

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Dependability management –
Part 1: Managing dependability**

**Gestion de la sûreté de fonctionnement –
Partie 1: Gérer la sûreté de fonctionnement**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2024 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC -

webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, ...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications, symboles graphiques et le glossaire. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Dependability management –
Part 1: Managing dependability**

**Gestion de la sûreté de fonctionnement –
Partie 1: Gérer la sûreté de fonctionnement**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.100.40, 03.120.01, 21.020

ISBN 978-2-8322-8320-2

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

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.)

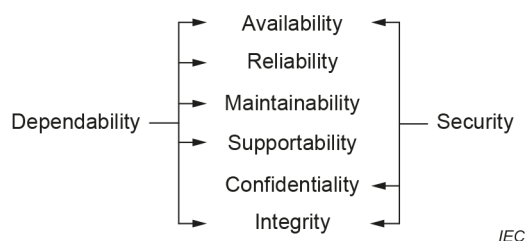


Figure 1 – Dependability and security attributes

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.

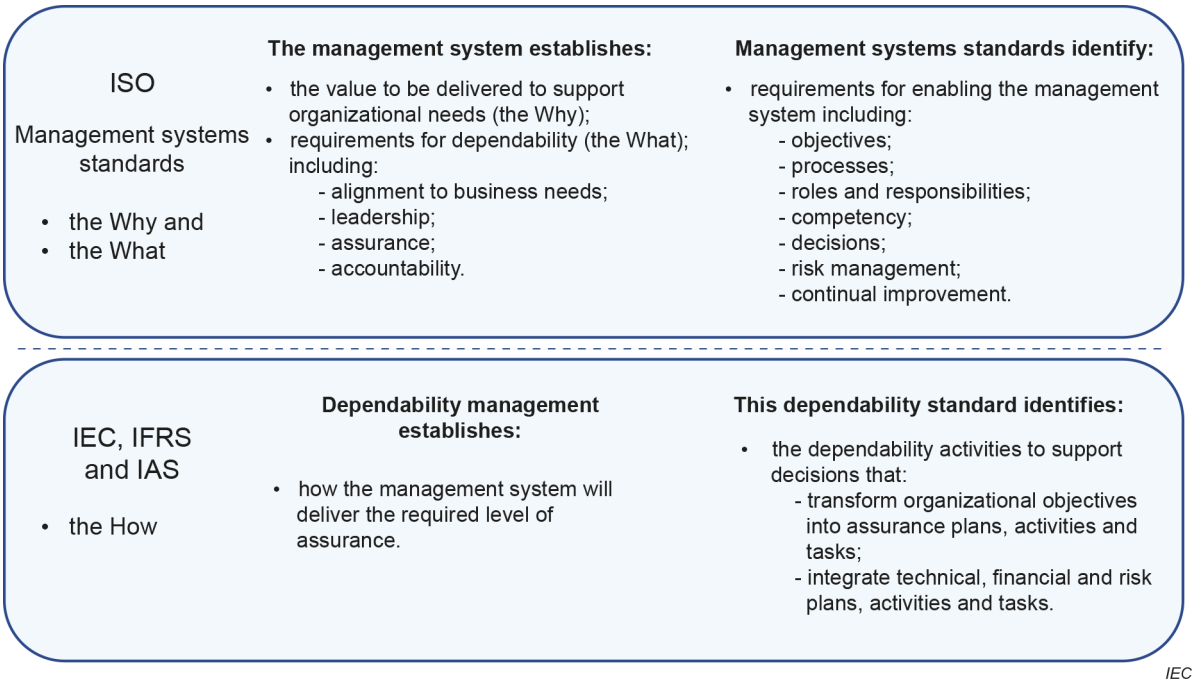


Figure 2 – Relationship between management system standards and dependability standards

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).

Dependability activities can be organised as separate but closely coordinated programmes for reliability, maintainability, supportability, maintenance and support or a combination of these, or be fully integrated into other programmes. The arrangement chosen is determined by technical considerations and stakeholder needs and by the organization's business priorities and values. Programmes can be established on a project-by-project basis or can be organization wide, with flexibility to allow for variations between projects. Variables include the stakeholders of relevance, cost, schedule, quality trade-offs, the technical difficulty of the work and the knowledge and experience of the people involved.

Whatever organizational arrangements are put in place, dependability activities should be coordinated to achieve dependability objectives and integrated with related activities for the project as a whole. The customised selection of dependability activities and tasks for a particular context is sometimes referred to as a dependability programme. Clause 6 discusses the design of a programme of dependability activities.

4.7 Life cycle concept

A system or product, irrespective of its size and complexity, evolves from its initial conception through to its eventual retirement and disposal or re-use. It is generally useful to build a model of this progression to help manage the evolution of the system. Such models are termed life cycle models. A life cycle model is segmented by stages to facilitate planning, provisioning, operating and supporting the system or product of interest. Movement from one stage to another represents the major milestones where investment decisions and resource commitments can be made and incorporated into the management process.

NOTE The concept of a life cycle model, an abstract functional model of the actual life cycle of a system, is detailed in ISO/IEC/IEEE 24748-1.

Dependability activities bring benefits whenever they commence. However the greatest gains are achieved by starting them from the earliest stages of the life cycle because:

- incorporating stakeholders' needs and expectations for dependability from the start helps to maintain stakeholder satisfaction;
- it is cheaper and easier to design-in reliability, availability, maintainability, and supportability and balance them from the earliest stages;
- rectifying problems relating to poor dependability once a system is in operation is often time consuming and costly. An investment in dependability during design activities in the early stages of the life cycle can repay itself in terms of the combined development, realization, utilization and retirement/re-use costs.

IEC 60300-3-3 describes life cycle costing and the relationships between dependability and cost.

There are many different formulations of the life cycle according to the nature, purpose, use and prevailing circumstances of the system or product. A simple generic life cycle model has the following stages:

- concept;
- development;
- realization (including manufacture, transport, acquisition and installation);
- utilization (including operation, maintenance, evolution and enhancement);
- retirement and re-use.

Some alternative life cycle models are described in Annex B.

It is possible that an organization will not have control of or interest in all stages or can require additional detail within a stage to account for the major decision points of relevance to them. For example, in some cases, where the operating stage is extensive, there are likely to be changes in context and usage and perhaps also in requirements. Managing change becomes particularly important. There will also inevitably be some failures and anomalies which will need to be investigated with results fed back to improve dependability. Changes, whether an evolution or significant enhancement, should be made in a controlled manner and the effects of design changes analysed for potential unwanted effects and interactions. Figure B.3 illustrates how change can be managed through the life cycle stages.

4.8 Dependability activity concept

A dependability activity is defined by its purpose, its outcomes and a list of tasks that together achieve the purpose and outcomes. Dependability activities can be considered in two groups:

- programme management activities;
- technical dependability activities.

Programme management activities are those needed to plan, implement, review and improve a set of technical activities that achieve dependability objectives and meet stakeholder needs.

The technical dependability activities described in this document are generic and likely to form some part of any programme. Each activity involves a number of tasks that are selected to achieve the purpose and outcomes of the dependability activity in the context concerned in a cost effective way. Clause 7 describes programme management activities and Clause 8 technical dependability activities.

NOTE In this document a dependability activity, and a task in a dependability activity do not have the same meaning as an activity and a task in ISO/IEC/IEEE 15288 (see 3.1.7). The relationship between the meaning in this document and that in ISO/IEC/IEEE 15288 is explained in Annex F.

5 Integrating dependability into an organization's management system

5.1 Overview

Clause 5 describes how dependability can be incorporated within the requirements of a management system that is assumed to conform to a management system standard that has the harmonized structure of ISO/IEC Directives, Part 1, Consolidated ISO Supplement:2022, Annex SL. Such standards include ISO 55001 (for asset management systems) and ISO 9001 (for quality management systems).

It is not intended that dependability management should be a separate management system. Figure 3 shows the elements of a management system and the dependability management aspects to be incorporated into it. The numbers in the arrows indicate the subclauses in this document where these dependability aspects are described.

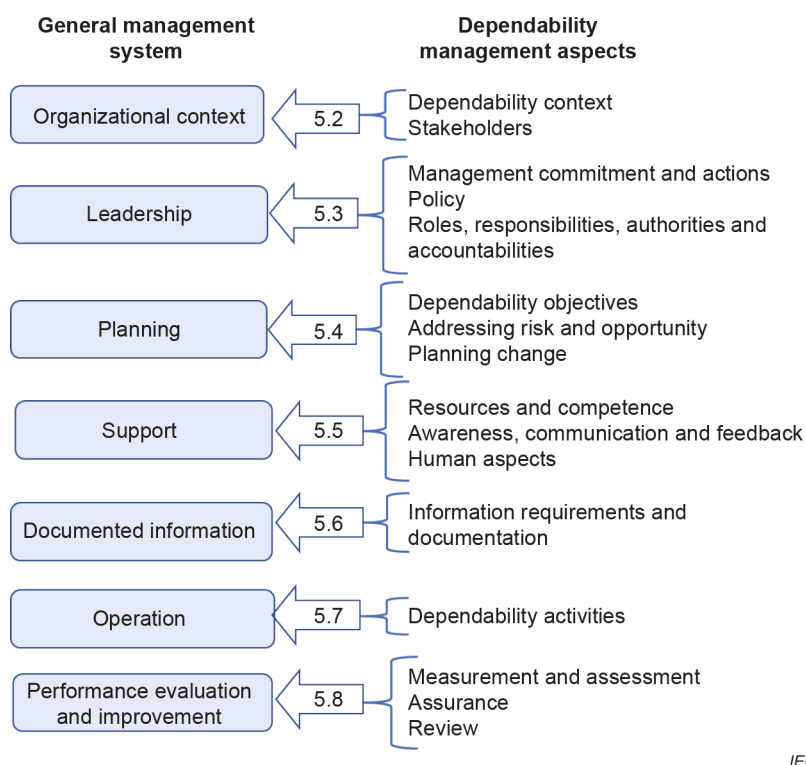


Figure 3 – Integration of dependability into a management system

5.2 Understanding the organization and its context

Organizational arrangements for managing dependability should take into account external and internal issues including the organization's objectives, threats, opportunities and risks.

Internal and external stakeholders with an interest in dependability should be identified and their needs and expectations determined (see Annex C). Stakeholders can change over time, therefore the organization should monitor, review and update information about stakeholders and their needs and expectations.

Dependability is affected by physical and psycho-social factors within the organization and by the performance of external organizations such as suppliers or service providers. Dependability requirements within the system of interest might be achieved, but if internal and external influences are not also understood and managed effectively stakeholder needs and expectations might not be met.

5.3 Leadership

Leaders should recognize the importance of dependability to achieving business objectives and demonstrate their commitment to dependability so that the importance of behaviours that promote dependability is transmitted clearly. They should communicate to external stakeholders the scope of management's accountability for dependability and their commitment to it, and should obtain external stakeholders' consent and confidence. High dependability can only be achieved where dependability is recognized as part of corporate strategy and accorded top management commitment and ongoing focus. Without this, dependability effort is liable to be compromised whenever time or cost pressures arise.

- **Policy:**

Dependability should be referred to in an organization's policy statement. This helps to ensure that appropriate resources are provided, and that the work practices and actions of all staff achieve high quality and dependable outcomes. It also provides accountability to external stakeholders.

- Roles, responsibilities, authorities and accountabilities:

Responsibilities, authorities and accountabilities for roles to manage dependability for different systems, products and services at relevant stages of the life cycle should be assigned. Often more than one organization is involved during the life of a system and some responsibilities and accountabilities need to be passed from one organization to another. Since organizational styles and procedures vary, the way dependability is managed needs to adapt to different situations. The results should be documented as agreements that clarify accountabilities for any failures.

Roles, responsibilities and authorities can change with time. Clarity on accountabilities is also important in this case. In some business areas, such as medical equipment, aerospace and machines, regulatory rules specify strict requirements on accountability and independence.

5.4 Planning

- Defining dependability objectives and planning to achieve them:

Dependability objectives that support the objectives of the organization should be defined, together with accountability for their achievement. Dependability objectives should be considered at organizational and project levels as well as at the level of the requirements of particular systems, products or services (see 7.2.3). Where more than one organization is involved, agreements on the objectives and plans should be recorded as the basis of dispute resolutions and for future improvement.

- Actions to address risks, threats and opportunities:

When planning how to manage dependability, the organization should determine the threats, opportunities and risks that need to be addressed to give assurance that the dependability activities can achieve their intended outcomes. Subclause 7.2 describes planning a programme of dependability activities.

Risks to the dependability of systems, products and services and to the effectiveness of dependability management activities should be identified and understood as part of the organization's risk management processes. Actions should be planned and implemented to address risks, threats and opportunities, taking into account how these can change with time (see 8.3). Managing risk starts from the earliest stages of a life cycle and continues through each stage. Information about risks should be passed from stage to stage and the understanding of risk refined as more information becomes available.

- Planning changes:

Changes should be carried out in a planned manner, taking into account the potential impact on arrangements to manage dependability and on dependability outcomes. This includes considering how dependability will be affected by the availability of resources and the reallocation of responsibilities and authorities. The way dependability is managed needs to be adaptable so that dependability continues to be assured in the face of unplanned changes.

5.5 Support

- Resources and competence:

The organization should provide the resources needed to achieve dependability objectives. Such resources include:

- skilled and motivated personnel;
- specialist expertise to carry out appropriate technical activities and analyses;
- an information and knowledge management system;
- infrastructure including equipment, buildings, hardware and software;
- an appropriate social, psychological and physical environment so people can perform effectively;
- resources to monitor and measure dependability;

- appropriate tools, including software tools and data, for analysis and simulation.

The resources necessary vary with the stage of the life cycle. For example, the development stage requires dependability design expertise and the realization stage can involve resources for detailed verification and testing.

NOTE Technical aspects of support are discussed in 8.6.

- Awareness, communication and feedback:

Perceptions of dependability can vary depending on the stakeholder and over time. Effective communication and consultation with relevant stakeholders should therefore be maintained over time. Information should be provided in a way that is unambiguous, complete, comprehensible, verifiable, consistent, and traceable. The quality of dependability communication and feedback affects customer confidence, trust, satisfaction and loyalty, and regulators' approval as well as the quality of customer care service.

Effective communication improves accuracy in incident reporting and data capture. This facilitates the choice of appropriate corrective and preventive actions.

Relevant feedback can help establish performance trends, identify critical areas requiring attention and provide objective evidence for verification, validation and improvement. A dependability case (see IEC 62741) can be a valuable medium of dependability communication and stakeholder feedback. Stakeholder engagement is discussed in 8.2.

- Human aspects:

People at all levels have a significant role to play in achieving dependability. Specific organizational factors that influence dependability performance include support for decision making and problem solving, communication, supervision, proceduralization and role clarity. Staff should be trained, motivated and given the appropriate resources to be able to perform their work dependably (see IEC 62508). The organization has the ability to support or impede the processes and behaviours that promote dependability. Therefore any approach to dependability should include a means for identifying and improving critical human factors.

5.6 Documented information

The organization should determine the information needed to manage dependability. The data collected should include those necessary to:

- provide confidence that processes have been carried out as intended;
- communicate with stakeholders;
- verify that dependability requirements are or will be met;
- validate that outcomes satisfy stakeholder needs and expectations;
- evaluate and improve dependability activities and their outcomes;
- provide a basis for accountability;
- improve the way dependability is managed.

If a clear purpose for data is not evident then the need to collect it should be questioned.

Examples of information and data relevant to dependability include:

- explicit agreements and accountabilities;
- dependability data from tests and in the field;
- results from dependability analyses;
- configuration control documents;
- information from or for acquirers and suppliers;
- data from DRACAS and FRACAS. Whether a data recording systems is referred to as DRACAS or FRACAS, both failures and successful periods of operation need to be recorded in order to quantify dependability and its contributory elements.

Ownership of dependability data should be defined and a means by which necessary information is communicated through the supply chain put in place. This can be the subject of explicit agreements. Dependability related data should be adequately protected (e.g. from loss of confidentiality, improper use or loss of integrity). A means to control dependability data and information and ensure that it is kept updated and is available when needed should be established as part of the organization's documented information systems. Data collection and interpretation are discussed in 8.5.

ISO/IEC/IEEE 15289 describes the purpose and content of information items that might be relevant.

5.7 Operation

The organization should implement and control dependability activities as outlined in Clause 7 and Clause 8 in order to achieve its desired outcomes.

5.8 Performance evaluation and improvement

The organization should plan and implement processes to monitor, measure, analyse and improve the effectiveness and efficiency of the way it manages dependability. This can be assisted by use of a dependability case (see IEC 62741).

Performance indicators and targets should be defined and performance assessed against them. This could involve:

- evaluating whether the organization's dependability policies and objectives are being met;
- reviewing the suitability of dependability policies and objectives;
- evaluating the dependability of systems, products and services against requirements;
- evaluating the efficiency of operation and effectiveness of dependability activities;
- assessing outcome measures such as customer satisfaction.

One method for self-assessment and improvement is through the use of a maturity matrix. A dependability maturity matrix is a checklist of desired characteristics of dependability management with various levels of achievement defined. It is used to assess current effectiveness and indicate what capabilities are needed next in order to improve performance. An example of dependability maturity matrix is provided in Annex D. Maturity models (also referred to as capability maturity models (CMMs)) can also be used by organizations to assess their software processes. CMM provides a benchmark against which to compare the software development processes that can be used as a predictor of product quality and to drive improvement.

Where possible, existing performance monitoring systems should be used to generate the information needed to improve dependability activities and outcomes. Examples of such systems include:

- DRACAS and FRACAS (see 8.6.3);
- a customer care and feedback system;
- a spares provisioning system;
- a maintenance and support system;
- a condition monitoring system;
- a quality control system.

Dependability aspects of the management system should be included in internal and external audits of the organization's management system and in management reviews.

The organization should identify and exploit opportunities for continual improvement and implement necessary actions to meet customer requirements and enhance stakeholder satisfaction.

6 Programme design

6.1 General

A coordinated set of dependability activities should be undertaken to meet the organization's objectives for dependability and stakeholder's needs. It should be customised to the organization and to the systems, products and services of interest. Clause 6 describes considerations for designing such a programme including coordination and integration with other activities, trade-offs and key success factors. Clause 7 describes how to plan, implement, review and improve a programme that is tailored to circumstances. Clause 8 describes technical dependability activities and tasks that can be included in the programme.

A plan should be developed for implementing the programme, with accountabilities, authorities and timelines defined (see 7.2). Human and organizational factors required to support the plan should be identified and incorporated into the programme. The people involved in implementing the plan at any stage in the life cycle should be aware of their responsibilities and accountabilities, and be adequately supported and competent.

6.2 Coordination and integration

Dependability can be managed as a separate programme by a dedicated organizational unit, be fully integrated into relevant areas, such as product development or manufacturing, or be a mixture of the two approaches. In some organizations the responsibility for dependability (like quality) rests with a separate department. (This is required for companies that approve their own products, for example for the European CE-marking system). For a large organization it can be worthwhile to set up a cross-departmental entity to serve the overall needs of the organization in an efficient manner. This helps eliminate duplication of effort and ensure consistency of dependability activities while enabling the highest level of expertise to be applied. In all cases the alignment of organizational structures, responsibilities, accountabilities, activities, resources and information is critical for efficient management.

It is generally more efficient to integrate dependability activities and tasks with those relating, for example, to scheduling, design, production, and operations and to develop an overall project plan. Coordination and integration are also important because it can be necessary to trade-off dependability against other stakeholder needs or organizational objectives.

Risks identified as part of the development of a dependability case or through the use of tools such as FMEA (see IEC 60812) should be integrated into the overall project risk management process. This provides better awareness of risks across a project, encourages a common view of the acceptability of risks and enables more efficient treatment strategies. Guidelines for managing risk in any context are provided by ISO 31000. IEC 31010 describes risk assessment techniques and how they are used and IEC 62198 provides guidance on managing risk in projects.

Coordination between different dependability activities within the same project, as well as between different projects, should be actively managed so that resources are used effectively. For example reliability, maintainability and supportability activities could use the same analysis tools and data sets (if for different purposes). Responsibility, authority and accountability for coordination should be assigned.

6.3 Trade-offs

A trade-off is a decision where one feature is diminished in return for gains in another. In dependability this can be because of limitations in resources or in the design. Trade-offs are made by considering the advantages and disadvantages of the characteristics being traded in the context concerned. Priorities that drive decisions about trade-offs and hence programme design should be agreed with relevant stakeholders.

Types of trade-off relevant to managing dependability include the following:

- Within a specific dependability attribute: For example, a high reliability can be achieved by designing a highly reliable item or by incorporating redundancy. Similarly, maintenance down time can be reduced by conducting preventive maintenance during operation or during a scheduled shut down.
- Between dependability attributes: For example the choice can be made between low reliability items that are cheap initially but are expensive to maintain, and high reliability items that can be expensive to design and construct but require little maintenance. Decisions relating to maintainability and maintenance influence the type of support (such as spare parts and maintenance skills) which affects supportability. The attributes of components can be combined in different ways to deliver the same overall availability.
- Between dependability and other criteria such as safety or performance: For example, the inclusion of safety features and safety systems can make an item so complex to use that its dependability is reduced. Other functional and non-functional requirements such as form, fit and function compatibility can also impact dependability.
- Between the effort put into the dependability programme (hence its costs and schedule), and the value added by it (e.g. improved stakeholder satisfaction, brand value and the overall savings from improved dependability): For systems and products with a long life, operational costs, particularly the cost of maintenance, can dominate life cycle costs. Additional effort spent in design can therefore produce significant cost savings later. However improved dependability can have to be traded off against meeting the project's schedule and budget. Decisions depend on the level of risk the organization is prepared to accept.

The trade-offs that are made should be explicit and decisions documented.

6.4 Tailoring a technical programme of dependability activities

The purpose of tailoring is to design a programme of dependability activities and tasks that achieve the specific dependability objectives within applicable constraints in a cost effective way. Examples of tailoring include:

- budget planning for the allocation of dependability resources or outsourcing in order to meet project delivery time scales;
- determining the activities and tasks that will provide on-going confidence that the dependability requirements will be achieved;
- deciding on the best approach to performing a particular activity in the particular context.

Programme design depends on:

- a) objectives, including any specified requirements (see 7.2.3);
- b) the nature of the system, product or service concerned;
- c) the relevant life cycle stages;
- d) the time frame adopted by the organization;
- e) the engineering approach.

EXAMPLE The engineering approach in the design stage would consider whether the design was for:

- a brand new item;
- an item based upon previous item designs;
- a system utilising the latest off-the-shelf technology;
- a transitional service such as manual to automated or electronic driven to software driven.

In some cases a statement of work from a customer, agreements with other stakeholders and internal policies define the tasks that need to be performed.

Other approaches include:

- reviewing an existing programme and its activities and tasks to see where improvements can be made and tailoring it to the particular circumstances;
- use of a dependability case where structured arguments are made and evidence is provided to support the claim that a system meets its dependability requirements. The activities and tasks needed to provide the evidence in support of the claim represent those activities and tasks required to achieve and assure dependability (see IEC 62741).

Where an organization has an existing dependability programme, criteria and guidelines can be developed for tailoring this to specific circumstances. This could involve a set of activities which apply in all cases and to which additions are made, or a set of activities from which those required in a particular case are selected.

6.5 Key success factors

Key factors that contribute to the success of the programme include:

- incorporation of dependability considerations into decision-making from an early stage;
- a common understanding of the system or product, its dependability needs and the means of achieving them;
- clearly defined and agreed responsibilities and accountabilities for meeting dependability requirements;
- effective coordination and integration among the various organizational entities that will be involved;
- an understanding of the factors that affect the dependability and costs of a particular system, product or service;
- an understanding of trade-offs that need to be made.
- provision of adequate resources (including competent personnel) for the dependability activities and tasks to be undertaken;
- incorporation of tasks that support, analyse and improve human performance;
- effective collection and use of information and data;
- customization to organizational, stakeholder and project needs.

7 Programme management activities

7.1 Overview

Clause 7 describes the activities required to establish a programme of technical dependability activities, namely:

- a) planning the programme to achieve objectives within the applicable context and constraints;
- b) implementing the plan;
- c) reviewing and improving the programme and plan;
- d) providing assurance that dependability objectives are achieved;

e) achieving accountability.

The overall management system and structures that support dependability activities are discussed in Clause 5.

7.2 Plan dependability activities

7.2.1 Purpose

The purpose of planning is to select and coordinate a set of dependability activities that achieve the organization's objectives for dependability in a cost effective way and to integrate these into related project plans and processes.

7.2.2 Outcomes

As a result of planning:

- a) the organization's objectives for dependability are defined;
- b) a clear approach for achieving those objectives is articulated;
- c) technical dependability activities, tasks and tools are selected;
- d) entry and exit criteria for each dependability activity are established;
- e) responsibilities and accountabilities for performing dependability tasks are defined and assigned to appropriate roles;
- f) information and resource requirements for tasks are defined;
- g) a schedule for the programme is developed;
- h) a dependability plan is developed including provisions for change of the programme;
- i) the dependability plan is integrated into the other relevant plans.

7.2.3 Tasks

The following tasks should be undertaken in accordance with organizational policies.

- a) Identify the programme objectives. These can include:
 - achieving dependability objectives or requirements for a system, product or service;
 - providing evidence that dependability objectives or requirements have been achieved;
 - satisfying legal or contractual requirements;
 - managing life cycle costs;
 - improving efficiency;
 - improving the capability of the organization to support human performance, including workers and product users, so that the full capability of the technical systems is achieved;
 - increasing stakeholder confidence;
 - improving support;
 - achieving specific targets or milestones;
 - satisfying safety and environmental requirements.
- b) Define the programme context. This can include:
 - defining the boundaries (open or closed) of the system, product or service under consideration;

EXAMPLE 1 A supplier of consumer goods to a general market might specify the dependability characteristics of the hardware and software which they are supplying, whereas a user might wish also to include human operators and external utilities.

EXAMPLE 2 A supplier of a bank teller terminal might set the boundary to include only hardware and software, and then specify their dependability characteristics. On the other hand, a bank customer might wish also to include human operators and connected server services in the boundary and to know the overall dependability characteristics.

- identifying stakeholders;
 - defining the life cycle model relevant to the situation and determining the specific life cycle stages that are applicable;
 - identifying relevant characteristics of the system, product or service to which the programme applies, such as its features, functions, novelty and complexity and application environment;
 - identifying the outputs or evidence required by relevant stakeholders.
- c) Identify programme constraints. These can include:
- the budget;
 - available time and resources;
 - technological capability;
 - expertise available;
 - other resource requirements (e.g. personnel, organizational policy and infrastructure);
 - acceptable risk;
 - management time and focus;
 - legal and contractual requirements.
- d) Identify risks to programme objectives.
- e) Identify the evidence necessary to provide assurance that the objectives are achieved.

NOTE 1 Identifying necessary evidence, and planning to obtain it, starts as soon as objectives are identified. Assurance that objectives are being, or have been, achieved is provided on an on-going basis.

- f) Identify the technical dependability activities required to achieve the programme objectives and the tasks and tools needed to achieve the required outcomes.
- g) Prioritize the dependability activities, tasks and tools, considering the objectives, constraints, context and risks.

NOTE 2 Multiple tools can be required to provide a single outcome.

- h) Determine the minimum depth and detail required from each tool selected in order to achieve the desired aims with the necessary confidence. This will assist in allocating resources and optimizing cost.
- i) Compare the time, capability and resources required to complete each task to the necessary depth with the resources available.
- j) Assess whether the planned dependability effort adds value and modify the programme if not. This can involve a cost benefit analysis of each activity taking into account the cost of failures, life cycle costs of ownership and the costs of dependability activities.
- k) Make decisions about trade-offs including the possibility of modifying objectives.
- l) Select the dependability activities and tools which will provide the desired programme objectives within the given constraints.
- m) Document the planning decisions and the details of how the dependability activities will be implemented. The dependability plan can be integrated into other plans, such as a quality plan or an overall project plan. It should state, as a minimum:
- the dependability objectives;
 - the required dependability activities, tasks and tools, and the justification for their inclusion;
 - the timing of dependability activities, the sequence, where relevant, and interactions between them, so they can be timed to give inputs to important development decisions;
 - the evidence and outputs required;

- milestone events and the entry and exit criteria for each step, including the conditions under which activities and tasks require ongoing review or are considered complete;
 - the estimated schedule and any dependencies between elements of the programme (the schedule can have to consider pressures from other business priorities and project plans);
 - responsibilities and accountabilities;
 - arrangements for dependability reviews.
- n) Plan for monitoring changes in the programme context, for reviewing progress of the programme, and for triggering re-planning according to defined criteria.

7.3 Implement the plan

7.3.1 Purpose

The purpose of implementing the plan is to achieve dependability objectives in an efficient and cost effective way that complies with relevant contracts, regulations and standards and satisfies stakeholders.

7.3.2 Outcomes

As a result of implementing the plan:

- a) organizational and stakeholder objectives with respect to dependability are met;
- b) stakeholders are aware of their responsibilities and accountabilities, and accountability for dependability is achieved;
- c) dependability is efficiently integrated into technical processes;

EXAMPLE Risk assessments relating to dependability can be combined with other project risk assessments and stakeholder engagement arrangements can be common across a wide range of issues.

- d) people tasked with implementing the plan at any stage in the life cycle are competent and adequately supported in their roles;
- e) the outcomes of technical activities (see Clause 8) are achieved;
- f) assurance is provided that dependability objectives have been or will be met (see 7.5);
- g) systems are established to collect, store and analyse dependability data.

7.3.3 Tasks

The following tasks can be involved in implementing a dependability plan.

- a) Engage with stakeholders to establish their needs, expectations and requirements on an ongoing basis and to keep them informed as appropriate (see 8.2).
- b) Provide information and training so that people are aware of their responsibilities and accountabilities and are competent to perform them.
- c) Establish explicit agreements between stakeholders, including accountabilities for fulfilling them.

Explicit agreements among stakeholders and accountability for fulfilling them are particularly important for systems with extended operational life or with changing and difficult-to-define boundaries. For those open systems, activities focused on consensus building and accountability achievement are required. See IEC 62853.

- d) Provide resources and support for dependability activities and the people involved in implementing them.
- e) Document decisions and actions to provide traceability and accountability. A dependability case can be used for this purpose (see IEC 62741, ISO/IEC/IEEE 15026-2 and ISO/IEC/IEEE 15026-4).

- f) Establish systems for monitoring the dependability of the system, product or service and the efficiency and effectiveness of dependability tasks.

7.4 Review and improve

7.4.1 Purpose

The purpose of reviewing dependability is to:

- a) provide assurance that specific objectives from both technical and business perspectives are being met throughout the life cycle;
- b) provide feedback on dependability deficiencies, deviations and risks;
- c) improve the dependability of systems, products and services and of the workforce;
- d) improve the way dependability is managed;
- e) determine the status of projects;
- f) assess the need for, and cost effectiveness of, dependability activities;
- g) recognize change and the need to adapt.

7.4.2 Outcomes

As a result of undertaking reviews:

- a) individual, organizational or technical weaknesses are identified and corrected early;
- b) systems, products and services and the dependability programme are improved;
- c) schedules and budgets are met;
- d) risks are identified and treatments implemented effectively.

7.4.3 Tasks

The following tasks should be undertaken in accordance with applicable organizational policies.

- a) Plan the scope and timing of reviews.

Dependability is reviewed at each stage of the life cycle of a system, product or service, particularly when moving from one stage to another or when responsibility for a project is transferred. The scope can be:

- technical, covering design and dependability performance aspects of a system, product or service or
- management focussed, covering cost and scheduling aspects of a project or the dependability programme.

- b) Identify stakeholders and involve them as appropriate.
- c) Review requirements on a regular basis to account for changing stakeholder needs, operating conditions and new technologies.
- d) Coordinate with, and participate in, other organizational and project reviews.

EXAMPLE 1 Design reviews normally incorporate both dependability and performance aspects.

- e) Identify targets.

EXAMPLE 2 Targets can be dependability requirements, or project timelines and budgets, etc., relevant to dependability.

- f) Collect evidence and information.
- g) Prepare for and conduct meetings.
- h) Assess the gap between required and actual performance.
- i) Identify and monitor risks and areas of concern.
- j) Analyse outcomes of review and recommend actions.

k) Check the effectiveness of changes made.

Dependability reviews that are carried out throughout the life cycle, including details of the tasks involved, are discussed in IEC 62960.

7.5 Providing assurance

7.5.1 Purpose

The purpose of dependability assurance is to give managers and other stakeholders justified confidence that their dependability objectives have been, or will be, achieved and that risks are controlled to an acceptable level. Assurance can relate to any aspect of dependability objectives (see 7.2.3).

NOTE This dependability activity is a version of the assurance process view provided in ISO/IEC/IEEE 15026-4 that is specific to the assurance of dependability.

7.5.2 Outcomes

As a result of providing assurance:

- a) stakeholders unambiguously understand the claimed achievement of dependability objectives by an explicit statement of dependability performance;
- b) it is verified that processes and systems, products and services conform to their requirements, standards and guidance and that defined procedures are followed;
- c) a justified statement of dependability performance can be provided;
- d) evidence and arguments are presented that provide stakeholders with the required level of confidence in the claimed achievement of dependability objectives;
- e) stakeholders, including managers, have greater confidence that stakeholder needs, objectives, expectations and requirements, as well as business objectives, have been, or will be, achieved.

7.5.3 Tasks

The following tasks should be undertaken in accordance with applicable organizational policies.

- a) Engage with stakeholders to establish their needs, expectations and requirements on an ongoing basis and to keep them informed as appropriate (see 8.2).
- b) Provide evidence that risks of not achieving a dependability objective have been identified and addressed and opportunities to improve dependability have been exploited (see 8.3).
- c) Provide evidence in the form of analysis that demonstrates that dependability can be achieved when direct measurement is impracticable or not appropriate (see 8.4).
- d) Collect and evaluate data relating to dependability performance of the system, product or service or its components, in use or under test conditions (see 8.5).
- e) Verify that requirements are, or will be, achieved and that any non-compliances have been corrected using evidence from b), c) and d) above.
- f) Verify that procedures are followed through inspection, review and audit, etc.
- g) Validate that systems, products and services meet stakeholder needs and expectations.
- h) Provide evidence that support is provided to sustain the performance of people and the capability of the system, enabling it to adapt to changing needs (see 8.6).

Progressive assurance that dependability requirements are being met or will be satisfied throughout the life cycle of a system can be provided through a dependability case (see IEC 62741). This provides:

- a set of claims that formulate the contention that dependability is achieved;
- a reasoned auditable argument supporting the set of claims;

- evidence that risks have been treated and the claim has been or will be achieved.

NOTE 1 Progressive assurance means that assurance tasks are carried out through the life cycle and results provided at project milestones. This reduces the risk of finding out only at the end of a project that the evidence is inadequate.

NOTE 2 The dependability activities and tasks necessary to provide evidence relating to a dependability claim also define the necessary dependability activities and tasks of a dependability programme.

7.6 Achieving accountability

7.6.1 Purpose

The purpose of the accountability achievement activity is to establish the relationship between a noncompliance with an explicit agreement and its implications for stakeholders and society in general. This includes ensuring that accountable stakeholders will fulfil their obligation to provide agreed remedies for damage caused by noncompliance, so as to gain confidence and trust in the system among non-accountable stakeholders and general public.

NOTE 1 Explicit agreements can include the acquisition contract on the system, specified system requirements, assurance of identified dependability claims or a specified dependability programme. They can involve external and internal stakeholders and the general public (via, e.g. regulations).

NOTE 2 IEC 62853 provides a more detailed instance of this dependability activity as the accountability achievement process view.

7.6.2 Outcomes

As a result of achieving accountability:

- a) for any noncompliance with explicit agreements, including a system failure, the affected stakeholders and, if relevant, the general public are able to identify the accountable stakeholders;
- b) the affected stakeholders and, if relevant, the general public are provided with adequate information and agreed remedies by the accountable stakeholders;
- c) information on readiness for a) and b) is available at any time, even before an event occurs, such that:
 - all stakeholders are aware of their accountability;
 - all stakeholders and general public have confidence in what will happen if the system fails or noncompliance with explicit agreements occurs.

NOTE Accountability achievement crucially complements dependability assurance in providing confidence and trust in the system. Confidence in what happens when dependability claims do not hold has significance independently of the required level of confidence in dependability claims, providing a possibility of trade-off between the two.

7.6.3 Tasks

The following tasks should be undertaken in accordance with applicable organizational policies:

- a) for each potential noncompliance with explicit agreements:
 - identify key decisions in the system life cycle and dependability activities that can cause the non-compliance;
 - identify the accountable stakeholder for each key decision;
 - assess the impacts of noncompliance on the non-accountable stakeholders and general public;
 - agree on the implications of non-compliance for the accountable stakeholders and also for the non-accountable stakeholders and general public, including remedies the accountable stakeholders will be obliged to provide;
- b) monitor, assess and feed back to the accountable stakeholders, the anticipated and unanticipated outcomes of key decisions, including noncompliance and its actual impacts;

- c) enable the accountable stakeholders to promptly provide adequate information and the agreed remedies to the non-accountable stakeholders and general public when a noncompliance occurs;
- d) communicate to all stakeholders and, where relevant, the general public how a), b) and c) are implemented.

8 Technical dependability activities

8.1 Overview

Clause 8 describes the technical dependability activities that aim to achieve dependability requirements and provide assurance that they have been or will be achieved. These are:

- stakeholder engagement (including consensus building and consultation);
- managing opportunities, threats and risks to dependability objectives;
- analysis of dependability attributes (including mathematical and statistical analysis, modelling, simulation and prediction of dependability attributes and life cycle costs);
- dependability assessment (including collection and evaluation of information and data);

NOTE Information and data include operating and test data relating to a system, product or service and information and data to support dependability and project management.

- maintenance, support and improvement.

Annex E provides examples of tasks and tools that can be applicable at each life cycle stage.

Annex F explains how these dependability activities can be related to the system life cycle processes provided in ISO/IEC/IEEE 15288.

Activities relevant to maintainability and supportability programmes are also covered in IEC 60300-3-10 and IEC 60300-3-14.

8.2 Stakeholder engagement, consensus building and communication

8.2.1 Purpose

The purpose of engaging with stakeholders in the context of dependability is to:

- a) achieve and maintain positive relationships with internal and external stakeholders;
- b) understand stakeholder needs and expectations so that dependability requirements can be articulated and achieved, and their achievement trusted;
- c) establish the basis of accountability through explicit agreements;
- d) establish and promote a common understanding of the system that enables dependability problems that are not anticipated in explicit agreements to be resolved;
- e) provide input to identifying risks so they can be treated as early as reasonably practicable;
- f) enable dependability activities to be efficiently integrated into projects and into business and technical processes;
- g) enhance the performance of the workforce so that the technical capabilities of the system and products can be fully realized and human dependability problems can be resolved;
- h) receive feedback from stakeholders to assist improvement.

Stakeholder engagement should commence at the first available opportunity and be ongoing throughout the life cycle. Stakeholders that can be relevant in a particular context are detailed in Annex C.

8.2.2 Outcomes

As a result of engaging with stakeholders:

- a) positive relationships are established with managers, project managers, customers, suppliers, regulators, etc., as appropriate;
- b) managers and staff are aware of the importance of dependability and motivated and supported to achieve it;
- c) there is a common understanding between relevant stakeholders of the purpose of the system, product or service, of its constraints and dependability requirements, and of responsibilities, accountabilities and authorities;
- d) stakeholder needs and expectations are understood and translated into verifiable requirements;
- e) dependability requirements and data are effectively communicated to appropriate stakeholders through different stages of the life cycle;
- f) explicit agreements are formulated and maintained that include agreements on accountability of each stakeholder in the event of non-compliance;
- g) traceability of dependability requirements to stakeholders and their needs is established;
- h) stakeholders are assured that their dependability expectations are being met;
- i) risks of not achieving dependability requirements are identified and treated as early as reasonably practicable;
- j) failures and successes are reported and understood so dependability can be improved;
- k) key decisions and agreements are recorded together with the rationale for them so that accountability can be traced and lessons learned when decisions turn out to be faulty;
- l) weaknesses in workforce or organizational performance, which might impair dependability, are identified and mitigated so that technical capabilities can be fully realized.

8.2.3 Tasks

The following tasks should be undertaken in accordance with applicable organization policies and outcomes required.

- a) Identify internal and external stakeholders and assess and document their interest and influence.

NOTE 1 Stakeholders can change over time, for example when ownership changes, when moving between stages of the life cycle or when there is a long utilization stage.

- b) Identify those stakeholders that should be involved in particular dependability tasks, such as risk assessment or verification, and those to whom results should be communicated.
- c) Develop communication plans.
- d) Develop a policy on managing changes to agreements.
- e) Engage with stakeholders in accordance with the communication plans.
- f) Agree on an arbitration process to resolve conflicts when consensus cannot be reached.
- g) Elicit and document stakeholder's needs, expectations and accountabilities for dependability. Consideration should be given to the following:
 - the stakeholder's intended use of, or interaction with, the system, product or service and its operating environment and life profile;
 - any accountabilities stakeholders have with regard to the system, product or service and its management, use or support;
 - stakeholder needs, wants and expectations with regard to reliability, availability, maintainability, supportability and any other dependability related requirements;
 - any constraints which will influence how dependability is managed;
 - how relevant dependability attributes can be measured or otherwise assured.

- h) Analyse stakeholder expectations and identify and resolve any conflicts.
- i) Establish and maintain explicit agreements, and record accounts of negotiations and the rationale for decisions taken.
- j) Communicate information associated with dependability to relevant stakeholders on a timely basis.
- k) Obtain feedback on dependability issues for problem resolution and continual improvement.
- l) Periodically review stakeholders and communication plans and update as necessary.

NOTE 2 IEC 62853 provides the consensus building process view, which details that part of the dependability activity concerning consensus building.

8.3 Managing opportunities, threats and risks

8.3.1 Purpose

The purpose of managing opportunities, threats and risks in the context of dependability is to:

- a) achieve dependability objectives and improve decision making by understanding and managing the effects of uncertainty on those objectives;

NOTE Dependability objectives include achieving the requirements of the system, product or service and any other organizational objectives that could affect or be affected by dependability activities, for example objectives relating to safety, to the environment or to customer satisfaction.

- b) understand how failures might occur so as to prevent failures or mitigate their effects;
- c) exploit opportunities to improve dependability and dependability activities;
- d) set priorities (of, for example, dependability objectives and activities) on the basis of risk;
- e) provide assurance by demonstrating that risks to dependability have been controlled.

8.3.2 Outcomes

As a result of managing risk, threats and opportunities:

- a) risks to the dependability of systems, products and services and to dependability activities are identified, understood and controlled;
- b) the efficiency of a programme of dependability activities is improved as activities are directed to best manage risk;
- c) opportunities to improve dependability and dependability activities are exploited;
- d) decisions are based on a good understanding of opportunities, threats and risks, and are justifiable and traceable;
- e) human actions and organizational processes, as well as systems, products and services fail less and are more dependable;
- f) the uncertainty in data is understood and where appropriate quantified;
- g) there is an understanding of how systems can fail, enabling designs to be improved and cost effective maintenance and support programmes to be implemented;
- h) change, and the need for enhancement, are identified and managed effectively;
- i) preparation is made for potential failures, including generic responses to failures that have not been recognized in advance;
- j) information about risks is available to those that need it;
- k) assurance is provided that risks are managed commensurate with the organization's appetite for risk.

8.3.3 Tasks

The following tasks should be undertaken as appropriate to the context.

- a) Identify stakeholders who should be involved in activities to assess risks, and those who should be kept informed.
- b) Establish a mechanism to communicate and consult about risks and their treatment to appropriate stakeholders.
- c) Determine the scope, context and timing of risk management tasks and how they should be included within the scope of the organization's other risk management activities.
- d) Decide how acceptable risk will be defined.
- e) Identify opportunities, threats and risks and take them into consideration in decisions made at each life cycle stage. Tools for identifying risks include failure modes and effects analysis (IEC 60812), HAZOP (IEC 61882) and other tools as described in IEC 31010.
- f) Analyse risk by looking at causes, consequences and the controls already in place. Where appropriate determine the probability that particular consequences will occur. Tools such as fault tree analysis (IEC 61025) and event tree analysis (IEC 62502) can be used (see also IEC 31010).

NOTE 1 Tools used for dependability analysis can also be used to analyse risk more generally.

- g) Coordinate risk management activities and the use of risk assessment tools to avoid duplication of effort.
- h) Identify opportunities and analyse them by comparing expected benefits and the risks of either pursuing or not pursuing the opportunity.
- i) Apply the understanding of risks in the design of the programme through each life cycle stage.
- j) Plan and implement actions based on the understanding gained from risk analysis so that unacceptable risks are treated.
- k) Allocate responsibilities, authorities and accountabilities for actions relating to risks and the risk management framework.
- l) Monitor the status of risks and their treatments.
- m) Analyse direct and underlying causes of failures so that lessons can be learnt and failures prevented (see IEC 62740).
- n) Monitor changes in the environment, context and purpose, etc., and analyse how they affect risk.
- o) Monitor anticipated and unanticipated outcomes from decisions, and relay results in a timely manner to improve failure response and accountability achievement.
- p) Collect, analyse, store, review and update information on risk, through the life cycle.
- q) Follow up recommended actions relating to risk, threats and opportunities.

NOTE 2 Guidance on the risk management principles, framework and process is given in ISO 31000. Managing risk in projects is discussed in IEC 62198 and risk assessment tools in IEC 31010.

8.4 Dependability analysis

8.4.1 Purpose

The purpose of dependability analysis is to provide a technical understanding of the system, product or service and factors affecting its dependability and life cycle costs. This can be used:

- as an input to decisions;
- to model and predict dependability outcomes of a design;
- to achieve and improve dependability in a cost effective way;
- to verify that requirements are being or can be met.

Analyses are also performed as part of managing opportunities, threat and risks (8.3), dependability assessment (8.5) and to verify safety, for example safety integrity level (SIL) for systems that include electronic safety related items (see the IEC 61508 series) and automotive safety integrity level (ASIL) for cars (see the ISO 26262 series).

8.4.2 Outcomes

As a result of dependability analysis:

- a) a technical understanding of the system, product or service and its operating environment is obtained;
- b) common characteristics and worst case constraints of the operating environment are identified;
- c) dependability, cost and risk characteristics of design options are predicted and compared;
- d) a cost effective design is selected that can be demonstrated to achieve requirements within specified conditions and constraints;
- e) assurance is provided to stakeholders that their needs and requirements for dependability have been or will be met;
- f) the system is designed with consideration of its eventual retirement taking into account the circular economy and the need to minimise environmental impact;
- g) potential failure modes are identified so they can be prevented or their effects mitigated;
- h) cost implications of decisions relating to dependability are understood;
- i) factors affecting reliability, maintainability, supportability and other dependability related attributes such as availability, operability, usability, durability, etc., are understood and trade-off decisions made;
- j) the roles of hardware, software and people in a system are optimized so that their performance does not impair the overall capabilities of the system;
- k) systems and products are retired in a way that is safe, secure, environmentally sound and in line with legislation and standards.

8.4.3 Tasks

Dependability analysis can include the following tasks.

- a) Map design characteristics to the end user environment to assist in defining requirements or selecting design options.

NOTE 1 Factors to consider can include electromagnetic compatibility, thermal conditions and mechanical stresses.

- b) Predict values for dependability attributes.
- c) Undertake an iterative process of analysis and improvement as the design progresses to improve dependability.
- d) Perform regression analysis to verify that changes have not affected the existing functionality of a system, product or service.
- e) Undertake life cycle cost analysis to optimize dependability performance within given life cycle cost constraints (see IEC 60300-3-3).
- f) Conduct trade-off analyses.
- g) Analyse potential failure modes, causes and effects in order to improve designs, plan maintenance and support programmes and plan failure response (IEC 60812).

NOTE 2 Techniques used for root cause analysis can also be used proactively to identify failure modes and causes (see IEC 62740).

- h) Analyse the dependability of the system by modelling stress conditions and corrupted or illegal data inputs.

- i) Analyse the effect of human performance on dependability activities and dependability attributes of the system, product or service. Where relevant, develop programmes to improve human error rate (IEC 62508).
- j) Analyse processes used in manufacture, delivery and installation to minimize impact on dependability. Process FMEA can be used (see IEC 60812).
- k) Analyse design changes and enhancements for safety and operability issues (see IEC 61882) and check intended improvements will be achieved.
- l) Analyse systems prior to retirement for potential second hand use or for re-use of modules, components and materials (see IEC 62309). Consider means of safe transfer or deletion of data.

NOTE 3 The systems analysis process (ISO/IEC/IEEE 15288) provides generic tasks that apply for any analysis task. A comparison of the two approaches is given in Annex F.

Analyses relevant to reliability, maintainability and supportability are discussed in IEC 62308, IEC 62508, IEC 60300-3-1, IEC 60300-3-10 and IEC 60300-3-14.

8.5 Dependability assessment

8.5.1 Purpose

The purpose of dependability assessment is to:

- r) determine dependability characteristics of a system, product or service;
- s) verify that the dependability of people, systems, products, services and processes meets requirements;
- t) validate that dependability meets stakeholder needs;
- u) detect and remove defects;
- v) monitor dependability as improvement strategies are implemented to meet business needs (e.g. to enhance dependability performance, reduce costs and improve timeliness of product releases);
- w) learn from operational data and tests to improve design;
- x) improve the way dependability activities are carried out;
- y) assess the dependability aspects of a project;
- z) provide information for dependability reviews (see IEC 62960).

NOTE ISO/IEC/IEEE 15288 describes the project assessment and control life cycle process that can be applied to assess dependability aspects of a project.

8.5.2 Outcomes

As a result of dependability assessment:

- a) performance measures are available;
- b) information needs and data collection methods are identified;
- c) information and data are collected, verified and stored;
- d) data are analysed and the results interpreted and reported;
- e) dependability characteristics for the system, product or service are known and quantified where possible;
- f) desired dependability characteristics are achieved, verified and validated;
- g) information and data are available, enabling dependability and its management to be improved;
- h) traceability of results is established;
- i) stakeholders are provided with the data they need in the format and within the time scales required;

j) project and dependability objectives are achieved.

8.5.3 Tasks

Dependability assessment can include the following tasks.

- a) Identify the problem or question that requires assessment.
- b) Determine stakeholder needs and requirements and the form of output required.
- c) Determine how dependability attributes will be measured or otherwise verified and the data required.
- d) Determine the inputs and associated data required to perform the assessment.
- e) Determine test conditions, data requirements and test methods (see IEC 60300-3-5).
- f) Determine resources available and constraints (e.g. time, funding, samples, personnel, tools and facilities). It is important that test results are ready to provide input to critical decisions. This can influence the design of the test procedure.
- g) Determine the source of data and how and when data will be collected (e.g. from simulations and models, from tests in a simulated environment, from observations during normal operation or from manufacturers data, etc.).

NOTE 1 Data from suppliers of components and modules, or from field observations and tests of similar systems, products and services can be used to predict and improve dependability during design (see IEC 62308).

NOTE 2 IEC 60300-3-2 provides guidance on the collection of data from the field.

- h) Integrate dependability assessment into relevant processes.
- i) Collect information and data. This can involve measuring dependability attributes, monitoring the performance of systems, products and services to check that performance is not degraded over time, surveys, observations and tests (see Annex G).
- j) Interpret data.
- k) Compare actual dependability characteristics with those desired, implement improvements and conduct regression tests as required (see IEC 61014).
- l) Record data in such a way that traceability can be achieved between product changes and cost and performance outcomes.
- m) Store data so it can be used for future reference.
- n) Communicate outcomes to stakeholders as appropriate.

Techniques for reliability testing are discussed in IEC 60300-3-5 and for maintainability testing in IEC 60300-3-10. Software testing techniques are covered in ISO/IEC/IEEE 29119-4.

8.6 Maintenance, support and improvement

8.6.1 Purpose

The purpose of maintenance, support and improvement in the context of dependability is to:

- o) sustain the performance of the system, product or service;
- p) manage life cycle costs;
- q) enable systems, products and services to continue to meet dependability objectives during operation in a cost effective way;
- r) manage information necessary for ongoing operation and for future improvement, (including data on faults and failures);
- s) minimize harm and disruption from failures;
- t) maintain fit for purpose status of the system or product despite changes in requirements, environments, objectives and purpose;
- u) manage obsolescence (see IEC 62402);

- v) support and enhance the capability of the stakeholders (e.g. workers or users) to operate the system or use the product;
- w) improve the dependability of systems, products and services and the efficiency and effectiveness of dependability activities.

8.6.2 Outcomes

As a result of the maintenance, support and improvement activity:

- a) systems, products and their components are designed so that they are safely and reliably operable, maintainable, testable and re-useable;
- b) user requirements for maintainability and for availability during operation are achieved and assured;
- c) maintenance programmes are planned and implemented;
- d) support is organized and operates effectively;
- e) people are supported to perform their roles effectively and efficiently;
- f) risks to maintenance and support arrangements are identified and treated;
- g) the effects of failures are minimized;
- h) the system, product or service performs as required despite changes in requirements, environments objectives and purpose;
- i) improvements are implemented through a controlled process;
- j) all changes to software and hardware are known and tracked at all times.

8.6.3 Tasks

Maintenance, support and improvement can include the following tasks.

- a) Provide input to the design team regarding maintainability and supportability.
- b) Identify potential failure modes, mechanisms and effects as input to defining a maintenance programme (see IEC 60812).
- c) Incorporate human aspects into design for usability, maintainability and supportability.
- d) Define a maintenance and support strategy (see IEC 60300-3-12).
- e) Define an initial maintenance programme during design and develop it continuously through the life cycle (see IEC 60300-3-10 and IEC 60300-3-11).
- f) Plan maintenance and support, including resource needs, skill levels and schedules to achieve an affordable, operable, supportable and sustainable solution.
- g) Specify external support services needed and develop agreements (see IEC 60300-3-16).
- h) Identify, analyse and treat risks to maintenance and support programmes including those associated with the contractual arrangements and the supply chain.
- i) Manage spare parts (see IEC 62550).
- j) Perform maintenance and organise maintenance support.
- k) Collect and review data concerning maintenance and support and compare with maintainability and supportability specifications and requirements.
- l) Establish a system for reporting failures and successes (FRACAS or DRACAS) and collect data related to successes, failures and non-conformances during tests and in the field (see IEC 60300-3-2 and IEC 60300-3-5).

NOTE 1 For failures of systems in operation, the observed failures relate only to the operating conditions when the failure occurred.

NOTE 2 Failure analysis during accelerated testing and stress testing can be used to identify failure modes that could also occur in use. (See IEC 62506 and the IEC 61163 series.)

- m) Provide input to decisions regarding evolution and enhancement.
- n) Control and track modifications to the system's design including hardware, firmware, software and documentation.
- o) Manage contractors and suppliers.
- p) Manage obsolescence (see IEC 62402).
- q) Provide information concerning the cost and practicalities of maintenance and support (including considerations of obsolescence) to assist in decisions about retirement.
- r) Evaluate and apply life extension methods such as update, upgrade or refurbishment.
- s) Identify items that can be suitable for re-use and provide relevant data concerning their condition.

Further information on maintenance and maintainability tasks is provided in IEC 60300-3-10 and on support and supportability in IEC 60300-3-14. Integrated logistic support is covered in IEC 60300-3-12.

Annex A (informative)

IEC standards related to dependability

Table A.1 – Classification of dependability standards by topic and life cycle stage

Classification	Life cycle stage				
	Conc.	Dev.	Real.	O/M.	Retir.
Fundamentals					
IEC 60500-192, <i>International Electrotechnical Vocabulary – Part 192: Dependability</i>	✓	✓	✓	✓	✓
IEC 61703, <i>Mathematical expressions for reliability, availability, maintainability and maintenance support terms</i>	✓	✓	✓	✓	✓
High level standards – Process standards					
IEC 60300-1, <i>Dependability management – Part 1: Managing dependability</i>	✓	✓	✓	✓	✓
IEC 62853, <i>Open systems dependability</i>	✓	✓	✓	✓	✓
IEC 62508, <i>Guidance on human aspects of dependability</i>	✓	✓	✓	✓	✓
IEC 60300-3-3, <i>Dependability management – Part 3-3: Application guide – Life cycle costing</i>	✓	✓	✓	✓	✓
IEC 62402, <i>Obsolescence management</i>	✓	✓	✓	✓	✓
IEC 62741, <i>Demonstration of dependability requirements – The dependability case</i>	✓	✓	✓	✓	✓
IEC TS 62775, <i>Application guidelines – Technical and financial processes for implementing asset management systems</i>	✓	✓	✓	✓	✓
IEC 62960, <i>Dependability reviews during the life cycle</i>	✓	✓	✓	✓	✓
Documentation and data					
IEC 60300-3-2, <i>Dependability management – Part 3-2: Application guide – Collection of dependability data from the field</i>			✓	✓	
IEC 60300-3-4, <i>Dependability management – Part 3-4: Application guide – Specification of dependability requirements</i>	✓	✓			
Software, communications and open systems					
IEC 61907, <i>Communication network dependability engineering</i>	✓	✓	✓	✓	
IEC 62673, <i>Methodology for communication network dependability assessment and assurance</i>	✓	✓	✓	✓	✓
IEC 62628, <i>Guidance on software aspects of dependability</i>	✓	✓	✓	✓	✓
Discipline based standards – Programme level					
IEC 60300-3-10, <i>Dependability management – Part 3-10: Application guide – Maintainability and maintenance¹</i>	✓	✓	✓	✓	✓
IEC 60300-3-14, <i>Dependability management – Part 3-14: Application guide – Supportability and support²</i>	✓	✓	✓	✓	✓
Reliability					
IEC 61014, <i>Programmes for reliability growth</i>		✓	✓	✓	
IEC 61709, <i>Electric components – Reliability – Reference conditions for failure rates and stress models for conversion</i>		✓			

¹ Under preparation. Stage at the time of publication: IEC CDV 60300-3-10:2024.

² Under preparation. Stage at the time of publication: IEC FDIS 60300-3-14:2024.

Classification	Life cycle stage				
	Conc.	Dev.	Real.	O/M.	Retir.
IEC 62308, <i>Equipment reliability – Reliability assessment methods</i>		✓	✓		
Maintenance and maintainability					
IEC 60300-3-11, <i>Dependability management – Part 3-11: Application guide – Reliability centred maintenance</i>		✓	✓	✓	
IEC 60706-2, <i>Maintainability of equipment – Part 2: Maintainability requirements and studies during the design and development phase</i>	✓	✓			
IEC 60706-3, <i>Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data</i>		✓	✓	✓	
IEC 60706-5, <i>Maintainability of equipment – Part 5: Testability and diagnostic testing</i>		✓	✓	✓	
IEC 62309, <i>Dependability of products containing reused parts – Requirements for functionality and tests</i>	✓	✓			✓
Supportability and support					
IEC 60300-3-12, <i>Dependability management – Part 3-12: Application guide – Integrated logistic support</i>		✓	✓	✓	
IEC 60300-3-16, <i>Dependability management – Part 3-16: Application guide – Guidelines for specification of maintenance support services</i>	✓	✓			
IEC 62550, <i>Spare parts provisioning</i>		✓	✓	✓	
Dependability and risk modelling and analysis					
IEC 31010, <i>Risk management – Risk assessment techniques</i>	✓	✓	✓	✓	✓
IEC 60300-3-1, <i>Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology</i>	✓	✓	✓	✓	
IEC 60812, <i>Failure modes and effects analysis (FMEA and FMECA)</i>	✓	✓	✓	✓	
IEC 61025, <i>Fault tree analysis</i>	✓	✓	✓	✓	
IEC 61078, <i>Reliability block diagrams</i>	✓	✓		✓	
IEC 61165, <i>Application of Markov techniques</i>		✓			
IEC 61882, <i>Hazard and operability studies (HAZOP studies) – Application guide</i>	✓	✓		✓	
IEC 62198, <i>Managing risk in projects – Application guidelines</i>	✓	✓	✓	✓	✓
IEC 62502, <i>Analysis techniques for dependability – Event tree analysis (ETA)</i>		✓		✓	
IEC 62508, <i>Guidance on human aspects of dependability</i>	✓	✓	✓	✓	✓
IEC 62740, <i>Root cause analysis (RCA)</i>		✓	✓	✓	
IEC 62551, <i>Analysis techniques for dependability – Petri net techniques</i>		✓		✓	
IEC TR 63039, <i>Probabilistic risk analysis of technological systems – Estimation of final event rate at a given initial state</i>	✓	✓			