IEC 60300-3-4

Edition 3.0 2022-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Dependability management – Part 3-4: Application guide – Specification of dependability requirements

Gestion de la sûreté de fonctionnement – Partie 3-4: Guide d'application – Spécification d'exigences de sûreté de fonctionnement

IEC 60300-3-4:2022-03(en-fr)

IEC Secretariat
3, rue de Varembé
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 It also gives information on projects, replaced and withdrawn publications.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. 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 22 300 terminological entries in English and French, with equivalent terms in 19 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. 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 22 300 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 19 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

IEC 60300-3-4

Edition 3.0 2022-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Dependability management – Part 3-4: Application guide – Specification of dependability requirements

Gestion de la sûreté de fonctionnement – Partie 3-4: Guide d'application – Spécification d'exigences de sûreté de fonctionnement

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 03.100.40; 03.120.01

ISBN 978-2-8322-1059-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

DEPENDABILITY MANAGEMENT –

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

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

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

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

a) consistency with the other of the six core IEC dependability standards;

b) a process for defining requirements has been included;

c) the definitions and language used have been made consistent with other system related standards.

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

Draft	Report on voting
56/1932/FDIS	56/1939/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/standardsdev/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,
- replaced by a revised edition, or
- amended.

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 expectations.

Dependability has many attributes, but is usually characterized in terms of reliability, maintainability, and supportability, and the derived characteristic of availability. Dependability also includes the performance characteristics such as durability, testability and restorability as well as security and integrity, particularly in relation to software-based systems.

Dependability is an important attribute that affects the value items generate. Consequently, relevant dependability attributes should be defined and specified in addition to functional performance requirements and physical attributes. Whilst mainly addressing system and equipment level dependability, many of the techniques described in the various dependability related IEC standards may also be applied to products or at the component level. The term "item" is used throughout this document to mean an individual part, component, device, functional unit, off-the-shelf (OTS) equipment, subsystem, or system. The item may consist of hardware, software, people or any combination thereof (see IEC 60050-192). In order to refer to a specific kind of "item", terms like component, OTS, product or large open system are used.

Dependability attributes may be specified for an individual system or product (for example, a vehicle) and/or a group of similar systems or products (for example, a fleet of similar vehicles).

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

The levels of reliability, maintainability, supportability and availability achieved by an item depend on the conditions under which it is realized, utilized, maintained and supported and also on the life profile of the system. The requirements in the dependability specification, should also define the following:

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

Dependability attributes may be specified, along with other performance characteristics, in various ways depending on the situation. In a basic project context where an acquirer obtains an item from a supplier, three main types are:

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

The guidance in this document is applicable to all three types of specifications and may be adapted to other situations as needed.

This document provides guidance for writing dependability requirements in specifications, together with a means of assuring the achievement of those requirements.

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

- IEC 60300-1 [1][1], which highlights the importance and benefits of managing dependability. It gives guidance on dependability activities and how to integrate them into an existing management system and life cycle processes;
- IEC 60300-3-1 [2], IEC 60300-3-10 [3], IEC 60300-3-14 [4] which provide guidance on how to identify and apply appropriate analysis and assurance techniques for reliability, maintainability (and maintenance) and supportability (and support) respectively. A standard to cover availability is planned.

[1] Numbers in square brackets refer to the Bibliography.

DEPENDABILITY MANAGEMENT –

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

1 Scope

This part of IEC 60300 gives guidance on specifying dependability requirements and collating these requirements in a specification, together with a list of the means of assuring the achievement of the dependability requirements.

The guidance provided includes:

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

Other obligations, such as legislation and governmental regulations, can also place requirements on items, in addition to any requirements derived in accordance with this document.

Whilst mainly addressing system and equipment level dependability, many of the techniques described in the various dependability related IEC standards can also be applied to products or at the component level. The term "item" is used throughout this document.

This guidance is given in a basic project context where an acquirer obtains an item from a supplier. It can be modified and adapted to other situations as needed.

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

NOTE 2 This document does not cover items with special multi-stakeholder long-term arrangements (e.g. services provided through Public-Private Partnership procurements) and how dependability is specified in such arrangements.

NOTE 3 The guidance in this document can be applied to some aspects of the specification of requirements relating to software but specific guidance can be found in IEC 62628 [5] and the different parts of the IEC 61508 series [6].

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, *International Electrotechnical Vocabulary (IEV) – Part 192: Dependability* (available at http://www.electropedia.org)

3 Terms and definitions

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

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

3.1
goal
statement which translates or expresses desires or aspirations and for which evidence of fulfilment either need not or cannot be provided

3.2
item
subject being considered

Note 1 to entry: The item may be an individual part, component, device, functional unit, equipment, subsystem, or system.

Note 2 to entry: The item may consist of hardware, software, people or any combination thereof.

Note 3 to entry: The item is often comprised of elements that may each be individually considered.

[SOURCE: IEC 60050-192:2015, 192-01-01, modified – Note 3 modified by omission of internal references and Notes 4 and 5 deleted.]

3.3
off-the-shelf
OTS
non-developmental item of supply that is both commercial and sold in substantial quantities in the commercial marketplace

Note 1 to entry: Sometimes referred to as COTS (commercial off-the-shelf) or MOTS (modified off-the-shelf).

3.4
requirement
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, product 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 [7], modified – Note 4 added.]

3.5
specification
<of 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 the methods intended to be applied for assurance of compliance with the requirements, including accept/reject criteria.

Note 2 to entry: ISO/IEC/IEEE 15289 [8] defines 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.

3.6
useful life
<of an item> time interval from first use until user requirements are no longer met due to performance, obsolescence and/or economic factors

Note 1 to entry: The applicable time interval is dependent on the nature and application of the item and can be elapsed time, operating hours, number of cycles, etc.

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

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

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 has residual value and could be repurposed.

Note 5 to entry: In this context, "first use" excludes testing activities prior to hand-over of the item to the end-user.

[SOURCE: IEC 60500-192:2015, 192-02-27, modified – "economics of operation and maintenance, or obsolescence" replaced by "performance, obsolescence and/or economic factors".]

4 Specifying dependability

4.1 Description of dependability specification

4.1.1 What is dependability?

Dependability is the ability to perform as and when required. A dependable item is one where there is justified confidence that it operates as desired and satisfy agreed stakeholder expectations.

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

Dependability is specified and verified using a set of measurable or demonstrable attributes, which are quantified, where practicable. Dependability is usually characterized in terms of reliability, maintainability, and supportability, and the derived characteristic of availability.

- Reliability relates to the ability to provide a required function for a given interval (time, operating cycles, distance, etc.).
- Maintainability relates to the ease and speed with which an item can be retained in, or restored to, a state to perform as required.
- Supportability is the ability to be supported to sustain the required operational capability with a defined use profile and given logistic and maintenance resources.
- Availability is the ability to be in a state to perform when called upon to do so. It is often quantified as ratio of uptime to total time. As reliability, maintainability and supportability are major contributors of uptime and downtime, availability is impacted by the trade-offs between these attributes.

Dependability is also related to other attributes of life cycle processes such as design, manufacturing, installation, and ongoing operation and support activity. In addition, dependability also affects other attributes such as safety and environmental protection, where the inability to perform a function has safety or environmental protection consequences. The dependability specification therefore should be part of the item specification with the interaction between dependability requirements and functional requirements recognized and considered.

4.1.2 What is a requirement?

A dependability requirement is a statement of a single aspect of a dependability attribute which expresses one or more stakeholder needs or expectations and for which evidence or assurance of compliance can be provided. Multiple requirements may be necessary to fully define how the stakeholder's needs and expectations are to be met for each dependability attribute. This involves decomposing the needs and expectations in terms of individual aspects of dependability attributes and setting the balance between the aspects.

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

Dependability performance measures are the different ways in which each of the dependability attributes can be expressed within a requirement. See 5.4.7 to 5.4.10 for further details.

4.1.3 What is assurance?

Assurance is grounds for justified confidence that a claim has been or will be achieved. It is typically provided as a body of evidence, which aims to decrease the uncertainty around the achievement of the dependability requirements. This evidence is the output of activities developed to meet and demonstrate the requirements and manage the risks, such as analysis and testing.

4.1.4 What is dependability specification?

The requirements for an item are collated into a specification. As the intended context in which the item is used, such as expected demand and operating environment, also affect the dependability performance, the context should also be provided in the specification as supporting information (see 5.3 for further guidance). Keeping specifications accurate across the item's life cycle is also important and the specification shall be updated in response to changes in requirement or context.

4.1.5 Which attributes to specify?

The way that dependability requirements are specified depends on the type and nature of the item, for example whether the item is repairable or non-repairable, and whether it is a single use device. For example, only reliability requirements need to be specified for non-repairable items that do not require maintenance. Examples of non-repairable items include sealed items and items where the cost of repair outweighs the cost of replacement, such as many consumer goods, and items at remote locations, such as deep-sea systems and satellites, where deployable maintenance resources are not available when needed. Single use devices include explosives, passenger airbags and emergency flares. For non-repairable items, replacement of sub-items are sometimes a concern and maintainability requirements may be specified, if applicable.

Many complex items, however, are repairable and maintainability is important for the acquirer or user, for example, to increase the item's useful life. Maintainability requirements should be specified if the maintenance costs contribute significantly to life cycle cost, if downtime could lead to a significant reduction in value or if maintenance is important for the acquirer or user. Preventive and corrective maintenance requirements may be specified, if applicable.

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

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

4.1.6 Contracting for dependability

The purpose of any specification is to provide a basis for development or purchase of an item. It usually forms part of the contract between the acquirer and supplier and therefore it is essential that the specification is written in such a way that it can be used for contracting. Contracting for dependability can take many forms, from milestone payments dependent upon the successful completion of a status review (see IEC 62960 [9]) or a demonstration test, to the use of penalty clauses and incentives for in-service achieved dependability, such as performance-based contracts.

The benefits and drawbacks of the different contract types are as follows.

- Penalties for poor performance encourage the supplier to give dependability its full attention and can lead to higher levels of dependability than would otherwise be achieved.
- Incentives for passing demonstration testing focus the supplier on demonstrating the dependability. However, demonstration testing can be costly and time-consuming and might only reveal, just before delivery, that the item does not meet its dependability requirements. Another important consideration when including dependability demonstrations into contracts are the relevant supplier and acquirer risks associated with the design of these demonstrations. For example, the design of the test determines the likelihood of incorrectly accepting a bad item (acquirer risk) as well as the likelihood of incorrectly rejecting a good item (supplier risk). The confidence levels to which a dependability measure shall be demonstrated, and the amount of testing required (or available) should be balanced in order to fairly manage these risks.
- Requiring the supplier to provide maintenance encourages the supplier to mitigate the risk that the item achieves poor availability as the supplier may then experience consequential losses as a result of item unreliability. However, this requires a much longer contract, for example a fixed cost maintenance agreement, with its associated difficulties.

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

- specifications written by the supplier;

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

- specifications written by the acquirer;

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

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

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

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

4.2 Principles

4.2.1 General

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

4.2.2 Systems approach

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

Requirements can be defined for:

- the system as a whole;
- any component or subsystem;
- a separate entity (e.g. a product or item);
- a collection of entities (e.g. a fleet of products or items);
- a collection of functions (e.g. a service or set of services).

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

4.2.3 Requirements and goals

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

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

Both requirements and goals should be defined. For example, for high availability or reliability systems, it might not be practicable or cost effective to provide justified evidence that the high level of availability or reliability has been achieved. The acquirer needs to clearly identify both the high availability and reliability goals, for which evidence cannot be provided, but also define demonstrable requirements for which evidence can be provided.