IEC 60300-3-4

Edition 2.0 2007-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Dependability management – Part 3-4: Application guide – Guide to the specification of dependability requirements

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

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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 corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

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 It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) 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 CEI

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

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 60300-3-4

Edition 2.0 2007-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Dependability management – Part 3-4: Application guide – Guide to the 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

PRICE CODE
CODE PRIX

W

ICS 03.100.40; 03.120.01

ISBN 2-8318-9308-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

Part 3-4: Application guide – Guide to the 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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
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.

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

This second edition cancels and replaces the first edition published in 1996 and constitutes a technical revision.

The main changes from the previous edition are as follows:

– the concept of systems has been included and the need to specify the dependability of the system and not just the physical equipment has been stressed;
– the need for verification and validation of the requirement has been included;
– differentiation has been made between requirements, that can be measured and verified and validated, and goals, which cannot;
– the content on availability, maintainability and maintenance support has been updated and expanded to similar level of detail to reliability.

The text of this standard is based on the following documents:

FDIS	Report on voting
56/1212/FDIS	56/1233/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

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

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

INTRODUCTION

In many systems, reliability, maintainability and availability are essential performance characteristics. These characteristics, together with maintenance support performance, are known collectively as dependability.

In systems where any of the dependability characteristics are important, it is necessary that these characteristics should be defined and specified in the same way as other system characteristics such as technical performance, dimensions and mass.

The levels of reliability, maintainability, availability and maintenance support performance achieved by a system depend on the conditions under which the system is used and also on the mission profile of the system. When requirements for dependability characteristics are specified, it is necessary to define the conditions of storage, transportation, installation and use that will be applied to the system. It may be important to take account not only of the conditions under which the system will operate, but also of the maintenance policy and organization for maintenance support of the system.

In order to assess the values of the dependability characteristics achieved, it is necessary to use statistical methods.

Dependability characteristics may be specified, like other performance characteristics, in three different ways:

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

This standard is applicable to all three types of specification.

This standard complements IEC 62347 which deals with the definitions of systems and their constituent elements and how to define these so that the dependability requirements of each element can be specified using this standard. The premise of IEC 62347 is to identify system requirements by functions from a system engineering perspective. It provides a process for transforming the purchaser's view on system applications into a technical view for engineering the system. IEC 62347 emphasises architectural and functional design for realisation of functions with appropriate selection of hardware, software and human elements to achieve the system dependability requirements relevant to the purchaser's needs.

DEPENDABILITY MANAGEMENT –

Part 3-4: Application guide – Guide to the specification of dependability requirements

1 Scope

This part of IEC 60300 gives guidance on specifying the required dependability characteristics in specifications, together with specifications of procedures and criteria for verification and validation.

The guidance provided includes the following:

– advice on specifying quantitative and qualitative reliability, maintainability, availability and maintenance support requirements;

– advice to purchasers of a system on how to ensure that the specified requirements will be fulfilled by suppliers;

– advice to suppliers to help them to meet purchaser requirements.

Other documents, such as legislation and governmental regulation may also place requirements on systems and these should be applied in addition to any specifications derived in accordance with this standard.

NOTE 1 Whilst mainly addressing system and equipment level reliability, many of the techniques described in the different parts of IEC 60300 may also be applied to products, items or at the component level. The term system is used throughout this standard.

NOTE 2 This standard does not give guidance on the management of dependability programmes or on the various activities necessary to fulfil stated availability, reliability, maintainability and maintenance support requirements. For this general guidance, see other standards.

NOTE 3 Safety and environment specifications are not directly considered in this guide. However, much of the guidance in this standard could also be applied to safety or environmental specification.

NOTE 4 Specifications for the dependability of a service are not considered in this guide. This includes the provision of a service such as those provided through Public-Private Partnership procurements.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the reference cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050-191, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service.*

IEC 60300-1, *Dependability management systems – Part 1: Dependability management systems*

IEC 60300-2, *Dependability management – Part 2: Guidelines for dependability management*

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

IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

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

IEC 60300-3-5, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

IEC 60300-3-10, *Dependability management – Part 3-10: Application guide – Maintainability*

IEC 60300-3-12, *Dependability management – Part 3-12: Application guide – Integrated logistic support*

IEC 60300-3-14, *Dependability management – Part 3-14: Application guide – Maintenance and maintenance support*

IEC 60605-4, *Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals*

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

IEC 60706-2, *Maintainability of equipment – Part 2: Maintainability requirements and studies during the design and development phase*

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

IEC 60706-5, *Maintainability of equipment – Part 5: Diagnostic testing*

IEC 61014, *Programmes for reliability growth*

IEC 61025, *Fault tree analysis (FTA)*

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

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

IEC 61123, *Reliability testing – Compliance test plans for success ratio*

IEC 61124, *Reliability testing – Compliance tests for constant failure rate and constant failure intensity*

IEC 61160, *Design review*

IEC 61164, *Reliability growth – Statistical test and estimation methods*

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

IEC 61649, *Goodness-of-fit tests, confidence intervals and lower confidence limits for Weibull distributed data*

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

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

IEC 61713, *Software dependability through the software life cycle processes – Application guide*

IEC 62198, *Project risk management – Application guidelines*

IEC 62308, *Equipment Reliability – Reliability assessment methods*

IEC 62347, *Guidance on system dependability specifications*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-191 and the following apply.

NOTE Definitions of "dependability", "availability (performance)", "reliability (performance)", "maintainability (performance)", "maintenance support", "failure", "fault", "item", "time to failure", and "operating time between failures" are given in IEC 60050-191.

3.1
verification
confirmation, through provision of objective evidence, that specified requirements have been fulfilled

[ISO 9000:2005, definition 3.8.4 modified]

NOTE 1 In the context of this standard, verification is the activity of demonstrating for each phase of the relevant life cycle, by analysis and/or tests, that, for the specific inputs, the deliverables meet in all respects the objectives and requirements set for the specific phase.

NOTE 2 Example verification activities include:

– reviews on outputs (documents from all phases of the life cycle) to ensure compliance with the objectives and requirements of the phase, taking into account the specific inputs to that phase;

– design reviews;

– tests and analysis performed on the designed systems to ensure that they perform according to their specification;

– integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together.

3.2
validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

[ISO 9000:2005, definition 3.8.5 modified]

NOTE Validation is the activity of demonstrating that the system under consideration, before or after installation, meets in all respects the requirements specification for that system. Therefore, for example, software validation means confirming by examination and provision of objective evidence that the software satisfies the software requirements specification.

4 General considerations for dependability specifications

4.1 The need for dependability

All systems exhibit some level of dependability, however often they might fail or require maintenance. However, if a system fails too often it might not be available to perform when required or it might cost too much to maintain. In addition, systems that fail repeatedly will get a bad reputation with the user and are unlikely to be bought again once a replacement is

required. On the other hand, designing and manufacturing systems with high levels of reliability can be costly and it may not be possible to produce such a system at an economical price. There is therefore a balance to be struck between low reliability systems that cost a lot to maintain and high reliability systems that may be expensive to design and construct. This is demonstrated by Figure 1, which shows the costs of design and operation for systems of different reliability.

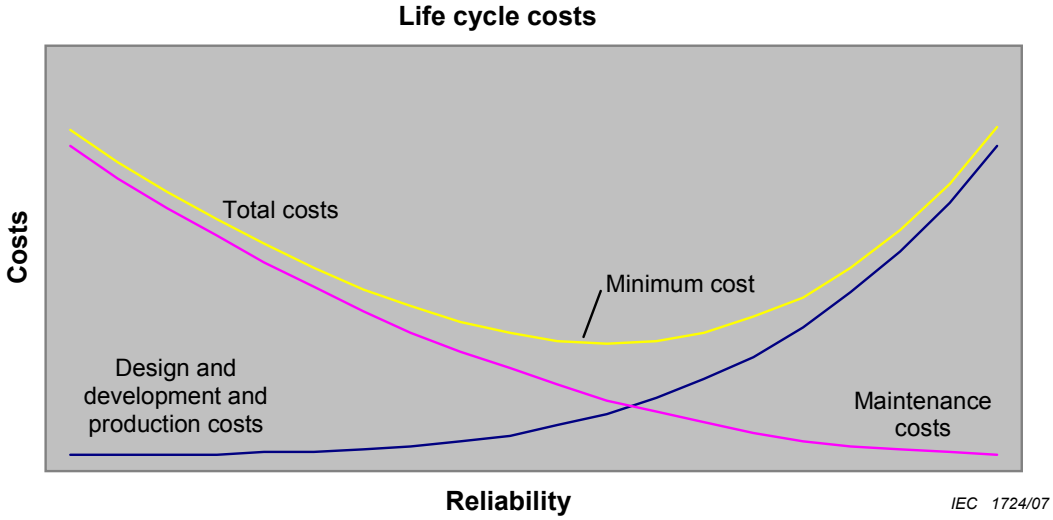

Figure 1 – Relationship between cost and reliability

Figure 1 shows that there is a level of reliability for which the costs over the lifetime of the system are minimized. If a system is Commercial Off The Shelf (COTS) (also known as off the shelf or commercially produced components) this minimum cost level will change as the design and development costs can be shared between many units. However, the optimum reliability for a system may be affected by other issues such as the safety requirements or system function and will not necessarily be the reliability corresponding to minimum life cycle costs.

It is probably true that systems produced by those organizations that do not actively manage dependability achieve levels of reliability much below the minimum life cycle cost point. An investment in dependability design and construction can therefore repay itself in terms of the combined development, manufacturing and operating costs for the system. IEC 60300-3-3 describes Life Cycle Costing and the relationships between dependability and cost.

Dependability includes a number of attributes that are specified differently. Within this standard, dependability has been considered under four headings, as follows:

– availability;
– reliability (R(t)), including mean time to failure (MTTF), mean operating time between failures (MTBF), Weibull or power law parameters;
– maintainability, including mean down time (MDT) and mean time to restoration (MTTR);
– maintenance support.

The dependability characteristics selected for specification should be related to the type and mission of the system, the intended application and the criticality of the required function. For example, only reliability requirements need to be specified if no maintenance actions are intended.

Availability performance requirements are generally specified for systems where down time could cause economic or other loss, through increased operating costs, or personnel injury or loss of service, for example, large systems, production plants, medical equipment, safety

equipment and military systems. Availability performance can be calculated from the system configuration, its subsystems and their reliability performance and maintainability performance requirements, if stated, and by taking into account the maintenance support performance.

Maintainability performance requirements should be specified for systems if the maintenance costs contribute significantly to life-cycle cost or if maintenance is important for the purchaser. Preventive and corrective maintenance requirements may be specified, if applicable.

NOTE The level of maintenance support is very often determined by the conditions of use and is not an intrinsic requirement of the system itself.

Clauses 6, 7, 8 and 9 contain further information on when each of the dependability characteristics would be the most appropriate.

The levels of dependability performance achieved by a system are strongly influenced by the conditions in which it is designed, developed, installed and operated. Dependability is therefore related to other attributes such as quality and the design and manufacturing process. The dependability specification therefore should be part of the total system specification and the interaction between the different attributes recognized and taken into account.

4.2 Requirements and goals

It is important to distinguish between formal requirements in a specification, and goals, as the method of acceptance is different.

A requirement is part of the specification that the purchaser considers is essential that the system meets and for which the supplier has to provide evidence. This evidence may be supplied before the system comes into service as part of the deliverables or once the system is in service, through the application of incentives and penalties for meeting the requirements.

A goal is not a requirement but is the purchaser's aspirations or aims and evidence of the achievement of the goal either need not or cannot be provided.

For high availability or reliability systems, it may not be practicable to provide formal evidence that the high level of availability or reliability has been achieved. The purchaser will need to provide both the high availability and reliability goals, for which evidence cannot be provided, and lower requirements for which evidence can be provided and make it clear which is which.

4.3 Systems

The specification of dependability should be at the system level. A system includes the equipment (both hardware and software) as well as the humans who operate and maintain the system and the procedures by which they operate and maintain it. The system also includes the environment in which the system operates, as shown in Figure 2.

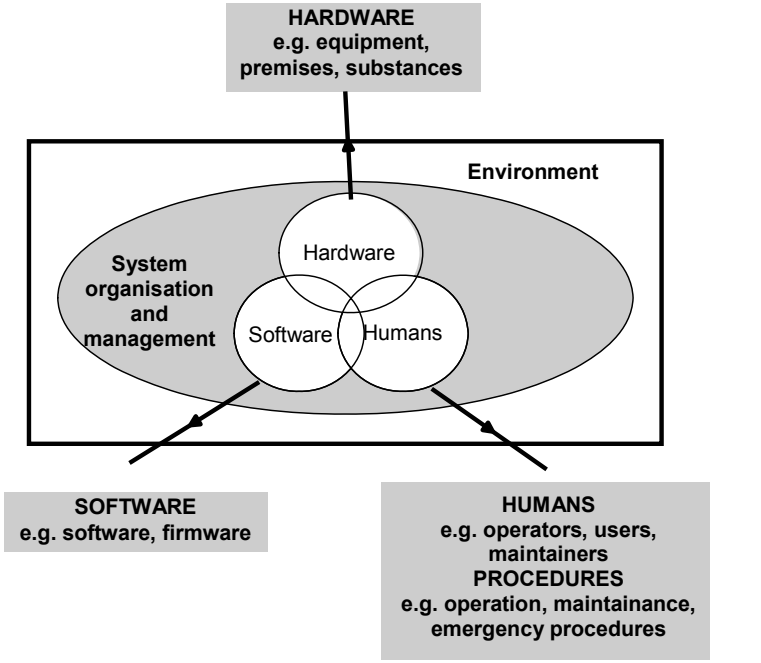

Figure 2 – System elements

Where, possible, all elements of a system should be included in a dependability specification as a change in any one can have a significant effect upon the achieved dependability of the system. For example, different operators of a system can misuse it or be more aggressive in their usage and lead to more failures and therefore achieve lower reliability. However, there may be instances where the supplier and purchaser have little or no control over subsequent maintenance procedures or skills, such as a system within a motor car once sold to a member of the public. The dependability requirements should recognise the particular circumstances of the system being specified.

In addition, the dependability requirements should be linked to the operational or use profile or the functional requirements of the system. The system should be defined in accordance with IEC 62347, which contains details of how to define a system, its elements and the criticality of each function so that the requirements for each element can be specified.

The dependability specification of a system should include the specification of the software and human elements as well as the requirements of the hardware. The guidance in this document may be applied to some aspects of the specification of software but specific guidance may be found in IEC 61713 and the different parts of IEC 61508.

Systems occur at many levels and any system may itself be made up of other systems, often referred to as a system of systems. For example, a bus is a system that includes the motor vehicle, the driver and the driving procedures. The motor vehicle is made up of subsystems that are themselves systems, for example the engine or gearbox, where the human input to the gearbox involves the operation of the gearlever. The subsystems are made up of components and equipment that can themselves be considered as systems and analysed accordingly. This includes considering the interaction of the humans who use the subsystem, how they do so and the manner in which different humans may subject the subsystem to different operational stresses, for example different drivers will drive differently and subject the gearbox to greater or lower loads.

The purchaser might set dependability requirements only at the highest level of system or might decide that it is important that one of the subsystems does not dominate the achieved reliability, and therefore also set requirements at lower levels. These lower level requirements have to be consistent with the top-level requirements and they have to be measurable and

achievable, or they will be goals and not requirements. For example, the contribution of the subsystem to the overall system dependability has to be estimated before the requirements can be apportioned to the subsystems. However, the apportionment to lower level subsystems is not straightforward other than in series systems where all subsystems have a constant failure rate. In other cases, such as systems with redundancy or where the failure rate changes with time, refer to standards such as IEC 61025 and IEC 61078. IEC 60300-3-1 and IEC 61703 give further guidance on the analysis of system dependability.

The type and nature of a system will affect the dependability specification. These include repairable and non-repairable systems and single use devices. Repairable systems cover those where failures can be repaired and the system returned to an operational state. Examples of non-repairable systems include sealed systems, COTS systems, systems where the cost of repair outweighs the cost of replacement, such as many consumer goods, and systems at remote locations where the skills and spares are not available for the time at risk. Single use devices include explosives, passenger air-bags and safety helmets.

Non-repairable systems have to be replaced rather than repaired and the maintainability and maintenance support requirements will be fundamentally different. Also, MTBF will not be a relevant measure for single use devices, where the correct measure would be reliability or alternatively the probability of premature activation. The purchaser has to ensure that the nature of the system and the effect that this can have upon the dependability requirements are identified before the specification is written.

4.4 Demonstration of achievement of requirements

4.4.1 Concept

There are two elements to any specification; the dependability performance requirements and the means by which the supplier has to demonstrate the achievement of the requirements to the purchaser. This means that the supplier has to provide sufficient evidence to the purchaser that the system meets its requirements to give the purchaser the confidence needed to pay the agreed price. Providing additional evidence costs money and is one element in the higher cost of higher reliability systems (see Figure 1) but, without these activities, there is the possibility that the system will not meet its requirements.

There are two main elements; verification and validation. These are defined in ISO 9000 and used for hardware as well as in the software industry as part of the software development process or “v-model” (see IEC 61508) and may be explained as follows. Verification is the process of providing evidence that the system, at any life cycle phase, meets its requirements from the previous life cycle phase(s). Validation is the process of providing evidence that the system meets the actual requirements, which might not always be reflected in the written specification. Both are essential elements.

The level of verification and validation required by the purchaser depends upon the confidence that the purchaser requires that the system will achieve the levels of dependability specified. If the purchaser is willing to maintain a system when it fails in use, then a lower level of evidence, and therefore confidence in the achieved dependability, may be acceptable. This is because the provision of evidence costs money and the purchaser may be willing to accept the risk that the system does not perform as required. The purchaser has to take a balanced decision on the risks that are acceptable when specifying verification and validation requirements (see IEC 62198 for further information on project risk management).

Verification and validation activities have to be planned and systematic in order to be effective. This requires the supplier to state the activities in advance and to obtain agreement from the purchaser, often through the contract. The dependability requirements should consider the various factors likely to affect the cost of dependability verification and validation. This includes the expected lifetime and disposal or recycling of the system.

For a long timescale procurement, activities might be planned many years before completion and, depending upon the contractual terms, the purchaser might have little control over them

until the end of the project. One way to reduce both the purchaser's and supplier's project risk that the system will not be able to provide the level of evidence required can be the progressive provision of verification and validation. This means that the activities are planned throughout the life cycle and the results provided to the purchaser at project milestones. In this way the purchaser builds up confidence in the system throughout the project and there is a much-reduced risk that the level of evidence will be inadequate.

One model that is used for the supplier to provide the evidence that the system has met its requirements to the purchaser is the Reliability and Maintainability Case (usually known as the R&M Case). The R&M Case provides a reasoned, auditable argument that the system has met its requirements and is summarized at project milestones in the R&M Case Report. The R&M Case is usually used to provide progressive evidence and will be issued at a number of project milestones. UK Defence Standard 00-42 Part 3 [1] contains further guidance on the application of the R&M Case philosophy.

4.4.2 Activities

Verification and validation cover a number of activities designed to provide the evidence that a system is meeting its dependability requirements. These activities may be achieved through different techniques, which have the same or similar overall aim but use different methods to achieve it. The choice of technique is dependent upon a number of factors and is discussed in IEC 60300-3-1.

Where the purchaser requires verification and validation to be provided, the supplier has to determine the purpose of the activity and its contribution to verification and validation. For example, a specification should not require a Fault Tree Analysis (FTA) to be performed but should call up analysis to determine the combinations of events that could lead to system 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.

Verification and validation activities include:

a) analysis:
   1) compliance with standards, regulations and guidelines;
   2) expert review / best practice / certification;
   3) calculations primarily used for other design purposes (e.g. finite element analysis for stress, fatigue);
   4) simulation (for example of system performance);
   5) dedicated dependability analysis.
b) 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, e.g. 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, fatigue life, software tests on system, module or component level).

Further details of dependability verification and validation techniques can be found in other parts of IEC 60300 and a list of relevant IEC standards is given in Annex A.

These activities are not all appropriate at all life cycle phases. System testing cannot be carried out until the system has been designed and a prototype or the system built. Similarly, analysis activities are more appropriate during the design stages to allow the exploration of the effects of different options upon the estimated dependability. However, system testing should be planned at the design stage so the supplier can determine the required sub-system tests before the system is constructed. In addition, the system should be designed for testability – i.e. the system and subsystems should be designed so that they can be tested (see IEC 60706-5).

It should be noted that all evidence provided during development is a prediction of the likely dependability performance and the results from analysis are likely to be a less accurate prediction than the results obtained from testing. Therefore the purchaser will probably not wish to 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 system have to be taken into account when the tests are planned. In cases where the test is performed close to the in-service conditions, the test will give a good estimate of the dependability, but the test will last a very long time, require a large number of test items and the low number of failures will result in a large uncertainty in the dependability estimates. If the test is accelerated, the sample size and the test time can be reduced. The larger number of failures will reduce the statistical uncertainty but the technical uncertainty will be higher, since the accelerated test conditions can cause failure modes that are not relevant in the field.

4.5 Contracting for dependability

The purpose of any specification is to provide a basis for a purchaser of a system. It will usually form part of the contract between the purchaser 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 demonstration test to the use of penalty clauses and incentives for in-service achieved reliability.

It is important to distinguish between the requirements, which detail how the system should perform, and the written specification, which details what the system contains. Depending upon the nature of the system, these may be at different levels of complexity, and either may be produced by the purchaser or the supplier. Both can utilise the guidance in this standard.

When writing dependability clauses for contracts, great care has to be taken that the clauses are meaningful and can be contracted for. For example, a clause in a contract for a single use device called up a requirement for 99,5 % reliability. The contract also required a full reliability demonstration test at 80 % confidence levels. This would have necessitated a minimum of 322 tests, or in excess of six times the expected purchase of 50 devices. Since the system was designed to be a single use device, this was clearly an unrealistic requirement and the purchaser had to find alternative methods of achieving the verification and validation required, through either the use of lower reliability goals for which evidence could be provided, analysis, simulation or subsystem testing.

The choice of which verification and validation activities to call up in a contract is dependent upon the level of project risk that the purchaser is willing to accept. If the purchaser is willing to take the risk that the system might fail but be maintained by the supplier, then the use of penalties for poor performance and incentives for exceeding the requirements might be the best method. If however, the purchaser is not willing to risk unavailability of the system, then formal reliability or availability demonstration testing might be necessary. Special care should be taken with rare events, since they can seldom be proven to be absent by testing.

The benefits of each type of approach are as follows.

a) penalties for poor performance will encourage the supplier to give dependability its full attention and can lead to higher levels of dependability than would otherwise be achieved;

b) demonstration testing is costly and time-consuming and might only reveal, just before the in-service date, that the system does not meet its dependability requirements;

c) requiring the supplier to provide maintenance requires a much longer contract e.g. a fixed cost maintenance agreement, with its associated difficulties but the supplier takes the risk that the system achieves poor reliability.

If a dependability specification is to be used as the basis for contracting, it is essential that the specification is fully defined, so as to prevent disagreements once the contract is used. Examples of the types of elements that have to be included in a specification that is used for contracting are:

– the precise and clearly defined criteria by which availability, reliability, maintainability or supportability are to be judged;

– the obligations and responsibilities of purchaser, supplier and any third parties;

– the system under consideration for example, the system, equipment or assembly to which the requirements apply;

– the intended function of the system;

– the various operating and environmental conditions under which the system is used including, where applicable, the relative amount of time spent in each condition;

– the definition of failure or failure criteria, e.g. whether this is total failure of the system to provide any functions, failure to provide essential functions, or partial failure or performance degradation;

– how the system will be installed and used;

– the qualifications and responsibilities of the personnel responsible for operating and maintaining the hardware, software and documentation;

– the maintenance policy to be applied and the associated procedures and support arrangements;

– the methods intended to be applied for verification and validation of compliance with the requirements, including accept/reject criteria;

– acceptable data sources to be used in any analytical techniques.

In order to reduce the number of failures and the down time of the system, it is necessary for the supplier and purchaser to cooperate during all phases of the system life cycle. This creates various obligations on the part of both purchaser and supplier; these should be specified. A formal reliability and maintainability management programme (see IEC 60300-1) can help to identify and specify these activities.

Where possible, it should be specified that the purchaser or distributor acknowledge the responsibility to monitor reliability in use and to report field experience (good or bad) to their suppliers.

4.6 Types of specification

The nature of the system being procured has a fundamental effect upon the manner in which the specification is written. There are three main types:

– specifications written by the supplier:

  these are mainly used for systems that need to have certain dependability characteristics, for example reliability, in order to be accepted in the market place;

– specifications written by the purchaser:

  these are mainly used for standard systems that have to meet certain dependability characteristics in order to satisfy the purchaser’s needs;

– specifications mutually agreed or written by the supplier and the purchaser:

  these are normally used in the case of custom-made systems or alterations to an existing design.

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

Examples of a custom-made system would be a military purchase of a main battle tank (where many subsystems are used only on military vehicles) or a nuclear power station. Examples of COTS systems include domestic washing machines and office IT systems.

For a custom-made system, the purchaser will specify the level and types of verification and validation that the supplier has to provide to demonstrate that the requirements have been met. This verification and validation will include testing and analytical evidence but, as the system is being built solely for the purchaser, cannot include evidence from the use of the system in the in-service environment, except after purchase. The supplier then includes the cost of that verification and validation activities in the quoted price for the system and the purchaser can determine the evidence required, in accordance with the acceptable business risks. However, the purchaser will know that the system is being designed and developed to meet the requirements.

For a COTS system, the supplier states what is available and may provide standard evidence that the system meets certain levels of dependability performance, which may include in-service data from previous applications. However, there is limited opportunity to provide verification and validation and many suppliers will be unwilling to provide in-service data that is considered commercially sensitive.

As a result of the reduced development effort and level of verification and validation activities, the costs of COTS systems are much less than those of a custom-made system. It is for this reason that many purchasers are now stating that requirements will be met through the use of COTS systems, accepting that such a system may not meet the requirements exactly.

However, if the purchaser requires any changes to the off-the-shelf system, it can no longer be considered a COTS system, as the changes might have a significant effect upon the achieved dependability. The purchaser therefore has to take care that a COTS system really is the same as the commercial system and that the evidence provided is adequate. If any changes are requested, the effect of these changes upon the dependability performance has to be considered in detail and additional verification and validation requested by the purchaser, if necessary.

4.7 Derivation of dependability specifications

All reliability, maintainability and availability requirements should be expressed quantitatively wherever possible, but it might also be appropriate to specify qualitative requirements in the specifications. Quantitative requirements are only appropriate when the requirement being specified can be measured during the verification and validation process. If the requirement cannot be measured during provision of evidence, then it is a goal and qualitative requirements will provide the basis of the evidence provided.

Requirements also have to be achievable. All purchasers would like 100 % reliability from their systems but this is not achievable and neither is very high reliability, except at significant cost. The purchaser therefore has to assess what levels of the different dependability measures are reasonable, based upon factors such as the achievement of previous similar systems, the desired performance and consideration of whether an improvement can be expected. Current systems are becoming increasingly complex to meet desired levels of functionality and many have reached the limit of cost-effective reliability performance.

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

a) supplier's own maintenance and servicing records;

b) generic data bases and data books;

c) manufacturer's data for subsystems and components.

As considered in Note 3 of the scope, safety and environment specifications are not considered directly in this guidance. However much of the guidance in this standard could also be applied to safety and environmental specifications. Therefore if there are dependability requirements related to safety and environment, the appropriate safety and environment requirements should be included in or referenced from the dependability requirements.

5 Dependability management

This standard deals with the specification of dependability, through specification of one or more of availability performance, reliability performance, maintainability and maintenance support. These measures are intrinsic characteristics of the system and verification and validation activities can demonstrate the likely levels of achievement. However, other factors can significantly reduce the achieved levels of these measures below the intrinsic levels. The most significant is potentially the quality of manufacture and maintenance of the system that can introduce new faults into the system. It is therefore essential that dependability be actively managed throughout the system life cycle. This includes both during the procurement process and during use and the management activities required will be different for each. If dependability is not managed correctly in either the procurement process or during use, there is a higher likelihood that reliability or availability performance requirements will not be achieved.

IEC 60300-1, IEC 60300-2 and IEC 61160 cover the management of dependability in detail and contain details of activities and techniques for dependability management.

NOTE It should be noted that IEC 61160:2005 does not cover all design reviews; for example, installation design review, user design review and disposal design review following final design review. These standards include details associated with the dependability life cycle.

A system life cycle consists of the following phases:

– concept and definition;

– design and development;

– manufacturing;

– installation;

– operation and maintenance;

– disposal.

The life cycle of the system can have a significant effect upon the achieved dependability of the system. For example, poor handling and extended periods of storage can significantly reduce the reliability performance of a system. In addition, the reliability performance can differ through life, with many systems exhibiting changing failure rate with usage due to component or subsystem wear-out. This change in reliability performance with usage means that, for many systems, the constant failure rate assumption is not valid and different probability distributions, which require more complex mathematical expressions for estimating reliability performance, have to be used. IEC 61649, IEC 61703 and IEC 61710 give further guidance.

Changes in system usage are a further factor that affects reliability performance. For example, a vehicle that normally runs on the road will almost certainly fail more often when used off-road due to the different stresses and loads placed on the vehicle. Thus the system

mission or usage is an essential part of the dependability specification and changes have to be monitored and managed as part of the dependability life cycle.

6 Availability

6.1 General

6.1.1 Choice of dependability characteristic

For some systems, particularly complex systems, it is necessary to consider reliability and maintenance together. In such systems, it might be appropriate at the system level to specify availability requirements rather than separate reliability and maintainability requirements. It is important that the purchaser defines which of the availability definitions is being specified or there is a risk that the required level of availability performance will not be achieved. Requirements for the steady-state availability are the most commonly used, although mean availability may also be appropriate.

Examples of industries where availability performance may be the prime dependability characteristic of interest include the rail industry, where the train operators require a percentage of the trains to be available for use during peak periods or maximum delay times, and the telecommunications industry, where the operator requires a certain number of communication channels to be available such that the system maintains an overall availability while some routes might be unavailable due to the diverse routeings available.

Steady-state availability is “the mean of the instantaneous availability under steady-state conditions over a given time interval.” For this definition of availability to be relevant, steady-state conditions have to exist. Since the mathematics is simplified if steady state conditions do exist, steady-state availability is sometimes specified when not appropriate.

Instantaneous availability is the “probability that an item is in a state to perform a required function under given conditions at a given instant of time, assuming that the required external resources are provided.” It is unlikely to be specified in dependability requirements.

Mean availability is the “mean of the instantaneous availability over a given time interval (t_1, t_2).” This measure is more useful for 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 60050-191).

6.1.2 Relationship between availability, reliability and maintainability

Availability, reliability and maintainability are not independent measures but are linked for a repairable system as follows:

$$\text{Steady-state availability} = \frac{\text{MUT}}{\text{MUT} + \text{MDT}}$$

where

MUT = mean up time;

MDT = mean down time.

If the case of constant failure rate and constant repair rate, and only in this case, the asymptotic and steady-state availability are identical and are often simply referred to as “availability”. This relationship is only applicable under these very specific conditions, which

do not often occur. This calculation should only be used as a first estimate, before more detailed and accurate assessments of availability are made.

All three dependability performance measures should not be specified as this will constrain the system dependability performance. However, it is usual to specify two of the three measures in order to ensure that the balance between up-time and down-time is operationally acceptable. The same availability may be achieved through high levels of MUT with long down-times or alternatively lower MUT but short down-times. For example, personal computer operating systems can fail regularly but only take minutes to reboot and restart, giving an overall high availability. This is frustrating for the user but might be more acceptable than the same availability from a computer that only fails infrequently but then is not available for use for some days following failure. However, for telecommunications networks achieving availability through lower reliability with short down-times might be unacceptable because they are not available for sufficient durations for data to be transmitted.

6.2 Availability specifications

6.2.1 Quantitative requirements

Any availability specification has to define exactly what is meant by availability, i.e. which type of availability is being specified, and what times are included in down time, whether logistic delays are included and to what extent.

Requirements for availability can be expressed as a decimal fraction or as a percentage, for example, mean up time as a percentage of observation time. Availability requirements cover both the occurrence of failures and down time. If mean availability is being specified, the time period over which it is measured also has to be specified, together with other relevant time information. For example, if the mean availability for commuter trains is required, it might be specified as mean availability measured over each hour between the hours of (say) 7 a.m. and 10 a.m. and 5 p.m. and 8 p.m. from Monday to Friday.

When specifying quantitative availability requirements, it is usual to accumulate the down times occurring over a certain time period (for example, a month or a year). If part of the system down time is excluded from the responsibility of the supplier (for example, logistic or administrative delay), this should be noted in the specification together with a statement of the values of the times concerned. Figure 191-10 in IEC 60050-191 gives guidance on the various maintenance times. Alternatively, an intrinsic availability may be specified which is calculated by excluding such maintenance times.

Annex B clause B.2 contains examples of quantitative availability requirements.

6.2.2 Qualitative requirements

Qualitative availability requirements might include a combination of qualitative reliability and maintainability requirements and quantitative availability requirements should be used if at all possible. Qualitative availability requirements might supplement the quantitative requirements where the quantitative requirements can not cover all aspects of the specification, for example, if downtime under certain operating conditions is more critical. However, the type of availability and the times included in downtime still have to be defined in the specification.

6.3 Provision of availability verification and validation

6.3.1 General

The specification should include the need for verification and validation of the required availability performance. Availability evidence is often provided through a combination of reliability and maintainability evidence, rather than directly.

6.3.2 Verification and validation by testing

Where verification and validation is to be carried out by testing, the standardized compliance test procedures for steady-state availability given in IEC 61070 may be applied. It should be noted, however, that for very high availability requirements (for example, > 0,999), it is very difficult to establish a meaningful test plan. Evaluation and verification and validation of subsystem availability performance can assist in this activity. This can be achieved by using observations at system and subsystem level in a system availability model. In any case, the feasibility of the methods applied to verify and validate high availability requirements needs to be proven.

For in-service or availability performance testing, a detailed field data collection program should be agreed in advance (see IEC 60300-3-2), including down time due to hardware failures, software failures, maintenance procedures and other reasons. The execution of the test then has to be monitored and analysed as it progresses to provide the necessary evidence.

Furthermore, if more than one item of the same type of system is used during the test, the number of items and the period of observation should be taken into account. A procedure should be specified such that, in the event of non-compliance, an improvement is agreed and introduced and testing is continued. Care should be taken that the use of more than one item is statistically valid, as 100 h of one item is only equivalent to 1 h of 100 items if a number of factors are taken into account and certain assumptions are true. These include the assumption of constant failure rate, the absence of early life failures or wear out failures and the degree of confidence that the samples used are representative of the system.

6.3.3 Verification and validation by analysis

If verification and validation is to be carried out by analysis methods, the standardized prediction techniques with detailed analysis methodology as specified in IEC 62308 may be applied.

Generally, data for calculation should be based on recognized sources of data, results obtained from operational experience on similar systems in the field, laboratory tests or from software/hardware integration. The data should be agreed between the supplier and the purchaser and the data sources should be recorded.

7 Reliability

7.1 General

For some systems, it is necessary to consider directly the reliability of the system. In such systems, it might be appropriate at system level to specify separate reliability and maintainability requirements. Reliability is, by definition, the ability of a system to perform a required function under given conditions for a given time interval, that is without failure. It is most correctly described by a probability that the system can complete its required mission. However, many specifications will define the required reliability through the use of alternative measures, such as mean time to failure or mean operating time between failures.

Examples of industries where reliability performance can be the prime dependability characteristic of interest include the aerospace industry, where once an aircraft has taken off it is essential that it completes the flight without total failure, and the automotive industry, where the driver needs to reach the destination and can maintain the vehicle once at the destination.

Examples of where time to failure can be the required reliability measure include electric light bulbs that are designed to a life. Other examples include process machinery, where the system is continuously operating and the time to failure is of importance to plan maintenance activities.

Care has to be taken by the purchaser that the appropriate reliability performance measure is specified and that the statistical implications of the requirement are understood. For example, if a 99 % reliability over one year is specified, this can seem sensible. However, this equates to a MTBF of 871 613 h (or greater than 99 years), if the failure rate is constant. Therefore MTBF is often considered an obsolete measure of reliability and subject to modification due to changes in use and it is recommended that availability, reliability or failure probability should be stated instead. For non constant failure rate the Weibull parameters or other applicable distributions may be used for specification (see IEC 61649). For non constant failure intensity the Power Law model may be used (see IEC 61164 and IEC 61710).

7.2 Reliability specification

7.2.1 Quantitative requirements

Reliability performance requirements should be quantitative and should be specified before design of the system begins. As with any statistic, any quantitative reliability requirement or measure should also specify the confidence with which the requirement is to be demonstrated or stated (see IEC 60605-4).

One early consideration is the failure mechanisms likely to be experienced by the system, as this will determine which of the reliability measures is appropriate and relevant. For example, motor vehicle engines fail according to how far they are driven rather than age since new, so that miles driven is the appropriate unit. They also wear-out so that the constant failure rate assumption is not valid. Household electric light bulbs primarily fail relative to the number of times they are switched on and off, and to a lesser extent the number of hours they are lit, so operations or operational hours are the appropriate units and the system is designed for a defined operational life. The inclusion, or not, of redundant elements is another factor that affects the choice of the reliability measure.

For every system, it is necessary to select and define each reliability characteristic that is required and to specify a quantitative requirement for each characteristic. When specifying quantitative requirements for a system, it is important to state the following:

– the system's application or use profile;
– the failure criteria or the definition of a failure, i.e. what constitutes a failure in the particular system in the intended application;

  NOTE A failure may be defined in various ways according to the consequences, for example, the loss of a service, the need for repair (see also 7.2.2).

– the operating conditions;
– the environmental conditions;
– the methods intended to be applied for the evidence of compliance with the requirements.

Without such statements, the specification of a reliability performance measure such as R(t), F(t), MTTF, MTBF, numbers of failures in a time interval, Weibull or Power Law parameters would be meaningless.

When selecting the value of the reliability performance measure to be specified, the following factors should be taken into account:

– limits imposed by the technological state of the art and the nature and complexity of the system;
– the experience of the purchaser in operating and maintaining the particular type of system;
– the feasibility of verifying the specified requirement;
– the reliability level of units, components, etc., from which the system can be manufactured;
– the cost of design, production and verification and validation of the system with a specified level of reliability.

If, during the development of a project, it becomes evident that the underlying assumptions are not valid, the reliability performance requirements might have to be reconsidered and changed. If the specification is to be changed, this should only be done with the agreement of all the parties concerned.

The quantitative requirements should be clearly specified in a form against which it will be possible to compare the results subsequently obtained.

Where evidence of conformity to the quantitative requirements is to be provided through testing, the confidence level required should be specified, or the actual test plan to be used should be specified. If a test plan is specified, the specification should include the test duration and the acceptance/rejection criteria.

A number of different types of reliability demonstration test exist and, all other things being equal, sequential test plans (see IEC 61123 and IEC 61124) should be used in preference to fixed time/failure terminated test plans, as the former are more efficient. If the reliability performance measure is known, or is likely to vary with time, the dependability should be specified by, for example, Weibull parameters for unrepairable systems (see IEC 61649) or Power Law parameters for repairable systems (IEC 61164 and IEC 61710). Alternatively the mean failure intensity over a stated time period can be specified. See IEC 60300-3-5 for information on statistical distributions.

Annex B, Clause B.3, contains examples of quantitative reliability requirements.

7.2.2 Qualitative requirements

Qualitative reliability requirements may be expressed in terms of either or both of the following:

– design criteria for the system;
– reliability improvement activities to be applied during the system life cycle phases.

Design criteria for a system, such as the physical, performance and operational requirements, usually stand alone, but might also be complementary to quantitative reliability requirements. Such criteria can indirectly impose reliability requirements for the system itself and for the way the system is installed and its performance is monitored. Some examples are as follows:

– single fault criterion, i.e. the system has to be such that no single fault can lead to a critical state of the system;
– accumulating fault criterion, i.e. the system has to be such that no undetected fault, when combined with additional faults, can cause system failure;
– path separation, i.e. redundant subsystems have to be kept independent by using separate paths for cables, pipes, etc., for signalling channels, power supply and other supporting supplies;
– monitoring of critical functions, i.e. provision has to be made for automatic or manual checking of critical functions either continuously or at intervals, in order to maintain a specified level of reliability performance.

In addition to specifying quantitative reliability performance requirements, it may often be advisable to specify a sequence of reliability (and maintainability) improvement activities to be implemented during system life-cycle phases. Such qualitative requirements may be applied to hardware, software and support. These activities are particularly important if the quantitative requirements do not specify all aspects of the reliability performance of the system. They should be mutually agreed between purchaser and supplier, both technically and in terms of time schedule and cost. Such qualitative requirements should be formalized in and managed through a reliability programme plan (or dependability plan) (see IEC 60300-2).

The reliability programme plan should be tailored according to the nature of the system and the requirements specified and typically includes the following:

– the types of analysis methods to be applied;
– a reliability growth programme, if necessary (see IEC 61014);
– statements about how to verify conformity to the requirements (see IEC 60300-3-5) or any other qualitative or quantitative measure to be used for expressing the degree of conformity to the requirements;
– criteria for component selection and arrangements for quality evidence;
– worst case analysis.

7.3 Reliability verification and validation

7.3.1 General

The specification should state the methods to be used to provide evidence that the specified requirements have been met.

Reliability verification and validation may be provided either by analysis during the design and before production, by laboratory tests or field tests after production or by field performance evaluation after delivery. In addition, verification and validation may be obtained from other activities during the development process. Examples include design analysis (such as stress analysis), performance testing, software testing and operational simulations. Evidence may be collected from all sources to provide verification and validation and will complement dedicated reliability verification and validation activities.

7.3.2 Verification and validation by testing

Preferred methods of reliability verification and validation by testing are normally selected by agreement between the purchaser and supplier and include:

– the collection and analysis of failure data from systems in the field i.e. the actual use (see IEC 60300-3-2 and IEC 60605-6). However, their validity requires sufficient data collection and they may be too late in the procurement process if high levels of evidence are required;
– testing systems in use or in the laboratory, using compliance or determination tests as described in IEC 60300-3-5, IEC 61123, IEC 61124, IEC 61649 or IEC 61710. When specifying laboratory tests, it is important to consider the associated factors such as cost and time.

All testing should be tailored to reflect the operational and environmental use and stresses that the system will experience or the result will not reflect the achieved in service reliability of the system.

Precise criteria should be specified to enable all failures in hardware and software, etc. to be classified into relevant or non-relevant categories. This classification is the basis of the acceptance/rejection criteria and it is essential that it should be clearly and precisely specified before the tests start and preferably defined early in the life cycle, so that there can be no suspicion that the results have been adjusted to provide the desired result. However it may not be possible to define all the test criteria until later in the life cycle or product development.

The verification and validation of reliability performance measures for repaired and non-repaired systems have each to be considered separately.

IEC 61123 contains details of tests that may be used if success ratio is used as the reliability performance measure and IEC 61124 contains tests which are appropriate if the constant failure rate or failure intensity assumption is valid. The constant failure rate or failure intensity assumption should be validated as the results of a test may be nullified if the assumption is incorrectly used (see IEC 60605-6).

7.3.3 Verification and validation by analysis

Reliability verification and validation of a system can be made prior to delivery by calculation based on reliability analysis. In some instances (for example systems having very high reliability), this can be the only practicable approach. Analysis can be used long before reliability validation during in-service operation or by laboratory testing is possible. Such a method can only determine by analysis whether the system to be delivered fulfils corresponding requirements laid down in the system specification; it does not measure the realized reliability directly.

Examples of analytical techniques for reliability verification and validation of a system including hardware and software include reliability block diagrams, fault trees, state diagrams and failure mode and effect analysis. See Annex A for standards that give guidance on various analysis tools.

The hardware element of a system should be analysed to establish that the failure rates of each of its subsystems, parts and electronic or other components take into account the expected usage and operational stress and that their derivation is appropriate and justifiable. Electrical, thermal or other measurements can be necessary for this purpose.

The software in the system should be similarly analysed to identify possible software failure modes and evaluate qualitatively their impact on the reliability performance of the system.

Data for such calculations can be based, for example, on results obtained from operational experience with similar systems in the field, from laboratory tests, from software/hardware integration or from recognized data sources. If the purchaser intends to specify the use of a certain database (for example, a particular failure rate data bank), this should be agreed between the supplier and the purchaser. Specifying the use of a certain database, however, does not relieve the supplier of his obligation to achieve the required reliability performance. In all cases, the data source should be identified and the assumptions used in the estimate recorded.

8 Maintainability

8.1 General

Maintainability is an important dependability measure for all repairable types of system and reflects the ability of a system to be retained in, or restored to, a state in which it can perform the required function. Examples may be mid-life updates for software projects to correct low levels of achieved availability or systems at remote locations that are difficult to maintain. In addition, for other systems maintainability can have a significant effect upon the achieved dependability if incorrectly specified, especially in systems not containing redundancy. Maintainability is generally dealt with in IEC 60300-3-10.

8.2 Maintainability specification

8.2.1 Quantitative requirements

IEC 60706-2 contains full details of specifying and contracting for maintainability. It might be necessary to specify requirements for corrective and preventive maintenance separately as the maintenance support required can be very different.

Where quantitative requirements are specified, it is important to specify how long a system is expected to be in a non-operating state due to maintenance or maintenance support. This time has to be specified in terms of appropriate measures such as mean or fractile repair time, or mean or fractile logistic delay. Quantitative requirements may also be in terms of the cost of maintenance as well as time or distance based, e.g. maintenance cost per operating hour.

A complete specification of maintainability performance requirements should cover five broad areas:

– the maintainability performance to be achieved by the design of the system;
– the constraints that will be placed on the use of the system which will affect maintenance;
– the maintainability programme requirements to be accomplished by the supplier to assure that the delivered system has the required maintainability characteristics;
– maintenance access requirements;
– the provision of maintenance support planning.

When specifying maintainability requirements, it is important to state the following:

– the various operating and environmental conditions under which the system is used;
– the qualifications, responsibilities and physical characteristics of the personnel responsible for operating and maintaining the system;
– the maintenance policy to be applied and the associated procedures and support arrangements (e.g. preventive maintenance or diagnostic testing);
– the tools available and any special tools required;
– the spare parts to be provided and how they are estimated and managed.

The maintainability performance specification should detail the requirements and the method of verifying them. It should also include precise definitions of terms used in the specification with references to standard vocabularies as appropriate.

Maintainability requirements may be specified in the specification either as goals or as definite requirements that are to be verified in accordance with prescribed procedures. Goals or requirements may be specified in either quantitative or qualitative terms.

A maintainability performance specification typically covers the various aspects of maintainability achievement at the operational level. However, since maintainability performance as a system characteristic affects maintenance support costs and can also affect maintenance times at different maintenance levels, requirements should be included in the specification covering achievements at all levels affected by the maintenance policy.

More detailed guidance on maintainability performance requirements in specifications and contracts is provided in IEC 60706-2.

Annex B, Clause B.4, contains examples of quantitative maintainability requirements.

8.2.2 Qualitative requirements

Where maintainability support requirements cannot be specified quantitatively, qualitative requirements should be used as a supplement. However, as with all dependability characteristics, both quantitative and qualitative requirements may be specified. This can for example be specifications of the degree to which a system has to conform to specific conditions and the constraints related to maintenance.

8.3 Maintainability verification and validation

Much of the verification and validation of maintainability may be provided through other development testing or analysis. For example, reliability testing will provide data on the maintainability of the system, provided that the relevant data is collected. Therefore, all development trials and analyses should be examined to see if they could provide meaningful maintainability data and, if so, the trials should be built into the trial plan at the earliest opportunity.

Verification and validation of maintainability performance is the process of determining that the requirements in the specification have been met. The methods and procedures for verification and validation should be specified with the maintainability requirements. Methods of verification and validation may range from the submission by the supplier of appropriate data or information to a requirement to perform a special maintainability demonstration.

Maintainability verification and validation should be regarded as a continuous process. Maintainability related data should be generated, collected and evaluated as they become available in the course of project development, and the results should be compared constantly with specified maintainability requirements.

Several methods of verifying maintainability performance are described in IEC 60706-3. They include the following:

– analysis and review of maintainability characteristics;
– special studies;
– demonstration tests;
– review of operational experience.

The specification may give guidance on, or may specify which of the above methods are to be applied.

Further information on maintainability verification and validation is given in IEC 60706-3. Information concerning diagnostic testing is given in IEC 60706-5 and statistical methods in maintainability allocation in IEC 60706-2.

9 Maintenance support

9.1 General

Maintenance support is the ability of a maintenance organisation to provide the resources necessary to maintain a system, i.e. when and where required and the provision of maintenance support is often critical in ensuring the dependability of systems. The level of maintenance support is very often influenced by the conditions of use and factors that change through the life cycle.

Maintenance support can be supplied fully or partly by the supplier, the purchaser of the system or a third party, depending upon the nature of the specification. The specification will therefore vary depending upon the source of maintenance support. Integrated Logistic Support (ILS) is the method by which all logistic support services are considered and provided as an integral part of product development (see IEC 60300-3-12). In other cases, especially where systems are constructed mainly of COTS equipment, suppliers provide only basic or standardized maintenance support planning and purchasers become responsible for providing the required maintenance and maintenance support for their specific application, often using internal resources (see IEC 60300-3-14).

To the extent that the maintenance support is supplied by the supplier, it should be specified as part of the delivery. Maintenance support by the purchaser (including the user) will be part of the specified conditions of operation of the system, a prerequisite for the stated reliability, availability and maintainability values.

9.2 Maintenance support specification

9.2.1 Quantitative requirements

Maintenance support requirements should, where possible, be specified in a quantitative way. Examples of such quantitative specifications are guaranteed response times, mean

administrative delay, mean logistic delay, spare shortage probability and spare shortage delay. Further information can be found in IEC 60300-3-12 and IEC 60706-2.

When specifying maintenance support requirements, it is important to state the following:

– the various operating and environmental conditions under which the system is used;
– the obligations and responsibilities of purchaser, supplier and third parties;
– the maintenance policy to be applied and the associated procedures and support arrangements;
– the tools available and any special tools or jigs required;
– the qualifications, responsibilities and physical characteristics of the personnel responsible for operating and maintaining the system.

The maintenance support specifications should be specified before design of the system begins and be updated before delivery of the system.

Annex B, Clause B.5, contains examples of quantitative maintenance support requirements.

9.2.2 Qualitative requirements

Where maintenance support requirements cannot be specified quantitatively, qualitative requirements should be used as a supplement. However, as with all dependability characteristics, both quantitative and qualitative requirements may be specified. This can for example be specifications of the required training level and workmanship, standard of maintenance personnel or requirements for workshop facilities and tools to be available.

Further information can be found in IEC 60300-3-12 and IEC 60706-2.

9.3 Maintenance support verification and validation

Verification and validation methods for maintenance support will be related closely to maintainability verification and validation and it is unlikely that they could be separated, as maintainability performance will depend upon the maintenance support available and no further information will be available. Other verification and validation will be qualitative evidence that the support is available and effective.

Annex A
(informative)

Reference standards for verification and validation techniques

A.1 Techniques for dependability testing

Table A.1 shows reference standards for dependability verification and validation through testing. Where no date is given the latest version is to be used.

Table A.1 – Techniques for dependability verification and validation through testing

Standard identifier	Standard title	Testing technique covered
IEC 60300-3-2	Dependability management – Part 3-2: Application Guide – Collection of dependability data from the field	Dependability data collection
IEC 60300-3-5	Dependability management – Part 3-5: Application guide — Reliability test conditions and statistical test principles	Reliability testing – Statistics
IEC 60300-3-7	Dependability management – Part 3-7: Application guide – Reliability stress screening of electronic hardware	Stress screening – Electronic hardware
IEC 60605-2	Equipment reliability testing – Part 2: Design of test cycles	Reliability testing
IEC 60605-3-1	Equipment reliability testing – Part 3-1: Preferred test conditions. Indoor portable equipment – Low degree of simulation	Reliability testing
IEC 60605-3-2	Equipment reliability testing – Part 3-2: Preferred test conditions. Equipment for stationary use in weatherprotected locations – High degree of simulation.	Reliability testing
IEC 60605-3-3	Equipment reliability testing – Part 3-3: Preferred test conditions – Test cycle 3: Equipment for stationary use in partially weatherprotected locations – Low degree of simulation	Reliability testing
IEC 60605-3-4	Equipment reliability testing – Part 3-4: Preferred test conditions – Test cycle 4: Equipment for portable and non-stationary use – Low degree of simulation	Reliability testing
IEC 60605-3-5	Equipment reliability testing – Part 3-5: Preferred test conditions – Test cycle 5: Ground mobile equipment – Low degree of simulation	Reliability testing
IEC 60605-3-6	Equipment reliability testing – Part 3-6: Preferred test conditions – Test cycle 6: Outdoor transportable equipment – Low degree of simulation	Reliability testing
IEC 60605-4	Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals	Reliability testing – statistics
IEC 60605-6	Equipment reliability testing – Part 6: Tests for the validity and validation of the constant failure rate and constant failure intensity	Maintainability data analysis
IEC 60706-3	Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data	Maintainability testing
IEC 60706-5	Maintainability of equipment – Part 5: Diagnostic testing	Maintainability testing

Table A.1 *(continued)*

Standard identifier	Standard title	Testing technique covered
IEC 61014	Programmes for reliability growth	Reliability growth programmes
IEC 61070	Compliance test procedures for steady-state availability	Availability demonstration
IEC 61123	Reliability testing – Compliance test plans for success ratio	Compliance test plans – success ratio
IEC 61124	Reliability testing – Compliance tests for constant failure rate and constant failure intensity	Compliance test plans – constant failure rate and constant failure intensity
IEC 61163-1	Reliability stress screening – Part 1: Repairable assemblies manufactured in lots	Stress screening
IEC 61163-2	Reliability stress screening – Part 2: Electronic components	Stress screening
IEC 61164	Reliability growth – Statistical test and estimation methods	Reliability growth test and estimation methods
IEC 61649	Goodness-of-fit tests, confidence intervals and lower confidence limits for Weibull distributed data	Goodness of fit tests – Weibull distribution
IEC 61650	Reliability data analysis techniques – Procedures for comparison of two constant failure rates and two constant failure (event) intensities	Reliability testing – statistics
IEC 61709	Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion	Reliability testing – statistics
IEC 61710	Power law model – Goodness-of-fit tests and estimation methods	Goodness of fit tests – power law model

A.2 Techniques for dependability analysis

Table A.2 shows reference standards for dependability verification and validation through analysis.

Table A.2 – Techniques for dependability verification and validation through analysis

Standard Reference	Standard Title	Analysis technique covered
IEC 60300-3-1	Dependability management – Part 3-1: Application Guide – Analysis techniques for dependability – Guide on methodology	Overview of analysis techniques
IEC 60706-2	Maintainability of equipment – Part 2: Maintainability requirements and studies during the design and development phase	Maintainability analysis
IEC 60812	Analysis techniques for system reliability – Procedure for failure modes and effects analysis (FMEA)	FMEA
IEC 61025	Fault tree analysis (FTA)	Fault Tree Analysis
IEC 61078	Analysis techniques for dependability – Reliability block diagram and boolean methods	Reliability Block Diagrams
IEC 61160	Design review	Formal design review
IEC 61165	Application of Markov techniques	Markov techniques
IEC 61703	Mathematical expressions for reliability, availability, maintainability and maintenance support terms	Mathematical expressions
IEC 61713	Software dependability through the software life cycle processes – Application guide	Software
IEC 62308	Equipment Reliability – Reliability assessment methods	Assessment methods

Annex B
(informative)

Examples of reliability, maintainability, maintenance support and availability requirements

B.1 General

Examples of dependability measures are given in Clause B.2 to Clause B.5. The values used in the examples are given only to illustrate how they may be stated in the specification. They should not be used as standardized values. Depending on the product, other measures may apply. In addition to these quantitative values the verification and validation requirements should also be specified along with the requirements for dependability management, as outlined in this standard.

NOTE For definitions of the measures see IEC 60050(191).

B.2 Availability requirements

Availability performance measure	Symbol/abbreviation	Requirement
Mean availability	$\overline{A}(t_1, t_2)$	≥ 0,9999
Mean unavailability	$\overline{U}(t_1, t_{22})$	$\leq 10^{-4}$
Mean down time	MDT	1h

B.3 Reliability requirements

Reliability performance measure	Symbol/abbreviation	Requirement
Mean failure rate	$\overline{\lambda}(t_1, t_2)$	$\leq 27 \times 10^{-6}$ / h
Mean time to failure	MTTF	≥ 37 000 h
Mean failure intensity	$\overline{z}(t_1, t_2)$	≤ 1,5 / h
Mean operating time between failures	MTBF	≥ 6 000 h
Useful life		≥ 8 years
Reliability	$R(t_1, t_2)$ $t_1 = 100$ h $t_2 = 1100$ h	≥ 0,9
NOTE The requirements state the acceptable value (contract value) which should be used to calculate the acceptance criterion for a statistical test.		

B.4 Maintainability requirements

Maintainability performance measure	Symbol/abbreviation	Requirement
Mean repair time	MRT	≤ 5 h
Mean active corrective maintenance time		≤ 5,5 h
Mean time to restoration	MTTR	≤ 7h
Fault coverage		≥ 0,95
Repair coverage		≥ 0,8

B.5 Maintenance support requirements

Maintenance support performance measure	Symbol/abbreviation	Requirement
Mean administrative delay	MAD	2 h
Mean logistic delay	MLD	1h
Spare shortage probability		0,005

Bibliography

IEC 60605-2, *Equipment reliability testing – Part 2: Design of test cycles*

IEC 60605-3-1, *Equipment reliability testing – Part 3: Preferred test conditions. Indoor portable equipment – Low degree of stimulation*

IEC 60605-3-2, *Equipment reliability testing – Part 3-2: Preferred test conditions. Equipment for stationary use in weatherprotected locations – High degree of simulation*

IEC 60605-3-3, *Equipment reliability testing – Part 3-3: Preferred test conditions – Test cycle 3: Equipment for stationary use in partially weatherprotected locations – Low degree of simulation*

IEC 60605-3-4, *Equipment reliability testing – Part 3-4: Preferred test conditions – Test cycle 4: Equipment for portable and non-stationary use – Low degree of simulation*

IEC 60605-3-5, *Equipment reliability testing – Part 3-5: Preferred test conditions – Test cycle 5: Ground mobile equipment – Low degree of simulation*

IEC 60605-3-6, *Equipment reliability testing – Part 3-6: Preferred test conditions – Test cycle 6: Outdoor transportable equipment – Low degree of simulation*

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

IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61165, *Application of Markov techniques*

IEC 61508-0, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508*

IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for E/E/PE safety-related systems*

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61508-5, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508–2 and IEC 61508–3*

IEC 61508-7, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

IEC 61650, *Reliability data analysis techniques – Procedures for comparison of two constant failure rates and two constant failure (event) intensities.*

IEC 61709, *Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion*

Other publications

[1] Def Stan 00-42 (Part 3) Issue 2. Reliability & Maintainability (R&M) Assurance Guidance. R&M Case. DStan, Glasgow available from www.dstan.mod.uk

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 Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – 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 la CEI"). 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI 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 la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
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 la CEI, 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 la CEI, 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 la CEI ou de toute autre Publication de la CEI, 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 la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme Internationale CEI 60300-3-4 a été établie par le comité d'études 56 de la CEI : Sûreté de fonctionnement.

Cette deuxième édition annule et remplace la première édition parue en 1996 et constitue une révision technique.

Les modifications majeures par rapport à l'édition précédente sont les suivantes:

– le concept de système a été introduit et la nécessité de spécifier la sûreté de fonctionnement du système et non uniquement celle des équipements physiques est mise en évidence ;
– la nécessité de la vérification et de la validation des exigences a été introduite ;
– une différenciation est apportée entre les exigences qui peuvent être mesurées, vérifiées et validées et les objectifs qui eux, ne le peuvent pas ;

– le contenu du support de disponibilité, de maintenabilité et de maintenance a été mis à jour et étendu à un niveau de détail similaire à celui du support de fiabilité.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1212/FDIS	56/1233/RVD

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

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 60300, sous le titre général *Sûreté de fonctionnement,* est disponible sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

Pour de nombreux systèmes, la fiabilité, la maintenabilité et la disponibilité constituent des caractéristiques essentielles de la performance. Ces caractéristiques, ainsi que la performance du support de maintenance sont reconnues collectivement sous le concept de sûreté de fonctionnement.

Dans des systèmes où chacune des composantes de la sûreté de fonctionnement est importante, il est nécessaire que ces caractéristiques soient définies et spécifiées de la même façon que les autres caractéristiques du système telles que les performances techniques, les dimensions et la masse.

Les niveaux de fiabilité, de maintenabilité, de disponibilité et de performance du support de maintenance atteints par un système dépendent des conditions sous lesquelles le système est utilisé et aussi du profil de mission du système. Lorsque des exigences pour les caractéristiques de sûreté de fonctionnement sont spécifiées, il est nécessaire de définir les conditions de stockage, de transport, d'installation et d'utilisation qui seront appliquées au système. Il peut être important de prendre en compte non seulement les conditions dans lesquelles le système fonctionnera mais aussi la politique de maintenance et l'organisation du support de maintenance pour le système.

Afin d'évaluer les valeurs des caractéristiques de sûreté de fonctionnement atteintes, il est nécessaire d'appliquer des méthodes statistiques.

Comme d'autres caractéristiques de performance, les caractéristiques de sûreté de fonctionnement peuvent être spécifiées selon trois voies différentes:

1) spécifications produites par le fournisseur ;
2) spécifications fournies par le client ;
3) spécifications agréées mutuellement ou produites par le fournisseur et le client.

La présente norme est applicable aux trois types de spécification.

La présente norme complète la CEI 62347 qui traite des définitions des systèmes et de leurs éléments constituants et comment définir ceux-ci de sorte que les exigences de sûreté de fonctionnement de chaque élément puissent être spécifiées en utilisant la présente norme. Le principe de la CEI 62347 est d'identifier par fonction les exigences applicables aux systèmes du point de vue de l'ingénierie du système. Cela donne un processus de transformation du point de vue du client sur les applications du système en une vision technique de l'ingénierie du système. La CEI 62347 met l'accent sur la conception architecturale et fonctionnelle dans la réalisation de fonctions avec une sélection appropriée du matériel, du logiciel et des éléments humains pour accéder aux exigences de sûreté de fonctionnement du système pertinentes pour les besoins du client.

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 la CEI 60300 donne des lignes directrices sur la façon de définir les caractéristiques de sûreté de fonctionnement dans des spécifications, avec des spécifications des procédures et critères pour la vérification et la validation.

Les lignes directrices fournies incluent:

– des conseils sur la façon de spécifier quantitativement et qualitativement les exigences de fiabilité, de maintenabilité, de disponibilité et de support de maintenance ;

– des conseils à l'attention des clients d'un système sur la façon de s'assurer que les exigences spécifiées seront respectées par les fournisseurs ;

– des conseils à l'attention des fournisseurs pour les aider à respecter les exigences des clients.

D'autres documents tels que des règlements législatifs ou gouvernementaux peuvent aussi apporter des exigences pour les systèmes et celles-ci doivent être appliquées en plus de toutes les spécifications établies conformément à la présente norme.

NOTE 1 Bien que principalement dédiées aux systèmes et à la fiabilité au niveau du système et des équipements, beaucoup des techniques décrites dans les différentes parties de la série CEI 60300 peuvent aussi être appliquées aux produits, aux entités ou au niveau des composants. Le terme << système >> est systématiquement utilisé dans la présente norme.

NOTE 2 La présente norme ne donne pas de recommandations pour la gestion des programmes de sûreté de fonctionnement ou sur les diverses activités nécessaires pour tenir une disponibilité, une fiabilité, une maintenabilité ou des exigences de support de maintenance établis. Pour ces recommandations générales, voir les autres normes.

NOTE 3 Les spécifications de sécurité et environnementales ne sont pas directement considérées dans le présent document. La plupart des recommandations de la présente norme peuvent aussi être appliquées à la spécification de sécurité ou environnementale.

NOTE 4 Les spécifications pour la sûreté de fonctionnement d'un service ne sont pas traitées dans ce document. Ceci inclut la disposition d'un service tel que ceux fournis à travers des partenariats de fourniture public-privé.

2 Références normatives

Les documents référencés suivants sont indispensables pour l'application de ce document. Pour des références datées, seule l'édition citée s'applique. Pour les références non datées, c'est la dernière édition du document référencé (y compris les amendements) qui s'applique.

CEI 60050-191, *Vocabulaire Electrotechnique International (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60300-1, *Gestion de la sûreté de fonctionnement – Partie 1: Gestion du programme de sûreté de fonctionnement*

CEI 60300-2, *Gestion de la sûreté de fonctionnement – Partie 2: Lignes directrices pour la gestion de la sûreté de fonctionnement*

CEI 60300-3-1, *Gestion de la sûreté de fonctionnement – Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique*

CEI 60300-3-2, *Gestion de sûreté de fonctionnement – Partie 3-2: Guide d'application – Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation*

CEI 60300-3-3, *Gestion de la sûreté de fonctionnement – Partie 3-3: Guide d'application – Evaluation du coût du cycle de vie*

CEI 60300-3-5, *Gestion de la sûreté de fonctionnement – Partie 3-5: Guide d'application – Conditions des essais de fiabilité et principes des essais statistiques*

CEI 60300-3-10, *Gestion de la sûreté de fonctionnement – Partie 3-10: Guide d'application – Maintenabilité*

CEI 60300-3-12, *Gestion de la sûreté de fonctionnement – Partie 3-12: Guide d'application – Soutien logistique intégré*

CEI 60300-3-14, *Gestion de la sûreté de fonctionnement – Partie 3-14: Guide d'application – Maintenance et support de maintenance*

CEI 60605-4, *Essai de fiabilité des équipements – Partie 4: Méthodes statistiques de distribution exponentielle – Estimateurs ponctuels, intervalles de confiance, intervalles de prédiction et intervalles de tolérance*

CEI 60605-6, *Essais de fiabilité des équipements – Partie 6: Tests pour la validité et l'estimation du taux de défaillance constant et de l'intensité de défaillance constante*

CEI 60706-2, *Maintenabilité de matériel – Partie 2: Exigences et études de maintenabilité pendant la phase de conception et de développement*

CEI 60706-3, *Maintenabilité de matériel – Partie 3: Vérification et recueil, analyse et présentation de données*

CEI 60706-5, *Guide de maintenabilité de matériel – Partie 5: Essais pour diagnostic*

CEI 61014, *Programmes de croissance de fiabilité*

CEI 61025, *Analyse par arbre de panne (AAP)*

CEI 61070, *Procédures d'essai de conformité pour la disponibilité en régime établi*

CEI 61078, *Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthodes booléennes*

CEI 61123*, Essai de fiabilité – Plans d'essai de conformité pour une proportion de succès*

CEI 61124, *Essais de fiabilité – Plan d'essais de conformité d'un taux de défaillance constant et d'une intensité de défaillance constante*

CEI 61160, *Revue de conception*

CEI 61164, *Croissance de la fiabilité – Tests et méthodes d'estimation statistiques*

CEI 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 61649, *Procédures pour les tests d'adéquation, les intervalles de confiance et les limites inférieures de confiance pour les données suivant la distribution de Weibull*

CEI 61703, *Expressions mathématiques pour les termes de fiabilité, de disponibilité, de maintenabilité et de logistique de maintenance*

CEI 61710, *Modèle de loi en puissance – Test d'adéquation et méthodes d'estimation des paramètres*

CEI 61713, *Sûreté de fonctionnement des logiciels pendant leurs processus de cycle de vie – Guide d'application*

CEI 62198, *Gestion des risques liés à un projet – Lignes directrices pour l'application*

CEI 62308, *Fiabilité de l'équipement – Méthodes d'évaluation de la fiabilité*

CEI 62347, *Lignes directrices pour les spécifications de sûreté de fonctionnement des systèmes*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans la CEI 60050-191 s'appliquent ainsi que ce qui suit.

NOTE Les définitions de « sûreté de fonctionnement », « disponibilité (performance) », « fiabilité (performance) », « maintenabilité (performance) », « support de maintenance », « défaillance », « panne », « élément », « temps avant défaillance » et « temps de fonctionnement entre défaillances » sont données dans la CEI 60050-191.

3.1
vérification
confirmation, au moyen de dispositions de démonstration d'atteinte d'objectifs, que les exigences spécifiées ont été respectées

[ISO 9000:2005, définition 3.8.4 modifiée]

NOTE 1 Dans le contexte de la présente norme, la vérification est l'activité de démonstration pour chaque phase du cycle de vie pertinent, par analyses et/ou essais, que, pour des conditions d'entrée spécifiques, les produits livrables sont conformes dans tous les aspects aux objectifs et exigences établis pour la phase spécifique.

NOTE 2 Exemples d'activités de vérification:

– revues des sorties (documents de toutes les phases du cycle de vie) pour garantir la conformité aux objectifs et exigences de la phase, en prenant en compte les entrées spécifiques de cette phase ;
– revues de conception ;
– essais et analyses réalisés sur les systèmes pour garantir que leur performance est conforme aux spécifications ;
– essais d'intégration réalisés quand différentes parties d'un système sont assemblées ensemble selon un processus étape par étape et par la réalisation d'essais d'environnement pour garantir que toutes les parties fonctionnent ensemble.

3.2
validation
confirmation au moyen de dispositions de démonstration d'atteinte d'objectifs que les exigences pour une utilisation spécifique prévue ont bien été respectées

[ISO 9000:2005, définition 3.8.5 modifiée]

NOTE La validation est l'activité de démonstration que le système à l'étude, avant et après installation est conforme en tout point à la spécification d'exigence de ce système. Ainsi par exemple, la validation logicielle signifie la confirmation par examen et dispositions de démonstration d'atteinte d'objectifs que le logiciel répond à la spécification d'exigences du logiciel.

4 Considérations générales sur les spécifications de sûreté de fonctionnement

4.1 Le besoin en sûreté de fonctionnement

Tous les systèmes montrent un certain niveau de sûreté de fonctionnement; néanmoins souvent cela signifie défaillance ou besoin de maintenance. Cependant, si un système est défaillant trop souvent, cela signifie qu'il peut ne pas être disponible pour travailler au moment voulu ou qu'il peut coûter trop cher en maintenance. De plus, les systèmes trop souvent défaillants acquièrent une mauvaise réputation chez l'utilisateur et il est peu probable qu'ils soient à nouveau achetés lors d'un remplacement. D'un autre côté, concevoir et fabriquer des systèmes de haut niveau de fiabilité est coûteux et il peut ne pas être possible de produire de tels systèmes à un prix compétitif. Il y a donc un équilibre à établir entre des systèmes de faible fiabilité et coûteux en maintenance et des systèmes de haute fiabilité qui sont coûteux à concevoir et à construire. Ceci est démontré dans la Figure 1 qui illustre les coûts de conception et d'utilisation pour des systèmes de fiabilités différentes.

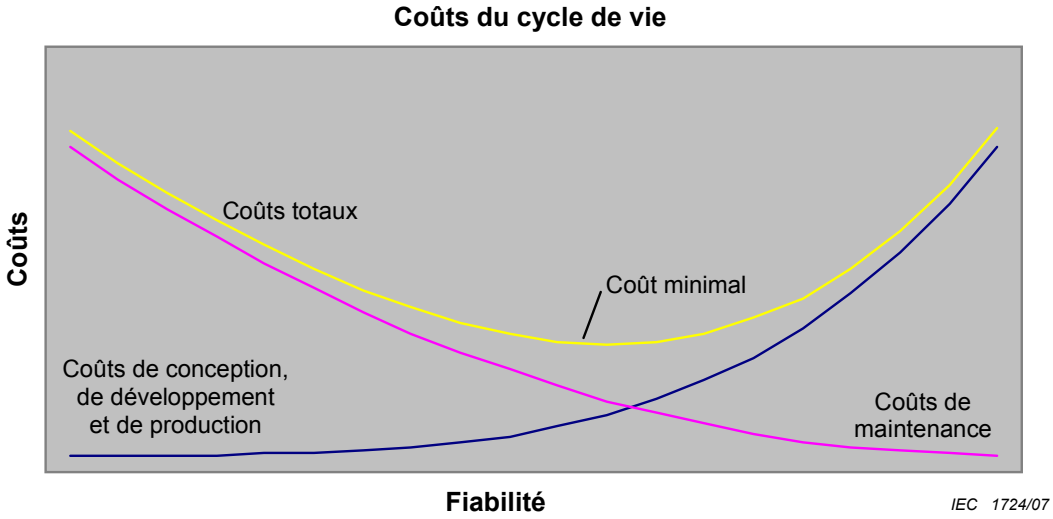

Figure 1 – Relation entre coût et fiabilité

La Figure 1 montre qu'il existe un niveau optimal de fiabilité pour lequel les coûts du cycle de vie du système sont minimaux. Si un système est disponible dans le commerce (sur étagère) ce niveau optimal sera modifié parce que les coûts de la conception et du développement peuvent être partagés entre différentes unités. Cependant, la fiabilité optimale d'un système peut être tributaire d'autres facteurs tels que les exigences de sécurité ou la fonction du système et elle ne sera pas nécessairement la fiabilité correspondant au coût optimal du cycle de vie.

Il est probablement vrai que des systèmes produits par des organisations qui ne gèrent pas activement la sûreté de fonctionnement atteignent des niveaux de fiabilité bien en dessous du point optimal. Un effort d'investissement dans la conception et la construction de la sûreté de fonctionnement peut donc être payant en termes de coûts combinés de développement, de fabrication et de fonctionnement du système. La CEI 60300-3-3 décrit les coûts du cycle de vie et la relation entre la sûreté de fonctionnement et le coût.

La sûreté de fonctionnement comprend un nombre d'attributs qui sont spécifiés différemment sous quatre rubriques, comme il est indiqué ci-après:

– disponibilité ;
– fiabilité (R(t)), incluant le temps moyen avant défaillance (MTTF), le temps moyen de fonctionnement entre défaillances (MTBF), les paramètres de la loi de Weibull ou de la loi en puissance ;

– maintainabilité, incluant le temps de non-disponibilité et le temps moyen avant remise en état (MTTR) ;
– support de maintenance.

Il convient que les caractéristiques de sûreté de fonctionnement sélectionnées pour la spécification soient en rapport avec le type de système et l'application prévue. Par exemple, seules les exigences de fiabilité nécessitent d'être spécifiées si aucune action de maintenance n'est prévue.

Les exigences de performance de disponibilité sont généralement spécifiées pour des systèmes où le temps de non-disponibilité peut provoquer des pertes économiques, ou autres, par le biais des coûts d'exploitation accrus ou des dommages corporels ou de pertes de service, par exemple pour des grands systèmes, des usines de production, des équipements médicaux, des équipements de sécurité et des systèmes militaires. La performance de disponibilité peut être calculée à partir de la configuration du système, de ses sous-systèmes et de leurs exigences de performance de fiabilité et de performance de maintenabilité, si elles sont établies et en prenant en compte la performance du support de maintenance.

Il convient que les exigences de performance de maintenabilité soient spécifiées pour les systèmes si les coûts de maintenance contribuent significativement au coût du cycle de vie ou si la maintenance est importante pour le client. Les exigences de maintenance préventive et corrective peuvent être spécifiées le cas échéant.

NOTE Le niveau du support de maintenance est très souvent déterminé par les conditions d'utilisation et il n'est pas une exigence intrinsèque du système lui-même.

Les Articles 6, 7, 8 et 9 contiennent d'autres informations sur le moment auquel chaque caractéristique de sûreté de fonctionnement est la plus appropriée.

Les niveaux de performance de sûreté de fonctionnement atteints par un système sont fortement influencés par les conditions dans lesquelles il est conçu, développé, installé et exploité. La sûreté de fonctionnement est donc liée aux autres attributs tels que la qualité et le processus de conception et de fabrication. Il convient donc que la spécification de la sûreté de fonctionnement soit une partie de la spécification totale du système et que l'interaction entre les différents attributs soit identifiée et prise en compte.

4.2 Exigences et objectifs

Il est important de bien faire une distinction entre des exigences formelles exprimées dans une spécification et des objectifs car la méthode d'acceptation est différente.

Une exigence fait partie de la spécification que le client considère qu'il est nécessaire que le système respecte et pour laquelle le fournisseur doit apporter la preuve. Cette preuve peut être fournie avant que le système entre en service, comme faisant partie des produits livrables ou bien une fois que le système est en service, par le biais de primes d'objectif ou de pénalités liées à la tenue des exigences.

Un objectif n'est pas une exigence mais un souhait ou une aspiration du client, que la preuve de l'atteinte de l'objectif soit fournie ou non.

Pour des systèmes de haute disponibilité ou de haute fiabilité, la preuve formelle de l'atteinte du haut niveau de disponibilité ou de fiabilité peut ne pas être réalisable. Le client exigera à la fois des objectifs de haute disponibilité et de haute fiabilité pour lesquels la preuve ne pourra être apportée et des exigences moins élevées pour lesquelles la preuve peut être apportée et clarifiera la distinction entre les deux.

4.3 Systèmes

Il convient que la spécification de la sûreté de fonctionnement porte sur le système. Un système comprend l'équipement (matériel et logiciel) tout autant que les personnes qui exploiteront et maintiendront le système, ainsi que les procédures utilisées pour l'exploitation et la maintenance. Le système intègre aussi l'environnement dans lequel se fera l'exploitation, comme cela est illustré dans la Figure 2.

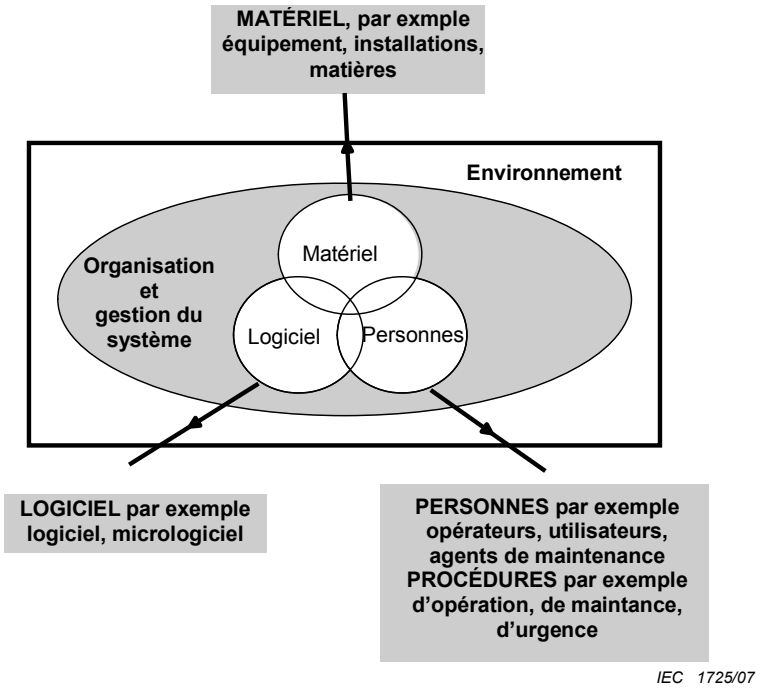

Figure 2 – Eléments du système

Lorsque cela est possible, il convient que tous les éléments d'un système soient pris en compte dans la spécification de la sûreté de fonctionnement, parce qu'une modification de l'un d'entre eux peut avoir un effet significatif sur la sûreté de fonctionnement du système obtenue. Par exemple, certains opérateurs du système peuvent mal l'utiliser ou être plus agressifs dans leur utilisation et conduire à plus de défaillances et donc obtenir une fiabilité plus faible. Cependant, il peut y avoir des instances où le fournisseur et le client ont peu ou pas de contrôle sur les procédures de maintenance ou les compétences, telles qu'un système dans un moteur de voiture une fois vendue à son utilisateur final. Il convient que les exigences de la sûreté de fonctionnement admettent les circonstances particulières du système dont la spécification a été établie.

De plus, il convient que les exigences de sûreté de fonctionnement soient liées au profil opérationnel ou d'utilisation ou aux exigences fonctionnelles du système. Le système peut être défini en accord avec la CEI 62347 qui donne des détails sur la façon de définir un système, ses éléments et la criticité de chaque fonction afin que les exigences de chaque élément puissent être spécifiées.

Il convient que la spécification de la sûreté de fonctionnement d'un système inclue la spécification du logiciel et des éléments humains au même titre que les exigences du matériel. Les recommandations de la présente norme peuvent être appliquées à différents aspects de la spécification des logiciels mais des recommandations spécifiques sont données dans la CEI 61713 et dans les normes pertinentes de la série 61508.

Des systèmes sont présents à différents niveaux et tout système peut être lui-même constitué d'autres systèmes, souvent identifiés comme étant des systèmes de systèmes. Par exemple, un autobus est un système constitué d'un véhicule motorisé, d'un conducteur et de

procédures de conduites. Le véhicule est composé de sous-systèmes qui sont eux-mêmes autant de systèmes, par exemple le moteur ou la boîte de vitesse sur laquelle l'action de l'opérateur implique le levier de vitesse. Les sous-systèmes sont constitués de composants et d'équipements qui peuvent eux-mêmes être considérés comme des systèmes et analysés en conséquence. Ceci inclut l'interaction avec les personnes qui utilisent le sous-système, comment ils le font et la manière selon laquelle différentes personnes peuvent soumettre le système à différentes contraintes opérationnelles, par exemple des conducteurs différents conduiront différemment et soumettront la boîte de vitesse à des charges plus ou moins fortes.

Le client peut établir les exigences uniquement au niveau le plus haut du système ou il peut décider qu'il est important que l'un des sous-systèmes n'ait pas une contribution dominante dans la fiabilité atteinte, et donc aussi établir des exigences à des niveaux plus bas. Ces exigences de niveau plus bas doivent rester cohérentes avec les exigences du niveau plus haut et elles doivent être mesurables et atteignables ou bien elles seront des objectifs et non des exigences. Par exemple, la contribution du sous-système à la sûreté de fonctionnement globale du système doit être estimée avant que les exigences soient réparties aux sous-systèmes. Cependant, cette répartition entre les sous-systèmes de niveau plus bas n'est pas directe sauf dans les systèmes « série » où tous les sous-systèmes ont un taux de défaillance constant. Dans les autres cas tels que les systèmes redondants ou bien quand le taux de défaillance varie dans le temps, se référer aux normes telles que la CEI 61025 et la CEI 61078. La CEI 60300-3-1 et la CEI 61703 donnent d'autres recommandations sur l'analyse de la sûreté de fonctionnement des systèmes.

Le type et la nature d'un système affectent la spécification de la sûreté de fonctionnement. Ceci est vrai pour les systèmes réparables, les systèmes non réparables et les dispositifs à utilisation unique. Les systèmes réparables sont ceux où les défaillances peuvent être réparées et où le système est rétabli dans un état opérationnel. Sont des exemples de systèmes non réparables les systèmes scellés, les systèmes disponibles dans le commerce (COTS), les systèmes pour lesquels les frais de réparation dépassent le coût de remplacement, tels que beaucoup de biens de grande consommation, et les systèmes situés dans des endroits éloignés où la compétence et les pièces de rechange ne sont pas disponibles à temps. Les dispositifs à utilisation unique comprennent les explosifs, les air-bags de passager et les casques de sécurité.

Les systèmes non réparables doivent être remplacés plutôt que réparés et les exigences de maintenabilité et de support de maintenance sont fondamentalement différentes. De plus, le MTBF ne sera pas une mesure pertinente pour les dispositifs à utilisation unique, où la mesure correcte pourra être soit la fiabilité, soit la probabilité d'activation prématurée. Le client doit s'assurer que la nature du système et l'effet qu'elle peut avoir sur les exigences de la sûreté de fonctionnement sont identifiés avant que la spécification soit écrite.

4.4 Démonstration de l'atteinte des exigences

4.4.1 Concept

Pour toute spécification, il y a deux éléments: les exigences de performance de sûreté de fonctionnement et les moyens par lesquels le fournisseur démontrera au client la conformité aux exigences. Ceci signifie que le fournisseur doit fournir au client les preuves suffisantes de la conformité du système aux exigences applicables, afin d'apporter au client la confiance nécessaire pour justifier le paiement du prix convenu. Fournir une preuve de plus a un coût et c'est un élément justifiant le coût plus élevé d'un système de plus haute fiabilité (voir Figure 1) mais, sans ces activités, il reste la possibilité que le système ne soit pas conforme à ses exigences.

La vérification et la validation sont deux éléments majeurs. Elles sont définies dans l'ISO 9000 et utilisées dans l'industrie du matériel et dans celle du logiciel comme partie du processus de développement ou modèle «en V» (voir la CEI 61508) et elles peuvent être expliquées selon ce qui suit. La vérification est le processus de fourniture de la preuve que le système, à chaque phase du cycle de vie, est conforme aux exigences des précédentes

phases de son cycle de vie. La validation est le processus de fourniture de la preuve que le système est conforme aux exigences réelles, qui peuvent ne pas toujours être reflétées dans la spécification écrite. Les deux sont des éléments essentiels.

Le niveau de vérification et de validation requis par le client dépend de la confiance qu'il a dans la faculté du système à atteindre les niveaux de sûreté de fonctionnement spécifiés. Si le client veut maintenir un système lorsqu'il est défaillant en utilisation, alors un niveau plus faible de preuve et donc de confiance dans l'atteinte de la sûreté de fonctionnement peut être acceptable. Ceci résulte du fait que les dispositions de preuve ont un coût et que le client peut accepter de prendre le risque que le système n'ait pas la performance exigée. Le client doit décider des risques qui sont acceptables quand il spécifie les exigences de vérification et de validation (voir la CEI 62198 pour plus d'informations sur la gestion des « risques projets »).

Pour être efficaces, les activités de vérification et de validation doivent être planifiées et systématiques. Ceci requiert du fournisseur qu'il établisse à l'avance les activités et qu'il obtienne du client un accord, souvent par l'intermédiaire d'un contrat. Il convient que les exigences de la sûreté de fonctionnement considèrent les différents facteurs qui probablement affecteront le coût de la vérification et de la validation de la sûreté de fonctionnement. Ceci comprend les durées de vie prévues et le démantèlement ou le recyclage du système.

Pour un approvisionnement sur le long terme, des activités peuvent être planifiées plusieurs années avant leur exécution et, en fonction des termes contractuels, le client peut avoir un contrôle limité sur elles jusqu'à la fin du projet. Une voie pour réduire le risque-projet pour le client et le fournisseur que constitue l'éventualité que le système ne puisse pas fournir le niveau de preuve requis peut être une disposition progressive de vérification et de validation. Les activités sont alors planifiées tout au long du cycle de vie et les résultats sont fournis au client à des points-clés du projet. De cette façon, le fournisseur établit progressivement la confiance dans le système tout au long du projet et il y a ainsi moins de risques que le niveau de confiance soit inadéquat.

Un modèle utilisé par le fournisseur pour apporter au client la preuve que le système est conforme à ses exigences est le « Reliability and Maintainability Case » (généralement appelé « R&M Case »). Le « R&M case » apporte une argumentation rationnelle auditable sur le fait que le système est conforme à ses exigences et ce statut est validé en différents points-clés du projet dans le rapport « R&M Case ». Le « R&M Case » est généralement utilisé pour apporter progressivement la preuve et il est publié à certains points-clés du projet. La norme de la défense britannique 00-42 Part 3 [1] contient d'autres recommandations de l'application de la philosophie « R&M Case ».

4.4.2 Activités

La vérification et la validation couvrent un nombre d'activités conçues pour apporter la preuve qu'un système est conforme à ses exigences de sûreté de fonctionnement. Ces activités peuvent être obtenues au moyen de différentes techniques qui ont un objectif global identique ou similaire mais en suivant des méthodes différentes. Le choix des techniques dépend de nombreux facteurs et il est étudié dans la CEI 60300-3-1.

Lorsqu'un client exige que la vérification et la validation soient produites, le fournisseur doit déterminer l'objet de l'activité et sa contribution à la vérification et à la validation. Par exemple, une spécification peut ne pas exiger la réalisation d'une analyse par arbre de panne (AAP) mais elle peut appeler une analyse pour déterminer les combinaisons d'événements qui peuvent conduire à une défaillance du système, de même un bloc-diagramme de fiabilité (BDF) peut être une technique également valide pour atteindre le même objectif. Le choix de la technique pour mener à terme une activité peut être laissé à la discrétion du fournisseur, mais en considérant 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 peut être préférable à une AAP mal menée par un analyste inexpérimenté.

Les activités de vérification et de validation comprennent:

a) analyses:
   1) conformité aux normes, réglementations et recommandations ;
   2) revues d'experts / meilleures pratiques / certification;
   3) calculs utilisés auparavant pour d'autres conceptions (par exemple, analyses par éléments finis pour les contraintes, la fatigue) ;
   4) simulation (par exemple pour les performances du système) ;
   5) analyse de sûreté de fonctionnement.
b) essais et démonstration:
   1) performance dans des utilisations précédentes, pour des produits 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, d'endurance à la fatigue, essais de logiciels sur le système, essais au niveau de modules ou de composants).

Plus de détails sur les techniques de vérification et de validation de la sûreté de fonctionnement sont donnés dans d'autres normes de la série CEI 60300 et une liste de normes CEI pertinentes est fournie en Annexe A.

Ces activités ne sont pas toutes appropriées à toutes les phases du cycle de vie. Les essais portant sur le système ne peuvent pas être effectués tant que le système n'a pas été conçu et qu'un prototype n'a pas été construit. 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. Cependant, il convient que les essais sur le système soient planifiés à l'étape de la conception de sorte que le fournisseur puisse déterminer les essais requis sur les sous-systèmes avant que le système soit construit. De plus, il convient que le système soit conçu en vue de sa testabilité, c'est-à-dire qu'il convient que le système et les sous-systèmes soient conçus de sorte qu'ils puissent être testés (voir la CEI 60706-5).

Il convient de noter que toute preuve apportée pendant le développement est une prédiction de la performance de sûreté de fonctionnement probable et que les résultats de l'analyse sont probablement moins précis que des résultats d'essai. Le client ne souhaitera donc pas forcément se fonder uniquement sur des résultats d'analyse et il pourra exiger une combinaison d'activités d'analyse et d'essai pour que la preuve de la conformité des exigences soit apportée. De plus, l'environnement et l'utilisation du système doivent être pris en compte lors de la planification des essais. Dans les cas pour lesquels les essais sont réalisés dans des conditions proches de celles de l'exploitation, l'essai donnera une bonne estimation de la sûreté de fonctionnement, mais l'essai exigera au moins une longue durée, un nombre élevé d'exemplaires en essai et un faible nombre de défaillances conduira à une grande incertitude associée à l'estimation de la sûreté de fonctionnement. Si l'essai est accéléré, la taille de l'échantillon peut être réduite. Le nombre plus élevé de défaillances réduira l'incertitude statistique mais l'incertitude technique sera plus élevée parce que l'essai accéléré peut provoquer des modes de défaillance qui ne sont pas pertinents en exploitation.

4.5 Contrat traitant de la sûreté de fonctionnement

L'objet de toute spécification est de fournir une base à l'acquéreur d'un système. La spécification sera généralement une partie du contrat entre l'acquéreur et le fournisseur et il

est donc essentiel que la spécification soit écrite de telle sorte qu'elle puisse être utilisée pour passer un contrat. Un contrat portant sur la sûreté de fonctionnement peut prendre différentes formes, des paiements à des points-clés dépendant de la conclusion satisfaisante d'un essai de démonstration à la mise en place de clauses de pénalités et de primes en regard de la fiabilité atteinte en exploitation.

Il est important de bien distinguer les exigences, qui détaillent comment il convient que le système fonctionne et les spécifications écrites qui détaillent ce que le système contient. En fonction de la nature du système, elles peuvent être de différents niveaux de complexité et elles peuvent être produites soit par le client, soit par le fournisseur. Chacun peut utiliser les recommandations de la présente norme.

Lors de la rédaction des clauses contractuelles relatives à la sûreté de fonctionnement, une grande attention doit être portée au sens des clauses et à leur portée contractuelle. Par exemple, une clause dans un contrat portant sur un dispositif à utilisation unique peut exiger une fiabilité de 99,5 %. Le contrat peut exiger aussi un essai de démonstration complète de la fiabilité avec un niveau de confiance de 80 %. Ceci nécessitera un minimum de 322 essais, soit six fois plus que les 50 exemplaires qu'il est prévu de commander. Puisque le système a été conçu en vue d'un dispositif à utilisation unique, c'est clairement une exigence irréaliste et le client doit trouver des méthodes alternatives pour obtenir la vérification et la validation requises, soit au moyen d'objectifs de fiabilité moins élevés pour lesquels la preuve pourra être apportée, soit par analyse, simulation ou essais de sous-systèmes.

Le choix des activités de vérification et de validation à appeler dans un contrat dépend du niveau de risques du projet que le client est prêt à accepter. Si le client accepte de prendre le risque que le système puisse être défaillant et alors être maintenu par le fournisseur, alors l'application de pénalités pour performance trop faible et de primes pour exigences dépassées peut s'avérer être la meilleure méthode. Si cependant le client n'accepte pas le risque d'indisponibilité du système, alors des essais de démonstration formelle de la fiabilité ou de la disponibilité peuvent être nécessaires. Il convient de porter attention aux événements rares car leur absence peut rarement être prouvée par des essais.

Le bénéfice de chaque approche peut être:

a) les pénalités pour performance insuffisante encourageront le client à porter sa pleine attention à la sûreté de fonctionnement et cela peut conduire à des niveaux plus élevés de la sûreté de fonctionnement que ce qui serait obtenu autrement ;

b) les essais de démonstration sont coûteux et nécessitent du temps, et ils peuvent révéler juste avant la date de mise en service, que le système n'est pas conforme à ses exigences de sûreté de fonctionnement ;

c) exiger du fournisseur la fourniture d'une maintenance suppose un contrat à bien plus long terme, par exemple un accord sur un coût fixe de maintenance avec les difficultés associées mais le fournisseur prend alors le risque que le système est une fiabilité faible.

Si une spécification de sûreté de fonctionnement doit être la base d'un contrat, il est essentiel que la spécification soit complète afin de prévenir tout désaccord une fois que le contrat est applicable. Des types d'éléments à inclure dans une spécification utilisée pour un contrat, sont par exemple:

– les critères précis et bien définis par lesquels la disponibilité, la fiabilité, la maintenabilité ou la supportabilité seront jugées ;

– les obligations et responsabilités du client, du fournisseur et de toute tierce-partie ;

– le système considéré, par exemple le système, l'équipement ou l'assemblage auxquels les exigences s'appliquent ;

– la fonction prévue pour le système ;

– les diverses conditions d'exploitation et environnementales dans lesquelles le système est utilisé, y compris le cas échéant la durée dans chaque condition ;

– la définition de la défaillance ou du critère de défaillance, par exemple si cela correspond à la défaillance totale du système, à la perte de fonctions essentielles, à une défaillance partielle ou à une dégradation de la performance d'un fonction ;
– comment le système sera installé et utilisé ;
– les qualifications et responsabilités du personnel en charge du fonctionnement et de la maintenance du matériel, du logiciel et de la documentation ;
– la politique de maintenance à appliquer, les procédures associées et les dispositions de support ;
– les méthodes prévues pour la vérification et la validation de la conformité aux exigences, y compris les critères d'acceptation / rejet ;
– les sources de données acceptables pour toute analyse technique.

Afin de réduire le nombre de défaillances et la durée d'indisponibilité du système, il est nécessaire que le client et le fournisseur coopèrent dans toutes les phases du cycle de vie du système. Ceci crée des obligations diverses de la part de chacun qu'il convient de spécifier. Un programme formel de gestion de la fiabilité et de la maintenabilité (voir la CEI 60300-1) peut aider à identifier et spécifier ces activités.

Quand cela est possible, il convient de spécifier que le client ou le distributeur accepte la responsabilité de la surveillance de la fiabilité en exploitation et communique l'expérience de l'exploitation (bonne ou mauvaise) à ses fournisseurs.

4.6 Types de spécification

La nature du système en cours de fourniture a un effet fondamental sur la manière d'écrire la spécification. Il y a trois types principaux:

– les spécifications rédigées par le fournisseur :

  elles sont surtout utilisées pour des systèmes qui nécessitent certaines caractéristiques de sûreté de fonctionnement, par exemple la fiabilité, afin d'être acceptés sur le marché ;

– les spécifications rédigées par le client :

  elles sont surtout utilisées pour les systèmes standards qui doivent être conformes à certaines caractéristiques de sûreté de fonctionnement afin de satisfaire les besoins du client ;

– les spécifications agréées mutuellement ou écrites par le fournisseur et le client :

  elles sont normalement utilisées dans le cas de systèmes dédiés à un client ou à des conceptions existantes mais modifiées.

Les systèmes dédiés à un client sont ceux pour lesquels le client spécifie les exigences et le fournisseur conçoit, développe et produit un système afin qu'il soit conforme aux exigences. Si cependant le fournisseur établit que des systèmes sont disponibles et que le client choisit le système qui s'approche le plus de ses exigences, ceci est appelé "disponible sur étagère", « matériel disponible dans le commerce » ou COTS. Dans ce cas, il n'y a pas de modifications au système standard disponible dans le commerce. En pratique, la plupart des fournitures majeures seront une combinaison d'éléments dédiés au client et d'éléments disponibles sur étagère et la spécification sera mutuellement agréée entre le client et le fournisseur.

Des systèmes dédiés à un client sont, par exemple, un achat militaire d'un char d'assaut (où plusieurs systèmes sont utilisés uniquement sur des véhicules militaires) ou une centrale nucléaire. A contrario, les machines à laver et les systèmes de technologie de l'information de bureau sont des exemples de COTS.

Pour un système dédié à un client, celui-ci spécifiera le niveau et les types de vérification et de validation que le fournisseur doit fournir pour démontrer que les exigences ont été respectées. Cette vérification et cette validation incluront des preuves d'essai et d'analyse mais comme le système sera construit uniquement pour ce client, on ne pourra pas apporter

la preuve d'une utilisation du système dans son environnement d'exploitation, sauf après l'achat. Le fournisseur inclut alors le coût de ces activités de vérification et de validation dans le prix du système et le client peut déterminer la preuve requise conformément aux risques acceptables dans son affaire. Cependant, le client saura que le système est conçu et développé dans le but d'être conforme aux exigences.

Pour un système COTS, le fournisseur établit ce qui est disponible et peut fournir une preuve standard de la tenue de certains niveaux de performance de sûreté de fonctionnement par le système, ce qui peut inclure des données en exploitation d'applications antérieures. Cependant l'opportunité de fournir la vérification et la validation est limitée et beaucoup de fournisseurs ne voudront pas fournir des données en exploitation qui sont considérées sensibles du point de vue commercial.

Du fait de la réduction des coûts de développement et du niveau des activités de vérification et de validation, les coûts des systèmes COTS sont bien moins élevés que ceux des systèmes dédiés à un client. C'est pour cette raison que beaucoup de clients établissent maintenant que les exigences seront respectées par l'utilisation de systèmes COTS, acceptant par là que ces systèmes ne respectent pas exactement les exigences.

Cependant, si le client exige des modifications au système COTS, ce dernier ne peut plus être considéré comme tel, puisque les modifications peuvent avoir des effets significatifs sur la sûreté de fonctionnement obtenue. Le client doit donc porter attention au fait qu'un système COTS est réellement inchangé et que la preuve apportée est pertinente. Si des modifications sont demandées, les effets de ces modifications sur la performance de sûreté de fonctionnement doivent être étudiés en détail et une vérification et une validation complémentaires doivent être demandées par le client, si cela est nécessaire.

4.7 Origine des spécifications de sûreté de fonctionnement

Il convient autant que possible d'exprimer quantitativement toutes les exigences de fiabilité, de maintenabilité et de disponibilité, mais il peut être aussi pertinent de spécifier des exigences qualitatives dans les spécifications. Les exigences quantitatives sont uniquement pertinentes quand l'exigence à spécifier peut être mesurée pendant le processus de vérification et de validation. Si l'exigence ne peut être mesurée lors des dispositions de preuve, c'est alors un objectif et des exigences qualitatives seront produites sur la base des preuves fournies.

Les exigences doivent aussi pouvoir être tenues. Tous les clients voudraient une fiabilité de 100 % pour leurs systèmes et ce n'est pas atteignable même avec une très haute fiabilité, sauf à un coût très élevé. Le client doit donc évaluer quels niveaux des différentes mesures de sûreté de fonctionnement sont raisonnables, en se basant sur des facteurs comme la réalisation de systèmes similaires antérieurs, la performance souhaitée et l'étude des améliorations qui peuvent être attendues. Les systèmes actuels deviennent de plus en plus complexes pour atteindre les niveaux de fonctionnalité souhaités et ils peuvent avoir atteint la limite de la performance de fiabilité économiquement applicable.

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

a) les enregistrements de données de maintenance et de service appartenant au fournisseur ;

b) les bases de données génériques et les recueils de données ;

c) les données de constructeurs pour les sous-systèmes et les composants.

Comme cela est évoqué dans la Note 3 du domaine d'application, les spécifications de sécurité et d'environnement ne sont pas traitées directement dans ces lignes directrices. Cependant beaucoup des recommandations de la présente norme peuvent être appliquées aux spécifications de sécurité et d'environnement. Ainsi quand des exigences de sûreté de fonctionnement ont trait à la sécurité et à l'environnement, les exigences appropriées à la

sécurité et à l'environnement peuvent être incluses ou être en référence dans les exigences de sûreté de fonctionnement.

5 Gestion de la sûreté de fonctionnement

La présente norme traite de la spécification de la sûreté de fonctionnement, par le biais de la spécification de l'une ou de plusieurs de ses composantes telles que la disponibilité, la fiabilité, la maintenabilité et le support de maintenance. Ces mesures sont des caractéristiques intrinsèques du système et les activités de vérification et de validation peuvent démontrer les niveaux probables d'obtention. Cependant, d'autres facteurs peuvent réduire significativement les niveaux obtenus pour ces mesures, en dessous de leurs niveaux intrinsèques. Les plus significatifs sont potentiellement la qualité de fabrication et la maintenance du système qui peut introduire de nouvelles pannes dans le système. Il est donc essentiel que la sûreté de fonctionnement soit activement gérée tout au long du cycle de vie du système. Ceci comprend le processus d'approvisionnement et l'exploitation et les activités de gestion seront différentes pour l'un et l'autre. Si la sûreté de fonctionnement n'est pas gérée correctement pendant le processus d'approvisionnement ou pendant l'exploitation, il y a une forte probabilité que les exigences de fiabilité ou de disponibilité ne soient pas tenues.

La CEI 60300-1, la CEI 60300-2 et la CEI 61160 couvrent en détail la gestion de la sûreté de fonctionnement et elles décrivent précisément les activités et techniques pour la gestion de la sûreté de fonctionnement.

NOTE Il convient de noter que la CEI 61160:2005 ne couvre pas toutes les revues de conception; par exemple, la revue de conception d'installation, la revue de conception de l'utilisateur et la revue de conception de démantèlement, qui surviennent après la revue de conception finale. Ces normes incluent des détails associés au cycle de vie de la sûreté de fonctionnement.

Le cycle de vie d'un système comprend les phases suivantes:

– faisabilité et définition ;
– conception et développement ;
– fabrication ;
– installation ;
– exploitation et maintenance;
– démantèlement.

Le cycle de vie du système peut avoir un effet significatif sur la sûreté de fonctionnement obtenue pour le système. Par exemple, des manipulations défectueuses et des durées de stockage étendues peuvent significativement réduire la performance de fiabilité d'un système. De plus, la performance de fiabilité peut varier dans le cycle de vie avec beaucoup de systèmes ayant des taux de défaillance variables avec l'utilisation, dus à l'usure de composant ou sous-systèmes. Cette modification dans la performance de fiabilité avec l'utilisation signifie que pour beaucoup de systèmes, l'hypothèse du taux de défaillance constant n'est pas valide et que différentes distributions de probabilité qui requièrent des expressions mathématiques plus complexes doivent être utilisées pour estimer la performance de fiabilité. La CEI 61649, la CEI 61703 et la CEI 61710 donnent d'autres lignes directrices.

Les changements dans l'utilisation du système sont un autre facteur affectant la performance de fiabilité. Par exemple, un véhicule qui roule normalement sur la route aura probablement plus de défaillances s'il est utilisé hors route, du fait des différentes contraintes et charges portées alors sur le véhicule. Ainsi, la mission du système ou son utilisation est une composante essentielle de la spécification de sûreté de fonctionnement et les modifications doivent être suivies et gérées comme faisant partie du cycle de vie.

6 Disponibilité

6.1 Généralités

6.1.1 Choix de la caractéristique de sûreté de fonctionnement

Pour certains systèmes, particulièrement pour les systèmes complexes, il est nécessaire de considérer ensemble la fiabilité et la maintenance. Dans de tels systèmes, il peut être pertinent au niveau système de spécifier les exigences de disponibilité plutôt que séparément les exigences de fiabilité et de maintenabilité. Il est important que le client définisse quelles définitions de la disponibilité sont à spécifier ou s'il y a un risque que le niveau requis de performance de disponibilité ne soit pas obtenu. Des exigences pour la disponibilité en régime permanent sont les plus communément utilisées bien que la disponibilité moyenne soit aussi pertinente.

Parmi les exemples industriels où la performance de disponibilité peut être la principale caractéristique de sûreté de fonctionnement, figurent l'industrie ferroviaire où les exploitants exigent un pourcentage de trains disponibles pour les périodes de pointe de trafic ou un retard à ne pas dépasser, l'industrie des télécommunications où les opérateurs exigent un certain nombre de canaux de communications disponibles afin que le système maintienne une disponibilité globale alors que certains routages sont indisponibles.

La disponibilité en régime permanent est "la moyenne de la disponibilité instantanée dans des conditions de régime permanent sur une période donnée". Pour que cette définition de la disponibilité soit pertinente, les conditions de régime permanent doivent exister. Parce que les traitements mathématiques sont simplifiés si des conditions de régime permanent existent, ces dernières sont souvent spécifiées alors qu'elles ne sont pas pertinentes.

La disponibilité instantanée est la « probabilité qu'un dispositif soit en état de réaliser une fonction requise dans des conditions données à un instant donné, l'hypothèse étant faite que les ressources externes nécessaires sont fournies ». C'est rarement spécifié dans des exigences de sûreté de fonctionnement.

La disponibilité moyenne est la « moyenne de la disponibilité instantanée sur un intervalle de temps donné (t_1, t_2) ». Cette mesure est plus utilisable pour une spécification et elle est intéressante dans les industries où différentes durées peuvent être modifiées du fait de conditions de fonctionnement, par exemple.

Il existe d'autres définitions de la disponibilité, telles que la disponibilité en exploitation (où les délais de logistique sont inclus) et la disponibilité asymptotique (voir la CEI 60050-191).

6.1.2 Relation entre disponibilité, fiabilité et maintenabilité

Disponibilité, fiabilité et maintenabilité ne sont pas des mesures indépendantes et pour un système réparable, elles sont liées par la relation:

$$\text{Disponibilité en régime permanent} = \frac{\text{MUT}}{\text{MUT} + \text{MDT}}$$

où

MUT = temps moyen de fonctionnement;

MDT = temps moyen d'indisponibilité.

Dans le cas d'un taux de défaillance constant et d'un taux de réparation constant, et uniquement dans ce cas, les disponibilités asymptotique et en régime permanent sont identiques et souvent appelées simplement « disponibilité ». Cette relation est uniquement applicable dans ces conditions très spécifiques qui sont assez rares. Il convient que ce calcul

soit uniquement utilisé comme première estimation avant que des évaluations plus détaillées et plus précises de la disponibilité soient faites.

Les trois mesures de la performance de sûreté de fonctionnement ne peuvent toutes être spécifiées parce que cela contraindrait la performance de sûreté de fonctionnement du système. Cependant, il est habituel de spécifier deux des trois mesures pour garantir que l'équilibre entre le temps de fonctionnement et le temps d'indisponibilité est acceptable en exploitation. La même disponibilité peut être atteinte par de hauts niveaux de MUT avec des durées d'indisponibilité longues ou inversement avec un MUT plus faible mais avec des durées d'indisponibilité plus courtes. Par exemple, des systèmes basés sur des ordinateurs personnels peuvent défaillir fréquemment mais nécessiter seulement quelques minutes pour redémarrer et fonctionner à nouveau, apportant ainsi une haute disponibilité globale. Cela est frustrant pour l'utilisateur mais peut être plus acceptable que la même disponibilité obtenue par un ordinateur tombant rarement en panne mais pour une longue durée, quand cela se produit. Cependant, pour les réseaux de télécommunication, une disponibilité résultant d'une fiabilité plus faible et de durées d'indisponibilité courtes peut être inacceptable parce que ces réseaux ne sont pas disponibles pour des durées suffisantes à la transmission des données.

6.2 Spécifications de disponibilité

6.2.1 Exigences quantitatives

Toute spécification de disponibilité doit définir exactement ce que signifie « disponibilité », c'est-à-dire quel type de disponibilité est spécifié et quelles durées sont comprises dans le temps d'indisponibilité, si les délais de logistiques sont inclus et à quoi elle s'étend.

Les exigences de disponibilité peuvent être exprimées comme une fraction décimale ou comme un pourcentage, par exemple le temps de fonctionnement comme un pourcentage de la durée observée. Les exigences de disponibilité couvrent à la fois la fréquence des défaillances et la durée d'indisponibilité. Si c'est la disponibilité moyenne qui est spécifiée, la durée sur laquelle elle est mesurée doit aussi être spécifiée, ainsi que toute autre information pertinente relative au temps. Par exemple, si la disponibilité moyenne d'un train-navette est requise, elle peut être spécifiée comme disponibilité moyenne mesurée pour chaque heure entre 7 h et 10 h et entre 17 h et 20 h, du lundi au vendredi.

Lorsqu'on spécifie les exigences quantitatives de disponibilité, il est usuel d'accumuler des temps d'indisponibilité sur une durée donnée (par exemple, un mois ou une année). Si une partie du temps d'indisponibilité est hors de la responsabilité du fournisseur (par exemple, des délais de logistique ou administratifs), il convient que cela soit noté dans la spécification avec des valeurs établies pour les temps concernés. La Figure 191-10 de la CEI 60050-191 donne des recommandations pour diverses durées de maintenance. Autrement, une disponibilité intrinsèque peut être spécifiée par calcul en excluant de telles durées de maintenance.

L'Article B.2 de l'Annexe B donne des exemples d'exigences quantitatives de disponibilité.

6.2.2 Exigences qualitatives

Les exigences qualitatives de disponibilité peuvent inclure une combinaison d'exigences qualitatives de fiabilité et de maintenabilité et il convient qu'elles ne soient utilisées que si c'est la seule possibilité. Les exigences qualitatives de disponibilité peuvent compléter les exigences quantitatives quand ces dernières ne peuvent pas couvrir tous les aspects de la spécification, par exemple si le temps d'indisponibilité dans certaines conditions d'exploitation est plus critique. Cependant, le type de disponibilité et les durées incluses dans la durée d'indisponibilité doivent encore être définis dans la spécification.

6.3 Dispositions de vérification et de validation de la disponibilité

6.3.1 Généralités

Il convient que la spécification inclue la nécessité de vérification et de validation de la performance de disponibilité exigée. La preuve de la disponibilité est souvent apportée au moyen d'une combinaison de preuves de fiabilité et de maintenabilité, plutôt que directement.

6.3.2 Vérification et validation par essais

Lorsque la vérification et la validation sont réalisées au moyen d'essais, les procédures d'essais de conformité normalisés pour la disponibilité en régime permanent données dans la CEI 61070 peuvent être appliquées. Il convient de noter cependant, que pour les exigences de très haute disponibilité (par exemple > 0,999), il est très difficile d'établir un plan d'essai réaliste. L'évaluation, la vérification et la validation de la performance de disponibilité de sous-systèmes peuvent aider dans cette activité. Ceci peut être obtenu en utilisant des observations au niveau du système et des sous-systèmes dans un modèle de disponibilité du système. Dans tous les cas, la faisabilité des méthodes appliquées pour vérifier et valider des exigences de haute fiabilité nécessite d'être démontrée.

Pour l'exploitation et les essais de performance de disponibilité, il convient que le programme de recueil des données d'exploitation soit agréé par avance (voir la CEI 60300-3-2), en incluant le temps d'indisponibilité résultant des défaillances du matériel, des défaillances du logiciel, des procédures de maintenance et d'autres causes. L'exécution des essais doit être surveillée et analysée pendant leur progression afin d'apporter la preuve nécessaire.

De plus, si plusieurs exemplaires du type de système sont utilisés pendant l'essai, il convient que le nombre d'exemplaires et la période d'observation soient pris en compte. Il convient qu'une procédure soit spécifiée de sorte qu'en cas de non-conformité, une amélioration soit agréée et introduite et que l'essai soit poursuivi. Il est recommandé qu'une attention particulière soit portée à la validité statistique de l'utilisation de plusieurs exemplaires, une durée de 100 h sur 1 exemplaire n'étant équivalente à une durée de 1 h sur 100 exemplaires que si certains facteurs sont pris en compte et que si certaines hypothèses sont vraies. Ceci inclut l'hypothèse du taux de défaillance constant, l'absence de défaillances précoces ou de défaillances d'usure et le degré de confiance dans la représentativité de l'échantillon utilisé.

6.3.3 Vérification et validation par analyses

Si la vérification et la validation sont menées par des méthodes d'analyse, les techniques normalisées de prédiction avec la méthodologie d'analyse détaillée comme cela est spécifié par la CEI 62308, peuvent être appliquées.

Généralement, les données pour calcul sont basées sur des sources reconnues de données, des résultats obtenus à partir de l'expérience en exploitation sur des systèmes similaires, des essais de laboratoires ou des intégrations de logiciel/matériel. Il convient que les données soient agréées entre le fournisseur et le client et que les sources de données soient enregistrées.

7 Fiabilité

7.1 Généralités

Pour certains systèmes, il est nécessaire de considérer directement la fiabilité du système. Dans ces systèmes, il peut être pertinent au niveau du système, de spécifier séparément les exigences de fiabilité et celles de maintenabilité. Par définition, la fiabilité est la capacité d'un système à réaliser sans défaillance une fonction requise dans des conditions données et pour une durée donnée. Elle est décrite plus correctement par la probabilité que le système remplisse la mission requise. Cependant, beaucoup de spécifications définissent la fiabilité exigée par l'utilisation d'autres mesures, telles que le temps moyen avant défaillance ou le temps de fonctionnement entre défaillances.

Des exemples d'industrie ou la performance de fiabilité peut être la principale caractéristique de sûreté de fonctionnement: l'industrie aérospatiale où une fois que l'aéronef a décollé, il est essentiel qu'il effectue son vol sans défaillance totale, et l'industrie automobile où le conducteur doit atteindre sa destination et peut effectuer la maintenance de son véhicule un fois à destination.

Les lampes électriques conçues pour une durée de vie sont un exemple où le temps avant défaillance peut être une exigence de fiabilité. De même, un processus industriel qui fonctionne en continu constitue un exemple où le temps avant défaillance est important pour planifier les activités de maintenance.

Le client doit porter attention à la pertinence de la spécification de la performance de fiabilité et à la bonne compréhension des implications statistiques de l'exigence. Par exemple, si une fiabilité de 99 % sur une durée d'un an est spécifiée, cela peut paraître critique. Cependant, cela correspond à un MTBF de 871 613 h (ou plus de 99 ans) si le taux de défaillance est constant. C'est pourquoi le MTBF est souvent considéré comme une mesure obsolète et sujette à des modifications du fait des évolutions de l'utilisation et il est recommandé que la disponibilité, la fiabilité et la probabilité de défaillance soient établies à sa place. Pour un taux de défaillance non constant, les paramètres de Weibull ou d'autres distributions applicables peuvent être utilisés pour la spécification (voir la CEI 61649). Pour une intensité de défaillance non constante, le modèle de loi en puissance peut être utilisé (voir la CEI 61164 et la CEI 61710).

7.2 Spécification de la fiabilité

7.2.1 Exigences quantitatives

Il convient que les exigences de performance de fiabilité soient quantitatives et qu'elles soient spécifiées avant le début de la conception du système. Comme pour toute statistique, il convient que toute exigence ou mesure de fiabilité quantitative spécifie aussi la confiance avec laquelle l'exigence doit être démontrée ou établie (voir la CEI 60605-4).

Les mécanismes de défaillance qui seront probablement rencontrés dans le système sont à considérer au début car ils détermineront quelle mesure de fiabilité est pertinente. Par exemple, des moteurs de véhicules ont des défaillances en rapport avec la distance parcourue plutôt qu'en rapport avec leur âge, de sorte que le kilométrage est la mesure pertinente. Ils sont soumis à une usure et donc l'hypothèse du taux de défaillance constant n'est pas valide. Les ampoules d'éclairage domestique tombent en panne principalement du fait du nombre de cycles de mise sous tension et moins de leur durée d'éclairage, de sorte que le nombre de cycles ou le nombre d'heures de fonctionnement sont les unités pertinentes et le système est donc produit pour une durée de fonctionnement définie. L'inclusion ou non d'éléments redondants est un autre facteur qui affecte le choix de la mesure de fiabilité.

Pour chaque système, il est nécessaire de sélectionner et de définir chaque caractéristique de fiabilité qui est exigée et de spécifier une exigence quantitative pour chaque caractéristique. Lors de la spécification des exigences quantitatives pour un système, il est important d'établir ce qui suit:

– les applications du système ou le profil d'utilisation ;
– les critères de défaillance ou la définition d'une défaillance, c'est-à-dire ce qui constitue une défaillance dans ce système et dans l'application prévue ;

  NOTE Une défaillance peut être définie de différentes façon, selon ses conséquence; par exemple, la perte d'un service, le besoin de réparation (voir aussi 7.2.2).

– les conditions de fonctionnement ;
– les conditions environnementales ;
– les méthodes destinées à être appliquées pour la preuve de la conformité aux exigences.

Sans ces précisions, la spécification d'une mesure de la performance de fiabilité telle que R(t), F(t), MTTF, MTBF, le nombre des défaillances pour une durée donnée, les paramètres de Weibull ou de la loi en puissance serait sans signification.

Lors de la sélection de la valeur de la mesure de la performance de fiabilité à spécifier, il convient de prendre en compte les facteurs suivants:

– les limites imposées par l'état de l'art technologique ainsi que par la nature et la complexité du système ;
– l'expérience du client dans le fonctionnement et la maintenance du type de système ;
– la faisabilité de la vérification de l'exigence spécifiée ;
– le niveau de fiabilité des unités, composants, etc. à partir duquel le système peut être fabriqué ;
– le coût de conception, de production et de vérification et la validation du système avec un niveau spécifié de fiabilité.

Si durant le développement d'un projet, il devient évident que les hypothèses de base ne sont pas valides, les exigences de la performance de fiabilité peuvent devoir être reconsidérées et modifiées. Si la spécification doit être changée, il convient que cela soit fait en accord avec toutes les parties concernées.

Il convient que les exigences quantitatives soient clairement spécifiées dans une forme dans laquelle il sera possible de comparer les résultats obtenus ensuite.

Lorsque la preuve de la conformité aux exigences quantitatives est à fournir par des essais, il convient que le niveau de confiance soit spécifié ou que le plan réel d'essai à appliquer soit spécifié. Si un plan d'essai est spécifié, il convient que la spécification comprenne la durée d'essai et les critères d'acceptation/rejet.

Différents types d'essai de démonstration de fiabilité existent et, toutes choses étant égales par ailleurs, il est préférable d'utiliser des plans d'essais séquentiels (voir la CEI 61123 et la CEI 61124) plutôt que des plans d'essais à durée/défaillances fixées qui sont moins efficaces. Si la mesure de la performance de fiabilité est connue ou si elle varie probablement dans le temps, il convient de spécifier la sûreté de fonctionnement par exemple, par les paramètres de Weibull pour les systèmes non réparables (voir la CEI 61649) ou par les paramètres de la loi en puissance pour les systèmes réparables (CEI 61164 et CEI 61710). Autrement, l'intensité de défaillance moyenne sur une durée établie peut être spécifiée. Voir la CEI 60300-3-5 pour plus d'informations sur les distributions paramétriques.

L'Article B.3 de l'Annexe B donne des exemples d'exigences quantitatives de fiabilité.

7.2.2 Exigences qualitatives

Les exigences qualitatives de fiabilité peuvent être exprimées en termes (l'un ou l'autre ou les deux) de:

– critères de conception pour le système ;
– activités d'amélioration de la fiabilité à appliquer pendant les phases du cycle de vie du système.

Les critères de conception pour un système, comme les exigences physiques, de performance ou de fonctionnement, généralement isolées/indépendantes les unes des autres peuvent aussi compléter des exigences quantitatives de fiabilité. De tels critères peuvent indirectement imposer des exigences de fiabilité pour le système lui-même et pour la façon de l'installer et dont sa performance est surveillée. Quelques exemples sont donnés ci-après:

– critère de panne unique, c'est-à-dire qu'aucune panne unique ne doit conduire à un état critique du système ;

– critère de pannes cumulées, c'est-à-dire que le système doit être tel qu'aucune panne non détectée, combinée à d'autres pannes, ne peut provoquer la défaillance du système ;
– séparation des chemins, c'est-à-dire que des systèmes redondants doivent être maintenus indépendants en utilisant des cheminements séparés pour les câbles, les conduits, etc. pour les canaux de signaux, d'alimentation et autres fournitures ;
– surveillance des fonctions critiques, c'est-à-dire que des dispositions doivent être prises pour des contrôles automatiques ou manuels soit en continu, soit par intervalles, afin de maintenir un niveau de performance de fiabilité spécifié.

En plus de la spécification quantitative de la performance de fiabilité, il peut souvent être avisé de spécifier une séquence d'activités d'amélioration de fiabilité (et de maintenabilité) à appliquer pendant les phases du cycle de vie du système. De telles exigences qualitatives peuvent être appliquées pour le matériel, le logiciel et le support. Ces activités sont particulièrement importantes si les exigences quantitatives ne spécifient pas tous les aspects de performance de fiabilité du système. Il convient qu'elles soient agréées par le client et le fournisseur, à la fois pour le contenu technique, leur planification et le coût. Il convient que ces exigences qualitatives soient formalisées et gérées dans le plan programme de fiabilité (ou dans le plan de sûreté de fonctionnement) (voir la CEI 60300-2).

Il convient que le plan programme de fiabilité soit optimisé en fonction de la nature du système et que les exigences spécifiées et usuelles incluent:

– les types de méthodes à appliquer ;
– un programme de croissance de fiabilité, si nécessaire (voir la CEI 61014) ;
– des clauses sur la manière de vérifier la conformité aux exigences (voir la CEI 60300-3-5) ou toute autre mesure qualitative ou quantitative à utiliser pour exprimer le degré de conformité aux exigences ;
– les critères pour la sélection des composants et les dispositions pour la preuve de qualité ;
– les analyses des pires cas.

7.3 Vérification et validation de la fiabilité

7.3.1 Généralités

Il convient que la spécification établisse les méthodes à utiliser pour fournir la preuve du respect des exigences.

La vérification et la validation de la fiabilité peuvent être apportées soit par analyse lors de la conception et avant la production, soit par des essais de laboratoire après la production, soit par l'évaluation de la performance après livraison. De plus, la vérification et la validation peuvent être obtenues à partir d'autres activités pendant le processus de développement. L'analyse de conception (comme une analyse des contraintes), des essais de performance, des essais de logiciels et des simulations de fonctionnement sont des exemples. La preuve peut être recueillie de toutes sources pour apporter la vérification et la validation et elle complètera les activités dédiées de vérification et de validation de la fiabilité.

7.3.2 Vérification et validation par essais

Les méthodes préférées de vérification et de validation de la fiabilité par des essais sont normalement sélectionnées par accord entre le client et le fournisseur, et elles comprennent:

– le recueil et l'analyse de données de défaillances d'autres systèmes en exploitation, c'est-à-dire en utilisation réelle (voir la CEI 60300-3-2 et la CEI 60605-6). Cependant, leur validité exige de recueillir suffisamment de données et cela peut être trop tardif dans le processus d'approvisionnement si un haut degré de preuve est exigé ;
– l'essai de systèmes en utilisation ou en laboratoire, par des essais de conformité ou de détermination décrits dans la CEI 60300-3-5, la CEI 61123, la CEI 61124, la CEI 61649 ou

la CEI 61710. Lors de la spécification d'essais de laboratoire, il est important de considérer les facteurs associés tels que le coût et la durée.

Il convient que tous les essais soient optimisés pour refléter l'exploitation et son environnement et les contraintes que le système subira ou bien le résultat ne reflètera pas la fiabilité du système obtenue en service.

Il convient que des critères précis soient spécifiés afin de permettre toutes les défaillances dans le matériel et dans le logiciel, etc. et leur classement en catégorie « pertinente » ou « non pertinente ». Ce classement est la base des critères d'acceptation/rejet et il est essentiel qu'il soit établi clairement, avec précision, avant le début des essais et de préférence défini très tôt dans le cycle de vie, de sorte qu'il n'y ait pas de suspicion sur une adaptation des résultats en vue d'atteindre l'objectif. Cependant, il peut ne pas être possible de définir tous les critères d'essai à temps dans le cycle de vie ou le développement du produit.

La vérification et la validation des mesures de la performance de fiabilité doivent être considérées séparément pour les systèmes réparés et non réparés.

La CEI 61123 contient des détails des essais qui peuvent être utilisés si un taux de succès est utilisé comme mesure de la performance de fiabilité et la CEI 61124 contient des essais qui sont pertinents si l'hypothèse du taux de défaillance constant ou de l'intensité de défaillance constante est valide. Il convient que l'hypothèse du taux de défaillance constant ou de l'intensité de défaillance constante soit validée parce que le résultat d'un essai peut être annulé si cette hypothèse est improprement utilisée (voir la CEI 60605-6).

7.3.3 Vérification et validation par analyse

La vérification et la validation de la fiabilité d'un système peuvent être réalisées avant la livraison, par des calculs basés sur l'analyse de fiabilité. Dans certains cas (par exemple des systèmes possédant une très haute fiabilité), ceci peut être la seule approche possible. L'analyse peut être utilisée longtemps avant la validation de la fiabilité pendant le fonctionnement en service ou par des essais en laboratoire. Une telle méthode peut uniquement déterminer par analyse si le système à livrer est conforme aux exigences correspondantes données dans la spécification du système; elle ne peut pas mesurer directement la fiabilité obtenue.

Des exemples de techniques d'analyse pour la vérification et la validation de la fiabilité d'un système constitué de matériels et de logiciels sont les blocs-diagrammes de fiabilité, les arbres de panne et l'analyse des modes de défaillance et de leurs effets. Voir l'Annexe A pour les normes qui donnent des recommandations sur les différents outils d'analyse.

Il convient que l'élément matériel d'un système soit analysé afin d'établir que le taux de défaillance de chacun de ses sous-systèmes, pièces et composants électroniques prend en compte l'utilisation à laquelle il est destiné et les contraintes opérationnelles et afin que leurs conclusions soient pertinentes et justifiables. Des mesures électriques, thermiques ou autres peuvent être nécessaires pour cela.

Il convient que le logiciel dans le système soit analysé de façon similaire pour identifier de possibles modes de panne logicielle et évaluer qualitativement leur impact sur la performance de fiabilité du système.

Les données pour ces calculs peuvent être basées par exemple sur des résultats issus du retour d'expérience sur des systèmes similaires en exploitation, d'essais en laboratoire, d'intégration matériel/logiciel de sources de données dûment reconnues. Si le client prévoit de spécifier l'utilisation d'une base de données particulière (par exemple une banque de données de taux de défaillance), il convient que cela soit agréé entre le fournisseur et le client. Cependant, spécifier l'utilisation d'une base de données particulière ne relève pas le fournisseur de ses obligations d'atteindre la performance de fiabilité exigée. Dans tous les

cas, il convient d'identifier la source des données et les hypothèses utilisées pour l'estimation enregistrée.

8 Maintenabilité

8.1 Généralités

La maintenabilité est une mesure importante de la sûreté de fonctionnement pour tous les types de systèmes réparables et reflète l'aptitude d'un système à être maintenu ou restauré dans un état dans lequel il peut réaliser la fonction requise. Des exemples sont les mises à jour à mi-vie pour des projets logiciels pour corriger des niveaux faibles de disponibilité obtenus ou les systèmes à distance qui sont difficiles à maintenir. De plus, pour les autres systèmes, la maintenabilité peut avoir un effet significatif sur la sûreté de fonctionnement atteinte si elle est incorrectement spécifiée, particulièrement dans les systèmes sans redondance. La maintenabilité est traitée en général dans la CEI 60300-3-10.

8.2 Spécification de maintenabilité

8.2.1 Exigences quantitatives

La CEI 60706-2 donne tous les détails pour spécifier et rendre contractuelle la maintenabilité. Il peut être nécessaire de spécifier séparément des exigences des maintenances corrective et préventive parce que le support de maintenance requis est différent.

Lorsque des exigences quantitatives sont spécifiées, il est important de spécifier la durée prévue sur laquelle un système ne sera pas opérationnel du fait de la maintenance ou du support de maintenance. Cette durée doit être spécifiée en termes de mesures pertinentes comme moyenne ou fractile de temps de réparation, ou comme moyenne ou fractile de délais de logistique. Les exigences quantitatives peuvent aussi être exprimées en termes de coûts de maintenance en fonction du temps ou de la distance par exemple coût de maintenance par heure de fonctionnement.

Il convient qu'une spécification complète des exigences de performance de maintenabilité couvre cinq larges domaines:

- la performance de maintenabilité à atteindre par la conception du système ;
- les contraintes qui seront rencontrées dans l'utilisation du système et qui affecteront la maintenance ;
- les exigences du programme de maintenabilité à accomplir par le fournisseur pour garantir que le système livré possède les caractéristiques requises de maintenabilité ;
- les exigences d'accès pour la maintenance ;
- les dispositions de la planification du support de maintenance.

Lorsque l'on spécifie les exigences de maintenabilité, il est important d'établir ce qui suit:

- les différentes conditions de fonctionnement et environnementales dans lesquelles le système est utilisé ;
- les qualifications, les responsabilités et les caractéristiques physiques du personnel impliqué dans le fonctionnement et la maintenance du système ;
- la politique de maintenance à appliquer et les procédures associées et les dispositions de support (par exemple, la maintenance préventive ou les tests de diagnostic) ;
- les outils disponibles et tous les outils spéciaux requis ;
- les pièces de rechange à fournir et comment elles sont estimées et gérées.

Il convient que la spécification de la performance de la maintenabilité détaille les exigences et la méthode pour les vérifier. Il convient aussi d'inclure des définitions précises des termes utilisés dans la spécification avec le cas échéant, des références au vocabulaire normalisé.

Les exigences de maintenabilité peuvent être spécifiées dans la spécification comme étant soit des objectifs, soit des exigences définies qui sont à vérifier conformément aux procédures prescrites. Les objectifs ou les exigences peuvent être spécifiés en termes quantitatifs ou en termes qualitatifs.

Typiquement, une spécification des exigences de performance de maintenabilité couvre les différents aspects de la réalisation de la maintenabilité au niveau opérationnel. Cependant, puisque la maintenabilité est une caractéristique du système qui affecte les coûts de support de maintenance et peut aussi affecter les durées de maintenance à différents niveaux de maintenance, il convient que les exigences soient incluses dans la spécification couvrant la réalisation de tous les niveaux affectés par la politique de maintenance.

Des recommandations plus détaillées sur les exigences de performance de maintenabilité dans les spécifications et les contrats sont données dans la CEI 60706-2.

L'Article B.4 de l'Annexe B contient des exemples d'exigences quantitatives de maintenabilité.

8.2.2 Exigences qualitatives

Lorsque les exigences de support de maintenabilité ne peuvent pas être spécifiées quantitativement, il convient d'utiliser des exigences qualitatives en complément. Cependant, comme pour toutes les caractéristiques de sûreté de fonctionnement, des exigences quantitatives et qualitatives peuvent être spécifiées ensemble. Ceci peut, par exemple, être des spécifications du degré auquel un système doit être conforme aux conditions spécifiques et aux contraintes liées à la maintenance.

8.3 Vérification et validation de la maintenabilité

La plus grande partie de la vérification et la validation de la performance de maintenabilité peut être apportée par d'autres essais ou analyses au cours du développement. Par exemple, les essais de fiabilité fourniront des données sur la maintenabilité du système si les données pertinentes sont recueillies. En conséquence, il convient que toutes les tentatives et analyses au cours du développement soient examinés pour voir si elles peuvent fournir des données de maintenabilité significatives et si ainsi, ces tentatives peuvent être construites dans un plan de tentatives à la première opportunité.

La vérification et la validation de la performance de maintenabilité est le processus de détermination des exigences de la spécification à tenir. Il convient que les méthodes et procédures pour la vérification et la validation soient spécifiées avec les exigences de maintenabilité. Les méthodes de vérification et de validation peuvent aller de la soumission par le fournisseur, de données appropriées ou d'informations jusqu'à la réalisation d'une démonstration particulière de maintenabilité.

Il convient de regarder la vérification et la validation de la maintenabilité comme un processus continu. Il convient que les données relatives à la maintenabilité soient générées, recueillies et évaluées dès qu'elles sont disponibles dans le déroulement du développement du projet et que les résultats soient comparés constamment aux exigences de maintenabilité spécifiées.

Plusieurs méthodes de vérification de la performance de maintenabilité sont décrites dans la CEI 60706-3. Elles incluent:

– l'analyse et la revue des caractéristiques de maintenabilité ;
– les études spécifiques ;
– les essais de démonstration ;
– la revue des expériences opérationnelles.

La spécification peut fournir des recommandations ou peut spécifier quelles méthodes ci-dessus sont à appliquer.

D'autres informations sur la vérification et la validation de la maintenabilité sont données dans la CEI 60706-3. Des informations concernant les tests de diagnostic sont données dans la CEI 60706-5 et des méthodes statistiques pour l'allocation de maintenabilité dans la CEI 60706-2.

9 Support de maintenance

9.1 Généralités

Le support de maintenance est l'aptitude d'une organisation de maintenance à fournir les ressources nécessaires pour maintenir un système, c'est-à-dire où et quand cela est requis et les dispositions de support de maintenance sont souvent critiques pour garantir la sûreté de fonctionnement des systèmes. Le niveau de support de maintenance est très souvent influencé par les conditions d'utilisation et des facteurs qui changent au cours du cycle de vie.

Le support de maintenance peut être fourni totalement ou partiellement par le fournisseur, le client du système ou par une tierce partie, en fonction de la nature de la spécification. La spécification dépendra donc de la source du support de maintenance. Le soutien logistique intégré (SLI pour Integrated Logistic Support) est la méthode par laquelle tous les services de soutien logistiques sont considérés et fournis comme partie intégrante du développement du produit (voir la CEI 60300-3-12). Dans d'autres cas, particulièrement quand des systèmes sont construits principalement à partir de matériels COTS, les fournisseurs apportent uniquement la planification de support de maintenance de base ou standard pour leur application spécifique, souvent en utilisant une ressource interne (voir la CEI 60300-3-14).

Dans le cas où le support de maintenance est apporté par le fournisseur, il peut être spécifié comme faisant partie de la livraison. Le support de maintenance par le client (ou l'utilisateur) fera partie des conditions spécifiées pour le fonctionnement du système, un prérequis pour les valeurs établies de la fiabilité, la disponibilité et la maintenabilité.

9.2 Spécification du support de maintenance

9.2.1 Exigences quantitatives

Quand cela est possible, il convient que les exigences du support de maintenance soient spécifiées de façon quantitative. Des exemples de spécifications quantitatives sont les temps de réponse, le délai administratif moyen, le délai logistique moyen, la probabilité de pénurie de pièces de rechange et la durée de cette dernière. Plus d'informations sont données dans la CEI 60300-3-12 et dans la CEI 60706-2.

Lors de la spécification des exigences du support de maintenance, il est important d'établir:

- les différentes conditions de fonctionnement et environnementales dans lesquelles le système est utilisé ;
- les obligations et les responsabilités du client, du fournisseur et des tierces parties ;
- la politique de maintenance à appliquer et les procédures associées et les dispositions de support ;
- les outils disponibles et les outils spéciaux et gabarits nécessaires ;
- les qualifications, les responsabilités et les caractéristiques physiques du personnel impliqué dans le fonctionnement et la maintenance du système.

Les spécifications du support de maintenance peuvent être spécifiées avant que la conception du système commence et elles peuvent être mises à jour avant la livraison du système.

L'Article B.5 de l'Annexe B donne des exemples d'exigences quantitative de support de maintenance.

9.2.2 Exigences qualitatives

Lorsque les exigences de support de maintenance ne peuvent pas être spécifiées quantitativement, il convient d'utiliser des exigences qualitatives en complément. Cependant, comme pour toutes les caractéristiques de sûreté de fonctionnement, des exigences quantitatives et qualitatives peuvent être spécifiées ensemble. Ceci peut par exemple être des spécifications du degré de formation et de qualification du personnel de maintenance ou des exigences d'installations d'atelier et d'outils devant être disponibles.

Plus d'informations sont données dans la CEI 60300-3-12 et la CEI 60706-2.

9.3 Vérification et validation de la maintenabilité

Les méthodes de vérification et de validation pour le support de maintenance sont étroitement liées à la vérification et la validation de la maintenabilité et il est peu probable qu'elles puissent être séparées puisque la performance de maintenabilité dépend de la disponibilité du support de maintenance et qu'aucune autre information ne sera disponible. Une autre voie pour la vérification et la validation peut être la preuve qualitative que le support est disponible et effectif.

Annexe A
(informative)

Normes de référence pour les techniques de vérification et de validation

A.1 Techniques pour les essais de sûreté de fonctionnement

Le Tableau A.1 donne des normes de référence pour la vérification et la validation de la sûreté de fonctionnement au moyen d'essais. Lorsque aucune date n'est donnée, la dernière édition est celle à utiliser.

Tableau A.1 – Techniques pour la vérification et la validation de la sûreté de fonctionnement par des essais

Norme identifiée	Titre de la norme	Technique d'essai couverte
CEI 60300-3-2	Gestion de la sûreté de fonctionnement – Partie 3-2: Guide d'application – Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation	Recueil de données de sûreté de fonctionnement
CEI 60300-3-5	Gestion de la sûreté de fonctionnement – Partie 3-5: Guide d'application – Conditions des essais de fiabilité et principes des essais statistiques	Essais de fiabilité – Statistique
CEI 60300-3-7	Gestion de la sûreté de fonctionnement – Partie 3-7: Guide d'application – Déverminage sous contraintes du matériel électronique	Stress screening – Matériel électronique
CEI 60605-2	Essai de fiabilité des équipements – Partie 2: Conception des cycles d'essai	Essais de fiabilité
CEI 60605-3-1	Essai de fiabilité des équipements – Partie 3-1 : Conditions d'essai préférentielles – Equipements portatifs d'intérieur – Faible degré de simulation	Essais de fiabilité
CEI 60605-3-2	Essai de fiabilité des équipements – Partie 3-2 : Conditions d'essai préférentielles – Equipement pour utilisation à poste fixe à l'abri des intempéries – Degré de simulation élevé	Essais de fiabilité
CEI 60605-3-3	Essai de fiabilité des équipements – Partie 3-3: Conditions d'essai préférentielles – Cycle d'essai n° 3: Equipements pour utilisation à poste fixe partiellement à l'abri des intempéries – Faible degré de simulation	Essais de fiabilité
CEI 60605-3-4	Essais de fiabilité des équipements – Partie 3-4: Conditions d'essai préférentielles – Cycle d'essai n° 4: Equipements portatifs à utilisation en déplacement – Faible degré de simulation	Essais de fiabilité
CEI 60605-3-5	Essai de fiabilité des équipements – Partie 3-5: Conditions d'essai préférentielles – Cycle d'essai n° 5: Equipements montés sur véhicules terrestres – Faible degré de simulation	Essais de fiabilité
CEI 60605-3-6	Essais de fiabilité des équipements – Partie 3-6: Conditions d'essai préférentielles – Cycle d'essai n° 6: Equipements portatifs d'extérieur – Faible degré de simulation	Essais de fiabilité
CEI 60605-4	Essai de fiabilité des équipements – Partie 4: Méthodes statistiques de distribution exponentielle – Estimateurs ponctuels, intervalles de confiance, intervalles de prédiction et intervalles de tolérance	Essais de fiabilité – statistique
CEI 60605-6	Essais de fiabilité des équipements – Partie 6: Tests pour l'estimation du taux de défaillance constant et de l'intensité de défaillance constante	Analyse de données de sûreté de fonctionnement
CEI 60706-3	Maintenabilité de matériel – Partie 3 : Vérification et recueil, analyse et présentation des données	Essais de maintenabilité

Tableau A.1 *(suite)*

Norme identifiée	Titre de la norme	Technique d'essai couverte
CEI 60706-5	Maintenabilité de matériel – Partie 5: Essais pour diagnostic	Essais de maintenabilité
CEI 61014	Programmes de croissance de fiabilité	Programmes de croissance de fiabilité
CEI 61070	Procédures d'essai de conformité pour la disponibilité en régime établi	Démonstration de disponibilité
CEI 61123	Essai de fiabilité – Plans d'essai de conformité pour une proportion de succès	Plans d'essais de conformité – proportion de succès
CEI 61124	Essais de fiabilité – Plans d'essai de conformité d'un taux de défaillance constant et d'une intensité de défaillance constante	Plans d'essais de conformité – taux de défaillance et intensité de défaillance constante
CEI 61163-1	Déverminage sous contraintes – Partie 1 : Assemblages réparables fabriqués en lots	Déverminage sous contraintes
CEI 61163-2	Déverminage sous contraintes – Partie 2 : Composants électroniques	Déverminage sous contraintes
CEI 61164	Croissance de la fiabilité – Tests et méthodes d'estimation statistiques	Essais de croissance de la fiabilité et méthodes d'estimation
CEI 61649	Procédures pour les tests d'adéquation, les intervalles de confiance et les limites inférieures de confiance pour les données suivant la distribution de Weibull	Tests d'adéquation – Distribution de Weibull
CEI 61650	Techniques d'analyse des données de fiabilité – Procédures pour la comparaison de deux taux de défaillance constants et de deux intensités de défaillance (événements) constantes	Essais de fiabilité – statistique
CEI 61709	Composants électroniques – Fiabilité – Conditions de référence pour les taux de défaillance et modèles d'influence des contraintes pour la conversion	Essais de fiabilité – statistique
CEI 61710	Modèle de loi en puissance – Test d'adéquation et méthodes d'estimation des paramètres	Tests d'adéquation – Distribution de Weibull – modèle de loi en puissance

A.2 Techniques pour analyses de sûreté de fonctionnement

Le tableau A.2 donne des normes de référence pour la vérification et la validation de la sûreté de fonctionnement par analyses.

Tableau A.2 – Techniques pour la vérification et la validation de la sûreté de fonctionnement par analyses

Norme identifiée	Titre de la norme	Technique d'essai couverte
CEI 60300-3-1	Gestion de la sûreté de fonctionnement – Partie 3-1 : Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique	Revue des techniques d'analyse
CEI 60706-2	Maintenabilité de matériel – Partie2 : Etudes de maintenabilité au niveau de la conception	Analyse de maintenabilité
CEI 60812	Techniques d'analyse de la fiabilité des systèmes – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)	AMDE
CEI 61025	Analyse par arbre de panne (AAP)	Analyse par arbre de pannes

Tableau A.2 *(suite)*

Norme identifiée	Titre de la norme	Technique d'essai couverte
CEI 61078	Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthode booléenne	Blocs-diagrammes de fiabilité
CEI 61160	Revue de conception	Revue de conception formalisée
CEI 61165	Application des techniques de Markov	Techniques de Markov
CEI 61703	Expressions mathématiques pour les termes de fiabilité, de disponibilité, de maintenabilité et de logistique de maintenance	Expressions mathématiques
CEI 61713	Sûreté de fonctionnement des logiciels pendant leurs processus de cycle de vie – Guide d'application	Logiciel
CEI 62308	Fiabilité de l'équipement Méthodes d'évaluation de la fiabilité	Méthodes d'évaluation

Annexe B
(informative)

Exemples d'exigences de fiabilité, de maintenabilité, de support de maintenance et de disponibilité

B.1 Généralités

Des exemples de mesures de sûreté de fonctionnement sont donnés de l'Article B.2 à l'Article B.5. Les valeurs utilisées sont données uniquement pour illustrer comment elles sont établies dans la spécification. Il convient de ne pas les utiliser comme valeurs normalisées. Selon le produit, d'autres mesures peuvent s'appliquer. De plus, pour ces valeurs quantitatives, les exigences de vérification et de validation peuvent aussi être spécifiées avec les exigences de gestion de la sûreté de fonctionnement comme le souligne la présente norme.

NOTE Pour les définitions des mesures, voir la CEI 60050(191).

B.2 Exigences de disponibilité

Mesure de la performance de disponibilité	Symbole/abréviation	Exigence
Disponibilité moyenne	$\overline{A}(t_1,t_2)$	$\geq 0{,}9999$
Indisponibilité moyenne	$\overline{U}(t_1,t_{22})$	$\leq 10^{-4}$
Temps moyen d'arrêt	MDT	1h

B.3 Exigences de fiabilité

Mesure de la performance de fiabilité	Symbole/abréviation	Exigence
Taux de défaillance moyen	$\overline{\lambda}(t_1,t_2)$	$\leq 27\times10^{-6}$ / h
Temps moyen avant défaillance	MTTF	$\geq 37\,000$ h
Intensité de défaillance moyenne	$\overline{z}(t_1,t_2)$	$\leq 1{,}5$ / h
Temps moyen de fonctionnement entre défaillances	MTBF	$\geq 6\,000$ h
Durée de vie utile		≥ 8 ans
Fiabilité	$R(t_1,t_2)$ $t_1 = 100$ h $t_2 = 1100$ h	$\geq 0{,}9$
NOTE Les exigences établissent la valeur acceptable (valeur contractuelle) qu'il convient d'utiliser pour calculer le critère d'acceptation pour un test statistique.		

B.4 Exigences de maintenabilité

Mesure de la performance de maintenabilité	Symbole/abréviation	Exigence
Temps moyen de réparation	MRT	≤ 5 h
Temps moyen de maintenance corrective		≤ 5,5 h
Temps moyen de remise en état	MTTR	≤ 7h
Taux de couverture de pannes		≥ 0,95
Taux de couverture de réparations		≥ 0,8

B.5 Exigences de support de maintenance

Mesure de la performance de support de maintenance	Symbole/abréviation	Exigence
Délai administratif moyen	MAD	2 h
Délai moyen de logistique	MLD	1h
Probabilité de pénurie de pièces de rechange		0,005

Bibliographie

CEI 60605-2, *Essai de fiabilité des équipements – Partie 2: Conception des cycles d'essai*

CEI 60605-3-1, *Essai de fiabilité des équipements – Troisième partie: Conditions d'essai préférentielles. Equipements portatifs d'intérieur – Faible degré de simulation*

CEI 60605-3-2, *Essai de fiabilité des équipements – Partie 3-2: Conditions d'essai préférentielles – Equipement pour utilisation à poste fixe à l'abri des intempéries – Degré de simulation élevé*

CEI 60605-3-3, *Essai de fiabilité des équipements – Partie 3-3: Conditions d'essai préférentielles – Cycle d'essai n° 3: Equipements pour utilisation à poste fixe partiellement à l'abri des intempéries – Faible degré de simulation*

CEI 60605-3-4, *Essais de fiabilité des équipements – Partie 3-4: Conditions d'essai préférentielles – Cycle d'essai n° 4: Equipements portatifs à utilisation en déplacement – Faible degré de simulation*

CEI 60605-3-5, *Essai de fiabilité des équipements – Partie 3-5: Conditions d'essai préférentielles – Cycle d'essai n° 5: Equipements montés sur véhicules terrestres - Faible degré de simulation*

CEI 60605-3-6, *Essais de fiabilité des équipements – Partie 3-6: Conditions d'essai préférentielles – Cycle d'essai n° 6: Equipements portatifs d'extérieur - Faible degré de simulation*

CEI 60605-6, *Essais de fiabilité des équipements – Partie 6: Tests de validité des hypothèses du taux de défaillance constant ou de l'intensité de défaillance constante*

CEI 60812, *Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

CEI 61165, *Application des techniques de Markov*

CEI 61508-0, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie: Sécurité fonctionnelle et CEI 61508*

CEI 61508-1, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

CEI 61508-2, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 2: Prescriptions pour les systèmes électriques /électroniques /électroniques programmables relatifs à la sécurité*

CEI 61508-3, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 3: Prescriptions concernant les logiciels*

CEI 61508-4, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 61508-5, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité*

CEI 61508-6, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

CEI 61508-7, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

CEI 61650, *Techniques d'analyse des données de fiabilité – Procédures pour la comparaison de deux taux de défaillance constants et de deux intensités de défaillance (événements) constantes*

CEI 61709, *Composants électroniques – Fiabilité – Conditions de référence pour les taux de défaillance et modèles d'influence des contraintes pour la conversion*

Autres publications

[1] Def Stan 00-42 (Part 3) Issue 2. Reliability & Maintainability (R&M) Assurance Guidance. R&M Case. DStan, Glasgow available from www.dstan.mod.uk

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
P.O. Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch