NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
300-2

Première édition
First edition
1995-12

Gestion de la sûreté de fonctionnement –

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

Dependability management –

Part 2:
Dependability programme elements and tasks

Numéro de référence
Reference number
CEI/IEC 300-2: 1995

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
300-2

Première édition
First edition
1995-12

Gestion de la sûreté de fonctionnement –

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

Dependability management –

Part 2:
Dependability programme elements and tas

Bureau Central de la Commission Electrotechnique Internationale 3, rue de Varembé Genève, Suisse

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE W

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

SOMMAIRE

Pages

CONTENTS

Articles Pages

Annexes

Clause Articles

Annexes

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 2: Eléments et tâches du programme 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 des 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 norme de la CEI et la norme nationale ou régionale 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 présente partie de la CEI 300 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:

DIS	Rapport de vote
56/437/FDIS	56/488/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 Norme Internationale CEI 300 est publiée en trois parties:

CEI 300-1: Gestion du programme de sûreté de fonctionnement

CEI 300-2: Eléments et tâches du programme de sûreté de fonctionnement

CEI 300-3: (Série de guides d'application)

L'annexe A fait partie intégrante de la présente norme.

Les annexes B, C et D sont données uniquement à titre d'information.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

Part 2: Dependability programme elements and tasks

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 cooperation 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 has been prepared by IEC technical committee 56: Dependability.

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

DIS	Report on voting
56/437/FDIS	56/488/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 international Standard is one of the several Parts:

IEC 300-1: Dependability programme management

IEC 300-2: Dependability programme elements and tasks

IEC 300-3: (Application guides series)

Annex A forms an integral part of this standard.

Annexes B, C and D are for information only.

INTRODUCTION

Trois facteurs sont d'une importance fondamentale pour ceux qui ont la responsabilité du développement d'un nouveau produit et pour ceux qui auront la responsabilité de l'utilisation ou de l'exploitation du produit, ce sont:

Les performances

Est-ce que les performances du produit (y compris la sûreté de fonctionnement) correspondront aux attentes et aux besoins de l'utilisateur final?

Le coût

Quel sera le coût, non seulement de développement et de fabrication du produit, mais aussi d'exploitation et de maintenance et éventuellement de mise au rebut, c'est-à-dire quel sera le coût global du produit?

Le planning

Est-ce que le produit sera disponible dans le délai exigé et apparaîtra-t-il sur le marché au moment approprié?

La satisfaction du client, la réputation du produit et de son fournisseur dépendent pour une grande part de la manière dont ces facteurs sont gérés et harmonisés pendant les différentes phases du cycle de vie.

Le terme sûreté de fonctionnement englobe la fiabilité, la maintenabilité, la disponibilité et le soutien logistique de maintenance. La fiabilité, la disponibilité et la maintenabilité sont elles-mêmes des caractéristiques de performance fondamentales et sont fréquemment spécifiées en tant qu'exigences clés d'un produit.

Le soutien logistique de maintenance est l'aptitude à fournir les moyens nécessaires pour maintenir le produit.

Les caractéristiques de sûreté de fonctionnement d'un produit ont une influence majeure sur l'aptitude d'ensemble du produit à satisfaire les exigences de l'utilisateur et pourraient bien être des aspects fondamentaux et dominants de la qualité. La sûreté de fonctionnement a aussi une influence majeure sur les coûts d'exploitation et de maintenance du produit en utilisation, ainsi que sur l'obtention d'un coût de cycle de vie acceptable.

Le coût initial ou d'achat d'un produit est souvent le facteur qui influence principalement le choix de l'utilisateur, mais il est important de reconnaître que le coût d'achat est seulement une partie du coût total de possession d'un produit. Les coûts d'exploitation et de maintenance peuvent être réduits de façon importante si le produit est conçu pour être fiable et maintenable, c'est-à-dire d'un fonctionnement plus sûr. L'amélioration et le développement du produit, dans ces conditions, accroît le coût d'achat, mais le coût supplémentaire le plus important est souvent compensé par des coûts d'exploitation et de maintenance réduits de façon importante. Il est important de réaliser des études de compromis pour optimiser le coût de l'amélioration de la fiabilité et de la maintenabilité par rapport à la baisse attendue du coût réalisée sur l'ensemble du cycle de vie du produit.

Il est important que le client comme le fournisseur reconnaissent que les caractéristiques de sûreté de fonctionnement peuvent avoir un impact majeur sur la performance et la qualité du produit, le coût et le planning, comme cela a été décrit plus haut.

INTRODUCTION

Three factors are of fundamental importance to those responsible for developing a new product and to those who will be responsible for using or operating the product; they are:

Performance

Will the performance (including dependability) of the product meet the expectations and needs of the end user?

Cost

What will be the cost, not only of developing and producing the product, but also of operating and maintaining and eventually disposing of it, i.e. what will be its life-cycle cost?

Timescale

Will the product be available when required and appear on the market at the appropriate time?

The customer's satisfaction with a product, and the reputation of the product and of its supplier, depends to a considerable degree on how well these factors are managed and harmonized during the various phases of the product life cycle.

The term dependability embraces reliability, maintainability, availability and maintenance support. Reliability, availability and maintainability are themselves fundamental product performance characteristics and are frequently specified as key product requirements.

Maintenance support is the ability to provide the resources required to maintain the item.

The dependability characteristics of a product have a major influence on the overall ability of the product to satisfy the requirements of the user and may well be fundamental and dominating aspects of quality. Dependability also has a major effect on the cost of operating and maintaining the product in use and on the achievement of acceptable life-cycle cost.

The initial or purchase cost of a product is often the major factor influencing the user's selection but it is important to recognize that the purchase cost is only a part of the total cost of ownership of a product. The costs of operation and maintenance can be greatly reduced if the product is designed to be reliable and maintainable. Improving and developing a product in this way usually adds to the purchase cost, but the greater additional cost is often compensated by greatly reduced operating and maintenance costs. It is important to perform studies to trade off the cost of improving reliability and maintainability against the expected reduction in cost achieved over the whole life of the product.

It is important that both supplier and customer should recognize that dependability characteristics may have a major impact on product performance, cost and time scale as described above.

Les exigences de la sûreté de fonctionnement sont souvent complexes et dans le but de les réaliser il est nécessaire de répartir les moyens appropriés, soigneusement planifiés et coordonnés au sein d'un programme de sûreté de fonctionnement. L'objectif de tels programmes est de s'assurer que toutes les exigences de fiabilité, maintenabilité, disponibilité et soutien logistique de maintenance sont remplies; un utilisateur aura besoin de réaliser un programme de sûreté de fonctionnement conçu pour s'assurer que les exigences du soutien logistique de maintenance sont satisfaites.

Il convient que les divers programmes de sûreté de fonctionnement (par exemple le programme de gestion de la fiabilité, le programme de gestion de la maintenabilité) soient complètement intégrés dans l'ensemble du programme associé au produit et dans le programme qualité du produit.

Une spécification des exigences de la sûreté de fonctionnement constitue souvent la base de la conception du produit et de son soutien logistique de maintenance et il convient en conséquence de le préparer avant que la phase de conception ne démarre.

Cette norme est un guide général pour établir les programmes de sûreté de fonctionnement et elle est applicable aux matériels et aux logiciels. Il convient que les éléments choisis pour élaborer le programme associé à un produit spécifique soient adaptés en fonction des exigences particulières, des circonstances et des conditions qui s'appliquent.

Il convient que le choix des éléments particuliers, l'importance à donner à chacun d'eux et le planning de l'ensemble du programme de sûreté de fonctionnement prennent en compte les conditions du marché, les exigences et attentes des utilisateurs, la situation contractuelle, et les exigences d'ensemble du produit et du soutien qui lui est associé. Les éléments d'un programme particulier doivent aussi être ajustés à la phase du cycle de vie dans laquelle ils sont situés.

Dependability requirements are often complex and in order to achieve them it is necessary to allocate appropriate resources, carefully planned and coordinated, into a dependability programme. The object of such programmes is to ensure that all reliability, maintainability, availability and maintenance support requirements are met. A supplier will typically need to implement dependability programmes to ensure that product reliability and maintainability requirements are met; a user will need to implement a dependability programme designed to ensure that maintainability support requirements are satisfied.

The various dependability programmes (for example the reliability management programme and the maintainability management programme) should be fully integrated into the overall product programme and into the product quality programme.

The specified dependability requirements are often a major feature of the design of the product and of its maintenance support and the specification should therefore be prepared before the design work is started.

This standard provides general guidance on the establishment of dependability programmes and is applicable to hardware products and systems containing software. The elements selected to provide the programme for a specific product should be tailored according to the individual requirements, circumstances and conditions that apply.

The selection of individual elements, the emphasis to be given to each element and the scale of the overall dependability programme should take account of the conditions of the market, the requirements and expectations of users, the contractual situation and the overall requirements for the product and its support. Individual programme elements also need to be adjusted to the phase of the life cycle in which they are implemented.

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

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

1 Domaine d'application

La présente partie de la CEI 300 décrit les éléments d'un programme de sûreté de fonctionnement et fournit un guide sur la sélection des tâches nécessaires afin d'aboutir à la sûreté de fonctionnement spécifiée des produits. Cette norme est harmonisée avec l'ISO 9004-1. Elle est applicable aux matériels et aux systèmes comprenant des logiciels.

Les descriptions des éléments d'un programme particulier sont fournies. Cependant, les procédures détaillées qui doivent être utilisées pour mettre en oeuvre les tâches ne sont pas incluses; à leur place, on se réfère aux guides d'application de la CEI 300-3 et aux Normes internationales de la CEI sur la gestion de la sûreté de fonctionnement.

Le cadre de cette partie de la CEI 300 concerne en premier lieu le cas des relations entre deux parties: un «fournisseur» qui fournit des produits ou des services de maintenance à un «client». Des parties du produit peuvent être achetées par le fournisseur à une autre source. Lorsqu'il est nécessaire de clarifier une telle situation, les termes «fournisseur» (en contact direct avec le client) et «sous-traitant» (en contact direct avec le fournisseur) sont utilisés. Le véritable utilisateur (utilisateur final) du produit peut être «le client» ou un tiers.

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 Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute norme est sujette à révision et les parties prenantes aux accords fondés sur la présente partie de la CEI 300 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes Internationales en vigueur à un moment donné.

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

CEI 300-1/ISO 9000-4: 1993, *Gestion de la sûreté de fonctionnement – Partie 1: Gestion du programme de sûreté de fonctionnement*

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

ISO 9001: 1994, *Systèmes qualité – Modèle pour l'assurance de la qualité en conception, développement, production, installation et soutien après la vente et prestations associées*

ISO 9004-1: 1994, *Gestion de la qualité et éléments de système qualité – Partie 1: Lignes directrices*

DEPENDABILITY MANAGEMENT –

Part 2: Dependability programme elements and tasks

1 Scope

This Part of IEC 300 describes the elements of a dependability programme and gives guidance on the selection of tasks necessary to achieve specified dependability of products. This standard cross-references and complements ISO 9004-1. It is applicable to hardware and systems containing software products.

Descriptions of individual programme elements are provided. Detailed procedures to be employed when implementing the tasks are not included but reference is made to related application guides contained in IEC 300-3 and to other IEC International Standards on dependability management.

The format of this part of IEC 300 primarily addresses the case of a two party relationship, between a "supplier" who provides products or maintenance services and a "customer". Parts of the product may be purchased from other sources by the supplier (by subcontracting). Where it is necessary to clarify such a situation, the terms "first level supplier" (with direct relation to the customer) and "second level supplier" ("subcontractor", with direct relation to the first level supplier) are used. The actual users (end users) of the product may be the customers themselves or a third body.

2 Normative references

The following normative documents contain provisions which, through reference in this text constitute provisions of this part of IEC 300. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this part of IEC 300 are encouraged to investigate the possibility of applying the most recent editions of the standards 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/ISO 9000-4: 1993, *Dependability management – Part 1: Dependability programme management*

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

ISO 9001: 1994, *Quality systems – Model for quality assurance in design, development, production, installation and servicing*

ISO 9004-1; 1994, *Quality management and quality system elements – Part 1: Guidelines*

3 Définitions

Pour *les* besoins de la présente Norme internationale les termes et définitions de la CEI 50(191), de la CEI 300-1 s'appliquent ainsi que l'ISO 8402. De plus les termes et définitions suivants sont utilisés:

3.1 **tâche du programme de sûreté de fonctionnement:** Ensemble d'activités concernant les aspects sûreté de fonctionnement d'un produit.

3.2 **élément du programme de sûreté de fonctionnement:** Un ensemble de tâches du programme de sûreté de fonctionnement appartenant au domaine d'un sujet spécifique.

3.3 **cycle de vie:** Intervalle de temps compris entre le concept et la définition d'un produit et son retrait du service.

3.4 **phase de concept et de définition:** Phase du cycle de vie d'un produit au cours de laquelle le besoin du produit est établi et (généralement) ses exigences sont spécifiées.

3.5 **phase de conception et de développement:** Phase du cycle de vie d'un produit au cours de laquelle le matériel et/ou le logiciel est créé et documenté suivant les spécifications détaillées de fabrication et/ou codage et pendant laquelle sont réalisées les autres documentations du produit, comme les instructions d'utilisation et de maintenance.

3.6 **phase de fabrication:** Phase du cycle de vie d'un produit au cours de laquelle le produit est fabriqué, le logiciel dupliqué et le produit est assemblé.

3.7 **phase d'installation:** Phase du cycle de vie d'un produit au cours de laquelle le produit est installé.

3.8 **phase d'exploitation et de maintenance:** Phase du cycle de vie d'un produit au cours de laquelle le produit est utilisé, maintenu et soutenu.

3.9 **phase de mise au rebut:** Phase du cycle de vie d'un produit, postérieure à la phase d'exploitation et de maintenance au cours de laquelle le produit est retiré de son site d'exploitation, mis hors service, désassemblé, détruit ou stocké si nécessaire dans un environnement protégé.

4 Vue générale d'un programme de sûreté de fonctionnement

4.1 *Généralités*

Les objectifs d'un programme de sûreté de fonctionnement sont de s'assurer que l'effort adéquat et effectif est apporté pour faire en sorte que la sûreté de fonctionnement soit une mesure principale de la qualité pendant toutes les phases du cycle de vie d'une entité (depuis la définition en passant par la phase de conception et d'acceptation, jusqu'à la fin de la vie) et que les activités qui contribuent à la sûreté de fonctionnement sont intégrées correctement avec les activités contractuelles et les spécifications. Il convient qu'un programme de sûreté de fonctionnement produise en continu l'étude des exigences qualitatives et quantitatives à travers toutes les phases d'un projet; il convient que les évaluations de sûreté de fonctionnement soient mises à jour, que les exigences spécifiées soient vérifiées, que les activités soient intégrées avec les autres éléments du programme de développement, de production et d'exploitation. Voir l'annexe A.

3 Definitions

For the purpose of this International Standard the terms and definitions of IEC 50(191) and IEC 300-1 apply together with ISO 8402. In addition, the following terms and definitions are used:

3.1 **dependability programme task:** A set of activities addressing dependability aspects of a product.

3.2 **dependability programme element:** A set of dependability programme tasks, pertaining to a specific subject area.

3.3 **life cycle:** The time interval from a product's inception until its ultimate disposal and removal from use.

3.4 **concept and definition phase:** That product life-cycle phase during which the need for the product is established and (usually) its requirements specified.

3.5 **design and development phase:** That product life-cycle phase during which the product's hardware and/or software is created and documented as detailed manufacturing/coding specifications, and other product documentation such as use and maintenance instructions produced.

3.6 **manufacturing phase:** That product life-cycle phase during which the product is produced, software replicated and the product assembled.

3.7 **installation phase:** That product life-cycle phase during which the product is installed.

3.8 **operation and maintenance phase:** That product life-cycle phase during which the product is used for any purpose and is maintained and supported.

3.9 **disposal phase:** That possible product life-cycle phase, after the operation and maintenance phase, during which the product is removed from its use site and decommissioned, dismantled, destroyed or stored if necessary in a protected environment.

4 Dependability programme overview

4.1 *General*

The aims of a dependability programme are to ensure that adequate and effective effort is brought to bear on dependability as a principal quality attribute during all phases of the life-cycle of an item (from definition through design and acceptance into service, to the end of its working life) and that the activities which contribute to dependability are properly integrated with other contract and specification activities. A dependability programme should provide continuous study of both quantitative and qualitative requirements throughout all phases of a project. This also includes the updating of dependability assessments and the verification of specified requirements. The dependability programme elements should be integrated with other elements of the development, production and operation programme. See annex A.

Il convient que l'étendue et le contenu du programme de sûreté de fonctionnement soient dépendants des caractéristiques particulières du projet et de toute contrainte spécifique, ainsi que de l'importance de la sûreté de fonctionnement pour le produit en question.

Pour de nombreux projets, il n'y a pas de démarcation précise entre les phases de définition, de conception, de développement, de production et d'exploitation. Toutefois, pour la clarté, ces distinctions sont faites au cours de cet article. Les activités propres à chacune des phases sont données en annexe B qui liste les tâches du programme de sûreté de fonctionnement qui peuvent être choisies et réalisées pendant les phases de cycle de vie. Elles sont expliquées dans le texte de cet article, en rapport avec les responsabilités liées à la gestion d'ensemble du projet et au planning. Il convient que le programme de sûreté de fonctionnement soit préparé conjoitement avec d'autres programmes en rapport avec le produit ou le projet. La référence aux normes de la CEI appropriées sont données en annexe C.

Les relations entre les phases du cycle de vie et les tâches du programme de sûreté de fonctionnement sont données en figure 1.

NOTE – La figure 1 ainsi que les annexes A, B et C présentent des aspects de programmes de sûreté de fonctionnement généraux, selon des perspectives différentes. Dans une certaine mesure, ces présentations sont simplifiées, ce qui entraîne le risque de quelques différences entre elles.

Un programme effectif de sûreté de fonctionnement peut être construit par le choix des éléments et tâches appropriés en accord avec le processus d'adaptation décrit dans l'article 5, pour correspondre aux besoins et aux circonstances spécifiques.

Les activités de sûreté de fonctionnement à mettre en oeuvre pour chaque phase du cycle de vie du produit doivent être sélectionnées suivant le contexte du cycle de vie total du produit. A quelque instant que ce soit, les décisions prises ont un impact sur la sûreté de fonctionnement du produit et le coût au moment de la décision et dans les phases ultérieures du cycle de vie.

Il convient de noter qu'une exigence légale ou réglementaire, soit dans la situation des moyens d'utilisation ou des moyens de fabrication, doit être prise en compte et que la conformité à la présente norme ne confère pas, par elle-même, une immunité en regard des obligations légales.

The extent and contents of the dependability programme should be governed by the particular needs of the project and any specific constraints, and on the importance of dependability of the actual product.

In many projects, there are no sharp demarcations between the definition, design and development, production and operation phases. However, for clarity, distinctions are drawn in this clause. The activities appropriate to the different phases are given in annex B which lists the dependability programme tasks that may be selected for implementation during the product life-cycle phases. They are explained in the text of this clause in relation to the overall project management responsibilities and time scale. The dependability programme should be prepared in conjunction with other project/product related programmes. References to appropriate IEC standards are given in annex C.

An example of the relationships between life-cycle phases and dependability programme elements and tasks is given in figure 1.

NOTE – Figure 1 and annexes A, B, and C present views of generalized dependability programmes from different perspectives. All are simplified to some extent and this gives rise to minor differences between them.

An effective dependability programme can be assembled by selecting the appropriate elements and tasks in accordance with the tailoring process, described in clause 5, to suit specific needs and circumstances.

The dependability activities to be implemented during each phase of the product life cycle should be selected in the context of the total life cycle of the product. Decisions made at any instant of time have an impact on product dependability and cost at that time and in subsequent phases of the product life.

It should be noted that a legal or regulatory requirement in either user or manufacturing facility location should be considered and that compliance with this standard does not of itself confer immunity from legal obligations.

Article	Tâche	Phase de cycle de vie					
		Concept et définition	Conception et développement	Fabrication	Installation	Exploitation et maintenance	Mise au rebut
6.1	PLANIFICATION ET GESTION						
6.1.1	Plans de sûreté de fonctionnement						
6.1.2	Gestion des décisions de projet						
6.1.3	Gestion de la traçabilité						
6.1.4	Gestion de la configuration						
6.2	REVUE DE CONTRAT ET LIAISON						
6.2.1	Revue de contrat						
6.2.2	Représentants de la direction						
6.3	EXIGENCES DE SÛRETÉ DE FONCTIONNEMENT						
6.3.1	Spécification des exigences de sûreté de fonctionnement						
6.3.2	Interprétation des exigences						
6.3.3	Répartition des exigences						
6.4	INGENIERIE						
6.4.1	Ingénierie de la fiabilité						
6.4.2	Ingénierie de la maintenabilité						
6.4.3	Ingénierie du soutien logistique de maintenance						
6.4.4	Ingénierie de la testabilité						
6.4.5	Ingénierie des facteurs humains						
6.5	PRODUITS FOURNIS EXTÉRIEUREMENT						
6.5.1	Produits sous-traités						
6.5.2	Produits fournis par le client						
6.6	ANALYSE, PRÉDICTION ET REVUE DE CONCEPTION						
6.6.1	Analyse des modes de défaillance et de leurs effets						
6.6.2	Analyse par arbre de panne						
6.6.3	Analyse des contraintes et des charges						
6.6.4	Analyse des facteurs humains						
6.6.5	Prévision						
6.6.6	Analyse de compromis						
6.6.7	Analyse des risques						
6.6.8	Revue de conception formalisée						
6.7	VÉRIFICATION, VALIDATION, ESSAI						
6.7.1	Planification de la vérification, de la validation et des essais						
6.7.2	Essai de durée de vie						
6.7.3	Essai de sûreté de fonctionnement						
6.7.4	Essai de croissance de fiabilité						
6.7.5	Essai en production						
6.7.6	Essai d'acceptation						
6.7.7	Essai de déverminage sous contrainte						
6.8	PROGRAMME DE COÛT DU CYCLE DE VIE						
6.9	PLANIFICATION DE L'EXPLOITATION ET DE LA MAINTENANCE						
6.9.1	Planification de la logistique de maintenance						
6.9.2	Installation						
6.9.3	Service de soutient						
6.9.4	Ingénierie de soutien						
6.9.5	Approvisionnement des rechanges						
6.10	AMÉLIORATION ET MODIFICATIONS						
6.10.1	Programmes d'amélioration						
6.10.2	Gestion des modifications						
6.11	RETOUR D'EXPÉRIENCE						
6.11.1	Acquisition des données						
6.11.2	Analyse des données						

Figure 1 – Relation entre les phases du cycle de vie et les tâches du programme de sûreté de fonctionnement

Clause	Element/task	Life-cycle phase					
		Concept and definition	Design and develop-ment	Manufac-turing	Instal-lation	Operation and main-tenance	Dis-posal
6.1	PLANNING AND MANAGEMENT						
6.1.1	Dependability plans						
6.1.2	Project decision management						
6.1.3	Traceability management						
6.1.4	Configuration management						
6.2	CONTRACT REVIEW AND LIAISON						
6.2.1	Contract review						
6.2.2	Management representative						
6.3	DEPENDABILITY REQUIREMENTS						
6.3.1	Specification of dependability requirements						
6.3.2	Requirements interpretation						
6.3.3	Requirements allocation						
6.4	ENGINEERING						
6.4.1	Reliability engineering						
6.4.2	Maintenability engineering						
6.4.3	Maintenance support engineering						
6.4.4	Testability engineering						
6.4.5	Human Factors engineering						
6.5	EXTERNALLY PROVIDED PRODUCTS						
6.5.1	Subcontracted products						
6.5.2	Customer-provided products						
6.6	ANALYSIS, PREDICTION AND DESIGN REVIEW						
6.6.1	Fault modes and effects analysis						
6.6.2	Fault tree analysis						
6.6.3	Stress and load analyses						
6.6.4	Human factors analysis						
6.6.5	Predictions						
6.6.6	Trade-off analysis						
6.6.7	Risk analysis						
6.6.8	Formal design review						
6.7	VERIFICATION, VALIDATION AND TEST						
6.7.1	Verification, validation and test planning						
6.7.2	Life testing						
6.7.3	Dependability testing						
6.7.4	Reliability growth testing						
6.7.5	Production testing						
6.7.6	Acceptance testing						
6.7.7	Reliability stress screening						
6.8	LIFE-CYCLE COST PROGRAMME						
6.9	OPERATION AND MAINTENANCE SUPPORT PLANNING						
6.9.1	Maintenance support planning						
6.9.2	Installation						
6.9.3	Support services						
6.9.4	Support engineering						
6.9.5	Spares provisioning						
6.10	IMPROVEMENTS AND MODIFICATIONS						
6.10.1	Improvement programmes						
6.10.2	Modification control						
6.11	EXPERIENCES FEEDBACK						
6.11.1	Data aquisition						
6.11.2	Data analysis						

Figure 1 – Relation between life cycle phases and dependability programme tasks

4.2 *Cycle de vie d'un produit*

4.2.1 *Phase de concept et de définition*

La phase de concept et de définition est la phase du cycle de vie pendant laquelle les besoins du produit sont définis et ses exigences spécifiées. Pendant cette phase, les bases de la sûreté de fonctionnement du produit et de son coût de cycle de vie sont établies. C'est dans cette phase que les décisions prises ont le plus grand impact sur le produit et son coût de cycle de vie.

Il convient que les activités de sûreté de fonctionnement dans cette phase se concentrent sur l'obtention des exigences adaptées au produit et à son soutien futur ainsi qu'à l'établissement d'un plan de sûreté de fonctionnement utilisé comme base pour le contrôle de la sûreté de fonctionnement pendant les phases ultérieures.

4.2.2 *Phase de conception et de développement*

C'est la phase du cycle de vie pendant laquelle les aspects matériel et/ou logiciel du produit sont créés et documentés, suivant les spécifications détaillées de fabrication et/ou codage et pendant laquelle sont réalisées les autres documentations du produit, comme les instructions d'utilisation et de maintenance.

Les objectifs premiers des activités de sûreté de fonctionnement pendant cette phase sont de s'assurer que:

– les exigences de la spécification de sûreté de fonctionnement sont totalement prises en compte pendant le processus de conception;

– les activités d'analyse et de prévision sont mises en oeuvre et utilisées pour atteindre la sûreté de fonctionnement du produit;

– les procédures et les critères de validation, de vérification et d'essais sont définis et exécutés selon les exigences de sûreté de fonctionnement;

– les exigences de sûreté de fonctionnement allouées à toutes les parties de produit livrées par des sous-traitants ou par le client sont respectées;

– les activités d'ingénierie et le planning du soutien logistique de maintenance sont coordonnés avec la conception du produit pour assurer la conformité avec toutes les exigences de sûreté de fonctionnement.

– les exigences de la mise au rebut sont définies.

4.2.3 *Phase de fabrication*

C'est la phase du cycle de vie pendant laquelle le matériel est fabriqué, le logiciel dupliqué et le produit assemblé.

Il convient que les activités de sûreté de fonctionnement soient dirigés afin de s'assurer que les performances de sûreté de fonctionnement du produit réalisées pendant la phase de conception et développement ne sont pas dégradées par le procédé de fabrication. Il convient que le programme de sûreté de fonctionnement établisse des procédures à suivre pendant la production des systèmes et des équipements afin de s'assurer que la fiabilité est conforme à des niveaux spécifié.

4.2 *Life cycle of product*

4.2.1 *Concept and definition phase*

The concept and definition phase is the life-cycle phase during which the need for the product is established and its requirements specified. During this phase the foundation is laid for the product's dependability and its life-cycle cost. Decisions made during this phase have greatest impact on the product and its life-cycle cost.

The dependability activities in this phase should concentrate on reaching the correct requirements for the product and its future support and for establishing the dependability plan used as a basis for the control of dependability during the subsequent phases.

4.2.2 *Design and development phase*

The design and development phase is the life-cycle phase during which the product's hardware and/or software is created and documented as detailed manufacturing/coding specifications, and other product documentation such as use and maintenance instructions are produced.

The prime objectives of dependability activities during this phase are to ensure that:

- the requirements of the dependability specification are taken into full consideration during the design process;
- analysis and prediction activities are implemented and used to achieve dependability of the product;
- validation, verification and test procedures and criteria are defined and executed based on dependability requirements;
- dependability requirements allocated to any part of the product provided by second level suppliers or customers are complied with;
- maintenance support planning and engineering activities are coordinated with the product design to ensure compliance with dependability requirements;
- disposal requirements are defined.

4.2.3 *Manufacturing phase*

The manufacturing phase is the life-cycle phase during which the product is produced, software replicated and the product assembled.

Dependability activities during this phase should be directed at ensuring that dependability performances of the product achieved during design and development are not degraded during the manufacturing process. The dependability programme should state procedures to be followed during the production of systems and equipment to ensure that dependability meets specified levels.

Pendant cette phase, les activités essentielles du programme de sûreté de fonctionnement sont:

– essai de fiabilité et de maintenabilité;
– essai de production;
– déverminage de fiabilité sous contrainte.

4.2.4 *Phase d'installation*

C'est la phase du cycle de vie pendant laquelle le produit est installé.

Il convient que les activités de sûreté de fonctionnement soient dirigées afin de s'assurer que les performances du produit ne sont pas dégradées pendant l'installation. Il convient de fournir les procédures et les instructions pour conduire l'inspection d'acceptation, l'essai des systèmes et des composants par vérification de la conformité à la spécification initiale et à la conception.

Pendant cette phase, les activités essentielles du programme de sûreté de fonctionnement sont:

– les essais de mise en service;
– les essais d'acceptation;
– les essais de croissance de fiabilité;
– la démonstration des performances de fiabilité et maintenabilité;
– la création et la mise à jour du recueil des données et leur analyse;
– la gestion des défaillances initiales.

4.2.5 *Phase d'exploitation et de maintenance*

C'est la phase du cycle de vie du produit pendant laquelle le produit est exploité, maintenu et soutenu. Pendant cette phase, les actions de maintenance corrective et préventive essentielles sont exécutées, si nécessaire, et la performance du produit est surveillée.

Afin de s'assurer que les niveaux requis de sûreté de fonctionnement sont valablement atteints pendant cette phase, il sera nécessaire d'établir:

– les procédures d'exploitation;
– les procédures de maintenance;
– les procédures d'alerte;
– le plan de formation;
– la liste des composants de rechanges.

La vie utile d'un produit se termine lorsque son exploitation devient trop onéreuse en raison de coûts de maintenance accrus ou d'autres facteurs, ou bien lorsque le produit devient techniquement périmé.

The principle dependability activities during this phase are:

- reliability and maintainability testing;
- production testing;
- reliability stress screening.

4.2.4 *Installation phase*

The installation phase is the life-cycle phase during which the product is installed.

Dependability activities should be directed at ensuring that the dependability performances of the product are not degraded during installation. Procedures and instructions should be provided for conducting acceptance inspection and testing of systems and components by verifying compliance with the initial specification and design.

Prime dependability activities during this phase are:

- commissioning tests;
- acceptance testing;
- reliability growth testing;
- reliability and maintainability demonstration;
- data collection and analysis;
- initial failure control.

4.2.5 *Operation and maintenance phase*

The operation and maintenance phase is the life-cycle phase during which the product is used for any purpose and is maintained and supported. During this phase, essential preventive and corrective maintenance actions are taken, as necessary, and the product's performance is monitored.

In order to ensure that required levels of dependability are consistently achieved during this phase, it will be necessary to provide:

- operating instructions;
- maintenance instructions;
- warning instructions;
- training;
- spares.

The useful life of the product ends when its operation becomes uneconomic due to increased maintenance cost or other factors, or when the product becomes technically obsolete.

4.2.6 *Phase de mise au rebut*

C'est la phase du cycle de vie qui suit les phases d'exploitation et de maintenance durant laquelle, il est mis au rebut, détruit ou stocké si nécessaire dans un environnement protégé.

Cette phase peut comprendre le desassemblage du produit afin de procéder à des activités telles que:

– essais et analyses d'usure
– retour d'informations au fournisseur afin d'améliorer la fiabilité et la maintenabilité
– récupération de matériaux à des fins de recyclage.

5 Critères d'ajustement pour programmes de sûreté de fonctionnement

5.1 *Généralités*

Les éléments et les tâches de programme de sûreté de fonctionnement définis dans cette partie de la CEI 300 ont un caractère générique. Il convient que pour un produit ou un projet spécifique, le programme de sûreté de fonctionnement soit adapté, en apportant une attention particulière aux aspects propres au produit ou au projet.

Lorsqu'on évoque cette partie de la CEI 300, il convient que les parties concernées se mettent d'accord sur l'étendue de son application et conservent trace de cet accord. Il convient que l'accord soit documenté. Pour les articles, ou partie d'articles identifiés par cet accord, selon le cas, les recommandations (utilisation de la forme verbale «il convient de») deviennent des exigences (forme verbale «doit/doivent»).

L'élaboration d'un programme effectif de sûreté de fonctionnement pendant n'importe quelle phase du cycle de vie du produit demande non seulement une connaissance des principes, des méthodes et des techniques de sûreté de fonctionnement mais aussi une compréhension du produit lui-même, de sa technologie, de l'usage auquel il est destiné et des différents facteurs relatifs à son coût.

Afin d'obtenir des résultats effectifs, il convient que les activités de sûreté de fonctionnement soient étroitement coordonnées avec les autres activités rattachées au produit plutôt que conduites séparément.

Pour adapter un programme de sûreté de fonctionnement, il convient que les instances dirigeantes du fournisseur et du client prennent en compte:

– l'application que l'utilisateur fera du produit (voir 5.2);
– le cadre contractuel, présent ou à venir (voir 5.3);
– l'applicabilité de tout ou partie des phases du cycle de vie d'un produit (voir 5.4);
– les caractéristiques relatives au produit (voir 5.5);
– l'historique de produits similaires;
– les aspects coût/bénéfices pour chaque tâche du programme;
– les analyses de compromis entre le matériel et le logiciel.

4.2.6 *Disposal phase*

The disposal phase is the life-cycle phase after the operation and maintenance phase, during which the product is removed from its use site and dismantled, decommissioned, destroyed or stored if necessary in a protected environment.

This phase may include disassembly of the product in order to perform activities such as:

- tests and wear analyses
- feedback of data to the supplier in order to improve reliability and maintainability
- recovery of materials for recycling processes.

5 Tailoring criteria for dependability programmes

5.1 *General*

The dependability programme elements and tasks defined in this part of IEC 300 are expressed in general terms. For a specific product or project, the dependability programme should be tailored, giving appropriate consideration to the relevant product and project aspects.

When invoking this part of IEC 300, the parties involved should agree upon and record the extent to which it is applied. The agreement should be documented. For those clauses, or parts of clauses, identified by that agreement, as applicable, the recommendation (use of the verbal form "should") can change to a requirement (the verbal form "shall").

The assembly of an effective dependability programme during any of the product life-cycle phases requires not only a knowledge of dependability principles, methods and techniques, but also an understanding of the product itself and its technology, its intended use and various related cost factors.

In order to obtain effective results, dependability activities should be closely coordinated with other activities connected with the product rather than managed separately.

In tailoring a dependability programme, management should take into account:

- the user application of the product (see 5.2);
- the contract situation, actual or anticipated (see 5.3);
- the applicability of all or some of the phases of a product's life cycle (see 5.4);
- product related characteristics (see 5.5);
- past history of similar products;
- cost/benefit aspects of each programme task;
- hardware/software trade off.

5.2 *Application propre à l'utilisateur*

La nécessité de spécifier les exigences de sûreté de fonctionnement et de les appliquer à un programme de sûreté de fonctionnement pour un produit et son soutien dépend des conditions du marché (utilisateur final) qui prévalent dans chaque cas. Des considérations de sûreté de fonctionnement peuvent être dictées par différents facteurs, tels que la sécurité, l'efficacité ou des considérations économiques liées aux différentes situations du marché. Les systèmes divers auxquels de telles considérations s'appliquent comprennent, par exemple: les systèmes aéronautiques, les centrales nucléaires, les équipements médicaux, les équipements de contrôle-commande, les produits militaires, les systèmes de télécommunication, les produits de grande consommation.

De toute évidence, l'importance de la sûreté de fonctionnement est différente pour chacune de ces situations et le programme de sûreté de fonctionnement doit être adapté en conséquence.

5.3 *Situation contractuelle*

L'application d'un élément de programme particulier dépend généralement de la situation contractuelle qui couvre les relations client - fournisseur dans le cadre du projet. Cela couvre les situations dans lesquelles le fournisseur est responsable:

– de la planification et du développement du produit conformément aux demandes du client;

– de la fabrication du produit conformément à une spécification établie et acceptée au préalable;

– de l'essai et de l'inspection finals;

– de l'installation du produit pour le compte de l'utilisateur à des fins d'exploitation, lorsqu'il a été développé et fabriqué préalablement suivant un contrat séparé;

– de la maintenance du produit conformément à une politique de maintenance donnée.

NOTE – Les dispositions de cette partie de la CEI 300 sont aussi applicables pour une situation non contractuelle, c'est-à-dire lorsqu'un produit a été planifié et développé en l'absence de contrat en fonction de besoins identifiés de clients et utilisateurs potentiels puis fabriqué et introduit sur le marché en conséquence. Cette recommandation pour l'adaptation d'un programme s'applique aussi à de telles situations.

5.4 *Application aux phases du cycle de vie*

Dans une situation donnée de projet ou de contrat, il convient que les éléments et tâches de sûreté de fonctionnement qu'il faut choisir pour les inclure dans le programme correspondent aux phases de cycle de vie avec lesquelles elles sont en rapport.

Les activités appropriées aux différentes phases sont données dans le tableau 1 et en annexe B.

5.5 *Caractéristiques du produit*

Lorsque l'on adapte à un produit un programme de sûreté de fonctionnement, il est important de prendre en compte les caractéristiques mêmes du produit, y compris:

– le caractère innovateur du produit

– la criticité de défaillance du produit

– le niveau requis de sûreté de fonctionnement.

5.2 *User application*

The need to specify dependability requirements and to apply a dependability programme for a product and its support depends on the market (end user) conditions prevailing in each case. Dependability considerations may be prescribed by various factors, such as safety or effectiveness, or by economical considerations related to different market situations. Examples of some of the varied systems to which such considerations apply include: flight systems, nuclear power plants, equipment for medical use, process control equipment, military products, telecommunication systems, consumer products.

The importance of dependability is obviously different in each of these situations and the dependability programme should be tailored accordingly.

5.3 *Contract situation*

The application of a specific dependability programme element generally depends on the contract situation that covers the supplier-customer relationship in the specific project case. This covers situations where the supplier is responsible for:

- product planning and development according to customer requirements;
- product manufacturing in accordance with a specification which has been previously established and agreed;
- final inspection and test;
- installing the product on behalf of the customer for operational use, when it has been previously developed and manufactured under a separate contract;
- maintenance of the product in accordance with a given maintenance policy.

NOTE – The provisions of this part of IEC 300 are also applicable to non-contractual situations, i.e. when a product is being planned and developed without a contract, according to identified needs of prospective customers and users, and is subsequently manufactured and introduced to the market. The advice on tailoring also applies to such situations.

5.4 *Life-cycle phase applications*

In a given project/contract situation the dependability elements and tasks to be selected for inclusion in the programme should correspond to the life-cycle phase(s) that are relevant.

The activities appropriate to the different phases are given in figure 1 and annex B.

5.5 *Product-related characteristics*

When tailoring a dependability programme, it is important to take account of the characteristics of the product itself including:

- the novelty of the product;
- the criticality of failure of the product;
- the required level of dependability.

5.6 *Considérations relatives au logiciel*

En termes généraux et dans sa philosophie, cette norme est également applicable à toutes les parties d'un système, y compris le logiciel.

Lorsque l'on s'intéresse au logiciel au cours du processus d'adaptation du programme de sûreté de fonctionnement, il convient de considérer l'application du logiciel, c'est-à-dire:

- s'il est critique du point de vue de la sûreté
- s'il s'agit d'un logiciel temps réel
- si l'application est militaire
- s'il s'agit d'une application de contrôle-commande d'un procédé
- s'il s'agit d'une application commerciale, etc.

Le type de l'application, associé à d'autres facteurs tels que la taille, la complexité, les conséquences d'une défaillance, détermineront les exigences d'adaptation. Un guide plus détaillé dans le domaine de la sûreté de fonctionnement pour les aspects logiciels est fourni dans la future CEI 300-3-6.

6 Eléments et tâches d'un projet ou d'un programme spécifique d'un produit ou d'un projet

6.1 *Planification et gestion*

6.1.1 *Plans de sûreté de fonctionnement*

Le programme de sûreté de fonctionnement a besoin d'une planification adéquate et de l'implication de la direction.

Le plan de sûreté de fonctionnement sert de document de base pour la gestion, la planification et le contrôle, en dirigeant la réalisation du programme de sûreté de fonctionnement. Il convient qu'il soit préparé, intégré aux autres plans et formellement revu avant le début d'un nouveau projet ou la planification d'un nouveau produit ou d'un produit modifié.

Il convient que le plan concerne les activités qui pourraient affecter la sûreté de fonctionnement du produit et définisse clairement l'engagement de la direction pour sa mise en oeuvre, décrive l'approche et la méthodologie appliquées à la réalisation et au contrôle des tâches, et assure l'efficacité dans la réalisation des tâches.

Il convient que le plan contienne:

- l'identification et la description des éléments et tâches du plan de sûreté de fonctionnement choisis pour le projet pour lequel le plan est préparé;
- l'identification et la description des tâches de revue et d'audit requis pour que l'on puisse s'assurer de l'exécution adéquate du plan, y compris de la bonne coordination avec les autres activités;
- l'identité (l'endroit dans l'organisation), la responsabilité, l'autorité et les relations entre les différentes catégories du personnel, celui qui dirige, celui qui exécute et celui qui vérifie l'exécution des tâches;

5.6 *Software considerations*

In general terms and philosophy this standard is equally applicable to all parts of a system, including the software.

When addressing software in the tailoring process the type of application of the software should be considered i.e.

- safety critical;
- real-time;
- military;
- process control;
- commercial etc.

The type of application, together with other factors such as size, complexity and impact of failure will determine the tailoring requirements. Further guidance in the field of software aspects of dependability can be found in future IEC 300-3-6.

6 Project-specific or product-specific programme elements and tasks

6.1 *Planning and management*

6.1.1 *Dependability plans*

The dependability programme needs adequate planning and management involvement.

The dependability plan serves as the basic management, planning and control document, governing the execution of the dependability programme. It should be prepared, integrated with other plans and formally reviewed before the start of a new project or the planning for a new or modified product.

The plan should address activities that might affect the product's dependability and should clearly define the management commitment for its implementation. It should present the approach and methodology applicable to task execution and control and should ensure effectiveness in the execution of the tasks.

The dependability plan should include:

- identification and description of the elements and tasks selected for the project for which this plan is being prepared;
- identification and description of audit and review tasks required to ensure adequate execution of the tasks of the plan, including proper coordination with other activities;
- identity (organizational location), responsibility, authority and interrelation of personnel who manage, execute and verify execution of the tasks;

– la description des détails de procédure concernant la mise en oeuvre des tâches, les prévisions des temps nécessaires, les étapes et les points clés, les revues de conception ainsi que les critères de vérification et de validation;

– la définition des moyens nécessaires pour réaliser en temps et en heure les tâches précitées, tout au long du programme;

– la définition des produits et documents livrables pour chaque étape et point clé et l'identification de l'organisation qui développera, sélectionnera et utilisera les documents exigés;

– la définition d'une maîtrise de la documentation et du système de gestion de configuration;

– l'établissement des liens d'information entre la sûreté de fonctionnement et les diverses disciplines auxquelles elle se rapporte pour s'assurer d'une transmission coordonnée des données nécessaires;

– la gestion de la sous-traitance.

NOTES

1 Dans leurs plans de sûreté de fonctionnement, il convient que les clients entreprennent toute action nécessaire pour s'assurer de la conformité aux conditions d'exploitation et de maintenance du produit comme spécifié.

2 Il convient, si nécessaire, que les clients assistent le fournisseur dans la préparation du plan de sûreté de fonctionnement , en incluant les informations nécessaires pour la définition des conditions d'exploitation et de logistique de maintenance.

6.1.2 *Gestion des décisions concernant le projet*

La gestion des décisions concernant le projet est la partie de la gestion du projet qui est en rapport avec la planification des aspects liés à la maitrise du projet.

Il convient que des étapes (c'est-à-dire des points clés) soient établis pour le programme de sûreté de fonctionnement. Il convient que ces étapes soient coordonnées avec le cycle de vie du produit.

6.1.3 *Gestion de la traçabilité*

Des moyens effectifs doivent être mis en place pour assurer le suivi du programme, y compris les dispositions nécessaires pour suivre l'évolution d'une activité de sûreté de fonctionnement et assurer la traçabilité de cette activité par rapport à l'exigence d'origine.

Il convient qu'une organisation intègre un système d'actions correctives, en accord avec l'article 15 de l'ISO 9004-1 pour résoudre les problèmes de sûreté de fonctionnement identifiés. Il convient que le client fournisse le soutien nécessaire en établissant les liens entre les exigences du client et les évaluations des performances opérationnelles.

6.1.4 *Gestion de configuration*

Il peut être nécessaire d'apporter des changements au produit et à sa logistique de maintenance pendant n'importe quelle phase du cycle de vie, il convient qu'il existe un système de gestion de configuration, en accord avec 8.8 de l'IS0 9004-1 et selon le cas, avec 6.1 de l'ISO 9000-3, qui établisse un processus systématique pour maîtriser, surveiller et documenter les modifications du produit et de sa logistique de maintenance.

Il convient que la spécification de sûreté de fonctionnement soit considérée en tant que base première du système de gestion de configuration.

– description of procedural details of task implementation, related time schedule, milestones and checkpoints, and design review, verification and validation criteria;

– definition of the resources required for the timely performance of the identified tasks throughout the programme;

– definition of deliverable products or documents for each milestone and checkpoint, and identification of the organization that will develop, select and use the required documents;

– definition of a document control and configuration management system;

– establishment of information links between dependability and related disciplines to ensure the coordinated transmission of relevant data;

– subcontractor control.

NOTES

1 In their dependability plans, customers should take any necessary action to ensure compliance with the operation and maintenance conditions for the product as specified.

2 Customers should assist suppliers as necessary in the preparation of the supplier's dependability plan, and should provide any information required for the definition of operation and maintenance support conditions.

6.1.2 *Project decision management*

Project decision management is that part of project management which is concerned with scheduling control aspects of the project.

Milestones and check-points should be established for the dependability programme. These milestones should be coordinated with those of the product life cycle.

6.1.3 *Traceability management*

Effective means should be provided to ensure traceability including the arrangements necessary to monitor the evolution of a dependability activity and ensure its traceability to the original requirement.

An organization should have a corrective action system in place, in accordance with clause 15 of ISO 9004-1, to resolve dependability issues that are identified. The customer should provide necessary support in establishing links between customer requirements and field performance evaluations.

6.1.4 *Configuration management*

It may be necessary to introduce changes to the product and its maintenance support during any phase of the life cycle. A configuration management system should be established, in accordance with 8.8 of ISO 9004-1 and, where appropriate, 6.1 of ISO 9000-3, that provides a systematic process for controlling, monitoring and documenting changes to the product and its maintenance support.

The dependability specification should be considered as the first baseline in the configuration management system.

6.2 *Revue de contrat et liaison*

6.2.1 *Revue de contrat*

Il convient que chaque revue de contrat soit conduite en tenant compte des exigences spécifiques de sûreté de fonctionnement. Cette revue est réalisée en même temps que celle des exigences stipulées en 4.3 de l'ISO 9001. Les exigences de sûreté de fonctionnement soumises à la revue de contrat peuvent typiquement comprendre:

- le domaine d'application et le planning des exigences de sûreté de fonctionnement;
- les objectifs spécifiques de livraison et les articles livrables;
- les moyens d'adaptation spécifiques, selon le cas;
- les exigences spécifiques de documentation;
- les dispositions spécifiques pour les démonstrations ou les essai;
- les autorisations, pénalités, bonus spécifiques;
- les conditions d'environnement dans lesquelles le produit doit être utilisé.

6.2.2 *Représentants de la direction*

Afin d'avoir une liaison effective entre les parties concernées, il convient que les représentants de la direction aient une connaissance suffisante du produit et de son soutien ainsi que des principes et pratiques de la sûreté de fonctionnement. Ils peuvent rechercher le soutien d'experts sur certains points. Voir 5.2.2 de l'ISO 9004-1.

Il convient qu'ils aient l'autorité nécessaire pour prendre des décisions dans les relations client - fournisseur concernant:

- les spécifications, les revues et les modifications des exigences de sûreté de fonctionnement;
- la conclusion d'accords avec l'autre partie au sujet des données de sûreté de fonctionnement, de la documentation, des programmes en commun et des revues de conception;
- l'assurance que les organisations respectives honorent les engagements signés sur la sûreté de fonctionnement;
- la définition des procédures et critères de validation et, d'acceptation de la sûreté de fonctionnement.

6.3 *Exigences de sûreté de fonctionnement*

6.3.1 *Spécification des exigences de sûreté de fonctionnement*

Il convient que les spécifications de sûreté de fonctionnement soient préparées par le client et/ou par le fournisseur, suivant le cas, pour le produit et ses composants ainsi que pour son soutien.

Cette tâche comprend l'analyse et l'établissement:

- des exigences qualitatives de fiabilité et de maintenabilité du produit la définition des fonctions du produit, les critères de panne, les conditions d'environnement et d'exploitation, la durée de vie de l'entité pendant laquelle les exigences doivent être remplies;

6.2 *Contract review and liaison*

6.2.1 *Contract review*

Contract review should be conducted with respect to specific dependability requirements. This review should be performed in conjunction with the requirements as stipulated in 4.3 of ISO 9001. Typical dependability related contract requirements subject to review may include:

- scope and schedule of dependability activities;
- specific delivery targets and deliverable items;
- specific resources tailored as appropriate;
- specific documentation requirements;
- specific test or demonstration provisions;
- warranty, penalty and specific incentive details;
- the environmental conditions under which the product is to be used.

6.2.2 *Management representative*

To provide effective liaison between the parties involved, management representatives should have adequate knowledge about the product and its support, and about dependability principles and practices. They may seek the support of experts on certain issues. See 5.2.2 of ISO 9004-1.

The representative should have the authority to make decisions in customer-supplier relations concerning:

- specification, review and modification of dependability requirements;
- concluding agreements with the other party with regard to dependability data, documentation, joint programme and design reviews;
- assurance that the respective organizations honour the agreements on dependability;
- definition of dependability validation, acceptance procedures and criteria.

6.3 *Dependability requirements*

6.3.1 *Specification of dependability requirements*

Dependability specifications should be prepared by the supplier and/or customer, as appropriate, for the product and its parts and for the product support.

This task should include the analysis and establishment of:

- qualitative product reliability and maintainability requirements, definition of product functions, fault criteria, environmental and operational conditions, life of the item during which compliance with the requirements is expected;

– des exigences quantitatives concernant les mesures des caractéristiques de fiabilité, de maintenabilité et de disponibilité (par exemple le taux de défaillance total, la fiabilité de la mission, le temps moyen d'indisponibilité). La préparation des entrées vers la spécification du système ainsi que les exigences de démonstration et d'assurance font partie de cette tâche;

– des exigences de testabilité (fonctions et procédures d'essai, précision de l'essai pour chaque niveau d'intervention défini pour le produit, etc.);

– des exigences qualitatives et quantitatives (ou les conditions) concernant la logistique de maintenance.

La spécification de sûreté de fonctionnement fournit une base de compréhension entre le client et le fournisseur, et entre les différents groupes de personnel (du client et du fournisseur) impliqués dans la conception et l'exploitation du produit.

La définition des types de cas de panne qui pourraient avoir un impact sur l'utilisation effective du produit est la base de chaque spécification de sûreté de fonctionnement. Il est recommandé que tout développement d'une spécification de sûreté de fonctionnement parte de cette considération.

Il convient que les exigences spécifiées aient des caractéristiques non-ambiguës, vérifiables, cohérentes et traçables.

NOTE - Il convient que toute interdépendance entre les exigences soit clairement établie.

Il convient que la spécification pour chaque exigence indique aussi les moyens et procédures de vérification de la conformité (méthodes analytiques, simulations, essais, etc.), ainsi que les phases du cycle de vie pendant lesquelles la conformité sera vérifiée.

Pour une information plus détaillée, voir la CEI/FDIS 300-3-4. Pour les applications qui impliquent des composants électroniques, voir la CEI 409 et la CEI 419.

6.3.2 *Interprétation des exigences*

Il convient que cette tâche inclue l'analyse des conditions et des contraintes qui sont particulières à l'utilisation attendue du produit, et qui peuvent affecter sa sûreté de fonctionnement, y compris.

– les conditions d'exploitation et de maintenance comprenant, par exemple, les types et durées de mission;

– l'identification des cycles de charges et obligations imposés au produit pendant l'utilisation attendue;

– la détermination des conditions d'environnement et d'exploitation supportées par chaque ensemble et sous-ensemble du produit pendant chaque phase d'utilisation et pendant les activités de maintenance et de soutien (y compris le stockage, le transport, etc.);

– la détermination des effets de la fabrication, des essais, du stockage, du conditionnement, du transport, de la manutention et de la maintenance.

Il convient d'identifier les contraintes exercées par la politique de maintenance, le niveau de qualification du personnel, etc., et de recommander les changements, le cas échéant.

– quantitative requirements on measures of reliability performance, maintainability performance and availability performance (for example overall failure rate, mission reliability, mean down time). The preparation of dependability inputs to the system specification, together with demonstration and assurance requirements, is part of this task;

– testability requirements (test functions and procedures, test accuracy of each indenture level of the product, etc.);

– qualitative and quantitative requirements on (or conditions for) maintenance support.

The dependability specification provides the basis of understanding between the customer and the supplier and between different (supplier and customer) groups of personnel involved with the product's design and use.

Basic to each dependability specification is the definition of the kind of fault situations that might have an impact on the effective use of the product. Any development of a dependability specification should start from this consideration.

The specified requirements should be unambiguous, assessable, consistent and traceable.

NOTE – All interdependence between requirements should be clearly indicated.

The specification of each requirement should also indicate the means and procedures for verifying conformity (for example by analytical methods, simulations, testing, etc.), and the life-cycle phase(s) during which conformity will be verified.

For more detailed information see IEC/FDIS 300-3-4. For applications involving electronic components see IEC 409 and IEC 419.

6.3.2 *Requirements interpretation*

The interpretation of requirements should include analysis of those conditions and constraints that are typical for the intended use of the product, and that may affect its dependability, including:

– operation and maintenance conditions, including, for example, mission types and durations;

– identification of load and duty cycles imposed on the product during the intended use;

– determination of environmental and operational conditions experienced by each assembly and sub-assembly of the product during each phase of use and during maintenance and support activities (including storage, transportation, etc.);

– determination of the effects of manufacturing, testing, storage, packaging, transportation, handling and maintenance.

Constraints caused by the maintenance policy, personnel skill level, etc. should be identified and changes recommended, if appropriate.

Il convient de consigner formellement et de relier à la spécification de sûreté de fonctionnement tout accord sur l'interprétation des dispositions de la spécification des exigences.

6.3.3 *Répartition des exigences*

Il convient que la répartition des exigences de sûreté de fonctionnement sur des parties du produit (ou sur certaines parties du système de soutien) soit faite en tenant compte de la structure du produit et des dispositions propres à la maintenance, des possibilités de vérification et de validation des exigences, et du processus de conception.

NOTE – Dans la répartition des mesures des caractéristiques de sûreté de fonctionnement, il peut s'avérer nécessaire, pour certaines parties ou pour certaines phases du cycle de vie, d'utiliser d'autres mesures que celles définies dans la spécification de sûreté de fonctionnement. Par exemple la maîtrise de la fiabilité peut nécessiter, pendant la phase de conception et de développement, l'utilisation de critères pour le nombre de pannes rencontrées pendant les diverses activités d'essais.

Il convient que la répartition soit incluse dans les spécifications pour toutes les parties sous-traitées du produit fini et soient utilisées comme base pour la vérification, la validation, la spécification de la procédure d'essai et la conception.

NOTE – Il peut arriver qu'il faille reconsidérer l'allocation des exigences au fur et à mesure que le processus de conception progresse, par exemple suite à un résultat d'analyse de compromis.

6.4 *Ingénierie*

6.4.1 *Ingénierie de la fiabilité*

Un haut degré de fiabilité est obtenu par des techniques de conception pour, soit prévenir de l'occurrence des défaillances (éviter la panne), soit éliminer leurs effets (tolérance aux pannes).

De telles activités de conception peuvent typiquement inclure:

– application des techniques de tolérance aux pannes (redondances, programmation parallèle, reconfiguration, remises en route) et de sûreté intégrée;

– application des procédures de conception (par exemple conception descendante, programmation structurée, réduction des charges des composants matériels);

– élimination des modes critiques de panne unique;

– maîtrise des contraintes appliquées aux pièces et aux composants;

– maîtrise de la charge d'exécution du logiciel;

– réduction des effets sur la performance de conception à partir de la variation d'un paramètre (par exemple usure);

– utilisation de composants et de technologies recommandées avec des caractéristiques de fiabilité démontrées;

– définition de méthodes pour réduire la sensibilité aux processus de fabrication;

– compatibilité avec les normes de sécurité;

– techniques spécifiques pour s'assurer d'un logiciel raisonnablement sans panne au moyen, par exemple, d'inspection de code, d'audit de code et d'une vérification pas à pas des instructions.

Lorsque le travail de conception s'appuie sur un produit existant, il convient que la performance de fiabilité de ce produit soit clairement documentée et que tout problème connu soit corrigé pendant la phase de développement.

Any agreed interpretation of the provisions of the requirements specification should be formally documented and attached to the dependability specification.

6.3.3 *Requirements allocation*

The allocation of dependability requirements to parts of the product (or to parts of the support process) should take account of the structure of the product and the arrangements for maintenance, the possibilities of verification and validation of requirements, and the design process.

NOTE – When allocating measures for dependability characteristics it may, for some parts of the product and for some life-cycle phases, prove necessary to use measures other than those defined in the dependability specification. For example the control of reliability may, during the design and development phase, use criteria for the number of faults found at various test activities.

Allocations should be included in specifications for any subcontracted parts of the end-product and should be used as a basis for verification, validation and test procedure specification and design.

NOTE – Allocations may have to be reconsidered as the design process progresses, for example as a result of trade-off studies.

6.4 *Engineering*

6.4.1 *Reliability engineering*

The required reliability performance is obtained by employing design techniques either to prevent failures from occurring (fault avoidance) or to eliminate their effects (fault tolerance).

Such design activities may typically include the following:

- application of fault-tolerance (redundancies, parallel programming, reconfiguration, restarts) and fail-safe techniques;
- application of design procedures (for example top-down design, structured programming, hardware component derating);
- elimination of critical single point fault modes;
- control of stresses applied to components and assemblies;
- control of execution load on software;
- reduction of effects on design performance from parameter variation (for example ageing);
- use of preferred and proven parts and technology;
- definition of methods to reduce sensitivity to manufacturing processes;
- adherence to safety standards;
- specific techniques for ensuring reasonably fault-free software by means of, for example, code inspection, code audit and walk-through processes.

When the design work is based on an existing product, the reliability performance of that product should be clearly documented and any known problems corrected during the development phase.

Il convient que la tâche inclue aussi l'identification des éléments critiques de sûreté de fonctionnement selon les critères et la définition de criticité spécifiées et l'élaboration d'un programme pour la maîtrise et la gestion spéciale des éléments critiques, depuis la phase de conception et de développement jusqu'à la phase de fabrication et d'installation.

NOTE – Il convient que l'ingénierie de la fiabilité soit en étroite relation avec l'ingénierie de la maintenabilité, de la logistique de maintenance, des facteurs humains, de la testabilité, avec les activités d'analyse, de prévisions et de revues de conception et avec l'ingénierie matérielle et logicielle.

6.4.2 *Ingénierie de la maintenabilité*

Un haut degré de maintenabilité peut être obtenu quand le produit est facile à maintenir et à réparer. Par exemple des techniques de maintenance automatiques telles que le redémarrage automatique après défaillance logicielle, peuvent être appliquées au produit.

Il convient que cette tâche inclue l'établissement et la revue périodique des critères de conception de maintenabilité détaillée à partir des exigences de maintenabilité spécifiées pour le produit. Il convient, par exemple, qu'elle décrive les méthodes et techniques pour minimiser:

– la complexité de la maintenance;

– la fréquence des activités de maintenance préventive dictées par la conception du produit;

– la contribution spécifique du produit même au temps d'indisponibilité;

– les coûts de logistique de maintenance dictés par la conception du produit;

– les exigences de qualification du personnel de maintenance;

– les erreurs de maintenance potentielles.

Lorsque le travail de conception est basé sur un produit existant, il convient que la performance de maintenabilité de ce produit soit clairement documentée et que tout problème connu soit considéré pendant la phase de développement.

Pour des informations plus détaillées, voir la CEI 706.

6.4.3 *Ingénierie de la logistique de maintenance*

La logistique de maintenance peut être spécifiée pendant la phase d'installation du produit et pendant la phase d'exploitation et de maintenance. Elle nécessite des moyens et des directives. Basée sur la définition d'une politique de maintenance, des procédures, des outils, des équipements d'essai, de la documentation et autres moyens nécessaires pour soutenir cette politique, des programmes de formation pour le personnel de maintenance etc., cette tâche doit couvrir l'identification et la préparation:

– des procédures et moyens pour recueillir, analyser et évaluer des données relatives aux rapports de panne et de maintenance;

– des procédures et moyens pour gérer les demandes de modification et les changements dans la conception du produit;

– l'identification de l'intervalle de temps pendant lequel le produit sera soutenu respectivement par le fournisseur et le client.

Lorsque le travail de conception s'appuie sur un produit existant, il convient que les hypothèses de la logistique de maintenance de ce produit soient revues et que chaque problème connu soit considéré.

Reliability engineering should also include the identification of items critical to dependability using specified criticality criteria and definitions, and the establishment of a programme for control and special handling of critical items, from the design and development phase to the manufacturing and installation phase.

NOTE – Reliability engineering should be performed in close working relationship with maintainability engineering, maintenance support engineering, human factors engineering, testability engineering, with analysis, prediction and design review activities and with component and software engineering.

6.4.2 *Maintainability engineering*

Good maintainability performance is achieved by making the product easy to maintain and repair. For example automatic maintenance techniques, such as automatic restarts at software induced failures, may be applied to the product.

The task of maintainability engineering should include the derivation and periodic review of detailed maintainability design criteria from the maintainability requirements specified for the product. Methods and techniques should be implemented to minimize:

- complexity of maintenance;
- frequency of preventive maintenance activities dictated by the product design;
- product-specific contribution to down time;
- maintenance support costs dictated by the product design;
- maintenance personnel skill requirements;
- potential for maintenance mistakes.

When the design work is based on an existing product, that product's maintainability performance should be clearly documented and any known problems considered during the development phase.

For more detailed information see IEC 706.

6.4.3 *Maintenance support engineering*

Maintenance support may be required during the installation of the product and during the operation and maintenance phase. It requires resources and directives. Based on the defined maintenance policy, procedures, tools, test equipment, documentation and other facilities required to support that policy, training programmes for maintenance personnel, etc., this task should cover identification and preparation of:

- procedures and resources needed for collection, analysis and evaluation of data-related fault and maintenance reports;
- procedures and resources needed for processing product change or modification requests and product changes;
- identification of the time intervals during which the product will be supported by the supplier and by the customer, respectively.

When the design work is based on an existing product, that product's maintenance support conditions should be reviewed and known problems considered.

Pour une information plus détaillée, voir la CEI 706.

6.4.4 *Ingénierie de la testabilité*

La fiabilité comme la maintenabilité du produit sont influencées par les moyens externes ou intégrés au produit pour la surveillance, la détection et la localisation des pannes, et toute dégradation des caractéristiques du produit.

Il convient que cette partie de la spécification de sûreté de fonctionnement du produit concernant la testabilité (fonctions et procédures d'essai, précision de l'essai pour chaque niveau de décomposition du produit, etc.) guide les activités de conception correspondantes.

Lorsque le travail de conception s'appuie sur un produit existant, il convient que les caractéristiques de testabilité de ce produit soient clairement documentées et que tout problème connu soit corrigé pendant la phase de développement.

6.4.5 *Ingénierie des facteurs humains*

Il convient que les activités de conception soient guidées par des lignes directrices concernant les considérations relatives au facteur humain, en particulier les interfaces entre le personnel et le produit lui-même. Il convient que les tâches de conception du produit prennent en compte la minimisation de l'erreur humaine et de ses conséquences pendant les phases du cycle de vie (la fabrication et l'installation, ainsi que l'exploitation, la maintenance et la mise au rebut).

L'ingénierie des facteurs humains doit être conduite pour s'assurer que:

– la sûreté de fonctionnement n'est pas trop dégradée par l'interaction entre le produit et son personnel d'exploitation et de maintenance;

– que ce personnel peut être effectivement et économiquement formé et utilisé;

– que tout matériel d'instruction est convenablement adapté aux utilisateurs futurs.

Il convient que l'ingénierie des facteurs humains influence aussi, si nécessaire, la planification et l'exécution des activités de vérification, de validation et d'essai pour que l'on puisse s'assurer que l'ensemble des objectifs du produit a été atteint.

6.5 *Produits fournis par des tiers*

6.5.1 *Produits fournis par des sous-traitants*

Lorsque certaines parties du produit sont fournies par un sous-traitant, il convient que ce fournisseur s'assure:

– que les exigences du programme de sûreté de fonctionnement, en accord avec la présente norme, ont été prises en considération;

– qu'elles correspondent exactement aux exigences relatives à la totalité du produit livrable.

Voir également l'article 9 de l'ISO 9004-1.

For more detailed information see IEC 706.

6.4.4 *Testability engineering*

Both the reliability performance and the maintainability performance of the product are influenced by the built-in or external facilities for monitoring, detection and localization of faults and any degradation of the product characteristics.

That part of the dependability specification addressing the testability requirements (test functions and procedures, test accuracy of each indenture level of the product, etc) should provide guidance on these design activities.

When the design work is based on an existing product, that product's testability characteristics should be clearly documented and known problems considered during the development phase.

6.4.5 *Human factors engineering*

Design activities should be guided by consideration of human factors with regard to the interfaces between personnel and the product itself. Product design tasks should aim to minimize human error and its consequences during the life-cycle phases of manufacturing and installation, operation and maintenance and disposal.

Human factors engineering should be conducted to ensure that:

– dependability is not unduly degraded by the interaction between the product and operations and maintenance personnel;

– the operations and maintenance personnel can be effectively and economically trained and utilized;

– any instructional material is suitably adapted to prospective users.

Human factors engineering should also influence, as necessary, the planning and execution of verification, validation and test activities to ensure that overall product objectives are met.

6.5 *Externally provided products*

6.5.1 *Subcontracted products*

When parts of the product are provided by second level suppliers (subcontractors), the supplier should ensure that:

– appropriate dependability programme requirements are invoked in accordance with this standard for those parts as well as for parts that are procured from others;

– the requirements for those parts adequately correspond to the requirements for the entire deliverable product.

See also clause 9 of ISO 9004-1.

6.5.2 *Produits fournis par le client*

Dans le cas où le client fournit des pièces du produit destinées à être intégrées dans le produit final, il convient que le fournisseur demande au client de fournir:

– la preuve que la pièce a été ou est conçue et fabriquée selon le programme de sûreté de fonctionnement en conformité avec les dispositions de la CEI 300-1/ ISO 9000-4;

– la soumission de toute information et données concernant les pièces fournies par le client nécessaires pour l'analyse de sûreté de fonctionnement et l'évaluation du produit fini;

– l'identification de tout problème qui peut être rencontré avec des pièces fournies par le client.

Voir également l'article 9 de l'ISO 9004-1.

6.6 *Analyse, prévision et revues de conception*

6.6.1 *Analyse des modes de défaillance et de leurs effets*

Il convient que les parties matérielles et logicielles du produit soient soumises à une analyse des modes de défaillance, de leurs effets et de leur criticité, ou niveau requis pour les nécessités fonctionnelles et de sécurité.

L'analyse des modes de défaillance et de leurs effets (AMDE) et l'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) sont des procédures utilisées pour l'identification systématique des modes de défaillance potentiels d'un produit, les effets de ces défaillances et de leur criticité.

Il convient que les AMDE et AMDEC soient aussi utilisées pour les prévisions et à des fins de vérification, pour les analyses de compromis et de risque, en tant que support pour la documentation des modifications du produit et pour la documentation de logistique de maintenance, et dans la détermination des besoins pour la surveillance et l'essai automatique du produit.

Il convient que la validation de ces analyses soit reconsidérée en même temps que l'avancement de la conception et quelle soit répétée lors des changements de conception ou lors des modifications des conditions d'exploitation et de soutien et, si possible, l'utiliser pour la vérification ou la validation des exigences qualitatives de sûreté de fonctionnement.

Il convient que les analyses donnent aussi des résultats pour:

– la détermination des éléments (activités de soutien ou pièces du produit) critiques pour la sûreté de fonctionnement;

– la détermination des éléments à durée de vie limitée pour les surveiller en permanence et entreprendre toute adaptation nécessaire de la politique de maintenance.

Pour une information plus détaillée, voir la CEI 812.

6.6.2 *Analyse par arbre de panne*

Il convient que les parties matérielles et logicielles du produit soient soumises à une analyse par arbre de panne.

6.5.2 *Customer-provided products*

In the case where the customer provides parts for inclusion in the deliverable product, the supplier should request the customer to provide:

– evidence that the part has been or is being designed and manufactured according to a dependability programme complying with the provisions of IEC 300-1/ISO 9000-4;

– relevant data and information about the customer-provided part needed for dependability analysis and evaluation of the end-product;

– identification of any problem that could be encountered with the parts.

See also clause 9 of ISO 9004-1.

6.6 *Analysis, prediction and design review*

6.6.1 *Fault modes and effects analysis*

The hardware and software parts of the product should be subjected to a fault modes, effects and criticality analysis to the extent required for functional and safety reasons.

Fault modes and effects analysis (FMEA) and fault modes, effects and criticality analysis (FMECA) are procedures used for a systematic identification of the potential fault modes of a product, the effects of these faults and their criticality.

FMEAs and FMECAs are used as a basis for dependability predictions and should also be used for verification purposes, for trade-off and risk analyses, as support for documentation at product changes and maintenance support documentation, and in determination of needs for monitoring and automatic testing of the product.

The validity of the analyses should be reconsidered as the design progresses, repeated when design changes or modifications are made to operation and support conditions, and, if possible, used for verification or validation of qualitative dependability requirements.

The analyses should also be used to identify:

– product parts or support activities critical to dependability;

– life limited items that will require continued attention and that may justify modification of the maintenance policy.

For more detailed information see IEC 812.

6.6.2 *Fault tree analysis*

Hardware and software parts of the product should be subjected to a fault tree analysis.

L'analyse par arbre de panne (AAP) est une approche structurée pour déterminer les causes (internes ou externes) qui, à elles seules ou combinées, conduisent à un état défini pour le produit (panne, condition peu sûre, etc.). Il convient que l'AAP soit utilisée comme un outil analytique pour déterminer les causes des modes de panne significatifs et pour clarifier l'origine du mode de panne identifié.

Pour une information plus détaillée, voir la CEI 1025.

6.6.3 *Analyses des contraintes et des charges*

Il convient que les éléments matériels soient soumis à une analyse des contraintes, et que les éléments logiciels soient soumis à une analyse des charges.

Les produits ou parties du produit peuvent être plus enclins à défaillance sous contrainte importante.

Il convient que la réduction des charges des composants soit en conformité avec une politique acceptée, sauf dans des cas spécifiquement documentés.

Il convient que les résultats des analyses des contraintes et des charges soient utilisés en tant qu'entrées pour la conception et le développement.

6.6.4 *Analyse des facteurs humains*

Il convient que chaque interface entre le produit (y compris sa documentation d'exploitation et de maintenance) et le personnel d'exploitation et de maintenance soit analysée, en ce qui concerne les effets potentiels des erreurs humaines, en termes de modes de panne du produit. En particulier:

– analyser le produit pour s'assurer que chaque niveau d'interface humain et que les tâches humaines correspondantes sont déterminés;

– évaluer les erreurs humaines potentielles pour chaque interface en termes de causes et de conséquences;

– entreprendre les modifications sur la conception et/ou les procédures pour réduire la possibilité des erreurs et leurs conséquences.

6.6.5 *Prévisions*

Il convient que les prévisions soient utilisées très tôt pendant la phase de conception et de développement, mises à jour au fur et à mesure de l'évolution de la conception ou de la modification des données et que les résultats soient utilisés pour fournir à la direction et aux concepteurs des éléments sur la faisabilité du produit et des dispositions de soutien pour répondre aux exigences de sûreté de fonctionnement. La prévision peut être le seul moyen de vérification ou de validation des exigences de sûreté de fonctionnement dans les phases préliminaires de conception et il convient de l'utiliser également pour toute analyse de compromis.

La prévision correspond à la construction d'un modèle en deux étapes:

– modélisation de structure, c'est-à-dire établissement des modèles logiques représentant les relations entre les éléments, les états ou les actions;

– modélisation mathématique, c'est-à-dire application de modèles mathématiques et de formules pour représenter les modèles de structure. Des données pour les éléments des modèles logiques sont alors introduites dans les modèles mathématiques pour obtenir des résultats au moyen de calculs.

Fault tree analysis (FTA) is a structured approach to identification of the causes (internal or external) that, alone or in combination, lead to a defined state for the product (fault, unsafe condition, etc.). FTAs should be used as an analytical tool to identify the causes of fault modes and to clarify the root cause of identified fault modes.

For more detailed information see IEC 1025.

6.6.3 *Stress and load analysis*

Hardware items should be subjected to a stress analysis, software items to a load analysis.

Products and parts of products may be more prone to failure at higher stress.

Derating of components should be in accordance with an agreed policy except in special documented cases.

The results of stress and load analyses should be used as input to design and development activities.

6.6.4 *Human factors analysis*

Interfaces between the product (including its operations and maintenance documentation) and its operation and maintenance personnel should be analyzed to identify the potential for, and the effects of, human errors in terms of product fault modes. Particular attention should be given to the following:

– the analysis of the product to ensure that the human interface, and related human tasks, are identified;

– the evaluation of potential human mistakes at the interface and their causes and consequences;

– the initiation of product and/or procedure modifications to reduce the possibility of mistakes and their consequences.

6.6.5 *Predictions*

Predictions should be used early during the design and development phase, and updated as the design progresses or data are changed and the results used to provide management and designers with feedback on the feasibility of the product and the support provisions to comply with the dependability requirements. Prediction may be the only means of verification of dependability requirements in early design stages and should also be utilized for any trade-off study.

Prediction consists of model building in two steps:

– structure modelling, i.e. establishment of logical models representing relationships between items, states or actions;

– mathematical modelling, i.e. derivation of mathematical models and formulas to represent the structure models. Data for the elements of the logical models are then inserted into the mathematical models to obtain results by means of calculations.

Pour une information plus détaillée, voir la CEI 863.

6.6.6 *Analyses de compromis*

Les analyses de compromis lors de la conception permettent d'atteindre le niveau de sûreté de fonctionnement requis pendant les différentes phases du cycle de vie. Les analyses de compromis dans la phase de concept et de définition et au début de la phase de conception et de développement fournissent des entrées pour la répartition des exigences de sûreté de fonctionnement. Les études réalisées aux dernières étapes permettent d'affiner la répartition et aident à choisir entre différentes solutions de conception et de soutien.

Les compromis spécifiques qu'il convient de considérer incluent:

– la fiabilité par rapport à la maintenabilité;
– la maintenabilité par rapport à la logistique de maintenance;
– la fiabilité par rapport aux caractéristiques du produit;
– les choix de conception de la sûreté de fonctionnement en fonction des coûts de cycle de vie (voir 6.8).

6.6.7 *Analyse des risques*

Il convient que les analyses des risques, basées sur les analyses de conception et les procédures de prévision, soient effectuées pour les produits pour lesquels une défaillance en cours d'exploitation pourrait mettre en danger le personnel ou être la cause de pertes économiques importantes comprenant, par exemple, des dégradations de l'environnement, et qu'elles comprennent:

– la détermination des parties du produit ou des modes de pannes qui sont critiques;
– l'analyse des moyens de détection des pannes pour ces parties du produit ou ces modes de pannes;
– la quantification des risques;
– la détermination des modifications nécessaires pour réduire les risques.

Pour une information plus détaillée, voir la CEI 300-3-9.

6.6.8 *Revues de conception formalisées*

Il convient que les revues de conception formalisées soient faites à des points clés importants avec l'idée de s'assurer que le produit développé sera conforme aux exigences de sûreté de fonctionnement. Les revues de conception devraient couvrir toutes les phases du cycle de vie. Il convient que ces revues soient formelles, indépendantes, qu'elles constituent des évaluations objectives du produit et de ses conditions de soutien prévues, et soient menées par des experts en la matière.

NOTE – Les revues de conception formalisées ne sont pas seulement réalisées à des fins d'évaluation de la sûreté de fonctionnement.

Il convient que l'information utilisée pour les revues de conception englobe:

– la prévision de sûreté de fonctionnement en cours;
– les faiblesses potentielles de conception ou de soutien identifiées;

For more detailed information see IEC 863.

6.6.6 *Trade-off analysis*

Design trade-offs allow the level of dependability required during the various life-cycle phases to be selected. Trade-off studies in the concept and definition phase and in the early design and development phase provide input to allocation of dependability requirements. Studies performed at later stages permit a refinement of allocations and assist in choosing between alternative design and support solutions.

Specific trade-off analyses that should be made include:

- reliability performance versus maintainability performance;
- maintainability performance versus maintenance support performance;
- reliability performance versus product features;
- dependability performance of design alternatives as a function of life-cycle cost (see 6.8).

6.6.7 *Risk analysis*

Risk analyses, based on design analysis and prediction procedures, should be performed for products for which failure in operation could endanger human beings or cause major economic losses, for example environmental losses. The analyses should include:

- identification of product parts or fault modes which are critical;
- analysis of fault detection facilities for these parts or fault modes;
- quantification of risks;
- identification of modifications necessary to reduce the risks.

For more detailed information see IEC 300-3-9.

6.6.8 *Formal design review*

Formal design reviews should be conducted at significant check-points with the purpose of ensuring that the product being developed will meet dependability requirements. Design reviews should cover all phases of the life cycle. The reviews should be formal, independent and objective assessments of the product and its intended support conditions and should be carried out by appropriate experts.

NOTE – Formal design reviews are not only used for dependability evaluation purposes.

The information used for design reviews should include:

- current dependability predictions;
- identified potential design or support weaknesses:

– les analyses de modes de défaillance et de leurs effets, de l'arbre de panne, des charges et des contraintes, des facteurs humains et des compromis;

– le statut des actions de revues précédentes;

– les résultats de vérification et d'essai.

Il convient que les revues de conception soient conduites et soigneusement documentées aux étapes suivantes:

– revue de conception préliminaire;

– revue de conception détaillée;

– revue de conception finale;

– revue de conception de fabrication;

– revue de conception d'installation;

– revue de conception d'utilisation.

Il convient que des experts dans les domaines de la fiabilité, de la maintenabilité et de la logistique de maintenance participent aux activités de revues de conception.

Le fournisseur peut, soit être sollicité, soit être chargé par le client d'accepter la présence du client aux activités de revue de conception du fournisseur.

NOTE – Il convient que le client communique au fournisseur toute information sur les conditions d'exploitation et de logistique de maintenance, demandée pour les analyses de conception du fournisseur.

Pour une information plus détaillée, voir la CEI 1160.

6.7 *Vérification, validation et essai*

6.7.1 *Planification des validations, des vérifications et des essais*

Il convient que le fournisseur établisse et maintienne des procédures pour la vérification, la validation et l'essai des exigences de sûreté de fonctionnement. Les activités d'essai peuvent être adaptées aux programmes d'essais fonctionnels (tels qu'essai d'un sous-ensemble, essai d'intégration, essai système, etc.) appropriés au produit conçu.

Il convient que les essais couvrent la fiabilité et la maintenabilité dans des conditions de pannes simulées. Un essai de maintenabilité devrait comprendre des activités de maintenance manuelles et automatiques concernant le produit essayé. Il convient que les essais de régression soient effectués lors de modifications ou pour des nouvelles versions du produit pour détecter des impacts imprévisibles sur la sûreté de fonctionnement du produit.

Il convient que les plans de vérification, de validation et d'essai, y compris les méthodes et les procédures, soient préparés à partir de la spécification de sûreté de fonctionnement, d'autres entrées et spécifications ainsi que des lignes directrices de l'ingénierie du produit.

NOTES

1 Pour la définition des termes «vérification» et «validation», voir les articles 2.17 et 2.18 de l'ISO 8402.

2 La validation et la vérification de sûreté de fonctionnement peuvent être faites par d'autres moyens que les essais, par exemple la prévision, l'analyse et la revue de conception, la simulation informatique, etc.

– fault mode and effects, fault tree, stress and load, human factors and trade-off analyses;
– status of previous review actions;
– verification and test results.

Design reviews should be conducted and carefully documented at the following stages:

– preliminary design review;
– detailed design review;
– final design review;
– manufacturing design review;
– installation design review;
– use design review.

Experts in the various fields of reliability, maintainability and maintenance support should participate in design review activities.

The supplier may either be requested, or directed, by the customer to have the customer participate in the supplier's design review activities.

NOTE – The customer should communicate to the supplier any information on operations and maintenance support conditions required for the supplier's design analyses.

For more detailed information see IEC 1160.

6.7 *Verification, validation and test*

6.7.1 *Verification, validation and test planning*

The supplier should establish and maintain procedures for verification, validation and testing to verify the achievement of dependability requirements. Test activities should be adapted to the functional test schedules (such as unit test, integration test, system test, etc.) as appropriate to the product being designed.

The tests should cover reliability performance and maintainability performance under simulated fault conditions. A maintainability test should involve manual and automatic maintenance activities, as relevant to the product being tested. Following product modifications or changes, earlier tests should be repeated to detect any unexpected adverse impact on product dependability.

Verification, validation and test plans, including methods, procedures and criteria, should be prepared based on the dependability specification and other input and specifications and the product engineering guidelines.

NOTES

1 For definition of verification and validation see ISO 8402, clause 2.17 and 2.18.

2 Dependability validation and verification may be done by means other than testing, for example prediction, design analysis and review, computer simulation, etc.

Il convient que les activités de vérification, de validation et d'essai soient adaptées aux caractéristiques du produit et aux exigences de sûreté de fonctionnement.

Les essais progressent habituellement par étapes à partir d'un niveau composant vers le produit complètement assemblé, selon les niveaux d'intervention sur le produit. La viabilité des essais de sûreté de fonctionnement à chacun de ces niveaux doit être analysée. Habituellement, il convient que les essais de fiabilité soient considérés à tous les niveaux, tandis que les essais de maintenabilité peuvent n'être utilisés qu'à certains niveaux. Il est recommandé que les essais de logistique de maintenance et de disponibilité soient effectués dans des conditions opérationnelles (réelles ou simulées).

Il convient que les plans d'essai, en plus de la définition de l'entité essayée, des conditions et des méthodes d'essai, définissent aussi le type d'analyse et de compte rendu de panne, ainsi que les techniques d'évaluation statistiques à appliquer.

6.7.2 *Essai de durée de vie*

Les essais de durée de vie peuvent être effectués dès le début, pendant la phase de conception et de développement ou pendant la fabrication, afin d'identifier et de détecter les faiblesses du produit, pour confirmer la durée de vie du produit, et fournir des informations pour les actions correctives et l'organisation de la logistique de maintenance, etc.

6.7.3 *Essai de sûreté de fonctionnement*

Les essais de vérification de fiabilité et de maintenabilité peuvent être effectués séparément ou conjointement pendant les phases postérieures à la phase de conception préliminaire.

Pour une information plus détaillée, voir la CEI 605, la CEI 1070, la CEI 1123 et la CEI 1124.

6.7.4 *Essai de croissance de fiabilité*

Il convient que cette tâche comprenne la planification, la mise en oeuvre et l'évaluation des essais conduits pour les besoins d'amélioration de la fiabilité du produit à travers la détermination, l'analyse et la correction des pannes, ainsi que la vérification de l'efficacité de l'action corrective.

Pour une information plus détaillée, voir la CEI 1014 et la CEI 1164.

6.7.5 *Essai en production*

Il convient que cette tâche comprenne la planification, la mise en oeuvre et l'évaluation des essais destinés à assurer la conformité de la fiabilité des éléments de production à la fiabilité atteinte démontrée dans les essais de qualification de la fiabilité. Il convient que le plan d'essai inclue l'analyse et le compte rendu des données collectées.

Pou une information plus détaillée, voir la CEI 605.

6.7.6 *Essai d'acceptation*

Il convient que l'objectif de cette activité de validation soit de montrer que le produit est conforme aux exigences de sûreté de fonctionnement.

NOTE – Des procédures d'acceptation peuvent être effectuées pas à pas, dans une approche multiétape, en incluant des activités réalisées pendant des phases précédentes.

Verification, validation and test activities should be adapted to product characteristics and to dependability requirements.

Testing usually progresses in steps from a component level to the completely assembled product, according to the product's indenture levels. The viability of dependability testing at each of these levels should be analyzed. Usually, reliability tests should be considered at all levels, while maintainability tests may only be useful at some levels. Maintenance support and availability tests should be performed under (actual or simulated) field conditions.

Test plans should define the test item, test conditions and test method together with the type of fault reporting and analysis, and the statistical evaluation techniques to be applied.

6.7.2 *Life testing*

Life testing should be performed during the design and development phase or during the manufacturing phase in order to detect and identify product weaknesses, to confirm product durability, to provide information for corrective actions and maintenance support planning purposes, etc.

6.7.3 *Dependability testing*

Reliability and maintainability verification test activities (and other dependability test activities as required) may be performed separately or combined during phases subsequent to the early design phase.

For more detailed information see IEC 605, IEC 1070, IEC 1123, and IEC 1124.

6.7.4 *Reliability growth testing*

The task should include planning, implementation and evaluation of tests conducted for the purpose of enhancing product reliability performance through identification, analysis and correction of faults, and the verification of the effectiveness of the corrective action.

For more detailed information see IEC 1014 and IEC 1164.

6.7.5 *Production testing*

This task should include planning, implementation and evaluation of tests aimed at ensuring conformity of the reliability performance of production items with the achieved reliability performance demonstrated in reliability qualification tests. The test plan should include analysis and reporting of the data collected.

For more detailed information see IEC 605.

6.7.6 *Acceptance testing*

The objective of acceptance testing is to show that the product conforms to dependability and other requirements.

NOTE – Acceptance procedures may be performed in steps, in a multistage approach, including activities performed during previous phases.

Pour une information plus détaillée, voir la CEI 410, la CEI 605-1, la CEI 605-7 et l'ISO 2859.

6.7.7 *Déverminage de fiabilité sous contraintes*

Le déverminage de fiabilité sous contraintes est un procédé qui utilise les contraintes d'environnement et/ou d'exploitation comme moyen de détecter les défectuosités (dues, par exemple à un manque de compétences ou à des déficiences de l'inspection de fabrication) en les transformant en défaillances détectables.

Il convient que cette tâche comprenne la planification, la mise en oeuvre et l'évaluation du procédé c'est-à-dire les conditions de déverminage à appliquer (en termes de durée, de type de contrainte, de niveau de contrainte et de nombre de cycles de contrainte), la préparation d'une spécification d'essai, l'évaluation des résultats d'essai et la préparation des rapports d'essai.

Voir la CEI 1163-1.

6.8 *Programme de coût du cycle de vie*

Il est recommandé de mettre en oeuvre une procédure d'analyse du coût de cycle de vie avec des modèles mathématiques qui représentent réellement le produit et ses conditions de soutien et d'effectuer les calculs de coût dans toutes les phases du cycle de vie avant de livrer le produit. Il convient que les résultats des analyses soient utilisés dans le processus de décision pour:

– guider la répartition et le compromis entre les différentes exigences de sûreté de fonctionnement, liées entre elles par des analyses de sensibilité;

– déterminer les facteurs de sûreté de fonctionnement critiques pour le coût de cycle de vie;

– guider dans le choix entre conception et soutien;

– optimiser la sûreté de fonctionnement sous les contraintes de coût de cycle de vie.

– choisir la méthode de mise au rebut du produit, avec les différentes possibilité de coûts et de contraintes.

NOTE - Il convient que le fournisseur sollicite le client afin qu'il fournisse les informations sur les conditions et les caractéristiques de logistique de maintenance qui dépendent de lui et qui sont planifiées pour que le calcul nécessaire du coût de cycle de vie du produit puisse être effectué.

Pour plus d'information, voir la CEI/FDIS 300-3-3.

6.9 *Planification de l'exploitation et de la logistique de maintenance*

6.9.1 *Planification de la logistique de maintenance*

Il convient que la planification de la logistique de maintenance commence dès la phase de concept et de définition, et concerne les différents aspects du dimensionnement des moyens (par exemple: personnel, rechanges, équipements d'essai et de réparation, etc.).

Il convient que la planification soit basée sur les parties correspondantes de la spécification de sûreté de fonctionnement et qu'elle débouche sur:

– la spécification des niveaux d'intervention sur le produit, des niveaux de maintenance et des échelons de maintenance à utiliser. Cette activité peut comprendre l'optimisation de l'approvisionnement des rechanges;

For more detailed information see IEC 410, IEC 605-1, IEC 605-7 and ISO 2859.

6.7.7 *Reliability stress screening*

Reliability stress screening is a process using environmental and/or operational stresses as a means of detecting flaws (due, for example to poor workmanship and deficiencies in manufacturing inspection etc) by precipitating them as detectable failures.

This task should cover the planning, implementation and evaluation of the process and should include definition of screening conditions to be applied (in terms of duration of stress types and stress levels and cycles), preparation of a specification for the trial, evaluation of results and preparation of reports.

For more detailed information see IEC 1163-1.

6.8 *Life-cycle cost programme*

A life-cycle cost analysis procedure, with mathematical models that realistically represent the product and its support conditions, should be implemented and performed in each life-cycle phase prior to product delivery. The results of the analyses should be used in the management decision processes to:

- guide the allocation of, and trade-off between, the various dependability requirements, for example by sensitivity analyses;
- identify factors of dependability critical to the life-cycle cost;
- guide the choice between design and support alternatives;
- optimize dependability characteristics under life-cycle cost constraints;
- select product disposal method and cost alternatives and constraints.

NOTE – The supplier should request the customer to provide information on customer-controlled maintenance support conditions and characteristics that are being planned so that necessary calculation of the life-cycle cost of the product can be performed.

For more detailed information see IEC/FDIS 300-3-3.

6.9 *Operation and maintenance support planning*

6.9.1 *Maintenance support planning*

Maintenance support planning should start in the concept and definition phase and should address the provision of all necessary resources (for example personnel, spare parts and equipment for test and repair).

The planning should be based on the relevant elements of the dependability specification and should result in:

- specification of the product's indenture levels, and the levels of maintenance and lines of maintenance to be used. This activity may include optimization of spares provisioning;

– la spécification des niveaux de qualification du personnel, des outils et des équipements de maintenance. Cette activité peut comprendre l'optimisation de la planification des forces de maintenance;

– la spécification de la période de soutien pour tout ou partie des produits.

NOTES

1 Pour certains produits ou parties d'un produit (par exemple logiciel d'un ordinateur intégré dans un système) la maintenance et les modifications peuvent être effectuées seulement pendant une période de temps limitée au-delà de laquelle un produit modifié (une nouvelle version) sera offert au client.

2 Il convient que le client prévoie des procédures d'installation et de mise en oeuvre, pour la vérification de la conformité du produit vis-à-vis des exigences de sûreté de fonctionnement, en incluant le recueil de données, les procédures d'analyses et la définition des essais de conformité avec les critères d'acceptation, jusqu'au point correspondant à sa participation dans le processus d'installation.

Pour plus de détails, voir la CEI 706.

6.9.2 *Installation*

Il convient que le processus d'installation comprenne des procédures pour l'essai d'acceptation et la vérification des mesures des caractéristiques de sûreté de fonctionnement qui soient possibles dans les conditions (temps, environnement, logistique de maintenance, etc.) valides pour le processus d'installation.

Il convient que les procédures d'essai et de vérification comprennent le recueil des données, l'analyse et les procédures nécessaires pour l'évaluation de la sûreté de fonctionnement.

6.9.3 *Service de soutien*

Il convient que, lors de cette étape, soient planifiées les activités de logistique de maintenance qui fournissent les moyens nécessaires pour la maintenance du produit. Elles peuvent être fournies par le client seul, le fournisseur seul, un tiers ou toute combinaison de ces parties.

6.9.4 *Ingénierie de soutien*

Il convient que cette tâche comprenne les activités techniques entreprises ayant pour objet de résoudre les problèmes et les déficiences de la logistique de maintenance après l'introduction du produit sur le marché. Il convient que de telles activités concernent les domaines du personnel de maintenance, la formation, l'équipement d'essai et de soutien, le soutien en fournitures, la documentation technique et les moyens de maintenance. Il est recommandé que les responsabilités concernant les modifications de la politique de maintenance du produit y soient aussi incluses.

6.9.5 *Approvisionnement des rechanges*

Il convient que cette tâche comprenne l'évaluation du type et du nombre des rechanges nécessaires pour les besoins de la maintenance, corrective et préventive (pour une période de temps donnée ou pour la «durée de vie»), déterminés sous les hypothèses en cours sur la politique de maintenance, (c'est-à-dire les niveaux d'intervention sur le produit, les niveaux et échelons de maintenance).

– specification of personnel skills, maintenance tools and equipment. This activity may include optimization of scheduling of maintenance forces;

– specification of the support period for the whole or parts of the products.

NOTES

1 For some products, parts of the product (for example, embedded software of a computer) may be given maintenance or modification for only a limited period, after which a modified product (a new release) will be offered to the customer.

2 Customers should plan for implementation of installation procedures, for verification of the product's conformity to dependability requirements, including data collection, analysis procedures and definition of conformance testing with acceptance criteria, to an extent corresponding to their participation in the installation process.

For more detailed information see IEC 706.

6.9.2 *Installation*

The installation process should contain procedures for acceptance testing and verification of measures of dependability characteristics that can be tested and verified under the conditions (time, environmental, maintenance support, etc) valid for the installation process.

Testing and verification procedures should contain necessary data collection, analysis and dependability evaluation procedures.

6.9.3 *Support services*

There should be planning activities for maintenance support services that provide resources necessary for the maintenance of the product. They may be provided by the customer, the supplier, a third party or any combination thereof.

6.9.4 *Support engineering*

This task should include engineering activities with the objective of solving maintenance support problems and deficiencies after the introduction of the product in the field. Such activities should address the areas of maintenance personnel, training, test and support equipment, supply support, technical documentation and maintenance facilities. Responsibility for modifications to the maintenance policy established for the product should also be included.

6.9.5 *Spares provisioning*

This task should include assessment of the type and number of spares needed for corrective and preventive maintenance purposes (for a given period or for the "life time"), determined under the prevailing maintenance policy assumption (i.e. indenture levels, maintenance levels and maintenance echelons).

6.10 *Améliorations et modifications*

6.10.1 *Programmes d'amélioration*

Il convient d'établir et de maintenir des procédures pour identifier et réaliser toute amélioration nécessaire de la fiabilité et de la maintenabilité du produit et de sa logistique de maintenance, afin d'assurer la conformité avec les exigences de sûreté de fonctionnement, et que de tels programmes d'amélioration soient basés sur des données adéquates et analysées selon des techniques statistiques appropriées et, en particulier, concernent les parties critiques au sens de la sûreté de fonctionnement du produit.

NOTE – Il convient que les parties critiques au sens de la sûreté de fonctionnement soient identifiées dès la phase de conception initiale par des analyses et des prévisions de sûreté de fonctionnement.

Il convient que les procédures d'analyse et de compte rendu effectif en temps et en heure soient établies et maintenues pendant la phase de conception et de développement complète, et soient étendus à la phase de fabrication et d'installation (si nécessaire) et à la phase d'exploitation et de maintenance.

6.10.2 *Gestion des modifications*

Il convient qu'une procédure formelle pour maîtriser les modifications du produit soit établie et maintenue et concerne les demandes de modification. L'évaluation des conséquences des modifications, la procédure pour approbation et autorisation, la responsabilité pour la mise en oeuvre et la vérification.

La sûreté de fonctionnement d'un produit peut être sévèrement dégradée par une gestion insuffisante des modifications du produit et de sa logistique de maintenance. En règle générale, il convient que toute modification d'un produit ou de son soutien soit soumise au même degré d'assurance de sûreté de fonctionnement que le produit et le soutien originaux. Cela signifie qu'il convient que toutes les dispositions de cette partie de la CEI 300 soient considérées et qu'un programme de sûreté de fonctionnement pour les modifications soit établi, maintenu et régulièrement revu. C'est une particularité importante pour des produits ayant une espérance de vie opérationnelle importante et pour les produits logiciels ayant de fréquentes révisions et mises à jour.

Il convient que le processus de modification soit soutenu par le système de gestion de configuration.

6.11 *Retour d'expérience*

6.11.1 *Acquisition des données*

Il convient que les données sur les pannes détectées ou sur les défaillances intervenant pendant les essais du produit dans la phase de conception et de développement soient analysées du point de vue de leur impact sur la sûreté de fonctionnement et, si nécessaire, que des actions correctives soient entreprises.

Il convient que la procédure d'acquisition de données soit poursuivie avec les informations provenant du produit en exploitation opérationnelle.

6.10 *Improvements and modifications*

6.10.1 *Improvement programmes*

Procedures should be established and maintained for systematic identification and implementation of any necessary improvement of the reliability performance and maintainability performance of the product and of the maintenance support performance, in order to ensure conformity to dependability requirements. Such dependability improvement programmes should be based on relevant data analyzed using appropriate statistical techniques and in particular, should address dependability-critical parts of the product.

NOTE – Dependability-critical parts should be identified in an early part of the design and development phase by dependability analyses and predictions.

Effective and timely fault reporting and analysis procedures should be established and maintained during the entire design and development phase, and continued into the manufacturing and installation phase (as necessary) and into the operations and maintenance phase.

6.10.2 *Modification control*

A formal procedure for controlling modifications to the product should be established and maintained. It should include arrangements for addressing change requests, evaluating the consequences of changes, approving and authorizing modifications and allocating responsibility for implementation and verification.

The dependability of a product can be severely degraded by insufficient control of field modifications of the product and its maintenance support. As a general rule, any modification of a product or its support should be subjected to the same degree of dependability verification as the original product and support. This means that all the provisions of this part of IEC 300 should be considered and a dependability programme for modification established, maintained and regularly reviewed. This is particularly important for products with a long expected operational life and for software products with frequent updates and revisions.

The modification process should be supported by the configuration management system.

6.11 *Experiences feedback*

6.11.1 *Data acquisition*

Data on faults detected, or failures occurring, during testing of the product within the design and development phase should be analyzed to determine the effect on dependability. Corrective actions should be initiated as necessary.

This process of data acquisition should continue with data from products in field operation.

A partir de la période d'installation, il convient que les données du produit en exploitation soient recueillies sur tous les aspects de la sûreté de fonctionnement qui ont un rapport avec le produit et la spécification de sûreté de fonctionnement, c'est-à-dire les données nécessaires pour les estimations de:

– la fiabilité: l'information sur l'apparition des défaillances et des effets des pannes s'y rapportant;

– la maintenabilité: à chaque défaillance, l'information sur les temps déterminant la maintenabilité, y compris le temps de non-détection de la panne et le temps de réparation (et si nécessaire des éléments de ces temps), les temps de maintenance préventive. Les éléments du temps de maintenance corrective active seront également notés;

– la disponibilité: le temps d'indisponibilité lié à chaque panne significatif pour les mesures de disponibilité selon la spécification de sûreté de fonctionnement;

– la logistique de maintenance: les délais administratifs et logistiques en rapport avec les mesures de logistique de maintenance de la spécification de sûreté de fonctionnement;

– le coût de maintenance.

De plus, il convient de recueillir les données sur l'environnement et les conditions d'utilisation, sur la configuration du produit, etc., qui sont nécessaires pour les analyses statistiques et techniques s'y rapportant.

Il convient que des procédures et des outils efficaces pour le recueil de données, leur transfert et leur stockage soient établies et maintenues. Il convient de ne procéder à une réduction de données qu'après avoir pris en considération les besoins des analyses statistiques et techniques s'y rapportant.

Pour une information plus détaillée, voir la CEI 300-3-2.

NOTES

1 Il convient que le client établisse et maintienne des procédures pour le recueil, le stockage et l'analyse des données requises pour l'évaluation de la sûreté de fonctionnement opérationnelle et pour la communication de cette information au fournisseur.

2 Il convient que les données de panne, de défaillance et celles sur la configuration du produit et les conditions d'exploitation et de maintenance soient organisées de façon appropriée pour l'évaluation de la conformité aux exigences de sûreté de fonctionnement, et qu'elles soient adaptées au recueil des données du fournisseur et aux procédures d'évaluation.

6.11.2 *Analyse des données*

Il convient que les données sur les défaillances, les pannes et les actions de maintenance provenant d'origines diverses soient utilisées pour:

a) les analyses techniques afin de déterminer les causes des défaillances et des pannes et de proposer des modifications sur le produit ou ses critères d'exploitation et son soutien, et

b) les analyses statistiques.

Les analyses techniques et statistiques doivent se compléter mutuellement.

With effect from the installation period, field data should be collected on all aspects of dependability, as relevant to the product and the dependability specification. This will include data needed for estimations of:

– reliability performance: this should include information on the occurrence of failures and related fault effects;

– maintainability performance: this will include, for each failure, the information needed to measure maintainability, including, undetected fault time and repair time (and, as necessary, elements of those times) when preventive maintenance is performed; the elements of any necessary active corrective maintenance time should also be recorded;

– availability performance: this should include the down time connected with each fault that is significant to the measures of availability performance defined in the dependability specification;

– maintenance support performance: this should include administrative delays and logistic delays relevant to the measures of maintenance support performance stated in the dependability specification;

– maintenance cost.

In addition, data on environmental and other conditions of use, and on product configuration, etc., needed for the subsequent technical and statistical analyses, should be collected.

Efficient procedures and tools for data collection, transfer and storage should be established and maintained. Data reduction should be done only after consideration of the needs of the subsequent technical and statistical analyses.

For more detailed information see IEC 300-3-2.

NOTES

1 The customer should establish and maintain procedures for collection, storage and analysis of data required for evaluation of the operational dependability and for communication of that information to the supplier.

2 Fault and failure information and data on product configuration and operation and maintenance conditions should be organized in a manner appropriate for evaluation of conformity to dependability requirements, as well as suitably adapted to the supplier's data collection and evaluation procedures.

6.11.2 *Data analysis*

Data on failures, faults and maintenance actions derived from all relevant sources should be used for:

a) technical analyses, to determine the causes of failures and faults and to propose modifications to the product or its operating criteria and to its support;

b) statistical analyses.

The technical and statistical analyses should complement and complete each other.

Il convient que les analyses techniques comprennent toute expertise technique nécessaire provenant de la conception, de la fabrication, de la logistique de maintenance et de l'assurance qualité avec l'objectif d'améliorer la conception, le procédé de fabrication, les conditions d'utilisation et les dispositions du soutien logistique de maintenance, comme il convient.

Il convient que les analyses statistiques, concernent:

– la validation des exigences pour les mesures telles qu'elles sont définies dans la spécification de sûreté de fonctionnement (et non validées par ailleurs);

– l'estimation des mesures de la spécification de sûreté de fonctionnement, aussi bien que les mesures de sûreté de fonctionnement utilisées pour d'autres sujets, par exemple recueil de données composant pour une banque de données;

– l'évaluation des propriétés statistiques des processus de défaillance et de maintenance étudiés;

– tout changement des caractéristiques de sûreté de fonctionnement;

– l'évaluation de l'importance relative des déviations entre les exigences de sûreté de fonctionnement et la valeur relative des améliorations sur le produit ou sur son soutien.

Il convient que toutes les déficiences rencontrées dans les données entraînent une amélioration du processus de recueil de données.

NOTES

1 Afin d'être réalisées effectivement et en temps et en heure, ces activités peuvent nécessiter des moyens de gestion, par exemple un tableau de bord des revues de panne.

2 Il convient que le client établisse et maintienne des procédures pour le stockage et l'analyse des informations de sûreté de fonctionnement opérationnelle. Les activités d'analyse des données devraient être soutenues par une prise en compte et des outils d'analyse statistiques efficaces. Il convient que les données et les outils soient facilement accessibles au personnel qui doit réaliser les analyses.