

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

300-3-4

Première édition
First edition
1996-08

Gestion de la sûreté de fonctionnement –

Partie 3:

Guide d'application –

**Section 4: Specification d'exigences
de sûreté de fonctionnement**

Dependability management –

Part 3:

Application guide –

**Section 4: Guide to the specification
of dependability requirements**



Numéro de référence
Reference number
CEI/IEC 300-3-4: 1996

Validité de la présente publication

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique.

Des renseignements relatifs à la date de reconfirmation de la publication sont disponibles auprès du Bureau Central de la CEI.

Les renseignements relatifs à ces révisions, à l'établissement des éditions révisées et aux amendements peuvent être obtenus auprès des Comités nationaux de la CEI et dans les documents ci-dessous:

- **Bulletin de la CEI**
- **Annuaire de la CEI**
Publié annuellement
- **Catalogue des publications de la CEI**
Publié annuellement et mis à jour régulièrement

Terminologie

En ce qui concerne la terminologie générale, le lecteur se reportera à la CEI 50: *Vocabulaire Electrotechnique International* (VEI), qui se présente sous forme de chapitres séparés traitant chacun d'un sujet défini. Des détails complets sur le VEI peuvent être obtenus sur demande. Voir également le dictionnaire multilingue de la CEI.

Les termes et définitions figurant dans la présente publication ont été soit tirés du VEI, soit spécifiquement approuvés aux fins de cette publication.

Symboles graphiques et littéraux

Pour les symboles graphiques, les symboles littéraux et les signes d'usage général approuvés par la CEI, le lecteur consultera:

- la CEI 27: *Symboles littéraux à utiliser en électro-technique;*
- la CEI 417: *Symboles graphiques utilisables sur le matériel. Index, relevé et compilation des feuilles individuelles;*
- la CEI 617: *Symboles graphiques pour schémas;*

et pour les appareils électromédicaux,

- la CEI 878: *Symboles graphiques pour équipements électriques en pratique médicale.*

Les symboles et signes contenus dans la présente publication ont été soit tirés de la CEI 27, de la CEI 417, de la CEI 617 et/ou de la CEI 878, soit spécifiquement approuvés aux fins de cette publication.

Publications de la CEI établies par le même comité d'études

L'attention du lecteur est attirée sur les listes figurant à la fin de cette publication, qui énumèrent les publications de la CEI préparées par le comité d'études qui a établi la présente publication.

Validity of this publication

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology.

Information relating to the date of the reconfirmation of the publication is available from the IEC Central Office.

Information on the revision work, the issue of revised editions and amendments may be obtained from IEC National Committees and from the following IEC sources:

- **IEC Bulletin**
- **IEC Yearbook**
Published yearly
- **Catalogue of IEC publications**
Published yearly with regular updates

Terminology

For general terminology, readers are referred to IEC 50: *International Electrotechnical Vocabulary* (IEV), which is issued in the form of separate chapters each dealing with a specific field. Full details of the IEV will be supplied on request. See also the IEC Multilingual Dictionary.

The terms and definitions contained in the present publication have either been taken from the IEV or have been specifically approved for the purpose of this publication.

Graphical and letter symbols

For graphical symbols, and letter symbols and signs approved by the IEC for general use, readers are referred to publications:

- IEC 27: *Letter symbols to be used in electrical technology;*
- IEC 417: *Graphical symbols for use on equipment. Index, survey and compilation of the single sheets;*
- IEC 617: *Graphical symbols for diagrams;*

and for medical electrical equipment,

- IEC 878: *Graphical symbols for electromedical equipment in medical practice.*

The symbols and signs contained in the present publication have either been taken from IEC 27, IEC 417, IEC 617 and/or IEC 878, or have been specifically approved for the purpose of this publication.

IEC publications prepared by the same technical committee

The attention of readers is drawn to the end pages of this publication which list the IEC publications issued by the technical committee which has prepared the present publication.

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

300-3-4

Première édition
First edition
1996-08

Gestion de la sûreté de fonctionnement –

Partie 3:

Guide d'application –

**Section 4: Spécification d'exigences
de sûreté de fonctionnement**

Dependability management –

Part 3:

Application guide –

**Section 4: Guide to the specification
of dependability requirements**

© CEI 1996 Droits de reproduction réservés — Copyright - all rights reserved

Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher

Bureau central de la Commission Electrotechnique Internationale 3, rue de Varembe Genève, Suisse



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

Q

● Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

	Pages
AVANT-PROPOS	4
INTRODUCTION	6
 Articles	
1 Domaine d'application	8
2 Références normatives	8
3 Définitions	10
4 Considérations générales pour la spécification des exigences de sûreté de fonctionnement	12
5 Spécification des caractéristiques de fiabilité	14
6 Spécification des caractéristiques de maintenabilité	22
7 Spécification des caractéristiques de disponibilité	24
8 Spécification du soutien logistique de maintenance	28
9 Coopération entre le client et le fournisseur	30
 Annexe A – Exemples d'exigences de fiabilité, de maintenabilité, de soutien logistique de maintenance et de disponibilité	 32

CONTENTS

	Page
FOREWORD	5
INTRODUCTION	7
Clause	
1 Scope	9
2 Normative references	9
3 Definitions	11
4 General considerations when specifying dependability requirements	13
5 Specifying reliability performance	15
6 Specifying maintainability performance	23
7 Specifying availability performance	25
8 Specifying maintenance support	29
9 Cooperation between customer and supplier	31
Annexe A – Examples of reliability, maintainability, maintenance support and availability requirements	33

COMMISSION ÉLECTRONIQUE INTERNATIONALE

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 3: Guide d'application –

Section 4: Spécification d'exigences de sûreté de fonctionnement

AVANT-PROPOS

- 1) La CEI (Commission Electrotechnique Internationale) 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. 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 intéressés sont représentés dans chaque comité d'études.
- 3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
- 4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes Internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la recommandation de la CEI et la norme nationale correspondante doit être indiquée en termes clairs dans cette dernière.
- 5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
- 6) L'attention est attirée sur le fait que certains des éléments de la présente Norme internationale 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 300-3-4 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/493/FDIS	56/519/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.

La CEI 300 comprend les parties suivantes, présentées sous le titre général *Gestion de la sûreté de fonctionnement*:

Partie 1: Gestion du programme de sûreté de fonctionnement

Partie 2: Eléments et tâches du programme de sûreté de fonctionnement

Partie 3: Série de guides d'application

L'annexe A est donnée uniquement à titre d'information.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

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

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 300-3-4 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/493/FDIS	56/519/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.

IEC 300 consists of the following parts, under the general title *Dependability management*:

- Part 1: Dependability programme management
- Part 2: Dependability programme elements and tasks
- Part 3: A series of application guides

Annex A is for information only.

INTRODUCTION

Les caractéristiques de fiabilité, de maintenabilité et de disponibilité sont essentielles pour de nombreux produits. Ces caractéristiques, associées au soutien logistique, sont désignées par l'expression collective «sûreté de fonctionnement».

Pour les produits dont la fiabilité, la disponibilité et la maintenabilité sont importantes, il convient de définir et de spécifier ces caractéristiques de la même façon que d'autres caractéristiques du produit comme les caractéristiques techniques, les dimensions, la masse, etc.

Les niveaux de fiabilité, de maintenabilité, de disponibilité et du soutien logistique associé atteints par un produit dépendent des conditions dans lesquelles le produit est utilisé. Quand on spécifie des exigences de sûreté de fonctionnement, il est nécessaire de définir les conditions de stockage, de transport, d'installation et d'utilisation qui seront appliquées au produit. Il peut aussi être important de prendre en compte, non seulement les conditions d'exploitation du produit, mais aussi la politique de maintenance, l'organisation du soutien logistique de maintenance associé au produit.

Il est nécessaire d'utiliser des méthodes statistiques pour évaluer les caractéristiques de sûreté de fonctionnement obtenues.

Tout comme les autres caractéristiques, les caractéristiques de sûreté de fonctionnement peuvent être définies dans trois sortes de spécifications:

- **des spécifications établies par le fournisseur**

C'est le cas, notamment, pour les produits qui doivent avoir certaines caractéristiques de sûreté de fonctionnement – par exemple de fiabilité – pour être acceptés sur le marché.

- **des spécifications établies par le client**

C'est le cas généralement pour les produits courants qui doivent répondre à certaines caractéristiques de sûreté de fonctionnement afin de répondre aux besoins du client.

- **des spécifications acceptées ou établies à la fois par le fournisseur et par le client**

C'est normalement le cas pour les produits faits à la demande ou pour les modifications de conceptions existantes.

INTRODUCTION

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

In products where reliability, availability and maintainability are important, it is necessary that these characteristics should be defined and specified in the same way as other product characteristics such as technical performance, dimensions, mass, etc.

The levels of reliability, maintainability, availability and maintenance support performance achieved by a product depend on the conditions under which the product is used. 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 product. It may be important to take account not only of the conditions under which the product will operate, but also of the maintenance policy and organization for maintenance support of the product.

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 types of specifications:

- **specifications produced by the supplier**

These are mainly used for products that need to have certain dependability characteristics, for example reliability, in order to be accepted in the market place.

- **specifications produced by the customer**

These are mainly used for standard products that have to meet certain dependability characteristics in order to satisfy the customer's needs.

- **specifications mutually agreed or produced by the supplier and the customer**

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

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

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

1 Domaine d'application

La présente section de la CEI 300-3 donne des recommandations pour spécifier les caractéristiques de sûreté de fonctionnement qui sont prescrites dans les spécifications de produits et de matériels, ainsi que pour spécifier les procédures et les critères de vérification.

On trouve notamment les recommandations suivantes:

- des conseils pour spécifier des exigences quantitatives et qualitatives de fiabilité, de maintenabilité et de disponibilité;
- des conseils pour aider les clients d'un produit à vérifier que les fournisseurs pourront tenir ces exigences;
- des conseils pour aider les fournisseurs à se conformer aux exigences du client.

NOTES

- 1 Le but de la présente norme n'est pas de donner des recommandations sur la gestion de la maintenabilité et de la fiabilité ni sur les étapes qui sont nécessaires pour que soient satisfaites les exigences de fiabilité, de maintenabilité et de disponibilité qui ont été fixées. Pour ces recommandations générales on consultera les autres parties de la CEI 300.
- 2 Le présent guide ne prend pas en compte les spécifications de sécurité.
- 3 On peut trouver dans la CEI 409 des recommandations pour introduire des exigences de fiabilité dans les spécifications de composants (ou de pièces détachées) pour les matériels électroniques.
- 4 On peut trouver dans la CEI 319 des recommandations sur la présentation des données de fiabilité pour les composants électroniques.

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente section de la CEI 300-3. Au moment de la publication, les éditions indiquées étaient en vigueur. Tout document normatif est sujet à révision et les parties prenantes aux accords fondés sur la présente section de la CEI 300-3 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 50(191): 1990, *Vocabulaire Electrotechnique International (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 300-1: 1993, *Gestion de la sûreté de fonctionnement – Partie 1: Gestion du programme de sûreté de fonctionnement*

CEI 300-2: 1995, *Gestion de la sûreté de fonctionnement – Partie 2: Eléments et tâches du programme de sûreté de fonctionnement*

CEI 300-3-1: 1991, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 1: Techniques d'analyse de la sûreté de fonctionnement: Guide méthodologique*

DEPENDABILITY MANAGEMENT –

Part 3: Application guide –

Section 4: Guide to the specification of dependability requirements

1 Scope

This section of IEC 300 gives guidance on specifying required dependability characteristics in product and equipment specifications, together with specifications of procedures and criteria for verification.

The guidance provided includes the following:

- advice on specifying quantitative and qualitative reliability, maintainability and availability requirements;
- advice to customers of a product to help them to ensure that the specified requirements will be fulfilled by suppliers;
- advice to suppliers to help them to meet customer requirements.

NOTES

- 1 It is not the intention of this standard to give guidance on the management of reliability and maintainability programmes or on the various activities necessary to fulfil stated reliability, maintainability and availability requirements. For this general guidance see other parts of IEC 300.
- 2 Safety specifications are not considered in this guide.
- 3 Guidance for the inclusion of reliability clauses in specifications for components (or parts) for electronic equipment is given in IEC 409.
- 4 Guidance for presentation of reliability data on electronic components can be found in IEC 319.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this section of IEC 300-3. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this section of IEC 300-3 are encouraged to investigate the possibility of applying the most recent editions of the normative documents listed below. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 50(191): 1990, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 300-1: 1993, *Dependability management – Part 1: Dependability programme management*

IEC 300-2: 1995, *Dependability management – Part 2: Dependability programme elements and tasks*

IEC 300-3-1: 1991, *Dependability management – Part 3: Application guide – Section 1: Analysis techniques for dependability: Guide on methodology*

CEI 300-3-2: 1993, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 2: Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation*

CEI 319: 1978, *Présentation des données de fiabilité pour les composants (ou pièces détachées) électroniques*

CEI 409: 1981, *Guide pour l'inclusion de clauses de fiabilité dans les spécifications de composants (ou pièces détachées) pour l'équipement électronique*

CEI 605-1: 1978, *Essais de fiabilité des équipements – Première partie: Prescriptions générales*

CEI 605-6: 1986, *Essais de fiabilité des équipements – Sixième partie: Tests de validité de l'hypothèse d'un taux de défaillance constant*

CEI 706-1: 1982, *Guide de maintenabilité de matériel – Première partie – Sections un, deux et trois: Introduction, exigences et programme de maintenabilité*

CEI 706-3: 1987, *Guide de maintenabilité de matériel – Troisième partie – Sections six et sept: Vérification et recueil, analyse et présentation des données*

CEI 706-5: 1994, *Guide de maintenabilité de matériel – Partie 5 – Section 4: Essais pour diagnostic*

CEI 706-6: 1994, *Guide de maintenabilité du matériel – Partie 6 – Section 9: Méthodes statistiques pour l'évaluation de la maintenabilité*

CEI 863: 1986, *Présentation des résultats de la prévision des caractéristiques de fiabilité, maintenabilité et disponibilité*

CEI 1070: 1991, *Procédure d'essai de conformité pour la disponibilité en régime établi*

CEI 1123: 1991, *Essai de fiabilité. Plans d'essai de conformité pour une proportion de succès*

CEI/FDIS 1124, *Essais de fiabilité – Plans d'essai de conformité pour un taux de défaillance constant et une intensité de défaillance constante (en préparation)*

ISO 8402: 1994, *Management de la qualité et assurance de la qualité – Vocabulaire*

ISO 9000-4: 1993, *Normes pour la gestion de la qualité et l'assurance de la qualité – Partie 4: Guide de gestion du programme de sûreté de fonctionnement*

3 Définitions

Pour les besoins de la présente section de la CEI 300-3, les définitions données dans la CEI 50(191) et l'ISO 8402 s'appliquent, notamment les définitions ci-après:

3.1 sûreté de fonctionnement: Ensemble des propriétés qui décrivent la disponibilité et les facteurs qui la conditionnent: fiabilité, maintenabilité et logistique de maintenance. [VEI 191-02-03]

NOTE – La sûreté de fonctionnement est une notion générale sans caractère quantitatif.

IEC 300-3-2: 1993, *Dependability management – Part 3: Application guide – Section 2: Collection of dependability data from the field*

IEC 319: 1978, *Presentation of reliability data on electronic components (or parts)*

IEC 409: 1981, *Guide for the inclusion of reliability clauses into specifications for components (or parts) for electronic equipment*

IEC 605-1: 1978, *Equipment reliability testing – Part 1: General requirements*

IEC 605-6: 1986, *Equipment reliability testing – Part 6: Tests for the validity of a constant failure rate assumption*

IEC 706-1: 1982, *Guide on maintainability of equipment – Part 1 – Sections One, Two and Three: Introduction, requirements and maintainability programme*

IEC 706-3: 1987, *Guide on maintainability of equipment – Part 3 – Sections Six and Seven: Verification and collection, analysis and presentation of data*

IEC 706-5: 1994, *Guide on maintainability of equipment – Part 5 – Section 4: Diagnostic testing*

IEC 706-6: 1994, *Guide on maintainability of equipment – Part 6 – Section 9: Statistical methods in maintainability evaluation*

IEC 863: 1986, *Presentation of reliability, maintainability and availability predictions*

IEC 1070: 1991, *Compliance test procedures for steady-state availability*

IEC 1123: 1991, *Reliability testing – Compliance test plans for success ratio*

IEC/FDIS 1124, *Reliability testing – Compliance test plans for constant failure rate and constant failure intensity (under preparation)*

ISO 8402: 1994, *Quality management and quality assurance – Vocabulary*

ISO 9000-4: 1993, *Quality management and quality assurance standards – Part 4: Guide to dependability programme management*

3 Definitions

For the purpose of this section of IEC 300-3, the definitions given in IEC 50 (191) and ISO 8402 apply, and in particular the following:

3.1 dependability: The collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance. [IEV 191-02-03]

NOTE – Dependability is used only for general descriptions in non-quantitative terms.

3.2 organisme: Compagnie, société, firme, entreprise ou institution, ou partie de celles-ci, à responsabilité limitée ou d'un autre statut, de droit public ou privé, qui a sa propre structure fonctionnelle et administrative. [ISO 8402]

3.3 fournisseur: Organisme qui fournit un produit au client. [ISO 8402]

3.4 client: Destinataire d'un produit fourni par le fournisseur. [ISO 8402]

3.5 vérification: Confirmation par examen et apport de preuves tangibles que les exigences spécifiées ont été satisfaites. [ISO 8402]

4 Considérations générales pour la spécification des exigences de sûreté de fonctionnement

Il est recommandé d'exprimer de façon quantitative toutes les exigences de fiabilité, de maintenabilité et de disponibilité chaque fois que cela est possible, mais il peut aussi être utile d'inclure des exigences qualitatives dans les spécifications. On détermine les exigences en tenant compte des besoins du client et en fonction de l'utilisation qui est prévue pour le produit.

Il convient de choisir des exigences réalistes, compatibles avec l'état de l'art.

Il convient que les exigences de sûreté de fonctionnement fassent partie de tout accord entre le client et le fournisseur chaque fois qu'il en existe un.

La spécification peut aussi définir les méthodes à suivre pour vérifier que les caractéristiques spécifiées de fiabilité, de maintenabilité ou de disponibilité sont bien satisfaites. Il est essentiel que les exigences relatives aux caractéristiques de sûreté de fonctionnement soient vérifiables et il convient que les méthodes de vérification soient mutuellement acceptées.

Il est particulièrement important de définir soigneusement les divers éléments suivants:

- la nature exacte du produit à considérer: par exemple le système, le matériel ou l'assemblage auxquels s'appliquent les exigences;
- les critères précis selon lesquels la fiabilité, la maintenabilité ou la disponibilité doivent être évaluées. Il est particulièrement important de définir exactement ce qui constitue une panne du produit en se référant, si nécessaire, à une spécification particulière de fonctionnement.

C'est le fournisseur qui est responsable de la conformité du produit aux exigences de fiabilité, de disponibilité et de maintenabilité en tenant compte des trois aspects suivants:

- la forme suivant laquelle les exigences sont exprimées;
- les dispositions relatives à la logistique de maintenance;
- les méthodes à utiliser pour évaluer les caractéristiques requises.

Les niveaux des caractéristiques de fiabilité et de maintenabilité observées sur un produit sont étroitement liés aux conditions d'installation et d'exploitation. Lors de la définition des exigences de sûreté de fonctionnement, il est donc important de préciser les conditions suivantes:

- la fonction prévue pour le produit (matériel ou système);
- les conditions d'installation et d'exploitation;
- la définition d'une panne, c'est-à-dire ce qui constitue une panne d'un dispositif particulier dans l'application pour laquelle il est prévu;

3.2 organization: Company, corporation, firm, enterprise or institution, or part thereof, whether incorporated or not, public or private, that has its own functions and administration. [ISO 8402]

3.3 supplier: Organization that provides a product to the customer. [ISO 8402]

3.4 customer: Recipient of a product provided by the supplier. [ISO 8402]

3.5 verification: Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled. [ISO 8402]

4 General considerations when specifying dependability requirements

All reliability, maintainability and availability requirements should be expressed quantitatively wherever possible, but it may also be appropriate to specify qualitative requirements in the specifications. Requirements are determined according to the needs of customers and how it is intended to use the product.

Requirements should be realistic and should be compatible with the technological state of the art.

Where a customer/supplier agreement is involved, the requirements should form a part of the agreement.

The specification should also specify the procedures to be used to verify that the specified reliability, maintainability or availability performance is met. It is essential that the dependability performance requirements are verifiable and the methods of verification should be mutually agreed.

It is particularly important to define precisely:

- the product under consideration for example, the system, equipment or assembly to which the requirements apply;
- the exact criteria by which reliability, maintainability or availability are to be judged. It is especially important to define exactly what constitutes a product fault, if necessary, by reference to a detailed performance specification.

It is the responsibility of the supplier to ensure that the product conforms to the required reliability, availability and maintainability performances, taking into account:

- the form in which the requirements are expressed;
- the arrangements for maintenance support;
- the methods to be used to assess the required characteristics.

The levels of reliability and maintainability performance achieved by a product are strongly influenced by the conditions in which it is installed and operated. When specifying dependability requirements it is important to state the following:

- the intended function of the product (equipment or system);
- how the equipment will be installed and used;
- the definition of fault, that is what constitutes a fault in this particular item in the intended application;

- les obligations et les responsabilités respectives du client, du fournisseur et d'une éventuelle tierce partie;
- les conditions diverses d'exploitation et d'environnement dans lesquelles le matériel est utilisé, y compris, si nécessaire, les durées correspondantes pour chaque condition;
- les méthodes prévues pour la vérification de conformité avec les exigences;
- les qualifications et les responsabilités du personnel chargé de l'exploitation et de la maintenance du matériel;
- la politique de maintenance à appliquer ainsi que les instructions et le soutien logistique associés.

NOTE – L'importance du soutien logistique de maintenance est très souvent déjà déterminée par la condition d'utilisation et ne résulte pas d'une exigence concernant intrinsèquement le produit lui-même.

Il convient de choisir les caractéristiques de sûreté de fonctionnement à spécifier selon l'application et le type de produit; par exemple, on considérera seulement des exigences de fiabilité si aucune action de maintenance n'est prévue.

Il est recommandé de spécifier des exigences de maintenabilité pour des matériels si les coûts de maintenance affectent le coût du cycle de vie ou si la maintenance a de l'importance pour l'utilisateur. On peut prescrire des exigences de maintenance préventive si ce type de maintenance s'applique au produit.

On prescrit généralement des exigences de disponibilité pour des produits (systèmes) dont les temps d'indisponibilité sont très coûteux ou contraires à la sécurité du personnel, par exemple les gros systèmes, les usines de production, les matériels médicaux, les matériels de sécurité. On peut calculer la disponibilité à partir de la configuration du système, de la fiabilité de ses sous-ensembles et à partir des exigences de maintenabilité sur ces sous-ensembles si elles sont déterminées; on tient compte également des conditions de logistique de maintenance.

Il convient, dans la spécification de sûreté de fonctionnement, d'attirer l'attention sur les différents éléments qui peuvent influencer le coût de la garantie de fiabilité et de maintenabilité. Ce coût comprend la durée de vie attendue et la mise au rebut ou le recyclage du produit.

5 Spécification des caractéristiques de fiabilité

5.1 Exigences de fiabilité

5.1.1 Exigences quantitatives

Il est recommandé de spécifier des exigences de fiabilité quantitatives et de les spécifier avant le début de la conception du produit.

Pour chaque produit, il est nécessaire de choisir et de définir chacune des caractéristiques de sûreté de fonctionnement à spécifier, et de prescrire pour chacune d'entre elles une exigence quantitative. Lorsque l'on fixe des exigences quantitatives pour un dispositif, il est important d'établir:

- l'application dans laquelle le dispositif sera utilisé;
- la définition d'une panne, c'est-à-dire ce qui constitue une panne pour ce dispositif particulier dans l'application pour laquelle il est prévu.

NOTE – Une panne peut être définie de plusieurs façons selon ses conséquences; par exemple par la perte de service, la nécessité d'une réparation.

- les conditions d'exploitation;
- les conditions d'environnement;
- les méthodes prévues pour la vérification de la conformité aux exigences.

- the obligations and responsibilities of customer, supplier and any third parties;
- the various operating and environmental conditions under which the equipment is used including, where applicable, the relative amount of time spent in each condition;
- the methods intended to be applied for verification of compliance with the requirements;
- the qualifications and responsibilities of the personnel responsible for operating and maintaining the equipment;
- the maintenance policy to be applied and the associated procedures and support arrangements.

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

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

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

Availability performance requirements are generally specified for products (systems) where down time could cause considerable economic loss or personnel injury, for example, large systems, production plants, medical equipment, safety equipment. 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.

The dependability specification should draw attention to the various factors likely to affect the cost of reliability and maintainability assurance. This includes the expected lifetime and disposal or recycling of the product.

5 Specifying reliability performance

5.1 Reliability requirements

5.1.1 Quantitative requirements

Reliability performance requirements should be quantitative and should be specified before design of the product begins.

For every product 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 an item it is important to state the following:

- the item's application;
- the definition of a fault i.e. what constitutes a fault in the particular item in the intended application;

NOTE – A fault may be defined in various ways according to the consequences, for example, the loss of a service, the need for repair.

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

Sans la connaissance de ces conditions, la spécification d'une mesure de la fiabilité telle que le MTTF, le MTBT et $R(t)$ n'aurait aucun sens.

Lorsque l'on choisit la valeur d'une caractéristique de fiabilité à spécifier, il convient de prendre en compte les facteurs suivants:

- les limites imposées par l'état de l'art (voir article 4), la nature et la complexité du produit (matériel ou système);
- l'expérience de l'utilisateur dans l'exploitation et la maintenance de ce type particulier de matériel;
- les possibilités de vérification de cette exigence;
- le niveau de fiabilité des unités, des composants, etc., à partir desquels le dispositif peut être fabriqué;
- le coût de la conception, de la production et de la vérification d'un dispositif d'un niveau spécifié de fiabilité.

S'il devient clair, au cours de l'étude du projet, que les hypothèses de base ne sont pas correctes, il peut être nécessaire de revoir et de modifier les exigences de fiabilité.

Si la spécification doit être modifiée, il convient que cela soit fait avec l'accord de toutes les parties prenantes.

Il convient de spécifier clairement les exigences quantitatives, dans une forme qui permette la comparaison avec les résultats qui seront obtenus ultérieurement.

Lorsque la conformité aux exigences quantitatives est à vérifier à l'aide d'essais, selon les indications de 5.2.1, il est nécessaire de spécifier le niveau de confiance requis ou de spécifier le plan d'essai à utiliser. Si un plan d'essai est spécifié, il convient que la spécification inclue la valeur de la durée de l'essai ainsi que les critères d'acceptation et de rejet.

Si l'on sait ou si l'on suppose que la caractéristique de fiabilité spécifiée dépend du temps, il convient de spécifier cette loi d'influence par exemple par une valeur moyenne de l'intensité de défaillance pour les premiers mois d'utilisation. Voir CEI 605-1 pour plus d'informations sur les répartitions statistiques possibles.

5.1.2 Exigences qualitatives

On peut exprimer des exigences qualitatives de fiabilité de deux façons:

- par des conditions à respecter lors de la conception du produit;
- par des tâches d'amélioration de la fiabilité à exécuter pendant les phases du cycle de vie du produit.

Les conditions à la conception sont en général prescrites seules mais elles peuvent aussi compléter des exigences quantitatives. De telles conditions peuvent constituer indirectement des exigences de fiabilité sur le produit lui-même, sur son mode d'installation et sur le mode de surveillance de ses caractéristiques. Les conditions suivantes sont des exemples possibles:

- une condition sur les pannes simples: par exemple, le produit doit être tel qu'aucune panne simple ne puisse conduire à un état critique du produit;
- une condition sur l'accumulation des pannes: par exemple, le produit doit être tel qu'aucune défaillance non détectée ne puisse conduire à une panne du système lorsqu'elle se combine à une nouvelle panne;

Without such statements the specification of a reliability performance measure such as MTTF, MTBF and $R(t)$ 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 (see clause 4) and the nature and complexity of the product (equipment or system);
- the experience of the user in operating and maintaining the particular type of equipment;
- the feasibility of verifying the specified requirement;
- the reliability level of units, components etc., from which the item can be manufactured;
- the cost of design, production and verification of the item 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 may 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 verification of conformity to the quantitative requirements is to be done through testing, as described in 5.2.1, it is necessary to specify the confidence level required, or to specify the actual test plan to be used. If a test plan is specified the specification should include the test duration and the acceptance/rejection criteria.

If the specified reliability performance measure is known, or is likely to vary with time, the dependency should be specified by, for example, specifying a mean failure intensity over the first months of use. See IEC 605-1 for information on statistical distribution.

5.1.2 Qualitative requirements

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

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

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

- single fault criterion, i.e. the product has to be such that no single fault can lead to a critical state of the product;
- accumulating fault criterion, i.e. the product has to be such that no undetected fault, when combined with additional faults, can cause system failure;

- une condition sur la séparation des chemins: l'indépendance de sous-systèmes en redondance doit être conservée grâce à la séparation des chemins pour les câbles, les conduits, etc., pour le cheminement des signaux, les alimentations et les alimentations auxiliaires;
- une condition sur la surveillance des fonctions critiques: on prescrit le contrôle automatique ou manuel des fonctions critiques, en permanence ou à certains intervalles de temps, dans le but de maintenir la valeur prescrite de la fiabilité.

En outre, lorsque l'on spécifie des exigences quantitatives de fiabilité, il peut être souvent utile de définir une séquence de tâches à effectuer pendant les phases du cycle de vie des produits pour améliorer la fiabilité (et la maintenabilité). De telles exigences qualitatives peuvent porter aussi bien sur le matériel que sur le logiciel et la logistique. Elles sont particulièrement importantes lorsque les exigences quantitatives ne spécifient pas avec suffisamment de précision les caractéristiques de fiabilité du produit. Il est recommandé au client et au fournisseur de s'entendre sur ces exigences aussi bien du point de vue technique que sur le calendrier à respecter et les coûts. Il est également recommandé de rendre officielles ces exigences qualitatives et de les gérer grâce à un plan de fiabilité (ou un plan de sûreté de fonctionnement) comme défini dans la CEI 300-2.

Il convient d'adapter le programme de sûreté de fonctionnement à la nature du produit et aux exigences spécifiées et qu'il comprenne typiquement les éléments suivants:

- les méthodes d'analyse à appliquer;
- un programme de croissance de la fiabilité, si nécessaire;
- l'indication des méthodes à suivre pour vérifier la conformité aux exigences (voir CEI 605-1) ou à toute autre caractéristique qualitative ou quantitative exprimant le degré de conformité aux exigences;
- les critères de choix des composants et les dispositions pour l'assurance de la qualité;
- l'analyse du pire cas.

5.2 Vérification de la fiabilité

5.2.1 Généralités

Il est recommandé de stipuler dans la spécification les méthodes permettant de vérifier que les exigences spécifiées ont été satisfaites.

On peut vérifier la fiabilité soit par des analyses pendant la conception et avant la production, soit par des essais en laboratoire ou par des essais en exploitation après la production, soit par un suivi des caractéristiques en exploitation après la mise en service.

Les paragraphes 5.2.2 et 5.2.3 donnent des recommandations sur des méthodes possibles de vérification ainsi que sur ce qu'elles impliquent.

5.2.2 Vérification par des essais en exploitation ou en laboratoire

Les méthodes préférentielles d'essais de vérification incluent:

- l'acquisition et l'analyse des données de défaillance concernant les produits en exploitation, c'est-à-dire en utilisation réelle;
- les essais de produits en exploitation, ou en laboratoire, en utilisant des tests de conformité ou de détermination de fiabilité tels que ceux décrits dans la CEI 1123.

- 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 product 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 with sufficient precision the reliability performance of the product. They should be mutually agreed between customer 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), as specified in IEC 300-2.

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

- the types of analysis methods to be applied;
- a reliability growth programme, if necessary;
- statements about how to verify conformity to the requirements (see IEC 605-1) 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 assurance;
- worst case analysis.

5.2 Reliability verification

5.2.1 General

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

Reliability verification may be done either by analysis during the design and before production, by laboratory tests or field tests after production or by field performance evaluation after delivery.

Subclauses 5.2.2 and 5.2.3 give guidance on the possible verification methods and their implications.

5.2.2 Verification by field or laboratory testing

Preferred methods of verification testing include:

- the collection and analysis of failure data from products in the field i.e. in actual use;
- testing products in the field or in the laboratory, using compliance or determination tests as described in IEC 1123.

Il convient de spécifier des critères précis afin de permettre la classification des défaillances du matériel et du logiciel en défaillance à prendre en compte ou non.

Cette classification est la base des critères d'acceptation et de rejet et il est essentiel qu'elle soit définie avec clarté et précision avant le début des essais.

Les procédures de vérification sont normalement choisies par accord entre le client et le fournisseur à partir d'essais en exploitation ou d'essais en laboratoire selon les principes suivants:

- les essais en exploitation sont souvent préférés mais leur validité nécessite de disposer d'un système suffisant d'acquisition de résultats en exploitation. On consultera la CEI 605-1 et la CEI 300-3-2 pour la spécification des exigences;
- vérification par des essais en laboratoire, selon la CEI 605-1. Lorsque l'on spécifie des essais en laboratoire, il est important de tenir compte de sujétions comme les coûts et les temps qui sont associés à ces tâches.

Il faut traiter séparément la vérification de la fiabilité sur des dispositifs réparables et sur des dispositifs non réparables.

Si la fiabilité est caractérisée par un rapport de succès, il convient d'utiliser la CEI 1123.

Si les exigences de fiabilité reposent sur l'hypothèse d'un taux de défaillance constant ou d'une intensité de défaillance constante, il est nécessaire de choisir un plan d'essai de conformité selon la CEI/FDIS 1124. Afin d'établir la validité de l'hypothèse d'un taux de défaillance constant ou d'une intensité de défaillance constante, on peut appliquer la CEI 605-6.

5.2.3 Vérification par analyse

On peut vérifier la fiabilité d'un produit avant la livraison à l'aide de calculs fondés sur l'analyse de fiabilité. Cette méthode peut être utilisée bien avant qu'il ne soit possible, immédiatement, de vérifier la fiabilité d'un produit en exploitation ou par des essais en laboratoire. Une telle vérification ne peut cependant que déterminer si le produit à livrer satisfait aux seules exigences figurant dans la spécification du produit; elle ne caractérise pas directement la fiabilité obtenue.

Les diagrammes de fiabilité, les arbres de pannes, les diagrammes d'états, l'analyse des modes de pannes et de leurs effets sont des exemples de méthodes de vérification par analyse de la fiabilité d'un dispositif, par exemple un système comprenant du matériel et du logiciel. La CEI 300-3-1 donne des recommandations sur ces différents outils d'analyse.

Il convient d'analyser la partie matérielle d'un système et de prouver que les taux de défaillance associés à chacun de ses sous-ensembles, pièces détachées, composants électroniques ou composants divers, sont correctement déterminés et qu'ils prennent en compte les contraintes prévues. A cette fin, des mesures électriques, thermiques ou autres peuvent être nécessaires.

Il convient également de contrôler le logiciel d'un système afin de déterminer les modes de pannes qui peuvent être dues au logiciel et d'évaluer qualitativement leur effet sur la fiabilité du système.

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.

Verification procedures are normally selected by agreement between the customer and supplier from either field tests or laboratory tests, as follows:

- field tests are often preferred, but their validity requires sufficient data collection. See IEC 605-1 and IEC 300-3-2 for the requirements to be stated;
- laboratory tests should be conducted as described in IEC 605-1. When specifying laboratory tests, it is important to consider the associated factors such as cost and time.

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

If success ratio is used as the reliability performance measure, the test should be carried out in accordance with IEC 1123.

If reliability performance requirements are based on a constant failure rate or failure intensity assumption it is necessary to select an appropriate test plan in accordance with IEC/FDIS 1124. Tests for validation of this assumption can be found in IEC 605-6.

5.2.3 *Verification by analysis*

Reliability verification of a product can be made prior to delivery by calculation based on reliability analysis. This method can be used long before reliability validation during field operation or by laboratory testing is possible. Such a method can only determine by analysis whether the product to be delivered fulfils corresponding requirements laid down in the product specification; it does not measure the realized reliability directly.

Examples of analytical methods for reliability verification of an item such as a system with hardware and software include reliability block diagrams, fault trees, state diagrams and fault mode and effect analysis. IEC 300-3-1 gives guidance on various analysis tools.

The hardware part of a system should be analysed to establish that the failure rates of each of its subsystems, parts and electronic or other components are adequately derived and take into account the expected stress. Electrical, thermal or other measurements may be necessary for this purpose.

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

Les données pour les calculs peuvent provenir de résultats en exploitation obtenus sur des matériels similaires, d'essais en laboratoire, de l'intégration de matériels ou de logiciels ou bien de sources de données unanimement reconnues. Si le client désire spécifier l'usage d'une certaine base de données (par exemple une base de taux de défaillances) il est recommandé au fournisseur et au client de se mettre d'accord sur ce point. Le fait que l'emploi d'une certaine base de données ait été prescrit ne dispense toutefois pas le fournisseur de l'obligation de satisfaire aux caractéristiques de fiabilité prescrites. Dans tous les cas, il convient de déterminer et de noter l'origine des données utilisées.

La CEI 863 donne des recommandations sur la présentation des prévisions de fiabilité, de maintenabilité et de disponibilité.

6 Spécification des caractéristiques de maintenabilité

6.1 Exigences de maintenabilité

Les exigences de maintenabilité peuvent être quantitatives ou qualitatives. Lorsque l'on définit des exigences quantitatives, il est important de spécifier le temps prévisionnel pendant lequel un dispositif sera dans l'état de non-fonctionnement en raison de la maintenance ou de la logistique de maintenance. Ce temps doit être spécifié sous la forme d'une mesure appropriée, par exemple une moyenne ou un fractile du temps de réparation active, une moyenne ou un fractile du temps de délai logistique. Lorsque l'on définit des exigences qualitatives, on doit définir à quel degré de concordance suivant laquelle un dispositif satisfait aux conditions et sujétions particulières relatives à la maintenance.

Il convient de couvrir quatre grands domaines lorsque l'on détermine des spécifications de maintenabilité complètes:

- les caractéristiques de maintenabilité qu'il faut satisfaire par la conception du dispositif;
- les sujétions qu'il faut prévoir pour l'utilisation du dispositif et qui touchent la maintenance;
- les exigences sur le programme de maintenabilité que le fournisseur doit tenir afin d'assurer que les dispositifs livrés ont bien les caractéristiques de maintenabilité exigées;
- les dispositions sur l'élaboration de la planification de la logistique de maintenance.

Lorsque l'on spécifie des exigences de maintenabilité, il est important de stipuler les points suivants:

- les conditions d'exploitation et d'environnement diverses dans lesquelles le matériel est utilisé;
- les compétences et responsabilités du personnel qui a la charge d'exploiter et de maintenir le matériel;
- la politique de maintenance qu'il faut appliquer ainsi que les procédures associées et les dispositions du soutien.

Il est recommandé de préciser dans la spécification de maintenabilité les exigences et la méthode à suivre pour que ces exigences soient tenues. Il est également recommandé d'inclure les définitions précises des termes utilisés dans la spécification avec les références appropriées aux vocabulaires normalisés si cela est opportun.

On peut définir dans la spécification soit des objectifs, soit des exigences fermes qui doivent être vérifiées suivant les méthodes prescrites. On peut définir des objectifs ou des exigences soit quantitatifs, soit qualitatifs.

Data for such calculations can be based, for example, on results obtained from operational experience with similar equipment in the field, from laboratory tests, from software/hardware integration or from recognized data sources. If the customer intends to specify the use of a certain data base (for example, a particular failure rate data bank), this should be agreed between the supplier and the customer. Specifying the use of a certain data base, 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 recorded.

IEC 863 gives guidance on the presentation of reliability, maintainability and availability predictions.

6 Specifying maintainability performance

6.1 Maintainability requirements

Maintainability requirements may be quantitative or qualitative. Where quantitative requirements are specified it is important to specify how long an item 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. Where qualitative requirements are specified, it is necessary to specify the degree to which an item has to conform to specific conditions and constraints related to maintenance.

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

- the maintainability performance to be achieved by the design of the item;
- the constraints that will be placed on the use of the item which will affect maintenance;
- the maintainability programme requirements to be accomplished by the supplier to assure that the delivered item has the required maintainability characteristics;
- 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 equipment is used;
- the qualifications and responsibilities of the personnel responsible for operating and maintaining the equipment;
- the maintenance policy to be applied and the associated procedures and support arrangements.

The maintainability performance specification should detail the requirements and the method to be followed to achieve 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 targets or as definite requirements that are to be verified in accordance with prescribed procedures. Targets or requirements may be specified in either quantitative or qualitative terms.

Une spécification de maintenabilité se rapporte ordinairement aux différentes tâches de maintenance qui sont exécutées pendant l'exploitation d'un dispositif. Toutefois, puisque la maintenabilité, en tant que caractéristique d'un produit, affecte les coûts de la logistique de maintenance et peut aussi influencer les temps de maintenance aux différents échelons de maintenance, il est recommandé de faire figurer dans la spécification des clauses qui se rapportent à tous les échelons de maintenance affectés par la politique de maintenance.

Pour plus de détails sur les exigences de maintenabilité dans les spécifications et les contrats, on consultera l'article 6 de la deuxième section de la CEI 706-1.

6.2 Vérification de la maintenabilité

La spécification d'exigences de maintenabilité est le processus permettant d'établir que les exigences prescrites dans la spécification ont été satisfaites. Il est recommandé de définir les méthodes de vérification parmi les exigences de maintenabilité. Ces méthodes sont de natures diverses: le fournisseur peut seulement se borner à fournir des résultats ou des renseignements appropriés; il peut, au contraire, être tenu de présenter une démonstration particulière de maintenabilité.

Il est recommandé de considérer la vérification de la maintenabilité comme un processus continu. On produit, on recueille et on évalue des résultats de maintenabilité au fur et à mesure qu'ils deviennent disponibles au cours du développement du projet; on les compare ensuite aux exigences de maintenabilité qui ont été spécifiées.

Plusieurs méthodes de vérification des exigences de maintenabilité sont décrites dans la CEI 706-3; on trouve notamment les méthodes suivantes:

- les analyses et revues de maintenabilité (bilans);
- les études particulières;
- les essais de démonstration;
- les revues de l'expérience en exploitation.

La spécification peut recommander ou imposer celles des méthodes ci-dessus qu'il faut appliquer spécifiquement.

Pour plus de détails sur la vérification de la maintenabilité, consulter la CEI 706-3, section six. Des informations relatives aux essais pour diagnostic sont données dans la CEI 706-5. Les méthodes statistiques pour l'évaluation de maintenabilité sont données dans la CEI 706-6.

7 Spécification des caractéristiques de disponibilité

7.1 Généralités

Pour les produits complexes comme les systèmes, il faut considérer simultanément la redondance et la maintenance. Pour de tels produits, il peut être intéressant sur le plan du système de ne prescrire directement que des exigences de disponibilité et non des exigences de fiabilité et de maintenabilité séparément. Les exigences les plus couramment adoptées portent sur la disponibilité en régime établi.

A maintainability performance specification typically covers the various aspects of maintainability achievement at the operational level. However, since maintainability performance as a product 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 706-1, Section Two, clause 6.

6.2 Maintainability verification

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

Maintainability verification 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 706-3; 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 is to be applied.

Further information on maintainability verification is given in IEC 706-3, Section Six. Information concerning diagnostic testing is given in IEC 706-5 and statistical methods in maintainability evaluation in IEC 706-6.

7 Specifying availability performance

7.1 General

For some products, such as complex systems, it is necessary to consider redundancy and maintenance together. In such products, it may be appropriate at system level to specify availability requirements rather than separate reliability and maintainability requirements. Requirements for the steady-state availability are the most commonly used.

7.2 Exigences de disponibilité

7.2.1 Généralités

Les exigences sur la disponibilité en régime établi sont exprimées par un nombre décimal inférieur à un ou par un pourcentage, par exemple le pourcentage du temps moyen d'indisponibilité en tant que pourcentage du temps d'observation. Les exigences de disponibilité se rapportent à la fois à la fréquence des défaillances et au temps d'indisponibilité.

NOTE – Il est important de ne pas imposer trop d'exigences. Il n'est ni nécessaire ni souhaitable de spécifier chacune des trois caractéristiques de la sûreté de fonctionnement (disponibilité, fiabilité et maintenabilité). Deux sur les trois suffisent.

Mais, par contre, il est souvent insuffisant de ne spécifier que la disponibilité. Il peut être aussi recommandé d'ajouter une exigence sur une caractéristique de fiabilité, par exemple l'intensité de défaillance.

7.2.2 Exigences quantitatives

Lors de la spécification des exigences quantitatives de disponibilité, il est usuel de cumuler deux ou plusieurs temps d'indisponibilité sur un certain intervalle de temps (par exemple un mois ou une année).

Si une partie du temps d'indisponibilité n'est pas de la responsabilité du fournisseur (par exemple le délai logistique ou le délai administratif), il convient de le mentionner dans la spécification en indiquant les valeurs des temps correspondants. La figure 191-10 de la CEI 50(191) donne des indications sur la signification de ces divers temps. Il est aussi possible de spécifier une disponibilité intrinsèque, c'est-à-dire en excluant de tels temps.

7.2.3 Exigences qualitatives

Il est recommandé de ne spécifier des exigences qualitatives de disponibilité que si les exigences quantitatives ne spécifient pas de façon suffisamment précise les caractéristiques de disponibilité du dispositif. Par exemple, le temps d'indisponibilité lorsqu'il est plus critique dans certaines conditions d'exploitation.

7.3 Vérification de la disponibilité

7.3.1 Généralités

La spécification ou le contrat peut demander une vérification des caractéristiques de la disponibilité prescrite.

7.3.2 Vérification par des essais en exploitation ou en laboratoire

Lorsque la vérification est à faire à l'aide d'essais en laboratoire ou en exploitation, on peut appliquer les méthodes d'essai de conformité normalisées figurant dans la CEI 1070 pour la disponibilité en régime établi. Il convient cependant de noter qu'il est très difficile d'établir un plan de vérification significatif dans le cas d'exigences de très bonne disponibilité (par exemple $\bar{A} > 0,9999$). A cet effet, on peut évaluer et vérifier les caractéristiques de fiabilité et de maintenabilité des sous-ensembles. On détermine donc la disponibilité du système par le calcul, selon un modèle théorique, à partir des observations faites sur le système et ses sous-ensembles. Dans tous les cas, il est nécessaire de prouver que les méthodes adoptées pour vérifier les très bonnes disponibilités sont effectivement utilisables.

Pour la vérification en exploitation, il convient de se mettre d'accord sur un programme détaillé d'acquisition de résultats en exploitation et de le mettre en oeuvre (voir CEI 300-3-2); ce programme doit inclure les temps d'indisponibilité ayant pour origine des défaillances du matériel, le logiciel, les procédures de maintenance et toute autre raison.

7.2 Availability requirements

7.2.1 General

Requirements for steady-state 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.

NOTE – It is important not to over-specify the requirements. It is neither necessary nor desirable to specify all three dependability characteristics (availability performance, reliability performance and maintainability performance). Two of the three are sufficient.

On the other hand, it is often insufficient to specify only the availability performance. A reliability performance measure such as failure intensity should also be specified.

7.2.2 Quantitative requirements

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 50(191) gives guidance on the various maintenance times. Alternatively, an intrinsic availability may be specified, that is by excluding such times.

7.2.3 Qualitative requirements

Qualitative availability requirements should only be specified if the quantitative requirement does not specify the availability performance of the item with sufficient precision. For example, if down time under certain operating conditions is more critical.

7.3 Availability verification

7.3.1 General

The specification or contract may include the need for verification of the required availability performance.

7.3.2 Verification by field or laboratory testing

Where verification is to be carried out by laboratory or field testing, the standardized compliance test procedures for steady-state availability given in IEC 1070 may be applied. It should be noted, however, that for very high availability requirements (for example, $\bar{A} > 0,9999$) it is very difficult to establish a meaningful verification plan. Evaluation and verification of subsystem 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 high availability requirements needs to be proven.

For field verification, a detailed field data collection program should be agreed and be performed (see IEC 300-3-2), including down time due to hardware failures, software failures, maintenance procedures and other reasons.

De plus, si l'on installe plus d'un dispositif du même type, il convient de préciser le nombre de dispositifs retenus ainsi que la période d'observation. En cas de non-conformité, il convient de se mettre d'accord sur une méthode pour améliorer la situation, d'appliquer cette méthode et de continuer l'essai.

7.3.3 Vérification par analyse

Si la vérification doit être faite par des méthodes de prévision, les techniques de prévision normalisées de la CEI 863, ainsi que les méthodologies d'analyse de détail spécifiées dans la CEI 300-3-1, peuvent être appliquées.

Généralement, les données de calcul doivent être basées sur des sources de données unanimement reconnues, des résultats d'expérience en exploitation sur des matériels similaires, des résultats provenant de laboratoires d'essai ou de l'intégration du logiciel et du matériel. Il convient que les données utilisées fassent l'objet d'un accord entre le client et le fournisseur.

Il convient de noter l'origine des données.

8 Spécification du soutien logistique de maintenance

8.1 Généralités

Les spécifications du soutien logistique de maintenance peuvent être fournies en totalité ou partiellement par le fabricant du matériel. Le client (y compris l'utilisateur) peut aussi fournir le soutien logistique de maintenance en totalité ou en partie.

Dans la mesure où le soutien logistique de maintenance est fourni par le fabricant, il convient de le spécifier en tant que partie de la fourniture. Le soutien logistique de maintenance, lorsqu'il est effectué par le client (y compris l'utilisateur), devra faire partie des conditions spécifiées d'exploitation du matériel, qui constituent une exigence préalable pour les valeurs spécifiées de la fiabilité et de la disponibilité.

Lorsque les exigences du soutien logistique de maintenance sont spécifiées, il est important de préciser les points suivants:

- les conditions d'exploitation et d'environnement diverses dans lesquelles le matériel est utilisé;
- les obligations et responsabilités du client, du fournisseur et des tierces parties;
- la politique de maintenance à appliquer ainsi que les procédures associées et les dispositions du soutien;
- les compétences et les responsabilités du personnel chargé de l'exploitation et de la maintenance du matériel.

Il convient que les spécifications du soutien logistique de maintenance soient établies avant que la conception du produit ne commence et qu'elles soient mises à jour avant la livraison du matériel.

8.2 Exigences quantitatives

Il convient, lorsque cela est possible, de spécifier quantitativement les exigences relatives au soutien logistique de maintenance. Des exemples de telles exigences quantitatives sont le délai administratif moyen, le délai logistique moyen et la probabilité de pénurie en pièces de rechange. Des informations complémentaires sont fournies dans la CEI 706-1 et dans la CEI 706-6.

Furthermore, if more than one item of the same type of product is installed, the number of items and the period of observation should be stated. A procedure should be specified such that, in the event of non-compliance, an improvement is agreed and introduced and testing is continued.

7.3.3 *Verification by analysis*

If verification is to be carried out by prediction methods, the standardized prediction techniques given in IEC 863 with detailed analysis methodology as specified in IEC 300-3-1 may be applied.

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

8 **Specifying maintenance support**

8.1 *General*

Maintenance support specifications can be supplied fully or partly by the manufacturer of the equipment. The customer (including the user) may also supply the maintenance support partially or fully.

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

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

- the various operating and environmental conditions under which the equipment is used;
- the obligations and responsibilities of customer, supplier and third parties;
- the maintenance policy to be applied and the associated procedures and support arrangements;
- the qualifications and responsibilities of the personnel responsible for operating and maintaining the equipment.

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

8.2 *Quantitative requirements*

Maintenance support requirements should, where possible, be specified in a quantitative way. Examples of such quantitative specifications are mean administrative delay, mean logistic delay and spare shortage probability. Further information can be found in IEC 706-1 and IEC 706-6.

8.3 Exigences qualitatives

Lorsqu'il n'est pas possible de spécifier quantitativement les exigences du soutien logistique de maintenance, il convient d'utiliser en complément des exigences qualitatives. Il peut s'agir, par exemple, des spécifications du niveau de formation et des capacités requis, du profil du personnel de maintenance ou des exigences relatives aux moyens de l'atelier et à la disponibilité des outils.

D'autres informations sont fournies dans la CEI 706-1

9 Coopération entre le client et le fournisseur

Dans le but de réduire le nombre de défaillances et les durées d'indisponibilité du produit, il est nécessaire que le client et le fournisseur aient une collaboration étroite pendant toutes les phases du cycle de vie du produit. Cela entraîne des obligations diverses et réciproques entre client et fournisseur; il convient de les spécifier.

Un programme rigoureux de gestion de fiabilité et de maintenabilité (voir CEI 300-1) peut aider à déterminer et à définir ces activités.

Il convient de spécifier, lorsque cela est possible, que le client ou le distributeur admettent leur responsabilité en ce qui concerne la surveillance de la fiabilité en utilisation et le retour d'expérience en exploitation (bonne ou mauvaise) à leur fournisseur.