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 It also gives information on projects, replaced and withdrawn publications.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

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.

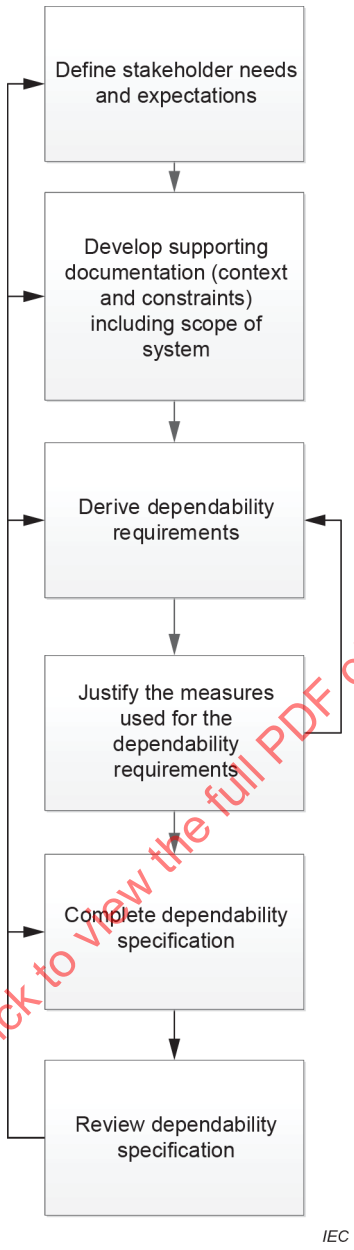

Figure 1 – High level process for derivation of dependability requirements in the specification

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.

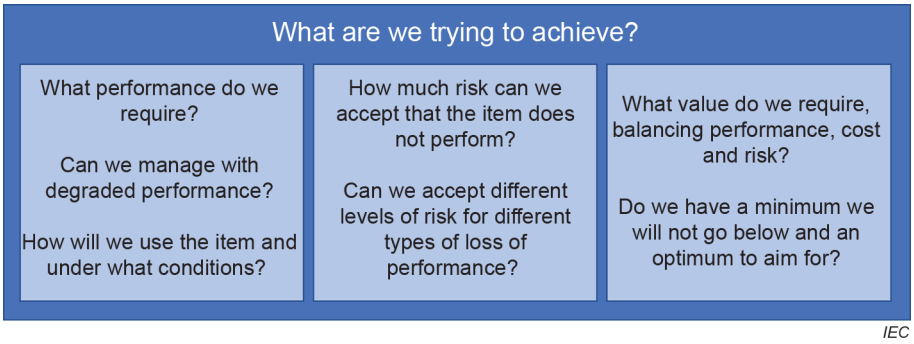

Figure 2 – What are we trying to achieve?

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.

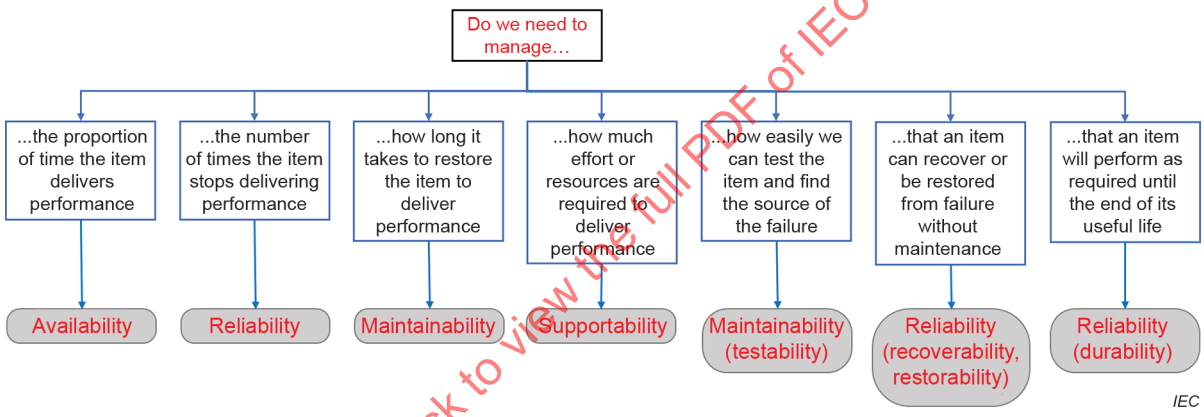

Figure 3 – What do we need to manage?

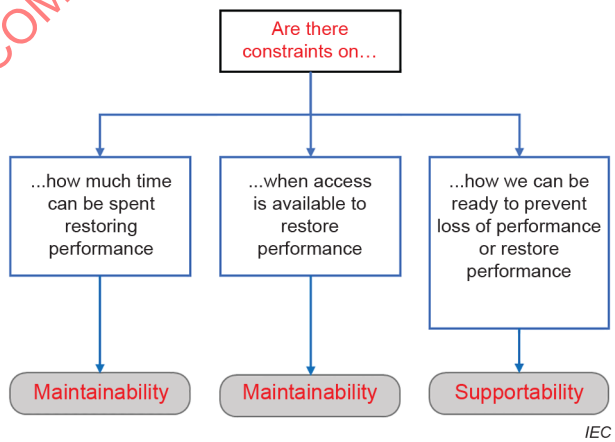

Figure 4 – What constraints are there?

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.

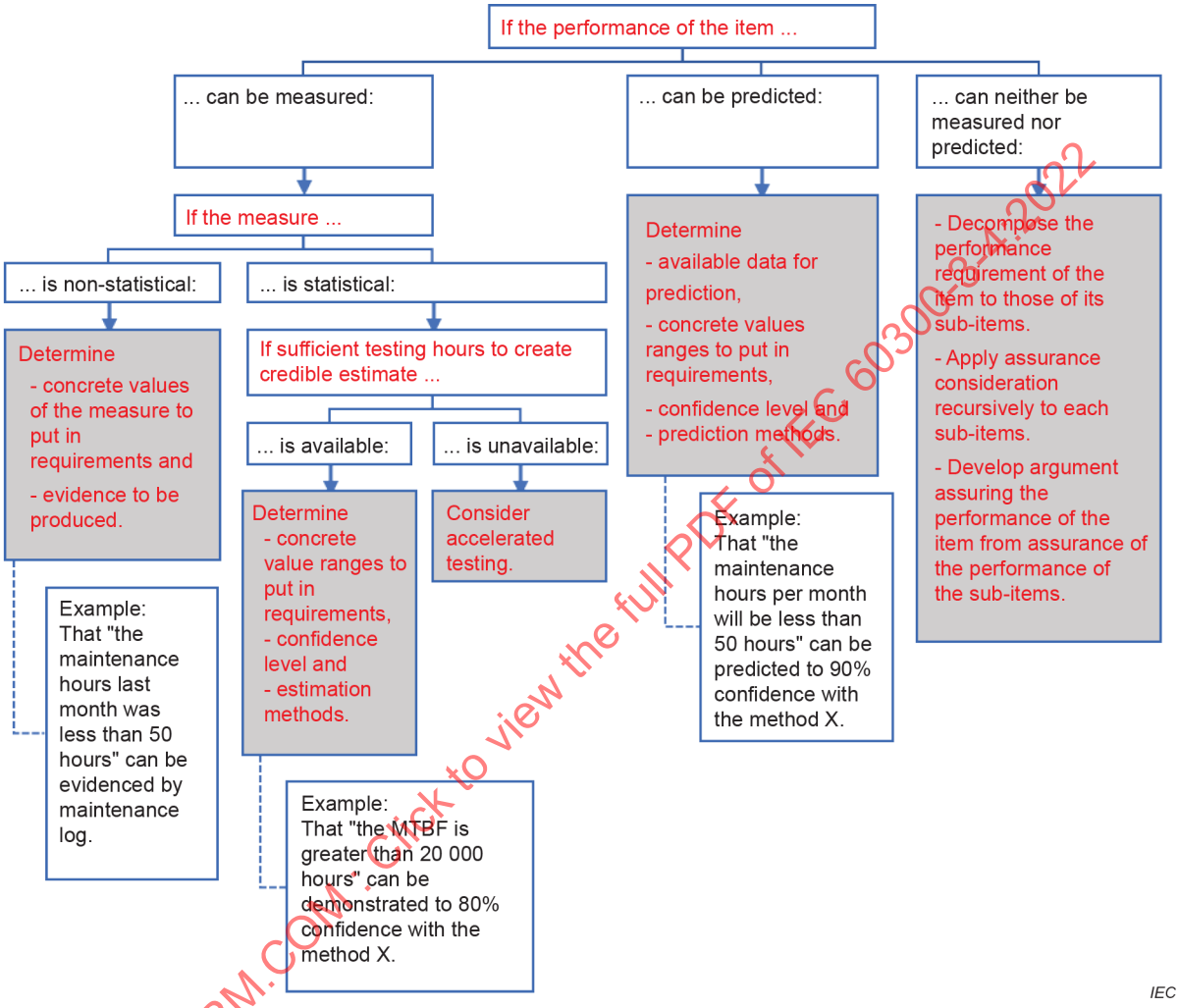

Figure 5 – Assurance considerations

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.

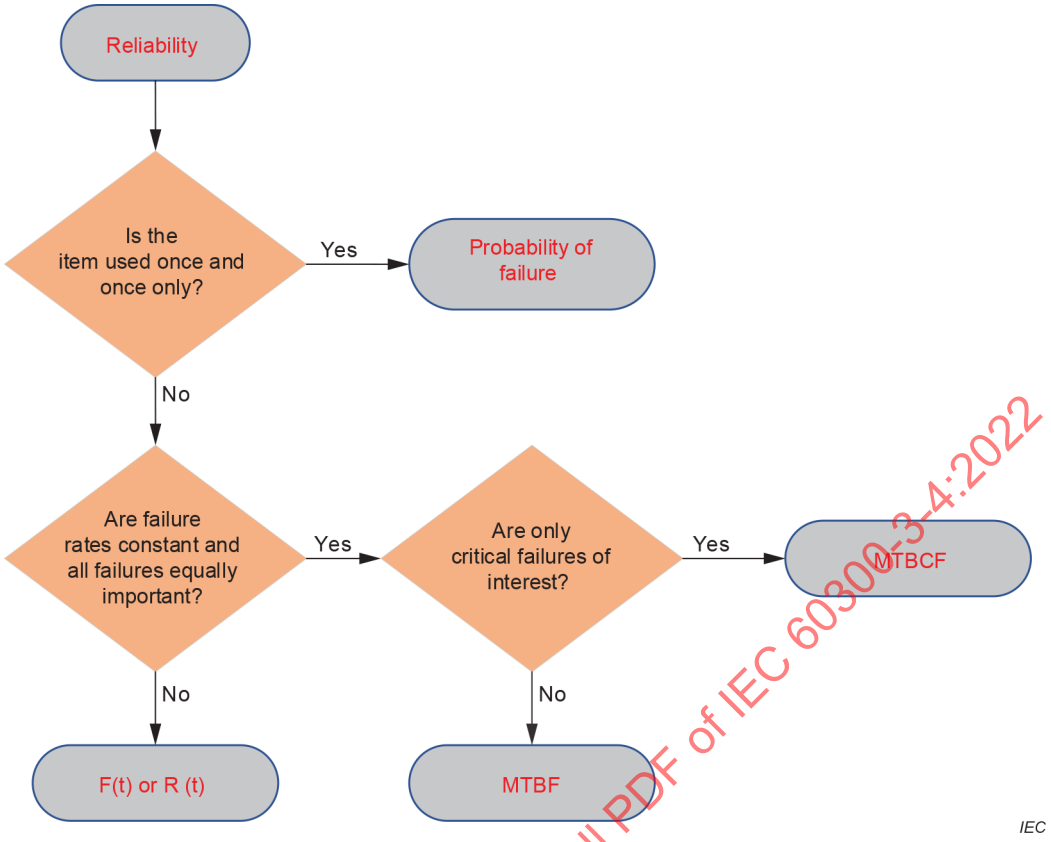

Figure 6 – Reliability requirements

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.

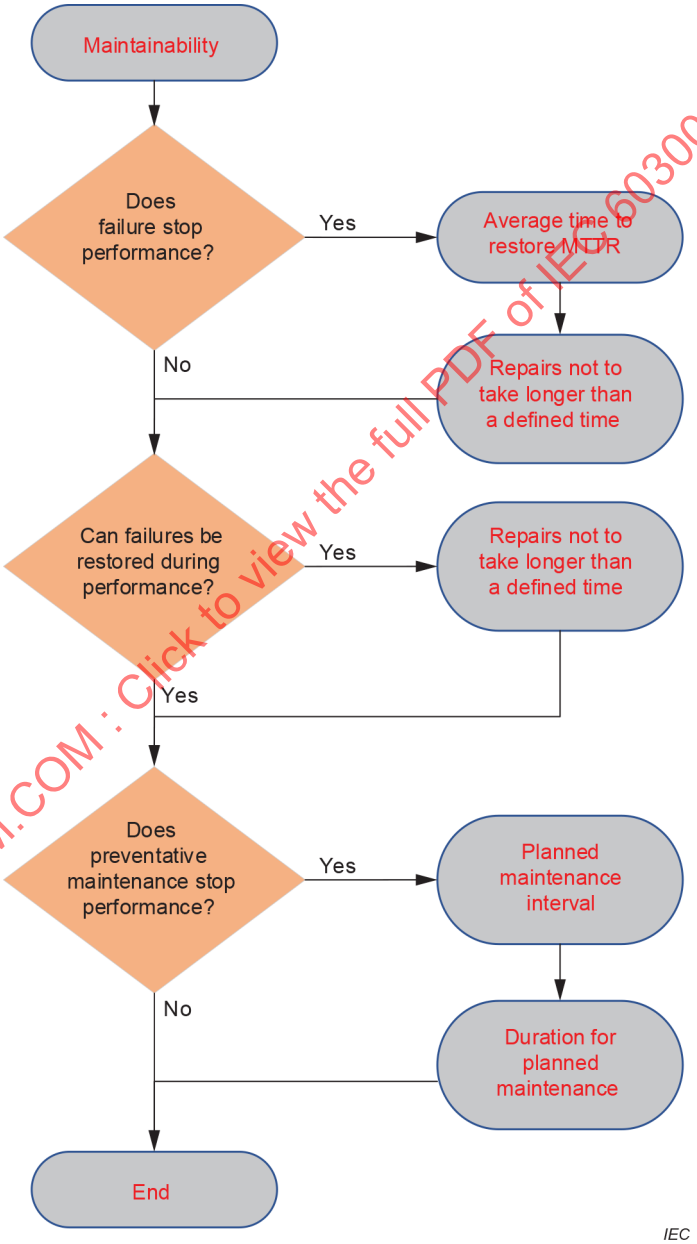

Figure 7 – Maintainability requirements

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.

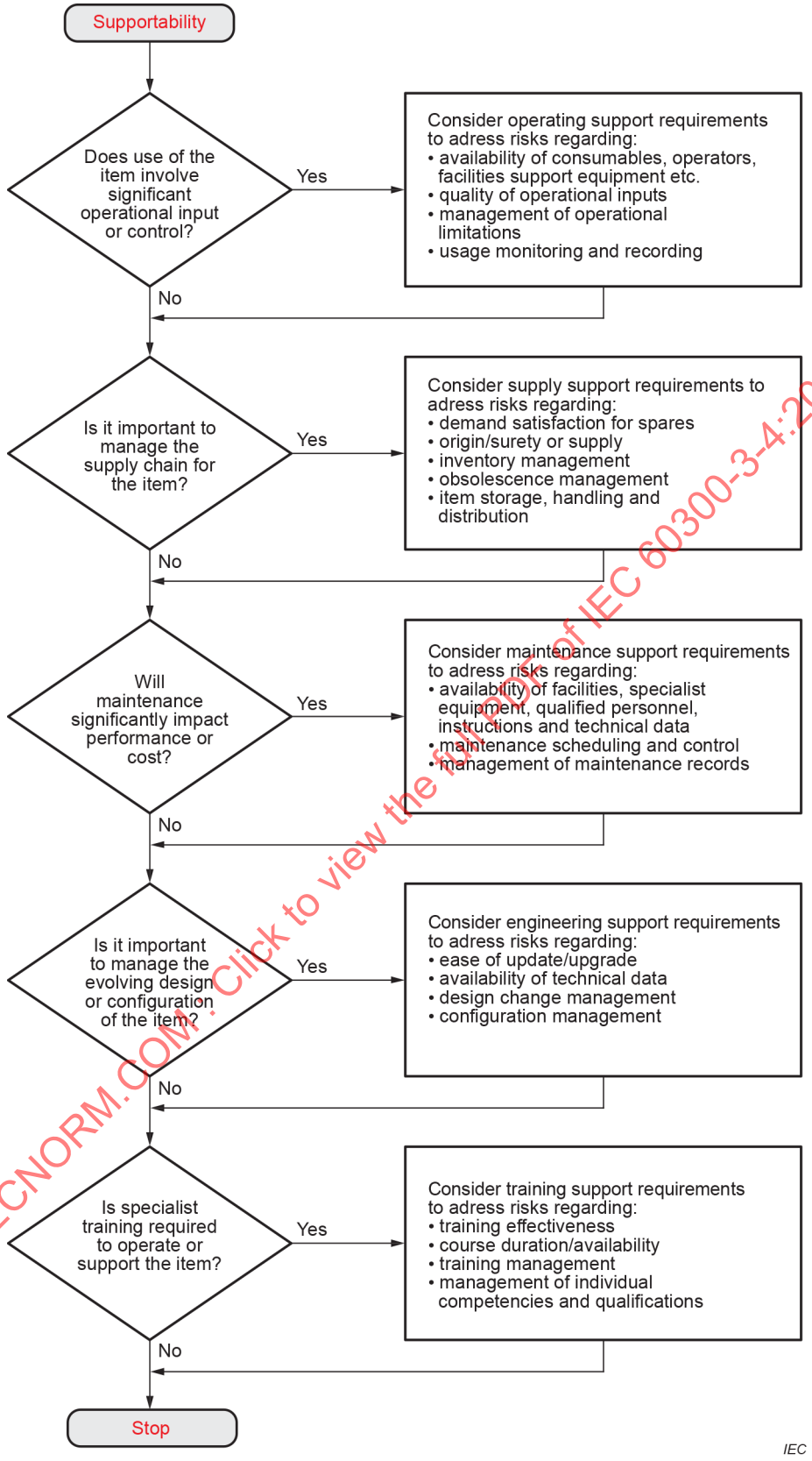

Figure 8 – Supportability requirements

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 (t1, t2)." 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.

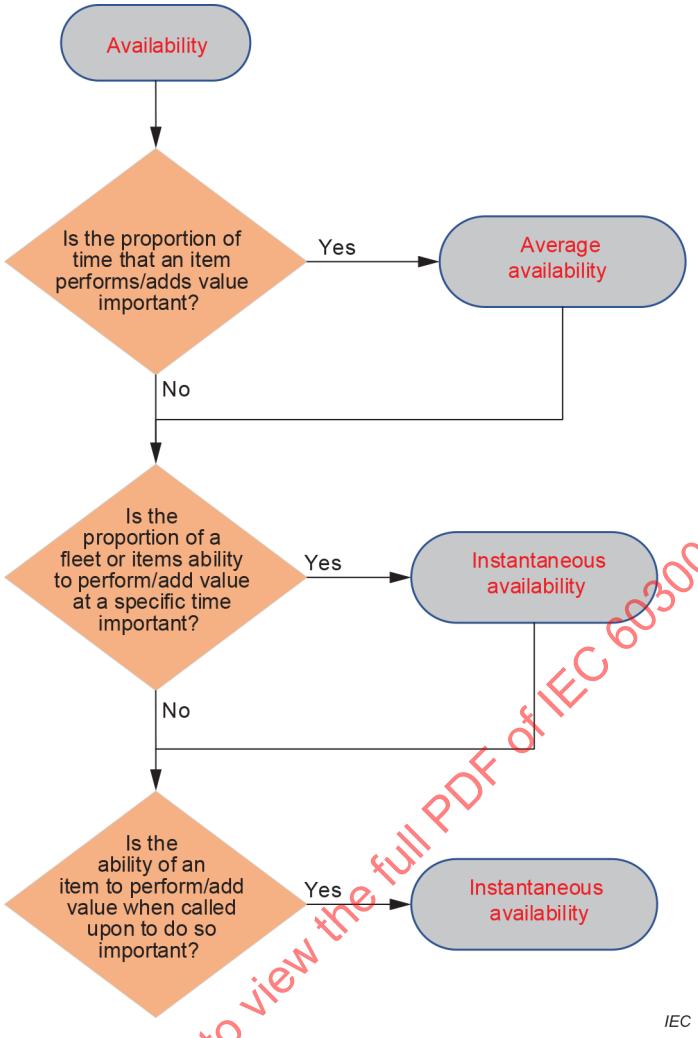

Figure 9 – Availability requirements

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.

Data on past achievement is available from a variety of sources, including:

- producer's testing records (during design and development phase – if testing is performed and outcomes are available and released);
- supplier's own maintenance and servicing records;
- manufacturer's data for sub-items and components;
- specialized databases – such as RIAC, SPIRD;
- generic databases and data books.

5.6 Complete dependability specification

Having decided which dependability attribute(s) to specify and the numerical values or qualitative requirements to be used, it is necessary to combine the requirements into the specification, along with the supporting information.

5.7 Review dependability specification

Once the specification has been completed, a review should be conducted to ensure that the set of dependability requirements are well structured, complete, concise, and consistent as well as understood by all stakeholders. This includes consideration of whether the requirements form a coherent set and that they can be allocated or aggregated between sub-items or different suppliers as required.

If it is found that the dependability requirements set is not well structured, the process needs to be repeated. Different decisions can lead to different dependability attributes being the most appropriate and therefore a different set of requirements being produced.

Annex A
(informative)

Discussion on useful life

A.1 General

Useful life is the length of time that an item is able to meet requirements for users and organizations, which involves different aspects that can be characterized as performance, obsolescence and economic factors. It also depends on whether the item is repairable or non-repairable.

Useful life is defined in terms of time, but the applicable time interval is dependent on the nature and application of the item and can be denoted as elapsed time, operating hours, number of cycles, number of demands or other time-related measures. The time period normally commences at "first use", which excludes testing activities prior to hand-over of the item to the end-user.

Useful life is an outcome of an item's design requirements, including trade-offs that are made with cost, performance and risk. The resultant design life is more limited since it is restricted to assumptions that are made, especially for OTS items, regarding use and requirements during actual utilization, which may well change. Useful life may be considered as a requirement that is relevant for the specification of dependability.

The determination of useful life is different for individual or small number of items and large numbers depending on the production volume of the item with either a few items or mass produced such as consumer products. For components with wear-out, the life expectancy of these components often determines the useful life of the product.

The useful life of an item may be longer than that required by the organization which may result in the item being repurposed by another organization. It may also be replaced by a more functional item especially with rapidly changing technology advances.

The useful life duration assumes that the performance of an item is defined under a set of given conditions. These can be environmental levels and stress levels (internal and external) that occur during the useful life and their durations. Usually these are defined within a useful life profile. Changes in the life profile can shorten or lengthen the useful life. For example, an engine operating occasionally at maximum stress may have a reduced useful life if required to operate permanently at maximum stress.

A.2 Factors that determine useful life

A.2.1 Useful life due to performance factors

The first aspect that could define the end of useful life is a final loss of acceptable performance or functionality either through degradation or failure. For a non-repairable item, as is the case with many smaller components, products and consumer items, this occurs when there is a failure. The useful life can be specified as the time when a stated percentage of the items have failed as further described in Clause A.3.

For repairable items, the end of useful life often occurs when there is final wear-out that cannot be repaired. For consumer products, estimating the useful life from field data is easier since the population is large (typically many thousands). But for other items such as large industrial items with a small number of items, where many repairs can be undertaken, the estimation of useful life based on performance is much more uncertain and the final determinant of useful life is more likely to be obsolescence or economic factors.

A.2.2 Useful life due to obsolescence factors

Obsolescence is defined as the transition of an item from available to unavailable from the manufacturer in accordance with the original specification. Obsolescence might occur because production of an item has ended or the lack of availability of service provision (such as the withdrawal of support resources), support of software or processed material.

Obsolescence should be managed through the life cycle as described in IEC 62402 [23].

A.2.3 Useful life due to economic factors

There are a number of economic factors to be considered for useful life. One such factor could be increases in operating costs such as energy usage or labour costs, making it uneconomic to operate the item. Another economic factor occurs when an item starts to incur excessive maintenance costs, for example, where the cost of spare parts becomes larger compared to the replacement cost of the item. Replacement may be warranted if a more efficient and cost effective option with lower operating and/or maintenance costs is worthwhile with a lower life cycle cost (see IEC 60300-3-3 [14]).

In a financial context, the useful life is related to the period during which the organization expects to use the item, which can be either shorter or longer than the period that the organization needs to use the item, for example, related to production feasibility or profitability. If the useful life of an item is longer than that required by the organization, it may have residual financial value. The item could still be in a condition that would allow it to be productive for another organization after being used by the initial organization, for example used vehicles.

The determination of economic useful life of an item requires an element of judgment and requires appropriately qualified and experienced personnel to make the assessment. Accordingly, assessing economic useful life should consider recommendations by operational and technical staff in the non-financial areas, as this information is used to determine a residual value at disposition.

When items start to reach the end of their useful life, an organization may want to evaluate the expected remaining useful life. This could be estimated from the condition of an item, when reliable condition deterioration profiles are available. When not available, the organization can use local knowledge and experience of the operation and service performance of similar items; hence the need to engage both financial and non-financial functional staff to arrive at a consensus on the remaining economic useful life.

A.3 Specification of useful life of non-repairable items (components)

For the purpose of specifying useful life as a part of a dependability specification for non-repairable items, only performance factors need to be considered when estimating useful life. It is possible to apply this to a non-repairable item by stating a time when a certain percentage of the items have failed. This approach is well known for mechanical items such as ball bearings and electric motors where expected life is defined as the point when a percentage of items have failed, for example 10 % of the items have failed at the stated life time (see IEC 61649 [21]).

Defining the life time as the time when a certain percentage of the items have failed has the advantage that it does not assume constant failure rate or non-constant failure rate (wear-out). Since the percentage failed is the accumulated percentage, it can be any combination of failures with constant failure rate, increasing failure rate and decreasing failure rate.

The expected useful life can be estimated and verified by a supplier in one of three different ways:

- through part count calculation and using life expectancy data from data handbooks for example IEC 61709 [24];
- through testing (IEC 62506 [17] and IEC 61649 [21]);
- from field data (IEC 60605-6 [25]).

For a more complex product, the manufacturer may identify the few components in the product that have a limited life (see IEC 61709 [24]). These components could either be life tested (IEC 61649 [21] and IEC 62506 [17]), or use the life stated by the component supplier. The rest of the components are assumed to have a constant failure rate which can be found from market data, from the component manufacturers or in handbooks (see IEC 61709 [24]). The failure probabilities of the constant failure rate components and the components with limited life are then added.

The specified useful life may be either just an agreement between the supplier and the acquirer or it may be based on more formal directives that are issued in a jurisdiction. A directive may state a number of ways in which the supplier or manufacturer is able to comply with the directive. Options for compliance may vary from a declaration of conformance, a valid ISO 9001 [26] certificate, to additional requirements such as a mandatory test for compliance at a notified laboratory. In nearly all cases, the supplier should keep a technical file describing the product and how it has been verified that it complies with all relevant directives. Authorities managing the directives could request access to this file. A supplier should also ensure compliance from sub-suppliers.

Useful life could also be estimated with approximation for mass produced products (e.g. consumer products) where only a small percentage of the products fail, for example 10 %, and where only approximately 1 % are repaired twice and approximately 0,1 % is repaired more than twice.

Annex B
(informative)

Process for prioritizing dependability attributes

This example process for prioritizing dependability attributes is to answer each bank of questions in relation to the item being specified but should be tailored before use. See Table B.1.

If the answer to any of the question is 'yes', follow the yes path in the flow chart shown in Figure B.1.

If the answer to all the questions is 'no', follow the no path in the flow chart shown in Figure B.1.

These question banks are not exhaustive and should be adjusted for each organization's context and business priorities.

Table B.1 – Questions for prioritizing dependability attributes

Reliability questions
Is the item non-repairable? e.g. light bulb
Is there limited or no repair capability due to location or complexity of item? e.g. satellite
Are there significant safety, environmental or operational consequences associated with unexpected or frequent failures? e.g. aircraft
Are repair actions extremely costly or cost prohibitive?
Is any failure extremely disruptive to service delivery, regardless of the amount of downtime associated with it? e.g. loss of a telecommunications line
Is it a single use device?
Is it critical to know the time-to-failure in order to plan maintenance activities?

Availability questions
Is the proportion of time that the service is delivered critical but the combination of dependability attributes less important? e.g. manufacturing equipment
Is the number of items available at any time important? e.g. rental car fleet availability

Primary maintainability and supportability questions	**Secondary maintainability and supportability questions**
Are there safety consequences associated with extended downtime? e.g. military environment	Are there safety or operational consequences with extended downtime? NOTE Operational consequences include consequences to reputation
Is there an unacceptable risk to service delivery due to secondary failures if primary failures are not repaired within acceptable time frames? e.g. redundant systems	Is there an unacceptable risk to service delivery due to secondary failures if primary failures are not repaired within acceptable time frames? e.g. redundant systems
Is availability critical but high levels of reliability unachievable due to complexity, novelty or cost?	

Primary maintainability questions	Secondary maintainability questions
Is the required service continuous and is it important to be able to conduct maintenance while the item is still functional?	Is preventive maintenance required to preserve necessary levels of reliability and can maintainability attributes be influenced?
Is minimal downtime critical but preventive maintenance is required to preserve necessary levels of reliability?	Is it important to be able to conduct maintenance while the item is still functional and can maintainability attributes be influenced?
Is minimal downtime critical?	Does an expansive support system already exist?

Supportability questions
Is there limited control over the physical design aspects of the item?
Is there limited ongoing resourcing for support?
Do physical constraints limit access to support artefacts i.e. space or weight restrictions, remote locality?
Is reaching the specified useful life critical?
Is there a large influence of human factors in the ability to restore functionality within time limitations?
Is the support of the item going to be subcontracted?

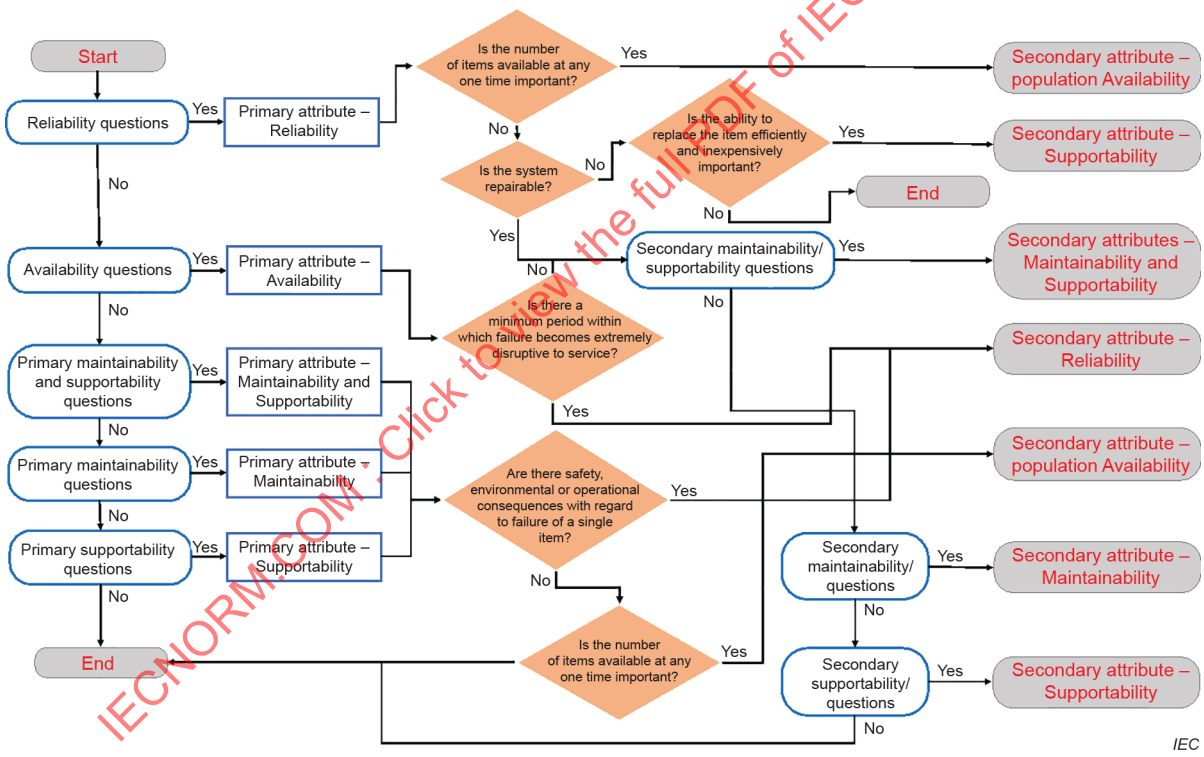

Figure B.1 – Process for prioritizing attributes

Annex C
(informative)

Development of a dependability specification for a home security system

NOTE The following example is used for illustration purposes. The system configuration and operating procedures are typical for a home security system. The dependability data in this example do not reflect the performance results of any specific manufacturer's product or service operation.

C.1 Define stakeholder needs and expectations

The homeowner needs a security system that sets an alarm automatically in case of fire and smoke hazards or intrusion and alerts a supporting service for security protection. The homeowner needs the system to set the alarms reliably when needed, without false alarms, and for the authorized people to be able to deactivate the alarm.

C.2 Develop supporting documentation

C.2.1 Describe the system

A home security system consists of two interacting systems: a stand-alone home alarm system and a separate supporting security service system, involving the police, fire brigade, medical emergency, and other security protection services.

C.2.2 Describe the system objectives

The objectives of the system are:

- to detect fire and smoke hazards and intrusion in the home and set an alarm;
- to alert the authorities (i.e. police, fire brigade, medical emergency, security service provider) for protection.

C.2.3 Identify the key functions to meet system objectives

A home security system has the following primary functions:

- detection function for hazards and home intrusion;
- control function for information processing;
- alarm function to alert home occupants and security services;
- security service function to protect home and occupants from possible harm.

C.2.4 Describe the functions

The detection, control, and alarm functions are needed at the home premises. These three basic functions are generally integrated into a self-contained alarm system for home installation. This meets the first objective of the home security system.

- Detection function includes:
  - Sensing the presence of fire, smoke, and carbon-monoxide emissions at a hazardous level in the home premises. A practical means for detection is to place monitoring devices such as heat sensors and smoke detectors at strategic locations throughout the home premises.

  - Sensing the intrusion, forced entry or presence of unauthorized persons in the home premises. A practical means for detection is to place perimeter sensors and motion detectors in strategic locations throughout the home premises. To prevent burglary or unauthorized access through locked doors and windows from the outside, magnetic, electrical and acoustic sensors can be installed for doors and windows to detect forced entry and window glass-breakage.

- Control function includes:
  - Processing the detected signals from the sensors to activate the alarm. A practical means for processing data is an electronic processor with embedded firmware to drive the processing unit.
  - Communicating the processed data for display on the control panel for manual intervention. A practical means for communication of processed data and display is by wire-line or wireless connections to facilitate signal processing.
  - Power conversion providing electrical energy to operate the system functions. In case of main power failure or outage, a rechargeable battery can be used as backup power supply.
  - Auto-bypassing can be programmed for control to permit optional home-away arming. When activated by an authorized code, the system allows home occupants to exit within a specified exit time (e.g. 90 s) before automatically reactivating the system. The authorized code is needed for re-entry to the home premises within a specified time without activating the alarm to alert for protection service.
- Alarm function includes:
  - Direct connection via telephone lines to alert security services of an alarm situation.
  - Generating a loud sound for a preset duration to alert the occupants. This can be a siren activated by the processor triggered by an alarm situation.
- Security service function includes:
  - Activating a command to alert the security service provider for emergencies. This can utilize the home telephone dial-up line connection between the control panel and the communication system of the security service provider.

The security service function requires the interaction of the home alarm system with other external systems provided by the security service provider for home protection services. There are protocols and procedures needed by regulations for responding to a service alarm call. Different security service providers have to activate their own specific systems to link to the home to be protected. This meets the second objective of the home security system.

The combined effects of the interacting systems (i.e. the home alarm system and the security service system) permit a comprehensive home security system in meeting the specified system objectives.

C.2.5 Identify the influencing factors affecting the functions

Using Table D.1 and Table D.2 as guidance, key influencing factors can be identified from the matrix relationships affecting the functions. The purpose is to focus on factors having significant impacts on system functions, hence affecting system performance.

The following key influencing factors have been identified for the selection or design of each of the necessary functions.

Detection
- type and cost of various sensors suitable for detection purposes;
- number of sensors needed for full or partial coverage to minimize risk exposures;
- technology and reliability of sensors;
- ease of sensor installation and maintenance;
- expected life of sensors.

Control
- specific design or use of commercially available control units with most features;
- ease of use and programming for arming and disarming the system;
- automatic bypass and delay activation time adjustments;
- number of detection zones available for monitoring by the control panel;
- wire-line or wireless connections to sensors;
- life of backup battery;
- trouble display for system diagnosis;
- communication to alert the security service agency for protection.

Alarm
- loudness of audible sound when activated;
- energy consumption of the audible alarm device (e.g. siren).

Security service
- maintenance contract schedule and cost;
- types of protection services available;
- surveillance and monitoring service provisions (e.g. around the clock);
- response time when alerted;
- regulations governing security service provision;
- false alarm consequences.

C.2.6 Evaluate the technical approach to achieve the needed functions

The technical approach deals with acquiring and maintaining the needed functions for sustained operation within cost and time constraints. The protection by security service providers readily available in the marketplace forms an essential part of the system evaluation process. Social and economic issues, such as impact on community crime prevention and effects on the environment resulting from the installation and use of the home security system, are not addressed.

Key technical issues include evaluation of the needed functions in terms of cost, technology, and protection services.

Detection	Technology is the main driver on detection cost. The types of sensors include smoke and motion sensors, magnetic and electrical sensors with proven reliability that can meet most detection needs. These sensors are available in various forms and configurations at reasonable cost but they require direct wiring connections at the home premises. This affects a one time installation cost. More expensive sensors for detection of window glass-breakage and wireless monitoring sensors are available for commercial applications. These sensors use more advanced technology at a premium price which cannot be cost justified for home use. Wireless technology for sensor detection is more susceptible to interference causing false alarms. However, new technology sensors are more suitable for a large building complex to facilitate installation, modification and maintenance services.
Control	The basic design for the control unit is reliable, inexpensive, and commercially available. The control unit is the heart of the home alarm system providing most operating features commonly needed for home alarm use. Wireless technology incorporated in new system designs facilitates installation and maintenance services, but at a premium price. Backup battery has a life of three to five years. From a home user perspective, there is no difference in performance between the wired system and the wireless system.
Alarm	All systems are using similar alarm devices. There is no difference in cost or technology variation.
Security service	Security service providers can offer various maintenance contracts to suit the home owner's needs. These contracts are based primarily on the initial installation of the system, the warranty schemes and subsequent support services and contract duration. There are some minor variations in cost and contract terms due to market competition in the home security business. A life cycle cost analysis would be appropriate to justify the investment of acquisition and ownership costs over the life period of the home security system. The hardware installed for the home alarm system should have a life expectancy of 15 years. Regular maintenance check and safety tests should be followed.

C.2.7 Describe the hardware, software, and human elements involved in the system operation

Hardware	All system hardware for the home alarm system can be integrated and installed in the home premises. The system is automated. It requires minimal attention to its operating functions. Maintenance and safety checks are simple procedures.
Software	The system control unit incorporates embedded firmware to drive its processing functions. Programming and changing access codes are straight forward. An instruction manual of the home alarm system provides a step-by-step procedure for the programming effort.
Human	The home alarm system is designed to ensure fitness-for-use under safety regulations for the home security system operation. User friendly access to the control panel display facilitates diagnosis and communication during daily normal mode of operation. When an alarm is activated resulting in a security service alert mode of operation, a standard protocol is followed by the responding security agencies (i.e. police, fire marshal, medical emergency, security service provider) according to their respective procedures. The procedure for verifying a false alarm is done by standard protocol initiated by the security service provider. The home owner may cancel the false alarm by entering the assigned pass code to the control panel. The false alarm rate is very important for a home security system.

C.2.8 Determine the use profile of the system

Different scenarios can be established to provide a specific use profile during the security service alert mode of operation. The following are three typical examples.

- When the home alarm system has detected an abnormal situation at the home premises, whether it is an actual hazard detected or a false alarm, only the security service provider is alerted to respond. The normal protocol is to immediately utilize the home telephone connection to contact the occupant and request proper identification to assess probable causes of the alert. Failing that, the security service provider calls other persons pre-authorized by the home owner to assess the situation. If not successful, the police are contacted to report the incident. The police respond to an emergency alarm at the home premises. This is the normal mode of operation.
- When the control panel panic button is activated by the home occupant, the police, fire marshal, and the security service provider are all alerted at the same time. They respond to the emergency alert to provide protection at the home premises according to their respective procedures. This is the panic mode of operation.
- For the security mode of operation, this is the extension of the normal mode of operation by engaging additional special protection services.

C.2.9 Describe the modes of operation of the system

- For normal mode of operation

  For the normal mode of operation, the home alarm system requires the availability of all the functions for detection, control and alarm operating full time for system dependability. In a home alarm system, upon detection of a hazard or an intrusion at the home premises, the control function immediately activates an alarm to alert the home occupants and the security service provider. Figure C.1 shows the system configuration for the normal mode of operation. The system can be reset by the homeowner. Reset within 30 s cancels the call to the security service provider.

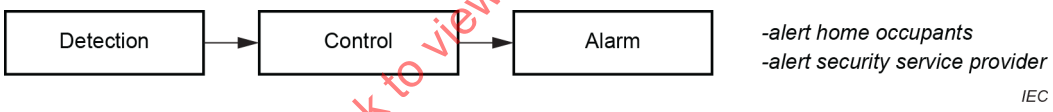

Figure C.1 – System configuration for normal mode of operation

- For security service alert mode of operation with panic scenario

  When the panic button is activated for any reason, the police, the fire marshal, and the security service provider is alerted directly by the home alarm system. The home alarm system is operating full time, but the detection function is bypassed and the alarm sound silent. A typical panic scenario could be the home occupant pressing the panic button on the control panel when noticing an emergency situation. Examples include a potential fire hazard the occupant is unable to control, a suspicious intruder near the home premises, or seeking immediate medical assistance. Figure C.2 shows the system configuration for the panic mode of operation.

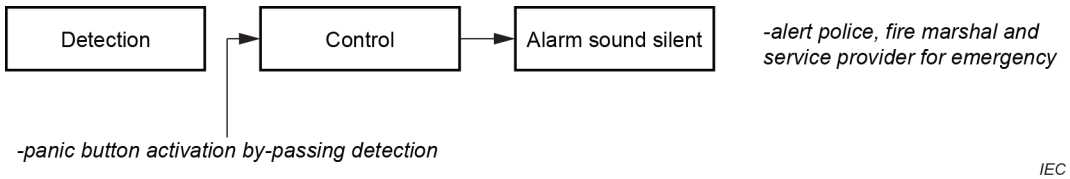

Figure C.2 – System configuration for panic mode of operation

- For security service alert mode of operation with security service alert scenario

  When the security service provider receives an alert signal from the home alarm system, a specific protocol is followed. The process includes automatically utilizing the phone line calling the home occupant to assess the situation. Failing that, other pre-authorized persons

are contacted. If not successful, the police are alerted for an emergency situation at the home premises. The availability of the home alarm system is operating full time and interacting with the system or systems used by the security service provider. The following are typical system elements utilized by the security service provider.

– Human element involving the security attendant making the necessary phone calls. The availability of the security attendant on-call is continuous 24 h per day and 7 days per week and year round service.

– The services provided by the telephone company to subscribers. The availability of the telephone service to subscribers is continuous year round.

– The police and emergency cruisers, usually employing a motor vehicle, but sometimes may engage a helicopter for transporting emergency services for medical attention. The availability of these transportation means is usually in terms of response time to arrive at the scene.

Figure C.3 shows the system configuration for the security service mode of operation.

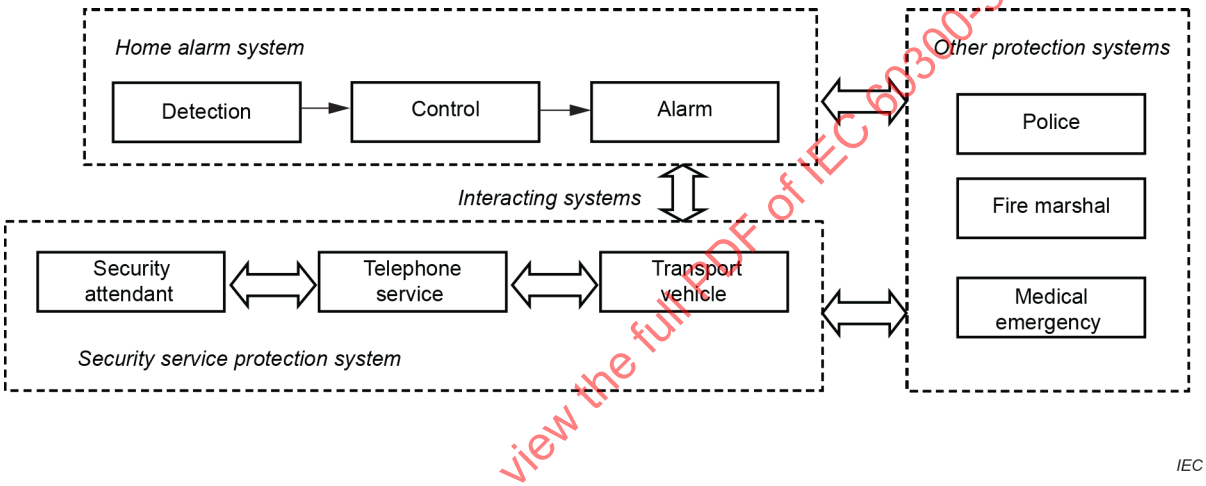

Figure C.3 – System configuration for security service mode of operation

C.2.10 Maintenance and support requirements

All maintenance and support shall be provided by the security service provider to provide the required availability (see Clause C.3). The homeowner shall undertake a monthly test of the system by activating the alarm then resetting it.

C.3 Derive the dependability requirements

NOTE The data presented in this example are for illustration purposes only. They do not represent the dependability data of any specific systems, products or services.

The dependability requirements of the system functions can be determined by establishing the system operating scenario and the requirements of the specific functions identified in the evaluation process. The following summarizes the dependability requirements of each function of the home security system. The numerical values of the functions representing the home alarm system are determined through market surveys and competitive product testing, as well as through technology evaluation and capability analysis of the selected elements for the system within cost and regulatory constraints. The numerical values of the functions identified for the security service protection system are derived from the respective field experience data. A series model is used for determining the overall availability of the system.

Home alarm system

- Detection function: 99,5 % availability; annual maintenance check, expected life 15 years.
- Control function: 99,9 % availability; monthly security system check, expected life 20 years.
- Alarm function: 99,9 % availability; annual maintenance check, expected life 20 years.

Security service protection system

- Security attendant function: 99,7 % availability with shift rotation 24 h year round service alert.
- Telephone service function: 99,999 7 % availability for wire-line service.
- Transport vehicle function: 99,8 % availability with redundant vehicles or other transportation means with a response time within 10 min.

C.4 Complete dependability specification

The system dependability requirements form part of the overall system specification. The following summarizes the data inputs for documenting the system dependability specification.

d) System identification

A home security system with the home alarm system installed at the home premises supported by a remote security service system.

e) System objectives

Automated detection and alarm for home protection by security services.

f) System use profile

- normal mode of operation;
- panic mode of operation;
- security mode of operation.

g) System maintainability and maintenance access requirements

The system is maintained by automatic built-in test monitoring of key functions and monthly manual security check by the home owner using the control key pad to verify the functioning and operation of the home security system.

h) System configurations

Reference Step 9 for the description of system configurations for each mode of operation.

i) System functions

- detection, control, and alarm functions needed for the home alarm system;
- security attendant, telephone service, and transport vehicle functions needed for the security service protection.

j) Dependability requirements for each function

- Home alarm system

  Detection function: 99,5 % availability; annual maintenance check, expected life 15 years.

  Control function: 99,9 % availability; monthly security system test, expected life 20 years.

  Expected life of backup battery is 5 years. Recommended replacement every 3 years.

  Alarm function: 99,9 % availability; annual maintenance check, expected life 20 years.

- Security service protection system

  Security attendant function: 99,7 % availability with shift rotation 24 h year round service alert.

  Telephone service function: 99,999 7 % availability for wire-line service.

  Transport vehicle function: 99,8 % availability with redundant vehicles or other transportation means.

k) Statement on system dependability

- home alarm system availability: 99,3 %;
- security service protection system availability: 99,5 %;
- home security system availability: 98,8 %.

Annex D
(informative)

Influencing factors for dependability specification

NOTE The following factors are arranged according to their importance for most situations.

D.1 Examples of constraints on system dependability

D.1.1 Economic constraints

Economic constraints are often due to budget restrictions, spending limitations or timing issues relevant to the advancement of a system's development and product realization. Economic constraints should be treated as influencing conditions on the dependability management process. Early planning regarding design-to-cost, supply chain management and life cycle cost analysis would help identify potential problem areas, provide insights for cost avoidance and create opportunities for improvement. Project risk analyses are often used in planning exercises to determine the criticality of the situation permitting to chart a course of action.

D.1.2 Time constraints

Time constraints are the second most important factor. Time to market and contractual deadlines are important for most items. The time to market is critical in order to obtain a market share, and the time to market is for most consumer products rapidly declining. The time schedule determines when analysis and tests have to be finished in order to influence the decisions. Therefore time delays are critical and can be very expensive in lost sale or delay penalties. Dependability problems are often the cause of delays due to design changes, repeated tests (regression tests) and changes in manufacturing as well as changing already produced or delivered items.

D.1.3 Regulatory constraints

Regulatory constraints may be imposed on systems for public utility services where considerations for safety and environment impact are paramount. The applicable legislation generally defines a set of methods, tools or technical impositions. These regulatory constraints are one of the influencing conditions in the evaluation of system design strategy and dependability plans.

EXAMPLE The imposition of a hood or cover over an element of a system for safety reasons could change the approach to access this element. As a consequence, it is possible that a change in the maintainability design or a modification of the existing support process will need to be incorporated.

D.2 Type of system operation

The type of operation affects the outcome of the overall system objectives. The type of operation is linked to the system application such as a transportation system for urban public transit, or a communication system for news broadcasting services. The dependability attributes associated with such systems should be evaluated in terms of regulatory, economic, social, technical and other relevant issues. This evaluation process is linked to positive expectations. For example, the expectation of a successful national electrical distribution network is linked to the effective distribution of electrical energy, thereby facilitating the country's economic activities. The result of the evaluation should create the need for a high level of reliability of the electrical system. The type of operation relates to the system application in general, whereas the mode of operation relates to the system operational scenario for a specific task performance.

D.3 Criticality of operation

D.3.1 General

Criticality is the degree to which a failure of the system may have severe consequences. The dependability attributes should be evaluated in terms of the effects on human interaction, economic impact, environmental consequences, abnormal stresses, operational impact and other relevant issues. This evaluation process is linked to consideration of events that would have a negative impact. For example, the maintainability of a national electrical distribution network is of high relevance, considering the social and economic impact of a prolonged outage or failure of the national electrical system. A blackout or brownout situation may occur in a city due to excessive use of electricity draining from the supply limit of an electrical distribution system at peak hours.

D.3.2 Type of use

A system may have several types of use, such as:

- a single use;
- short time of use and short time of storage;
- short time of use and long time of storage;
- long time of use and short time of storage;
- long time of use with maintenance;
- long time of use without maintenance.

The type of use of the system affects the dependability attributes.

- For a single use, dependability depends on the system functioning as required. Attributes include availability and reliability. Maintainability and supportability are only relevant to the storage or standby scenario.

  EXAMPLE 1 A space launcher, during storage, maintained for preparation and readiness, will achieve very high reliability during its flight.

- For a short time of use and short time of storage, the importance of supportability for a successful dependability is high due to the short time available to maintain the system.

  EXAMPLE 2 A plane that has a very efficient supportability programme will have a high flight operation to ground maintenance ratio.

- For a long time of use with maintenance, reliability, maintainability and supportability are of equal importance. The dependability attributes should be optimized for the system's operation.

  EXAMPLE 3 A nuclear power plant is relevant for this type of long time use with maintenance.

- For a long time of use without maintenance, reliability is of major importance and maintainability is of minor importance.

  EXAMPLE 4 It is impractical to repair a satellite during its orbit, and its dependability in space relies solely on the high reliability.

D.3.3 Type of users

There are different types of users of varying skills and knowledge who can operate a system. Some users may be trained professionals with an in-depth knowledge and skills on how to operate the system. Other users may not have acquired the same level of skills and knowledge to operate the same system. This influencing condition may affect the dependability attributes that are imposed on the system's design to meet varying user requirements. Special consideration should be given to the extent of human interaction with a system when designing the appropriate functions, especially for a system with an open interface to the public.

EXAMPLE Supportability requirements vary with the skill level of the system's users. System shut-down could be a simple operation by pressing a button, or it can require an elaborate procedure.

D.3.4 Dependency of interacting systems

A system may be linked to another system or interact with multiple systems to achieve its objective. In this case, their dependency should be defined in the dependability specification, especially in the primary and secondary roles of the system's operating relationship.

- High dependency: the purpose of a secondary system is to support the primary system in its operation.
- Medium dependency: a system is linked with other systems but its functions are independent from these systems.
- Low dependency: a system has no relation (apart from sources of energy) to other systems. It is able to operate alone.
- Temporary dependency governed, for example, by initiating a software routine upon command for realizing a special service or planned action.

For a high dependency system, it is important to integrate the dependability specification of the secondary system as part of the dependability requirements of the primary system.

EXAMPLE Dependability of a backup power supply that forms part of the dependability specification of the main power supply in the system specification.

D.3.5 Structure or configuration of a system

A system could have different structures or configurations consisting of a combination of various contributing elements. For example:

Type 1: a hardware system only, with no software or human element involved;

Type 2: a hardware system with no software element involved, but with strong human interaction;

Type 3: a system with hardware and software elements, but without human interaction in its operation;

Type 4: a system comprising a combination of hardware, software and human elements.

For a Type 1 system, classical dependability methods and tools as recommended in this document are fully applicable.

For a Type 2 system, the studies shall integrate human factors approaches and specifically human factors databases. These approaches are standardized in IEC 61709 [24] and for some industrial sectors.

Type 3 and Type 4 systems involve software element. Software in its pure form is deterministic, but software in use in a hardware system with real inputs cannot be assessed by classical deterministic methods. A probabilistic approach should be used to assess the degree of confidence of software dependability in the system performance. The identification of functions is similar for both hardware and software elements. Only the methodology for dependability assessment differs in the process (see IEC 62429 [27]).

In practice, most systems are combinations of both custom-made and off-the-shelf elements.

D.3.6 Technical novelty

For new technological systems, novelty implies the implementation of new technology or the use of new technical processes for problem resolution in an existing system. Three classes of system are identified:

- a completely new system using new technology;
- a new system based on an existing technological system and mature technology;
- an existing system to be modified.

For a completely new system, the lack of prior experience data imposes the use of formal methods to gain confidence in a detailed design with a high degree of engineering rigour.

For a new system based on an existing technological system and mature technology, classical dependability methods and tools applicable to the existing system may be used, but additional processes should be employed for verification and validation of the new system configuration. This is to ensure confidence in the design of the new system based on the existing technological system and mature technology.

For an existing system that is to become a modified system, classical dependability methods and tools applicable to the existing system may be used but should be verified.

D.3.7 Novelty of operation

The novelty of operation refers to setting new and uncharted operational objectives. Examples are:

- setting a completely new system operational objective;
- extending an existing system operation to meet new objectives.

For a completely new system with uncharted operational objectives, the lack of prior experience imposes a thorough assessment of the use profile and task identification, including an evaluation of all possible influencing conditions encountered during the operation in order to define the system's dependability objectives.

For extending an existing system operation to meet new objectives, prior experience data could be used to project the extension of system application. A thorough examination of the anticipated changes may need to be undertaken to ensure adequate resources are available to maintain the system extension.

D.3.8 Legacy issues

Legacy issues are matters arising from existing infrastructure in large complex systems which require service extension, capacity upgrade and capability enhancement. In systems engineering, most of the initial requirements definition and preliminary design efforts have to deal with legacy issues. Typical legacy issues include, but are not limited to:

- preservation of investments in existing infrastructure;
- societal resistance to change and regulatory constraints;
- insurance coverage of existing versus new installations;
- re-deployment of current resources;
- statement on useful life (e.g. European Union rules);
- training needs for skills transition;
- life cycle cost benefits and justification for enhancement efforts.

Sometimes the ramification of legacy issues is far more complex and costly to extend or upgrade an existing system than building a completely new system.

D.3.9 Complexity

The complexity of a system should be evaluated from a technical and functional viewpoint.

The complexity may be evaluated according to the number of interfaces between elements or subsystems included in the system and its environment, as well as according to the number of possible different system configurations to be established.

The technical complexity may be evaluated according to the number of different technologies intended for use in the system.

The functional complexity is related to the variety of service features or application functions of the system.

D.3.10 Number of systems in use

The number of systems in use may influence the choice of methods and tools used to implement dependability. If the number of the same system in use is high, the experience data feedback is relevant and test data are often available. A low number of systems in use may result in a lack of user experience data feedback. The choice of methods and tools to implement dependability may be limited. The need for a dependability demonstration may be necessary for verification. In this case probabilistic methods and tools for modelling and system simulation may be used.

D.4 Determining relevant influencing factors for the evaluation of system functions

Table D.1 and Table D.2 facilitate the determination of influencing factors affecting dependability attributes of system functions.

Table D.1 – Examples of influencing factors under each influencing condition

	Influencing conditions							
	Task requirements	**Human interaction**	**Process**	**Environment**	**Support services**	**Utilities**	**Interacting systems**	**Other factors**
Influencing factors	Nature of task	Command authorized	Input/ output	Temperature	Maintenance	Power	Boundary	Economic constraints
	Scope	Unauthorized interaction	Modes	Humidity	Documentation	Fuel	Protocol	Regulatory constraints
	Duration	Job-defined interaction	Stages	Vibration	Technical support	Energy	Interference	Technical novelty
	Sequence	Training	Cycles	Shock	Spare parts	Public utilities	Dependency	Novelty of operation
	Mode of operation	Skills	Failure protocol	Pressure	Special tools	Private utilities		Complexity
	Start-up	Interfaces		Radiation	Maintenance access	Communi cations		Number of systems
	Normal operation			Contaminations	Levels of support			Degree of redundancy
	Emergency operation			Storage				
	Shut-down			Transports				

Table D.2 – Relationship of system properties with influencing conditions

	System properties					
Influencing conditions	**Functionality**	**Performance**	**Operability**	**Dependability**	**Supportability**	**Application specifics**
Task requirements	Identify relevant functions to meet task requirements	Identify the adequacy of the functions to perform tasks under stated conditions	Identify the operational needs and interfaces with the functions	Identify the extent of reliability, maintainability and supportability of the functions	Identify the logistic support services to maintain operation of functions	Identify the health, safety and regulatory issues imposed on the functions
Human interaction	Identify the involvement of the human element in the functions	Identify the skills needed for human performance of functions	Identify the degree of difficulty in human operations with the functions	Identify the reliance of human intervention affecting dependability of functions	Identify human resources needed to support the functions	Identify the human aspects in specific application of functions
Process	Identify the procedures and methods for operating the functions	Identify the accuracy, consistency and repeatability in operating the functions	Identify the ease of use and access to operate the functions	Identify the availability and reliability in operating the functions	Identify the extent of procedural instructions and maintenance efforts to sustain operation of the functions	Identify any special processes needed for operating the functions
Environment	Identify the dominating environment affecting the design and operation of functions	Identify the operating limits or restrictions in the performance functions exposed to the environment	Identify the limitations to access and use of the functions exposed to the environment	Identify the effects on dependability of functions exposed to the environment	Identify the limitations to support or service the functions exposed to the environment	Identify any special precautions when operating in extreme or hostile environment
Support services	Identify the need for support services to maintain operation of functions	Identify the effects of support services needed to maintain accuracy of performance functions	Identify the effects of support services to enhance system operability	Identify the effects of support services to sustain dependable performance of functions	Identify any special support services needed for system modification, upgrade or disposal	Identify any special support services needed for specific application
Utilities	Identify the infrastructure for operation of functions	Identify the adequacy of utilities to sustain performance functions	Identify the effects of utilities to enhance system operability	Identify the needs and effects of utilities to sustain dependability	Identify any special power, energy, fuel, etc. to support system operation	Identify any specific tools or enabling systems needed for specific application
Interacting system	Identify the influence of interacting systems on the functions	Identify the effects of interacting system on performance functions	Identify the dependency of interacting system on system operability	Identify the effects of interacting system on dependability	Identify the system boundary and jurisdiction for supportability of interacting system	Identify the interacting system for specific application
Other factors	Identify the technical and technological constraints imposed on the functions	Identify the extent of use and the complexity in applications affecting the performance functions	Identify social and human factors affecting the normal and specific operation of functions	Identify any special factors limiting or restricting dependable performance	Identify any special factors limiting or restricting supportability of the system	Identify the economic and regulatory constraints for specific application

Bibliography

[1] IEC 60300-1:—[2], *Dependability management – Part 1: Managing dependability*

[2] IEC 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

[3] IEC 60300-3-10[3], *Dependability management – Part 3-10: Application guide – Maintainability and maintenance*

[4] IEC 60300-3-14[4], *Dependability management – Part 3-14: Application guide – Supportability and support*

[5] IEC 62628, *Guidance on software aspects of dependability*

[6] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[7] ISO/IEC/IEEE 29148:2018, *Systems and software engineering – Life cycle processes – Requirements engineering*

[8] ISO/IEC/IEEE 15289, *Systems and software engineering – Content of life-cycle information items (documentation)*

[9] IEC 62960, *Dependability reviews during the life cycle*

[10] IEC 60706-3, *Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data*

[11] IEC 62308, *Equipment reliability – Reliability assessment methods*

[12] IEC 61070, *Compliance test procedures for steady-state availability*

[13] IEC 62741, *Demonstration of dependability requirements – The dependability case*

[14] IEC 60300-3-3, *Dependability management – Part 3-3: Application guide – Life cycle costing*

[15] ISO 9000, *Quality management systems – Fundamentals and vocabulary*

[16] IEC 60706-5, *Maintainability of equipment – Part 5: Testability and diagnostic testing*

[17] IEC 62506, *Methods for product accelerated testing*

[18] IEC 61025, *Fault tree analysis (FTA)*

[19] IEC 61078, *Reliability block diagrams*

---

2 Fourth edition under preparation. Stage at the time of publication IEC PCC 60300-1:2022.

3 Second edition under consideration.

4 Second edition under consideration

[20] IEC 61703, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms*

[21] IEC 61649, *Weibull analysis*

[22] IEC 61710, *Power law model – Goodness-of-fit tests and estimation methods*

[23] IEC 62402, *Obsolescence management*

[24] IEC 61709, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*

[25] IEC 60605-6, *Equipment reliability testing – Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity*

[26] ISO 9001, *Quality management systems – Requirements*

[27] IEC 62429, *Reliability growth – Stress testing for early failures in unique complex systems*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

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

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 60300-3-4 a été établie par le comité d'études 56 de l'IEC: Sûreté de fonctionnement. Il s'agit d'une Norme internationale.

Cette troisième édition annule et remplace la deuxième édition parue en 2007. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) harmonisation avec les autres versions des six normes fondamentales de l'IEC en matière de sûreté de fonctionnement;
b) un processus de définition des exigences a été inclus;

c) les définitions et le langage utilisés ont été harmonisés avec d'autres normes relatives au système.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
56/1932/FDIS	56/1939/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Le présent document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Une liste de toutes les parties de la série IEC 60300, publiées sous le titre général *Gestion de la sûreté de fonctionnement*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu du présent document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture du présent document indique qu'il contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

La sûreté de fonctionnement est la capacité à fonctionner correctement et au moment voulu. Une entité sûre de fonctionnement est une entité dont le fonctionnement tel que souhaité et la satisfaction des attentes convenues des parties prenantes s'inscrivent dans le cadre d'une confiance légitime.

La sûreté de fonctionnement comprend de nombreux attributs, mais est généralement caractérisée par la fiabilité, la maintenabilité et la supportabilité, ainsi que par la caractéristique dérivée de la disponibilité. La sûreté de fonctionnement comprend également les caractéristiques de performances telles que la durabilité, de testabilité et de capacité de remise en état de fonctionnement, ainsi que de sûreté et d'intégrité, notamment par rapport aux systèmes logiciels.

La sûreté de fonctionnement est un attribut important qui a une influence sur la valeur générée par les entités. Par conséquent, il convient de définir et de spécifier les attributs de sûreté de fonctionnement pertinents en plus des exigences de performance fonctionnelle et des attributs physiques. Bien que principalement dédiées à la sûreté de fonctionnement au niveau du système et des équipements, de nombreuses techniques décrites dans les différentes normes IEC relatives à la sûreté de fonctionnement peuvent également être appliquées aux produits ou au niveau des composants. Le terme "entité" est utilisé tout au long du présent document pour désigner une pièce isolée, un composant, un dispositif, une unité fonctionnelle, un produit du commerce (OTS - *off-the-shelf*), un équipement, un sous-système ou un système. L'entité peut être composée de matériel, de logiciel, de personnel ou d'une quelconque de leurs combinaisons (voir l'IEC 60050-192). Pour une référence à un type spécifique d'"entité", des termes comme composant, OTS, produit ou grand système ouvert sont utilisés.

Les attributs de sûreté de fonctionnement peuvent être spécifiés pour un système ou un produit isolé (par exemple, un véhicule) et/ou un groupe de systèmes ou de produits similaires (par exemple, une flotte de véhicules similaires).

Les attributs de sûreté de fonctionnement peuvent être spécifiés au moyen de mesures quantitatives et/ou qualitatives. Des méthodes statistiques peuvent s'avérer nécessaires pour apprécier les valeurs de certains attributs de sûreté de fonctionnement parmi les attributs atteints.

Les niveaux de fiabilité, de maintenabilité, de supportabilité et de disponibilité atteints par une entité dépendent des conditions de réalisation, d'utilisation, de maintenance et de support de cette dernière, ainsi que du profil de cycle de vie du système. Il convient également de définir les éléments suivants dans les exigences de la spécification de la sûreté de fonctionnement:

- les conditions de stockage, de transport, de réalisation et d'utilisation de l'entité;
- le profil de cycle de vie et la vie utile prévue;
- les politiques de maintenance;
- le support disponible.

Les attributs de sûreté de fonctionnement ainsi que d'autres caractéristiques de performance peuvent être spécifiés de différentes manières selon la situation. Dans le cadre d'un projet de base où un acquéreur obtient une entité auprès d'un fournisseur, il en existe trois types principaux:

1) les spécifications produites par le fournisseur;
2) les spécifications produites par l'acquéreur;
3) les spécifications convenues ou produites mutuellement par le fournisseur et l'acquéreur.

Les recommandations du présent document sont applicables à ces trois types de spécifications et peuvent être adaptées à d'autres situations si cela est nécessaire.

Le présent document fournit des recommandations pour la production d'exigences en matière de sûreté de fonctionnement dans les spécifications, ainsi qu'un moyen d'assurer le respect de ces exigences.

Le présent document constitue l'une des six principales normes de sûreté de fonctionnement corrélatives qui fournissent aux responsables et au personnel technique des recommandations relatives à la planification et la mise en œuvre efficaces des activités de sûreté de fonctionnement. De fait, il convient d'utiliser le présent document conjointement avec:

- l'IEC 60300-1 [1][1], qui souligne l'importance et les avantages de la gestion de la sûreté de fonctionnement. Elle fournit des recommandations sur les activités de sûreté de fonctionnement et la façon de les intégrer dans un système de gestion existant, et sur les processus de cycle de vie;
- l'IEC 60300-3-1 [2], l'IEC 60300-3-10 [3], l'IEC 60300-3-14 [4] qui fournit des recommandations sur l'identification et l'application les techniques d'analyse et d'assurance appropriées pour la fiabilité, la maintenabilité (et la maintenance) et la supportabilité (et le support) respectivement. Une norme traitant de la disponibilité est planifiée.

[1] Les chiffres entre crochets renvoient à la bibliographie

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

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

1 Domaine d'application

La présente partie de l'IEC 60300 fournit des recommandations relatives à la spécification des exigences de sûreté de fonctionnement et au rassemblement de ces exigences dans une spécification, ainsi qu'une liste des moyens permettant d'assurer la réalisation des exigences de sûreté de fonctionnement.

Les recommandations fournies comprennent:

- la spécification d'exigences quantitatives et qualitatives de fiabilité, de maintenabilité, de supportabilité et de disponibilité;
- des conseils aux acquéreurs portant sur la façon d'assurer que les exigences peuvent être satisfaites par les fournisseurs;
- des conseils aux fournisseurs afin de les aider à satisfaire aux exigences des acquéreurs.

D'autres obligations telles que des règlements législatifs et gouvernementaux peuvent aussi imposer des exigences relatives aux entités, en plus de toutes les exigences déduites conformément au présent document.

Bien que principalement dédiées à la sûreté de fonctionnement au niveau du système et des équipements, de nombreuses techniques décrites dans les différentes normes IEC relatives à la sûreté de fonctionnement peuvent également être appliquées aux produits ou au niveau des composants. Le terme "entité" est utilisé dans l'ensemble du présent document.

Ces recommandations sont données dans le cadre d'un projet de base où un acquéreur obtient une entité auprès d'un fournisseur. Elles peuvent être modifiées et adaptées à d'autres situations si cela est nécessaire.

NOTE 1 Le présent document ne prend pas directement en considération les spécifications de sécurité et environnementales, bien que la majorité des recommandations du présent document puissent également s'y appliquer.

NOTE 2 Le présent document ne couvre pas les entités qui font l'objet de dispositions particulières à long terme impliquant plusieurs parties prenantes (par exemple, les services fournis par le biais de partenariats d'approvisionnement public-privé) et la manière dont la sûreté de fonctionnement est spécifiée dans ces dispositions.

NOTE 3 Les recommandations du présent document peuvent être appliquées à différents aspects de la spécification des exigences relatives aux logiciels, mais des recommandations spécifiques peuvent être consultées dans l'IEC 62628 [5] et dans les différentes parties de la série IEC 61508 [6].

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60050-192, *Vocabulaire électrotechnique international (IEV) – Partie 192: Sûreté de fonctionnement* (disponible à l'adresse http://www.electropedia.org)

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC 60050-192 ainsi que les suivants, s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

NOTE Les définitions de "sûreté de fonctionnement", "disponibilité", "fiabilité", "maintenabilité", "supportabilité", "défaillance", "panne", "temps avant défaillance", "temps de bon fonctionnement", "vérification" et "validation" sont données dans l'IEC 60050-192.

3.1
objectif
déclaration qui traduit ou exprime des souhaits ou des aspirations et pour laquelle la preuve de réalisation n'est pas nécessaire ou ne peut pas être apportée

3.2
entité
sujet que l'on considère

Note 1 à l'article: L'entité peut être une pièce isolée, un composant, un dispositif, une unité fonctionnelle, un équipement, un sous-système ou un système.

Note 2 à l'article: L'entité peut être composée de matériel, de logiciel, de personnel ou d'une quelconque de leurs combinaisons.

Note 3 à l'article: L'entité est souvent composée d'éléments dont chacun peut être examiné individuellement.

[SOURCE: IEC 60050-192:2015, 192-01-01, modifié – Note 3 modifiée par l'omission des références internes et Notes 4 et Notes 5 supprimées.]

3.3
produit du commerce
OTS
entité immédiatement disponible qui est à la fois commerciale et vendue en quantité importante sur le marché

Note 1 à l'article: Parfois appelé COTS (*commercial off-the-shelf* - disponible dans le commerce) ou MOTS (*modified off-the-shelf* - disponible avec modification).

Note 2 à l'article: L'abréviation "OTS" est dérivée du terme anglais développé correspondant "*off-the-shelf*".

3.4
exigence
déclaration qui traduit ou exprime un besoin et les contraintes et conditions qui y sont associées

Note 1 à l'article: Les exigences se retrouvent à différents niveaux de la structure du système.

Note 2 à l'article: Une exigence est l'expression d'un ou plusieurs besoins particuliers d'une manière très spécifique, précise et explicite.

Note 3 à l'article: Une exigence se rapporte toujours à un système, un produit ou un service, ou toute autre entité, présentant un intérêt.

Note 4 à l'article: Une exigence est une déclaration pour laquelle une preuve ou une assurance de conformité peut être fournie.

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.19 [7], modifié – Note 4 ajoutée.]

3.5
spécification
<de sûreté de fonctionnement> information qui définit les exigences et les objectifs de sûreté de fonctionnement d'un système, d'un produit ou d'un service, ainsi que toute information complémentaire

Note 1 à l'article: Les informations complémentaires peuvent inclure des informations d'utilisation, des conditions de fonctionnement et environnementales, des critères de défaillance et les méthodes prévues pour l'assurance de la conformité aux exigences, y compris les critères d'acceptation/de rejet.

Note 2 à l'article: L'ISO/IEC/IEEE 15289 [8] définit la spécification comme une information qui définit de manière exhaustive, précise et vérifiable les exigences, la conception, le comportement ou d'autres caractéristiques prévues du système, du service ou du processus. La spécification de la sûreté de fonctionnement a un domaine d'application plus large que celui utilisé dans l'ISO/IEC/IEEE 15289.

3.6
vie utile
<d'une entité> intervalle de temps depuis la première utilisation jusqu'à ce que les besoins de l'utilisateur ne soient plus satisfaits à cause de facteurs de performance, d'obsolescence et/ou économiques

Note 1 à l'article: L'intervalle de temps applicable dépend de la nature et de l'application de l'entité et peut être le temps écoulé, les heures de fonctionnement, le nombre de cycles, etc.

Note 2 à l'article: Les facteurs de performance à prendre en considération pour la vie utile incluent une réduction des performances de l'entité en dessous des limites acceptables qui ne peut pas être corrigée, une modification des exigences de performance ou de service, une plus grande probabilité de défaillance ou une disponibilité réduite.

Note 3 à l'article: Les facteurs économiques à prendre en considération pour la vie utile incluent des coûts de maintenance excessifs, des coûts d'exploitation plus élevés et l'émergence de solutions plus rentables.

Note 4 à l'article: Dans certains cas, la vie utile d'une entité est plus longue que celle exigée par un organisme, auquel cas sa valeur est résiduelle et son objet peut être redéfini.

Note 5 à l'article: La première utilisation exclut, dans ce contexte, les essais préalables à la livraison de l'entité à l'utilisateur final.

[SOURCE: IEC 60500-192:2015, 192-02-27, modifié – "coûts de fonctionnement et de maintenance ou pour obsolescence" remplacé par "facteurs de performance, d'obsolescence et/ou économiques".]

4 Spécification de la sûreté de fonctionnement

4.1 Description de la spécification de sûreté de fonctionnement

4.1.1 Qu'est-ce que la sûreté de fonctionnement?

La sûreté de fonctionnement est la capacité à fonctionner correctement et au moment voulu. Une entité sûre de fonctionnement est une entité dont le fonctionnement tel que souhaité et la satisfaction des attentes convenues des parties prenantes s'inscrivent dans le cadre d'une confiance légitime.

La sûreté de fonctionnement a une forte influence sur la perception par l'utilisateur de la valeur d'une entité conçue ou fournie par un organisme. Ainsi, une faible sûreté de fonctionnement a une influence sur la profitabilité et la réputation d'un organisme.

Un ensemble d'attributs mesurables ou démontrables permet de spécifier et de vérifier la sûreté de fonctionnement. Lorsque la pratique le permet, ces attributs sont quantifiés. La sûreté de fonctionnement est généralement caractérisée par la fiabilité, la maintenabilité et la supportabilité, ainsi que par la caractéristique dérivée de la disponibilité.

- La fiabilité se rapporte à la capacité de fournir une fonction exigée pendant un intervalle donné (temps, cycles de fonctionnement, distance, etc.).

- La maintenabilité se rapporte à la facilité et à la rapidité avec lesquelles une entité peut être maintenue ou restaurée dans un état de fonctionnement exigé.
- La supportabilité est la capacité de support qui permet de maintenir la capacité opérationnelle exigée avec un profil d'utilisation défini et compte tenu des ressources logistiques et de maintenance.
- La disponibilité est la capacité à être en état de fonctionner lorsque cela est nécessaire. Elle est souvent définie comme le rapport entre le temps de disponibilité et le temps total. Étant donné que la fiabilité, la maintenabilité et la supportabilité constituent des facteurs qui contribuent de manière significative au temps de disponibilité et au temps d'indisponibilité, la disponibilité est influencée par les compromis entre ces attributs.

La sûreté de fonctionnement est également liée à d'autres attributs des processus du cycle de vie tels que la conception, la fabrication, l'installation, ainsi que l'activité d'exploitation et de support en cours. En outre, la sûreté de fonctionnement a également une influence sur d'autres attributs tels que la sécurité et la protection de l'environnement; en effet, l'incapacité à exécuter une fonction a des conséquences sur la sécurité ou la protection de l'environnement. Il convient donc que la spécification de la sûreté de fonctionnement fasse partie de la spécification de l'entité et que l'interaction entre les exigences de sûreté de fonctionnement et les exigences fonctionnelles soit identifiée et prise en considération.

4.1.2 Qu'est-ce qu'une exigence?

Une exigence de sûreté de fonctionnement est une déclaration d'un seul aspect d'un attribut de sûreté de fonctionnement qui exprime un ou plusieurs besoins ou attentes des parties prenantes et pour laquelle des preuves ou une assurance de conformité peuvent être fournies. Plusieurs exigences peuvent s'avérer nécessaires afin de définir pleinement la méthode qui doit être appliquée afin de satisfaire aux besoins et attentes d'une partie prenante pour chaque attribut de sûreté de fonctionnement. Cela implique la fragmentation des besoins et des attentes en matière d'aspects individuels des attributs de sûreté de fonctionnement et la détermination de l'équilibre entre ces aspects.

Les exigences constituent la partie de la spécification à laquelle l'acquéreur demande au fournisseur de se conformer et de fournir la preuve ou l'assurance de cette conformité. Cette preuve peut être fournie avant que l'entité soit utilisée comme partie des produits livrables ou dès utilisation de l'entité, par le biais d'incitations (ou de pénalités) liées à la satisfaction (ou à la non-satisfaction) des exigences.

Les mesures de la performance de sûreté de fonctionnement constituent les différentes méthodes qui permettent de définir chacun des attributs de ladite sûreté dans le cadre d'une exigence. Voir 5.4.7 à 5.4.10 pour de plus amples informations.

4.1.3 Qu'est-ce que l'assurance?

L'assurance est un motif de confiance légitime qu'une revendication a été ou est satisfaite. Elle est généralement fournie comme un élément de preuve visant à réduire l'incertitude liée à la réalisation des exigences de sûreté de fonctionnement. Ces preuves sont le résultat d'activités développées pour satisfaire aux exigences, les démontrer et gérer les risques, telles que l'analyse et les essais.

4.1.4 Qu'est-ce que la spécification de sûreté de fonctionnement?

Les exigences applicables à une entité sont rassemblées dans une spécification. Étant donné que le contexte prévu dans lequel l'entité est utilisée, tel que la demande attendue et l'environnement d'exploitation, a aussi une influence sur les performances en matière de sûreté de fonctionnement, il convient également de fournir ce contexte dans la spécification sous forme d'informations complémentaires (voir 5.3 pour des recommandations supplémentaires). Il est également important de veiller à l'exactitude des spécifications tout au long du cycle de vie de l'entité et celles-ci doivent être mises à jour conformément aux modifications des exigences ou du contexte.

4.1.5 Quels attributs spécifier?

La méthode de spécification des exigences de sûreté de fonctionnement dépend du type et de la nature de l'entité, par exemple le fait qu'elle soit une entité réparable ou non réparable, et le fait qu'elle soit ou non un dispositif à utilisation unique. Par exemple, seules les exigences de fiabilité pour les entités non réparables qui n'exigent pas de maintenance doivent être spécifiées. Les exemples d'entités non réparables incluent les entités scellées et les entités dont les frais de réparation dépassent le coût de remplacement, telles que de nombreux biens de grande consommation, et les entités distantes, telles que les systèmes en haute mer et les satellites, pour lesquelles les ressources de maintenance utilisables font défaut lorsqu'elles s'avèrent nécessaires. Les dispositifs à utilisation unique comprennent les explosifs, les coussins d'air pour passager et les torchères de sécurité. Pour les entités non réparables, le remplacement de sous entités est parfois une préoccupation et des exigences de maintenabilité peuvent être spécifiées, le cas échéant.

Cependant, de nombreuses entités complexes sont réparables et la maintenabilité est importante pour l'acquéreur ou l'utilisateur, par exemple pour augmenter la vie utile de l'entité. Il convient de spécifier les exigences de maintenabilité si les coûts de maintenance contribuent significativement au coût du cycle de vie, si les temps d'indisponibilité peuvent entraîner une réduction significative de la valeur ou si la maintenance est importante pour l'acquéreur ou l'utilisateur. Les exigences de maintenance préventive et corrective peuvent être spécifiées le cas échéant.

La supportabilité est le résultat combiné du support exigé et de la logistique exigée pour fournir ce niveau de support. Le niveau de supportabilité est très souvent influencé par les conditions d'utilisation et des facteurs qui varient au cours du cycle de vie. Par conséquent, les exigences de supportabilité et/ou de support peuvent être importantes dans une spécification.

Les exigences de disponibilité sont généralement spécifiées pour des entités pour lesquelles le temps d'indisponibilité peut provoquer des pertes économiques, ou autres, par le biais des coûts d'exploitation accrus, des dommages corporels ou de pertes de service, par exemple pour les réseaux de communication des usines de production, des appareils médicaux, des équipements de sécurité et des systèmes militaires. La disponibilité peut être déterminée à partir de la configuration de l'entité, de ses sous-systèmes et de sa fiabilité, sa maintenabilité et sa supportabilité dans le contexte des dispositions opérationnelles et de support. La disponibilité peut également être exprimée en tant que niveaux de service à fournir à un opérateur ou à des utilisateurs finaux.

4.1.6 Contrat portant sur la sûreté de fonctionnement

L'objet de toute spécification est de fournir une base de développement ou d'acquisition d'une entité. La spécification fait généralement partie du contrat entre l'acquéreur et le fournisseur et il est donc essentiel que la production de la spécification soit telle qu'elle puisse être utilisée pour passer un contrat. Un contrat portant sur la sûreté de fonctionnement peut prendre de nombreuses formes, des paiements d'étapes dépendant de la réussite d'une revue d'état (voir IEC 62960 [9]) ou d'un essai de démonstration à la mise en place de clauses de pénalités et d'incitations à la satisfaction de la sûreté de fonctionnement durant l'exploitation, comme les contrats axés sur les performances.

Les avantages et les inconvénients des différents types de contrats sont les suivants.

- Les pénalités pour performance insuffisante incitent le fournisseur à accorder toute son attention à la sûreté de fonctionnement et peuvent conduire à des niveaux de sûreté de fonctionnement plus élevés que les niveaux obtenus autrement.
- Les incitations à la satisfaction à l'essai de démonstration encouragent le fournisseur à se concentrer sur la démonstration de la sûreté de fonctionnement. Toutefois, les essais de démonstration peuvent être onéreux et chronophages, et n'indiquer que peu avant la livraison que l'entité ne satisfait pas à ses exigences de sûreté de fonctionnement. Il est également important de prendre en considération, lors de l'inclusion de démonstrations de sûreté de fonctionnement dans les contrats, les risques pertinents pour le fournisseur et

l'acquéreur associés à la conception de ces démonstrations. Par exemple, la conception de l'essai détermine la probabilité d'accepter par erreur une mauvaise entité (risque pour l'acquéreur) ainsi que la probabilité de rejeter par erreur une bonne entité (risque pour le fournisseur). Pour gérer équitablement ces risques, il convient d'équilibrer les niveaux de confiance auxquels une mesure de sûreté de fonctionnement doit être démontrée ainsi que le nombre d'essais exigés (ou disponibles).

- Exiger du fournisseur qu'il assure la maintenance l'incite à atténuer le risque d'une faible disponibilité de l'entité, dans la mesure où il peut ensuite connaître des pertes conséquentes de la non-fiabilité de l'entité. Toutefois, cette disposition exige un contrat d'une durée bien plus longue, par exemple, un contrat de maintenance à coût fixe, avec les difficultés associées.

Les modalités de production de la spécification dépendent des circonstances. Il existe trois principaux types de spécifications:

- les spécifications produites par le fournisseur;

  Ces spécifications sont principalement utilisées pour des entités produites en série qui doivent présenter certaines caractéristiques de sûreté de fonctionnement afin d'être acceptées par le marché. Ces spécifications sont par conséquent utilisées entre l'équipe de gestion du fournisseur et son équipe de développement de produits. Les spécifications servent principalement pour des entités normalisées telles que des produits industriels, des produits de consommation ou des composants.

- les spécifications produites par l'acquéreur;

  Ces spécifications sont utilisées principalement lorsqu'un acquéreur recherche une entité à des fins spécifiques comme des composants ou des OTS. Elles sont également utilisées lorsqu'un acquéreur lance un appel d'offres.

- les spécifications convenues ou produites mutuellement par le fournisseur et l'acquéreur;

  Ces spécifications sont utilisées principalement pour des entités spécifiées par l'acquéreur qui sont des entités habituellement uniques ou des entités produites en petites quantités. Souvent, le processus débute par un appel d'offres provenant de l'acquéreur, suivi par une offre provenant d'un fournisseur. Un contrat est négocié y compris la spécification finale produite par le fournisseur et l'acquéreur.

Le contenu de la spécification varie selon son type. Le paragraphe 5.3 énumère les différents types de documentations explicatives qu'il est nécessaire d'adapter à la nature exacte de la spécification.

4.2 Principes

4.2.1 Généralités

Le développement des exigences de sûreté de fonctionnement et la création de la spécification de sûreté de fonctionnement reposent sur un ensemble de principes. Il convient que ces principes aient une influence sur le but d'un organisme, ainsi que sur son approche en matière de conception et de sûreté de fonctionnement d'une entité. L'application de l'ensemble de ces principes permet de tirer un profit maximal de la spécification de sûreté de fonctionnement.

4.2.2 Approche d'un système

Généralement, un système dont la sûreté de fonctionnement doit être spécifiée peut inclure des équipements (tant matériels que logiciels), les personnes en charge de sa gestion, de son exploitation et de sa maintenance, des données, des processus et des procédures, ainsi que des installations, des matériaux et des entités dont l'occurrence est naturelle.

Des exigences peuvent être définies pour:

- le système dans son ensemble;
- tout composant ou sous-système;

- une entité distincte (par exemple, un produit ou une entité);
- un ensemble d'entités (par exemple, une flotte de produits ou d'entités);
- un ensemble de fonctions (par exemple, un service ou un ensemble de services).

La sûreté de fonctionnement d'une entité est généralement influencée par ses conditions d'utilisation, par les personnes qui l'utilisent ainsi que par son environnement d'exploitation. Par conséquent, il convient de spécifier les exigences de sûreté de fonctionnement en prenant en considération non seulement l'entité proprement dite, mais également le système plus large de son utilisation, ainsi que les interfaces avec d'autres systèmes. Cette disposition implique les personnes qui utilisent l'entité, ainsi que son mode d'utilisation. Il convient de surveiller les conditions d'utilisation et de gérer les modifications comme faisant partie de l'obtention de la sûreté de fonctionnement au cours du cycle de vie de l'entité.

4.2.3 Exigences et objectifs

Il est important de différencier clairement les exigences et les objectifs des parties prenantes décrits dans une spécification, car la méthode d'assurance diffère.

Une exigence est un élément essentiel des besoins et attentes de l'acquéreur et la preuve ou l'assurance de la conformité à l'exigence doit pouvoir être apportée. Un objectif n'est pas une exigence, mais le souhait ou le but de l'acquéreur. Par ailleurs, la preuve du degré d'atteinte de l'objectif n'est pas nécessaire ou ne peut pas être apportée.

Il convient de définir à la fois les exigences et les objectifs. Par exemple, pour des systèmes de haute disponibilité ou de haute fiabilité, la preuve justifiée de l'atteinte du haut niveau de disponibilité ou de fiabilité peut ne pas être réalisable ou rentable. Il est nécessaire que l'acquéreur identifie clairement à la fois des objectifs de haute disponibilité et de haute fiabilité pour lesquels la preuve ne peut pas être apportée, mais qu'il définisse également des exigences démontrables pour lesquelles la preuve peut être apportée.

4.2.4 Assurance de la satisfaction aux exigences

Toute spécification comporte deux éléments: les exigences de sûreté de fonctionnement et les moyens par lesquels le fournisseur doit démontrer ou assurer à l'acquéreur la satisfaction aux exigences. Cette disposition signifie que le fournisseur doit fournir à l'acquéreur la preuve suffisante de la conformité de l'entité aux exigences applicables, afin d'apporter à celui-ci la confiance nécessaire pour le paiement du prix convenu. L'IEC 60300-3-1 [2], l'IEC 60300-3-10 [3], l'IEC 60300-3-14 [4], l'IEC 60706-3 [10] et l'IEC 62308 [11] traitent de l'évaluation de la sûreté de fonctionnement pour la fiabilité, la maintenabilité (et la maintenance) et la supportabilité (et le support). L'IEC 61070 [12] traite du mesurage de la disponibilité et de l'assurance.

Le choix des activités d'assurance à spécifier dans un contrat dépend du niveau de risque du projet que l'acquéreur est prêt à accepter. L'acquéreur peut accepter de prendre le risque que l'entité puisse être défaillante, si le fournisseur en assure la maintenance. Dans ce cas, il peut être préférable d'assurer la disponibilité globale de l'entité en appliquant des pénalités pour performances insuffisantes et d'incitations au dépassement des exigences, plutôt que d'assurer la fiabilité de l'entité en tant que telle. Si, toutefois, l'acquéreur n'accepte pas le risque d'indisponibilité de l'entité, alors des essais de démonstration formelle de la fiabilité ou de la disponibilité peuvent être nécessaires. Étant donné que les essais permettent rarement de démontrer la non-occurrence d'événements très peu fréquents, il peut alors être nécessaire que le processus d'assurance repose sur un argument parfaitement étayé. Une étude de sûreté de fonctionnement (voir l'IEC 62741 [13]) fournit une méthode de présentation de ce type d'argument.

En général, les preuves exigées afin d'assurer la conformité aux exigences des entités de plus haute fiabilité sont plus coûteuses, car elles exigent des essais plus poussés pour obtenir la confiance exigée. Cette preuve représente un facteur du coût plus élevé des entités de plus haute fiabilité, mais, sans ces activités, le fournisseur fournit à l'acquéreur une confiance limitée dans la satisfaction aux exigences de l'entité.

4.2.5 Implications en matière de coût

Toutes les entités présentent un certain niveau de fiabilité, quelle que soit la fréquence de défaillance ou quel que soit le niveau exigé de maintenance. À tout moment, il convient de rechercher un équilibre entre le coût, le risque et la performance des entités. Cela inclut tout compromis potentiel entre le coût de la conception et de la garantie d'une sûreté de fonctionnement élevée et le coût et les autres risques résultant d'une sûreté de fonctionnement moindre pendant toute la durée de vie de l'entité. La nature de la fonction de l'entité, les risques associés (performance, coût, sécurité, environnement et réputation) et d'autres facteurs contextuels déterminent ces compromis. Un investissement en matière de conception et la mise en œuvre de la sûreté de fonctionnement peut donc être payant par rapport aux coûts combinés de développement, de réalisation et d'exploitation de l'entité. L'IEC 60300-3-3 [14] décrit l'évaluation du coût du cycle de vie et la relation entre la sûreté de fonctionnement et le coût. Afin d'atteindre le point minimal du coût du cycle de vie de l'entité, il convient que l'organisation qui le produit gère activement la sûreté de fonctionnement; dans le cas contraire, le niveau de fiabilité atteint par l'entité est généralement bien inférieur au niveau exigé au point minimal du coût, ce qui entraîne des retards de projet, des surcoûts et de faibles niveaux de disponibilité.

4.2.6 Gestion de la sûreté de fonctionnement

Il est essentiel d'exercer une gestion active de la sûreté de fonctionnement tout au long du cycle de vie du système, aussi bien au cours du processus d'approvisionnement que pendant l'utilisation, les activités de gestion étant différentes pour chaque cas. La gestion de la sûreté de fonctionnement fournit une approche systématique qui permet de traiter la sûreté de fonctionnement en se concentrant sur les besoins des parties prenantes en optimisant la sûreté de fonctionnement afin d'améliorer les objectifs organisationnels et les retours sur investissement.

Le présent document traite de la spécification de la sûreté de fonctionnement en établissant des exigences applicables à un ou à plusieurs attributs de ladite sûreté. Ces attributs sont des caractéristiques de l'entité qui peuvent être assurées. Cependant, d'autres facteurs peuvent réduire significativement les niveaux obtenus pour ces attributs en dessous de leur niveau intrinsèque de conception. Les facteurs les plus significatifs sont potentiellement la qualité de fabrication et la maintenance de l'entité qui peuvent entraîner de nouvelles pannes dans l'entité. Si la sûreté de fonctionnement n'est pas gérée correctement, la probabilité de ne pas satisfaire les exigences de sûreté de fonctionnement est plus élevée.

L'IEC 60300-1 [1] fournit des recommandations sur la gestion de la sûreté de fonctionnement des systèmes, produits et services impliquant des aspects matériels, logiciels et humains. Elle fournit des recommandations sur la planification et la mise en œuvre d'un programme d'activités et de tâches de sûreté de fonctionnement tout au long du cycle de vie, ainsi que sur la responsabilité et l'assurance.

4.2.7 Vie utile prévue

La durée pendant laquelle une entité est capable de satisfaire aux exigences relatives aux utilisateurs et aux organismes est un aspect important de la sûreté de fonctionnement. Les performances, l'obsolescence ou les aspects économiques peuvent entrer en ligne de compte dans la détermination de la vie utile (voir l'Annexe A). La vie utile dépend également du fait que l'entité soit une entité réparable ou une entité non réparable.

La détermination de la vie utile peut faire partie intégrante d'une spécification de la sûreté de fonctionnement. Une bonne compréhension de la vie utile des entités peut faciliter la détermination de l'entité à acquérir pour répondre au mieux à une application donnée. Dans certains cas, une directive légale applicable à certains marchés peut également exiger de déterminer la vie utile prévue. Il est important de connaître la vie utile d'une entité afin d'estimer le coût de son cycle de vie (IEC 60300-3-3 [14]).

4.3 Avantages

Les avantages de la spécification de la sûreté de fonctionnement sont les suivants:

- pour le fournisseur:
  - possibilité de déterminer des compromis entre la fiabilité, la maintenabilité et la supportabilité lors de la conception et de l'acquisition des entités;
  - justification effective du caractère applicable, réalisable et assurable des exigences de sûreté de fonctionnement.
- pour l'acquéreur:
  - définition, documentation et apport de preuves fondées sur des données et une évaluation, qui conviennent de la satisfaction aux besoins et attentes des parties prenantes en matière de performances de sûreté de fonctionnement;
  - gestion des variations des besoins et attentes des parties prenantes, y compris les modifications des exigences elles-mêmes.
- pour les deux:
  - meilleure appréhension des exigences de sûreté de fonctionnement;
  - vérification et validation effective des exigences contractuelles;
  - assurance pour les autorités de réglementation que toutes les exigences réglementaires relatives à la sûreté de fonctionnement sont prises en compte et satisfaites.

5 Déduction des exigences de sûreté de fonctionnement

5.1 Généralités

Il convient dans toute la mesure du possible d'exprimer quantitativement toutes les exigences de fiabilité, de maintenabilité, de supportabilité et de disponibilité, mais il peut être aussi pertinent de définir des exigences qualitatives dans la spécification. Les exigences quantitatives ne sont pertinentes que quand les exigences spécifiées peuvent être mesurées ou calculées pendant le processus d'assurance.

Étant donné que les entités et leur utilisation sont très différentes selon les organismes, il n'est pas possible de produire une approche normalisée qui exprime le processus de développement de normes de sûreté de fonctionnement. En revanche, l'Article 5 définit un processus de haut niveau qui permet de déterminer quelles informations sont exigées, quelles décisions peuvent être prises et quel peut être le résultat du processus décisionnel. Il n'est également pas possible de fournir un ensemble exhaustif de décisions qui ont une influence sur le développement des exigences de sûreté de fonctionnement pour toutes les situations. Ainsi, il convient que l'utilisateur du présent document adapte l'approche décrite à sa situation. Il convient que les utilisateurs prennent particulièrement en considération ce qui relève de leur contrôle dans la prise de décisions lors de l'application du processus décrit.

La Figure 1 décrit l'approche de développement des exigences de sûreté de fonctionnement.

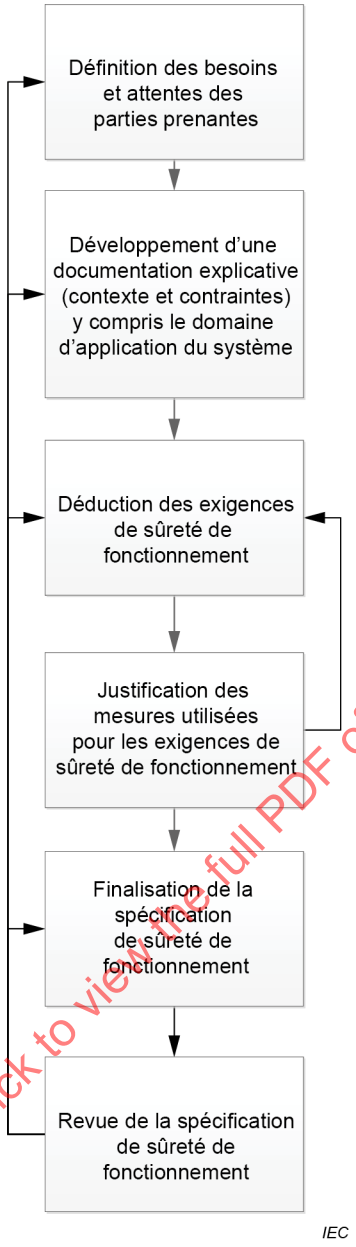

Figure 1 – Processus de haut niveau qui permet de déduire les exigences de sûreté de fonctionnement dans la spécification

L'étape 1 consiste à examiner et à documenter les besoins et attentes des parties prenantes. Cette étape établit une compréhension commune des besoins et attentes des parties prenantes en matière de sûreté de fonctionnement. Cette étape d'analyse, qui peut prendre la forme d'un échange direct ou d'un atelier dirigé, détermine en quoi la performance de sûreté de fonctionnement est importante pour les parties prenantes et documente ce que ces dernières "doivent" avoir et ce qu'elles "souhaitent" avoir, c'est-à-dire leurs exigences et objectifs de sûreté de fonctionnement. Voir 5.2 pour de plus amples informations.

L'étape 2 consiste à développer une documentation explicative qui détaille le contexte et les contraintes dans le cadre desquels les exigences doivent être satisfaites. Il ne suffit pas de spécifier les exigences relatives aux attributs de sûreté de fonctionnement pour définir les performances exigées en matière de sûreté de fonctionnement. Il convient de développer une documentation explicative afin de fournir le contexte d'établissement des exigences. Par ailleurs, il convient que la spécification de sûreté de fonctionnement contienne ou fasse référence à ces documents. Le paragraphe 5.3 décrit cette étape de manière plus détaillée.

L'étape 3 consiste à déduire les exigences de sûreté de fonctionnement. La première partie de cette étape consiste à déterminer quel attribut est le plus important parmi les attributs de sûreté de fonctionnement, c'est-à-dire la fiabilité, la maintenabilité, la supportabilité ou la disponibilité, et quel attribut il convient par conséquent de définir en premier. Suivant la définition de l'attribut primaire, il convient de déterminer l'attribut ou les attributs secondaires éventuels le cas échéant. Cette détermination s'effectue non seulement par des considérations techniques, mais également par les priorités et les valeurs commerciales de l'organisme. L'Annexe B fournit un exemple de méthode de priorisation des attributs. Les attributs spécifiés ultérieurs doivent être conformes aux attributs primaires et secondaires sélectionnés.

Il convient, par un processus d'échange et d'analyse, d'affiner les exigences de sûreté de fonctionnement, de déduire les attributs associés et de déterminer les critères d'assurance (voir 5.4.4). Après détermination de l'attribut ou des attributs les plus importants, il est nécessaire de déterminer la manière dont est ou sont définis ces attributs (voir les paragraphes 5.4.7 à 5.4.10), de même qu'il est nécessaire de rédiger l'exigence, y compris la détermination des mesures de performance pertinentes. Il convient d'éviter les doubles spécifications telles que l'intensité de défaillance et la moyenne des temps de bon fonctionnement (MTBF) ou la probabilité de défaillance et la vie utile, car ces facteurs peuvent entraîner des incohérences. Il convient que la déduction des attributs prenne en considération les processus décisionnels décrits en 5.4. Les exigences peuvent également inclure des attributs supplémentaires liés à la sûreté de fonctionnement tels que la durabilité (voir l'IEC 60300-1 [1]) avec un moyen de vérification de leur définition.

L'étape 4 consiste à justifier les mesures de performance des attributs de sûreté de fonctionnement, voir 5.5. Il convient de justifier les mesures de performance internes aux exigences de sûreté de fonctionnement en prenant en considération les besoins et les objectifs des parties prenantes et par justification des mesures. Il convient que la justification des mesures de performance assure leur caractère rationnel et réaliste, de même qu'elles peuvent être démontrées dans le cadre des contraintes budgétaires, opérationnelles et temporelles du projet. Les méthodes qui peuvent être utilisées pour justifier les mesures de performance incluent la modélisation, la comparaison avec les données d'exploitation et l'expérience acquise par les parties prenantes.

L'étape 5 consiste à finaliser la spécification de sûreté de fonctionnement qui intègre les exigences de sûreté de fonctionnement et la documentation explicative dans un document unique.

L'étape 6 consiste à examiner la cohérence et l'applicabilité de la spécification de sûreté de fonctionnement. Il s'agit d'une étape très importante étant donné que les décisions prises lors des étapes précédentes peuvent avoir une influence sur les exigences de sûreté de fonctionnement. Le cas échéant, la spécification de sûreté de fonctionnement est examinée par des fournisseurs potentiels et ainsi peut exiger une mise à jour du fait de cet examen. Cette opération peut inclure la modification des besoins et attentes des parties prenantes, par exemple s'il a été démontré qu'il est impossible de déduire les exigences qui satisfont à ces besoins et attentes.

A chaque étape, il peut s'avérer nécessaire de revenir à une étape antérieure du processus si les exigences sont considérées comme incohérentes, inapplicables, voire irréalisables.

5.2 Définition des besoins et attentes des parties prenantes

Pour définir les besoins et attentes des parties prenantes, il peut être utile de les exprimer tout d'abord en des termes simples, en ce qui concerne ce que les parties prenantes essaient d'obtenir, voir la Figure 2. Lors de leur réflexion sur la performance, il convient également que les parties prenantes déterminent quel niveau de risque que la performance exigée ne soit pas satisfaite elles peuvent accepter, s'il existe un niveau de performance minimal qui doit être obtenu, et quelle somme elles souhaitent dépenser pour réduire le risque de non-satisfaction de la performance exigée.

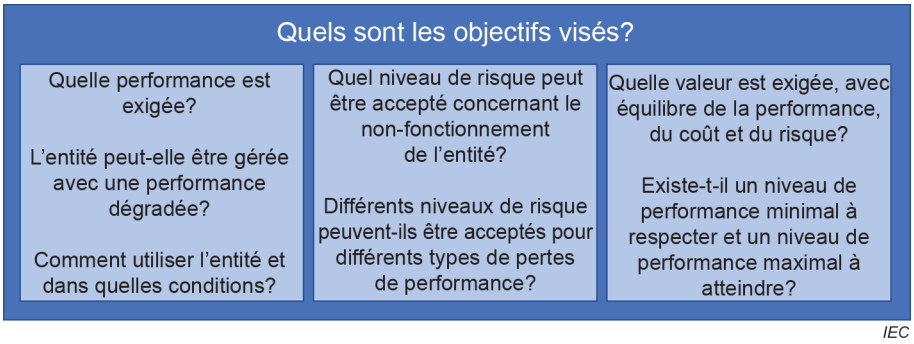

Figure 2 – Quels sont les objectifs visés?

La non-réalisation des exigences dérivées peut s'avérer onéreuse; par conséquent, il est important lors de l'analyse de vérifier par essai le caractère applicable des besoins exprimés. Les parties prenantes peuvent avoir des besoins différents, auquel cas les exigences dérivées doivent être comparées, par exemple, en prenant en considération la sûreté de fonctionnement du produit ou du service, de l'optimisation des ressources (tout au long du cycle de vie) et de la sûreté de fonctionnement du service client.

Les besoins et les attentes des parties prenantes sont différents des exigences propres à l'entité qui constituent les exigences techniques de la conception (voir l'étape 4 du processus).

5.3 Développement d'une documentation explicative

Si une spécification de sûreté de fonctionnement doit servir de base d'établissement d'un contrat, il est essentiel de pleinement définir la sûreté de fonctionnement de l'entité afin d'éviter tout désaccord après mise en application du contrat. L'Annexe C fournit un exemple de documentation explicative pour la spécification d'un système de sécurité d'habitation individuelle.

Exemples d'éléments qu'il convient d'inclure dans la documentation explicative:

- une description de l'entité pour laquelle les exigences de sûreté de fonctionnement sont produites, y compris la capacité ou les fonctions fournies, les limites de l'équipement et/ou l'entité;
- les conditions d'installation, d'utilisation et de support de l'entité;
- les critères précis et clairement définis avec lesquels les attributs de sûreté de fonctionnement choisis doivent être démontrés ou assurés (voir 5.4.4).

Il convient de fournir les éléments suivants dans la description de l'entité:

- l'identification de l'entité, y compris son nom, le local d'utilisation ou d'exploitation et l'objet principal d'application;
- l'objectif opérationnel que doit atteindre l'entité;
- les fonctions clés nécessaires à la réalisation des performances exigées;

  (Il convient d'indiquer l'objet de chaque fonction du point de vue des exigences d'un système. Le cas échéant, il convient d'établir les relations de ces fonctions.)
- les critères de réussite ou de défaillance sur lesquels sont fondées les exigences de sûreté de fonctionnement pour chaque fonction, par exemple la défaillance totale de l'entité, la perte de fonctions essentielles, une défaillance partielle ou une dégradation de la performance d'une fonction;
- les facteurs qui ont une influence sur chaque fonction et leur effet sur les performances de l'entité;

  (L'Annexe D fournit des recommandations relatives aux contraintes types et aux facteurs d'influence clés.)

- l'approche technique adoptée pour l'acquisition et le maintien des fonctions nécessaires pour maintenir le fonctionnement dans les contraintes de coût et de délai.

La description de l'utilisation et du support de l'entité comprend:

- les aspects matériels, logiciels et humains du fonctionnement de l'entité, y compris les exigences de qualification et les responsabilités du personnel en charge du fonctionnement et de la maintenance du matériel, du logiciel et de la documentation;
- les différentes conditions d'exploitation et environnementales dans lesquelles l'entité est utilisée, y compris le cas échéant, la durée relative dans chaque condition;
- les aspects des conditions d'exploitation et environnementales qu'il peut être nécessaire de prendre en considération, ainsi que tout élément du reste du système qui peut avoir une influence sur le comportement de l'entité ou être influencé par elle;

  (Ces aspects peuvent inclure l'environnement physique, l'environnement psychosocial de l'organisme ou l'environnement général plus large.)
- le ou les profils d'utilisation qui servent à mesurer les exigences de sûreté de fonctionnement, qu'il convient de développer avec une attention toute particulière accordée au mode d'exploitation, d'utilisation, de maintenance et de stockage de l'entité;
- les informations relatives à la supportabilité y compris la maintenance et les ressources de soutien disponibles ou exigées comme le niveau et l'effectif du personnel de maintenance qualifié, les pièces de rechange, les installations de maintenance, la surveillance des conditions, les techniques d'inspection et d'essai employées, ainsi que l'équipement de travail;
- la politique de maintenance à appliquer et les procédures et dispositions de support associées;
- les sources de données acceptables à utiliser avec les techniques d'analyse, quelles qu'elles soient.

Une spécification qui fait partie d'un contrat peut également inclure:

- les obligations, les responsabilités et les redevabilités de l'acquéreur, du fournisseur et des tierces parties éventuelles;
- les méthodes prévues pour l'assurance de la conformité aux exigences, y compris les critères d'acceptation/de rejet.

5.4 Déduction des exigences de sûreté de fonctionnement

5.4.1 Généralités

L'étape du processus qui consiste à définir les exigences de sûreté de fonctionnement comporte de nombreuses sous-étapes.

- La première sous-étape consiste à prendre en considération les différents scénarii qui peuvent utiliser ou fournir l'entité, voir 5.4.2.
- La deuxième sous-étape consiste à décider du niveau de risque acceptable, à déterminer s'il existe différents aspects de performance qu'il est particulièrement nécessaire de gérer, et si les ressources disponibles sont soumises à des contraintes éventuelles, dans la mesure où celles-ci peuvent avoir une influence sur l'attribut de sûreté de fonctionnement exigé, voir 5.4.3.
- La troisième sous-étape consiste à prendre en considération l'assurance exigée étant donné que ce facteur a une influence sur le mode de spécification de la sûreté de fonctionnement, voir 5.4.4.
- La quatrième sous-étape consiste à déterminer s'il convient de définir les exigences au niveau de l'entité, de la sous-entité ou du composant, voir 5.4.5.
- La cinquième sous-étape consiste à équilibrer le résultat de ces processus décisionnels et de définir la priorité des attributs de sûreté de fonctionnement, voir 5.4.6.

- La sixième sous-étape consiste à définir chaque attribut, après avoir décidé des attributs de sûreté de fonctionnement à spécifier, voir 5.4.7 à 5.4.10, qui examine les décisions probables et les types de mesures pour chacun des attributs de sûreté de fonctionnement.

5.4.2 Scénarii de spécification

5.4.2.1 Généralités

Il existe différents scénarii à appliquer concernant le niveau selon lequel les attributs de sûreté de fonctionnement doivent être intégrés dans une spécification (voir 5.4.2.2 à 5.4.2.5).

Les entités personnalisées sont celles pour lesquelles l'acquéreur spécifie les exigences et le fournisseur conçoit, développe et produit une entité uniquement pour satisfaire à cette spécification. Si, toutefois, le fournisseur établit quelles entités sont disponibles et que l'acquéreur choisit l'entité qui satisfait le mieux aux exigences, cette entité est appelée "produit du commerce", "matériel disponible dans le commerce" ou "OTS". Dans ce cas, l'entité normalisée disponible dans le commerce ne fait l'objet d'aucune modification. En pratique, la majorité des fournitures majeures sont une combinaison d'éléments et de composants personnalisés et disponibles dans le commerce et la spécification fait l'objet d'un accord mutuel entre l'acquéreur et le fournisseur.

Lorsque l'entité est une entité non réparable, sa durée de vie totale et parfois son remplacement constituent des facteurs de préoccupation essentiels. Lorsque l'entité est une entité réparable, la maintenabilité et la supportabilité doivent également être prises en considération. Ces facteurs peuvent être proposés par le fournisseur, mais peuvent également l'être par des fournisseurs indépendants, la logistique étant prise en considération dans certains cas. La disponibilité qui en résulte est un facteur important. La conception de l'entité implique vraisemblablement la nécessité pour le constructeur de spécifier et de choisir des composants et des entités industrielles afin de satisfaire aux exigences de ceux qui assurent la maintenance et le soutien.

NOTE La différenciation des scénarii s'applique de manière égale aux matériels, aux logiciels et à leurs combinaisons. Dans le cas des logiciels, le terme "réparable" se rapporte à un degré d'assistance à la clientèle, par exemple, existence de clauses de contrats de licences ou de communautés actives de développeurs par lesquelles les fournisseurs et les développeurs répondent aux rapports transmis par les utilisateurs, découverte des failles de sécurité informatique, etc., par une application en temps utile de retouches et de mises à niveau.

5.4.2.2 Scénarii de spécification pour les entités OTS incorporés dans des entités plus importantes

Les entités OTS de grande consommation, telles que les ordinateurs portables et les imprimantes, et les entités OTS industrielles, telles que les moteurs et les pompes électriques, peuvent être achetées dans le cadre d'une transaction commerciale interentreprises (B2B) et utilisées comme composants d'ensembles ou de sous-ensembles, incorporés dans des entités plus grandes. Elles sont fournies potentiellement à des parties intermédiaires sans implication directe des utilisateurs finaux ou des opérateurs.

La spécification la plus simple est destinée aux entités simples non réparables avec un niveau de fonction faible. La fiabilité est le principal attribut de préoccupation dont la durée de vie est spécifiée pour les composants qui ont une durée de vie opérationnelle limitée. La difficulté relative à la spécification de telles entités consiste à décrire les conditions d'utilisation (la zone d'exploitation sûre) de manière à couvrir toutes les applications et conditions d'utilisation pertinentes.

Un type de spécification plus complexe est destiné aux entités industrielles réparables. Ce type d'entité peut aller d'une entité relativement simple telle qu'une vanne de canalisation ou une carte électronique, à une entité bien plus complexe telle qu'un moteur électrique ou un moteur à combustion interne conçu pour de nombreuses applications différentes. Étant donné qu'il s'agit d'une entité réparable, la fiabilité tout comme la maintenabilité et la supportabilité sont des attributs importants à prendre en considération. Le fournisseur de ces entités n'a pas nécessairement une compréhension complète de l'application finale et de l'environnement d'exploitation. Il peut s'avérer nécessaire que la spécification de fiabilité couvre plusieurs

fonctions qui peuvent être défaillantes selon des taux de défaillance différents. La prise en considération de la maintenabilité peut ne pas être exhaustive étant donné que l'environnement d'utilisation et les détails de l'installation peuvent être incertains et varier. De même, l'estimation des spécificités de la maintenance et du support attendu ne peut être effectuée qu'avec des exigences, des procédures et des ressources de maintenance génériques. L'emplacement de l'entité, qui peut être fixe ou mobile, peut être un facteur non identifié par rapport à la logistique exigée pour fournir le support recommandé. L'acquéreur peut devoir ajuster le support nécessaire, après détermination de son application réelle.

5.4.2.3 Scénario de spécification pour les entités OTS destinées à un utilisateur final

Un acquéreur peut souhaiter spécifier une entité généralement disponible et fabriquée pour être vendue directement à de nombreux utilisateurs, qui ne sont toutefois pas identifiés de manière spécifique, par exemple un véhicule personnel, un avion commercial, une machine à laver domestique, un téléphone mobile et un ordinateur portable. Dans ce cas, la spécification est produite par l'acquéreur afin de permettre un choix entre les entités disponibles. Il est également possible que le fournisseur produise la spécification et que l'acquéreur décide si celle-ci satisfait suffisamment à ses besoins et attentes.

Pour une entité OTS destinée à un utilisateur final, le fournisseur établit ce qui est disponible et peut fournir une preuve classique de satisfaction de l'entité à certains niveaux de sûreté de fonctionnement, ce qui peut inclure des données d'exploitation d'applications antérieures. Cependant, la possibilité d'une assurance est limitée et de nombreux fournisseurs ne veulent pas fournir des données d'exploitation considérées comme sensibles du point de vue commercial.

L'objectif de cet approvisionnement OTS est de réduire ou de supprimer la nécessité d'un développement, de sorte que les capacités souhaitées peuvent être fournies plus rapidement et à un coût réduit. Une des difficultés de l'approvisionnement OTS réside dans le fait que les entités OTS satisfont rarement à toutes les exigences définies et que différentes entités OTS présentent des caractéristiques et des capacités différentes tout en ne satisfaisant pas exactement aux exigences. Par conséquent, il convient de définir les exigences de sûreté de fonctionnement de manière à assurer que l'entité OTS satisfait au besoin spécifique, tout en permettant la proposition de compromis fondés sur ce qui peut être obtenu de manière réaliste, et afin de prendre en considération toutes les solutions potentielles. Il est essentiel que la définition d'exigences de sûreté de fonctionnement inappropriées n'appelle pas inutilement des modifications de conception. Il est également nécessaire de reconnaître que les entités OTS atteignent le niveau de sûreté de fonctionnement spécifié par le fournisseur uniquement lorsqu'elles sont utilisées selon leur conception. Par conséquent, la performance obtenue est différente (et peut ne pas être connue) si l'utilisation est différente.

Si l'acquéreur exige des modifications, quelles qu'elles soient, de l'entité OTS, cette entité ne plus être considérée comme une entité OTS puisque les modifications peuvent avoir des effets significatifs sur la sûreté de fonctionnement obtenue. L'acquéreur doit donc assurer qu'une entité OTS est véritablement identique à l'entité disponible dans le commerce et que la preuve fournie est pertinente. Si des modifications, quelles qu'elles soient, sont demandées, les effets de ces modifications sur la sûreté de fonctionnement doivent être étudiés en détail et une assurance complémentaire doit être demandée et réglée par l'acquéreur, si cela est nécessaire.

5.4.2.4 Scénario de spécification pour les entités personnalisées destinées à un utilisateur final

Un acquéreur peut souhaiter spécifier une entité provenant d'un constructeur afin de satisfaire à ses exigences spécifiques uniques, comme du matériel militaire ou une centrale nucléaire. La disponibilité constitue l'objectif principal de l'acquéreur. Il est important de prendre en considération la fiabilité et la maintenabilité lors de la conception. Les exigences de maintenance, ainsi que la supportabilité et la disponibilité qui en résulte sont établies et spécifiées avec des compromis entre ces attributs et le coût, le risque et les performances. La configuration finale peut une nouvelle fois impliquer la spécification et le choix d'entités OTS qui satisfont aux exigences minimales comme partie intégrante de l'entité finale.

Pour une entité personnalisée destinée à un utilisateur final, l'acquéreur et le fournisseur doivent convenir du niveau d'assurance que ce dernier doit proposer pour démontrer que les exigences ont été satisfaites. Cette assurance inclut des preuves d'essai et d'analyse, mais comme l'entité est construite uniquement pour l'acquéreur, elle ne peut pas comporter la preuve d'une utilisation de l'entité dans son environnement d'exploitation, sauf après l'achat. Le fournisseur inclut alors le coût de ces activités d'assurance dans le prix indiqué de l'entité et l'acquéreur peut déterminer la preuve exigée conformément aux risques commerciaux acceptables. Cependant, l'acquéreur sait que l'entité est conçue et développée afin de satisfaire aux exigences.

5.4.2.5 Scénario de spécification pour une solution totale pour les entités destinées à un utilisateur final

Un acquéreur peut souhaiter qu'un fournisseur propose une solution totale pour la vie utile l'entité. La spécification consiste en une exigence fondée sur les performances comprenant la disponibilité, ou en un niveau de service approprié qui constitue l'attribut primaire de sûreté de fonctionnement. Le constructeur ou le fournisseur est chargé d'établir les attributs contributifs de fiabilité, de maintenabilité et de supportabilité avec les compromis applicables afin de satisfaire à cette exigence de disponibilité. La solution totale assure tout le soutien nécessaire pendant la durée d'utilisation convenue dans un contrat.

5.4.3 Attributs de sûreté de fonctionnement à spécifier

Le paragraphe 5.4.2 décrit la façon dont les différents types d'entités et leur mode de spécification peuvent produire différents attributs de sûreté de fonctionnement considérés comme les attributs les plus importants. Le présent paragraphe 5.4.3 décrit les différents aspects de performance qui peuvent avoir une influence sur cette décision et qu'il convient de prendre en considération séparément des décisions mentionnées en 5.4.2.

Prendre d'abord en considération les questions représentées à la Figure 3. Ces questions prises en considération, il est alors nécessaire de prendre en considération les contraintes éventuelles qui s'exercent (voir la Figure 4), particulièrement sur les ressources disponibles pour la maintenance et la restauration de l'entité après une défaillance, étant donné que ces contraintes contribuent à renforcer plus que d'habitude l'importance de la maintenabilité ou de la supportabilité.

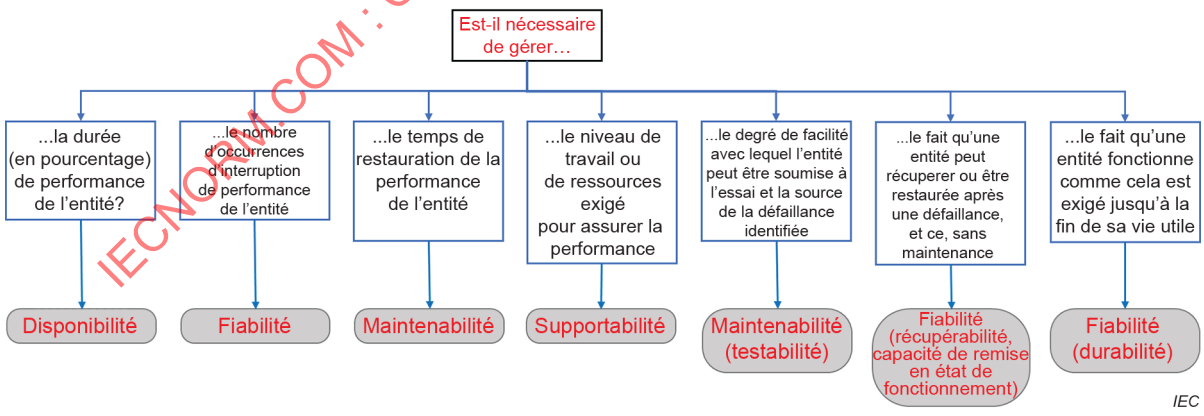

Figure 3 – Quels sont les facteurs dont la gestion est nécessaire?

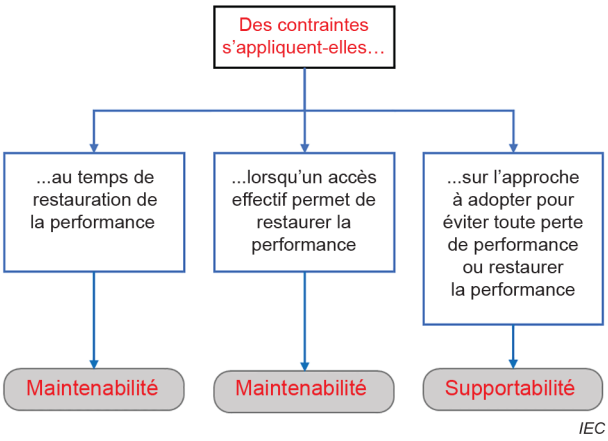

Figure 4 – Quelles sont les contraintes existantes?

5.4.4 Preuve et assurance effectives des attributs de sûreté de fonctionnement

Enfin, il est nécessaire de déterminer si la satisfaction des exigences de sûreté de fonctionnement peut être démontrée, voir la Figure 5. Comme cela est décrit précédemment, la satisfaction aux exigences doit pouvoir être démontrée. Ainsi, il peut être nécessaire de transformer la mesure de sûreté de fonctionnement choisie par rapport à celle soulignée par les décisions décrites en 5.4.2 et 5.4.3 en une mesure qui peut être démontrée de manière rentable et en temps utile.

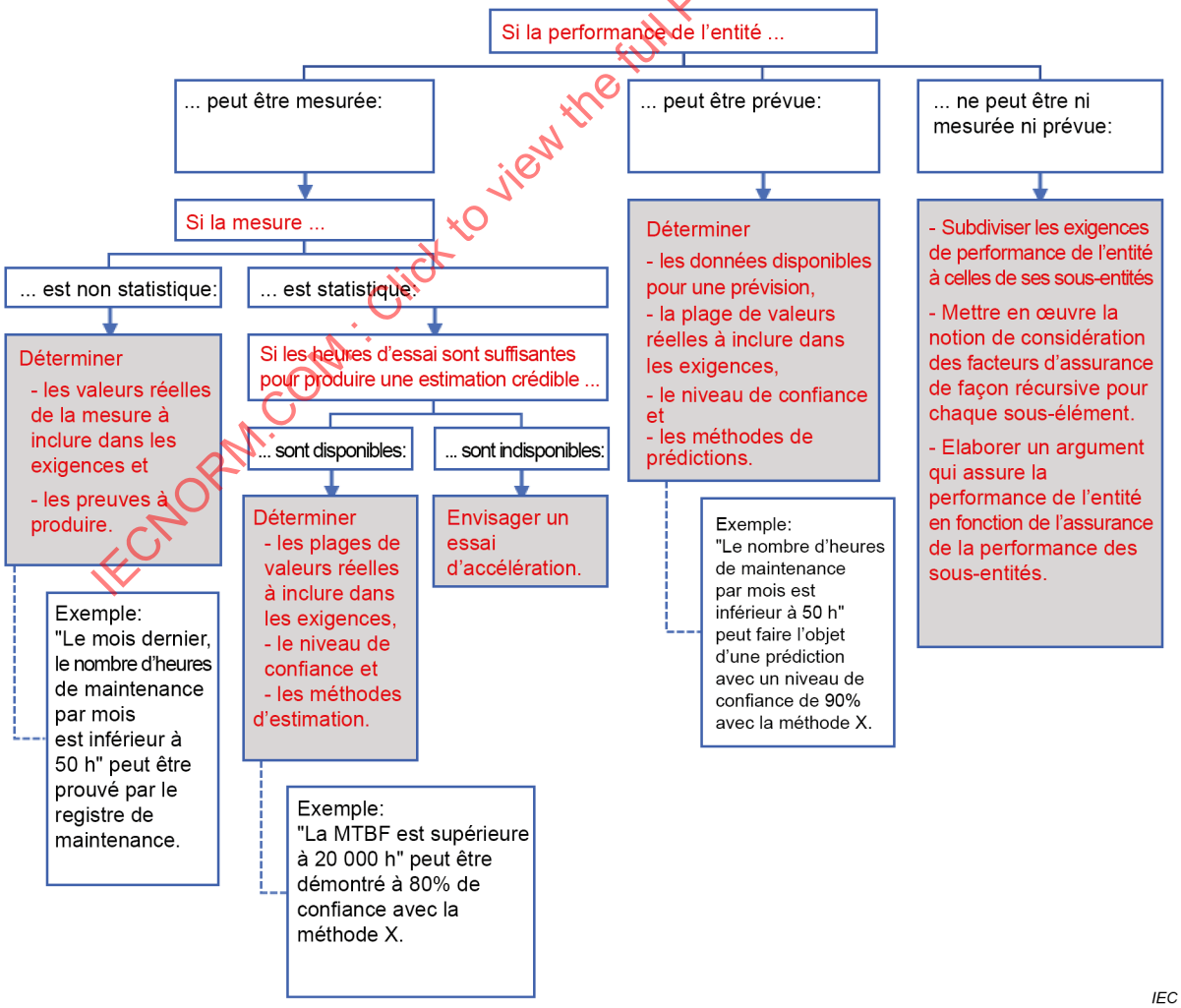

Figure 5 – Facteurs d'assurance pris en considération

La vérification et la validation constituent les deux principaux éléments de la démonstration et de l'assurance. Ces éléments sont définis dans l'ISO 9000 [15] et utilisés tant dans l'industrie du matériel que dans l'industrie du logiciel comme partie du processus de développement du logiciel (voir l'IEC 61508 (toutes les parties) [6]) et peuvent être expliqués comme suit. La vérification est le processus de fourniture de la preuve que l'entité au stade actuel satisfait aux exigences du stade actuel ainsi qu'à celles du ou des précédents stades de son cycle de vie (c'est-à-dire est-ce que la fabrication des entités est correcte?). La validation est le processus de fourniture de la preuve que l'entité satisfait aux besoins et aux attentes réels des parties prenantes, qui peuvent ne pas toujours être reflétés dans la spécification produite (c'est-à-dire les entités fabriquées sont-elles les bonnes?). Vérification et validation sont des éléments essentiels.

Le niveau d'assurance exigé par l'acquéreur dépend de la confiance qu'il a dans la faculté de l'entité à atteindre les niveaux de sûreté de fonctionnement spécifiés. Si l'acquéreur souhaite assurer la maintenance d'une entité défaillante en cours d'utilisation, alors un niveau plus faible de preuve et donc de confiance dans l'atteinte de la sûreté de fonctionnement peut être acceptable. Cette situation résulte du fait que la fourniture de preuve requiert du temps, a un coût et que l'acquéreur peut accepter de prendre le risque que le niveau de fonctionnement de l'entité ne soit pas celui exigé. L'acquéreur doit prendre une décision équilibrée concernant les risques acceptables lors de la spécification des exigences d'assurance.

Il convient que le fournisseur indique l'activité d'assurance qu'il convient de réaliser comme partie intégrante de la spécification et obtienne l'accord de l'acquéreur, souvent par le biais du contrat. Dans sa définition des exigences de sûreté de fonctionnement, il convient que l'acquéreur prenne en considération les différents facteurs susceptibles d'avoir une influence sur le coût de l'assurance de la sûreté de fonctionnement. Ces facteurs incluent la durée de vie prévue, ainsi que le retrait ou le recyclage de l'entité.

Pour un approvisionnement de longue durée, les activités peuvent être planifiées de nombreuses années avant leur exécution. Selon les modalités contractuelles, l'acquéreur ne peut par conséquent avoir qu'un contrôle limité sur ces activités au cours du projet. L'assurance progressive peut constituer une méthode de réduction du risque inhérent au projet, tant pour l'acquéreur que pour le fournisseur, dans la mesure où l'entité ne fournit pas le niveau de preuve exigé. Cette disposition signifie que les activités sont planifiées tout au long du cycle de vie et que les résultats sont fournis à l'acquéreur à des étapes importantes du projet. De cette façon, l'acquéreur établit la confiance dans l'entité tout au long du projet et le risque d'un niveau de confiance inadéquat est ainsi nettement réduit.

L'étude de sûreté de fonctionnement constitue un modèle qui peut être utilisé par le fournisseur pour apporter à l'acquéreur la preuve que l'entité a satisfait à ses exigences. L'étude de sûreté de fonctionnement fournit une argumentation rationnelle auditable portant sur le fait que l'entité satisfait ou a satisfait à ses exigences, ce statut étant synthétisé à des étapes importantes du projet dans le rapport d'étude de sûreté de fonctionnement. L'étude de sûreté de fonctionnement sert généralement de preuve progressive et est publiée à de nombreuses étapes importantes du projet. Cette preuve peut consister à démontrer la maîtrise effective des risques d'une non-satisfaction de la revendication de sûreté de fonctionnement. L'IEC 62741 [13] fournit des recommandations relatives à l'étude de sûreté de fonctionnement.

Lorsque l'acquéreur exige que l'assurance soit produite, le fournisseur doit déterminer l'objet de l'activité et sa contribution à l'assurance. Par exemple, il convient qu'une spécification ne fasse pas référence à une technique spécifique, telle qu'une analyse par arbre de panne (AAP), mais qu'elle spécifie en revanche une analyse pour déterminer les combinaisons d'événements qui peuvent conduire à une défaillance de l'entité, dans la mesure où un bloc-diagramme de fiabilité (BDF) peut être une technique également valide pour atteindre le même objectif. Il convient de laisser le choix de la technique pour mener à terme une activité à la discrétion du fournisseur, mais en prenant en considération les facteurs tels que l'expérience de l'analyste, le temps disponible et les exigences d'information et de documentation. Par exemple, un BDF réalisé par un analyste expérimenté est préférable à une AAP mal menée par un analyste inexpérimenté.

Les activités d'assurance comprennent:

- analyse:
  1) conformité aux normes, réglementations et lignes directrices;
  2) revue d'expert, meilleures pratiques et certification;
  3) calculs utilisés principalement pour d'autres conceptions (par exemple, des analyses par éléments finis pour les contraintes, la fatigue);
  4) simulation (par exemple, des performances de l'entité);
  5) analyse de la sûreté de fonctionnement (voir l'IEC 60300-3-1 [2]).
- essais et démonstration:
  1) performance dans des utilisations précédentes, pour des entités identiques ou similaires dans des applications identiques ou similaires;
  2) essais de sûreté de fonctionnement dédiés, comprenant:
     i) des essais de démonstration de fiabilité, par exemple des essais à durée fixée ou nombre de défaillances fixé, essais séquentiels, essais à proportion de succès, essais accélérés, ou essais de durée de vie;
     ii) essais de démonstration de disponibilité;
     iii) essais de démonstration de maintenabilité.
  3) autres essais de développement (par exemple, de performance, de durée de vie, d'endurance à la fatigue, essais de logiciels sur l'entité, essais au niveau des modules ou des composants);
  4) démonstration physique de la fourniture d'une installation ou d'un équipement de support.

Pour de plus amples informations relatives aux techniques d'assurance de la sûreté de fonctionnement, consulter l'IEC 60300-1 [1].

Les activités d'assurance ne sont pas toutes appropriées ou efficaces à tous les stades du cycle de vie. Les essais portant sur l'entité ne peuvent pas être effectués tant que l'entité n'a pas été conçue et qu'un prototype n'a pas été construit. Cependant, il convient de planifier les essais au stade de la conception de sorte que le fournisseur puisse déterminer les essais exigés portant sur les sous-entités avant que l'entité soit construite. De plus, il convient de concevoir l'entité et les sous-entités de manière à pouvoir les soumettre à l'essai (voir l'IEC 60706-5 [16]). De même, les activités d'analyse sont plus appropriées pendant les étapes de conception pour permettre l'exploration des effets des différentes options sur la sûreté de fonctionnement estimée.

Il convient de noter que toute preuve fournie pendant le développement constitue une prédiction de la sûreté de fonctionnement probable et que les résultats de l'analyse sont probablement moins précis que les résultats d'essai. Par conséquent, il convient que l'acquéreur ne se fonde pas uniquement sur des résultats d'analyse et qu'il exige que la preuve de la satisfaction aux exigences repose sur une combinaison d'analyses et d'essais. De plus, l'environnement et l'utilisation de l'entité doivent être pris en considération lors de la planification des essais. Dans les cas pour lesquels l'essai est réalisé dans des conditions proches des conditions d'utilisation, celui-ci fournit une bonne estimation de la sûreté de fonctionnement. Toutefois, pour une entité à haute fiabilité, l'essai peut être un essai de très longue durée, exiger un nombre élevé d'entités d'essai et produire un faible nombre de défaillances, ce qui entraîne une grande incertitude des estimations de sûreté de fonctionnement. Si l'essai est accéléré, la taille de l'échantillon et l'intervalle d'essai peuvent être réduits (voir l'IEC 62506 [17]). Le nombre plus élevé de défaillances réduit l'incertitude statistique, mais l'incertitude technique est plus grande parce que les conditions d'essai accéléré peuvent provoquer des modes de défaillance non pertinents sur le terrain.

5.4.5 Décider du niveau des exigences

La définition de l'entité comprend la prise en considération du niveau interne à l'entité globale auquel les exigences doivent être spécifiées. L'acquéreur peut établir les exigences de sûreté de fonctionnement uniquement au niveau le plus haut de l'entité ou il peut décider qu'il est important que l'une des sous-entités n'ait pas une contribution dominante dans la non-fiabilité résultante, et donc aussi établir des exigences à des niveaux plus bas. Ces exigences de niveau plus bas doivent être cohérentes avec les exigences du niveau plus haut et elles doivent être mesurables (ou démontrables) et réalisables. Par exemple, la contribution de la sous-entité à la sûreté de fonctionnement de l'entité globale doit être estimée avant de pouvoir répartir les exigences entre les sous-entités.

La répartition entre les sous-entités de niveau plus bas n'est pas directe sauf pour les structures relativement simples telles que les entités en série dont toutes les sous-entités ont un taux de défaillance constant. Dans les autres cas tels que les entités redondantes ou lorsque le taux de défaillance varie dans le temps, se reporter aux normes telles que l'IEC 61025 [18], l'IEC 61078 [19], l'IEC 60300-3-1 [2] et l'IEC 61703 [20] pour d'autres recommandations relatives à l'analyse de la sûreté de fonctionnement des entités.

5.4.6 Equilibre des résultats

Toutes les décisions et considérations décrites en 5.4.2, en 5.4.3 et en 5.4.4 peuvent aboutir à ce que le même attribut de sûreté de fonctionnement soit considéré comme le plus important et qu'il constitue l'attribut qu'il convient de spécifier en premier. Il est toutefois possible que les résultats des différentes sous-étapes soient autres. Cette étape consiste à équilibre les résultats des sous-étapes précédentes de manière à déterminer la priorité des attributs de sûreté de fonctionnement afin de constituer la base des exigences.

5.4.7 Exigences de fiabilité

Il convient de choisir les mesures qui permettent de définir les exigences après identification de la fiabilité comme attribut important de la sûreté de fonctionnement. Il convient que l'acquéreur assure la spécification de la ou des mesures de fiabilité appropriées, ainsi que la compréhension des implications statistiques de l'exigence et de leurs conséquences sur le coût, les calendriers du projet et le potentiel de réalisation.

EXEMPLE Une fiabilité de 99 % sur une année peut être spécifiée pour une entité dans la mesure où ce pourcentage semble être une exigence raisonnable. Toutefois, un taux de défaillance constant d'une entité implique un taux de défaillance inférieur à un sur une période de 99 ans, qu'il peut être difficile ou coûteux d'obtenir et/ou démontrer. La nécessité d'une haute fiabilité de cette nature est donc évaluée en tenant compte de ces implications.

La fiabilité, lorsqu'elle est utilisée comme une mesure, est, par définition, la capacité d'une entité à fonctionner comme cela est exigé, sans perte de sa ou de ses fonctions exigées, pendant un intervalle donné et dans des conditions données. La fiabilité est décrite plus correctement par la probabilité que l'entité puisse créer son profil d'utilisation exigé. Toutefois, la fiabilité, dans son acception généralement admise, peut être exprimée ou spécifiée par un grand nombre d'autres mesures comme le temps moyen de fonctionnement avant défaillance, la moyenne des temps de bon fonctionnement (MTBF) ou le taux de défaillance. Dans tous les cas, il convient que l'acquéreur admette que toute mesure de fiabilité ne garantit pas la fiabilité d'une entité unique, car elle représente une expression statistique de ce qui peut être prévu avec un degré de confiance spécifié. De fait, il convient que les exigences d'assurance incluent des techniques d'analyse de données appropriées lorsque la fiabilité quantifiée est spécifiée.

NOTE L'application de la MTBF implique toujours un taux de défaillance constant de l'entité avec la durée ou l'utilisation, c'est-à-dire que la probabilité de défaillance de l'entité au cours de la première heure d'utilisation est identique à sa probabilité de défaillance au cours d'une heure ou lors d'une utilisation, par exemple, au cours d'un cycle de mille ans.

Les exemples de secteurs industriels pour lesquels la fiabilité peut être le principal attribut de sûreté de fonctionnement applicable incluent:

- l'industrie aérospatiale, pour laquelle il est essentiel qu'un aéronef, lorsqu'il a décollé, effectue le vol sans perte de fonctions essentielles;
- l'industrie automobile, pour laquelle il convient qu'un conducteur soit capable d'effectuer un voyage (dans une plage de vitesses spécifiée, avec un terrain spécifié, etc.) sans nécessité d'une maintenance de quelque type que ce soit.

Les exemples pour lesquels le temps de fonctionnement avant défaillance peut être la mesure de fiabilité exigée incluent:

- les ampoules électriques conçues pour un pourcentage élevé de survie par rapport à une durée de vie donnée;
- des machines de transformation avec lesquelles l'entité fonctionne en continu et le temps de fonctionnement avant défaillance est important pour planifier les activités de maintenance.

Il convient de n'utiliser le MTBF que dans le cas où un taux de défaillance constant est défini par hypothèse. Il convient donc d'utiliser à la place, si possible, une probabilité de défaillance (c'est-à-dire la fiabilité) ou des distributions de taux de défaillance non constants. Des distributions appropriées de taux de défaillance non constants, comme la distribution de Weibull (IEC 61649 [21]), peuvent être utilisées pour la spécification de produits et de composants non réparables. Pour les produits réparables, voir l'IEC 61710 [22].

Il convient également de prendre en considération l'effet de la défaillance lors de la définition des mesures de fiabilité. Par exemple, y a-t-il des défaillances qui n'interrompent pas les performances et qui peuvent être rétablies ultérieurement?

La durabilité est un attribut de sûreté de fonctionnement qui décrit la capacité à restaurer l'état de fonctionnement des entités jusqu'à ce que cette opération ne soit plus réalisable, voire plus viable d'un point de vue économique ou du point de vue de la sécurité, c'est-à-dire qu'une condition limite soit atteinte. Ainsi, il peut être considéré que la durabilité est caractérisée par la période ou l'utilisation de l'entité jusqu'à ce que la condition limite soit atteinte, qui est exprimée dans les mêmes termes que la durée de vie d'exploitation de l'entité (par exemple, cycles, années, miles). Il est également possible d'exprimer la durabilité d'une entité par rapport à la probabilité de pouvoir atteindre une période ou une utilisation donnée jusqu'à ce que l'état limite soit atteint.

La récupérabilité est un attribut de la sûreté de fonctionnement qui décrit la capacité à se remettre d'une défaillance, sans recourir à la maintenance corrective. La capacité de récupération peut exiger ou non des actions externes, par exemple l'allumage et l'extinction d'un ordinateur personnel pour réinitialiser le système d'exploitation. La récupérabilité est exprimée à l'aide de mesures telles que la probabilité de récupération dans un intervalle de temps spécifié.

La Figure 6 donne des recommandations relatives aux différentes méthodes possibles de définition de la fiabilité.

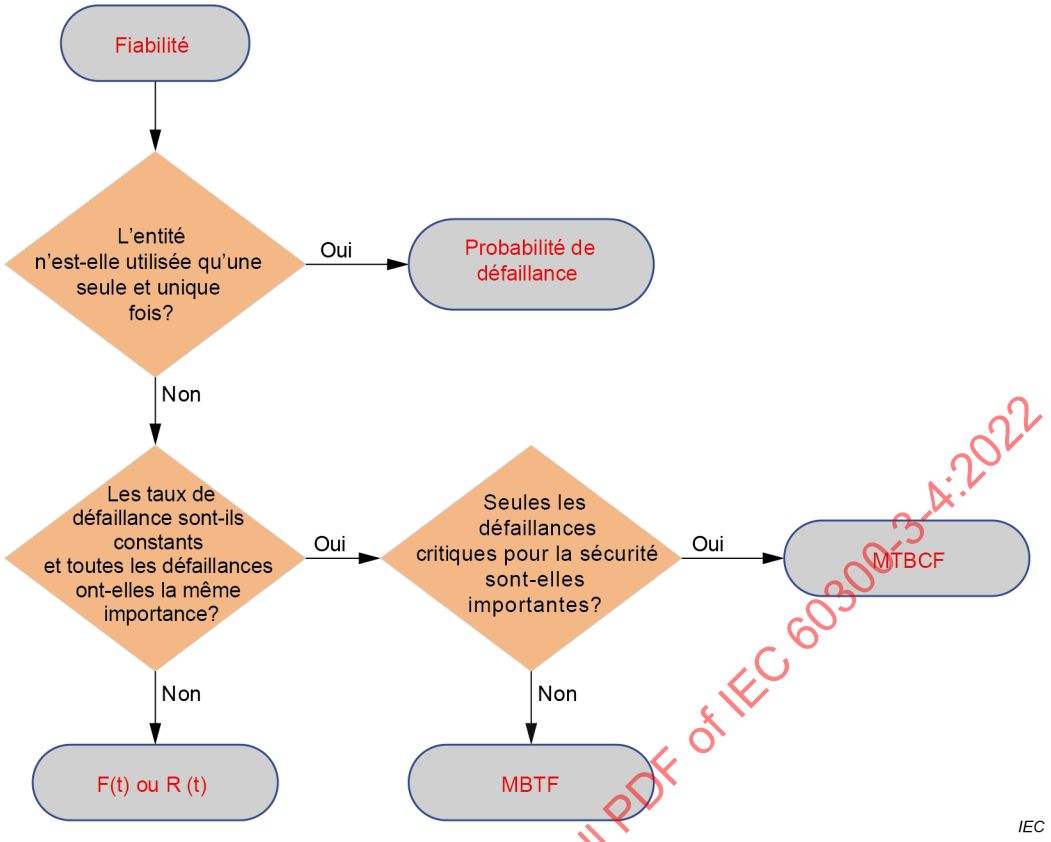

Figure 6 – Exigences de fiabilité

5.4.8 Maintenabilité et exigences de maintenance

La maintenabilité est un attribut important de la sûreté de fonctionnement pour toutes les entités réparables et reflète l'aptitude d'une entité à être maintenue ou restaurée dans un état de fonctionnement comme cela est exigé, dans les conditions d'utilisation et de maintenance données. Les exemples où la maintenabilité peut être importante sont les entités telles que les aéronefs pour lesquels il existe des contraintes sur le temps de maintenance en raison de l'improductivité de l'entité pendant la maintenance, ou les entités dont la maintenance est difficile, ou les entités qui sont prêtes à être utilisées. La maintenabilité est traitée de façon générale dans l'IEC 60300-3-10 [3].

La maintenance peut être soit corrective, c'est-à-dire effectuée après l'apparition d'une défaillance, soit préventive. En cas de redondance, la défaillance d'une entité peut ne pas entraîner nécessairement une défaillance opérationnelle. Cependant, si une défaillance n'est pas corrigée en temps utile, une défaillance opérationnelle peut se produire si les entités de secours sont également défaillantes. En général, l'objectif d'une exigence de maintenabilité est de prévenir les défaillances opérationnelles, de prolonger la vie opérationnelle et de réduire le plus possible l'indisponibilité.

La maintenabilité, associée à la testabilité de ses sous-ensembles, traite de la reconnaissance et de la localisation d'une défaillance, des procédures de réparation ou remplacement, des activités d'entretien et des essais ultérieurs destinés à assurer que l'entité peut être rendue opérationnelle. La maintenabilité inclut également les délais techniques tels que le temps de refroidissement des entités, le temps d'interprétation des informations issues des essais et les temps de traitement. La spécification de la maintenabilité prend en considération des contraintes telles que le site de réparation et l'environnement de réparation, mais ne traite pas des aspects logistiques. Les aspects tels que le soutien logistique, le coût des pièces de rechange, le temps d'obtention des pièces de rechange, le temps d'arrivée d'un agent de maintenance ou de livraison des pièces de rechange à un centre de réparation sont pris en considération dans la maintenabilité.

Les systèmes complexes présentent souvent différents niveaux/classes de maintenance ou de réparation. Ces niveaux peuvent refléter les différences de compétences, d'équipement de soutien ou de durée nécessaires à l'exécution des différentes tâches de maintenance. Par exemple, il peut être attendu que l'utilisateur soit capable d'effectuer une maintenance secondaire sur une voiture, mais qu'une maintenance approfondie soit effectuée par un mécanicien dans un atelier. Les exigences de maintenabilité peuvent être spécifiées pour tenir compte des contraintes entre les niveaux/classes de réparation.

La testabilité est un attribut de la sûreté de fonctionnement qui décrit le degré auquel une entité peut être soumise à des essais fonctionnels dans des conditions indiquées. La testabilité permet de déterminer l'état d'une entité et d'isoler les pannes de cette entité en temps utile et de manière efficace. La testabilité d'un logiciel comprend la commandabilité, qui décrit la capacité d'influencer et de reproduire le comportement du logiciel. La testabilité est exprimée à l'aide de mesures telles que la couverture des pannes (rapport entre les fonctions défectueuses détectables et le nombre total de fonctions), le taux de fausses alarmes (nombre de fausses alarmes par rapport au nombre total de défaillances) et l'observabilité.

La Figure 7 donne des recommandations relatives aux différentes méthodes possibles de définition de la maintenabilité.

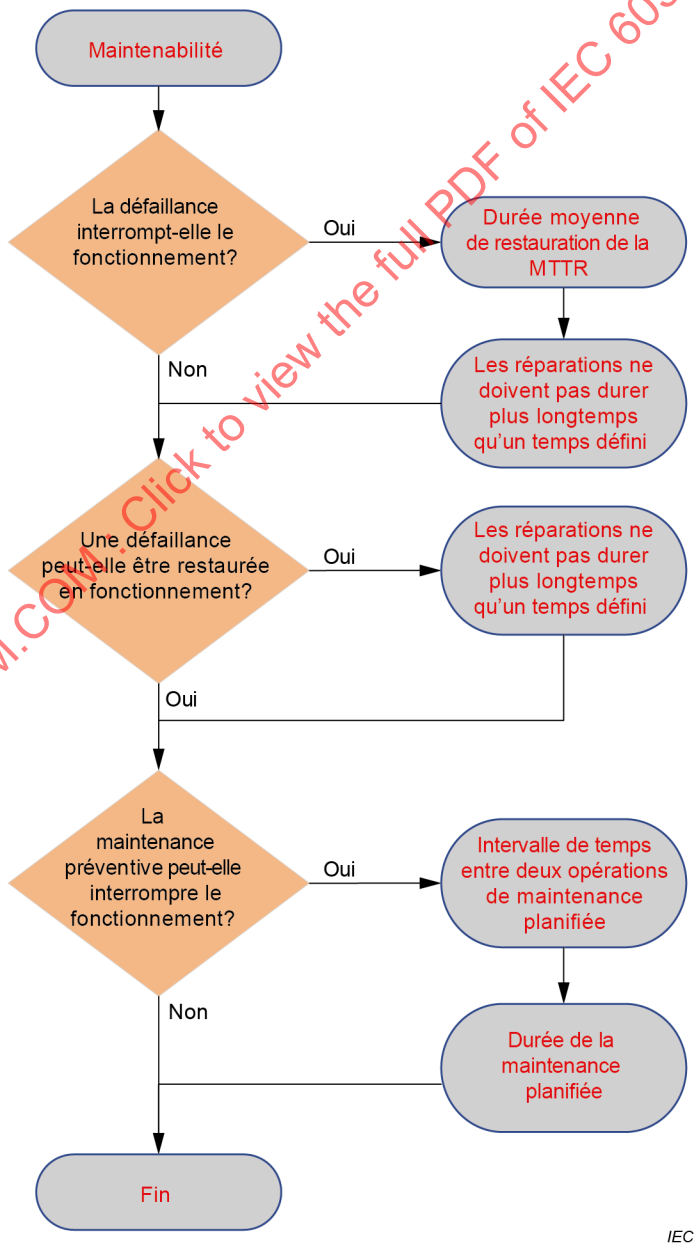

Figure 7 – Exigences de maintenabilité

Lors de la définition des exigences de maintenabilité, il convient de prendre en considération le type de maintenance (par exemple, uniquement la maintenance qui interrompt les performances, toute la maintenance et/ou la maintenance à un niveau/une classe spécifique) et les activités incluses dans la durée de la maintenance (par exemple, le temps consacré à la maintenance, ou tout le temps, y compris le temps consacré aux essais et au diagnostic des défaillances).

5.4.9 Exigences de supportabilité et de support

5.4.9.1 Généralités

La supportabilité est la capacité d'une entité à être soutenue de telle sorte qu'elle puisse fonctionner comme cela est exigé, dans des conditions d'utilisation et de maintenance données. Une mauvaise supportabilité peut nuire à la capacité d'exploiter, d'assurer la maintenance ou de mettre à jour des entités, et augmenter considérablement le coût d'une entité au cours de son cycle de vie. Par conséquent, il peut être important de spécifier des exigences de supportabilité pour assurer qu'une entité peut être exploitée comme et quand cela est prévu et qu'elle peut continuer à fournir de la valeur tout au long de sa vie utile. La supportabilité est traitée de façon générale dans l'IEC 60300-3-14 [4].

Les aspects de la supportabilité qu'il convient de spécifier dépendent fortement du contexte d'utilisation et du concept de support prévu pour l'entité. Par exemple, une entité simple peut remplir des fonctions avec peu ou pas d'infrastructure de support ou d'interactions avec un opérateur et être remplacée en cas de défaillance par une entité comparable selon les exigences générales de forme, d'ajustement et de fonctionnement. Dans ce cas, la spécification de la supportabilité peut s'avérer peu nécessaire. Inversement, une entité complexe peut exiger des éléments de soutien importants et une utilisation ou un contrôle précis par des utilisateurs qualifiés, ainsi que des dispositions complexes pour gérer tous les aspects du support de l'entité afin de trouver un équilibre entre le coût, le risque et les performances. Dans cet exemple, les exigences de supportabilité peuvent être essentielles pour atteindre l'équilibre souhaité.

Etant donné l'importance du contexte pour la spécification de la supportabilité, il est souvent utile d'examiner les cinq capacités constitutives du support de l'entité et d'évaluer si ces capacités comportent des risques importants qu'il convient de gérer par le biais de la spécification. Les cinq capacités constitutives du support de l'entité sont:

- le soutien opérationnel;
- l'approvisionnement;
- le support de maintenance;
- le soutien technique;
- le support de formation.

5.4.9.2 Soutien opérationnel

Le soutien opérationnel concerne les éléments extérieurs à l'entité nécessaires à son fonctionnement et peut comprendre des installations et services d'exploitation, des opérateurs du système, des équipements de soutien, des procédures et des manuels d'utilisation, des données techniques ainsi que des systèmes d'information pertinents.

5.4.9.3 Approvisionnement

L'approvisionnement vise à assurer que les équipements et les consommables nécessaires au fonctionnement et à la maintenance des entités sont disponibles de façon rationnelle, au moment et à l'endroit exigés. Cela comprend la prévision de la demande, la gestion des stocks, les systèmes d'entreposage, de distribution et de transport, l'emballage et la manutention, l'approvisionnement et les systèmes d'information pertinents.

5.4.9.4 Support de maintenance

Le support de maintenance prend en considération les systèmes et les éléments de soutien nécessaires pour développer, exécuter et optimiser un système de maintenance afin de satisfaire aux exigences pertinentes de maintenabilité et de disponibilité. Le soutien à la maintenabilité peut comprendre du personnel formé, des installations, des équipements de soutien et d'essai, des consignes de maintenance, des systèmes de gestion de la maintenance, des données techniques et des systèmes d'information.

5.4.9.5 Soutien technique

Le soutien technique décrit la gestion des processus de conception et d'autres informations pour assurer que la configuration d'une entité est gérée et peut être mise à jour pour satisfaire aux exigences évolutives. Cela peut inclure le personnel, les données techniques, les processus d'ingénierie, les systèmes d'information et les outils ou logiciels de soutien.

5.4.9.6 Support de formation

Le support de formation prend en considération les éléments et les systèmes exigés pour assurer que les personnes sont correctement formées au fonctionnement, à la maintenance et au soutien d'une entité. Il peut s'agir d'équipes chargées de l'instruction et du développement de la formation, d'installations, de matériels et d'aides à la formation, de processus et de systèmes d'information.

La Figure 8 donne des recommandations relatives aux différentes méthodes possibles de définition de la supportabilité.

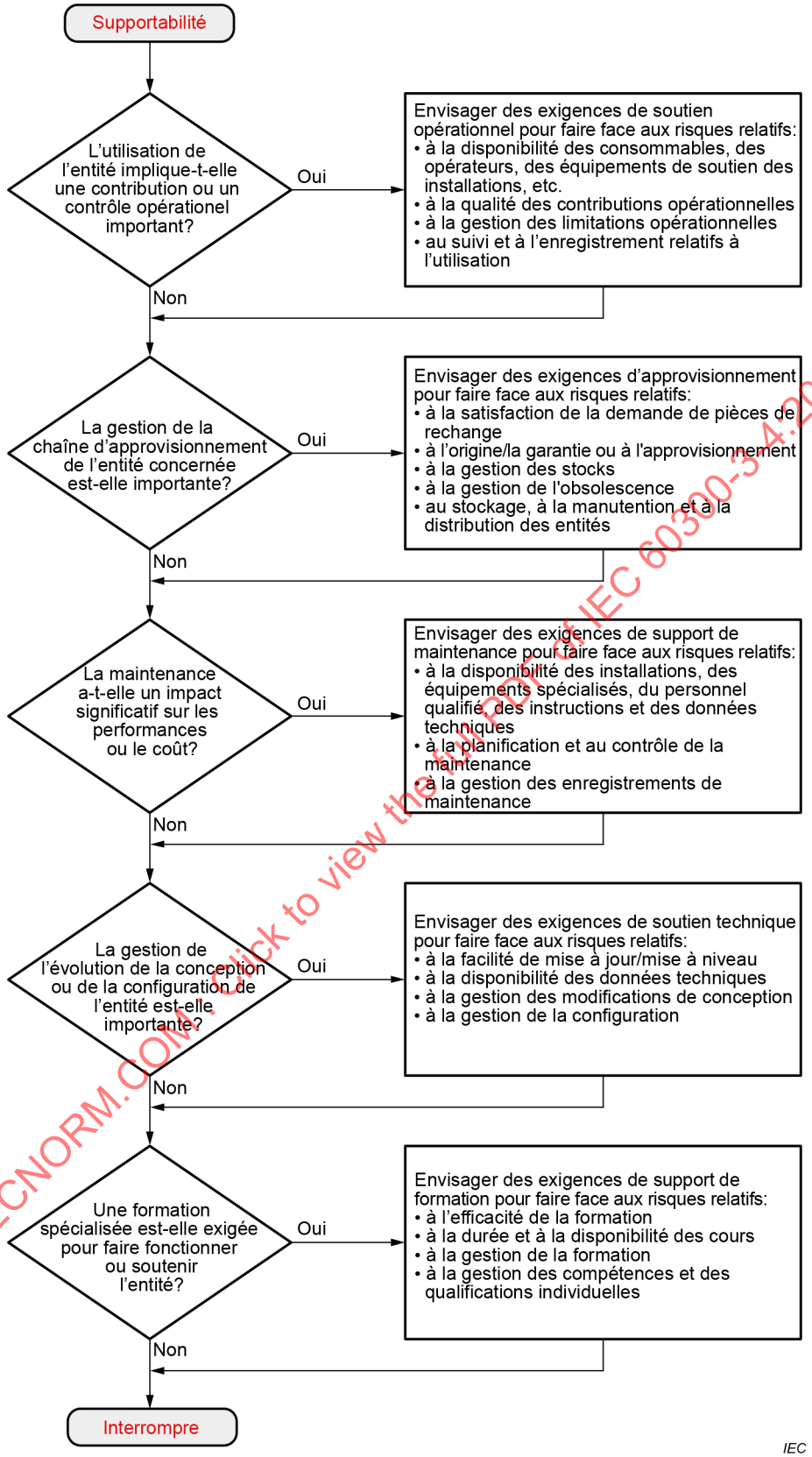

Figure 8 – Exigences de supportabilité

5.4.10 Exigences de disponibilité

La disponibilité d'une entité est la capacité à être en état de fonctionner comme cela est exigé. La disponibilité dépend des attributs combinés de fiabilité, de maintenabilité, de récupérabilité

et de supportabilité et de la performance de la maintenance et du soutien. Il est important que l'acquéreur identifie la définition de la disponibilité utilisée dans la spécification.

EXEMPLE 1 La disponibilité en régime permanent est utilisée dans l'industrie ferroviaire: les exploitants exigent un pourcentage de trains disponibles pour les périodes de pointe de trafic ou des retards à ne pas dépasser.

EXEMPLE 2 La disponibilité moyenne est utilisée dans l'industrie des télécommunications: l'opérateur exige un certain nombre de canaux de communications disponibles afin que l'entité maintienne une disponibilité globale grâce à divers acheminements utilisant les routes disponibles même lorsque certaines routes sont indisponibles.

EXEMPLE 3 La disponibilité est utilisée pour les systèmes fonctionnant en continu, par exemple lorsque l'acquéreur d'une station au sol avec 100 modems peut exiger une analyse qui démontre avec un niveau de confiance de 90 % que le système enregistre moins de 10 min d'interruptions de liaison combinées sur 90 liaisons de communication simultanées sur une période donnée de 6 mois.

Définitions types de la disponibilité:

- la disponibilité en régime permanent qui est la "limite, si elle existe, de la disponibilité instantanée lorsque le temps tend vers l'infini". Pour que cette définition de la disponibilité soit pertinente, les conditions de régime permanent doivent exister. Bien que les mathématiques soient plus simples dans l'hypothèse de conditions stables, il convient de ne pas utiliser la disponibilité en régime permanent sans valider cette hypothèse;
- la disponibilité instantanée est la "probabilité qu'une entité soit en état d'exécuter une fonction exigée dans des conditions données à un instant donné, avec l'hypothèse de la fourniture des ressources externes exigées". Il est peu probable que les exigences de sûreté de fonctionnement spécifient cet élément;
- la disponibilité moyenne est la "moyenne de la disponibilité instantanée pendant un intervalle de temps donné (t1, t2)." Cette mesure est plus utile pour une spécification et s'avère intéressante dans les industries avec lesquelles la disponibilité peut varier pendant différents intervalles de temps, peut-être en raison de conditions de fonctionnement différentes.

Il existe également d'autres définitions de la disponibilité, telles que la disponibilité opérationnelle (qui inclut les délais de logistique) et la disponibilité asymptotique (voir l'IEC 60050-192 et l'IEC 61703 [20]).

La Figure 9 donne des recommandations relatives aux différentes méthodes possibles de définition de la disponibilité.

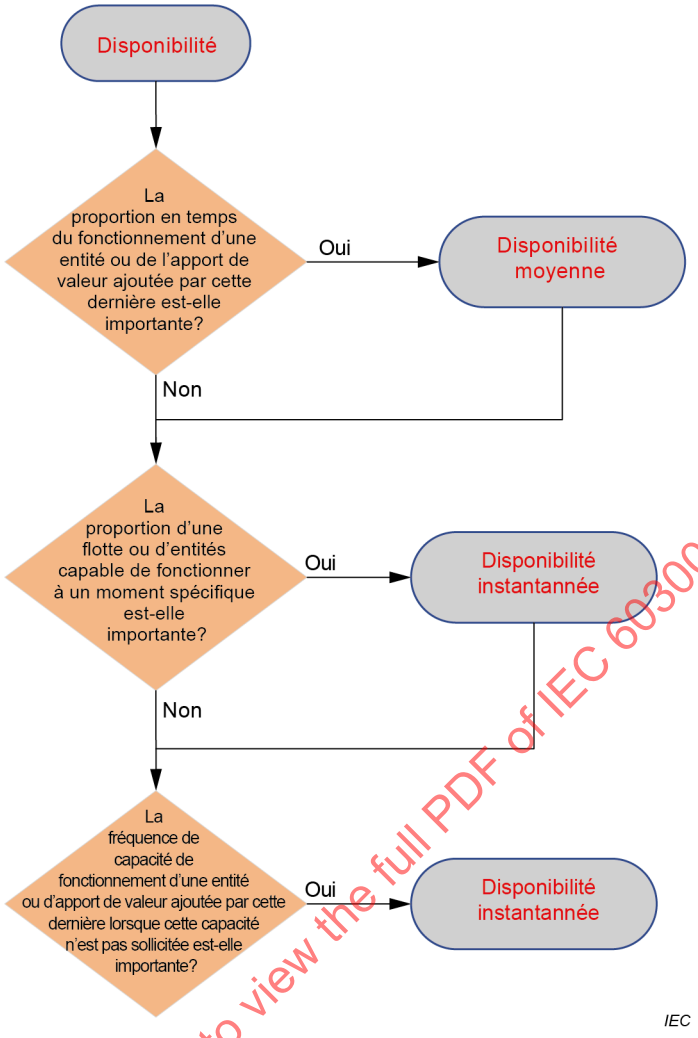

Figure 9 – Exigences de disponibilité

5.5 Justification des mesures utilisées pour les exigences de sûreté de fonctionnement

Cette étape consiste à développer les valeurs numériques cibles pour les mesures quantitatives des attributs de sûreté de fonctionnement et à établir des déclarations pour les mesures qualitatives utilisées dans la spécification de sûreté de fonctionnement. L'IEC 61703 [20] fournit des recommandations sur le développement des valeurs numériques pour les attributs de sûreté de fonctionnement.

Les exigences doivent être réalisables. Une fiabilité de 100 % peut être souhaitable, mais n'est pas possible, et des exigences de haute fiabilité peuvent entraîner des coûts exagérément élevés de conception et de développement, ainsi que la fourniture de preuves. L'acquéreur doit donc évaluer quels niveaux des différents attributs de sûreté de fonctionnement sont raisonnables, en se fondant sur des facteurs comme la réalisation d'entités similaires antérieures, la performance souhaitée et l'étude de l'amélioration qui peut être attendue au cours de l'utilisation. Les entités actuelles deviennent de plus en plus complexes pour satisfaire aux niveaux de fonctionnalité souhaités, et nombre d'entre elles ont atteint la limite d'une fiabilité économiquement rentable.

Des données d'expériences déjà réalisées sont disponibles à partir de diverses sources parmi lesquelles:

- les enregistrements d'essais du producteur (pendant la phase de conception et de développement – si des essais sont effectués et que les résultats sont disponibles et publiés);
- les enregistrements de maintenance et d'entretien propres au fournisseur;
- les données du constructeur pour les sous-entités et les composants;
- les bases de données spécialisées - telles que RIAC, SPIRD;
- les bases de données génériques et les recueils de données.

5.6 Finalisation de la spécification de sûreté de fonctionnement

Après détermination de l'attribut ou des attributs de sûreté de fonctionnement à spécifier et des valeurs numériques ou des exigences qualitatives à utiliser, il est nécessaire de combiner les exigences dans la spécification ainsi que les informations complémentaires.

5.7 Revue de la spécification de la sûreté de fonctionnement

Il convient d'effectuer une revue de la spécification exhaustive afin d'assurer que l'ensemble des exigences de sûreté de fonctionnement est correctement structuré et est exhaustif, concis et cohérent. Cette revue permet également de vérifier que ledit ensemble est compris par toutes les parties prenantes. Cette revue consiste également à établir si les exigences forment un ensemble cohérent et si elles peuvent être affectées ou cumulées entre des sous-entités ou différents fournisseurs comme cela est exigé.

Si la revue détermine que l'ensemble des exigences de sûreté de fonctionnement n'est pas correctement structuré, il est nécessaire de répéter le processus. Différentes décisions peuvent entraîner différents attributs de sûreté de fonctionnement qui constituent les attributs les plus appropriés, ainsi que la génération d'un ensemble différent d'exigences.