

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2022 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 It also gives information on projects, replaced and withdrawn publications.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. 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.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**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

**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.....	4
INTRODUCTION.....	6
1 Scope.....	8
2 Normative references	8
3 Terms and definitions	8
4 Specifying dependability	10
4.1 Description of dependability specification.....	10
4.2 Principles.....	13
4.3 Benefits	15
5 Derivation of dependability requirements	15
5.1 General.....	15
5.2 Define stakeholder needs and expectations	17
5.3 Develop supporting documentation	18
5.4 Derive dependability requirements	19
5.5 Justify the measures used for the dependability requirements.....	33
5.6 Complete dependability specification	34
5.7 Review dependability specification.....	34
Annex A (informative) Discussion on useful life.....	35
A.1 General.....	35
A.2 Factors that determine useful life	35
A.3 Specification of useful life of non-repairable items (components)	36
Annex B (informative) Process for prioritizing dependability attributes	38
Annex C (informative) Development of a dependability specification for a home security system.....	40
C.1 Define stakeholder needs and expectations	40
C.2 Develop supporting documentation	40
C.3 Derive the dependability requirements	45
C.4 Complete dependability specification	46
Annex D (informative) Influencing factors for dependability specification.....	48
D.1 Examples of constraints on system dependability.....	48
D.2 Type of system operation	48
D.3 Criticality of operation	49
D.4 Determining relevant influencing factors for the evaluation of system functions	52
Bibliography.....	54
Figure 1 – High level process for derivation of dependability requirements in the specification.....	16
Figure 2 – What are we trying to achieve?	18
Figure 3 – What do we need to manage?	22
Figure 4 – What constraints are there?	22
Figure 5 – Assurance considerations	23
Figure 6 – Reliability requirements.....	27
Figure 7 – Maintainability requirements.....	28
Figure 8 – Supportability requirements.....	34

Figure 9 – Availability requirements	33
Figure B.1 – Process for prioritizing attributes.....	39
Figure C.1 – System configuration for normal mode of operation	44
Figure C.2 – System configuration for panic mode of operation.....	44
Figure C.3 – System configuration for security service mode of operation	45
Table B.1 – Questions for prioritizing dependability attributes	38
Table D.1 – Examples of influencing factors under each influencing condition	52
Table D.2 – Relationship of system properties with influencing conditions	53

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.

4.2.4 Assuring achievement of requirements

There are two elements to any specification; the dependability requirements and the means by which the supplier shall demonstrate or assure the achievement of the requirements to the acquirer. This means that the supplier shall provide sufficient evidence to the acquirer that the item meets its requirements to give the acquirer the confidence needed to pay the agreed price. IEC 60300-3-1 [2], IEC 60300-3-10 [3], IEC 60300-3-14 [4], IEC 60706-3 [10] and IEC 62308 [11] discuss dependability evaluation for reliability, maintainability (and maintenance) and supportability (and support). Availability measurement and assurance is discussed in IEC 61070 [12].

The choice of which assurance activities to specify in a contract is dependent upon the level of project risk that the acquirer is willing to accept. The acquirer might be willing to take the risk that the item might fail, so long as it is maintained by the supplier. In such a case, assuring the overall availability of the item by the use of penalties for poor performance and incentives for exceeding the requirements might be preferable to assuring the reliability of the item on its own. If however, the acquirer is not willing to risk unavailability of the item, then formal reliability or availability demonstration testing may be necessary. Rare events can seldom be proven to be absent by testing so assurance may need to be via a well-reasoned argument. A dependability case (see IEC 62741 [13]) provides one method of presenting such an argument.

Generally, evidence required to provide assurance that the higher reliability items have met their requirements is more costly, as greater testing is required to obtain the confidence required. This is one factor in the higher cost of higher reliability items but, without these activities, the supplier provides the acquirer with limited confidence that the item meets its requirements.

4.2.5 Cost implications

All items exhibit some level of reliability, whatever the frequency of failure or the required level of maintenance. At all times, a balance should be sought between the cost, risk and performance of items. This includes any potential trade-offs between the cost of designing for, and assuring, high dependability and the cost and other risks of resulting from lower dependability over the entire life of the item. The nature of the item's function, associated risks (performance, cost safety environmental and reputational) and other contextual factors informs these trade-offs. An investment in dependability design and implementation can therefore repay itself in terms of the combined development, realization and operating costs for the item. IEC 60300-3-3 [14] describes life cycle costing and the relationships between dependability and cost. In order to attain the minimum life cycle cost point for the item, the organization producing it should actively manage dependability; otherwise, the item's achieved level of reliability is usually much lower than the level required at the minimum cost point, causing project delays, cost overruns and low levels of availability.

4.2.6 Dependability management

It is essential that dependability is actively managed throughout the system life cycle. This includes both during the procurement process and during use, with the management activities differing for each. Dependability management provides a systematic approach for addressing dependability, focusing on the needs of stakeholders in optimizing dependability to enhance organizational objectives and return-on-investments.

This document deals with the specification of dependability, through the setting of requirements for one or more of the dependability attributes. These attributes are characteristics of the item that can be assured. However, other factors can significantly reduce the achieved levels of these attributes below the level intrinsic to their design. The most significant are potentially the quality of manufacture and maintenance of the item that can introduce new faults into the item. If dependability is not managed correctly, there is a higher likelihood that dependability requirements are not achieved.

IEC 60300-1 [1] provides guidance on managing dependability of systems, products and services involving hardware, software and human aspects. It provides guidance on planning and implementing a programme of dependability activities and tasks through the life cycle and on providing accountability and assurance.

4.2.7 Expected useful life

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

The determination of useful life may be included as a part of a dependability specification. Understanding the useful life of items could assist in the decision as to which item to acquire as the most appropriate solution for an application. Expected useful life in some cases may also be required by a legal directive in certain markets. Knowledge of an item's useful life is important for estimating its life cycle cost (IEC 60300-3-3 [14]).

4.3 Benefits

The benefits of specifying dependability are:

- for the supplier:
 - enabling trade-offs between reliability, maintainability and supportability to be determined during design and acquisition of items;
 - providing justification that dependability requirements are applicable, achievable and assurable.
- for the acquirer:
 - defining, documenting and providing evidence, based on data and evaluation, that agreed stakeholder needs and expectations for dependable performance are met;
 - managing changes in stakeholder needs and expectations, including changes in requirements themselves.
- for both:
 - improved knowledge of dependability requirements;
 - providing verification and validation of contract requirements;
 - providing assurance to the regulators that any dependability related regulatory requirements are addressed and are achieved.

5 Derivation of dependability requirements

5.1 General

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

As items and their usage are very different across different organizations, it is not possible to write a standardized approach that articulates how to develop dependability requirements. Instead, Clause 5 provides a high-level process to determine what information is required, the decisions that could be made and what the output of the decision making process might be. It is also not possible to provide a fully comprehensive set of decisions which affect the development of dependability requirements for all situations, so the user of this document should tailor the approach described to their situation. The users should particularly consider what is within their control in making decisions using the process described.

Figure 1 describes the approach to developing the dependability requirements.

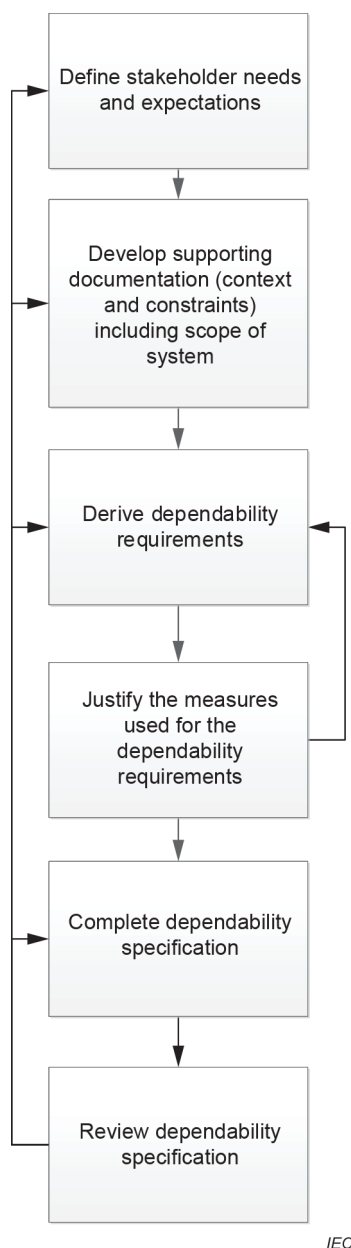


Figure 1 – High level process for derivation of dependability requirements in the specification

Step 1 is to review and document stakeholders' needs and expectations. This step establishes a common understanding of the stakeholders' dependability performance needs and expectations. Through discussion, which could be one-to-one or a facilitated workshop, this step determines what dependability performance is important to the stakeholders and document, what they "must" have and what they would "like" to have, i.e. their dependability requirements and goals. See 5.2 for further information.

Step 2 is to develop supporting documentation which detail the context and constraints within which the requirements need to be met. It is not enough to specify requirements for dependability attributes on their own to define the required dependability performance. Supporting documentation should be developed to provide the context on which the requirements are based and should be captured or referenced within the dependability specification. Subclause 5.3 describes this step in further detail.

Step 3 is to derive the dependability requirements. The first part of this step is to decide which of the dependability attributes, i.e. reliability, maintainability, supportability or availability, is the most important and which therefore should be defined first. Following the definition of the primary attribute, any secondary attribute(s), if appropriate, should be determined. This is determined not only by technical considerations but also by the organization's business priorities and values. Annex B provides an example of a method to prioritize attributes. Any subsequent specified attributes shall be consistent with the selected primary and secondary attributes.

Through discussion and analysis, dependability requirements should be refined, associated attributes should be derived and assurance criteria should be determined (see 5.4.4). Having decided upon the most important attribute(s), the way in which that attribute is defined needs to be decided (see 5.4.7 to 5.4.10) and the requirement drafted, including determining the relevant performance measures. Double specifications such as failure intensity and MTBF or failure probability and useful life should be avoided as these might lead to inconsistencies. The derivation of attributes should consider the decision-making processes described in 5.4. Requirements can also include additional dependability related attributes such as durability, sustainability (see IEC 60300-1 [1]) with a means for verifying them defined.

Step 4 is to justify the performance measures of the dependability attributes, see 5.5. The performance measures within the dependability requirements should be justified through consideration of the stakeholders' needs and objectives and through justification of the measures. Justification of the performance measures should ensure they are rational, realistic and can be demonstrated within the project's budgetary, operational and time constraints. Methods that can be used to justify the performance measures include modelling, comparison with in-service data and experience of stakeholders obtained.

Step 5 is to complete the dependability specification which captures the dependability requirements and supporting documentation within a single document.

Step 6 is to review the dependability specification for consistency and applicability. This is a very important step as the decisions made at the previous steps can affect the dependability requirements. If appropriate, the dependability specification is reviewed by potential suppliers and, as such, might require update as a result. This can include modification of the stakeholder needs and expectations, for example if it has proven impossible to derive requirements which satisfy these needs and expectations.

At any step, it may be necessary to return to an earlier step in the process if the requirements are found to be inconsistent, unachievable or otherwise impracticable.

5.2 Define stakeholder needs and expectations

In defining the stakeholder needs and expectations, it can be helpful to articulate these first in plain language, in terms of what the stakeholder is trying to achieve, see Figure 2. In thinking about performance, the stakeholders should also decide what level of risk they can accept that the required performance is not achieved, whether there is a minimum performance level that shall be achieved and how much money they are willing to spend to reduce the risk that the required performance is not achieved.

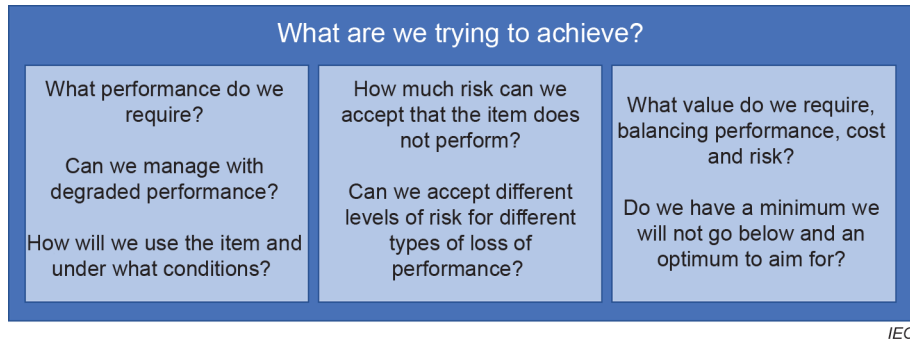


Figure 2 – What are we trying to achieve?

It can be costly if the derived requirements cannot be achieved; therefore, during discussion it is important to test the practicality of the needs being articulated. Stakeholders may have different needs, in which case the derived requirements need to be compared, for example by considering the dependability of product or service, value for money (throughout life) and dependability of customer service.

The stakeholder needs and expectations are different from the item requirements which are the technical requirements against which the design occurs (see step 4 in process).

5.3 Develop supporting documentation

If a dependability specification is to be used as the basis for contracting, it is essential that the item dependability is fully defined, so as to prevent disagreements once the contract is applied. Annex C provides an example of supporting documentation for the specification of a home security system.

Examples of the elements that should be included in supporting documentation include:

- a description of the item for which the dependability requirements are being written, including the capability or functions being procured, equipment and/or item boundaries;
- how the item is to be installed, used and supported;
- the precise and clearly defined criteria by which the chosen dependability attributes are to be evidenced or assured (see 5.4.4).

The description of the item should provide the following:

- item identification including name, premise for use or operation, and primary purpose of application;
- the operational objective to be achieved by the item;
- the key functions needed to achieve the required performance;
(The purpose of each function should be stated from a system requirements perspective. Where appropriate, the relationships of these functions should be established.)
- success/failure criteria upon which dependability requirements for each function are based, for example total failure of the item to provide any functions, failure to provide essential functions, or partial failure or performance degradation;
- the influencing factors affecting each function and their impact on item performance;
(Annex D provides guidance on typical constraints, and key influencing factors.)
- the technical approach being taken to acquire and maintain the functions needed for sustained operation within cost and time constraints.

The description of the item's use and support includes:

- the hardware, software and human aspects of the item's operation including the skill requirements and responsibilities of the personnel responsible for operating and maintaining the hardware, software and documentation;
- the different operating and environmental conditions under which the item is used including, where applicable, the relative amount of time spent in each condition;
- aspects of the operating and environmental conditions that might need to be considered, including anything in the rest of the system that could affect the behaviour of the item or be affected by it;
(This can include the physical environment, the psychosocial environment of the organization or the wider global environment.)
- the use profile(s) over which the dependability requirements are measured, which should be developed with careful consideration of how the item is operated, used, maintained and stored;
- information on supportability including maintenance and support resources available or required, such as level and numbers of skilled maintenance personnel, spare parts, maintenance facilities, condition monitoring, inspection and testing techniques being used, and work equipment;
- the maintenance policy to be applied and the associated procedures and support arrangements;
- acceptable data sources to be used in any analytical techniques.

A specification that is part of a contract can also include:

- the obligations, responsibilities and accountabilities of acquirer, supplier and any third parties;
- the methods intended to be applied for assurance of compliance with the requirements, including accept/reject criteria.

5.4 Derive dependability requirements

5.4.1 General

There are a number of sub-steps within the process step to define the dependability requirements.

- The first sub-step is to consider the different scenarios by which the item might be utilized or procured, see 5.4.2.
- The second sub-step is to decide the level of risk that is acceptable, whether there are different aspects of performance which particularly need to be managed and whether there are any constraints on the resources available, as these can affect the required dependability attribute, see 5.4.3.
- The third sub-step is to consider what assurance is required as this affects how dependability is specified, see 5.4.4.
- The fourth sub-step is to determine whether the requirements should be set at the item, sub-item or component level, see 5.4.5.
- The fifth sub-step is to balance the outcome of these decision making processes and define the priority of the dependability attributes, see 5.4.6.
- The sixth sub-step, having decided upon the dependability attributes to be specified, is to define each attribute, see 5.4.7 to 5.4.10, which look at the likely decisions and types of measure for each of the dependability attributes.

5.4.2 Specification scenarios

5.4.2.1 General

There are different scenarios for the extent to which dependability attributes shall be included in a specification as described in 5.4.2.2 to 5.4.2.5.

Custom-made items are where the acquirer specifies what is required and the supplier designs, develops and produces an item solely to meet that specification. If, however, the supplier states what items are available and the acquirer chooses the item which best meets the requirements, this is known as off-the-shelf, commercially produced equipment or OTS. In this case, there are no changes to the standard commercially available item. In practice, most major procurements are a combination of both custom-made and off-the-shelf elements and components and the specification is mutually agreed between the acquirer and supplier.

If the item is non-repairable, its total life and sometimes replacement are main concerns. If the item is repairable, maintainability and supportability also shall be considered. These could be provided by the supplier but may also be available from independent providers with logistics being a consideration in some cases. The resultant availability is important. Design of the item likely involves the need by the manufacturer to specify and choose components and industrial items to meet the requirements of those providing maintenance and support.

NOTE Distinction of scenarios applies equally to hardware, software and combinations thereof. For software, "repairable" translates to a degree of customer support, e.g., existence of licensing agreement clauses or active developer communities whereby vendors or developers respond to bug-reports from users, discovery of security vulnerabilities, etc., through timely application of patches and upgrades.

5.4.2.2 Specification scenario for OTS items incorporated in larger items

Consumer OTS items such as laptops and printers, and industrial OTS items such as electric motors and pumps, can be bought in business to business trade (B2B), and used as components in assemblies or sub-assemblies, incorporated in larger items. They would potentially be supplied to intermediate parties with no direct involvement from final users or operators.

The simplest specification is for simple items that are non-repairable with a low level of function. Reliability is the main attribute of concern with a life time specified for components that have a limited operational life. The difficulty in specifying such items is to describe the conditions of use (the safe operating area) so that it covers all relevant applications and use conditions.

A more complex type of specification is for industrial items that are repairable. This type of item could range from a fairly simple one such as a pipeline valve or an electronic card to a much more complex item such as an electric motor or internal combustion engine designed for a variety of applications. Since the item is repairable, not only reliability but also maintainability and supportability are important attributes to be considered. The supplier of these items does not necessarily have a complete understanding of the final application and operating environment. The specification of reliability may need to cover multiple functions that could fail with different failure rates. Consideration of maintainability may not be complete since the use environment and installation details could be uncertain and could vary. As well, the specifics of maintenance and expected support can only be estimated with generic maintenance requirements, procedures and resources. Location of the item, which could be fixed or moving, may be an unknown factor with respect to the logistics required to provide the recommended support. The acquirer may well have to adjust the support needed once its actual application has been determined.

5.4.2.3 Specification scenario for OTS end-user items

An acquirer may want to specify an item that is generally available and is manufactured for sale directly to many, but not specifically identified, users, such as a personal vehicle, commercial aircraft, domestic washing machine, mobile phone and a laptop. In this case, the specification would be made by the acquirer to enable a choice to be made between available items. Alternatively, the supplier might write the specification and the acquirer would decide if this sufficiently meets their needs and expectations.

For an OTS end-user item, the supplier states what is available and may provide standard evidence that the item meets certain levels of dependability, which may include in-service data from previous applications. However, there is limited opportunity to provide assurance and many suppliers are unwilling to provide in-service data that is considered commercially sensitive.

The objective of this OTS procurement is to reduce or eliminate the need for development so that the desired capabilities can be procured more quickly and at a lower cost. One of the difficulties with OTS procurement is that the OTS items rarely meet all the requirements defined and that different OTS items have different features and capabilities while not meeting the requirements exactly. Therefore, the dependability requirements should be defined in such a way to ensure the OTS item meets the specific need, while allowing trade-offs to be proposed based on what can realistically be achieved and in order for all potential solutions to be considered. It is essential not to invoke design changes unnecessarily through the definition of inappropriate dependability requirements. It also needs to be recognized that OTS items achieve the supplier specified level of dependability only when used as designed. Therefore, the achieved performance is different (and may be unknown) if the usage is different.

If the acquirer requires any changes to the off-the-shelf item, it can no longer be considered an OTS item, as the changes might have a significant effect upon the achieved dependability. The acquirer shall ensure that an OTS item really is the same as the commercial item and that the evidence provided is adequate. If any changes are requested, the effect of these changes upon the dependability shall be considered in detail and additional assurance requested and paid for by the acquirer, if necessary.

5.4.2.4 Specification scenario for custom made end-user items

An acquirer may want to specify an item from a manufacturer to meet their specific and unique requirements, such as military equipment or a nuclear power station. The main focus for the acquirer is availability. Reliability and maintainability are important considerations during design. Maintenance requirements and supportability and resultant availability are established and specified with trade-offs between these attributes and cost, risk and performance. The final configuration may again involve specifying and choosing OTS items that fulfil the minimum requirements as part of the final item.

For a custom-made end-user item, the acquirer and supplier need to agree the level of assurance that the supplier shall provide to demonstrate that the requirements have been met. This assurance includes testing and analytical evidence but, as the item is being built solely for the acquirer, cannot include evidence from the use of the item in the in-service environment, except after purchase. The supplier then includes the cost of those assurance activities in the quoted price for the item and the acquirer can determine the evidence required, in accordance with the acceptable business risks. However, the acquirer knows that the item is being designed and developed to meet the requirements.

5.4.2.5 Specification scenario for a total solution for end-user items

An acquirer may want a supplier to provide a total solution for the useful life of the item. The specification consists of a performance-based requirement with availability or an appropriate service level being the primary dependability attribute. The manufacturer or supplier is responsible for establishing the contributing attributes of reliability, maintainability and supportability with applicable trade-offs to meet this availability requirement. The total solution provides all the support needed during utilization for the time agreed to in a contract.

5.4.3 Dependability attributes to be specified

Subclause 5.4.2 describes how the different types of item and how they are specified can lead to different dependability attributes being considered the most important. This Subclause 5.4.3 describes the different aspects of performance which can affect this decision and should be considered separately from the decisions in 5.4.2.

First consider the questions in Figure 3. Having done this, it is then necessary to consider whether there are any constraints, (see Figure 4), particularly on the resources available for maintenance and restoration of the item following failure, as these constraints lead to maintainability or supportability being more important than otherwise.

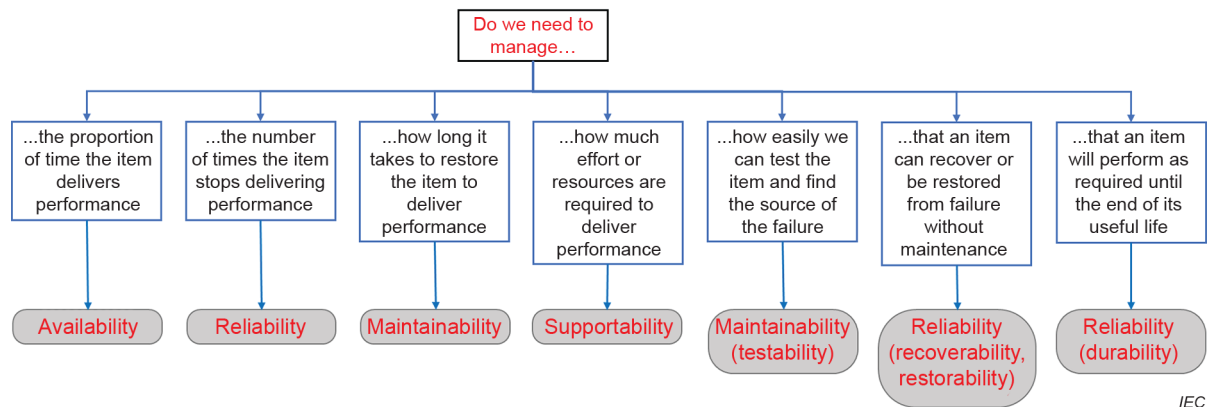


Figure 3 – What do we need to manage?

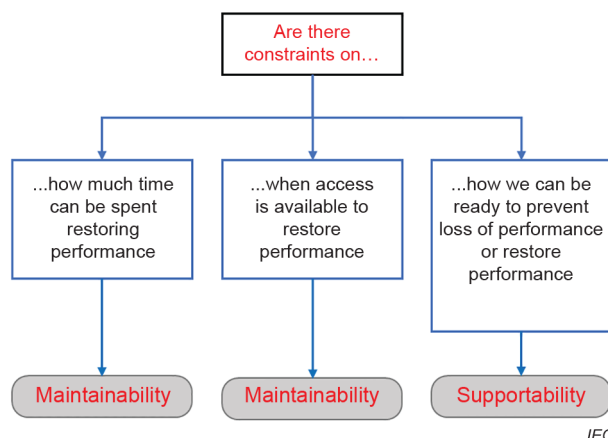
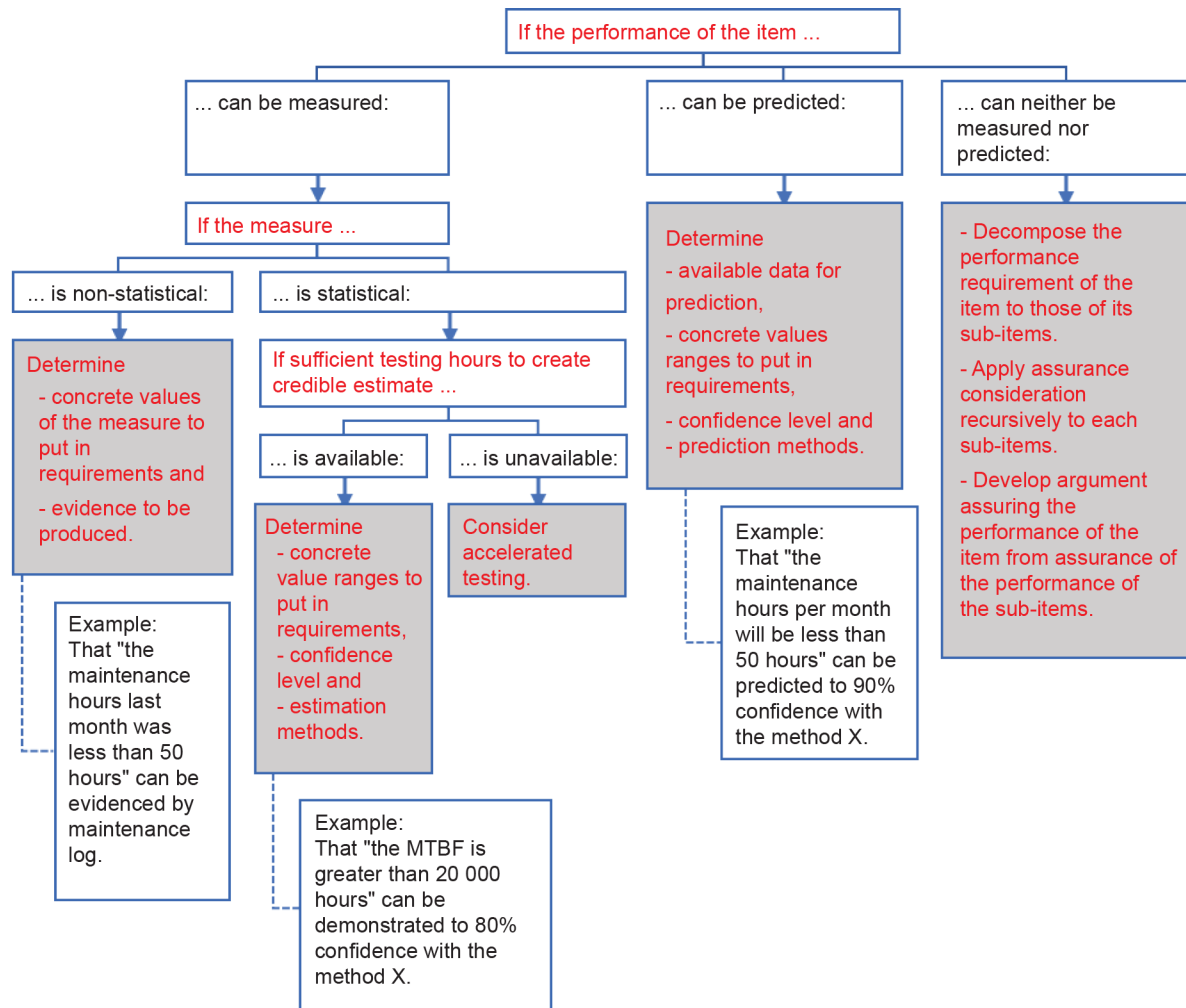


Figure 4 – What constraints are there?

5.4.4 Providing evidence and assurance of dependability attributes

Finally, it is necessary to consider whether the evidence can be provided that the dependability requirements have been met, see Figure 5. As described earlier, the satisfaction of requirements has to be able to be demonstrated, so it may be necessary to change the chosen dependability measure from that highlighted by the decisions described in 5.4.2 and 5.4.3 to one which can be evidenced in a cost effective and timely manner.



IEC

Figure 5 – Assurance considerations

There are two main elements to the demonstration and assurance of requirements; verification and validation. These are defined in ISO 9000 [15] and used for hardware as well as in the software industry as part of the software development process (see IEC 61508 (all parts) [6]) and may be explained as follows. Verification is the process of providing evidence that the item at the present stage meets its requirements from the present as well as for the previous life cycle stage(s) (i.e. are we building things right?). Validation is the process of providing evidence that the item meets the actual stakeholder needs and expectations, which might not always be reflected in the written specification (i.e. are we building the right things?). Both are essential elements.

The level of assurance required by the acquirer depends upon the confidence that the acquirer requires that the item achieves the levels of dependability specified. If the acquirer is willing to maintain an item when it fails in use, then a lower level of evidence, and therefore lower confidence in the achieved dependability, may be acceptable. This is because the provision of evidence takes time, costs money and the acquirer may be willing to accept the risk that the item does not perform as required. The acquirer shall take a balanced decision on the risks that are acceptable when specifying assurance requirements.

The supplier should state the assurance activity the supplier should perform as part of the specification and obtain agreement from the acquirer, often through the contract. When defining dependability requirements, the acquirer should consider the various factors likely to affect the cost of dependability assurance. These factors include the expected life time and retirement or recycling of the item.

For a long timescale procurement, activities might be planned many years before completion. Depending upon the contractual terms, the acquirer might therefore have little control over them during the project. One way to reduce both the acquirer's and supplier's project risk that the item does not provide the level of evidence required can be the progressive assurance. This means that the activities are planned throughout the life cycle and the results provided to the acquirer at project milestones. In this way the acquirer builds up confidence in the item throughout the project and there is a much-reduced risk that the level of evidence is inadequate.

The dependability case is one model that can be used for the supplier to provide the evidence to the acquirer that the item has met its requirements. The dependability case provides a reasoned, auditable argument that the item will meet or has met its requirements and is summarized at project milestones in the dependability case report. The dependability case is usually used to provide progressive evidence and is issued at a number of project milestones. This evidence can be in the form of demonstration that the risks that a dependability claim will not be met have been controlled. IEC 62741 [13] provides guidance on the dependability case.

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

Assurance activities include:

- analysis:
 - 1) compliance with standards, regulations and guidelines;
 - 2) expert review, best practice and certification;
 - 3) calculations primarily used for other design purposes (e.g. finite element analysis for stress, fatigue);
 - 4) simulation (for example of item performance);
 - 5) dependability analysis (see IEC 60300-3-1 [2]).
- testing and demonstration:
 - 1) performance in previous usage, for identical or similar items in identical or similar applications;
 - 2) dedicated dependability testing, including:
 - i) reliability demonstration tests, for example fixed failure/time tests, sequential tests, success ratio tests, accelerated tests or life tests;
 - ii) availability demonstration tests;

- iii) maintainability demonstration tests.
- 3) other development testing (e.g. performance life, fatigue life, software tests on item, module or component level);
- 4) physical demonstration that a support facility or equipment has been provided.

Further details of dependability assurance techniques can be found in IEC 60300-1 [1].

Not all assurance activities are appropriate or effective at all life cycle stages. Item testing cannot be carried out until it has been designed and a prototype built. However, testing should be planned at the design stage, so the supplier can determine the required sub-item tests before the item is constructed. In addition, the item and sub-items should be designed so that they can be tested (see IEC 60706-5 [16]). Similarly, analysis activities are more appropriate during the design stages to allow the exploration of the effects of different options upon the estimated dependability.

It should be noted that all evidence provided during development is a prediction of the likely dependability and the results from analysis are likely to be a less accurate prediction than the results obtained from testing. Therefore, the acquirer should probably not rely upon analysis results only and should require a combination of both analysis and testing activities to provide evidence of meeting the requirements. In addition, the environment and usage of the item shall be considered when the tests are planned. In cases where the test is performed close to the utilization conditions, the test gives a good estimate of the dependability, but, for an item with high reliability, the test may last a very long time, require a large number of test items and provide a low number of failures resulting in a large uncertainty in the dependability estimates. If the test is accelerated, the sample size and the test interval can be reduced (see IEC 62506 [17]). The larger number of failures reduces the statistical uncertainty but the technical uncertainty is higher, since the accelerated test conditions can cause failure modes that are not relevant in the field.

5.4.5 Decide on the level of the requirements

Definition of the item includes consideration of the level within the overall item at which the requirements are to be specified. The acquirer might set dependability requirements only at the highest level of the item or might decide that it is important that one of the sub-items does not dominate the resulting unreliability, and therefore also set requirements at lower levels. These lower level requirements shall be consistent with the top-level requirements and they shall be measurable (or demonstrable) and achievable. For example, the contribution of the sub-item to the overall item dependability shall be estimated before the requirements can be apportioned to the sub-items.

The apportionment to lower level sub-items is not straightforward other than for relatively simple structures such as series items where all sub-items have a constant failure rate. In other cases, such as items with redundancy or where the failure rate changes with time, refer to standards such as IEC 61025 [18], IEC 61078 [19], IEC 60300-3-1 [2] and IEC 61703 [20] for further guidance on the analysis of item dependability.

5.4.6 Balance the results

The decisions and considerations described in 5.4.2, 5.4.3 and 5.4.4 might all lead to the same dependability attribute being considered most important and which therefore should be specified first. However, it is possible that the outcomes of the different sub-steps are different. This step is to balance the results of the previous sub-steps so that the priority of the dependability attributes is decided to form the basis of the requirements.

5.4.7 Reliability requirements

Where reliability has been identified as an important dependability attribute, the measures used to define the requirements should be selected. The acquirer should ensure that the appropriate reliability measure, or measures are specified and that the statistical implications of the

requirement and their consequences on cost, project timescales and achievability are understood.

EXAMPLE A 99 % reliability over one year can be specified for an item as this appears to be a reasonable requirement. However, if the item failure rate is constant, this would imply a failure rate of less than one in 99 years which can prove difficult or expensive to achieve and/or demonstrate. The need for such a high reliability is therefore assessed taking these implications into account.

Reliability, when used as a measure, is by definition the ability of an item to perform as required, without loss of its required function or functions, for a given interval, under given conditions. It is most correctly described by a probability that the item can complete its required use profile. However, reliability in the generally accepted sense can be expressed or specified using a number of other measures such as mean time to failure or mean operating time between failures (MTBF) or failure rate. In all cases, it should be recognized by the acquirer that any reliability measure does not guarantee a reliability of a single item, as it represents a statistical expression of what may be expected with a specified confidence. Hence, any assurance requirements should include appropriate data analysis techniques where reliability quantification is specified.

NOTE The use of MTBF always implies that the rate of failure of the item is constant with time or use, i.e. the probability that the item will fail within the first hour of use is the same as the probability of it failing during one hour or use in, for example, a thousand years' time.

Examples of industries where reliability can be the primary dependability attribute of interest include:

- the aerospace industry, where once an aircraft has taken off it is essential that it completes the flight without loss of critical functions;
- the automotive industry, where a driver should be able to complete a journey (within a specified range of speed, terrain, etc.) without need for maintenance of any type.

Examples of where time to failure can be the required measure for reliability include:

- electric light bulbs that are designed for high percentage to survive to a given life;
- process machinery, where the item is continuously operating and the time to failure is of importance to plan maintenance activities.

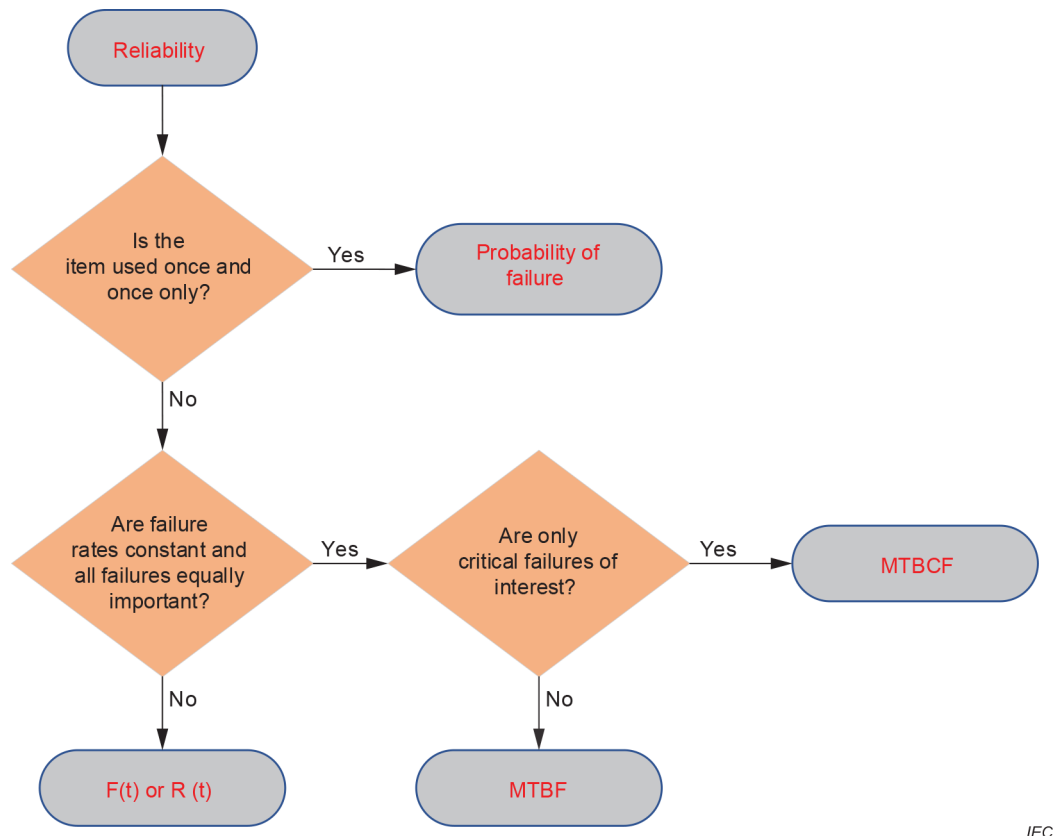
MTBF should only be used where constant failure rate can be assumed. It is therefore recommended a failure probability (i.e. reliability) or non-constant failure rate distributions should be used instead, if possible. Suitable non-constant failure rate distributions such as the Weibull distribution (IEC 61649 [21]) may be used for specification of non-repairable products and components. For repairable products see IEC 61710 [22].

The effect of failure should also be considered when defining reliability measures, for example will failures occur that do not stop performance and can be restored later.

Durability is a dependability attribute which describes the ability to restore items to a functioning condition until it is no longer feasible, economically or safely viable, to do so; i.e. a limiting condition is reached. Thus, it may be considered that durability is characterized by the period or usage of the item until the limiting condition is reached, which is expressed in the same terms as the operating life of the item (e.g. cycles, years, miles). It would also be possible to express the durability of an item in terms of the probability of being able to achieve a given period or usage until the limiting state is reached.

Recoverability is a dependability attribute which describes the ability to recover from a failure, without corrective maintenance. The ability to recover may or may not require external actions, for example a personal computer being switched on and off to reset the operating system. Recoverability is expressed using measures such as the probability of recovery within a specified time interval.

Figure 6 gives guidance on the different ways in which reliability can be defined.



IEC

Figure 6 – Reliability requirements

5.4.8 Maintainability and maintenance requirements

Maintainability is an important dependability attribute for all repairable items and reflects the ability of an item to be retained in, or restored to, a state to perform as required, under given conditions of use and maintenance. Examples where maintainability might be important are items such as aircraft where there are constraints on maintenance time due to the item being non-productive during maintenance, or for items that are difficult to maintain, or for items that are at a state of readiness to be used. Maintainability is generally dealt with in IEC 60300-3-10 [3].

Maintenance can be either corrective, i.e. carried out after a failure occurs, or preventative. If there is redundancy, failure of an item may not necessarily result in operational failure. However, if a failure is not rectified in a timely manner, operational failure could occur as back-up items also fail. Generally, the objective of a maintainability requirement is to prevent operational failure, prolong operational life and to minimize unavailability.

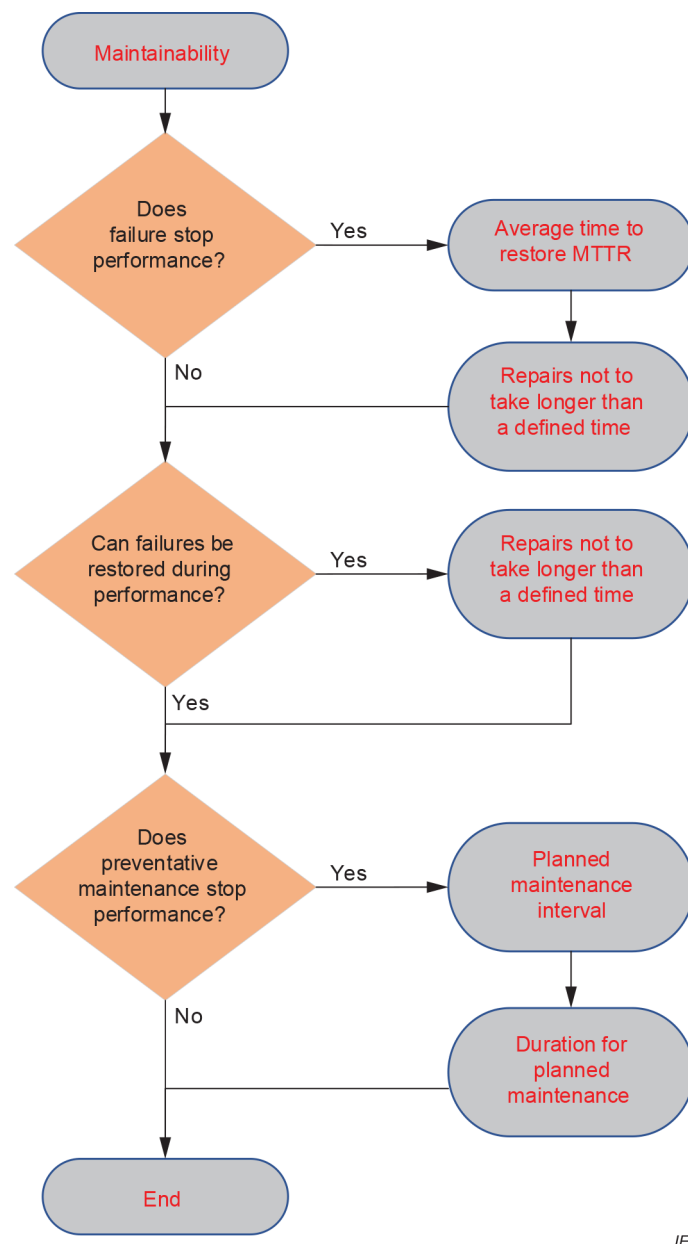
Maintainability, together with its subset testability, addresses the recognition and localization of a failure, the repair or replacement procedures, servicing activities and the subsequent testing to ensure that the item can be made operational. It also includes technical delays such as time for items to cool down, time to interpret test information and curing times. The specification of maintainability considers constraints such as repair location and repair environment but does not address logistic aspects. Aspects such as logistic support, cost of spares, time to obtain spares, time for a maintainer to arrive or deliver spares to a repair centre are considered within supportability.

Complex systems often have different levels/grades of maintenance or repair. These levels/grades may reflect differences in skill, support equipment or duration required to perform different maintenance tasks, for example the user may be expected to be able to conduct minor maintenance on a car, but extensive maintenance would be done by a mechanic in a workshop.

Maintainability requirements may be specified to address constraints between levels/grades of repair.

Testability is a dependability attribute which describes the degree to which an item can be functionally tested under stated conditions. Testability allows the status of an item to be determined and the isolation of faults in the item to be performed in a timely and efficient manner. Testability for software includes controllability, which describes the ability to affect and replicate the software behaviour. Testability is expressed using measures such as fault coverage (ratio of faulty functions detectable to total number of functions), false alarm rate (number of false alarms to total failures) and observability.

Figure 7 gives guidance on the different ways in which maintainability can be defined.



IEC

Figure 7 – Maintainability requirements

When defining maintainability requirements consideration should be given to the type of maintenance (for example, only maintenance that stops performance, all maintenance and/or maintenance at a specific level/grade) and what activities are included as part of the

maintenance duration (for example, time spent carrying out maintenance, or all time including time spent testing and diagnosing failure).

5.4.9 Supportability and support requirements

5.4.9.1 General

Supportability is the ability of an item to be supported such that it can perform as required, under given conditions of use and maintenance. Poor supportability can adversely affect the ability to operate, maintain or update items, as well as significantly increase an item's cost over its lifecycle. Therefore, it may be important to specify supportability requirements to ensure an item can be operated as and when intended and that it can continue to deliver value throughout its useful life. Supportability is generally dealt with in IEC 60300-3-14 [4].

The aspects of supportability that should be specified are highly dependent on the context of use and the intended support concept for the item. For example, a simple item may perform functions with little or no supporting infrastructure or interactions with an operator and be replaced on failure with a comparable item based on general form, fit and functional requirements. In this situation there may be little need for supportability specification. At the other extreme, a complex item may require extensive supporting elements and accurate input or control from skilled operators as well as complex arrangements to manage all facets of support for the item in order to balance cost, risk and performance. In this example, supportability requirements may be critical to achieve the desired balance.

Given the importance of context to supportability specification, it is often helpful to consider the five constituent capabilities for item support and assess whether there are any significant risks within these capabilities that should be managed via specification. The five constituent capabilities for item support are:

- operating support;
- supply support;
- maintenance support;
- engineering support;
- training support.

5.4.9.2 Operating support

Operating support addresses the elements external to the item that are needed for operation and may include operating facilities, system operators, support equipment, operator procedures and manuals, technical data as well as relevant information systems.

5.4.9.3 Supply support

Supply support is concerned with ensuring that the equipment and consumables necessary to operate and maintain items are available when and where required in an efficient manner. This includes demand forecasting, inventory management, warehouse and distribution and transportation systems, packaging and handling, procurement and relevant information systems.

5.4.9.4 Maintenance support

Maintenance support considers the systems and supporting elements needed to develop, execute and optimize a system of maintenance to meet relevant maintainability and availability requirements. Maintainability support may include trained personnel, facilities, support and test equipment, maintenance instructions, maintenance management systems, technical data and information systems.

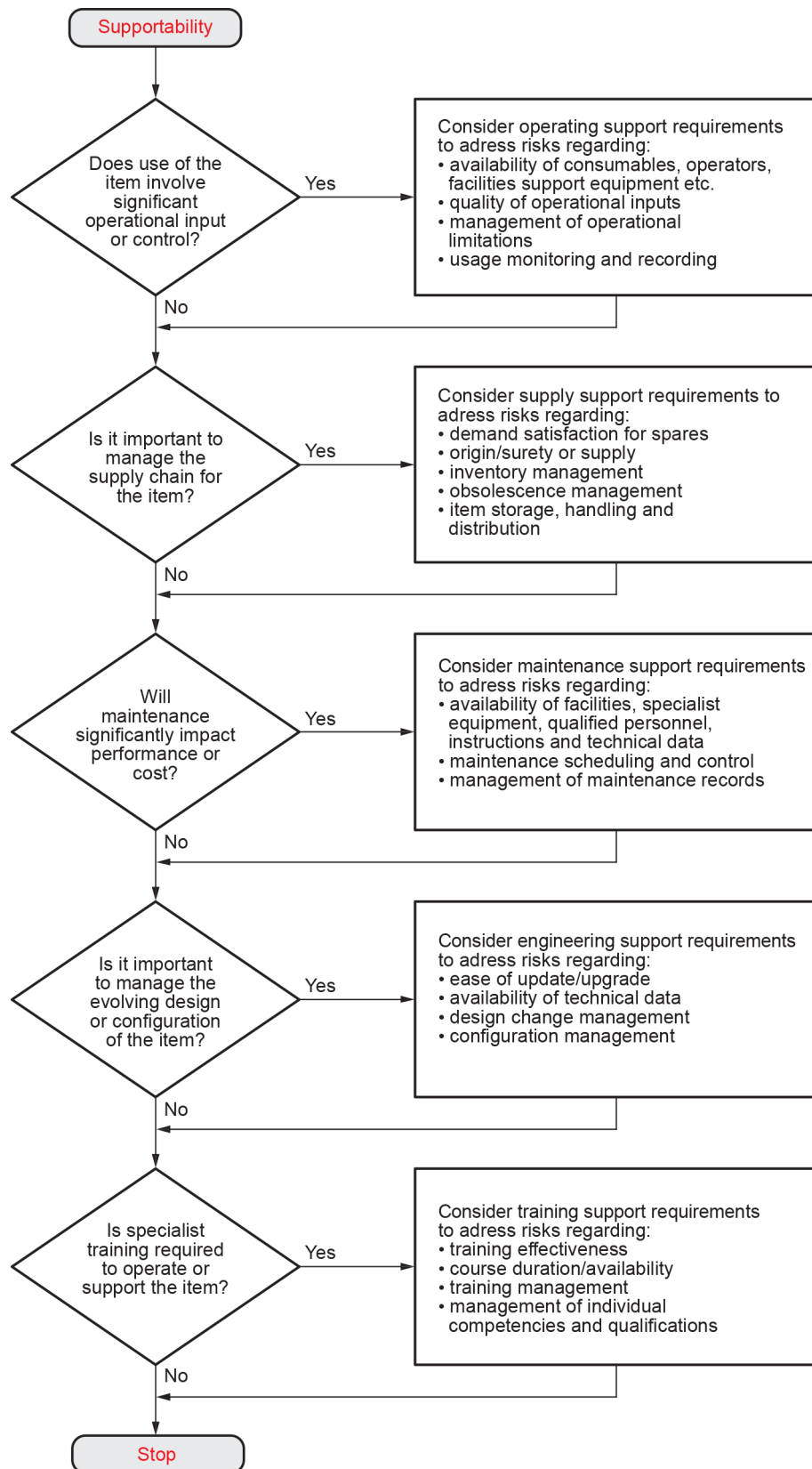
5.4.9.5 Engineering support

Engineering support describes the management of design processes and other information to ensure an item's configuration is managed and can be updated to meet evolving requirements. This can include personnel, technical data, engineering processes, information systems and supporting tools or software.

5.4.9.6 Training support

Training support considers the elements and systems required to ensure that people are adequately trained to operate, maintain and support an item. It may include instructional and training development teams, facilities, training materials and aides, processes and information systems.

Figure 8 gives guidance on the different ways in which supportability can be defined.



IEC

Figure 8 – Supportability requirements

5.4.10 Availability requirements

The availability of an item is the ability to be in a state to perform as required. Availability depends on the combined attributes of reliability, maintainability, recoverability and supportability and the

performance of maintenance and support. It is important that the acquirer identifies the definition of availability used in the specification.

EXAMPLE 1 Steady state availability is used in the rail industry, where train operators require a percentage of the trains to be available for use during peak periods or maximum delay times.

EXAMPLE 2 Mean availability is used in the telecommunications industry, where the operator requires a certain number of communication channels to be available such that the item maintains an overall availability through diverse routings using available routes even when some routes are unavailable.

EXAMPLE 3 Availability is used for continuously operating systems, for example where the acquirer of a satellite ground station with 100 modems can require analysis to demonstrate with 90% confidence that the system will achieve less than 10 min of combined link outages across 90 concurrent communication links in any given 6-month period.

Typical availability definitions are:

- Steady-state availability which is the "limit, if it exists, of the instantaneous availability when the time tends to infinity". For this definition of availability to be relevant, steady-state conditions have to exist. Although the mathematics is simpler under the assumption of steady state conditions, steady-state availability should not be used without validating the assumption.
- Instantaneous availability which is the "probability that an item is in a state to perform a required function under given conditions at a given instant in time, assuming that the required external resources are provided." It is unlikely to be specified in dependability requirements.
- Mean availability which is the "mean of the instantaneous availability over a given time interval (t_1 , t_2).". This measure is more useful for a specification and is of interest in industries where the availability over different time intervals may change, perhaps due to different operating conditions.

Other definitions of availability also exist, such as operational availability (where logistic delays are included) and asymptotic availability (see IEC 60050-192 and IEC 61703 [20]).

Figure 9 gives guidance on the different ways in which availability can be defined.

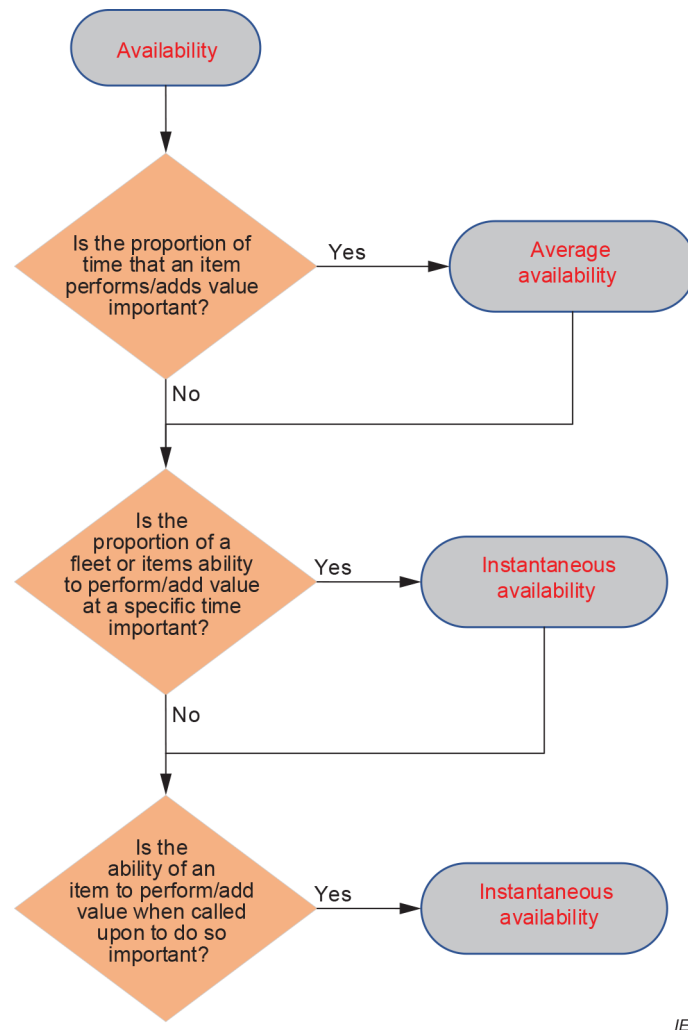


Figure 9 – Availability requirements

5.5 Justify the measures used for the dependability requirements

This step is about developing the target numerical values for quantitative measures of dependability attributes and claim statements for qualitative measures used in the dependability specification. IEC 61703 [20] provides guidance on developing the numerical values for dependability attributes.

Requirements shall be achievable. 100 % reliability may be desirable but is not possible and high reliability requirements can lead to disproportionately high costs of design, development and the provision of evidence. The acquirer therefore shall assess what levels of the different dependability attributes are reasonable, based upon factors such as the achievement of previous similar items, the desired performance and consideration of whether an improvement can be expected during utilization. Current items are becoming increasingly complex to meet desired levels of functionality and many have reached the limit of cost-effective reliability.