements in terms of functions to be performed, when the performance is to be achieved, and the life profile conditions, are specified by the customers, users or stakeholders.

Note 4 to entry: The attributes of dependability can be expressed qualitatively or quantitatively.

Note 5 to entry: It is also a common practice to use the term dependability in the context of a subject of study or discipline.

[SOURCE: IEC 60050-192:2015, 192-01-22, modified – "of an item" has been deleted, the notes have been deleted and new notes to entry have been added.]

3.1.7

dependability activity

set of cohesive tasks carried out to achieve a dependability related purpose

Note 1 to entry: A dependability activity can be mapped to a process view that uses a combination of life cycle processes, activities and tasks as defined in ISO/IEC/IEEE 15288.

3.1.8

dependability case

evidence-based, reasoned, traceable argument created to support the contention that a defined system does and/or will satisfy the dependability requirements

Note 1 to entry: A dependability case is an assurance case for dependability-related claims, see ISO/IEC/IEEE 15026-2.

[SOURCE: IEC 62741:2015, 3.1.1, modified – Note 1 to entry has been added.]

3.1.9

dependability plan

information item that presents a systematic course of action for achieving a declared purpose related to dependability including when, how and by whom specific tasks are to be performed

3.1.10

durability

ability to perform as required, under defined conditions of use and maintenance until a defined end state is reached

Note 1 to entry: The degree to which maintenance and repair are within the scope of durability will vary by product or product group.

Note 2 to entry: The end state can be based on technological, social or economic aspects.

Note 3 to entry: Durability can be expressed in units appropriate to the part or product concerned, e.g. calendar time, operating cycles, distance run, etc. or the probability of being able to achieve a given period of usage. The units should always be clearly stated.

Note 4 to entry: Durability as a measure relates to the longevity of the interval.

[SOURCE: IEC 60050-192:2015, 192-01-21, modified – "end of useful life" has been replaced with "defined end state", and notes to entry have been added.]

3.1.11**integrity**

<in dependability> ability to prevent or withstand unauthorised modification

Note 1 to entry: Modification can involve hardware, software or data.

3.1.12**life profile**

stresses and their levels, content, duration and sequence encountered during the life of an item

Note 1 to entry: Stresses can be internal (such as operating cycles) or external (such as environmental stress, input power level, or rate of service requests over a network).

Note 2 to entry: Life profile can be actual, expected or predicted.

3.1.13**maintainability**

ability to be retained in, or restored to a state to perform as required, under given conditions

Note 1 to entry: Given conditions include location for maintenance, accessibility, maintenance procedures and maintenance resources as well as conditions defined in the life profile.

Note 2 to entry: Maintainability can be quantified using appropriate measures. See IEC 60050-192:2015, 192-07, *Maintainability and maintenance support measures*.

3.1.14**measurement**

process of experimentally obtaining one or more values that can reasonably be attributed to a quantity

Note 1 to entry: Measurement does not apply to nominal properties.

Note 2 to entry: Measurement implies comparison of quantities, including counting of entities.

Note 3 to entry: Measurement presupposes a description of the quantity commensurate with the intended use of a measurement result, a measurement procedure, and a calibrated measuring system operating according to the specified measurement procedure, including the measurement conditions.

Note 4 to entry: The French word "mesure" has several meanings in everyday French language. It is for this reason that the French word "mesurage" has been introduced to describe the act of measurement. Nevertheless, the French word "mesure" occurs many times in forming terms, following current usage, and without ambiguity. Examples are: unité de mesure (unit of measurement), méthode de mesure (measurement method), instrument de mesure (measurement instrument). This does not mean that the use of the French word "mesurage" in place of "mesure" in such terms is not permissible when advantageous.

[SOURCE: ISO/IEC GUIDE 99:2007, 2.1, modified – Note 4 to entry has been added.]

3.1.15**need**

prerequisite identified as necessary, to achieve an intended outcome, implied or stated, within a specific context of use

3.1.16

reliability

ability to perform as required, without failure, for a given interval under given conditions

Note 1 to entry: The interval can be expressed in units appropriate to the item concerned, for example calendar time, operating cycles, distance run, etc., and the units should always be clearly stated.

Note 2 to entry: Given conditions include aspects that affect reliability such as: mode of operation, stress levels, environmental conditions and maintenance.

Note 3 to entry: Reliability can be quantified using measures defined in IEC 60050-192:2015, 192-05, *Reliability related concepts: measures*.

[SOURCE: IEC 60050-192:2015, 192-01-24, modified – in the definition "of an item" and "time" have been deleted.]

3.1.17

requirement

<in dependability> statement which translates or expresses a need and its associated constraints and conditions

Note 1 to entry: Requirements exist at different levels in the system structure.

Note 2 to entry: A requirement is an expression of one or more particular needs in a very specific, precise and unambiguous manner.

Note 3 to entry: A requirement always relates to a system, software or service, or other item of interest.

Note 4 to entry: A requirement is a statement where evidence or assurance of compliance can be provided.

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.19, modified – Note 4 to entry has been added.]

3.1.18

risk

effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive or negative or both and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

[SOURCE: ISO 31000:2018, 3.1]

3.1.19

safety

freedom from unacceptable risk of physical injury or damage to the health of people or damage to property or the environment

3.1.20

security

protection against intentional subversion or forced failure

3.1.21 specification

<in dependability> information item that identifies the dependability requirements and goals of a system, product or service together with any supporting information

Note 1 to entry: Supporting information can include details of use, operating and environmental conditions, failure criteria and methods intended to be applied for assurance of compliance with requirements, including accept or reject criteria.

Note 2 to entry: ISO/IEC/IEEE 15289 defines a specification as an information item that identifies in a complete, precise and verifiable manner the requirements, design, behaviour or other expected characteristics of the system, service or process. The specification of dependability has a greater scope than that used in ISO/IEC/IEEE 15289.

3.1.22 stakeholder

person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

EXAMPLE: End users, end user organizations, supporters, developers, producers, trainers, maintainers, disposers, acquirers, supplier organizations and regulatory bodies.

Note 1 to entry: Some stakeholders can have conflicting interests.

[SOURCE: ISO Guide 73:2009, 3.2.1.1, modified – example added and Note 1 to entry reworded.]

3.1.23 support

<in dependability> provision of resources to enable an item to continue to function as required

Note 1 to entry: Examples of resources are human effort, training, tools, jigs, test equipment, lifting equipment, materials, spare parts, facilities, documentation, information and information systems.

Note 2 to entry: Support is concerned with providing a quality resource to the correct location at the best time for the optimum cost, taking into account environmental, social and economic impacts.

3.1.24 supportability

ability of an item to be supported to perform as required with a defined life profile and given resources

3.1.25 system

combination of interacting parts that collectively has one or more purposes

Note 1 to entry: A system is sometimes considered as a product or as the service it provides.

Note 2 to entry: Parts can include the associated equipment, facilities, material, computer programs, firmware, technical documentation, other systems, services and personnel required.

3.1.26 usability

extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

[SOURCE: ISO 9241-210:2019, 3.13, modified – notes to entry omitted.]

3.1.27

useful life

interval from defined first use of an item until a defined end state is reached due to performance obsolescence or other factors

Note 1 to entry: The first use has to be defined. In this context, "first use" excludes testing activities prior to hand-over of the item to the end-user. The "first use" can commence after an initial period of early mortality.

Note 2 to entry: The end state has to be defined and can include safety margins that prevent the onset of failure or percentages of accumulated failures.

Note 3 to entry: The applicable interval is expressed in units appropriate to the item concerned, for example calendar time, operating cycles, distance run, etc. The units should be clearly stated.

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

3.2 Abbreviated terms

AI	Artificial intelligence
ASIL	Automotive safety integrity level
CMM	Capability maturity model
DRACAS	Data reporting, analysis and corrective action system
FMEA	Failure modes and effects analysis
FRACAS	Failure reporting, analysis, and corrective action system
HAZOP	Hazard and operability
IAS	International accounting standards
IFRS	International financial reporting standards
IOT	Internet of things
SIL	Safety integrity level

4 Key concepts and application of this document

4.1 Overview

Dependability is the ability to perform as and when required. The term applies equally well to items, products, processes and services, as well as to systems ranging from a simple component to a system of systems. A dependable system, product or service provides the user with assurance that requirements will be met into the future and quality maintained over time.

Clause 4 explains the concept of dependability and the attributes of systems, products and services that fall under the umbrella of dependability. The principles of dependability management and the benefits of devoting effort to it are described. The relationship between an organization's management system and dependability is discussed. The concept of a technical programme of dependability activities which is carried out through the life cycle is introduced.

4.2 Principles of dependability management

Dependability management encompasses a number of principles as follows.

- Holistic approach: Managing dependability integrates considerations of performance, cost, risk and compliance across the entire life of a system, product or service. It does so by taking a systems approach with continual optimization over the life.

- **Assurance and accountability:** Managing dependability establishes the grounds for justified confidence that claims relating to dependability have been, or will be, achieved. This satisfies the assurance and accountability requirements of the organization's management framework, which in turn fulfils the needs and expectations of stakeholders for assurance and accountability.
- **Risk based:** Managing dependability involves identifying factors that could cause systems, products and services, and the systems that support them, to fail or deviate from requirements. These risks represent a potential cost throughout the life of a system, product or service. Improving dependability represents an initial cost to the designer or manufacturer, but can result in a saving when considered across the life of the product. Deciding how much to invest to improve dependability at all stages of the life cycle is directly related to risk and value, and the amount of risk that the organization is willing to accept.
- **Adaptability:** Dependability activities and the systems to manage them need to be sufficiently flexible to be able to respond to changes in needs and context in a timely way. Adaptability can also be a desirable attribute of a system, product or service which can improve its maintainability and supportability and extend its useful life.
- **Sustainability:** For a system, product or service to meet the needs and expectations of stakeholders, economic, social and environmental issues need to be considered as well as technical excellence. For example as well as seeking to achieve a reliable, maintainable and supportable system, product or service, a dependable design should also aim to reduce energy consumption and environmental impacts and consider including re-usable components. A system, product or service that is reliable, maintainable and supportable is likely to have a longer life, use fewer resources, and produce less waste than one which does not have these attributes.
- **Balance:** Dependability is managed to achieve an appropriate balance of cost, risk and performance over the life of the system, product or service. A trade-off can also be required with requirements such as safety and security that can sometimes conflict with dependability, and with constraints such as contractual and legal requirements.

4.3 Benefits of managing dependability

Managing dependability is essential to managing the value that organizations or individuals derive from their assets. This value is often defined in terms of performance, cost and compliance as well as less tangible, but equally important elements such as brand, reputation, customer goodwill and trust.

Managing dependability provides benefit to an organization by:

- providing justified confidence that systems, products and services will provide value by performing as and when required;
- optimising life cycle costs and demonstrating affordable levels of dependability performance;
- achieving compliance with regulatory requirements or mandated standards;
- managing the risks of failure or degraded performance to achieve a balance of cost, risk and performance;
- providing transparency of decision making;
- underpinning the development of management systems, for example asset management systems and quality management systems, and providing objective evidence of the achievement of their intended outcomes. (Outcomes can include financial, safety, environmental and security outcomes as well as technical performance outcomes);
- improving design;
- optimising maintenance and support needs;
- reducing the need for unplanned maintenance activities that could expose staff to potential hazards;

- enabling informed decisions in a changing operational environment (including changes in requirements themselves);
- providing input to the design, implementation and ongoing improvement of maintenance and support;
- providing information so that mistakes of the past are not repeated, lessons are learnt and successes are built upon;
- improving an organization's resilience to adverse events and circumstances.

4.4 Attributes of dependability

The dependability of a system, product or service is specified and verified using a set of attributes. Where practicable these are quantified to facilitate providing assurance that requirements are met, and to unambiguously demonstrate improvements. Dependability has many attributes but is usually characterized in terms of reliability, maintainability, supportability and availability.

Reliability relates to the ability to provide a required function without failure for a given interval (time, operating cycles, distance, etc.). Reliability can be quantified as a probability of success (e.g. the probability of an item performing its intended function for a specified time period) or expressed through related measures, for example the failure rate. To specify reliability unambiguously it is necessary to define a point at which any particular function is said to have failed.

Maintainability relates to the ease and speed with which an item can be retained in, or restored to, a state to perform as required. It can be quantified as the probability that a given maintenance action, performed under stated conditions, can be completed in a specified time. "Retained in" refers to maintenance whilst a system is in an operational state (such as on-line maintenance or repairs to redundant components). "Restored to" refers to maintenance whilst the system is in a non-operational state such as planned down time servicing. Software differs from hardware in that it does not wear out and faults originate in the specification, design logic or coding process and can lie hidden until specific input conditions occur. Maintainability of software relates to the ease and speed with which software can be modified to change or add capabilities, to correct faults or defects, improve performance, or to adapt it to a different environment.

Supportability is concerned with identifying and quantifying:

- the support required for a defined item in a given context of use;
- the time to provide that support;
- the resourcing, cost and quality of that support;
- the quality of the delivered support.

Specifically, supportability is concerned with what is required for an item to continue to function as well as how to implement this requirement. The "what is required" element is inherent within the item design, but the way in which it is implemented is determined by the organization conducting the support.

Availability is the ability to be in a state to perform when called upon to do so. It is often quantified as the ratio of up 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.

EXAMPLE: A reliable item does not fail very often, an available item works when it is needed and a dependable item, as well as being available, performs correctly over time and is easy to maintain and support.

Factors such as cost, resources, the time available for dependability activities, and usage conditions influence the level of reliability, maintainability and supportability that can be achieved in practice.

Measures of reliability, maintainability, supportability and availability are discussed in IEC 62308, IEC 60300-3-10, IEC 60300-3-14 and IEC 61070 respectively. IEC 61703 explains the mathematical meaning of a range of dependability related measures and how they are established.

Measures of reliability, maintainability, supportability and availability are stochastic or statistical quantities, i.e. sufficient data need to be available to provide statistical validity (see IEC 60300-3-2 and IEC 60605-6). Verifying high reliability, or providing a high level of confidence for a dependability measure, requires a large number of tests which will not always be practicable, time feasible or cost effective to perform. The expected reliability in these circumstances can however be verified using results of reliability models (see IEC 60300-3-1).

Other attributes that can fall under the umbrella of dependability include the following.

- Durability, which is the ability to perform as required, under defined conditions of use, maintenance and repair until a defined end state is reached. It relates to the ability to continue to restore a system or product to a functioning condition until it is no longer needed.
- Recoverability, which is the ability to recover from failure without corrective maintenance (for example automatic re-initialization after software failure detection).
- Fault tolerance, which is the ability to continue functioning with certain faults present.
- Usability, which is the ability of a system, product or service to be used effectively and efficiently. Usability affects the performance of operators and maintainers and hence has an influence on the overall reliability and maintainability of an item. It includes for example learnability, operability, and prevention and protection mechanisms against errors. See IEC 62508.
- Testability, which is a design characteristic that determines the degree to which a system, product or service can be tested to determine one or more characteristics under stated conditions. Testability is discussed in IEC 60706-5.
- Operability, which is the ability of a system, product or service to operate safely and reliably to provide an intended result or function.
- Robustness, which is the ability of a system, product or service to function correctly in the presence of stressful inputs or environmental conditions.
- Resilience, which is the ability to adapt to change and return to functional capability within an acceptable time period after having been affected by stressful inputs or environmental conditions.
- Integrity, which is the ability to prevent or withstand unauthorized modification. This includes both non-malicious alteration (e.g. unexpected wear of hardware or the uncoordinated automatic update of software) and malicious or unauthorized alteration (e.g. malware infection or counterfeit components). For hardware, integrity refers to the ability of a system to sustain its form stability and robustness. For software and data the focus is on accuracy, completeness and security.

Often these attributes will affect reliability, maintainability and supportability and can be included in the measurement of those attributes. Guidance for writing dependability requirements in specifications, together with a means of assuring them, is provided by IEC 60300-3-4. Methods for specifying requirements and evaluating performance for some other quality attributes that can affect dependability more indirectly, such as learnability, error tolerance and error protection, are given in ISO/IEC 25023.

Safety, security and trustworthiness can overlap with dependability. Safety functions are required to be dependable to prevent harm to people, property and the environment. In some situations, a failure can lead to an unsafe situation, therefore improved reliability can enhance safety. In other cases safety requirements can result in increased maintenance and hence decrease availability. Dependable items require less maintenance and therefore avoid exposing staff to potential hazards during repair operations.

Security requires a system, product, or service to be available only to those authorized to use it (a combination of the attributes of availability and integrity) with the added requirement of confidentiality (absence of unauthorized disclosure). See Figure 1 (the lines with arrows in the figure indicate the attributes of dependability and of security.)

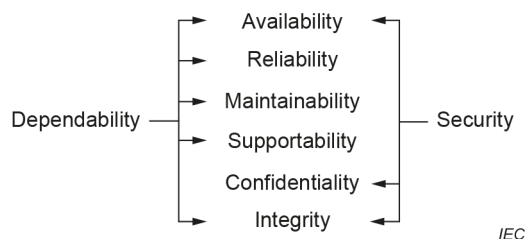


Figure 1 – Dependability and security attributes

Security and dependability are linked. Security can sometimes reduce dependability. For example access restriction to a system can reduce its maintainability. Poor dependability can also adversely affect security. For example poor maintainability of software can lead to a security breach. Trustworthiness is a concept that is applied in software intensive systems such as artificial intelligence (AI) and the internet of things (IOT). It is defined as the ability to meet stakeholders' expectations in a verifiable way. Trustworthiness characteristics include reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality, usability and accuracy (see e.g. ISO/IEC 30145-2).

It can be difficult to define quantitative measures for dependability attributes of AI and related technologies. The user's perception of a failure depends on their expectations of the system. The behaviour of the system changes as a result of interactions with the user so experiences differ from user to user. This means that failure to perform as required depends on the user's expertise, goals, mental models, and past experience in using the product as well as on the design of the algorithms and the data on which they are based. However qualitative analyses are still possible.

In general users, providers, operators, maintainers and others who interact with a system can have overlapping dependability requirements but with different objectives and usage expectations. This can result in differing needs and differing perceptions of dependability. A user perspective of overall dependability can in some circumstances be obtained using qualitative statements or an ordinal rating scale.

For an open system, such as a system of systems or a large system that operates for an extended period in a real world environment, the attributes of dependability have to be considered in the context where no single stakeholder has a full understanding of the system or its risks. Achieving and assuring dependability in this case relies on building consensus between stakeholders, achieving accountability and accommodating change. Since identifying and controlling risks is more difficult, it is particularly important that the system is able to respond effectively to failure. IEC 62853 provides guidance on dependability of open systems.

4.5 Relationship between an organization's management system and dependability

An organization's management system provides and documents the infrastructure needed to achieve the value and outcomes that are to be delivered. Within this management system, processes, activities and tasks are developed, documented and implemented to achieve specific objectives. ISO standards such as ISO 9001 and ISO 55001 describe the requirements of an organization's management system. Technical and financial standards provided by IEC, IFRS and IAS provide detailed guidance on the processes, activities and tasks. IEC TS 62775 shows how the IEC dependability suite of standards, systems engineering and the IFRS and IAS standards can support the requirements of asset management, as described by the ISO 5500x suite of standards.

Figure 2 shows the relationship between management system standards and dependability standards. Annex A lists dependability related standards from IEC.

The dependability of equipment, people, processes and services is central to the organization's ability to achieve its objectives. Therefore dependability management should be integrated into the management system of the organization. Dependability management is not a separate endeavour to the business, and dependability objectives should align with the business objectives. Dependability attributes are interlinked with other aspects of performance and functionality; hence dependability should be considered in conjunction with other organizational drivers such as cost, schedule, performance, risk and profitability.

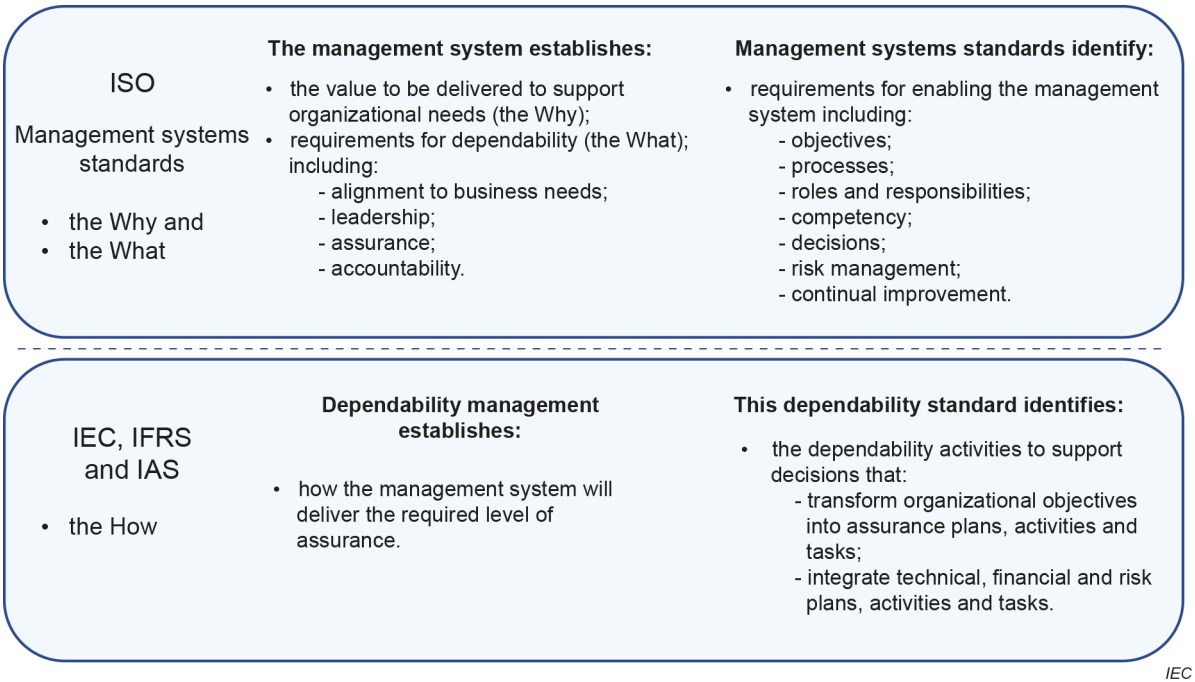


Figure 2 – Relationship between management system standards and dependability standards

Clause 5 describes how managing dependability can be incorporated into a management system that is assumed to conform to a management system standard with the harmonized structure of ISO/IEC Directives, Part 1, Consolidated ISO Supplement:2022, Annex SL.

4.6 Technical programmes for dependability

In order to achieve dependability objectives and targets and provide assurance that they have been, or will be, achieved, a customized set of coordinated dependability activities is carried out. Activities are broken down into individual tasks (and sometimes sub-tasks). These are usually documented in a plan which provides details of the objectives and the context and constraints. It identifies the tasks to be undertaken, the techniques, tools and resources required, responsibilities and accountabilities and how dependability activities and tasks will be integrated with other related activities.

NOTE A dependability activity can be a life cycle process, activity, task or process view as defined in ISO/IEC/IEEE 15288 (see Annex F).