NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60300-2

Deuxième édition
Second edition
2004-03

Gestion de la sûreté de fonctionnement –

Partie 2:
Lignes directrices pour la gestion de la sûreté de fonctionnement

Dependability management –

Part 2:
Guidelines for dependability management

Numéro de référence
Reference number
CEI/IEC 60300-2:2004

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Informations supplémentaires sur les publications de la CEI

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 cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- **Site web de la CEI (www.iec.ch)**
- **Catalogue des publications de la CEI**

  Le catalogue en ligne sur le site web de la CEI (http://www.iec.ch/searchpub/cur_fut.htm) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.
- **IEC Just Published**

  Ce résumé des dernières publications parues (http://www.iec.ch/online_news/justpub/jp_entry.htm) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.
- **Service clients**

  Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

  Email: custserv@iec.ch
  Tél: +41 22 919 02 11
  Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

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 this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**
- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (http://www.iec.ch/searchpub/cur_fut.htm) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.
- **IEC Just Published**

  This summary of recently issued publications (http://www.iec.ch/online_news/justpub/jp_entry.htm) is also available by email. Please contact the Customer Service Centre (see below) for further information.
- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60300-2

Deuxième édition
Second edition
2004-03

Gestion de la sûreté de fonctionnement –

Partie 2:
Lignes directrices pour la gestion de la sûreté de fonctionnement

Dependability management –

Part 2:
Guidelines for dependability management

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE XA

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

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 2: Lignes directrices pour la gestion de la 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, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente, les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 60300-2 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Cette deuxième édition annule et remplace la première édition parue en 1995 ainsi que la CEI 60300-3-6 (1997). Cette édition constitue une révision technique.

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

a) alignement structurel et terminologique avec l'ISO;
b) mise au point des processus des systèmes;
c) mise à disposition de lignes directrices additionnelles dans les annexes afin de faciliter les applications.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

Part 2: Guidelines for dependability management

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60300-2 has been prepared by IEC technical committee 56: Dependability.

This second edition cancels and replaces the first edition, published in 1995, as well as IEC 60300-3-6 (1997). This edition constitutes a technical revision.

This edition includes the following significant technical changes with regard to the previous edition:

a) structural and terminological alignment with ISO;
b) focus on system processes;
c) provision of additional guidelines in annexes to facilitate applications.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/913/FDIS	56/934/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 présente publication a été rédigée conformément aux Directives de l'ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2010. A cette date, la publication sera

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

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

FDIS	Report on voting
56/913/FDIS	56/934/RVD

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

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

The committee has decided that the contents of this publication will remain unchanged until 2010. At this date, the publication will be

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

INTRODUCTION

La sûreté de fonctionnement traite des performances de disponibilité d'un produit. Les facteurs qui ont une incidence sur l'aptitude de disponibilité sont l'aptitude de fiabilité, de maintenabilité et de soutien logistique à la maintenance. La sûreté de fonctionnement est une discipline technique qu'il convient de gérer correctement pour atteindre ses objectifs et en tirer les profits escomptés. La gestion de la sûreté de fonctionnement suppose une écoute du client clairement définie et que cette dernière soit intégrée dans le système de management d'ensemble de l'organisme afin de coordonner les activités de sûreté de fonctionnement et d'en rentabiliser les résultats.

La présente partie de la CEI 60300 fournit des lignes directrices sur la gestion de la sûreté de fonctionnement. Elle vient à l'appui de la norme CEI 60300-1 de niveau supérieur définissant le système de gestion de la sûreté de fonctionnement, en identifiant et en référençant les processus et méthodes pertinents pour une large gamme de produits. La présente norme associe les différentes étapes du processus de management aux normes de sûreté de fonctionnement applicables afin de promouvoir l'amélioration continue.

Le concept de cycle de vie d'un produit est introduit de manière à traiter de l'importance des activités de sûreté de fonctionnement et de leur planification afin d'en assurer une mise en œuvre efficace. Les phases du cycle de vie d'un produit, d'une part, et les éléments et tâches applicables du programme de sûreté de fonctionnement, d'autre part, sont associés de manière à faciliter l'ajustement des programmes de sûreté de fonctionnement aux besoins de projets spécifiques.

La présente norme présente le processus générique des applications de sûreté de fonctionnement en se fondant sur des pratiques appliquées avec succès dans le domaine industriel. Elle peut être tout autant intégrée aux systèmes de management de grandes sociétés qu'adaptée aux petites entreprises.

Elle aborde également les caractéristiques à dépendance chronologique des performances de fiabilité, de maintenabilité et de soutien logistique à la maintenance du produit.

La présente norme fait référence à d'autres normes publiées par le TC 56 ainsi qu'à plusieurs normes ISO/CEI et à quelques normes traitant de la fiabilité dans des secteurs spécifiques. Ces références sont énumérées dans la bibliographie.

L'Annexe A fournit une description concise des éléments et tâches à appliquer dans le cadre d'un programme de sûreté de fonctionnement.

L'Annexe B définit les phases du cycle de vie d'un produit.

L'Annexe C présente une association entre les phases du cycle de vie d'un produit, d'une part, et les éléments et tâches applicables de sûreté de fonctionnement, d'autre part.

L'Annexe D présente les étapes et les normes du processus de gestion de la sûreté de fonctionnement.

L'Annexe E donne une liste de questions facilitant la revue de gestion de la sûreté de fonctionnement.

L'Annexe F fournit des lignes directrices pour le processus d'ajustement.

L'Annexe G présente la classification des normes de sûreté de fonctionnement en fonction des phases du cycle de vie.

INTRODUCTION

Dependability deals with the availability performance of a product. The factors influencing availability performance are reliability, maintainability and maintenance support performance. Dependability is a technical discipline that needs to be managed in order to achieve its objectives and benefits. Dependability management should provide a clear customer focus. It should be incorporated into an organization's overall management system to coordinate dependability activities for cost-effective results.

This part of IEC 60300 provides guidelines on dependability management. It supports the top-level dependability management system standard IEC 60300-1 by identifying and referencing relevant processes and methods for a broad range of products. This standard links the management process steps with applicable dependability standards to foster continual improvement.

The concept of product life cycle is introduced to deal with the significance of dependability activities and timing for their effective implementation. The association of product life cycle phases with the applicable dependability programme elements and tasks are presented to facilitate tailoring of dependability programmes to meet specific project needs.

This standard outlines the generic process for dependability applications based on successfully applied industry practices. It can be incorporated into the management systems of large corporations as well as being adaptable to small businesses.

Time-dependent reliability, maintainability and maintenance support performance characteristics in products are addressed.

This standard references other published TC 56 standards and also makes reference to several ISO/IEC standards as well as some sector specific reliability standards. These references are listed in the bibliography.

Annex A provides a summary description of the elements and tasks of a dependability programme for application.

Annex B defines the product life cycle phases.

Annex C presents an association of product life cycle phases with the applicable dependability elements and tasks.

Annex D presents process steps and standards for managing dependability.

Annex E provides a list of questions to facilitate dependability management review.

Annex F provides guidelines for the tailoring process.

Annex G presents the classification of dependability standards with the life cycle phases.

GESTION DE LA SÛRETE DE FONCTIONNEMENT –

Partie 2: Lignes directrices pour la gestion de la sûreté de fonctionnement

1 Domaine d'application

La présente partie de la CEI 60300 fournit les lignes directrices pour la gestion de la sûreté de fonctionnement en matière de conception, de développement, d'évaluation du produit et d'amélioration du processus. Des modèles de cycle de vie sont utilisés pour décrire les phases de développement du produit ou du projet. Un processus d'ajustement est recommandé pour le choix de tâches pertinentes du programme de sûreté de fonctionnement en vue d'une mise en œuvre planifiée dans le temps, permettant de répondre aux besoins divers d'utilisateurs variés.

La présente partie de la CEI 60300 s'applique à une planification et une mise en œuvre détaillées d'un programme de sûreté de fonctionnement destiné à répondre à des besoins spécifiques du produit. Le processus d'ajustement fournit une méthode de sélection des éléments d'un programme de sûreté de fonctionnement et des processus correspondants, du point de vue du produit ou du projet. Cette norme est applicable à tous les organismes, au cours de toutes les phases du cycle de vie et dans n'importe quelle situation contractuelle, quels que soient le type, la taille et le produit fourni.

2 Références normatives

Les documents de référence énumérés ci-après sont indispensables à l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document auquel il est fait référence (y compris ses éventuels amendements) s'applique.

CEI 60300-3-1, *Gestion de la sûreté de fonctionnement – Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique* (disponible en anglais seulement)

CEI 61014, *Programmes de croissance de fiabilité*

ISO/CEI 15026, *Technologies de l'information – Niveaux d'intégrité du système et du logiciel* (disponible en anglais seulement)

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivantes s'appliquent.

NOTE 1 Certains termes et définitions proviennent de la CEI 60050(191) et de la CEI 60300-1.

NOTE 2 L'ISO 9000 est utilisée comme référence pour le vocabulaire de la qualité.

3.1
sûreté de fonctionnement
ensemble des propriétés qui décrivent la disponibilité et les facteurs qui la conditionnent: fiabilité, maintenabilité et logistique de maintenance

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

[CEI 60050, 191-02-03]

DEPENDABILITY MANAGEMENT –

Part 2: Guidelines for dependability management

1 Scope

This part of IEC 60300 provides guidelines for dependability management of product design, development, evaluation and process enhancements. Life cycle models are used to describe product development or project phases. A tailoring process is recommended for the selection of relevant dependability programme tasks for time-phased implementation to meet varied user needs.

This part of IEC 60300 is applicable for detailed planning and implementation of a dependability programme to meet specific product needs. The tailoring process provides a method for selection of dependability programme elements and associated processes from a product or project perspective. This standard is applicable to all organizations, during all life-cycle phases and in any contract situation, regardless of type, size and product provided.

2 Normative references

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

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

IEC 61014, *Programmes for reliability growth*

ISO/IEC 15026, *Information technology – System and software integrity levels*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE 1 Certain terms and definitions are taken from IEC 60050(191) and IEC 60300-1.

NOTE 2 ISO 9000 is used as a reference to quality vocabulary.

3.1
dependability
collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance

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

[IEC 60050, 191-02-03]

3.2
gestion de la sûreté de fonctionnement
activités coordonnées destinées à orienter et gérer un organisme en matière de sûreté de fonctionnement

NOTE La gestion de la sûreté de fonctionnement fait partie du système de management d'ensemble d'un organisme.

[CEI 60300-1, définition 3.2]

3.3
système de gestion de la sûreté de fonctionnement
système de gestion destiné à orienter et maîtriser un organisme en matière de sûreté de fonctionnement

NOTE 1 Le système de gestion de la sûreté de fonctionnement d'un organisme fait partie de son système de management d'ensemble.

NOTE 2 La structure, les responsabilités, les procédures, les processus et les ressources de l'organisme utilisés pour la gestion de la sûreté de fonctionnement sont fréquemment désignés par l'expression «programme de sûreté de fonctionnement».

[CEI 60300-1, définition 3.3]

3.4
plan de sûreté de fonctionnement
document énonçant les pratiques, les ressources et les séquences d'activités particulières liées à la sûreté de fonctionnement, spécifiques à un produit, projet ou contrat particulier

[CEI 60300-1, définition 3.4]

3.5
élément du programme de sûreté de fonctionnement
ensemble de tâches du programme de sûreté de fonctionnement appartenant au domaine d'un sujet spécifique

3.6
tâche du programme de sûreté de fonctionnement
ensemble d'activités concernant les aspects spécifiques de sûreté de fonctionnement d'un produit

3.7
produit
résultat d'un processus

NOTE 1 Il existe quatre catégories génériques de produits:

– les services (par exemple, transport);

– les «software» logiciels (par exemple logiciel, dictionnaire);

– les (produits) matériels (par exemple, pièces mécaniques de moteur);

– les produits issus de processus à caractère continu (par exemple, lubrifiant).

De nombreux produits sont constitués d'éléments appartenant à différentes catégories génériques de produits. Le produit est appelé service, logiciel, matériel ou produit issu de processus à caractère continu selon l'élément dominant. Par exemple, l'offre produit «automobile» se compose de matériel (par exemple les pneus), de produits issus de processus à caractère continu (par exemple carburant, liquide de refroidissement), de «software» (par exemple logiciel de commande de moteur, manuel d'utilisation) et de services (par exemple explications du vendeur concernant le fonctionnement).

NOTE 2 Un service est le résultat d'au moins une activité nécessairement réalisée à l'interface entre le fournisseur et le client et est généralement immatériel. La prestation d'un service peut impliquer par exemple:

– une activité réalisée sur un produit tangible fourni par le client (par exemple, réparation d'une voiture);

– une activité réalisée sur un produit immatériel (par exemple, une déclaration de revenus nécessaire pour déclencher l'impôt);

– la fourniture d'un produit immatériel (par exemple, fourniture d'informations dans le contexte de la transmission de connaissances);

– la création d'une ambiance pour le client (par exemple, dans les hôtels et les restaurants).

3.2
dependability management
coordinated activities to direct and control an organization with regard to dependability

NOTE Dependability management is part of an organization's overall management.

[IEC 60300-1, definition 3.2]

3.3
dependability management system
management system to direct and control an organization with regard to dependability

NOTE 1 The dependability management system of an organization is part of its overall management system.

NOTE 2 The organizational structure, responsibilities, procedures, processes and resources used for managing dependability are often referred to as a dependability programme.

[IEC 60300-1, definition 3.3]

3.4
dependability plan
document setting out the specific dependability practices, resources and sequences of activities relevant to a particular product, contract or project

[IEC 60300-1, definition 3.4]

3.5
dependability programme element
set of dependability programme tasks, pertaining to a specific subject area

3.6
dependability programme task
set of activities addressing specific dependability aspects of a product

3.7
product
result of a process

NOTE 1 There are four generic product categories, as follows:

– services (e.g. transport);
– software (e.g. computer program, dictionary);
– hardware (e.g. engine mechanical part);
– processed materials (e.g. lubricant).

Many products comprise elements belonging to different generic product categories. Whether the product is then called service, software, hardware or processed material depends on the dominant element. For example, the offered product "automobile" consists of hardware (e.g. tyres), processed materials (e.g. fuel, cooling liquid), software (e.g. engine control software, driver's manual), and service (e.g. operating explanations given by the salesman).

NOTE 2 Service is the result of at least one activity necessarily performed at the interface between the supplier and customer and is generally intangible. Provision of a service can involve, for example, the following:

– an activity performed on a customer-supplied tangible product (e.g. automobile to be repaired);
– an activity performed on a customer-supplied intangible product (e.g. the income statement needed to prepare a tax return);
– the delivery of an intangible product (e.g. the delivery of information in the context of knowledge transmission);
– the creation of ambience for the customer (e.g. in hotels and restaurants).

Un «software» se compose d'informations, est généralement immatériel et peut se présenter sous forme de démarches, de transactions ou de procédures.

Un produit matériel est généralement tangible et son volume constitue une caractéristique dénombrable. Les produits issus de processus à caractère continu sont généralement tangibles et leur volume constitue une caractéristique continue. Les produits matériels et issus de processus à caractère continu sont souvent appelés biens.

NOTE 3 L'assurance de la qualité porte principalement sur le produit intentionnel.

[ISO 9000, définition 3.4.2]

NOTE 4 Dans le contexte de la sûreté de fonctionnement, un produit peut être simple (par exemple, un dispositif ou un algorithme logiciel) ou complexe (par exemple, un système ou un réseau intégré comprenant des produits matériels et logiciels, des facteurs humains ainsi que des installations et activités de soutien).

[CEI 60300-1, définition 3.5]

3.8
système
ensemble d'éléments corrélés ou interactifs

[ISO 9000, définition 3.2.1]

NOTE 1 Dans le contexte de la sûreté de fonctionnement, un système disposera

a) d'un objet défini exprimé en termes de fonctions prévues,

b) de conditions spécifiées de fonctionnement/utilisation,

c) de limites définies.

NOTE 2 Il est admis que la structure d'un système soit hiérarchique.

[CEI 60300-1, définition 3.6]

3.9
fiabilité (aptitude)
aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné

[CEI 60050, 191-02-06, modifiée]

3.10
maintenabilité (aptitude)
dans des conditions données d'utilisation, aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données, avec des procédures et des moyens prescrits

[CEI 60050, 191-02-07, modifiée]

3.11
logistique de maintenance
aptitude d'un organisme de maintenance à fournir sur demande, dans des conditions données, les moyens nécessaires à la maintenance d'une entité, conformément à une politique de maintenance donnée

[CEI 60050, 191-02-08, modifiée]

3.12
niveau d'intégrité
délimitation d'une plage de valeurs pour une propriété d'entité donnée, nécessaire au maintien des risques d'un système donné dans des limites acceptables

NOTE Pour des entités qui réalisent des fonctions de réduction des risques, la propriété est la fiabilité avec laquelle l'entité accomplit cette fonction de réduction des risques. Pour des entités dont la défaillance peut donner lieu à une menace, la propriété est la limite de fréquence des défaillances.

[ISO/CEI 15026, définition 3.9 modifiée]

Software consists of information and is generally intangible and can be in the form of approaches, transactions or procedures.

Hardware is generally tangible and its amount is a countable characteristic. Processed materials are generally tangible and their amount is a continuous characteristic. Hardware and processed materials often are referred to as goods.

NOTE 3 Quality assurance is mainly focussed on intended product.

[ISO 9000, definition 3.4.2]

NOTE 4 In the context of dependability, a product may be simple (e.g. a device, a software algorithm) or complex (e.g. a system or an integrated network comprising hardware, software and human elements and support facilities and activities).

[IEC 60300-1, definition 3.5]

3.8
system
set of interrelated or interacting elements

[ISO 9000, definition 3.2.1]

NOTE 1 In the context of dependability, a system will have

a) a defined purpose expressed in terms of intended functions,

b) stated conditions of operation/use,

c) defined boundaries.

NOTE 2 The structure of a system may be hierarchical.

[IEC 60300-1, definition 3.6]

3.9
reliability (performance)
ability of an item to perform a required function under given conditions for a given time interval

[IEC 60050, 191-02-06, modified]

3.10
maintainability (performance)
ability of an item under given conditions of use, to be retained in, or restored to, a state in which it can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources

[IEC 60050, 191-02-07, modified]

3.11
maintenance support performance
ability of a maintenance organization, under given conditions, to provide upon demand, the resources required to maintain an item, under a given maintenance policy

[IEC 60050, 191-02-08, modified]

3.12
integrity level
denotation of a range of values of a property of an item necessary to maintain system risks within tolerable limits

NOTE For items that perform mitigating functions, the property is the reliability with which the item has to perform the mitigating function. For items whose failure can lead to a threat, the property is the limit on the frequency of the failure.

[ISO/IEC 15026, definition 3.9 modified]

3.13
entité
dispositif
individu
tout élément, composant, sous-système, unité fonctionnelle, équipement ou système que l'on peut considérer individuellement

NOTE Une entité peut être constituée de matériel, de logiciel ou des deux à la fois, et peut aussi dans certains cas comprendre le personnel.

[CEI 60050, 191-01-01, modifiée]

3.14
processus
ensemble d'activités liées utilisant des ressources qui transforme des éléments d'entrée en éléments de sortie

NOTE 1 Les éléments d'entrée d'un processus sont généralement les éléments de sortie d'autres processus.

NOTE 2 Les processus d'un organisme sont généralement planifiés et mis en œuvre dans des conditions maîtrisées afin d'apporter une valeur ajoutée.

NOTE 3 Lorsque la conformité du produit résultant ne peut être immédiatement ou économiquement vérifiée, le processus est souvent appelé « procédé spécial ».

[ISO 9000, définition 3.4.1, modifiée]

3.15
chaîne d'approvisionnement
ensemble coordonné de processus de management liant les activités du fournisseur, de l'organisme et du client pour atteindre un objectif commun

3.16
management
activités coordonnées pour orienter et contrôler un organisme

NOTE En français, il ne convient pas d'utiliser le terme «management» pour désigner des personnes, c'est-à-dire «personne ou groupe de personnes ayant les responsabilités et les pouvoirs nécessaires pour la conduite et la maîtrise d'un organisme». Il est préférable d'utiliser l'expression «l'encadrement doit...» ou «la direction doit...», plutôt que l'expression «le management doit...».

[ISO 9000, définition 3.2.6]

3.17
direction au plus haut niveau
personne ou groupe de personnes qui oriente et gère un organisme au plus haut niveau

[ISO 9000, définition 3.2.7, modifiée]

3.18
revue
examen entrepris pour déterminer la pertinence, l'adéquation et l'efficacité de ce qui est examiné à atteindre des objectifs établis

NOTE La revue peut également inclure la détermination de l'efficience.

EXEMPLE Revue de direction, revue de conception et développement, revue des exigences du client et revue de non-conformité.

[ISO 9000, définition 3.8.7]

3.19
cycle de vie
intervalle de temps entre la conception d'un produit et sa mise au rebut

[CEI 60300-3-3, définition 3.1]

3.13
item
entity
any part, component, device, subsystem, functional unit, equipment or system that can be individually considered

NOTE An item may consist of hardware, software or both, and may also in particular cases, include people.

[IEC 60050, 191-01-01, modified]

3.14
process
set of interrelated activities utilizing resources to transform inputs into outputs

NOTE 1 Inputs to a process are generally outputs of other processes.

NOTE 2 Processes in an organization are generally planned and carried out under controlled conditions to add value.

NOTE 3 A process where the conformity of the resulting product cannot be readily or economically verified is frequently referred to as a "special process".

[ISO 9000, definition 3.4.1, modified]

3.15
supply-chain
coordinated set of management processes linking the activities of the supplier, the organization and the customer to meet a common objective

3.16
management
coordinated activities to direct and control an organization

NOTE In English, the term "management" sometimes refers to people, i.e. a person or group of people with authority and responsibility for the conduct and control of an organization. When "management" is used in this sense it should always be used with some form of qualifier to avoid confusion with the concept "management" defined above. For example, "management shall..." is deprecated whereas "top management shall..." is acceptable.

[ISO 9000, definition 3.2.6]

3.17
top management
person or group of people who directs and controls an organization at the highest level

[ISO 9000, definition 3.2.7]

3.18
review
activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

NOTE Review can also include the determination of efficiency.

EXAMPLE Management review, design and development review, review of customer requirements and nonconformity review.

[ISO 9000, definition 3.8.7]

3.19
life cycle
time interval between a product's conception and its disposal

[IEC 60300-3-3, definition 3.1]

4 Système de gestion de la sûreté de fonctionnement

Le système de gestion de la sûreté de fonctionnement fait partie intégrante du système de management d'ensemble d'un organisme. Il fournit un cadre organisationnel permettant de diriger stratégiquement la politique de sûreté de fonctionnement, de maîtriser les fonctions de sûreté de fonctionnement et de coordonner toutes les activités de sûreté de fonctionnement. Il faut dès que possible porter une attention toute particulière aux plans de sûreté de fonctionnement et à l'affectation des ressources appropriées pour ajuster au mieux les efforts nécessaires à la réalisation des objectifs de sûreté de fonctionnement souhaités. Pour assurer la sûreté de fonctionnement d'un produit, il est essentiel que la fiabilité et la maintenabilité soient conçues en tant que partie intégrante du produit et que leur acceptabilité soit vérifiée à divers stades du processus de réalisation du produit. Un effort de soutien logistique à la maintenance approprié est nécessaire pour soutenir la sûreté de fonctionnement dans des applications produits pour lesquelles la technologie disponible ne permet pas d'avoir des cycles de vie exempts de défaillances.

Il convient que le système de gestion de la sûreté de fonctionnement prévoie une structure de cycle de vie du produit pour la mise en œuvre de programmes de sûreté de fonctionnement adéquats (voir 3.3, Note 2) et ainsi répondre aux objectifs commerciaux de l'organisme, y compris la satisfaction du client. Le cycle de vie du produit constitue un processus de bout en bout; depuis la conception initiale du produit, en passant par la phase de développement et de fonctionnement, jusqu'à la fin de la vie et la mise hors service du produit. Le processus du cycle de vie fournit un cadre qui permet de regrouper les éléments et tâches du programme de sûreté de fonctionnement correspondant.

Les différentes étapes du processus de gestion de la sûreté de fonctionnement sont présentées au niveau supérieur définissant le système de gestion de la sûreté de fonctionnement dans la CEI 60300-1. Ces étapes sont les suivantes:

– la définition des objectifs de la sûreté de fonctionnement;
– l'analyse de la portée des tâches de sûreté de fonctionnement requises et de leurs implications;
– la planification de la stratégie et des activités permettant d'atteindre les objectifs de la sûreté de fonctionnement;
– la mise en œuvre des tâches de sûreté de fonctionnement sélectionnées;
– l'analyse des résultats des tâches de sûreté de fonctionnement mises en œuvre;
– l'évaluation de résultats de sûreté de fonctionnement obtenus pour une amélioration ultérieure.

La Figure 1 illustre un organigramme-type du processus correspondant. L'Annexe D présente les normes de sûreté de fonctionnement applicables associées à chaque étape du processus.

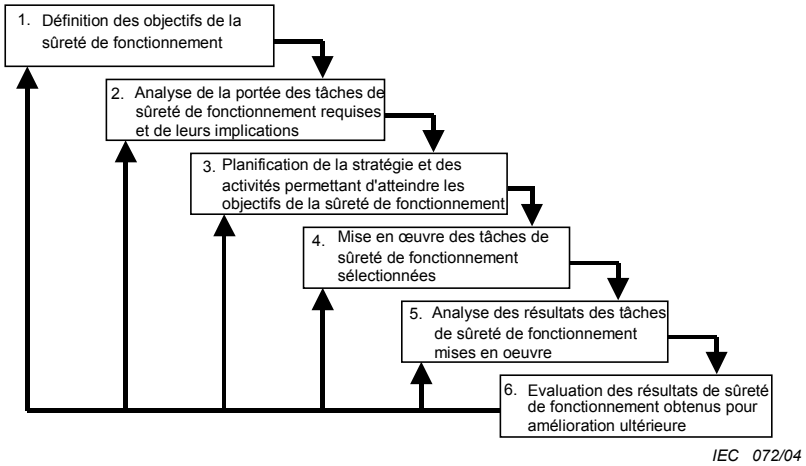


Figure 1 – Etapes du processus de gestion de la sûreté de fonctionnement

4 Dependability management system

The dependability management system is part of the overall management system of an organization. It provides an organizational framework for strategic direction of dependability policy, control of dependability functions and coordination of all dependability activities. Early attention to dependability plans and allocation of appropriate resources is needed for tailoring of effort to achieve the desired dependability objectives. To ensure dependability of a product, it is essential that reliability and maintainability are designed into the product and verified for their acceptance at various stages of the product realization process. Appropriate maintenance support effort is needed to sustain dependability in product applications, where available technology does not allow failure-free life cycles.

The dependability management system should provide a product life cycle framework for implementation of appropriate dependability programmes (see 3.3, Note 2) to meet the organization's business objectives, including customer satisfaction. The product life cycle reflects an end-to-end process; from product inception through development and operation to its end-of-life or withdrawal from use. The life cycle process provides a useful framework to group related dependability programme elements and tasks.

The process steps for managing dependability are presented in the top-level dependability management standard IEC 60300-1. They include:

– defining dependability objectives;
– analysis of the scope of dependability work needed and implications;
– planning strategy and activities to achieve dependability objectives;
– implementation of selected dependability tasks;
– analysis of results of dependability tasks implemented;
– evaluation of achieved dependability results for further improvement.

A typical process flow diagram is shown in Figure 1. The applicable dependability standards associated with each process step are presented in Annex D.

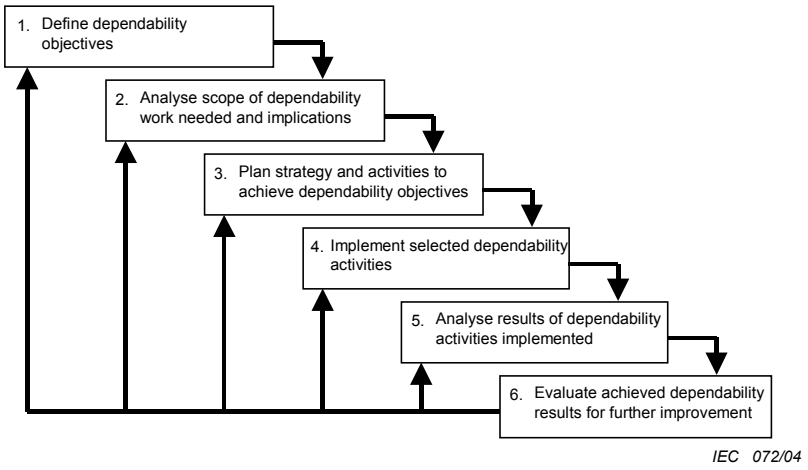


Figure 1 – Process steps for managing dependability

L'Annexe B décrit les phases du cycle de vie d'un produit. Il convient de comprendre les interactions entre les phases du cycle de vie du produit et le processus du cycle de vie du système associé tel qu'il est appliqué à la planification du projet. Cette relation est établie en découpant les phases du cycle de vie du produit (voir l'Annexe C) dans le domaine temps et les processus du cycle de vie du système dans le domaine fonction.

Les phases du cycle de vie du produit permettent de traiter des questions de management en phases planifiées dans le temps, en les associant aux tâches du programme de sûreté de fonctionnement impliquées à chaque phase du cycle de vie du produit: concept, développement, production, fonctionnement et maintenance, puis mise au rebut.

Les processus du cycle de vie du système permettent d'identifier les activités de management spécifiques et les fonctions techniques impliquées en matière d'approvisionnement, de fourniture, de planification et de maîtrise, de conception, de construction, d'évaluation et d'estimation.

Il est souhaitable que le système de gestion de la sûreté de fonctionnement soit adaptable pour répondre aux nouvelles orientations de l'entreprise. L'objectif d'une infrastructure de management flexible est de tirer au mieux profit des ressources disponibles et de répondre avec ponctualité aux engagements du projet. Les projets à long terme impliquant la sûreté de fonctionnement peuvent être gérés par déploiement des moyens-clés. Il peut être constitué des groupes-clés de sûreté de fonctionnement afin de conserver les compétences essentielles au sein de l'organisme.

Il est admis de faire appel à des compétences supplémentaires en passant des contrats destinés à répondre à des besoins particuliers du projet. Les projets en co-entreprise, les alliances dans des consortiums de recherche et la sous-traitance de tâches de sûreté de fonctionnement sont des méthodes communément employées dans un organisme dynamique pour répondre de manière compétitive aux besoins de l'entreprise.

5 Responsabilité de la direction

5.1 Fonction directoriale en matière de sûreté de fonctionnement

Il convient d'identifier les rôles et objectifs spécifiques de la fonction directoriale en matière de sûreté de fonctionnement, eu égard à la qualité et autres disciplines techniques et en fonction de l'organisme ou du projet. La direction au plus haut niveau de l'organisme rend compte de tous les résultats obtenus en matière de sûreté de fonctionnement. Les activités courantes de sûreté de fonctionnement sont en général coordonnées au jour le jour par le personnel technique affecté au projet de manière à répondre à des besoins spécifiques.

a) Il est souhaitable que la direction au plus haut niveau:
   - définisse les perspectives et stratégies en matière de sûreté de fonctionnement de manière cohérente avec les activités de l'organisme;
   - établisse la politique en matière de sûreté de fonctionnement et communique ses orientations, valeurs et engagements à l'organisme, aux fournisseurs et aux clients;
   - crée un environnement et une infrastructure qui favorisent la promotion, la compréhension et la rentabilisation du système et des processus de gestion de fonctionnement;
   - fournisse les ressources appropriées pour soutenir les programmes et les fonctionnements, les développements et la maintenance de la base de connaissances;
   - établisse les critères de mesures des performances de sûreté de fonctionnement réalisées;
   - concentre son attention sur la satisfaction du client et encourage les retours d'information pour une amélioration continue.

The product life cycle phases are described in Annex B. The interrelationship of product life cycle phases and the associated system life cycle processes as applied to project planning should be understood. This relationship is established by partitioning the product life cycle phases (see Annex C) in the time domain and the system life cycle processes in the function domain.

Product life cycle phases help address the time-phased management issues associated with the involvement of dependability programme tasks at each product life cycle phase: concept, development, production, operation and maintenance and disposal.

System life cycle processes help identify the activities of specific management and technical functions involved in acquisition, supply, planning and control, design, construction, evaluation and assessment.

The dependability management system should be adaptive to meet changing business needs. The objective of a flexible management infrastructure is to maximize available resources and to ensure timeliness in meeting project commitments. Long-term projects involving dependability may be managed through deployment of core resources. Core dependability groups may be maintained for retention of critical competence within the organization.

Additional competence may be sought through contracting to meet special project needs. Joint ventures, alliances in research consortia and subcontracting dependability tasks are commonly employed in a dynamic organization to meet competitive business demands.

5 Management responsibility

5.1 Management function on dependability

The management function on dependability should be identified with specific roles and objectives in relation to quality and other technical disciplines as needed by the organization or project. Top management of the organization is accountable for all dependability results. Routine day-to-day dependability activities are normally coordinated by technical project personnel assignments to meet specific needs.

a) Top management should:
   - establish vision and strategy on dependability consistent with the organization's business;
   - set dependability policy and communicate its direction, values and commitments to the organization, suppliers and customers;
   - create an environment and infrastructure for promotion, understanding and cost-effective implementation of dependability management system and processes;
   - provide adequate resources to support dependability programmes, development and maintenance of knowledge base;
   - establish criteria for performance measurement on dependability achievement;
   - focus on customer satisfaction and encourage information feedback for continual improvement.

b) Il convient que le personnel chargé de gérer les programmes de sûreté de fonctionnement:

- soit compétent et bien informé pour traiter des questions qu'implique la sûreté de fonctionnement;
- ait une bonne connaissance de la politique des processus et des méthodes de sûreté de fonctionnement de l'organisme;
- comprenne les objectifs du programme de sûreté de fonctionnement;
- reconnaisse l'importance des interfaces avec les clients et les fournisseurs;
- s'assure de la disponibilité des moyens appropriés pour soutenir les engagements pris et les délais de livraison;
- planifie et mette en œuvre des programmes de travail permettant d'atteindre les objectifs de la sûreté de fonctionnement;
- adapte les programmes de sûreté de fonctionnement spécifiques de manière à satisfaire les besoins du client;
- affecte le personnel compétent nécessaire aux activités de sûreté de fonctionnement;
- surveille les éléments d'entrée et de sortie des processus afin de vérifier l'efficacité de mise en œuvre;
- évalue la performance du travail et les progrès et rapporte les résultats à la revue de direction;
- identifie les risques potentiels et les domaines à problème liés à la sûreté de fonctionnement, pour revue de direction et résolution des problèmes;
- mette en œuvre les actions préventives et correctives pour une amélioration continue;
- mène à bien des analyses de données facilitant l'amélioration du processus et l'enrichissement de la base de connaissances.

5.2 Satisfaction des besoins du client en matière de sûreté de fonctionnement

Il convient que les exigences et les attentes d'un client en matière de sûreté de fonctionnement soient traduites en objectifs permettant de formuler un programme de sûreté de fonctionnement spécifique. Il convient que les exigences et les attentes d'un client en matière de sûreté de fonctionnement soient comprises et qu'un processus d'ajustement les convertisse en tâches effectives du programme de sûreté de fonctionnement. Le cas échéant, une implication précoce du client dans la planification du projet peut être essentielle pour obtenir la confiance du client. Il convient de maintenir un enregistrement des questions de sûreté de fonctionnement et de le revoir régulièrement pour résoudre en temps opportun les problèmes qui peuvent directement ou indirectement affecter les résultats de la sûreté de fonctionnement. Il est recommandé de mettre en place un processus de revue après clôture des actions correctives mises en œuvre. Le but est de rechercher une amélioration continue en mettant en œuvre rapidement les actions correctives et en lançant des mesures préventives efficaces pour éviter la récurrence des problèmes.

La satisfaction des besoins et des attentes du client exige également un déploiement correct des moyens et l'attribution de responsabilités techniques dédiées.

5.3 Politique de sûreté de fonctionnement et implications réglementaires

Certaines activités liées à la sûreté de fonctionnement peuvent être déterminées par des exigences réglementaires et statutaires. En général, ces obligations sont reflétées dans la politique de l'organisme en matière de sûreté de fonctionnement et questions connexes. Il convient que le personnel chargé des tâches de sûreté de fonctionnement soit conscient de ces situations et agisse en conséquence. Une liste non exhaustive des questions réglementaires et statutaires-types impliquant la sûreté de fonctionnement est fournie ci-après:

– questions de responsabilités éventuelles dues à une non-conformité;

b) Personnel managing dependability programmes should:

- be competent and knowledgeable in dealing with the dependability issues involved;
- be familiar with the organization's dependability policy, processes and methods;
- understand the objectives of the dependability programme;
- recognize the importance of interfaces with the customers and suppliers;
- ensure adequate resources to support commitments and delivery schedules;
- plan and implement work programmes for meeting dependability objectives;
- tailor the specific dependability programmes to meet customer's needs;
- assign competent staff to work on dependability activities;
- monitor process inputs and outputs to verify effectiveness of implementation;
- evaluate work performance and progress, and report results for management review;
- identify risks and problem areas associated with dependability for management review and resolution;
- implement preventive and corrective actions for continual improvement;
- conduct data analysis to facilitate process improvement and knowledge base enhancement.

5.2 Meeting customer dependability needs

The needs and expectations of the customers on dependability issues should be translated into objectives for formulating a specific dependability programme. Customer needs and expectations on dependability should be fully understood and converted to actionable dependability programme tasks by means of a tailoring process. Where applicable, early customer involvement in project planning may be essential to ensure achieving customer confidence. A record of dependability issues should be maintained and should be regularly reviewed to ensure timely resolution of problems that may directly or indirectly affect dependability results. A review process should be put in place on closure of action items. The aim is to seek continual improvement by prompt corrective actions and initiation of effective preventive measures to avoid problem reoccurrence.

Meeting customer needs and expectations also demands proper deployment of resources and assignment of dedicated technical responsibilities.

5.3 Dependability policy and regulatory implications

Some dependability-related activities may be determined by regulatory and statutory requirements. These obligations are usually reflected in the organizational policy dealing with dependability and related issues. Personnel assigned to dependability tasks should be aware of such situations and act accordingly. Typical regulatory and statutory issues involving dependability include but are not limited to the following:

– potential liability issues due to non-compliance;

– questions de responsabilités éventuelles dues à une défaillance du produit (perte de fonction critique, sécurité compromise ou violation de la sécurité);
– risques identifiables associés à la mise au rebut;
– la maîtrise des déchets et produits dérivés qui risquent d'affecter l'environnement;
– les conditions de «reprise» et de «rachat» dans les contrats de maintenance de matériel précédemment fourni.

NOTE Une condition de «reprise» existe lorsque, par exemple, l'organisme convient de retirer ou de reprendre d'anciens équipements avant que le client n'en rachète de nouveaux. Une condition de «rachat» existe lorsque, par exemple, l'organisme convient de rembourser le client ou de racheter des pièces de rechange excédentaires non consommées à l'expiration d'un contrat de soutien à la maintenance.

5.4 Programmes de sûreté de fonctionnement

Il convient d'utiliser un processus d'ajustement pour choisir de manière appropriée et mettre en œuvre en temps opportun les tâches pertinentes du programme de sûreté de fonctionnement, pendant toutes les phases applicables du cycle de vie du produit. Cela permet d'obtenir un programme de sûreté de fonctionnement efficace, d'améliorer les performances de disponibilité du système dans son ensemble et d'atteindre les objectifs de sûreté de fonctionnement. L'objectif d'ensemble est d'apporter une plus-value au client par la planification et le déploiement stratégique de processus de qualité et de tâches du programme de sûreté de fonctionnement interdépendants, destinés à répondre aux besoins du client et à le satisfaire. Il est nécessaire que les programmes de sûreté de fonctionnement soient financés et soutenus par des moyens et des ressources appropriés.

5.5 Représentant de la direction

La direction au plus haut niveau peut désigner un représentant de la direction et donner l'autorité nécessaire pour gérer, surveiller, évaluer et coordonner le système de gestion de la sûreté de fonctionnement. Sa mission est de rendre plus efficace le système de gestion de la sûreté de fonctionnement et de l'améliorer. Il convient qu'il rende compte directement à la direction au plus haut niveau et il est admis qu'il communique avec les clients et autres tierces parties concernées sur des questions relatives au système de gestion de la sûreté de fonctionnement.

5.6 Revue de direction

Il est recommandé que la direction au plus haut niveau revoie régulièrement le système de gestion de la sûreté de fonctionnement afin de s'assurer qu'il demeure adapté à la politique, aux objectifs et au système de sûreté de fonctionnement de l'organisme.

Il convient que la fréquence de ces revues soit définie en fonction des besoins de l'organisme. Il est recommandé que les éléments de sortie de ces revues fournissent des données qui seront utilisées pour planifier l'amélioration des performances de l'organisme. Il y a lieu de conserver les enregistrements relatifs à la revue de gestion de la sûreté de fonctionnement comme partie intégrante du processus d'amélioration.

6 Management des ressources

6.1 Mise à disposition des ressources

Il convient que l'organisme fournisse des ressources suffisantes pour soutenir un système de gestion de la sûreté de fonctionnement permettant la réalisation des objectifs commerciaux. Parmi les principaux moyens nécessaires pour soutenir la sûreté de fonctionnement, citons les ressources humaines, les ressources financières et les ressources en matière d'information. Les ressources humaines comprennent le personnel et les compétences de l'organisme qui sont impliqués en matière de sûreté de fonctionnement. Les ressources

– potential liability issues due to failure of product (i.e. loss of mission, compromised safety or breach of security);
– identifiable risks associated with disposal of items;
– control of wastes and by-products that may impact the environment;
– “take-back” and “buy-back” conditions in maintenance contracts of previously supplied materials.

NOTE A “take-back” condition exists when, for example, the organization agrees to remove or take back old equipment before the customer purchases new ones. A “buy-back” condition exists when, for example, the organization agrees to refund the customer or buy-back the surplus spares not consumed at the end of a maintenance support contract.

5.4 Dependability programmes

A tailoring process should be used to ensure adequate selection and timely implementation of relevant dependability programme tasks during all applicable product life cycle phases. This is in order to achieve an effective dependability programme, to enhance total system availability performance, and to realize the dependability objectives. The overall objective is to deliver customer value through strategic planning and deployment of interrelated quality processes and dependability programme tasks to meet customer needs and satisfaction. Dependability programmes need to be funded and supported with adequate resources and facilities.

5.5 Management representative

A management representative may be appointed and given authority by top management to manage, monitor, evaluate and coordinate the dependability management system. This appointment is to enhance effective and efficient operation and improvement of the dependability management system. The representative should report to top management and may communicate with customers and other interested parties on matters pertaining to the dependability management system.

5.6 Management review

Top management should review the dependability management system on a regular basis to determine the continuing suitability of the organization’s dependability policy, objectives and system.

The frequency of these reviews should be determined by the needs of the organization. Outputs from reviews should provide data for use in planning for performance improvement of the organization. Dependability management review records should be maintained as part of the improvement process.

6 Resource management

6.1 Provision of resources

The organization should provide adequate resources to sustain an effective dependability management system to meet business objectives. The major resources needed to support dependability include human resources, financial resources, and information resources. Human resources include the organization’s personnel and expertise involved in dependability. Financial resources include the organization’s assets and capital facilities needed for dependability projects. Information resources include dependability knowledge

financières comprennent les actifs de l'organisme et ses disponibilités en capitaux requis pour des projets de sûreté de fonctionnement. Les ressources informatiques comprennent la base de données de sûreté de fonctionnement et les droits de propriété intellectuelle appartenant à l'organisme. Ces trois principales ressources fournissent conjointement à l'organisme la capacité de sûreté de fonctionnement essentielle pour s'engager avec succès dans des entreprises commerciales et faire face à la concurrence. Il convient que la gestion des ressources de sûreté de fonctionnement reflète la perspective, la mission et les objectifs du plan de développement de l'organisme et de sa stratégie d'entreprise. Outre ces ressources principales, il est évident que d'autres moyens tels que les laboratoires, les installations de fabrication et d'essai pourraient être nécessaires afin de réaliser des tâches spécifiques de sûreté de fonctionnement telles que les recherches de composants, les essais de contrainte, les vérifications et la validation de logiciels, etc.

6.2 Planification, développement et maintien des ressources

6.2.1 Ressources humaines

Il est recommandé que la planification des ressources fasse partie intégrante du plan d'exploitation de l'organisme et de sa stratégie d'entreprise. Il est recommandé de tenir à jour les compétences en matière de sûreté de fonctionnement afin de permettre à l'organisme de s'adapter aux fluctuations des activités du marché. Il est nécessaire de former et d'instruire le personnel pour que ces connaissances demeurent actualisées et qu'il puisse appréhender les progrès technologiques.

6.2.2 Ressources financières

Il convient que le développement des ressources financières en matière de sûreté de fonctionnement se concentre principalement sur la planification budgétaire et sa mise en œuvre. Il est recommandé de mettre des ressources financières adéquates à la disposition des tâches du programme de sûreté de fonctionnement.

6.2.3 Ressources informatiques

Le développement des ressources informatiques est primordial pour maintenir à jour une base de connaissances de sûreté de fonctionnement. Il convient d'encourager, de reconnaître et de récompenser en conséquence les enregistrements de brevets et de droits de propriété intellectuelle. Il y a lieu d'envisager des accords de non-divulgation et de confidentialité lorsque l'organisme traite avec des tiers extérieurs sur des projets conjoints. De tels accords impliquent le partage ou le transfert d'informations de caractère propriétaire dont il convient d'identifier clairement la propriété dans l'accord contractuel.

La gestion des ressources informatiques implique l'utilisation de processus efficaces de circulation des flux d'information destinés à promouvoir l'innovation, les opportunités de travail et l'amélioration grâce à une dissémination adéquate des informations pertinentes à ceux qui en ont besoin. Il est admis que les tâches du programme de sûreté de fonctionnement puissent quelquefois nécessiter le développement ou l'acquisition d'informations sensibles qui pourraient affecter les résultats de l'entreprise ou entraver leur aptitude à soutenir la concurrence sur le marché. Il convient de développer et de maintenir un processus de maîtrise de la sécurité des informations afin de protéger les données sensibles en archivage, sauvegarde, transfert et diffusion ainsi que contre les intrusions.

Il convient de revoir régulièrement le processus de gestion des documents sous contrôle, droits à la propriété intellectuelle, des méthodes et des procédures qui affectent la sûreté de fonctionnement et le cycle de vie des produits. Il est recommandé d'établir clairement et par écrit la durée pendant laquelle la documentation du projet doit être conservée à des fins légales ou réglementaires afin de faciliter leur déclassification et leur destruction.

base and intellectual properties owned by the organization. These three major resources jointly provide the organization with the essential dependability capability to successfully enter into business ventures and competition. Dependability resource management should reflect the vision, mission, and objectives of the organization's business plan and strategy. Further to these major resources, evidentially other resources like laboratories, manufacturing and testing resources might be needed in order to carry out dependability specific tasks, like component investigations, stress testing, software verification and validation, etc.

6.2 Resource planning, development and maintenance

6.2.1 Human resources

Resource planning should form part of the organization's business plan and strategy. Competence in dependability should be kept current to enable the organization to adapt to business and market changes. Personnel training and education are necessary to keep the knowledge current and to deal with technological advances.

6.2.2 Financial resources

Financial resource development for dependability should concentrate primarily on budget planning and implementation. Adequate financial resources should be made available for dependability programme tasks.

6.2.3 Information resources

Information resource development is critical for maintaining a current dependability knowledge base. Intellectual properties and patent registrations should be encouraged, recognized and awarded accordingly. Non-disclosure agreements should be considered when dealing with outside organizations on joint projects. Such agreements involve sharing or transferring of proprietary information where ownership of the information should be clearly identified in the contract agreement.

Information resource management involves the utilization of effective information flow process to drive innovation, work expediency and improvement by proper dissemination of relevant information to those who need it. Dependability programme tasks sometimes may require development or acquisition of sensitive information that could affect business results or hinder market competition. A control process for information security should be developed and maintained to protect sensitive data in storage, backup, transfer and dissemination, and from intrusion.

The process for managing controlled documents, intellectual properties, methods and procedures that affect dependability and the life cycle of products should be reviewed on a regular basis. The length of time that project documentation has to be retained for regulatory or statutory purposes should be clearly documented to facilitate declassification and destruction.

6.3 Sous-traitance

Les tâches du programme de sûreté de fonctionnement courantes et à court terme peuvent être externalisées ou sous-traitées à l'extérieur. Des exemples-types sont les essais de conformité, la conception des outils d'essai ainsi que la collecte et l'analyse des données. Dans de telles situations, l'interface avec le fournisseur ou le contractant devient importante pour l'organisme afin qu'il conserve la maîtrise des engagements du projet dans son ensemble et des plannings de livraison des produits.

7 Réalisation du produit

7.1 Planification de la réalisation du produit

En matière de sûreté de fonctionnement, la planification de réalisation du produit utilise le cadre du cycle de vie du produit établi dans le processus de gestion de la sûreté de fonctionnement.

Le cycle de vie du produit décrit les diverses phases qui recouvrent la durée de vie d'un produit. Il peut être utilisé pour définir des objectifs, des résultats, des processus et autres caractéristiques à dépendance chronologique importantes pour la sûreté de fonctionnement du produit, à chaque phase du cycle de vie du produit. La décomposition en phases définissables du cycle de vie du produit peut faciliter la gestion du projet en termes de réalisation du produit. A chaque phase critique, des décisions d'investissement et des engagements de ressources peuvent être effectués et incorporés dans le processus de gestion de l'entreprise. Les données de sûreté de fonctionnement évaluées au cours de chaque phase du cycle de vie du produit peuvent constituer des informations déterminantes nécessaires à la prise de décision de gestion pour justifier la continuité du projet et l'identification des besoins d'amélioration.

Le cycle de vie du produit aide à traiter les questions dépendant de la chronologie affectant la sûreté de fonctionnement à chaque phase du produit: à la conception, pendant le développement, la fabrication, l'installation, l'opération et la maintenance ainsi qu'à la mise au rebut.

La responsabilité d'établir les objectifs du programme de sûreté de fonctionnement incombe à la direction. Un plan de sûreté de fonctionnement décrit la séquence d'activités de sûreté de fonctionnement associée au plan de réalisation du produit et ajusté de manière à répondre à des besoins spécifiques du produit. L'application du plan de sûreté de fonctionnement est donnée en 7.3.

Il convient que l'élaboration d'un plan de sûreté de fonctionnement tienne compte des éléments suivants:

– la détermination des besoins et attentes spécifiques du marché ou du client en matière de sûreté de fonctionnement;
– la détermination et la manière dont le produit sera utilisé ainsi que l'environnement correspondant;
– la détermination des processus essentiels et le classement par ordre de priorité de mise en œuvre dans le temps des tâches du programme de sûreté de fonctionnement afin de répondre aux besoins du marché ou du client spécifique;
– l'assurance d'atteindre les objectifs du marché ou de répondre aux besoins du client par le biais de processus de vérification et de validation;
– la collecte des données de sûreté de fonctionnement pertinentes pour les enregistrements relatifs à la qualité afin de faciliter l'amélioration continue.

6.3 Outsourcing

Routine, short-term dependability programme tasks can be done by outsourcing or subcontracting the task externally. Typical examples include compliance testing, design of test tools, and data collection and analysis tasks. In such cases, supplier or contractor interface become important for the organization to maintain control of overall project commitments and product delivery schedules.

7 Product realization

7.1 Planning for product realization

Planning for product realization on dependability utilizes the product life cycle framework established in the dependability management process.

The product life cycle depicts the various phases that span the lifetime of a product. It can be used to define objectives, outcomes, processes and other time-dependent characteristics important to product dependability at each phase of the product life cycle. The separation of definable product life cycle phases can facilitate project management in terms of product realization. At each critical phase, investment decisions and resource commitments can be made and incorporated into the business management process. Dependability data assessed during each product life cycle phase can represent crucial information needed for management decisions to support rationale in project continuation and identification of improvement needs.

The product life cycle helps address the time dependent dependability issues at each phase of the product: concept, development, manufacture, installation, operation and maintenance, and disposal.

Establishing dependability programme objectives is a management responsibility. A dependability plan outlines the sequence of dependability activities associated with the product realization plan and tailored to meet specific product needs. The application of a dependability plan is provided in 7.3.

The creation of a dependability plan should consider the following:

– determination of specific dependability needs and expectations of the market or the customer;
– determination of how and in what environment the product will be used;
– determination of essential processes and prioritizing the time-phase implementation of dependability programme tasks to meet market or specific customer needs;
– assurance that market objectives or customer needs are met through verification and validation processes;
– obtain relevant dependability data for quality records to facilitate continual improvement.

7.2 Adaptation des programmes de sûreté de fonctionnement

L'adaptation est un processus de sélection, à partir d'un ensemble de tâches éligibles, de celles qui sont essentielles pour répondre à un objectif spécifique du projet. Pour une mise en œuvre efficace, il convient que le programme de sûreté de fonctionnement soit ajusté de manière à répondre aux besoins de l'application spécifique. L'objectif de l'adaptation est d'optimiser l'affectation des ressources de sûreté de fonctionnement. Il y a lieu de sélectionner, par un processus d'adaptation, les tâches spécifiques du programme de sûreté de fonctionnement qui sont pertinentes pour la phase de cycle de vie du produit ou du besoin du projet.

Les activités d'ordre général du processus d'adaptation sont les suivantes:

– l'identification de l'environnement du projet reflétant la politique et l'infrastructure de l'organisme;
– l'analyse des clauses du contrat, des caractéristiques et objectifs qui peuvent être difficiles à réaliser et à livrer;
– les capacités et ressources nécessaires et réellement disponibles pour la mise en œuvre du projet;
– la détermination de la ou des phases du cycle de vie spécifique applicables au projet;
– la détermination des caractéristiques relatives au produit telles que les propriétés et fonctions du produit, l'historique de produits similaires, l'usage final prévu du produit et les environnements d'application envisagés;
– la sélection des éléments pertinents du programme de fiabilité ainsi que des tâches correspondant aux phases identifiées du cycle de vie du produit;
– identification des processus pertinents du cycle de vie du système liés au projet à associer à la planification et à la durée des éléments du programme de fiabilité et des applications des activités pour l'affectation des ressources;
– justificatifs documentés de la formalisation des décisions d'adaptation en tant que partie intégrante du plan de projet.

Il convient de tenir compte des coûts induits par l'adaptation d'un programme de sûreté de fonctionnement pour atteindre les objectifs du projet spécifique. Il convient de rationaliser les efforts consentis en matière de sûreté de fonctionnement et choisis pour la mise en œuvre des programmes de manière à s'assurer que les activités sélectionnées constituent une valeur ajoutée. Les lignes directrices du processus d'adaptation sont décrites à l'Annexe F. Il convient d'exprimer les données de sortie du processus d'ajustement dans un plan de sûreté de fonctionnement documenté.

7.3 Application du plan de sûreté de fonctionnement

Lors de l'application d'un plan de sûreté de fonctionnement à un produit, il est important de traiter les questions de sûreté de fonctionnement d'un point de vue système. Il est nécessaire que la spécification système définisse les conditions de fonctionnement prévues et que les interactions des sous-systèmes et des composantes du système soient décrites autant que nécessaire pour les considérations relatives à la sûreté de fonctionnement. Il convient de mesurer ou d'évaluer les performances de disponibilité du système pour valider la réalisation des objectifs de sûreté de fonctionnement déclarés en termes de fiabilité, de maintenabilité et de logistique de maintenance.

L'aspect logiciel de la sûreté de fonctionnement est associé à l'intégrité du composant logiciel dans le fonctionnement du système. L'intégrité est un attribut inhérent à la conception. L'aptitude d'un système et de sa composante logicielle à atteindre l'objectif de sûreté de fonctionnement dépend de l'architecture du système, de la conception en matière de tolérance aux pannes, du processus de réduction des risques et du degré de rigueur dans l'application de l'assurance de qualité correspondante ou des méthodes formelles au processus de développement et de maintenance du logiciel. La criticité de l'application logicielle associée au niveau d'intégrité attribué au moment de traiter des effets du logiciel sur les performances du système crée une relation étroite entre la sûreté de fonctionnement et l'intégrité. Les niveaux d'intégrité du système et du logiciel sont décrits dans l'ISO/CEI 15026.

7.2 Tailoring of dependability programmes

Tailoring is a process of selecting those tasks from a set of eligible tasks essential to meet a specific project objective. For effective implementation, the dependability programme should be tailored to meet the needs of the specific application. The objective of tailoring is to optimize the allocation of dependability resources. Specific dependability programme tasks relevant to the product life cycle phase or the project needs should be selected by tailoring.

The general tailoring process activities include the following:

- identification of the project environment reflecting the organizational policy and infrastructure;
- analysis of the contract stipulations, characteristics and objectives which may be difficult to realize and to deliver;
- capability and resources needed and actually available for project implementation;
- determination of the specific life cycle phase or phases applicable to the project;
- determination of the product related characteristics such as the product features and functions, past history of similar products, the intended end use of the product, and the anticipated application environments;
- selection of applicable dependability programme elements and tasks relevant to the specific life cycle phases identified;
- identification of the project's relevant system life cycle processes associated with the timing and duration of dependability programme elements and activity applications for resource allocation;
- documentation of the rationale in formalizing the tailoring decisions as part of the project plan.

Consideration should be given to the costs involved when tailoring a dependability programme to meet specific project objectives. Dependability effort selected for programme implementation should be rationalized to ensure that the selected activities add value. Guidelines for the tailoring process are described in Annex F. The output from the tailoring process should be a documented dependability plan.

7.3 Application of dependability plan

In applying a dependability plan to a product, it is important to address the dependability issues from a system viewpoint. In the system specification the expected operating conditions need to be defined and the interactions of the subsystems and system components need to be described, as far as necessary for dependability considerations. The availability performance of the system should be measured or assessed to validate the achievement of stated dependability objectives in terms of reliability, maintainability, and maintenance support.

The software aspect of dependability is associated with the integrity of the software component in system operation. Integrity is an inherent design attribute. The ability of a system and its software component to achieve a dependability objective is dependent on the system architecture, fault tolerant design, mitigation process and the degree of rigour in the application of relevant quality assurance or formal methods to the software development and maintenance process. The relationship between dependability and integrity is closely linked by the criticality of software application associated with the assigned integrity levels when dealing with the software affecting system performance. ISO/IEC 15026 describes the system and software integrity levels.

Du point de vue de la sûreté de fonctionnement, il convient de tenir compte de la conception des interfaces homme-machine, de la facilité d'exploitation et de maintenance ainsi que de la sécurité des personnes chargées du fonctionnement, de la maintenance, de l'utilisation ou de la mise au rebut du système.

Il y a lieu d'intégrer les éléments du programme de sûreté de fonctionnement à d'autres éléments des processus de développement et de production du produit ainsi qu'aux activités opérationnelles de l'organisme de manière à optimiser les résultats et réduire les coûts.

7.4 Gestion de la chaîne d'approvisionnement

Le processus d'acquisition inclut la gestion de la chaîne d'approvisionnement qui est un élément important en matière de sûreté de fonctionnement pour la réalisation du produit.

Pour atteindre la sûreté de fonctionnement du produit spécifié, l'organisme s'appuie sur les fournisseurs des composants et des services conformes aux besoins et applications spécifiées utilisées pour la conception et la fabrication du produit. Citons par exemple les stocks de pièces de rechange génériques, des dispositifs spéciaux, des outils d'essai disponibles dans le commerce qui permettent de faciliter l'intégration des systèmes; les services d'assistance pour l'évaluation de l'impact du produit sur l'environnement et la certification en matière de sécurité. Dans tous les cas, il convient d'élaborer et de négocier les spécifications contractuelles avec les fournisseurs pour répondre aux objectifs du projet. Il est recommandé que la sélection des sources d'approvisionnement permette d'identifier quelques fournisseurs privilégiés ayant une expérience cohérente en matière de sûreté de fonctionnement, avant de conclure des contrats. Il convient que la surveillance et la revue des fournisseurs fasse l'objet d'un processus continu assurant une livraison contractuelle dans les délais et le maintien d'une liste de sources préférentielles d'approvisionnement. La gestion de la chaîne d'approvisionnement plaide en faveur d'un partenariat entre l'organisme et les fournisseurs. Le processus de gestion de la chaîne d'approvisionnement s'applique à des produits standards du commerce ainsi qu'à des produits d'équipement d'origine. Il convient que le responsable technique chargé des questions de sûreté de fonctionnement joue un rôle actif dans le processus de gestion de la chaîne d'approvisionnement pour assurer la livraison et l'utilisation de produits fiables permettant de répondre aux objectifs de sûreté de fonctionnement.

Le partenariat entre un fournisseur et l'organisme peut inclure une collaboration en matière d'activité d'assurance de la qualité. L'objectif commun est de réduire les coûts et les délais. Il convient également que l'organisme constitue un partenariat avec des clients qui intègrent le produit au système final destiné aux utilisateurs finaux.

Il convient que l'organisme collabore avec le client pour résoudre les problèmes, recueillir des données sur le terrain et établir les tendances de performances, de disponibilité du système ainsi que les taux de retour. Il convient que l'organisme conseille le client en temps utile en ce qui concerne l'utilisation des articles à durée de vie limitée et l'interruption planifiée de pièces de rechange pour le produit livré.

8 Mesures, analyses et amélioration

8.1 Mesure de la sûreté de fonctionnement

Les clients relient la sûreté de fonctionnement à la qualité et à la valeur du produit. La confiance de l'utilisateur est tout d'abord gagnée au cours du développement en utilisant des processus de conception, de fabrication et d'évaluation appropriés. La confiance de l'utilisateur est ensuite reconfirmée par une logistique de maintenance adéquate démontrant les bonnes performances du produit en fonctionnement.

Il est possible de prédire la sûreté de fonctionnement du produit grâce à l'historique des performances passées de produits similaires, la prédiction de fiabilité de nouvelles configurations du produit, les résultats d'essais de prototypes et la vérification de maintenabilité qui sert d'indicateur de la sûreté de production du produit fini qui peut être obtenue. Cette méthode est fréquemment utilisée au cours des premières phases de développement du produit.

From a dependability perspective, the design of human–machine interfaces, the ease of operation and maintenance and the safety of humans who are operating, maintaining, using or disposing of the system should be considered.

The dependability programme elements should be integrated with other elements of the product development and production processes and the operational activities of the organization to maximize results and minimize costs.

7.4 Supply-chain management

The purchasing process includes supply-chain management, which is critical in dependability for product realization.

To achieve specified product dependability, the organization relies on the suppliers in providing components and services conforming to specified needs and applications in designing and manufacturing of the product. Examples include generic parts inventory, special devices, commercial test tools to facilitate systems integration; support services for product environmental impact evaluation and safety certification. In all cases, the contract specifications should be developed and negotiated with the suppliers to meet project objectives. Source selection should identify a limited number of preferred suppliers with consistent dependability history prior to entering into contracts. Supplier monitoring and review should be a continuous process to assure timely contract delivery and maintenance of a preferred source list. Supply-chain management advocates partnership of the organization with the suppliers. The supply-chain management process applies to commercial off-the-shelf products and original equipment manufacture products. The technical leader representing dependability interests should play an active role in the supply-chain management process to ensure delivery and application of reliable products to meet dependability objectives.

The partnership between a supplier and the organization can include cooperative quality assurance activities. The common objective is aimed at reducing the time and cost involved. The organization should also form a partnership with customers who integrate the product to provide the final system to the end users.

The organization should collaborate with the customer in problem resolution and field data collection and in establishing system availability performance trends and product return rates. The organization should advise the customer on a timely basis regarding the use of items with a limited shelf life and the planned discontinuation of supply of spares to delivered products.

8 Measurement, analysis and improvement

8.1 Dependability measurement

Customers link dependability to product quality and value. User confidence is first gained during development, by using appropriate design, assessment and manufacturing processes. This user confidence is subsequently reconfirmed by adequate maintenance support in successful product performance demonstration during operation.

Product dependability can be predicted by past performance history of similar products, reliability prediction of a new product configuration, prototype test results and maintainability verification to serve as indicators of achievable end product dependability. This method is commonly used in the early phase of product development.

En général, la sûreté de fonctionnement est mesurée en terme de performance de disponibilité. Pour ce faire, il convient de mesurer et de démontrer les performances de fiabilité du produit, ses performances de maintenabilité, et les performances de la logistique de maintenance correspondante, afin de déterminer si les performances du produit sont acceptables. Il convient d'utiliser comme élément-clé de l'effort de mesure, un processus de compte-rendu de problèmes et de résoudre rapidement ces problèmes. Ce processus donnera lieu à un produit amélioré qui profitera autant au fournisseur qu'au client.

8.2 Surveillance et assurance de la sûreté de fonctionnement

L'intégration de la sûreté de fonctionnement dans des produits repose sur l'efficacité et l'efficience des applications des processus de sûreté de fonctionnement.

Les processus qui affectent la sûreté de fonctionnement peuvent avoir leur origine dans des produits tels qu'un système de détection de défaut, des procédures de prédiction de sûreté de fonctionnement ou des domaines de recueil des données et d'autres liés à des infrastructures telles que les systèmes de gestion d'information ou des services d'assistance informatique. L'objectif de la surveillance du processus est de s'assurer de la cohérence du processus et de l'exactitude des données impliquées dans le processus. Il convient que le résultat des processus de sûreté de fonctionnement applicables ajoute de la valeur au produit et améliore la confiance de l'utilisateur dans le produit. Il convient que les changements et modifications de processus fassent l'objet de procédures écrites et accompagnées des justifications nécessaires. En général, la surveillance des processus est réalisée par le biais d'un processus de revue de routine, des audits internes réguliers et de l'estimation de l'application.

8.3 Estimation et analyse de la sûreté de fonctionnement

L'estimation de la sûreté de fonctionnement fournit le processus d'évaluation et d'analyse essentiel à la justification des décisions de la direction. L'estimation de la sûreté de fonctionnement implique souvent une évaluation de l'architecture système, de la conception du produit ou de la stratégie de logistique de maintenance pour le projet en question. L'évaluation peut être expérimentale ou analytique, sur la base de l'historique des performances passées, d'enregistrements d'essai ou de résultats d'enquêtes. Il y a lieu d'utiliser des techniques statistiques pour déterminer la probabilité d'occurrence d'événements ou les intervalles de confiance d'une valeur estimée. La modélisation de la fiabilité et de la maintenabilité est une méthode d'estimation qui permet d'évaluer le résultat d'un ensemble de caractéristiques interdépendantes. Pour déterminer les taux de défaillance du produit sur la base de caractéristiques fonctionnelles et de l'environnement appliqué, on peut prédire les performances de fiabilité et de maintenabilité pour ensuite estimer la sûreté de fonctionnement. Il convient que des modèles de sûreté de fonctionnement dédiés aux réseaux soient disponibles pour caractériser les paramètres des réseaux, pour optimiser l'architecture et les performances fonctionnelles des réseaux.

L'analyse de la sûreté de fonctionnement traite de domaines qui posent des problèmes spécifiques et qui nécessitent l'application de méthodes ou de pratiques de sûreté de fonctionnement particulières (pour des exemples, voir la CEI 60300-3-1). Les applications de ces analyses pour estimation de la sûreté de fonctionnement sont à dépendance chronologique en fonction des besoins spécifiques des phases du cycle de vie correspondantes du produit ou du projet. Il y a lieu d'utiliser les analyses de sûreté de fonctionnement pour apporter des réponses techniques significatives aux questions posées par le projet.

8.4 Utilisation des informations de sûreté de fonctionnement

Les informations de sûreté de fonctionnement constituent un élément de valeur qui contient souvent des richesses intellectuelles utilisées pour soutenir ou améliorer les activités commerciales de l'organisme. Il convient de traiter en conséquence l'utilisation des informations de sûreté de fonctionnement correspondantes pour le maintien de communications commerciales et techniques, tant à l'intérieur qu'à l'extérieur de l'organisme.

Dependability is commonly measured in terms of availability performance. To do this, product reliability performance, maintainability performance, and associated maintenance support performance should be duly measured and demonstrated to determine if product performance is acceptable. A key element of the measurement effort should be a process for reporting problems, identifying root causes of problems, and promptly resolving these problems. This process will result in an improved product to the benefit of both supplier and customer.

8.2 Dependability monitoring and assurance

Building dependability into products relies on the effectiveness and efficiency of applications of dependability processes.

The processes affecting dependability can be product oriented such as a defects-monitoring system, dependability prediction procedures, and field return data collection, or those that are infrastructure oriented such as the organization's management information systems and computer support services. The objective of process monitoring is to ensure consistency of the process and the accuracy of the data involved in the process. The outcome of the applicable dependability processes should add value and enhance user confidence in the product. Process changes and modifications should be documented with justifications. Process monitoring is generally achieved through routine review process, regular internal audits, and application assessment.

8.3 Dependability assessment and analysis

Dependability assessment provides the essential evaluation process and analysis to support management decisions. Dependability assessment often involves an evaluation of the system architecture, product design or maintenance support strategy to the project in question. The evaluation may be experimental or analytical, based on past performance history, test records or survey information. Statistical techniques should be used to determine the probability of event occurrences or the confidence intervals of an assessed value. Reliability and maintainability modelling is a form of assessment to evaluate the outcome of a set of interrelated characteristics. In determining product failure rates based on functional characteristics and the applied environment, reliability and maintainability performance can be predicted and subsequently the dependability assessed. Network dependability models should be used to characterize network parameters for optimizing the network architecture and functional performance optimization of the network. Spares provisioning models should be used to evaluate alternate logistic support strategies.

Dependability analysis focuses on specific problem areas requiring the application of specific dependability methods or practices (see IEC 60300-3-1 for examples). The application of these analyses for dependability assessment are time dependent, subject to the specific needs at appropriate product or project life cycle phases. The dependability analyses should be used to provide meaningful technical answers to questions raised by the project.

8.4 Use of dependability information

Dependability information is a valuable asset often containing intellectual properties needed to sustain or enhance the organization's business. The use of relevant dependability information should be treated accordingly in business and technical communications internally and externally to the organization. Dependability information can be generally categorized as business information and technical information. Dependability information related to business

En général, les informations de sûreté de fonctionnement peuvent être classées en informations commerciales et informations techniques. Il est admis que les informations de sûreté de fonctionnement concernant les activités commerciales contiennent des informations contractuelles à caractère contraignant telles que capacité de fonctionnement garantie, garantie de durée de vie, revendications écologiques en matière de mise au rebut, qui peuvent avoir des implications légales. Les informations de sûreté de fonctionnement relatives aux questions techniques peuvent influencer les choix conceptuels et les coûts de possession tels que les taux de retour des produits, les performances de disponibilité et les délais de réapprovisionnement en pièces de rechange.

Les utilisations des informations de sûreté de fonctionnement peuvent être cruciales pendant les phases de concept et de définition d'un projet. Environ 70 % des coûts de cycle de vie d'un produit sont fixés dès achèvement de la spécification fonctionnelle du produit. Les informations critiques utilisées pendant les phases de concept et de définition comprennent des informations sur les environnements d'utilisation des produits, la configuration de système et les interfaces réseau, les objectifs de fiabilité du produit, les informations concernant la concurrence et l'historique des performances des produits. Au cours des phases de conception et de développement, 95 % des coûts du cycle de vie du produit sont engagés dès achèvement des spécifications de conception qui détaillent la manière dont le produit sera construit, fabriqué et lancé sur le marché pour application ou utilisation. Les informations critiques utilisées pendant les phases de conception et de développement comprennent des informations relatives aux règles de conception, aux lignes directrices d'utilisation des composants, aux résultats d'analyse des modes et effets des défauts/défaillances pour la conception de la décomposition fonctionnelle et la testabilité ainsi que des prédictions de fiabilité pour la planification des essais de redondance et de croissance.

Les informations critiques de la sûreté de fonctionnement utilisées pendant la phase de fabrication comprennent des résultats d'essais de recette permettant d'établir les tendances de l'efficience au premier traitement du produit et la planification pour mise en circulation des versions de logiciel. Il convient de recueillir des données de performances opérationnelles et de les utiliser pendant la phase d'exploitation et de maintenance pour déterminer les performances de disponibilité du produit, ajuster les objectifs de coût de la garantie et mettre en œuvre des stratégies de soutien logistique appropriées. Avant de passer à la phase de mise au rebut, il est recommandé d'utiliser les enregistrements relatifs à la maintenance et à la réparation pour déterminer la situation en fin de vie et prendre des décisions quant à la cessation ou le retrait du produit.

Il convient de revoir les modifications de conception et les changements opérationnels des produits et d'analyser les données de modification le cas échéant, pour surveiller l'efficacité de la modification et établir les tendances.

L'utilisation des informations de sûreté de fonctionnement nécessite l'établissement d'une base de connaissances afin de saisir l'historique de performance du produit et aussi, par écrit, les informations de sûreté de fonctionnement pertinentes pour référence ultérieure.

8.5 Mesure des résultats

Les mesures des résultats valident la portée des réalisations en matière commerciale. Des indicateurs ou systèmes de mesure de l'activité sont souvent utilisés pour exprimer l'accomplissement des objectifs atteints. En matière de programme de sûreté de fonctionnement, des mesures courantes des objectifs du projet comprennent de manière non exhaustive, les actions suivantes:

a) Pendant la phase de concept et de définition

- Le concept est réalisable et peut être vérifiable en termes de conformité aux objectifs de fiabilité et de maintenabilité.
- Des caractéristiques de fiabilité et de maintenabilité de produit peuvent être définies et spécifiées en termes numériques.

may contain binding contract information, such as guaranteed performance capability, lifetime warranty and environmental-friendly disposal claims, which may have statutory implications. Dependability information related to technical issues may impact design options and ownership costs such as product return rates, availability performance uptime and turnaround time for spares replenishment.

The use of dependability information may be crucial during the concept and definition phase of a project. Approximately 70 % of a product's life cycle cost is fixed upon completion of the product functional specification. Critical information used during the concept and definition phase includes information on product use environments, systems configuration and network interfaces, product reliability objectives, competitive information, and product past performance history. During the design and development phase, 95 % of the product life cycle costs are committed upon completion of the design specifications detailing how the product is to be built, manufactured, and introduced into market for application or use. Critical information used during the design and development phase includes information on design rules, part application guidelines, fault/failure modes and effects analysis results for functional partitioning and testability design, and reliability predictions for redundancy and growth test planning.

Critical dependability information used during the manufacturing phase includes acceptance test data to establish product first-pass yield trends, and timing for software release. Field performance data should be gathered and used during the operation and maintenance phase to determine product availability performance, reset warranty cost targets, and implement appropriate logistic support strategies. Before entering the disposal phase, the maintenance and repair records should be used to determine the end-of-life situation for deciding on product termination or withdrawal.

Design changes and field modifications on products should be reviewed and the change data analysed, where appropriate, to monitor effectiveness of change and to establish trends.

The use of dependability information advocates the need to establish a knowledge base to capture product performance history and document the relevant dependability information for future reference.

8.5 Measurement of results

Measurement of results is a validation of the extent of achievement in business. Activity indicators or metrics are often used to express achievement of objectives met. In the application of dependability programme, the common measures against project objectives include, but are not limited to, the following:

a) During concept and definition phase
   - Concept is feasible and can be verified to meet reliability and maintainability objectives.
   - Product reliability and maintainability characteristics can be defined and numerical value specified.

b) Pendant la phase de conception et de développement

- Les fonctions de performance du produit peuvent être vérifiées par des prédictions de fiabilité ou de disponibilité.
- Le prototype fonctionne et peut être testé pour en déterminer la fonctionnalité.
- Des essais et des analyses (par exemple, par simulation) peuvent être menés pour valider la conception, identifier les faiblesses et améliorer la conception (croissance de fiabilité – voir la CEI 61014).

c) Pendant la phase de fabrication

- Les données de productivité indiquent la maturité du processus en terme de conformité et de fiabilité du produit.
- Le lancement du produit permet d'entamer les études de croissance de la fiabilité.
- Les défaillances de mortalité infantile peuvent être identifiées avant la livraison du produit.

d) Au cours de la phase d'installation

- L'intégration du système facilite les essais de performance de disponibilité et d'acceptation.
- Le système de recueil de données est efficace pour l'identification et la maîtrise des défaillances prématurées.

e) Au cours de la phase d'exploitation et de maintenance

- Les arrêts de système sont conformes aux objectifs de performance et de disponibilité.
- Les retours du terrain proprement dit ne comportent pas d'articles défectueux.

f) Au cours de la phase de mise au rebut

- Les caractéristiques d'usure indiquent que la fin de vie du produit est atteinte.

8.6 Amélioration de la sûreté de fonctionnement

Le système de gestion de la sûreté de fonctionnement peut être amélioré grâce à la prédominance de la direction au plus haut niveau et à la planification stratégique visant à l'évolution et au développement de son efficacité. Il convient de fixer les objectifs d'amélioration en fonction des objectifs commerciaux et de la satisfaction du client. La diversification commerciale et l'évolution technologique exigent parfois de revoir la pertinence pour une application efficace des éléments de programme de sûreté de fonctionnement et des processus correspondants nécessaires au projet. Il peut être nécessaire de procéder à des ajustements pour s'adapter aux changements et aux écarts de procédés et répondre à de nouveaux objectifs commerciaux.

L'amélioration du produit est atteinte grâce au management systématique de projet, au contrôle de la conception et à la mise en œuvre efficace et dans les temps d'actions préventives et correctives. Il convient que les processus de sûreté de fonctionnement puissent s'adapter à l'innovation technologique et provoquer une amélioration continue. Il convient d'établir une base de connaissances de la sûreté de fonctionnement afin d'encourager le développement des connaissances et d'en saisir les informations pertinentes.

Il convient de considérer les processus d'amélioration de la sûreté de fonctionnement qui suivent.

- Déployer les méthodes et les outils adéquats pour la vérification de la conception dans les délais et la validation de la conformité du produit pour réduire la durée du cycle de conception et accélérer l'approbation du produit.
- Analyser la cause profonde pour résoudre dans les plus brefs délais les éventuels problèmes critiques de conception en apportant des solutions globales pour l'évitement des coûts et les mesures préventives.

b) During design and development phase
   - Product performance functions can be verified by reliability or availability predictions.
   - Prototype works and can be tested to determine functionality.
   - Testing and analysis (e.g. simulation) can be conducted to validate design, identify weaknesses and improve the design (reliability growth – see IEC 61014).

c) During manufacturing phase
   - Production yield data indicates process maturity in product reliability conformance.
   - Product introduction permits initiation of reliability growth studies.
   - Infant mortality failures can be identified prior to shipping product.

d) During installation phase
   - System integration facilitates availability performance and acceptance testing.
   - Data collection system is effective for identification and control of early failures.

e) During operation and maintenance phase
   - System outages are consistent with availability performance objectives.
   - Actual field returns can account for “no fault found” items.

f) During disposal phase
   - Wear-out characteristics indicate the end-of-life period.

8.6 Dependability improvement

Dependability management system improvement is achieved through top management leadership and strategic planning for evolution and for enhancing its effectiveness and efficiency. The improvement objectives should be set against business objectives and customer satisfaction. Business diversification and technology changes often demand a review of the relevancy for effective application of the dependability programme elements and related processes needed for the project. Adjustments may be necessary to adapt process changes and deviations to meet new business objectives.

Product improvement is achieved through systematic project management, design control, effective and timely initiation of preventive and corrective actions. Dependability processes should be agile to accommodate technology innovation and motivate continual improvement. A core dependability knowledge base should be established to encourage knowledge development and to capture relevant information.

The following dependability improvement processes should be considered.

- Relevant methods and tools should be deployed for timely design verification and product conformance validation to reduce design cycle time and speed up product acceptance.
- Root-cause analysis should be employed to promptly resolve potential critical design problems providing total solutions for cost avoidance and preventive measure.

– Utiliser les informations sur l'estimation des risques à certains moments décisifs de prise de décision dans le projet ou lors des revues de direction pour déterminer l'exposition aux risques et les conséquences éventuelles, et recommander des actions correctives et/ou préventives rentables.

– Développer un contrôle adéquat des données pour assurer la précision et la fiabilité des informations afin de faciliter la gestion des décisions relatives au projet.

– Organiser des revues de direction et des revues techniques portant précisément sur la détermination des potentiels des processus de sûreté de fonctionnement et les possibilités d'amélioration.

– Entretenir les interfaces client et d'obtenir des informations des fournisseurs pour recueillir des retours d'information constructifs permettant l'activation dans les délais des processus d'amélioration nécessaires qui sont à valeur ajoutée.

- Risk assessment information should be used at project decision points or management reviews to determine risk exposures and potential impact, and recommend cost-effective preventive and/or corrective actions.
- Appropriate data control should be developed to sustain the accuracy and integrity of information for project decision management facilitation.
- Technical as well as management reviews should focus on determining dependability process strengths and opportunities for enhancement.
- Close customer interface should be maintained and suppliers' information should be obtained to gain valuable feedback information permitting timely activation of the needed improvement processes that are value added.

Annexe A
(informative)

Eléments du programme de sûreté de fonctionnement et tâches des applications des systèmes, du matériel et du logiciel

A.1 Elément 1: Management

Le management est un élément-clé du programme de sûreté de fonctionnement. La planification détermine la portée et les objectifs du projet, identifie les activités du projet, et établit l'ordonnancement des tâches et les résultats attendus. Le management a recours aux stratégies commerciales et techniques adéquates, assure la direction et attribue les ressources nécessaires à une mise en œuvre efficace d'une tâche pour atteindre les objectifs du projet. Les tâches 1 à 7 décrivent les principales activités de l'élément «management».

Cela est obtenu en affectant des responsables techniques à la tête des projets de sûreté de fonctionnement. Le responsable technique chargé de la sûreté de fonctionnement joue un rôle de management qui comprend notamment la responsabilité de constituer une équipe, de diriger les membres de l'équipe, de communiquer avec les clients et les fournisseurs pour ce qui concerne les questions de sûreté de fonctionnement, et d'entretenir un lien technique essentiel dans le processus de gestion de la chaîne d'approvisionnement sur les problèmes de sûreté de fonctionnement. Il convient d'entretenir des communications après vente avec le client afin de le fidéliser.

A.1.1 Tâche 1: Plan de sûreté de fonctionnement

Le programme de sûreté de fonctionnement requiert une planification adéquate et l'implication de la direction au plus haut niveau. Le plan de sûreté de fonctionnement sert de document de base pour la gestion, la planification et le contrôle, en régissant la réalisation du programme de sûreté de fonctionnement. Il convient d'intégrer le plan de sûreté de fonctionnement d'un produit donné à l'ensemble du plan de projet, sous réserve de le soumettre à la revue de la direction et au processus d'approbation. Un plan de sûreté de fonctionnement peut couvrir un produit spécifique sur une seule étape, sur plusieurs ou sur toutes les étapes de son cycle de vie. Il convient que le plan de sûreté de fonctionnement identifie les tâches du programme de sûreté de fonctionnement concerné applicables au produit, ainsi que la maîtrise de ses composants matériels et logiciels. Il convient que le plan de sûreté de fonctionnement identifie le responsable technique chargé de la mise en œuvre du programme de sûreté de fonctionnement, ainsi que le représentant de la direction le cas échéant. Il convient de délimiter les tâches du programme de sûreté de fonctionnement avec l'ordonnancement des tâches et les résultats attendus.

A.1.2 Tâche 2: Spécifications de sûreté de fonctionnement

Les spécifications de sûreté de fonctionnement impliquent le processus d'identification des besoins et de définition des conditions du produit pour la livraison du projet. La spécification est générée pour répondre aux besoins du client ou définir les critères de sélection des fournisseurs privilégiés. Le résultat de la spécification peut devenir l'accord formel du contrat des parties impliquées. La collaboration entre le client et le fournisseur contribue largement à accélérer la préparation de la spécification et faciliter la compréhension commune des objectifs et des contraintes de la sûreté de fonctionnement afin de parvenir à un accord. La spécification de sûreté de fonctionnement peut contenir des mesures quantitatives telles que des performances de disponibilité, la durée de vie prévue du produit et la durée de panne autorisée ou les limites de dégradation. Il convient de définir les conditions relatives à ces mesures quantitatives et de les documenter à des fins de démonstration et d'acceptation du produit. Il convient de faire la distinction entre les spécifications de sûreté de fonctionnement qui concernent directement les performances globales du produit et celles liées à l'utilisation ou l'utilisation prévue des composants matériels ou logiciels. Il y a lieu d'utiliser la CEI 60300-3-4 comme référence.

Annex A
(informative)

Dependability programme elements and tasks for systems, hardware and software applications

A.1 Element 1: Management

Management is a key element of a dependability programme. Planning defines the scope and objectives of the project, identifies the project activities, and establishes the milestone schedule and deliverables. Management employs the appropriate business and technical strategies, provides leadership and allocates the necessary resources for effective task implementation to meet planned project objectives. Tasks 1 to 7 describe the essential activities in the management element.

This is accomplished by appointment of technical leaders to lead dependability projects. The management role of the technical leader responsible for dependability includes team building, leadership responsibility to team members, communication with customers and suppliers on dependability matters and maintaining a key technical link in the supply-chain management process on dependability issues. After-sales communications with the customer should be maintained to build customer loyalty.

A.1.1 Task 1: Dependability plan

The dependability programme needs adequate planning and top management involvement. The dependability plan serves as the basic management, planning and control document, governing the execution of the dependability programme. A dependability plan for a product should be integrated with the overall project plan, subject to review by management and approval process. A dependability plan can cover a specific product over a single stage, several or all stages of its life cycle. The dependability plan should identify the relevant dependability programme tasks applicable to the product, and the control of its constituent hardware and software components. The dependability plan should identify the technical leader responsible for the dependability programme implementation, and the management representative where designated. Dependability programme tasks should be delineated with milestone schedule and deliverables.

A.1.2 Task 2: Dependability specifications

Dependability specifications involve the process of identifying the needs and defining the conditions of the product for project delivery. The specification is generated to meet customer needs, or to define the criteria for selecting preferred suppliers. The outcome of the specification may become the formal contract agreement of the parties involved. Customer and supplier collaboration would greatly expedite the preparation of the specification and facilitate the mutual understanding of the dependability objectives and constraints in order to reach agreement. The dependability specification may contain quantitative measures such as availability performance, product life expectancy and permissible outage duration or degradation limits. The conditions for these quantitative measures should be defined and documented for product demonstration and acceptance. The dependability specification should distinguish those directly affecting the overall performance of the product and those related to the intended use or application of the hardware or software components. IEC 60300-3-4 should be used as a reference.

Le processus de spécification de sûreté de fonctionnement utilise parfois des techniques de répartition. La répartition de la sûreté de fonctionnement est effectuée en découpant et en cartographiant les besoins en sûreté de fonctionnement exprimés dans l'architecture du système. Cela permet de répartir les ressources nécessaires à la criticité des fonctions du système afin d'atteindre les objectifs de la sûreté de fonctionnement de l'ensemble du système. Les techniques de répartition facilitent les compromis sur la conception fonctionnelle, permettent la rationalisation des décisions de production/achat, ainsi que la planification et la mise en œuvre du niveau d'effort approprié ou du degré de rigueur technique nécessaire pour le développement, l'acquisition ou le soutien des composants matériels ou logiciels pour divers niveaux d'utilisations critiques.

A.1.3 Tâche 3: Maîtrise des processus

Il convient que le système de gestion de la sûreté de fonctionnement permette de maîtriser tous les processus ayant une incidence sur la sûreté de fonctionnement. Il convient d'activer la fonction de maîtrise sur les processus qui affectent la fiabilité du produit et les performances de disponibilité du système. Les processus-types liés aux projets de sûreté de fonctionnement concernent la sélection des composants, les méthodes d'évaluation de la fiabilité, les critères d'acceptation du produit, le compte rendu des incidents de type défaillance, l'analyse des causes profondes, les actions préventives et correctives. Il convient d'identifier le propriétaire des processus. Il convient de vérifier l'exactitude et la cohérence des éléments d'entrée et de sortie des processus par rapport à leurs objectifs prévus. Les principaux objectifs du projet relatifs à la sûreté de fonctionnement reflètent généralement un ensemble coordonné de résultats attendus et de calendriers qui permet de faciliter les décisions concernant le projet lors des revues de direction et à l'interface entre le client et les fournisseurs.

A.1.4 Tâche 4: Maîtrise de la conception

La maîtrise de la conception est un processus de management essentiel pour assurer que le développement d'un produit permet d'atteindre les objectifs de sûreté de fonctionnement. Les activités de maîtrise de la conception impliquent l'établissement de règles de conception et l'élaboration de lignes directrices sur la conception pour une exploitation sûre, la répartition physique et fonctionnelle permettant d'obtenir une modularité nécessaire pour faciliter l'assemblage et le désassemblage, la mise en œuvre du processus d'assurance permettant de garantir la conformité du produit à la réglementation. L'amélioration de la conception entraîne normalement la croissance de la fiabilité. Il convient d'intégrer un suivi correct du niveau de fiabilité de la conception dans le processus de maîtrise de la conception. Il convient de vérifier les éléments d'entrée et de sortie en termes d'exactitude et d'exhaustivité. Il y a lieu que les revues de conception se concentrent sur la maturité progressive de la conception afin de garantir la capacité de fabrication et de soutien du produit. Il convient que les modifications apportées à la conception suivent le processus de gestion de configuration afin de faciliter la traçabilité des modifications ou mises à jour de la conception.

A.1.5 Tâche 5: Suivi et revue

Le processus de revue se compose de la revue de contrat, de la revue de management et de la revue technique.

Il convient de mener la revue de contrat en conjonction avec le processus global de revue de projet. Les exigences particulières du contrat liées aux résultats attendus de la sûreté de fonctionnement sont revues avec le client pour acceptation et, le cas échéant, avec les fournisseurs d'éléments sous-traités. Lorsque des écarts sont constatés, il convient de résoudre les questions spécifiques et d'amender le contrat afin qu'il reflète la situation la plus récente. Il convient de conserver des enregistrements des revues de contrat.

Il convient d'effectuer régulièrement des revues de management sur les questions de sûreté de fonctionnement.

The dependability specification process sometimes employs allocation techniques. The allocation of dependability is achieved by partitioning and mapping the desired dependability needs onto the system architecture. This provides a means for allocation of proper resources relevant to the criticality of system functions to meet overall system dependability objectives. The allocation techniques facilitate functional design trade-off, permit rationalization of make/buy decisions and allow planning and implementation of the appropriate level of effort or the degree of engineering rigour necessary in the development, acquisition or support of the hardware or software components for various levels of critical applications.

A.1.3 Task 3: Control of processes

The dependability management system should control all processes affecting dependability. The control function should be activated on those processes affecting product reliability and system availability performance. Typical processes related to dependability projects are parts selection, reliability assessment methods, product acceptance criteria, failure incidents reporting, root-cause analysis and preventive and corrective actions. The owner of the processes should be identified. The process inputs and outputs should be verified for accuracy and consistency for their intended purposes. Project milestone objectives related to dependability should reflect a coordinated set of project deliverables and schedules to facilitate project decision at management reviews, and at customer and suppliers interface.

A.1.4 Task 4: Design control

Design control is an essential management process to ensure development of a product to meet dependability objectives. Design control activities involve establishing design rules and setting design guidelines for safe operation, physical and functional partitioning to achieve modularity to facilitate assembly and disassembly, implementation of the assurance process to ensure product conformance to regulation. Reliability growth resulting from improvement in the design is expected. Proper monitoring of the design reliability status should be integrated into the design control process. Design inputs and outputs should be verified for accuracy and completeness. Design reviews should focus on progressive design maturity to ensure product manufacturability and supportability. Design changes should follow the configuration management process to facilitate traceability of design modification or updates.

A.1.5 Task 5: Monitoring and review

The review process consists of contract review, management review and technical review.

Contract review should be conducted in conjunction with the overall project review process. Specific contract requirements pertaining to the dependability deliverables are reviewed with the customer for acceptance, and where applicable with the suppliers of subcontract items. Where discrepancies occur, the specific issues should be resolved and the contract amended to reflect the latest status. Contract review records should be maintained.

Management review of dependability issues should be conducted regularly.

Des revues techniques sont normalement organisées régulièrement au niveau du projet pendant toute sa durée ou lorsque les circonstances l'imposent. Lors de phases spécifiques du projet, les revues techniques impliquent un processus plus formel permettant d'assurer la conformité avec le contrat ou les exigences réglementaires. Il convient de conserver tous les enregistrements de revues. Il y a lieu d'utiliser la CEI 61160 comme base pour effectuer une revue de conception formelle.

A.1.6 Tâche 6: Gestion de la chaîne d'approvisionnement

Il convient d'activer le processus de gestion de la chaîne d'approvisionnement. Il convient que le responsable technique chargé de la sûreté de fonctionnement joue un rôle actif dans le processus de gestion de la chaîne d'approvisionnement afin d'assurer la livraison et l'utilisation de produits fiables. Il convient d'entretenir le dialogue entre le client et les fournisseurs. Il y a lieu de maîtriser le flux d'informations pour des besoins de confidentialité et de sécurité. Il convient d'établir un processus de revue commun. Le paragraphe 7.4 fournit des informations supplémentaires sur la gestion de la chaîne d'approvisionnement relative à la réalisation du produit. Du point de vue de la gestion de la sûreté de fonctionnement, il convient de tenir compte des activités suivantes:

– Recommander une liste de composants privilégiés pour la conception et la fabrication du produit;
– Etablir les critères de sélection des fournisseurs privilégiés;
– Partager les données sur la sûreté de fonctionnement concernant l'application et l'historique des performances de composants critiques;
– Partager le processus d'évaluation du produit et les données de sortie;
– Effectuer des revues communes sur les non-conformités et les défaillances anormales;
– Résolution commune de problèmes pour l'amélioration continue;
– Revues communes concernant les limitations sur la vie du produit dues à l'évolution des techniques ou l'obsolescence du marché;
– Suivi des fournisseurs.

A.1.7 Tâche 7: Introduction du produit

Il convient de planifier et de gérer l'introduction du produit afin de faciliter la transition du nouveau produit vers la phase d'exploitation et de maintenance. L'importance accordée à la sûreté de fonctionnement permet d'assurer la maturité du produit, l'adéquation des plans de soutien logistique, la gestion des relations avec le client, les réclamations et les renvois de produits, ainsi que la répartition des ressources afin de répondre aux situations de routine prévues et aux situations d'urgence. Il convient que le processus d'introduction du produit implique la participation du client pour l'évaluation des performances du produit et le retour d'information en vue de l'amélioration. Il convient de résoudre la question de la date de commercialisation du produit en même temps que les questions de version, de mise à jour ou de modification du produit en vue d'améliorer ses fonctionnalités, réduire les risques/coûts et d'améliorer le processus de décision de l'entreprise. Le cas échéant, il convient que le lancement du produit s'inscrive dans un processus de gestion de projet intégré afin d'obtenir des solutions globales et procurer de la valeur ajoutée pour le client.

A.2 Elément 2: Disciplines liées à la sûreté de fonctionnement

La sûreté de fonctionnement des produits est obtenue en premier lieu grâce à une ingénierie cohérente et l'application de pratiques industrielles éprouvées. Des disciplines d'ingénierie spécifiques sont nécessaires pour obtenir des solutions techniques associées à la fiabilité et à la maintenabilité du produit. Les tâches 8 à 12 décrivent des disciplines essentielles liées à la sûreté de fonctionnement.

Technical reviews are normally conducted at the project level on a regular basis for the duration of the project or as the need arises. At specific project phases, the technical reviews may involve a more formal process for compliance to the contract or regulatory requirements. All review records should be maintained. IEC 61160 should be used as guidance to conduct formal design review.

A.1.6 Task 6: Supply-chain management

The supply-chain management process should be activated. The technical leader representing dependability interests should play an active role in the supply-chain management process to ensure delivery and application of reliable products. Dialogue between the customer and the suppliers should be maintained. Information flow should be controlled for sensitivity and security purposes. A joint review process should be established. Subclause 7.4 provides additional information on supply-chain management related to product realization. From a dependability management perspective, the following activities should be considered:

– Recommendation of preferred parts list appropriate to the product design and construction;
– Establishment of criteria for selection of preferred suppliers;
– Sharing dependability data on critical parts application and performance history;
– Sharing of product evaluation process and output data;
– Joint reviews on non-conformances and abnormal failures;
– Joint problem resolutions for continual improvement;
– Joint reviews on product life limitations due to technology change or market obsolescence;
– Supplier monitoring.

A.1.7 Task 7: Product introduction

Product introduction should be planned and managed to facilitate the transition of a new product into its operation and maintenance phase. The dependability emphasis is to ensure product maturity on fitness for use, adequacy of the logistic support plans, handling of customer relations, complaints and product recalls and resource allocation to meet anticipated routine and emergency situations. The product introduction process should involve customer participation for product performance evaluation and feedback for improvement. The product time-to-market issue should be addressed in conjunction with product release, update or modification for feature enhancement, risk/cost reduction and improvement of the business decision process. Where appropriate, product introduction should function in an integrated project management process to achieve total solutions and delivery of value to the customer.

A.2 Element 2: Dependability disciplines

Dependability in products is achieved primarily through sound engineering effort and application of successfully applied industry practices. Special engineering disciplines are needed to provide technical solutions associated with the reliability and maintainability of the product. Tasks 8 to 12 describe the essential dependability disciplines.

A.2.1 Tâche 8: Ingénierie de la fiabilité

L'ingénierie de la fiabilité est une discipline technique utilisée pour caractériser l'environnement et les contraintes de fonctionnement du système et pour établir des règles de conception et des lignes directrices d'application afin de concevoir et fabriquer des produits fiables. L'ingénierie de la fiabilité implique des conceptions tolérantes aux pannes, l'analyse et la vérification de la fiabilité afin d'assurer la maturité et la résistance de la conception ainsi que l'opportunité de la fabrication du produit. Les activités d'ingénierie de la fiabilité applicables aux logiciels sont associées au degré de rigueur technique nécessaire pour l'application des méthodes appropriées. L'apport de la fiabilité d'un composant logiciel dans un produit contenant le logiciel dépend largement du processus de développement et de la conception du logiciel.

A.2.2 Tâche 9: Ingénierie de la maintenabilité

L'ingénierie de la maintenabilité est une discipline technique utilisée dans la conception d'un produit pour des besoins de facilité, d'économie et d'efficacité de la maintenance; elle comprend la conception en termes de testabilité, d'accessibilité, d'interchangeabilité et de normalisation. Il convient de déterminer l'origine et la revue régulière des critères de conception relatifs à la maintenabilité à partir des exigences spécifiées pour le produit. L'ingénierie de la maintenabilité est impliquée dans la conception relative à la testabilité. La testabilité représente la mesure dans laquelle un essai réalisable peut être conçu dans le produit afin de déterminer si un objectif est atteint. A la testabilité est associée la couverture des essais qui représente la mesure dans laquelle les tests élémentaires sont élaborés pour tester le système ou ses composants afin d'assurer la conformité avec des critères établis. L'objet des essais pendant le développement est de déceler des défaillances dans les composants. L'objet des essais diagnostiques pendant la maintenance est de déterminer les causes profondes d'une défaillance ou d'un dysfonctionnement identifié du système.

A.2.3 Tâche 10: Ingénierie de la logistique de maintenance

La maintenance et la logistique de maintenance sont essentielles pour garantir la sûreté de fonctionnement des produits pendant tout leur cycle de vie. Les performances prévues de fonctionnalité, d'aptitude et de sûreté de fonctionnement sont obtenues en fournissant les services de maintenance et de logistique de maintenance nécessaires, en conjonction avec la conception, la maintenabilité, la qualité et des pratiques de travail cohérentes.

L'importance et le type des services de maintenance et de logistique de maintenance dépendent des besoins du client, de la nature des produits, de la disponibilité spécifiée et d'autres facteurs. A mesure que ces facteurs évoluent, notamment pendant la phase d'exploitation et de maintenance, la maintenance et la logistique de maintenance peuvent devoir être adaptées. Il existe plusieurs scénarios pour la planification et la fourniture de services de maintenance et de logistique de maintenance, en fonction de la personne qui prend la responsabilité de leur mise en œuvre et de la phase du cycle de vie pendant laquelle elles se déroulent.

Pour de nombreux produits, le fabricant fournit des services de maintenance et de logistique de maintenance complets qui font partie intégrante de la livraison du produit. Ces services sont fournis sur une base contractuelle ou à la demande de l'utilisateur ou du consommateur. La planification et la fourniture de services de maintenance et de logistique de maintenance peuvent donc se produire pendant la conception et le développement et incombent en premier lieu au fabricant, au vendeur ou à tout autre organisme de logistique externalisée. L'utilisateur du produit dépend principalement de ce réseau pour fournir des services de logistique d'ensemble pendant la phase d'exploitation et de maintenance. Des informations sur la logistique intégrée appliquée à ces cas particuliers sont présentées dans la CEI 60300-3-12. Des lignes directrices sur la maintenance des logiciels sont présentées dans l'ISO/CEI 14764.

A.2.1 Task 8: Reliability engineering

Reliability engineering is the technical discipline employed to characterize the system operating environment and operational stresses, and to establish design rules and application guidelines for designing and manufacturing reliable products. Reliability engineering involves fault tolerant designs, reliability analysis and verification to ensure design maturity and robustness, and readiness for product manufacturing. The reliability engineering effort applicable to software is associated with the degree of engineering rigour in the application of relevant methods. Reliability contribution of software component to a product containing the software is highly dependent on the development process and the design of the software.

A.2.2 Task 9: Maintainability engineering

Maintainability engineering is the technical discipline employed to design a product for ease, economy, and effectiveness of maintenance; it includes designing for testability, accessibility, inter-changeability, and standardization. The derivation and periodic review of detailed maintainability design criteria should be obtained from requirements specified for the product. Maintainability engineering is involved in designing for testability. Testability is the extent to which a feasible test can be designed into the product to determine whether an objective is met. Associated with testability is test coverage, which is the extent to which the test cases are developed to test the system or its components for conformance with established criteria. The purpose for testing during development is to find faults within the components. The purpose of diagnostic testing during maintenance is to determine the root-cause of an identified system failure or malfunction.

A.2.3 Task 10: Maintenance support engineering

The provision of maintenance and maintenance support is a key component for ensuring the dependability of products throughout their life cycle. Intended functionality, capability and dependability performance are achieved by providing the necessary maintenance and maintenance support in conjunction with appropriate design, maintainability, quality manufacturing and sound operating practices.

The amount and type of maintenance and maintenance support depends on customer needs, the nature of the products, specified availability and other factors. As these factors change, especially during the operation and maintenance phase, maintenance and maintenance support may need to be adjusted. There are different scenarios for planning and providing maintenance and maintenance support, depending on who takes responsibility for their implementation and on which phase of the life cycle they occur.

For many products, the manufacturer provides complete maintenance and maintenance support services as an integrated component of the delivery of the product. These services are either provided on a contractual basis or are accessed as needed by the user or consumer. The planning and provision of maintenance and maintenance support can thus occur during design and development and remains the primary responsibility of the manufacturer, vendor or other outsourced support organization. The user of the product depends primarily upon this network to supply total support services during the operation and maintenance phase. Information on integrated logistic support, as applied in these cases, is provided in IEC 60300-3-12. Guideline for software maintenance is provided in ISO/IEC 14764.

Dans d'autres cas, les vendeurs des produits n'élaborent qu'une planification de base de la logistique de maintenance. Les utilisateurs et les clients fournissent ensuite les services de maintenance et de logistique de maintenance nécessaires pour des applications spécifiques en utilisant souvent des ressources internes. C'est le cas notamment lorsque des produits existants sont combinés dans des systèmes complexes par un autre vendeur ou un autre organisme puis fournis à un utilisateur ou à un opérateur. La responsabilité de l'élaboration de la maintenance et de la logistique de maintenance doit ensuite être déterminée entre le vendeur et l'utilisateur ou l'opérateur (voir la CEI 60300-3-14).

A.2.4 Tâche 11: Normalisation

La normalisation est la partie de la discipline de sûreté de fonctionnement relative à la conformité de la conception avec les spécifications du produit et au respect des procédures de modification de la conception. La normalisation des parties matérielles facilite la sélection et la qualification des fournisseurs. Il convient d'utiliser des normes de conception, de production, d'exploitation et de logistique de service pour réduire au minimum les problèmes de non-conformité.

Il convient d'établir un plan de gestion de configuration et de le mettre en œuvre pour le projet. Il y a lieu d'utiliser ce plan pour l'identification, la maîtrise, le compte rendu de l'état d'avancement, l'évaluation, la gestion des modifications, des versions et de la livraison du matériel, des logiciels et des documentations compris dans le projet global. Pour plus de détails sur la gestion de configuration, voir l'ISO 10007.

A.2.5 Tâche 12: Facteurs humains

Les facteurs humains ont un impact significatif sur les performances du système. Il convient d'utiliser des lignes directrices et des normes de conception afin d'améliorer l'interface homme/machine pour faciliter l'exploitation et la maintenance. Ces interfaces comprennent les commandes, les affichages, les alarmes et les indicateurs. Il convient de tenir compte dans la conception du produit de caractéristiques anthropométriques, des limitations sensorielles humaines et de facteurs psychologiques qui affectent les perceptions et les actions humaines.

Il convient d'ajouter, dans les tests élémentaires et procédures d'essai documentées, les facteurs humains liés à l'environnement de travail du système afin d'assurer que les objectifs généraux de sûreté de fonctionnement sont atteints.

Il y a lieu que le niveau d'ingénierie humaine corresponde au domaine d'application du projet. Il convient d'étudier l'impact potentiel d'un dysfonctionnement du système dû à une erreur humaine sur son environnement immédiat.

A.3 Elément 3: Analyse, évaluation et estimation

L'ingénierie de la fiabilité et de la maintenabilité fait appel à plusieurs techniques et méthodes pour résoudre les problèmes de sûreté de fonctionnement. La méthodologie employée peut être quantitative ou qualitative ou les deux, mais il convient que la solution adoptée s'appuie sur un jugement technique solide et des pratiques industrielles éprouvées. Les tâches 13 à 21 décrivent les méthodes les plus utilisées dans les domaines de l'analyse, l'évaluation et l'estimation.

A.3.1 Tâche 13: Analyse de l'environnement de travail

Les spécifications du produit doivent comprendre des définitions précises du scénario de fonctionnement à élaborer. Il convient de spécifier les conditions de l'environnement d'utilisation applicables aux produits en termes de caractéristiques de performance spécifiques et de limites normalisées établies. Cela permet de classer les environnements des produits et d'identifier les expositions environnementales applicables afin de faciliter la conception du produit et satisfaire aux exigences concernant l'environnement de travail et

In other cases, product vendors provide only basic maintenance support planning. Users and customers then provide the required maintenance and maintenance support for specific application often using internal resources. This occurs especially when existing products are combined into complex systems by another vendor or organization and are then supplied to a user or operator. The responsibility for developing maintenance and maintenance support then needs to be established between the vendor and user or operator (see IEC 60300-3-14).

A.2.4 Task 11: Standardization

Standardization is part of the dependability discipline concerned with design conformance to product specifications and the adherence to design change procedures. Standardization of hardware parts facilitates selection and qualification of suppliers. Standards for design, production, operation and service support should be used to minimize non-conformance problems.

A configuration management plan should be established and implemented for the project. This plan should be used for identification, control, status accounting, evaluation, change management, release management and delivery of the hardware, software and documentations involved in the overall project. Refer to ISO 10007 for guidance on configuration management.

A.2.5 Task 12: Human factors

Human factors have a significant impact on system performance. Design guidelines and standards should be used to enhance the human-machine interface for ease of operation and maintenance. These interfaces include controls, displays, alarms and indicators. Design of the product should account for anthropometrics, human sensory limitations and psychological factors that affect human perception and action.

Documented test cases and test procedures should be extended to include human factor elements relating to the operating environment of the system to ensure that the overall dependability objectives are met.

The level of human engineering effort required should be consistent with the project application. The potential impact on its immediate environment in case of a system malfunction due to human error should be explored.

A.3 Element 3: Analysis, evaluation and assessment

Reliability and maintainability engineering employs various techniques and methods to solve dependability problems. The methodology may be quantitative or qualitative or both, but the solution should embrace sound engineering judgement and the use of successfully applied industry practices. Tasks 13 to 21 describe the most common methods used in the analysis, evaluation and assessment element.

A.3.1 Task 13: Analysis of application environment

Product specifications need clear definitions of the operating scenario to be established. The application environment conditions applicable to products should be specified in terms of specific performance characteristics and established standard limits. This permits product environment classifications and identification of applicable environmental exposures to facilitate product design to meet anticipated operating environment and exposures. Typical

l'exposition prévus. Les expositions-types du produit aux conditions de l'environnement d'utilisation concernent les interférences électromagnétiques, les conditions climatiques et les contraintes mécaniques. Il est essentiel d'analyser l'environnement d'utilisation du produit afin d'assurer que la conception du produit respecte les conditions de fonctionnement et les objectifs de performance.

A.3.2 Tâche 14: Modélisation et simulation de la fiabilité

Il convient d'utiliser la modélisation et la simulation de la fiabilité le cas échéant pour évaluer les performances de disponibilité d'un produit. Les techniques de modélisation et de simulation fournissent une approche analytique permettant de garantir les conditions de fonctionnement prévues et les caractéristiques de performance du produit dans des situations normales et défavorables. Ces techniques sont utiles dans chaque phase initiale de concept et de définition du produit afin de déterminer l'ampleur des problèmes techniques impliqués, et dans la phase de conception et de développement pour examiner les caractéristiques de performance à des fins de compromis de conception et d'atténuation des risques. L'incidence du coût du cycle de vie dans la conception du produit est significative sur la sûreté de fonctionnement du produit en raison de la découverte précoce et du savoir-faire acquis sur les caractéristiques de performance pour les mesures de réduction des coûts.

Il convient que la modélisation et la simulation de la fiabilité permettent de déterminer les causes et effets des environnements et contraintes de performance du produit dans le cadre de l'élaboration de modèles, la définition de limites et d'hypothèses sur le système, la pertinence des données utilisées et l'interprétation des résultats de simulation qui peuvent influer sur les résultats du produit dans le processus de décision de l'entreprise.

Des informations sont présentées dans la CEI 60300-3-1.

A.3.3 Tâche 15: Evaluation et maîtrise des composants

L'évaluation et la maîtrise des composants pour l'application en conception et l'utilisation dans des assemblages de produits sont essentielles pour obtenir la sûreté de fonctionnement du produit. Il convient que l'importance de l'effort d'évaluation et de maîtrise des composants réponde aux besoins du projet. Cet effort est essentiel, notamment pour assurer que les produits standard (du commerce) choisis sont adéquats pour les applications prévues du produit. Il convient d'appliquer un processus de gestion de la chaîne d'approvisionnement si nécessaire. Il y a lieu d'appliquer les processus suivants:

– Il convient que la sélection des composants permette de déterminer les paramètres critiques et les spécifications des composants disponibles auprès de plusieurs fournisseurs potentiels. Il convient d'identifier les sources d'approvisionnement uniques ou limitées.

– Il y a lieu de revoir la capacité des fournisseurs potentiels à fournir les composants et de tenir compte d'affaires précédentes avec ces derniers. Ce processus est essentiel lors de l'acquisition de logiciels de série ou personnalisés pour les applications prévues du produit.

– Il est recommandé d'examiner les processus de fabrication et les méthodes d'assurance du fournisseur. La revue dans les locaux du fournisseur, si nécessaire, favorise la confiance et l'établissement de relations avec ce dernier.

– Il convient de s'assurer que le composant spécifié présente les caractéristiques fonctionnelles, physiques, de qualité et de fiabilité nécessaires pour l'application prévue. Cela est obtenu par la qualification, la vérification et la validation des composants, ainsi que par l'évaluation et les essais des nouveaux composants si nécessaire. Les éléments de sortie du processus permettent d'élaborer une liste de composants privilégiés avec des fournisseurs qualifiés. Il convient d'identifier les composants critiques dont l'organisme a besoin. Il y a lieu de mettre à jour les composants et les informations associées.

– Les composants critiques sont par exemple des composants ayant une durée de vie limitée, impliquant de longs délais de livraison, des composants critiques pour la sécurité ou les processus, des composants personnalisés, etc.

product exposures to the application environment conditions are electromagnetic interference, climatic conditions and mechanical stresses. Analysis of the product application environment is essential to assure that the product design adequately meets the operating conditions and performance objectives.

A.3.2 Task 14: Reliability modelling and simulation

Reliability modelling and simulation should be used where appropriate to assess the availability performance of a product. The modelling and simulation techniques provide an analytical approach to ascertain the expected product operating conditions and performance characteristics under normal and adverse situations. These techniques are useful in early product concept and definition phase to determine the magnitude of the technical problems involved, and in the design and development phase to examine the performance characteristics for design trade-off and risk mitigation. The life cycle cost implication in the product design is significant in affecting product dependability due to early discovery and the knowledge gained on performance characteristics for cost avoidance measures.

Reliability modelling and simulation should determine the cause and effects of product performance environments and constraints in model formulation, definition of system boundaries and assumptions, the relevancy of the data used and the interpretation of the simulation results that may impact product outcomes in the business decision process.

Guidance is provided in IEC 60300-3-1.

A.3.3 Task 15: Parts evaluation and control

Parts evaluation and control for design application and use in product assemblies are crucial in achieving product dependability. The extent of parts evaluation and control effort should be tailored to meet project needs. This effort is essential, especially to ensure that the commercial off-the-shelf items selected are suitable for the intended product applications. A supply-chain management process should be exercised where appropriate. The following processes should be applied:

– Parts selection should determine the critical parameters and specifications of the parts that are available from several potential suppliers. Sole source suppliers or limited supply sources should be identified.

– The capabilities of the potential suppliers in delivering the parts should be reviewed. Past business dealings with the suppliers should be taken into consideration. This process is critical when acquiring off-the-shelf software or customized software for the intended product applications.

– The supplier’s manufacturing processes and assurance methods should be examined. On-site review at the supplier’s premises, if needed, would gain confidence in establishing the relationships.

– The specified part should be ascertained to meet its functional, physical, quality and reliability characteristics for the intended application. This is achieved through parts qualification, verification and validation and evaluation and testing of new parts as necessary. The process output is to develop a preferred parts list with qualified suppliers. Critical parts needed by the organization should be identified. The parts and associated information should be kept current.

– Critical parts are, for example, those with limited shelf life, long lead items, safety or process critical parts, and customized components, etc.

– La maîtrise des composants implique de conserver des enregistrements des données relatives aux défaillances des composants et des non-conformités qui serviront pour une analyse ultérieure et une résolution des problèmes.

Il convient que la qualification des fournisseurs fasse partie d'un processus continu.

A.3.4 Tâche 16: Analyse de la conception et évaluation du produit

L'analyse de la conception est essentielle pour assurer que la conception respecte les spécifications du produit. Les méthodes d'analyse de la conception associées à la sûreté de fonctionnement incluent la modélisation et la simulation de la fiabilité (par exemple, analyse contrainte/résistance), la prédiction de fiabilité, l'analyse des modes de panne/défaillance et de leurs effets, l'analyse par arbre de pannes, les performances de sécurité et l'analyse des risques. L'évaluation du produit comprend les essais de vérification de la conception dans des environnements de fonctionnement simulés et les essais de validation du produit dans des conditions de fonctionnement sur site réelles.

En général, la méthodologie d'analyse des logiciels est fondée sur l'expérience pratique et les données d'essai sur des applications spécifiques de logiciels et les environnements de fonctionnement associés. Des modèles de performance des logiciels, y compris ceux qui essayent d'imiter les modèles de performance de la fiabilité des produits logiciels, sont élaborés pour des besoins de prédiction de la fiabilité et d'estimation de l'amélioration de la fiabilité. Ces modèles représentent les fonctions mathématiques liées à des paramètres de performance de logiciels spécifiques permettant de fournir des éléments de sortie quantitatifs en utilisant les éléments d'entrée des données d'ingénierie. Les modèles de fiabilité des logiciels qui analysent le comportement temporel peuvent être utilisés pour élaborer des prédictions. Ces modèles nécessitent une cartographie précise, depuis l'environnement d'essai jusqu'au profil opérationnel du système. Les modèles de performance des logiciels sont spécifiques selon les applications. Les pratiques industrielles élaborées pour l'analyse de logiciels spécifiques comprennent:

– l'analyse de la complexité des logiciels afin d'évaluer les éléments défaillants dans un ensemble donné de modules logiciels;
– l'analyse de la couverture des codes afin de déterminer l'exhaustivité des essais;
– la corrélation de la classification des défauts des logiciels pour une analyse rapide des causes profondes et l'amélioration en cours de processus.

Il convient de confirmer l'évaluation des produits de série au moyen du processus de gestion de la chaîne d'approvisionnement afin d'assurer la qualité et la sûreté de fonctionnement des produits utilisés pour l'intégration du système ou les assemblages de produits. Il convient d'encourager la collaboration pour faciliter les besoins d'introduction rapide sur le marché et éviter des coûts liés à la duplication des évaluations effectuées de manière indépendante.

Des méthodes génériques d'analyse de la sûreté de fonctionnement utilisées pour la conception et l'évaluation des produits sont présentées dans la CEI 60300-3-1. Des méthodes statistiques communes pour les applications et spécifications normalisées sont présentées dans l'ISO/TR 13425 et l'ISO/TR 10017.

A.3.5 Tâche 17: Impact des causes et effets et analyse du risque

Il convient d'analyser les causes de défaillances potentielles, leurs effets et leur impact sur les performances du produit afin de vérifier les aspects liés à la sécurité de la conception et de réduire au minimum les expositions dangereuses en cours d'exploitation. Parmi les méthodes d'analyse types, on trouve:

– l'analyse des modes de défaillance et de leurs effets (AMDE), qui est une méthode d'analyse de la sûreté de fonctionnement qualitative, du bas vers le haut, particulièrement adaptée à l'étude des défaillances des matériaux, composants et équipements et de leurs effets sur le niveau de système fonctionnel immédiatement supérieur. Des lignes directrices sont fournies dans la CEI 60812;

– Parts control includes maintaining a record on part failure data and non-conformances suitable for further analysis and resolutions.

Supplier qualification should be an on-going process.

A.3.4 Task 16: Design analysis and product evaluation

Design analysis is essential to ensure that the design meets product specifications. Design analysis methods associated with dependability include reliability modelling and simulation (e.g. load-strength analysis), reliability prediction, fault/failure modes and effects analysis, fault tree analysis, safety performance and risk analysis. Product evaluation includes design verification testing under simulated operating environments, and product validation testing in actual field operating conditions.

Software analysis methodology in general is based on practical experience and test data with specific software applications and associated operating environments. Software performance models, including those that emulate reliability performance of software products, are formulated for reliability prediction and reliability growth assessment purposes. These models represent the mathematical functions relating to specific software performance parameters to provide a quantitative output using the engineering data input. Software reliability models tracking behaviour of time can be used to make predictions. These models necessitate a clear mapping from the testing environment to the operational profile of the system. Software performance models are application specific. Industry practices developed for specific software analysis include:

– software complexity analysis to estimate the fault contents in a given set of software modules;
– analysis of code coverage to determine test completeness;
– correlation of software defects classification for rapid root-cause analysis and in-process improvement.

Commercial off-the-shelf product evaluation should be ascertained through the supply-chain management process to ensure quality and dependability of the products used for system integration or product assemblies. A joint collaborative effort should be employed to facilitate speed-to-market needs and cost avoidance of duplicating product evaluation efforts carried out independently.

Generic dependability analysis methods used in design and product evaluation is found in IEC 60300-3-1. Common statistical methods for standard applications and specifications are provided in ISO/TR 13425 and ISO/TR 10017.

A.3.5 Task 17: Cause-effect impact and risk analysis

Analysis of potential failure causes and their effects and impact to product performance should be conducted to verify the safety aspects of the design and to minimize risk exposures when in operation. Typical analysis methods include:

– failure mode and effects analysis (FMEA), which is a bottom-up, qualitative dependability analysis method, particularly suited to the study of material, component and equipment failures and their effects on the next higher functional system level. Guidelines are provided in IEC 60812;

– l'analyse par arbre de panne, qui est une approche du haut vers le bas pour l'analyse de la sûreté de fonctionnement et de la fiabilité du produit, concerne l'identification et l'analyse des conditions et des facteurs qui entraînent, ou contribuent à, l'apparition d'un résultat indésirable donné et qui affectent les caractéristiques spécifiées de performance, de sécurité, d'économie ou autres du produit. Des lignes directrices sont fournies dans la CEI 61025;

– l'analyse de Markov permet de déterminer les performances de disponibilité du système avec la probabilité relative aux transitions d'état entre l'état de défaillance et l'état de fonctionnement et vice versa. Des lignes directrices sont fournies dans la CEI 61165;

– l'analyse des risques technologiques permet de déterminer l'importance des expositions dangereuses et la probabilité d'occurrence d'événements. Des lignes directrices sont fournies dans la CEI 60300-3-9.

A.3.6 Tâche 18: Prédiction

Il convient d'effectuer des prédictions au cours de la phase initiale de conception et de développement et de les actualiser à mesure de l'avancement de la conception. Les résultats des prédictions permettent d'évaluer les performances de fiabilité du produit en termes de durée moyenne jusqu'à la défaillance, de durée moyenne entre les défaillances ou de taux de défaillances. Les performances de disponibilité des systèmes sont interprétées en pourcentage de durée de fonctionnement ou d'immobilisation sur une période d'exploitation spécifiée.

Il convient dans les prédictions associées aux produits de tenir compte de l'environnement d'application, de la charge et de la complexité du fonctionnement, de l'architecture de la configuration du système et des données empiriques sur lesquelles s'appuient les prédictions de performance de fiabilité des produits. Des informations sur l'utilisation de données sur les taux de défaillance pour les prédictions de fiabilité des composants dans les équipements électroniques sont fournies dans la CEI 61709. Des informations sur la présentation des prédictions de fiabilité, de maintenabilité et de disponibilité sont fournies dans la CEI 60863.

Trois approches génériques sont utilisées pour les méthodes de prédiction sur les logiciels. La première est fondée sur les propriétés du processus d'élaboration du logiciel. La seconde est fondée sur les caractéristiques du logiciel. La troisième est fondée sur des données empiriques recueillies au moyen du processus de vérification et dans le cadre du fonctionnement réel du logiciel.

Les modèles de prédiction dérivés des propriétés du processus d'élaboration des logiciels sont influencés par les paramètres du processus. Le concept est que les disciplines de management et d'ingénierie (c'est-à-dire la portée de la maîtrise des processus, le degré de rigueur technique, l'application de méthodes formelles, etc.) utilisées pour l'élaboration des logiciels pourraient fournir des cibles de projection de la fiabilité du logiciel. A cet égard, les paramètres du processus sont utilisés comme repères pour évaluer l'amélioration de la fiabilité.

Les modèles de prédiction dérivés des caractéristiques des logiciels sont influencés par les paramètres du logiciel tels que sa structure et sa complexité. Les prédictions de fiabilité fondées sur ces modèles sont généralement utilisées pour l'évaluation et l'analyse comparatives des logiciels de série.

Les modèles de prédiction dérivés des données de performance des logiciels sont influencés par l'application spécifique et l'environnement de fonctionnement du logiciel. Des méthodes statistiques sont utilisées pour les prédictions de fiabilité afin d'évaluer les projections de croissance de la fiabilité fondées sur les données observées.

– fault tree analysis (FTA), which is a top-down approach for analysing product dependability and reliability is concerned with the identification and analysis of conditions and factors that cause, or contribute to, the occurrence of a defined undesirable outcome and which affect product performance, safety, economy or other specified characteristics. Guidelines are provided in IEC 61025;

– Markov analysis to determine system availability performance with probability of state transitions from failed state to operating state and vice versa. Guideline is provided in IEC 61165;

– technological risk analysis to determine the extent of risk exposures and the probability of event occurrences. Guidelines are provided in IEC 60300-3-9.

A.3.6 Task 18: Prediction

Predictions should be conducted during the early design and development phase and updated as the design progresses. Prediction results provide assessments of product reliability performance in terms of mean-time-to-failure, mean-time-between-failures or in failure rates. Availability performance of systems is interpreted in percentage uptime or downtime duration over a specified operating period.

Predictions associated with products should consider the application environment, operating load and complexity, architecture of system configuration and the empirical data used to base the reliability performance predictions of the products. Guidance on the use of failure rate data for the reliability prediction of parts in electronic equipment is provided in IEC 61709. Guidance on the presentation of reliability, maintainability and availability predictions is provided in IEC 60863.

There are three generic approaches towards prediction methods for software. The first is based on the software development process properties. The second is based on the software product characteristics. The third is based on empirical data gathered from verification process and actual operation of the software.

Prediction models derived from software development process properties are influenced by the process parameters. The concept is that the management and engineering disciplines (i.e. extent of process control, degree of engineering rigour, application of formal methods, etc.) used for software development could provide reliability projection targets for the software. In this respect, the process parameters are used as benchmarks for reliability improvement.

Prediction models derived from software product characteristics are influenced by the software product parameters such as structure and complexity of the software. Reliability prediction based on such models is generally used for off-the-shelf software product evaluation and comparative analysis.

Prediction models derived from software performance data are influenced by the specific application and operating environment of the software. Statistical methods are used for reliability prediction to estimate reliability growth projection based on observed data.

A.3.7 Tâche 19: Analyse de compromis

Il convient d'effectuer l'analyse de compromis pendant la phase de concept et de définition et dans la phase initiale de conception et de développement afin de générer des éléments d'entrée appropriés pour la répartition de la fiabilité. L'analyse de compromis peut être effectuée pendant toute phase du cycle de vie en fonction du problème d'analyse. Il convient également d'effectuer une analyse de compromis proche de la fin de la vie du produit pour déterminer la valeur économique du maintien de la production ou du remplacement du produit. Il convient qu'une analyse du coût du cycle de vie vienne compléter l'analyse de compromis. L'analyse de compromis peut être efficacement utilisée pour choisir des options de conception, prendre des décisions de fabrication/d'achat et effectuer des analyses comparatives entre différentes solutions. Il convient d'utiliser l'analyse de compromis pour la décision concernant le choix d'une approche technologique appropriée ou d'une solution combinée de type matériel et logiciel dans l'architecture de calcul afin que les performances du système atteignent des objectifs rentables définis dans le projet.

A.3.8 Tâche 20: Détermination du coût du cycle de vie

Le coût du cycle de vie est déterminé pour obtenir une évaluation quantitative de la répartition des coûts du processus du cycle de vie en fonction de la structure de répartition des tâches et afin d'évaluer la répartition des ressources et les dépenses potentielles. Les résultats quantitatifs sont souvent étayés par des raisons de type qualitatif qui permettent de justifier les recommandations d'amélioration ou de modification. La détermination du coût du cycle de vie facilite les décisions de la direction concernant la maîtrise des projets. Une analyse de sensibilité est souvent effectuée pour identifier des situations de type «si». Les résultats de l'analyse du cycle de vie peuvent être utilisés pour

– orienter la répartition et les compromis parmi les objectifs de sûreté de fonctionnement;
– identifier les facteurs de sûreté de fonctionnement critiques et leur impact sur les coûts;
– choisir des options de conception et des alternatives de logistique;
– optimiser les caractéristiques des performances de disponibilité en fonction de contraintes de coût de cycle de vie données;
– sélectionner des méthodes de mise au rebut des produits pour réduire au minimum l'exposition environnementale et réduire les risques dans des limites budgétaires données.

Des lignes directrices sur la détermination du coût du cycle de vie sont présentées dans la CEI 60300-3-3.

A.3.9 Tâche 21: Croissance de la fiabilité

Il convient de mener des programmes de croissance de la fiabilité afin d'améliorer les performances de fiabilité du produit. Le processus de croissance de la fiabilité comprend des activités concernant l'identification des pannes, l'analyse des causes profondes, les actions correctives et la vérification de l'efficacité des actions correctives appliquées. Lorsque cela est possible et efficace, il convient de recommander des mesures préventives en vue de l'amélioration continue. La CEI 61014 fournit des informations sur l'élaboration de programmes et de procédures d'amélioration de la fiabilité. La CEI 61164 présente une méthodologie d'essai et d'estimation de l'amélioration de la fiabilité.

Des modèles de croissance de la fiabilité spécifiques applicables aux logiciels comprennent les éléments suivants:

– une représentation du processus de défaillance constituée d'un ensemble de formules mathématiques incorporant certains paramètres;
– une méthode d'estimation des paramètres par l'analyse de données de défaillance précédentes;
– une méthode de combinaison des valeurs paramétriques estimées avec les formules afin d'obtenir des estimations numériques des mesures de fiabilité.

A.3.7 Task 19: Trade-off analysis

Trade-off analysis should be conducted during the concept and definition phase and in the early design and development phase to provide timely inputs for reliability allocation. Trade-off analysis may be conducted during any phase of the life cycle, depending on the analysis problem. Trade-off analysis should also be performed near the end of life of the product to determine the economic value of sustain operation or for replacement. Life cycle cost analysis should complement the trade-off analysis.

Trade-off analysis can be effectively used for selection of design options, make/buy decisions, and comparative analysis for alternate solutions. Trade-off analysis should be used for decision-making to select an appropriate technology approach, an alternate hardware or software approach, or a combined hardware and software solution in the design architecture to achieve system performance to meet cost-effective project objectives.

A.3.8 Task 20: Life cycle costing

Life cycle costing is conducted to provide quantitative assessment of cost breakdown of the life cycle process related to the work breakdown structure to assess resource allocations and potential expenditures. The quantitative results are often supported by qualitative rationale to justify recommendations for enhancement or changes. Life cycle costing facilitates management decision in the control of projects. Sensitivity analysis is often performed to determine “what-if” situations. Results of the life cycle analysis can be used to

– guide the allocation and trade-off amongst dependability objectives;
– identify critical dependability factors and impact on costs;
– choose design options and support alternatives;
– optimize availability performance characteristics under given life cycle cost constraints;
– select product disposal methods to minimize environmental exposure and for risk reduction within given cost limits.

Guidelines for life cycle costing are provided in IEC 60300-3-3.

A.3.9 Task 21: Reliability growth

Reliability growth programmes should be conducted for the purpose of improving product reliability performance. The reliability growth process includes activities on fault identification, root-cause analysis, corrective actions and verification of the effectiveness of the corrective actions taken. Where possible and practical, preventive measures should be recommended for continual improvement. IEC 61014 provides guidance for development of reliability growth programmes and procedures. IEC 61164 provides a methodology for reliability growth testing and estimation.

Specific reliability growth models applicable to software consist of the following elements:

– a representation of the failure process by a set of mathematical formulae incorporating certain parameters;
– a method of estimating the parameters by analysis of previous failure data;
– a method of combining the estimated parametric values with the formulae to obtain numerical estimates of reliability measures.

A.4 Elément 4: Vérification et validation

Il convient de vérifier la fiabilité et la maintenabilité de la conception du produit afin d'assurer la conformité aux spécifications de la conception. Il convient de valider les caractéristiques de performance associées à la sûreté de fonctionnement pendant la mise en service ou au début de la phase d'exploitation et de maintenance afin de confirmer que les caractéristiques de performance spécifiques associées aux objectifs de sûreté de fonctionnement ont été respectées. Il y a lieu que la vérification et la validation fassent partie du processus de revue. Les tâches 22 à 24 décrivent l'élément de vérification et de validation.

A.4.1 Tâche 22: Stratégie de vérification et de validation

Il convient de planifier les activités de vérification et de validation.

Il y a lieu que la stratégie de vérification comprenne si possible une simulation et des essais sur le produit afin de déterminer l'adéquation des fonctions de conception relatives à la sûreté de fonctionnement et d'évaluer les limites de performance des caractéristiques de fiabilité et de maintenabilité soumises à des conditions environnementales données et des contraintes de charge. Il convient que la stratégie de vérification ait pour objet de confirmer les performances fonctionnelles et physiques des modèles d'ingénierie ou des prototypes par l'évaluation, la qualification et des essais environnementaux.

Il y a lieu d'effectuer la stratégie de validation sur le produit final dans des conditions de fonctionnement définies lorsque la situation le permet. Il convient d'appliquer le processus de validation en commun avec le client lorsque le système est installé dans les locaux du client. Il convient de documenter les résultats de la validation en tant que preuve pour l'acceptation du système.

A.4.2 Tâche 23: Démonstration de la sûreté de fonctionnement

La démonstration de la sûreté de fonctionnement est une forme d'essai d'acceptation. Pour les grands systèmes complexes, il convient d'effectuer la démonstration immédiatement avant ou pendant la mise en service du système pour l'acceptation du client. Pour les dispositifs fonctionnels ou les composants, la démonstration s'inscrit généralement dans des programmes d'essai spéciaux tels que des essais de durée de vie ou des essais de durée de vie accélérée.

L'objectif de ces essais est de démontrer l'adéquation des performances dans l'atteinte des objectifs. Lorsque cela est possible et économiquement réalisable, il convient d'effectuer les essais de démonstration en conjonction avec d'autres essais planifiés applicables au projet, dans des conditions d'essai similaires. Cela permet d'obtenir une validation des performances plus réaliste par rapport aux critères d'acceptation. Il convient de documenter les procédures d'essai en détaillant les mesures et les conditions d'essai. Il convient d'enregistrer les données d'essai afin d'obtenir des informations appropriées pour l'analyse des résultats de performance en vue de l'acceptation du produit.

Les essais d'acceptation des logiciels sont associés à la stratégie de vérification et de validation des logiciels. Il existe trois niveaux d'essai de logiciels pour l'acceptation :

– les essais de chaque sous-système et module de logiciel afin d'assurer la conformité aux spécifications ou normes établies ;
– les essais d'unités intégrées et des ensembles de composants de logiciels, généralement appelés essais d'intégration ;
– les essais d'installation du logiciel pour la mise en service et l'acceptation finale afin d'assurer que le logiciel fonctionne dans un système configuré pour opérer dans un environnement réel et des conditions établies conformément aux exigences contractuelles ou aux spécifications d'essai.

A.4 Element 4: Verification and validation

The reliability and maintainability of the product design should be verified for conformance to design specifications. The performance characteristics associated with dependability should be validated during commissioning or early in the operation and maintenance phase to confirm that the specific performance characteristics associated with dependability objectives have been met. Verification and validation should form part of the review process. Tasks 22 to 24 describe the verification and validation element.

A.4.1 Task 22: Verification and validation strategy

Verification and validation activities should be planned.

The verification strategy should include, where practical, product simulation and tests to determine the adequacy of the dependability design functions and evaluate the performance limits of reliability and maintainability characteristics subject to environmental and stress load conditions. The aim of the verification strategy should be to confirm the functional and physical performance of engineering models or prototypes by evaluation, qualification and environmental testing.

The validation strategy should be performed on the final product under defined operating conditions when practical and feasible. The validation process should be conducted jointly with the customer where the system is normally installed in the customer's premise. Validation results should be documented as proof for system acceptance.

A.4.2 Task 23: Dependability demonstration

Dependability demonstration is a form of acceptance test. For large complex systems, the demonstration should be conducted just prior to or during system commissioning for customer acceptance. For functional devices or parts, the demonstration is usually conducted in special test programmes such as life testing or accelerated life testing.

The objective of these tests is to demonstrate performance adequacy in meeting intended objectives. Where possible and economical, demonstration testing should be conducted in conjunction with other planned tests applicable to the project, under similar test conditions. This would provide a more realistic performance validation of the test results against acceptance criteria. Test procedures should be documented detailing the test measurements and test conditions. Test data should be recorded to provide adequate information for analysis to determine the performance results for product acceptance.

Acceptance testing for software is associated with software verification and validation. There are three levels of testing of software for acceptance:

– testing of each software subsystem and module to ensure conformance to established specifications or standards;
– testing of integrated software units and components as an aggregate, generally known as integration testing;
– testing of the software installation for commissioning and final acceptance to ensure that the software works in the system configured to operate in the actual environment and established conditions as specified in the contract requirements or test specifications.

A.4.3 Tâche 24: Déverminage sous contraintes

Le déverminage sous contraintes est un processus qui utilise des conditions environnementales et/ou opérationnelles comme moyen de détection des failles. Ces failles sont cachées, elles peuvent être dues à une qualité d'exécution médiocre ou à des défaillances dans le processus de conception ou de fabrication. La méthode de déverminage sous contraintes permet de transformer les défauts latents ou cachés des dispositifs et des composants en défaillances permanentes détectables par des essais normaux.

Le déverminage sous contraintes est une méthode d'amélioration de la fiabilité pour les produits matériels. Des installations et équipements d'essai spéciaux peuvent être nécessaires et le déverminage est souvent effectué en conjonction avec des essais accélérés. Des lignes directrices sur le déverminage sous contraintes sont présentées dans la CEI 60300-3-7, dans la CEI 61163-1 et la CEI 61163-2[1].

A.5 Elément 5: Base de connaissances

Une base de connaissances de la sûreté de fonctionnement est une condition préalable essentielle pour le fonctionnement efficace et efficient d'un organisme. Le recueil de données pertinentes sur la sûreté de fonctionnement et les informations et connaissances acquises au moyen d'innovations technologiques, d'améliorations de processus et de connaissance du marché procurent un avantage commercial. La base de connaissances retenue par un organisme joue un rôle important dans la compétition pour la prédominance et pour le déploiement stratégique des produits afin de répondre rapidement aux demandes du marché. Il convient de considérer la protection de la compétence et de la connaissance comme un point essentiel d'une stratégie de gestion de l'information. Les tâches 25 à 28 décrivent les éléments de la base de connaissances.

A.5.1 Tâche 25: Etablissement de la base de connaissances

Il convient d'établir une base de connaissances sur la sûreté de fonctionnement qui correspond aux activités de l'entreprise. Cela permet d'assurer que des informations adéquates et à jour sur la sûreté de fonctionnement sont disponibles pour soutenir les activités courantes concernant la gamme de produits et pour développer de nouveaux marchés. Il y a lieu que la base de connaissances sur la sûreté de fonctionnement comprenne:

– des informations sur la conception du produit et concernant la sûreté de fonctionnement;

– des données sur les performances du produit tirées du fonctionnement sur site; et

– des informations des fournisseurs sur la fiabilité et la qualité des composants.

Il convient que les informations sur la conception du produit ayant trait à la sûreté de fonctionnement incluent les objectifs de la conception, les spécifications de sûreté de fonctionnement, des lignes directrices sur l'utilisation des composants, des données prédictives sur la fiabilité et la maintenabilité, les sources des modèles de fiabilité et de maintenabilité, des informations sur les essais et l'historique d'acceptation du produit, si nécessaire.

Il convient que les données de performance du produit incluent des tendances de croissance de la fiabilité du produit, des informations sur la logistique de maintenance, des retours sous garantie, des rapports d'incident et résolutions de suivi, des réclamations de clients et des retours d'information (voir la CEI 60300-3-2).

Il y a lieu que les informations des fournisseurs incluent l'historique de fiabilité des composants, les limites d'application de la fiabilité des dispositifs, des données sur le déverminage et le contrôle, les critères de qualification et les sources des fournisseurs privilégiés.

---

[1] D'autres parties sont à l'étude.

A.4.3 Task 24: Reliability stress screening

Reliability stress screening is a process using environmental and/or operational stresses as a means of detecting flaws. These flaws are hidden flaws, which may be due to poor workmanship or deficiencies in the design or manufacturing process. The reliability stress screening method permits the latent or hidden defects embedded in the devices and parts to be precipitated into hard failure for normal test detection.

Reliability stress screening is a reliability improvement method for hardware products. Special test facilities and equipment may be needed and screening is often conducted in conjunction with accelerated testing. Guidelines for reliability stress screening are provided in IEC 60300-3-7 and in IEC 61163-1 and IEC 61163-2[1].

A.5 Element 5: Knowledge base

A dependability knowledge base is a critical prerequisite for effective and efficient operation in an organization. The relevant dependability data capture, and the information and knowledge gained through technology innovations, process enhancements and market intelligence provide a competitive business advantage. The knowledge base retained by an organization plays a significant role in leadership challenge and strategic deployment of products to meet timely market demands. The focal point for competence and knowledge retention should be treated as a strategic information resource. Tasks 25 to 28 describe the knowledge base elements.

A.5.1 Task 25: Knowledge base establishment

A dependability knowledge base relevant to the organization's business should be established. This ensures that adequate and up-to-date dependability information is available to support on-going business relating to the product portfolio as well as for new market development. The dependability knowledge base should include:

– product design information relevant to dependability;
– product performance data gathered through field service operation; and
– suppliers' information on reliability and quality of parts.

Product design information relevant to dependability should include product design objectives, dependability specifications, guidelines for part application, reliability and maintainability prediction data and reliability and maintainability model sources, test yield information and product acceptance history, as necessary.

Product performance data should include product reliability growth trends, maintenance support information, warranty returns, incident reports and follow-up resolutions, customer complaints and feedback information (see IEC 60300-3-2).

Supplier information should include part reliability history, device reliability application limits, screening and inspection data, qualification criteria and preferred suppliers' sources.

---

[1] Other parts are under consideration.

A.5.2 Tâche 26: Analyse des données

L'analyse des données est essentielle pour obtenir des tendances sur la sûreté de fonctionnement et identifier des anomalies afin de mener des actions préventives ou correctives, le cas échéant. L'analyse des données issues des tests élémentaires, des résultats d'essai, des données de performance sur site ou d'autres sources pertinentes, peut fournir un aperçu et des informations utiles telles que le suivi de la croissance de la fiabilité, des indications sur la maturité pour les versions de logiciel et les problèmes systématiques pour l'analyse des causes profondes. Il y a lieu de justifier et de revoir toutes les données analysées pour faciliter les décisions de la direction et les actions de suivi afin de contribuer au processus d'amélioration continue.

A.5.3 Tâche 27: Collecte et diffusion des données

Il convient que le système de collecte et de diffusion des données se concentre sur le recueil de données auprès de sources pertinentes et la diffusion rapide des informations essentielles aux responsables qui en ont besoin pour prendre des décisions. Des données factuelles sont essentielles pour l'amélioration de la sûreté de fonctionnement et la prise de décisions. Il convient que l'interprétation des données s'appuie sur des motifs permettant de justifier les recommandations d'investissements pour l'amélioration.

Les données-types recueillies et diffusées dans le système comprennent des données pertinentes sur les performances continues du produit, sur l'exploitation sur site et des retours d'information d'utilisateurs. Il convient d'inclure les résultats de l'évaluation du produit, des tests élémentaires, du processus de vérification et de validation des performances du produit, des revues et des enquêtes des fournisseurs dans les éléments d'acquisition de données. Il y a lieu que le système de collecte et de diffusion des données soit simple et approprié pour fournir les données nécessaires à l'analyse de la sûreté de fonctionnement et pour faciliter la prise de décision. Dans l'idéal, il convient que les données brutes associées aux défaillances de matériel, aux défauts de logiciel et aux erreurs de procédure puissent être facilement isolées en vue de leur analyse. Il convient donc de prendre en compte la conception de la procédure d'acquisition de données et l'établissement du système de collecte et de diffusion des données au regard de la rapidité et de l'efficacité d'exploitation. Il y a également lieu que le système de collecte et de diffusion des données soit utilisé dans le cadre de la classification de la documentation, des archives et de la récupération, de la maîtrise des données, de la sécurité et de la protection des informations.

A.5.4 Tâche 28: Enregistrements relatifs à la sûreté de fonctionnement

Il convient que les enregistrements liés à la sûreté de fonctionnement comprennent des données pertinentes sur la sûreté de fonctionnement requises dans les accords contractuels et pour des besoins de conformité avec la réglementation. Les enregistrements-types à conserver comprennent:

- l'historique de fiabilité du produit en vue de la sélection des sources de fournisseurs privilégiés;
- les rapports de fiabilité, de maintenabilité et de disponibilité;
- les informations sur la vérification et la validation venant à l'appui des tendances sur la maturité du produit et l'assurance de l'aptitude à l'emploi du produit;
- les rapports d'analyse des causes profondes pour obtenir des informations qui serviront aux activités de réduction des risques et de limitation des coûts;
- les enregistrements de démonstration de la sûreté de fonctionnement pour l'acceptation du produit;
- les enregistrements de poursuite et de garantie pour l'amélioration et la croissance.

La traçabilité (par exemple, marquage par code à barres) des sous-ensembles et des composants contribue largement à la valeur des enregistrements de la sûreté de fonctionnement. La durée de conservation des enregistrements dépend du contrat et des conditions statutaires.

A.5.2 Task 26: Data analysis

Data analysis is essential to provide dependability trends and to identify anomalies for initiation of preventive or corrective action, as appropriate. Analysis of data derived from test cases, test results, field performance data, or from other relevant sources could provide valuable insights and information such as monitoring reliability growth, maturity indication for software release and systemic problems for root-cause analysis. All analysed data should be interpreted with rationale and reviewed for management decisions and follow-up actions to affect the continual improvement process.

A.5.3 Task 27: Data collection and dissemination

Data collection and dissemination system should focus on data acquisition from relevant sources and prompt delivery of essential information to those responsible personnel needing the information for decision-making. Fact-based data is crucial to support dependability enhancement and business decisions. Data interpretation should provide rationale to justify recommendations for improvement investments.

Typical data collected and disseminated through the system include relevant data related to on-going product performance, field service operation and experience feedback from users. Results from product evaluation, test cases, and product performance verification and validation, reviews and suppliers' surveys should be included as part of the data acquisition. The data collection and dissemination system should be simple and adequate to provide the essential data necessary for analysis of dependability and supporting decision-making. In an ideal situation, the raw data associated with hardware failures, software faults and procedural errors should be easily segregated for further analysis. Hence the design of the data acquisition procedure and the establishment of a data collection and dissemination system should be considered for expediency and effectiveness in operation. The data collection and dissemination system should also be considered for use in documentation classification, archives and retrievals, data control, information security and protection.

A.5.4 Task 28: Dependability records

Dependability records should include relevant dependability data required by contract agreements and regulatory compliance purposes. Typical records suitable for retention include:

- product reliability history for selection of preferred supplier sources;
- reliability, maintainability and availability reports;
- verification and validation information to support product maturity trends and assurance of product fitness for use;
- root-cause analysis reports to gain knowledge for initiation of risk mitigation and cost avoidance effort;
- dependability demonstration records for product acceptance;
- field tracking and warranty records for improvement and enhancement.

Traceability (e.g. bar marking) of sub-assemblies and components adds significantly to the value of dependability records. The duration for record retention is subject to contract and statutory conditions.

A.6 Elément 6: Amélioration

L'amélioration est un processus essentiel pour assurer la pérennité et la croissance de l'entreprise par l'amélioration de ses processus et de ses produits. L'amélioration continue fournit l'élan nécessaire pour le développement durable. Les percées technologiques occasionnelles et les innovations apportées aux produits peuvent procurer des avantages commerciaux. La planification est essentielle pour mettre les efforts d'amélioration au service du retour sur investissements. Les tâches 29 à 32 décrivent les éléments concernant l'amélioration.

A.6.1 Tâche 29: Actions préventives et correctives

Des actions préventives sont menées pour éliminer les causes d'un problème potentiel ou d'une situation indésirable. Des actions correctives sont menées pour éliminer les causes d'un problème existant ou d'une situation indésirable. Les actions correctives sont menées pour prévenir la récurrence alors que les actions préventives sont menées pour prévenir l'occurrence.

Les actions préventives et correctives font partie du processus d'amélioration. Le succès ou l'efficacité des actions préventives ou correctives dépend de l'approche de mise en œuvre et des méthodes employées. Il convient d'utiliser un système d'information afin de faciliter l'application d'actions préventives ou correctives. Il y a lieu de répartir les responsabilités et de fixer des délais pour la réalisation ou la clôture des tâches. Il convient de vérifier le résultat des actions afin de juger de leur efficacité à résoudre un problème donné. Il convient de documenter et d'assurer la traçabilité des actions préventives et correctives pour des besoins de référence.

A.6.2 Tâche 30: Mise à niveau et modification

Il convient d'effectuer des mises à niveau en vue de l'amélioration du produit en ce qui concerne ses caractéristiques ou le renforcement de ses capacités. Il y a lieu d'effectuer des modifications dans le cadre de procédures de modification du produit. Les mises à niveau et les modifications reflètent généralement les résultats générés par l'application d'un processus d'amélioration et une mise en œuvre efficace. Il convient que les mises à niveau et les modifications se conforment au processus de gestion de configuration pour des besoins de traçabilité des enregistrements et pour faciliter l'analyse des données afin de définir des tendances d'amélioration. L'ISO 10007 fournit des informations sur la gestion de configuration.

Les mises à jour des logiciels sont normalement effectuées au cours de leur maintenance. On trouve par exemple l'amélioration des caractéristiques des logiciels, l'augmentation des capacités de stockage et la simplification des procédures administratives afin de réaliser des opérations rentables. Il convient de conserver les données d'événement des logiciels afin d'obtenir des indications sur les tendances d'amélioration. Il y a lieu de tenir compte de la maintenance corrective et de perfectionnement pour l'amélioration des logiciels dans le cadre du processus de maintenance. La maintenance de perfectionnement qui vise à l'amélioration des logiciels consiste à réduire les défauts de mise en œuvre des logiciels plutôt qu'à réagir face à l'apparition d'une défaillance du système.

Il convient que la maîtrise des modifications de matériel et de logiciels soit conforme au processus de gestion de configuration établi lorsque les procédures administratives et techniques appropriées sont appliquées. Cela permet d'identifier, d'enregistrer et de rendre compte de l'état d'avancement de la modification afin de garantir son exhaustivité, sa cohérence et son exactitude et d'assurer ainsi une qualité de service et une efficacité continues.

A.6 Element 6: Improvement

Improvement is a key process to ensure business survival and growth through the improvement of the business's processes and its products. Continual improvements provide the needed incentives for sustained development. Occasional technology breakthroughs and product innovations can generate competitive market advantage. Timing is critical to harness the improvement effort for return on investments. Tasks 29 to 32 describe the improvement elements.

A.6.1 Task 29: Preventive and corrective actions

Preventive action is taken to eliminate the cause of a potential problem or undesirable situation. Corrective action is taken to eliminate the cause of an existing problem or undesirable situation. The corrective action taken is to prevent recurrence whereas the preventive action taken is to prevent occurrence.

Preventive and corrective actions form part of the improvement process. The success or effectiveness of the preventive or corrective actions depend on the implementation approach and the methods employed. An information system should be used to facilitate initiation of preventive or corrective actions. Responsibility should be assigned with a designated timeline allotted for task completion or closure. The result of the action should be verified to determine its effectiveness in eliminating the problem. Preventive and corrective actions should be documented and traceable for reference.

A.6.2 Task 30: Upgrade and modification

Upgrade should be performed for product improvement concerning features or capability enhancement. Modification should be conducted in association with product change procedures. Upgrade and modification should reflect the results generated from improvement process initiation and effective implementation. They should conform to the configuration management process for traceability of records and facilitating data analysis to establish improvement trends. ISO 10007 provides guidance on configuration management.

Software upgrade is normally performed during software maintenance. Examples include software features enhancement, increased storage capabilities and simplification of administrative procedures to achieve cost-effective operations. Software event data should be maintained to provide indications of improvement trends. Corrective and "perfective" maintenance for software improvement should be considered in the maintenance process. Perfective maintenance for software enhancement is to reduce a shortcoming in the software implementation rather than reacting to a system failure occurrence.

Hardware and software modification control should conform to the established configuration management process where the appropriate administrative and technical procedures are applied. This is in order to identify, record and report on the status of the modification to ensure its completeness, consistency, and correctness for maintenance of continuous service quality and effectiveness.

A.6.3 Tâche 31: Développement et renforcement des compétences

Il convient de prendre en compte le développement des compétences du personnel pour renforcer la base de connaissances et définir les ressources consacrées à l'amélioration continue. Des compétences critiques sont essentielles pour la capacité de l'organisme à conserver sa puissance technologique et maintenir sa compétitivité sur le marché.

Les connaissances et compétences dans le domaine de la sûreté de fonctionnement peuvent être acquises en encourageant l'éducation formelle et la formation informelle sur le tas, en instituant des programmes de parrainage et d'apprentissage, et en participant à des systèmes de coopération entre l'industrie et les établissements de formation dans le cadre de cours de formation continue sur la gestion de la sûreté de fonctionnement en relation avec les progrès technologiques.

Il convient de considérer le renforcement des compétences comme des mises à jour techniques de court terme des connaissances sur la sûreté de fonctionnement. Cela peut être obtenu par une plus grande participation du personnel aux forums technologiques et aux séminaires professionnels sur des aspects pertinents de la sûreté de fonctionnement, par la création de réseaux et de groupes de discussion spécialisés dans la résolution de problèmes liés à la sûreté de fonctionnement, et par la formation d'équipes interdisciplinaires fonctionnelles afin d'acquérir de l'expérience dans la sûreté de fonctionnement au niveau de pratiques industrielles. Toutefois, dans des discussions aussi ouvertes, il convient de respecter les droits de propriété intellectuelle et les règles de non-divulgation de l'organisme.

A.6.4 Tâche 32: Amélioration du système de management

Il convient d'évaluer régulièrement l'efficacité du système de gestion de la sûreté de fonctionnement afin d'autoriser l'application du processus d'amélioration. Il y a lieu de tenir compte des activités suivantes pour l'amélioration du système de gestion de la sûreté de fonctionnement :

– il convient que la direction au plus haut niveau crée un environnement de travail et encourage des infrastructures propices à la créativité, l'efficacité, la prise de responsabilité, des résultats commerciaux réalisables et à la facilitation du processus d'amélioration de la sûreté de fonctionnement;

– la sûreté de fonctionnement découle souvent du marché et de technologies innovantes. Il y a lieu que l'organisme et ses employés modifient en permanence le processus de formation et renforcent leurs compétences et leur base de connaissances en matière de sûreté de fonctionnement;

– il y a lieu que la direction au plus haut niveau fixe des objectifs réalisables, des performances de référence et mette en œuvre l'élaboration de pratiques de sûreté de fonctionnement pour préserver la compétitivité de l'organisme;

– il y a lieu de communiquer et de partager de nouvelles idées visant à améliorer la sûreté de fonctionnement et à réduire les coûts au sein de l'organisme et parmi ses employés;

– il convient d'établir un programme de reconnaissance et de remise de prix afin de favoriser les résultats liés à l'amélioration;

– il convient de conserver des enregistrements de performance pertinents en tant que ressource d'information afin d'engager des activités d'amélioration de la sûreté de fonctionnement lorsque leurs avantages se justifient.

A.6.3 Task 31: Competence development and enhancement

Personnel competence development should be considered for knowledge base enhancement and resource investment for continual improvement. Critical competence is essential to the organization's ability to sustain technology leverage and maintain market competitiveness.

Dependability knowledge and competence can be achieved through encouragement of formal education and informal on-the-job training, instituting mentoring and apprenticeship programmes as well as and participation in industry-academic cooperation in continuous education courses on dependability management for technology advancement.

Competence enhancement should be considered as short-term technical updates on dependability knowledge infusion. This can be achieved by greater personnel exposure to technology forums and professional seminars on relevant dependability subjects, networking and focus group discussions in dependability problem solving, and cross functional teams to gain experience in dependability application of industry practices. However, in such open discussions, the intellectual property rights and non-disclosure rules of the organization should be followed.

A.6.4 Task 32: Management system improvement

The effectiveness of the dependability management system should be evaluated on a regular basis. This is to permit initiation of improvement process. The following activities should be considered for dependability management system improvement:

– top management should create a work environment and promote an infrastructure to encourage creativity, efficiency, empowerment, achievable business results and facilitation of the dependability improvement process;

– dependability is often driven by the market and innovative technology. The organization and its people should continually evolve a lifetime learning process and enhance its dependability competence and knowledge base;

– top management should set achievable objectives, benchmark performance and development of dependability practices for competitive leverage;

– new ideas for dependability improvement and cost avoidance issues should be communicated and shared within the organization and its people;

– a recognition and award programme should be established to encourage achievement of improvement results;

– relevant performance records should be maintained as an information resource to launch dependability improvement efforts when its benefits justify it.

Annexe B
(informative)

Phases du cycle de vie du produit

B.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 induits par le produit sont établis et ses objectifs spécifiés. Pendant cette phase, les bases de la sûreté de fonctionnement du produit et des implications du coût de son cycle de vie sont établies. Les décisions prises au cours de cette phase sont déterminantes pour les fonctions de performance du produit et les coûts de propriété.

Il convient d'établir un plan de sûreté de fonctionnement afin de guider les phases ultérieures. Il convient que les tâches du programme de sûreté de fonctionnement appliquées pendant la phase de concept et de définition s'attachent à atteindre les objectifs prévus pour le produit et à déterminer les principaux besoins en soutien afin de venir à l'appui des fonctions de performance. Il convient d'envisager l'élaboration et l'évaluation d'autres approches pendant la phase de concept et de définition.

B.2 Phase de conception et de développement

La phase de conception et de développement est la phase du cycle de vie pendant laquelle l'architecture du système, le matériel et/ou le logiciel sont créés. Les informations pertinentes sur le produit sont recueillies et documentées pour faciliter la fabrication et l'assemblage ultérieurs du matériel, le codage et la réplication du logiciel et l'intégration du système.

Il convient que les tâches du programme de sûreté de fonctionnement appliquées pendant la phase de conception et de développement permettent d'assurer l'adéquation des spécifications de conception de la sûreté de fonctionnement, l'exhaustivité des activités de vérification et de validation de la conception avant sa mise à disposition et la capacité d'application de la stratégie de logistique de maintenance pour l'exploitation du produit, la logistique de maintenance et la mise au rebut en fin de vie. Il y a lieu d'appliquer une gestion de configuration conforme à l'ISO 10007 pour l'identification, la traçabilité et la maîtrise du produit. Le cas échéant, il y a lieu d'évaluer les modifications de conception au regard de leur impact potentiel sur la dégradation de la sûreté de fonctionnement et des performances. Il convient de clairement identifier les produits fournis par le client pour l'intégration du système dans le cadre de la coordination du projet.

B.3 Phase de fabrication

La phase de fabrication est la phase du cycle de vie pendant laquelle le produit est fabriqué, le logiciel est répliqué et les composants du système sont assemblés.

Il convient que les tâches du programme de sûreté de fonctionnement appliquées pendant la phase de fabrication permettent d'établir la conformité avec les processus établis et avec les objectifs de performance spécifiés par la vérification et la validation des résultats d'essai. Lorsque cela est nécessaire et approprié, il y a lieu d'appliquer un processus de maîtrise pour surveiller les données d'efficacité des essais et ainsi établir des tendances sur l'efficacité du processus d'acceptation du produit en vue de réduire les retours sur site précoces. Une méthode de déverminage sous contraintes peut être appliquée lorsqu'il est nécessaire et pratique de supprimer les défauts latents. Il convient de déterminer les causes profondes des aspects liés à la sûreté de fonctionnement des problèmes de non-conformité en vue d'améliorer le produit ou les processus.

Annex B
(informative)

Product life cycle phases

B.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 objectives specified. During this phase, the foundation is laid for the product's dependability and its life cycle cost implications. Decisions made during this phase have the greatest impact on the product performance functions and ownership costs.

A dependability plan should be established to guide subsequent phases. The dependability programme tasks applied during the concept and definition phase should focus on meeting intended product objectives and for determining the essential support needs to sustain dependable performance functions. Development and evaluation of alternative approaches should be considered during the concept and definition phase.

B.2 Design and development phase

The design and development phase is the life cycle phase during which the system architecture, hardware and/or software are created. The relevant product information are captured and documented to facilitate subsequent hardware manufacturing and assembly, software coding and replication and system integration.

The dependability programme tasks applied during the design and development phase should ensure the adequacy of the dependability design specifications, the completeness of design verification and validation prior to design release, and the applicability of the maintenance support strategy for product operation, maintenance support and end of life disposal. Configuration management in accordance with ISO 10007 should be initiated for product identification, traceability and control. Where appropriate, design changes should be evaluated for their potential impact on dependability and performance degradation. Customer supplied products for system integration should be clearly identified for project coordination.

B.3 Manufacturing phase

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

Dependability programme tasks applied during the manufacturing phase should focus on conformance to established processes for consistent quality output and compliance to specified performance objectives through verification and validation of test results. Where necessary and appropriate, a control process should be initiated to monitor test yield data to establish product acceptance yield trends that link to reducing early field returns. Reliability stress screening may be deployed when needed and practical to remove latent defects. Dependability focus on non-conformance issues should address root-cause problems for product or process improvement.

B.4 Phase d'installation

La phase d'installation est la phase du cycle de vie pendant laquelle le produit est mis en place pour l'application et l'exploitation. Les activités correspondantes englobent l'installation du système, l'intégration des fonctions de logistique de maintenance et l'introduction du nouveau produit dans le matériel et le logiciel installés pour des essais sur site. Le système intégré ou le produit final est soumis au processus de démonstration des performances dans l'environnement de travail réel en vue de l'acceptation finale pour exploitation.

B.5 Phase d'exploitation et de maintenance

La phase d'exploitation et de maintenance est la phase du cycle de vie pendant laquelle le produit est utilisé pour son usage prévu. Le cas échéant, le produit est conservé pour son exploitation continue. La durée de vie utile du produit s'achève lorsque son exploitation devient non rentable en raison de coûts de logistique de maintenance accrus ou d'autres facteurs tels que l'obsolescence technique ou des dommages non réparables.

Il convient que les tâches du programme de sûreté de fonctionnement appliquées pendant la phase d'exploitation et de maintenance permettent d'assurer que les performances du produit sont surveillées; les résultats relatifs aux performances sont recueillis pour faciliter les actions préventives et correctives dans le cadre des activités de logistique de maintenance. Le cas échéant, les processus de collecte des données, de compte rendu et d'analyse des défaillances, de logistique de maintenance et de soutien logistique intégré sont déployés pour contribuer à la réalisation des objectifs.

B.6 Phase de mise au rebut

La phase de mise au rebut est la phase du cycle de vie pendant laquelle la durée d'utilisation du produit s'achève, le produit est retiré de son site d'exploitation, démantelé, détruit, recyclé ou le cas échéant, stocké.

Il convient que les tâches du programme de sûreté de fonctionnement appliquées pendant la phase de mise au rebut soient conformes le cas échéant, aux exigences réglementaires et environnementales sur le recyclage et la réutilisation de matériels désassemblés et sur les moyens de destruction ou de mise au rebut à la fin de la durée de vie du produit. Lors de la phase de mise au rebut, il convient de tenir compte des accords contractuels sur les questions de «reprise» et de «rachat» ainsi que des obligations statutaires.

B.4 Installation phase

The installation phase is the life cycle phase during which the product is put in place for application and operation. The activities involve system installation, maintenance support functions integration and new product introduction of the installed hardware and software for field trials. The integrated system or end product is put through its performance demonstration in an actual operating environment prior to final acceptance for operation.

B.5 Operation and maintenance phase

The operation and maintenance phase is the life cycle phase during which the product is used for its intended purpose. Where applicable, the product is maintained for its continual operation. The useful life of the product ends when its operation becomes uneconomical to run due to increased maintenance support costs or other factors such as technology obsolescence or damage beyond salvage.

Dependability programme tasks applied during the operation and maintenance phase should ensure that the product performance is monitored; its performance results are captured to facilitate preventive and corrective actions in its maintenance support effort. Where applicable, data collection, failure reporting and analysis, maintenance support and integrated logistic support processes are deployed to help achieve product performance objectives.

B.6 Disposal phase

The disposal phase is the life cycle phase during which the product is terminated from use, removed from its operation site, dismantled, destroyed, recycled or, where appropriate, put in storage.

Dependability programme tasks applied during the disposal phase should comply with the regulatory and environmental requirements, where applicable, concerning recycle and reuse of disassembled materials and the means of destroying or disposing of the end-of-life product. Contractual agreements concerning “take-back” and “buy-back” issues, as well as statutory obligations, should be taken into consideration at the disposal phase.

Annexe C
(informative)

Association des phases du cycle de vie du produit avec les éléments et les tâches applicables de la sûreté de fonctionnement

Légende

C et D Concept et définition

D et D Conception et développement

MFG Fabrication

INS Installation

O et M Exploitation et maintenance

DIS Mise au rebut

Eléments et tâches relatifs à la sûreté de fonctionnement	Phases du cycle de vie					
	C et D	D et D	MFG	INS	O et M	DIS
Elément 1: Management						
Tâche 1: Plan de sûreté de fonctionnement	xxx	xxx	xxx	xxx	xxx	xxx
Tâche 2: Spécifications de sûreté de fonctionnement		xxx	xxx	xxx		
Tâche 3: Maîtrise des processus		xxx	xxx	xxx	xxx	
Tâche 4: Maîtrise de la conception		xxx	xxx	xxx		
Tâche 5: Suivi et revue		xxx	xxx	xxx	xxx	xxx
Tâche 6: Gestion de la chaîne d'approvisionnement			xxx	xxx	xxx	xxx
Tâche 7: Introduction du produit				xxx	xxx	
Elément 2: Disciplines liées à la sûreté de fonctionnement						
Tâche 8: Ingénierie de la fiabilité	xxx	xxx	xxx			
Tâche 9: Ingénierie de la maintenabilité	xxx	xxx	xxx			
Tâche 10: Ingénierie de la logistique de maintenance		xxx	xxx	xxx	xxx	
Tâche 11: Normalisation		xxx	xxx	xxx	xxx	
Tâche 12: Facteurs humains	xxx	xxx	xxx	xxx	xxx	xxx
Elément 3: Analyse, évaluation et estimation						
Tâche 13: Analyse de l'environnement de travail	xxx	xxx	xxx			
Tâche 14: Modélisation et simulation de la fiabilité	xxx	xxx	xxx			
Tâche 15: Evaluation et maîtrise des composants		xxx	xxx			
Tâche 16: Analyse de la conception et évaluation du produit		xxx	xxx			
Tâche 17: Impact des causes et effets et analyse du risque		xxx	xxx	xxx	xxx	xxx
Tâche 18: Prédiction	xxx	xxx	xxx			
Tâche 19: Analyse de compromis	xxx	xxx	xxx			xxx
Tâche 20: Détermination du coût du cycle de vie	xxx	xxx	xxx	xxx	xxx	xxx
Tâche 21: Croissance de la fiabilité				xxx	xxx	

Annex C
(informative)

Association of product life cycle phases with the applicable dependability elements and tasks

Key

C&D Concept and definition
D&D Design and development
MFG Manufacturing
INS Installation
O&M Operation and maintenance
DIS Disposal

Dependability elements and tasks	Life cycle phases					
	C&D	D&D	MFG	INS	O&M	DIS
Element 1: Management						
Task 1: Dependability plan	xxx	xxx	xxx	xxx	xxx	xxx
Task 2: Dependability specifications		xxx	xxx	xxx		
Task 3: Control of processes		xxx	xxx	xxx	xxx	
Task 4: Design control		xxx	xxx	xxx		
Task 5: Monitoring and review		xxx	xxx	xxx	xxx	xxx
Task 6: Supply-chain management			xxx	xxx	xxx	xxx
Task 7: Product introduction				xxx	xxx	
Element 2: Dependability disciplines						
Task 8: Reliability engineering	xxx	xxx	xxx			
Task 9: Maintainability engineering	xxx	xxx	xxx			
Task 10: Maintenance support engineering		xxx	xxx	xxx	xxx	
Task 11: Standardization		xxx	xxx	xxx	xxx	
Task 12: Human factors	xxx	xxx	xxx	xxx	xxx	xxx
Element 3: Analysis, evaluation and assessment						
Task 13: Analysis of use environment	xxx	xxx	xxx			
Task 14: Reliability modelling and simulation	xxx	xxx	xxx			
Task 15: Parts evaluation and control		xxx	xxx			
Task 16: Design analysis and product evaluation		xxx	xxx			
Task 17: Cause-effect impact and risk analysis		xxx	xxx	xxx	xxx	xxx
Task 18: Prediction	xxx	xxx	xxx			
Task 19: Trade-off analysis	xxx	xxx	xxx			xxx
Task 20: Life cycle costing	xxx	xxx	xxx	xxx	xxx	xxx
Task 21: Reliability growth				xxx	xxx	

Eléments et tâches relatifs à la sûreté de fonctionnement	Phases du cycle de vie					
	C et D	D et D	MFG	INS	O et M	DIS
Elément 4: Vérification et validation						
Tâche 22: Stratégie de vérification et de validation		xxx	xxx	xxx		
Tâche 23: Démonstration de la sûreté de fonctionnement				xxx	xxx	
Tâche 24: Déverminage sous contraintes			xxx			
Elément 5: Base de connaissances						
Tâche 25: Etablissement de la base de connaissances		xxx	xxx	xxx	xxx	xxx
Tâche 26: Analyse des données		xxx	xxx	xxx	xxx	xxx
Tâche 27: Collecte et diffusion des données		xxx	xxx	xxx	xxx	xxx
Tâche 28: Enregistrements relatifs à la sûreté de fonctionnement		xxx	xxx	xxx	xxx	xxx
Elément 6: Amélioration						
Tâche 29: Actions préventives et correctives		xxx	xxx	xxx	xxx	
Tâche 30: Mise à niveau et modification				xxx	xxx	
Tâche 31: Développement et renforcement des compétences	xxx	xxx	xxx	xxx	xxx	
Tâche 32: Amélioration du système de management	xxx	xxx	xxx	xxx	xxx	

Dependability elements and tasks	Life cycle phases					
	C&D	D&D	MFG	INS	O&M	DIS
Element 4: Verification and validation						
Task 22: Verification and validation strategy		xxx	xxx	xxx		
Task 23: Dependability demonstration				xxx	xxx	
Task 24: Reliability stress screening			xxx			
Element 5: Knowledge base						
Task 25: Knowledge base establishment		xxx	xxx	xxx	xxx	xxx
Task 26: Data analysis		xxx	xxx	xxx	xxx	xxx
Task 27: Data collection and dissemination		xxx	xxx	xxx	xxx	xxx
Task 28: Dependability records		xxx	xxx	xxx	xxx	xxx
Element 6: Improvement						
Task 29: Preventive and corrective actions		xxx	xxx	xxx	xxx	
Task 30: Upgrade and modification				xxx	xxx	
Task 31: Competence development and enhancement	xxx	xxx	xxx	xxx	xxx	
Task 32: Management system improvement	xxx	xxx	xxx	xxx	xxx	

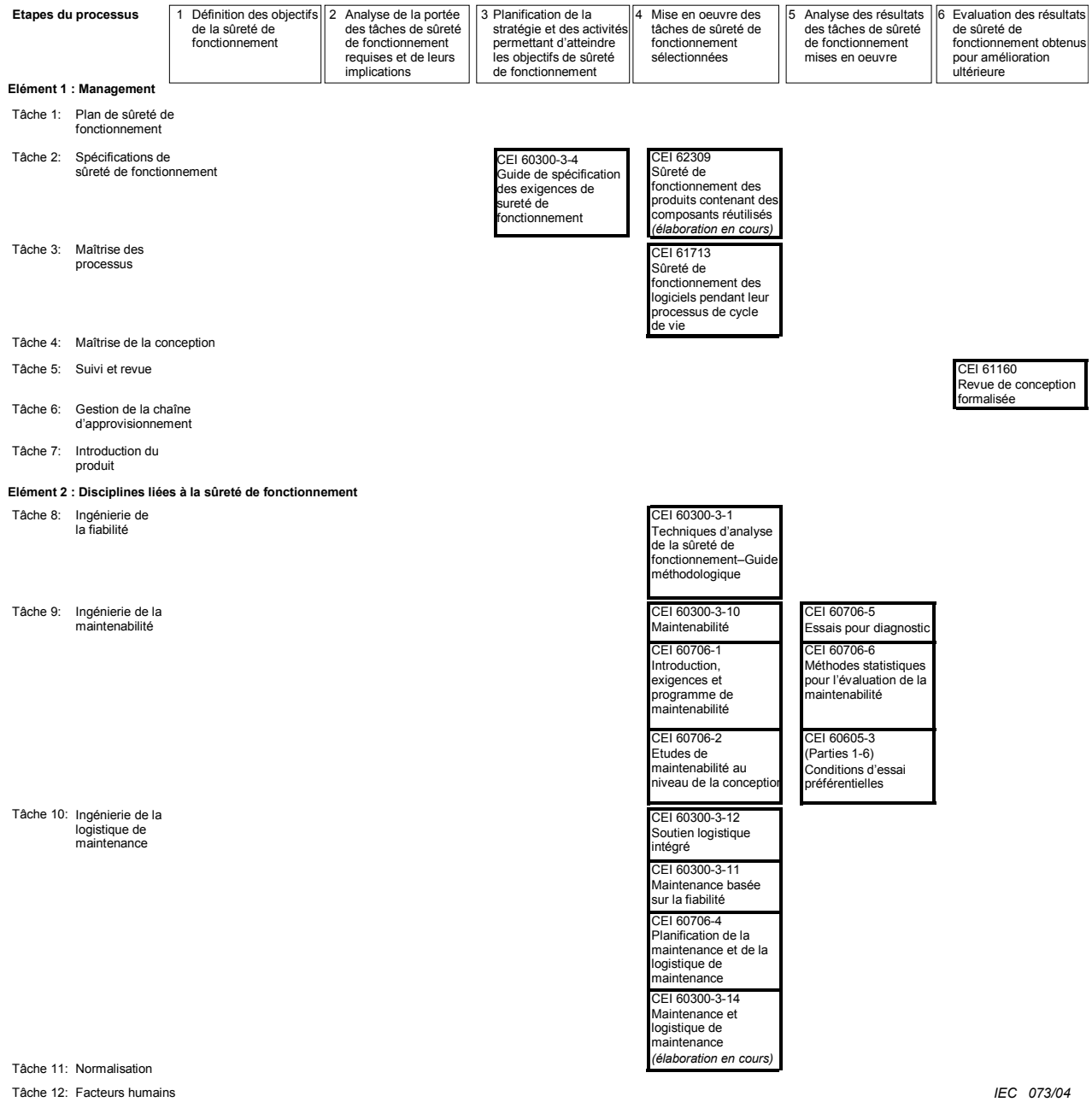
Annexe D
(informative)

Etapes de processus et normes relatives à la gestion de la sûreté de fonctionnement

Les normes de base suivantes sont génériques pour toutes les tâches et s'appliquent à toutes les étapes de processus:

CEI 60300-1, CEI 60300-2, CEI 60050(191) et CEI 61703.

Des normes-clés sur la sûreté de fonctionnement sont présentées dans la matrice suivante afin d'identifier l'utilisation des normes dans une tâche spécifique associée à l'étape de processus correspondante.



Annex D
(informative)

Process steps and standards for managing dependability

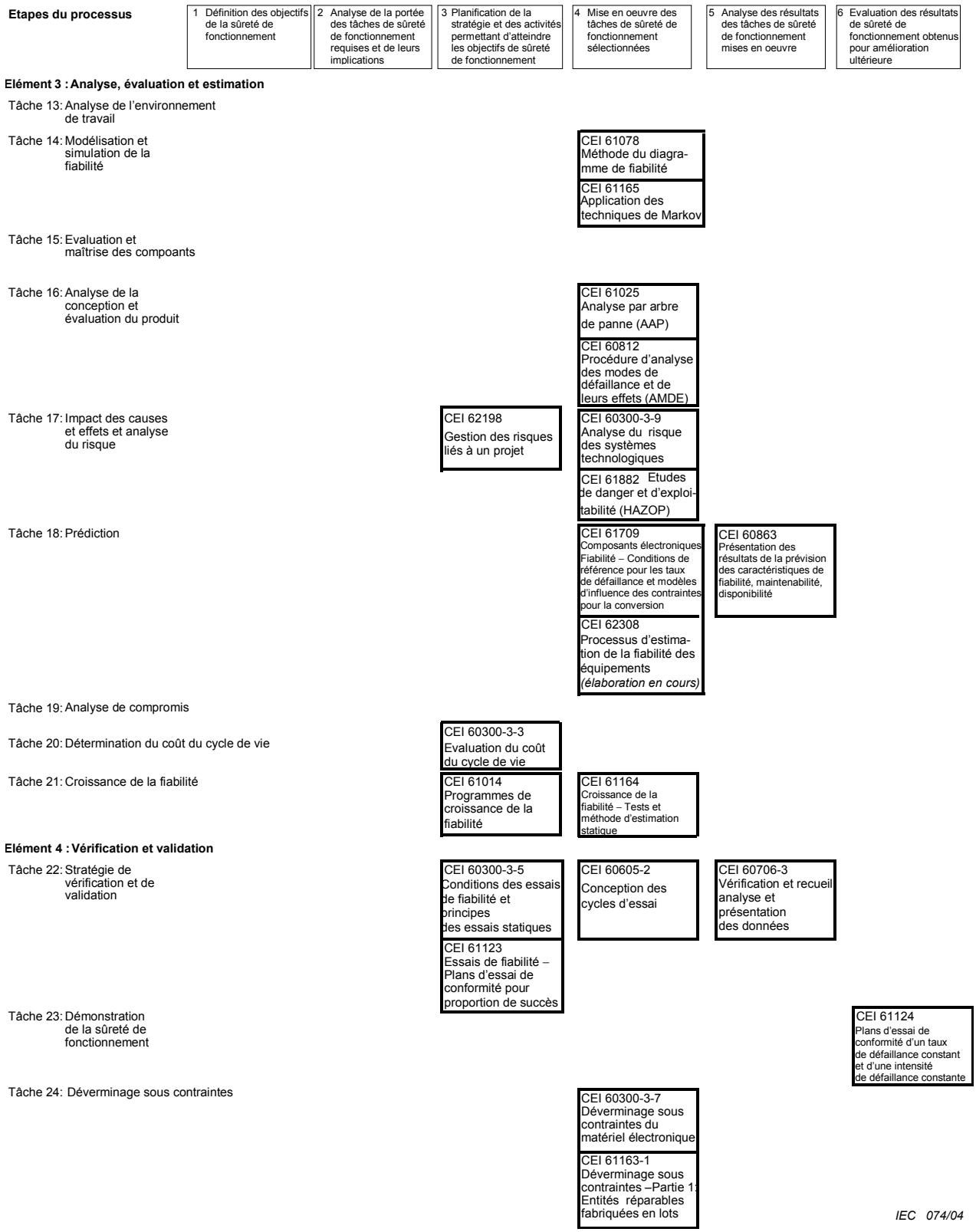
The following core standards are generic to all tasks and apply to all process steps:

IEC 60300-1, IEC 60300-2, IEC 60050(191) and IEC 61703.

Key dependability standards are presented in the following matrix in order to identify the use of the standards in a specific task associated with the relevant process step.

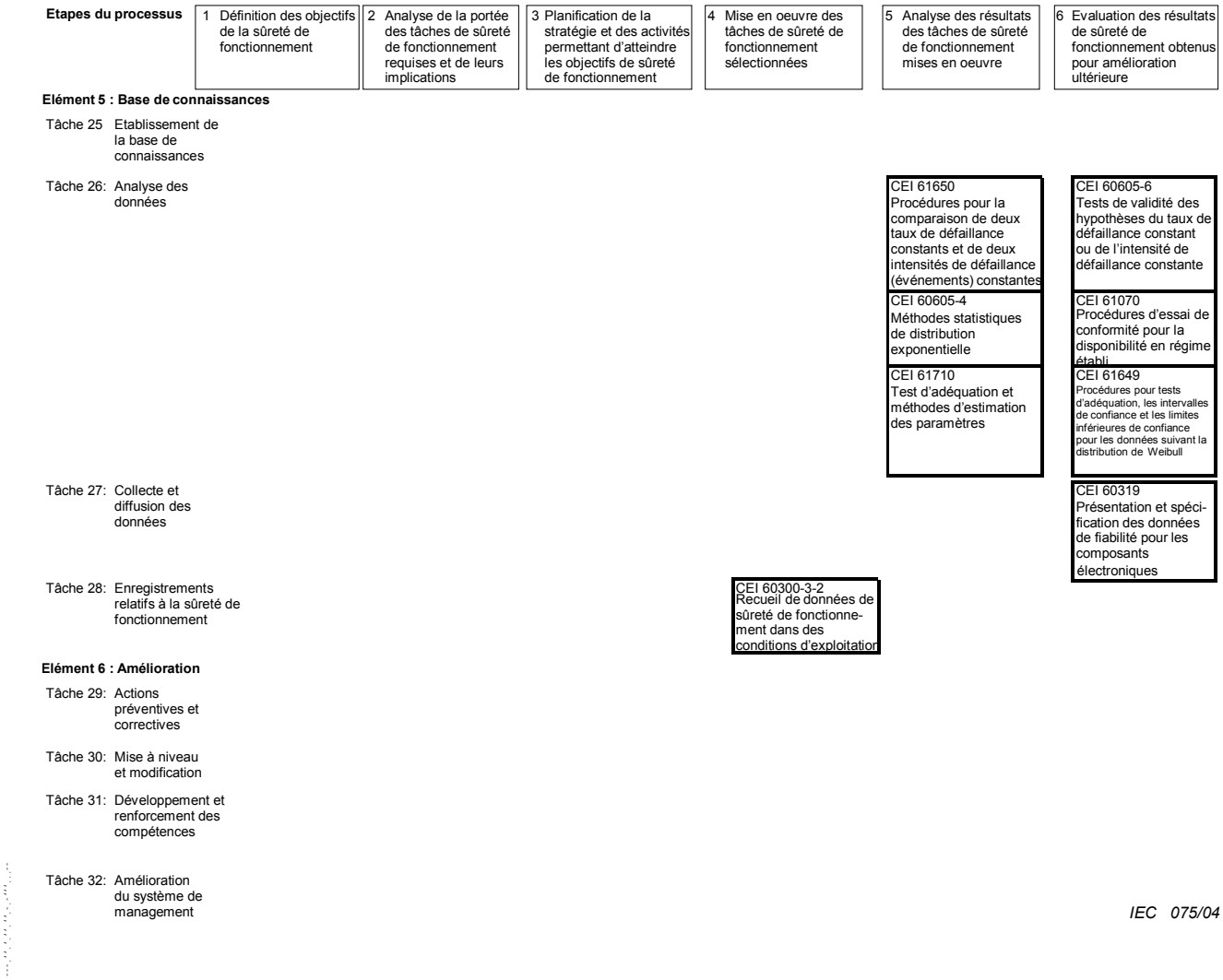
Process steps	1 Define dependability objectives	2 Analyze scope of dependability work needed and implications	3 Plan strategy and activities to achieve dependability objectives	4 Implement selected dependability activities	5 Analyze results of dependability activities implemented	6 Evaluate achieved dependability results for further improvement
Element 1: Management						
Task 1: Dependability plan						
Task 2: Dependability specifications			IEC 60300-3-4 Guide to the specification of dependablity requirements	IEC 62309 Dependability and quality of products containing used parts (*under development*)		
Task 3: Control of processes				IEC 61713 Guide to software dependability through the software life cycle processes		
Task 4: Design control						
Task 5: Monitoring and review						IEC 61160 Formal design review
Task 6: Supply-chain management						
Task 7: Product introduction						
Element 2: Dependability disciplines						
Task 8: Reliability engineering				IEC 60300-3-1 Analysis techniques for dependability: Guide on methodology		
Task 9: Maintainability engineering				IEC 60300-3-10 Maintainability IEC 60706-1 Introduction, requirements and maintainability programme IEC 60706-2 Maintainability studies during the design phase	IEC 60706-5 Diagnostic testing IEC 60706-6 Statistical methods in maintainability evaluation IEC 60605-3 (Parts 1-6) Preferred test conditions	
Task 10: Maintenance support engineering				IEC 60300-3-12 Integrated logistic support IEC 60300-3-11 Reliability centered maintenance IEC 60706-4 Maintenance and maintenance support planning IEC 60300-3-14 Maintenance and maintenance support		
Task 11: Standardization						
Task 12: Human factors						

IEC 073/04



Process steps	1 Define dependability objectives	2 Analyze scope of dependability work needed and implications	3 Plan strategy and activities to achieve dependability objectives	4 Implement selected dependability activities	5 Analyze results of dependability activities implemented	6 Evaluate achieved dependability results for further improvement
Element 3: Analysis, evaluation and assessment						
Task 13: Analysis of use environment						
Task 14: Reliability modeling and simulation				IEC 61078 Reliability block diagram method IEC 61165 Application of the Markov techniques		
Task 15: Parts evaluation and control						
Task 16: Design analysis and product evaluation				IEC61025 Fault tree analysis IEC 60812 Procedure for failure mode and effects analysis		
Task 17: Cause-effect impact and risk analysis			IEC 62198 Project risk management	IEC 60300-3-9 Risk analysis of technological systems IEC 61882 Guide for hazard and operability studies		
Task 18: Prediction				IEC 61709 Electronic components reliability - Reference conditions for failure rates and stress models for conversion IEC 62308 Process for assessing reliability of equipment (*under development*)	IEC60863 Presentation of reliability, maintainability and availability predictions	
Task 19: Trade-off analysis						
Task 20: Life cycle costing			IEC 60300-3-3 Life cycle costing			
Task 21: Reliability growth			IEC 61014 Programmes for reliability growth	IEC 61164 Reliability growth - Statistical test and estimation methods		
Element 4: Verification and validation						
Task 22: Verification and validation strategy			IEC 60300-3-5 Reliability test conditions and statistical test principles IEC 61123 Reliability testing - Compliance test plans for success ratio	IEC 60605-2 Design of test cycles	IEC 60706-3 Verification and collection, analysis and presentation of data	
Task 23: Dependability demonstration						IEC 61124 Compliance tests for constant failure rate and constant failure intensity
Task 24: Reliability stress screening				IEC 60300-3-7 Reliability stress screening of electronic hardware IEC 61163-1 Reliability stress screening, Part 1: Repairable items manufactured in lots		

IEC 074/04



IEC 075/04

Process steps	1 Define dependability objectives	2 Analyze scope of dependability work needed and implications	3 Plan strategy and activities to achieve dependability objectives	4 Implement selected dependability activities	5 Analyze results of dependability activities implemented	6 Evaluate achieved dependability results for further improvement
Element 5: Knowledge base						
Task 25 Knowledge base establishment						
Task 26: Data analysis					IEC 61650 Procedures for the comparison of two constant failure rates and two constant failure (event) intensities IEC 60605-4 Statistical procedure for exponential distribution IEC 61710 Goodness-of-fit for the power law model	IEC 60605-6 Test for the validity of the constant failure rate or constant failure intensity assumptions IEC 61070 Compliance test procedures for steady-state availability IEC 61649 Goodness-of-fit tests, confidence intervals and lower confidence limits for Weibull distrubuted data
Task 27: Data collection and dissemination						IEC 60319 Presentation of reliability data on electronic components or parts
Task 28: Dependability records				IEC 60300-3-2 Collection of dependability data from the field		
Element 6: Improvement						
Task 29: Preventive and corrective actions						
Task 30: Upgrade and modification						
Task 31: Competence development and enhancement						
Task 32: Management system improvement						

IEC 075/04

Annexe E
(Informative)

Questions pour la revue de gestion de la sûreté de fonctionnement

NOTE Une liste de questions est fournie pour contribuer à la revue de gestion de la sûreté de fonctionnement. Ces questions peuvent être utilisées pour déterminer si les questions liées à la sûreté de fonctionnement sont correctement traitées ou déployées pendant une phase spécifique du produit afin de s'assurer que le produit peut passer à la phase suivante. Il convient que ce processus soit mené en conjonction avec la revue globale du projet afin de tirer parti de l'expérience et des actions interdisciplinaires pour une résolution globale des problèmes. Cette liste de questions n'est pas exhaustive. Il y a lieu que son utilisation reflète la situation particulière du projet.

E.1 Questions applicables à la phase de concept et de définition

a) Les objectifs de sûreté de fonctionnement établis sont-ils adaptés aux besoins et applications du client ?

b) Les attentes et exigences prévues du marché, les exigences réglementaires et environnementales sont-elles définies et comprises ?

c) Une analyse préliminaire de la sûreté de fonctionnement a-t-elle été effectuée pour venir à l'appui des décisions relatives à l'élaboration du projet ?

d) L'impact du coût du cycle de vie a-t-il été déterminé pour évaluer la sûreté de fonctionnement et l'exposition à des risques potentiels ?

e) Le plan d'élaboration du produit est-il disponible à des fins de revue ?

f) Existe-t-il des ressources appropriées consacrées à la sûreté de fonctionnement pour pouvoir respecter le calendrier d'élaboration du produit ?

g) L'environnement d'exploitation est-il connu ?

E.2 Questions applicables à la phase de conception et de développement

a) La spécification de conception du produit est-elle disponible à des fins de revue ?

b) Les paramètres de performance du produit liés à la sûreté de fonctionnement sont-ils spécifiés ?

c) Le plan de sûreté de fonctionnement a-t-il été établi pour la mise en œuvre du programme de sûreté de fonctionnement en vue de la réalisation des performances et des services de soutien du produit ?

d) Une analyse du coût du cycle de vie a-t-elle été menée pour déterminer des coûts d'investissement et de propriété ?

e) Les outils de conception et d'analyse appropriés ont-ils été identifiés et utilisés pour la sûreté de fonctionnement dans le cadre de la conception ?

f) Les principaux processus de maîtrise ont-ils été mis en place ?

g) La stratégie de vérification et de validation et les plans des essais sont-ils adéquats pour l'évaluation et l'acceptation du produit ?

h) Le processus de transfert de la conception vers la fabrication est-il prêt à être mis en œuvre ?

E.3 Questions applicables à la phase de fabrication

a) Le plan de fabrication et les spécifications de fabrication sont-ils prêts à être mis en œuvre ?

b) Les résultats des essais sur le produit et les tendances relatives à l'acceptation sont-ils cohérents avec les prédictions d'efficacité ?

c) Les non-conformités associées à des problèmes de sûreté de fonctionnement sont-elles rapidement résolues pour empêcher leur récurrence ?

Annex E
(informative)

Questions for dependability management review

NOTE A list of questions is provided to assist dependability management review. These questions can be used to determine if the dependability issues are adequately addressed or deployed during a specific product phase to ensure project readiness to advance to the next phase. This process should be conducted in conjunction with the general project review to benefit from cross-disciplinary actions and experience for total problem resolution. This list of questions is not exhaustive. Its application should reflect the individual project situation.

E.1 Questions applicable to concept and definition phase

a) Are the dependability objectives established suitable for the customer's needs and applications?

b) Are the intended market needs and expectations, regulatory and environmental requirements defined and understood?

c) Has a preliminary dependability analysis been carried out to support development decisions?

d) Has life cycle cost impact been determined to assess dependability and potential risk exposures?

e) Is the product development plan available for review?

f) Are adequate dependability resources available to meet the product development schedule?

g) Is the operating environment known?

E.2 Questions applicable to design and development phase

a) Is the product design specification available for review?

b) Are the product performance parameters related to dependability specified?

c) Has the dependability plan been established for dependability programme implementation towards realization of product performance and support services?

d) Has a life cycle cost analysis been conducted to determine investment and ownership costs?

e) Have appropriate design and analysis tools been identified and used to design for dependability?

f) Are the essential control processes put in place?

g) Are the verification and validation strategy and test plans adequate for product evaluation and acceptance?

h) Is the design transfer to manufacturing process ready for implementation?

E.3 Questions applicable to manufacturing phase

a) Are the product manufacturing plan and manufacturing specifications ready for implementation?

b) Are the product test results and acceptance trends consistent with the yield predictions?

c) Are non-conformances traceable to dependability problems promptly resolved to prevent recurrence?

d) Le déverminage sous contraintes est-il justifié dans le processus de fabrication pour éliminer les défauts latents ?

e) La gestion de la chaîne d'approvisionnement est-elle pleinement utilisée pour bénéficier aux fournisseurs et aux clients ?

f) Le plan de lancement de nouveaux produits est-il disponible à des fins de revue ?

E.4 Questions applicables à la phase d'installation

a) Toutes les procédures d'exploitation et de maintenance sont-elles prêtes à être mises en œuvre ?

b) Le plan de lancement ou le processus de mise en service du produit est-il prêt pour la mise en œuvre par le client et l'acceptation du produit ?

c) Le plan de logistique de maintenance est-il appliqué pour le transfert des responsabilités dans le cadre de l'exploitation et de la maintenance du produit ?

d) Les facteurs humains sont-ils pris en compte pour l'installation et l'exploitation du produit ?

E.5 Questions applicables à la phase d'exploitation et de maintenance

a) Toutes les instructions de soutien et procédures de formation relatives au produit sont-elles mises en œuvre et tous les documents relatifs aux produits sont-ils mis à disposition des utilisateurs ?

b) Le processus de soutien logistique est-il approprié pour assurer le réapprovisionnement en pièces de rechange, les mises à niveau ou les modifications de logiciels selon les calendriers prévus ?

c) Le système de compte rendu des incidents sur site pour la collecte des données, l'analyse et la diffusion des informations est-il approprié pour activer des actions préventives et correctives ?

d) Le programme de surveillance de la croissance de fiabilité est-il appliqué pour l'amélioration de la fiabilité du produit ?

e) Les réclamations de clients et les retours d'information sont-ils pris en compte pour l'amélioration du système de management ?

E.6 Questions applicables à la phase de mise au rebut

a) Les défaillances sur site du produit sont-elles plus fréquentes et les activités de maintenance plus onéreuses qu'en temps normal, ce qui indiquerait des caractéristiques de fin de vie du produit ?

b) Une analyse du coût du cycle de vie a-t-elle été menée pour rationaliser les décisions de réparation ou de remplacement des produits ?

c) La mise au rebut appropriée du produit a-t-elle été prise en compte au vu des situations contractuelles de «reprise» pertinentes et des questions réglementaires ou environnementales ?

d) Un plan de mise au rebut du produit est-il disponible à des fins de revue ?

d) Is reliability stress screening justified in the manufacturing process to eliminate latent defects?

e) Is supply-chain management fully utilized to benefit the suppliers and the customers?

f) Is the new product introduction plan ready for review?

E.4 Questions applicable to installation phase

a) Are all operation and maintenance procedures ready for implementation?

b) Is the product introduction plan or commissioning process ready for customer implementation and product acceptance?

c) Is the maintenance support plan initiated for transfer of responsibilities for product operation and maintenance?

d) Have human factors been taken into consideration for product installation and operation?

E.5 Questions applicable to operation and maintenance phase

a) Are all product support instructions and training procedures implemented and all relevant product documentation available for user access?

b) Is the logistic support process adequate to meet turn-around-time, spares replenishment or software upgrades or modifications when scheduled?

c) Is the field incident reporting system for data collection, analysis and information dissemination adequate to activate preventive and corrective actions?

d) Is the reliability growth monitoring programme initiated for product reliability improvement?

e) Are customer complaints and feedback information taken into consideration for management system improvement?

E.6 Questions applicable to disposal phase

a) Are the product field failures more frequent and the maintenance effort more costly than normal operations, indicating product end of life characteristics?

b) Has life cycle cost analysis been conducted to rationalize appropriate product repair or replacement decisions?

c) Has consideration been given to the proper disposal of the product recognizing the relevant contractual “take-back” situations and the regulatory or environmental issues?

d) Is a disposal plan for the product available for review?

Annexe F
(informative)

Lignes directrices sur le processus d'ajustement

NOTE Les activités générales du processus d'ajustement sont présentées en 7.2. La présente annexe contient des détails spécifiques sur le processus d'ajustement en vue de faciliter sa mise en œuvre.

F.1 Identification de l'environnement du projet, reflet de la politique et de l'infrastructure organisationnelle

a) Déterminer l'effort à anticiper pour le projet de sûreté de fonctionnement selon les capacités et les ressources de l'organisme afin d'obtenir des résultats réalisables et concluants. Il est utile d'identifier la politique commerciale de l'organisme.

b) Déterminer si des tâches spécifiques de sûreté de fonctionnement pourraient nuire à des questions de responsabilité ou des problèmes légaux tels que des brevets, droits d'auteur, réglementations et obligations liées à des redevances.

c) Déterminer quelles activités il convient de sous-traiter.

d) Déterminer toutes les contraintes qui nécessitent l'affectation de personnel spécifique pour des tâches particulières.

F.2 Analyse des accords contractuels, criticité et impact des résultats attendus, capacités et ressources disponibles pour la mise en œuvre du projet

a) Evaluer les exigences contractuelles selon les ressources disponibles, le niveau de compétence requis et les délais de livraison. S'assurer que cette évaluation est analysée et prise en compte par la direction au plus haut niveau qui approuve la poursuite du contrat.

b) Etablir les priorités du projet en ce qui concerne les besoins en ressources.

c) Déterminer le coût et les pénalités résultant d'un retard ou du non-respect du calendrier de livraison avant de débuter le contrat.

d) Noter la criticité des éléments d'entrée des fournisseurs ou de la livraison et identifier l'impact d'activités de récupération non planifiées.

F.3 Détermination de la ou des phases spécifiques du cycle de vie applicables au projet

a) Définir les critères de progression d'une phase du projet à la suivante.

b) Déterminer les éléments d'entrée et de sortie du projet pour chaque phase.

F.4 Détermination des caractéristiques relatives au produit telles que ses particularités et ses fonctions, l'historique de produits similaires, l'utilisation finale prévue du produit et les environnements d'utilisation anticipés

a) Etudier les performances précédentes pour avoir un aperçu de l'élaboration, de la fabrication et de la commercialisation de produits similaires.

b) Noter que les environnements d'utilisation finale dictent souvent le choix des techniques employées, des méthodes de fabrication, des stratégies de logistique de maintenance et des besoins logistiques.

Annex F
(informative)

Guidelines for the tailoring process

NOTE The general tailoring process activities are provided in 7.2. The following expands on specific details to assist implementation of the tailoring process.

F.1 Identification of the project environment reflecting the organizational policy and infrastructure

a) Determine the anticipated dependability project effort to the organization's capability and resource availability to realize accomplishable and successful project results. It is useful to identify the policy of the organization in doing business.

b) Determine whether specific dependability work might infringe on liability issues or legal problems such as patents, copyrights, regulations and royalty obligations.

c) Determine what efforts should be outsourced.

d) Determine any constraints requiring specific personnel assignment for specific tasks.

F.2 Analysis of the contract agreements, criticality and impact of deliverables, capability and resources available for project implementation

a) Map contract stipulations against available resources, competence level needed and timeline in delivery. Ensure that this mapping is analysed and appreciated by top management approving the contract go ahead.

b) Set project priorities for competing demands on resources.

c) Determine cost and penalty of late or missed delivery schedule prior to start of contract.

d) Note the criticality of supplier inputs or delivery and identify impact of unplanned recovery effort.

F.3 Determination of specific life cycle phase or phases applicable to the project

a) Define the criteria for advancing from one project phase to the next.

b) Determine project inputs and outputs at each project phase.

F.4 Determination of product related characteristics such as the product features and functions, past history of similar products, the intended end use of the product and the anticipated application environments

a) Use past performance history to provide insights on similar product development, manufacturing, and market introduction.

b) Note that end use application environments often dictate the technology selection, manufacturing methods, maintenance support strategies and logistic needs.

F.5 Sélection des éléments et des tâches applicables du programme de sûreté de fonctionnement en fonction des phases spécifiques du cycle de vie identifiées

a) Identifier les éléments et les tâches spécifiques du programme de sûreté de fonctionnement appropriés pour la mise en œuvre du projet par rapport aux phases spécifiques identifiées.

b) Noter que certaines tâches du programme de sûreté de fonctionnement peuvent se prolonger sur plusieurs phases du projet. Il convient que la portée des activités spécifiques relatives à la sûreté de fonctionnement corresponde aux objectifs et besoins du projet pour cette phase. On peut prendre comme exemple la prédiction de fiabilité: elle est très utile pendant la phase de conception et de développement mais elle est moins intéressante au moment de la fabrication et des essais du produit lorsque des données réelles sont obtenues pour valider les performances de fiabilité du produit.

c) Prendre en compte le coût d'adaptation du programme de sûreté de fonctionnement à des objectifs spécifiques de projet.

d) Noter les caractéristiques de performance durée/phase associées à la sûreté de fonctionnement.

F.6 Identification des processus pertinents du cycle de vie du système devant être associés à la planification et à la durée des éléments du programme de sûreté de fonctionnement et des activités pour l'attribution de ressources

a) Noter que les éléments relatifs à la sûreté de fonctionnement appliqués lors d'une phase spécifique du cycle de vie vont influer sur les engagements en termes de ressources et de délais de livraison du projet.

b) S'assurer que le coût des activités liées à la sûreté de fonctionnement correspond aux besoins spécifiques du projet.

c) Rationaliser les activités liées à la sûreté de fonctionnement choisies pour la mise en œuvre du programme afin de s'assurer que les activités choisies permettent d'obtenir de la valeur ajoutée.

F.7 Justification écrite de la formalisation des décisions relatives au processus d'ajustement dans le cadre du plan du projet

a) Envisager le processus d'ajustement dans le cadre d'un processus d'optimisation au moment de déterminer le niveau des activités de sûreté de fonctionnement nécessaire pour atteindre les objectifs du projet ou respecter les accords contractuels.

b) Utiliser la rationalisation comme un exercice pour l'analyse de compromis, la justification des approches techniques et la détermination de la criticité et de l'impact des décisions, en fonction des contraintes commerciales.

c) Conserver des enregistrements des décisions relatives au processus d'ajustement en vue de la revue de projet et de l'amélioration continue.

F.5 Selection of applicable dependability programme elements and tasks relevant to the specific life cycle phases identified

a) Identify the specific dependability programme elements and tasks appropriate for project implementation relevant to that specific phase.

b) Note that some dependability programme tasks might overlap several project phases. The extent of specific dependability effort should correspond to the intent and needs for the project at that phase. An example is reliability prediction: this is very helpful during concept and development phase, but less useful after the product is manufactured and tested where actual data becomes available to validate product reliability performance.

c) Consider cost when tailoring a dependability programme to meet specific project objectives.

d) Note the time-phase performance characteristics associated with dependability.

F.6 Identification of relevant system life cycle processes to associate with the timing and duration of dependability programme elements and activity applications for resource allocation

a) Note that dependability elements initiated at a specific product life cycle phase will impact resource commitments and delivery schedules of the business operation.

b) Ensure that costing of dependability effort should correspond to meeting the specific project needs.

c) Rationalize the dependability effort selected for programme implementation to ensure that the selected activities add value.

F.7 Documenting the rationale in formalizing the tailoring decisions as part of the project plan

a) View the tailoring process as part of an optimization process in determining the level of dependability effort necessary to meet project objectives or contract agreements.

b) Use rationalization as an exercise for trade-off analysis, justification of technical approaches, and determining the criticality and impact of the decisions, subject to business constraints.

c) Retain records for tailoring decisions to help project review and continual improvement.

Annexe G [2]
(informative)

Classification des normes relatives à la sûreté de fonctionnement selon les phases du cycle de vie pour lesquelles elles sont applicables

Légende

C et D Concept et définition

D et D Conception et développement

MFG Fabrication

INS Installation

O et M Exploitation et maintenance

DIS Mise au rebut

Classification des normes de sûreté de fonctionnement	Phases du cycle de vie					
	C et D	D et D	MFG	INS	O et M	DIS
1. Normes clé						
1.1 Normes fondamentales						
CEI 60050(191), Vocabulaire Electrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service	xxx	xxx	xxx	xxx	xxx	xxx
CEI 61703, Expressions mathématiques pour les termes de fiabilité, de disponibilité, de maintenabilité et de logistique de maintenance	xxx	xxx	xxx	xxx	xxx	xxx
1.2 Management						
CEI 60300-1, Gestion de la sûreté de fonctionnement – Partie 1: Gestion du programme de sûreté de fonctionnement (en anglais seulement)	xxx	xxx	xxx	xxx	xxx	xxx
CEI 60300-2, Gestion de la sûreté de fonctionnement – Partie 2: Lignes directrices pour la gestion de la sûreté de fonctionnement	xxx	xxx	xxx	xxx	xxx	xxx
2. Normes de processus						
2.1 Gestion des risques						
CEI 60300-3-9, Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 9: Analyse du risque des systèmes technologiques	xxx	xxx	xxx	xxx	xxx	xxx
CEI 62198, Gestion des risques liés à un projet – Lignes directrices pour l'application	xxx	xxx	xxx	xxx	xxx	xxx
CEI 61160: Revue de conception formalisée		xxx	xxx			
2.2 Evaluation du coût du cycle de vie						
CEI 60300-3-3, Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 3: Evaluation du coût du cycle de vie	xxx	xxx	xxx	xxx	xxx	xxx
2.3 Logiciel	xxx	xxx	xxx	xxx	xxx	xxx
CEI 61713, Sûreté de fonctionnement des logiciels pendant leurs processus de cycle de vie – Guide d'application	xxx	xxx	xxx	xxx	xxx	xxx
2.4 Analyse						
CEI 60300-3-1, Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 1: Techniques d'analyse de la sûreté de fonctionnement– Guide méthodologique	xxx	xxx			xxx	
2.6 Croissance de la fiabilité						
CEI 61014: Programmes de croissance de la fiabilité		xxx	xxx	xxx	xxx	

[2] A utiliser aussi comme bibliographie.

Annex G [2]
(informative)

Classification of dependability standards with the life cycle phases to which they are applicable

Key

C&D Concept and definition

D&D Design and development

MFG Manufacturing

INS Installation

O&M Operation and maintenance

DIS Disposal

Classification of dependability standards	Life cycle phases					
	C&D	D&D	MFG	INS	O&M	DIS
1. Core standards						
1.1 Fundamentals						
IEC 60050(191), International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service	xxx	xxx	xxx	xxx	xxx	xxx
IEC 61703, Mathematical expressions for reliability, availability, maintainability and maintenance support terms	xxx	xxx	xxx	xxx	xxx	xxx
1.2 Management						
IEC 60300-1, Dependability management – Part 1: Dependability management systems	xxx	xxx	xxx	xxx	xxx	xxx
IEC 60300-2, Dependability management – Part 2: Guidelines for dependability management	xxx	xxx	xxx	xxx	xxx	xxx
2. Process standards						
2.1 Risk management						
IEC 60300-3-9, Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems	xxx	xxx	xxx	xxx	xxx	xxx
IEC 62198, Project risk management – Application guidelines	xxx	xxx	xxx	xxx	xxx	xxx
IEC 61160, Formal design review		xxx	xxx			
2.2 Life cycle costing						
IEC 60300-3-3, Dependability management – Part 3: Application guide – Section 3: Life cycle costing	xxx	xxx	xxx	xxx	xxx	xxx
2.3 Software	xxx	xxx	xxx	xxx	xxx	xxx
IEC 61713, Software dependability through the software life-cycle processes – Application guide	xxx	xxx	xxx	xxx	xxx	xxx
2.4 Analysis						
IEC 60300-3-1, Dependability management – Part 3: Application guide – Section 1: Analysis techniques for dependability: Guide on methodology	xxx	xxx			xxx	
2.6 Reliability growth						
IEC 61014, Programmes for reliability growth		xxx	xxx	xxx	xxx	

[2] Serves also as bibliography.

Classification des normes de sûreté de fonctionnement	Phases du cycle de vie					
	C et D	D et D	MFG	INS	O et M	DIS
2.7 Maintenabilité et logistique de maintenance						
CEI 60300-3-10, Gestion de la sûreté de fonctionnement – Partie 3-10: Guide d'application – Maintenabilité		xxx				
CEI 60300-3-11, Gestion de la sûreté de fonctionnement – Partie 3-11: Guide d'application – Maintenance basée sur la fiabilité		xxx	xxx			
CEI 60300-3-12, Gestion de la sûreté de fonctionnement – Partie 3-12: Guide d'application – Soutien logistique intégré	xxx	xxx	xxx	xxx	xxx	xxx
CEI 60300-3-14, Gestion de la sûreté de fonctionnement – Partie 3-14: Guide d'application – Maintenance et logistique de maintenance (A publier)	xxx	xxx	xxx	xxx	xxx	xxx
CEI 60706-1, Guide de maintenabilité de matériel. Première partie – Sections un, deux et trois: Introduction, exigences et programme de maintenabilité		xxx				
CEI 60706-2, Guide de maintenabilité de matériel. Partie 2 – Section cinq: Etudes de maintenabilité au niveau de la conception		xxx				
CEI 60706-4, Guide de maintenabilité de matériel – Partie 4 – Section 8: Planification de la maintenance et de la logistique de maintenance		xxx	xxx			
2.8 Produits contenant des composants réutilisés						
CEI 62309, Sûreté de fonctionnement des produits contenant des composants réutilisés – Exigences pour la fonctionnalité et les essais	xxx	xxx				
3. Soutien						
3.1 Modélisation et analyse de la sûreté de fonctionnement						
CEI 60812, Techniques d'analyse de la fiabilité des systèmes – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)	xxx	xxx				
CEI 61025, Analyse par arbre de panne (AAP)	xxx	xxx				
CEI 61078, Techniques d'analyse de la sûreté de fonctionnement – Méthode du diagramme de fiabilité	xxx	xxx				
CEI 61165, Application des techniques de Markov		xxx				
CEI 61709, Composants électroniques – Fiabilité – Conditions de référence pour les taux de défaillance et modèles d'influence des contraintes pour la conversion		xxx				
CEI 61882, Etudes de danger et d'exploitabilité (études HAZOP) – Guide d'application	xxx	xxx				
CEI 62308, Processus d'estimation de la fiabilité des équipements (*A l'étude*)	xxx	xxx	xxx			
3.2 Analyse statistique						
CEI 60300-3-5, Gestion de la sûreté de fonctionnement – Partie 3-5: Guide d'application – Conditions des essais de fiabilité et principes des essais statistiques		xxx	xxx	xxx	xxx	
CEI 60605-4, Essai de fiabilité des équipements – Partie 4: Méthodes statistiques de distribution exponentielle – Estimateurs ponctuels, intervalles de confiance, intervalles de prédiction et intervalles de tolérance		xxx	xxx	xxx	xxx	
CEI 60605-6, Essais de fiabilité des équipements – Partie 6: Tests de validité des hypothèses du taux de défaillance constant ou de l'intensité de défaillance constante		xxx	xxx	xxx		
CEI 60706-6, Guide de maintenabilité de matériel – Partie 6: Section 9: Méthodes statistiques pour l'évaluation de la maintenabilité			xxx	xxx	xxx	

Classification of dependability standards	Life cycle phases					
	C&D	D&D	MFG	INS	O&M	DIS
2.7 Maintainability and maintenance support						
IEC 60300-3-10, Dependability management – Part 3-10: Application guide – Maintainability		xxx				
IEC 60300-3-11, Dependability management – Part 3-11: Application guide – Reliability centred maintenance		xxx	xxx			
IEC 60300-3-12, Dependability management – Part 3-12: Application guide – Integrated logistic support	xxx	xxx	xxx	xxx	xxx	xxx
IEC 60300-3-14, Dependability management – Part 3-14: Application guide – Maintenance and maintenance support (To be published)	xxx	xxx	xxx	xxx	xxx	xxx
IEC 60706-1, Guide on maintainability of equipment – Part 1: Sections One, Two and Three. Introduction, requirements and maintainability programme		xxx				
IEC 60706-2, Guide on maintainability of equipment – Part 2: Section Five: Maintainability studies during the design phase		xxx				
IEC 60706-4, Guide on maintainability of equipment – Part 4: Section 8: Maintenance and maintenance support planning		xxx	xxx			
2.8 Products containing reused parts						
IEC 62309, Dependability and quality of products containing reused parts – Requirements for functionality and tests	xxx	xxx				
3. Support						
3.1 Dependability modelling and analysis						
IEC 60812, Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)	xxx	xxx				
IEC 61025, Fault tree analysis (FTA)	xxx	xxx				
IEC 61078, Analysis techniques for dependability – Reliability block diagram method	xxx	xxx				
IEC 61165, Application of Markov techniques		xxx				
IEC 61709, Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion		xxx				
IEC 61882, Hazard and operability studies (HAZOP studies) – Application guide	xxx	xxx				
IEC 62308, Process for assessing reliability of equipment (*Under consideration*)	xxx	xxx	xxx			
3.2 Statistical analysis						
IEC 60300-3-5, Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles		xxx	xxx	xxx	xxx	
IEC 60605-4, Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals		xxx	xxx	xxx	xxx	
IEC 60605-6, Equipment reliability testing – Part 6: Tests for the validity of the constant failure rate or constant failure intensity assumptions		xxx	xxx	xxx		
IEC 60706-6, Guide on maintainability of equipment – Part 6: Section 9: Statistical methods in maintainability evaluation			xxx	xxx	xxx	

Classification des normes de sûreté de fonctionnement	Phases du cycle de vie					
	C et D	D et D	MFG	INS	O et M	DIS
3.2 Analyse statistique (suite)						
CEI 61070, Procédures d'essai de conformité pour la disponibilité en régime établi		xxx	xxx	xxx	xxx	
CEI 61123, Essai de fiabilité – Plans d'essai de conformité pour une proportion de succès		xxx	xxx	xxx		
CEI 61124, Essais de fiabilité – Plans d'essai de conformité d'un taux de défaillance constant et d'une intensité de défaillance constante		xxx	xxx	xxx		
CEI 61164, Croissance de la fiabilité – Tests et méthodes d'estimation statistiques			xxx	xxx	xxx	
CEI 61649, Procédures pour le test d'adéquation, les intervalles de confiance et les limites inférieures de confiance pour les données suivant la distribution de Weibull		xxx	xxx	xxx		
CEI 61650, Techniques d'analyse des données de fiabilité – Procédures pour la comparaison de deux taux de défaillance constants et de deux intensités de défaillance (événements) constantes		xxx	xxx	xxx		
CEI 61710, Modèle de loi en puissance – Test d'adéquation et méthodes d'estimation des paramètres		xxx	xxx	xxx		
3.3 Essais						
CEI 60605-2, Essais de fiabilité des équipements – Partie 2: Conception des cycles d'essai			xxx	xxx		
CEI 60605-3-1, Essai de fiabilité des équipements. Troisième partie: Conditions d'essai préférentielles. Equipements portatifs d'intérieur – Faible degré de simulation				xxx	xxx	
CEI 60605-3-2, Essai de fiabilité des équipements. Troisième partie: Conditions d'essai préférentielles. Equipements pour utilisation à poste fixe à l'abri des intempéries – Degré de simulation élevé				xxx	xxx	
CEI 60605-3-3, Essai de fiabilité des équipements – Partie 3: Conditions d'essai préférentielles – Section 3: Cycle d'essai n° 3: Equipements pour utilisation à poste fixe partiellement à l'abri des intempéries – Faible degré de simulation				xxx	xxx	
CEI 60605-3-4, Essais de fiabilité des équipements – Partie 3: Conditions d'essai préférentielles – Section 4: Cycle d'essai n° 4: Equipements portatifs à utilisation en déplacement – Faible degré de simulation				xxx	xxx	
CEI 60605-3-5, Essai de fiabilité des équipements – Partie 3: Conditions d'essai préférentielles – Section 5: Cycle d'essai n° 5: Equipements montés sur véhicules terrestres – Faible degré de simulation				xxx	xxx	
CEI 60605-3-6, Essais de fiabilité des équipements – Partie 3: Conditions d'essai préférentielles – Section 6: Cycle d'essai n° 6: Equipements portatifs d'extérieur – Faible degré de simulation				xxx	xxx	
CEI 60706-5, Guide de maintenabilité de matériel – Partie 5: Section 4: Essais pour diagnostic		xxx			xxx	
3.4 Déverminage						
CEI 60300-3-7, Gestion de la sûreté de fonctionnement – Partie 3-7: Guide d'application – Déverminage sous contraintes du matériel électronique			xxx			
CEI 61163-1: Déverminage sous contraintes – Partie 1: Entités réparables fabriquées en lots			xxx			
CEI 61163-2: Déverminage sous contraintes – Partie 2: Composants électroniques			xxx			

Classification of dependability standards	Life cycle phases					
	C&D	D&D	MFG	INS	O&M	DIS
3.2 Statistical analysis (continued)						
IEC 61070, Compliance test procedures for steady-state availability		xxx	xxx	xxx	xxx	
IEC 61123, Reliability testing – Compliance test plans for success ratio		xxx	xxx	xxx		
IEC 61124, Reliability testing – Compliance tests for constant failure rate and constant failure intensity		xxx	xxx	xxx		
IEC 61164, Reliability growth – Statistical test and estimation methods			xxx	xxx	xxx	
IEC 61649, Goodness-of-fit tests, confidence intervals and lower confidence limits for Weibull distributed data		xxx	xxx	xxx		
IEC 61650, Reliability data analysis techniques – Procedures for the comparison of two constant failure rates and two constant failure (event) intensities		xxx	xxx	xxx		
IEC 61710, Power law model – Goodness-of-fit tests and estimation methods		xxx	xxx	xxx		
3.3 Testing						
IEC 60605-2, Equipment reliability testing – Part 2: Design of test cycles			xxx	xxx		
IEC 60605-3-1, Equipment reliability testing – Part 3: Preferred test conditions. Indoor portable equipment – Low degree of simulation				xxx	xxx	
IEC 60605-3-2, Equipment reliability testing – Part 3: Preferred test conditions. Equipment for stationary use in weather-protected locations – High degree of simulation				xxx	xxx	
IEC 60605-3-3, Equipment reliability testing – Part 3: Preferred test conditions – Section 3: Test Cycle 3: Equipment for stationary use in partially weather-protected locations – Low degree of simulation				xxx	xxx	
IEC 60605-3-4, Equipment reliability testing – Part 3: Preferred test conditions – Section 4: Test cycle 4: Equipment for portable and non-stationary use – Low degree of simulation				xxx	xxx	
IEC 60605-3-5, Equipment reliability testing – Part 3: Preferred test conditions – Section 5: Test cycle 5: Ground mobile equipment – Low degree of simulation				xxx	xxx	
IEC 60605-3-6, Equipment reliability testing – Part 3: Preferred test conditions – Section 6: Test cycle 6: Outdoor transportable equipment – Low degree of simulation				xxx	xxx	
IEC 60706-5, Guide on maintainability of equipment – Part 5: Section 4: Diagnostic testing		xxx			xxx	
3.4 Screening						
IEC 60300-3-7, Dependability management – Part 3-7: Application guide – Reliability stress screening of electronic hardware			xxx			
IEC 61163-1, Reliability stress screening – Part 1: Repairable items manufactured in lots			xxx			
IEC 61163-2, Reliability stress screening – Part 2: Electronic components			xxx			

Classification des normes de sûreté de fonctionnement	Phases du cycle de vie					
	C et D	D et D	MFG	INS	O et M	DIS
3.5 Documentation et données						
CEI 60300-3-2, Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 2: Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation				xxx	xxx	
CEI 60300-3-4, Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 4: Spécification d'exigences de sûreté de fonctionnement	xxx	xxx				
CEI 60319, Présentation et spécification des données de fiabilité pour les composants électroniques		xxx		xxx	xxx	
CEI 60706-3, Guide de maintenabilité de matériel – Troisième partie: Sections six et sept: Vérification et recueil, analyse et présentation des données				xxx	xxx	
CEI 60863, Présentation des résultats de la prévision des caractéristiques de fiabilité, maintenabilité, disponibilité		xxx				

Classification of dependability standards	Life cycle phases					
	C&D	D&D	MFG	INS	O&M	DIS
3.5 Documentation and data						
IEC 60300-3-2, Dependability management – Part 3: Application guide – Section 2: Collection of dependability data from the field				xxx	xxx	
IEC 60300-3-4, Dependability management – Part 3: Application guide – Section 4: Guide to the specification of dependability requirements	xxx	xxx				
IEC 60319, Presentation and specification of reliability data for electronic components		xxx		xxx	xxx	
IEC 60706-3, Guide on maintainability of equipment – Part 3: Sections Six and Seven: Verification and collection, analysis and presentation of data				xxx	xxx	
IEC 60863, Presentation of reliability, maintainability and availability predictions		xxx				

Bibliographie[3]

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

CEI 60300-1, *Gestion de la sûreté de fonctionnement – Partie 1: Gestion du programme de sûreté de fonctionnement* (disponible en anglais seulement)

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

CEI 60300-3-4, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 4: Spécification d'exigences de sûreté de fonctionnement*

CEI 60300-3-9, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 9 : Analyse du risque des systèmes technologiques*

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

CEI 60300-3-11, *Gestion de la sûreté de fonctionnement – Partie 3-11: Guide d'application – Maintenance basée sur la fiabilité*

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

CEI 60300-3-14, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Maintenabilité et soutien de maintenabilité* [4]

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

CEI 60863, *Présentation des résultats de la prévision des caractéristiques de fiabilité, maintenabilité, disponibilité*

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

CEI 61160, *Revue de conception formalisée*

CEI 61163-1, *Déverminage sous contraintes – Partie 1: Entités réparables fabriquées en lots*

CEI 61163-2, *Déverminage sous contraintes – Partie 2: Composants électroniques*

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

CEI 61165, *Application des techniques de Markov*

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

ISO 9000, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

---

3 Voir aussi l'Annexe G.

4 A publier.

Bibliography[3]

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

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

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

IEC 60300-3-4, *Dependability management – Part 3: Application guide – Section 4: Guide to the specification of dependability requirements*

IEC 60300-3-9, *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*

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

IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

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

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

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

IEC 60863, *Presentation of reliability, maintainability and availability predictions*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61160, *Formal design review*

IEC 61163-1, *Reliability stress screening – Part 1: Repairable items manufactured in lots*

IEC 61163-2, *Reliability stress screening – Part 2: Electronic components*

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

IEC 61165, *Application of Markov techniques*

IEC 62198, *Project risk management – Application guidelines*

ISO 9000, *Quality management systems – Fundamentals and vocabulary*

---

[3] See also Annex G.

[4] To be published.

ISO 10007, *Systèmes de management de la qualité – Lignes directrices pour la gestion de la configuration*

ISO/TR 10017, *Lignes directrices pour les techniques statistiques relatives à l'ISO 9001:2000* (disponible en anglais seulement)

ISO/TR 13425, *Guide pour la sélection des méthodes statistiques en normalisation et en spécification*

ISO/CEI 15288, *Ingénierie systèmes – Processus du cycle de vie des systèmes* (disponible en anglais seulement)

ISO/CEI 12207, *Technologies de l'information – Processus du cycle de vie du logiciel* (disponible en anglais seulement)

ISO/CEI TR 14764, *Technologies de l'information – Maintenance du logiciel* (disponible en anglais seulement)

IEEE Std 1332, *Norme IEEE de programme de fiabilité pour l'élaboration et la production de systèmes et d'équipements électroniques*

Society of automotive engineers, Inc. SAE G-11 JA 1000, *Norme de programme de fiabilité*

Society of automotive engineers, Inc. SAE G-11 JA 1000-1, *Norme de programme de fiabilité – Guide de mise en œuvre*

Society of automotive engineers, Inc. SAE G-11 JA 1002, *Norme de programme de fiabilité des logiciels*

DEF STAN 00-40 (Partie 1), Edition 4, *Fiabilité et maintenabilité (R&M) – Partie 1: Responsabilités et exigences de gestion pour les programmes et les plans*

IECQ – CMC LC0305B, *Evaluation de la fiabilité des équipements électroniques*

ISO 10007, *Quality management systems – Guidelines for configuration management*

ISO/TR 10017, *Guidance on statistical techniques for ISO 9001:2000*

ISO/TR 13425, *Guide for the selection of statistical methods in standardization and specification*

ISO/IEC 15288, *Systems engineering – System life cycle processes*

ISO/IEC 12207, *Information technology – Software life cycle processes*

ISO/IEC TR 14764, *Information technology – Software maintenance*

IEEE Std 1332, *IEEE standard reliability program for the development and production of electronic systems and equipment*

Society of automotive engineers, Inc. SAE G-11 JA 1000, *Reliability program standard*

Society of automotive engineers, Inc. SAE G-11 JA 1000-1, *Reliability program standard – Implementation guide*

Society of automotive engineers, Inc. SAE G-11 JA 1002, *Software reliability program standard*

DEF STAN 00-40 (Part 1), Issue 4, *Reliability and Maintainability (R&M) – Part 1: Management responsibilities and requirements for programmes and plans*

IECQ – CMC LC0305B, *Reliability assessment of electronic equipment*

Standards Survey

The IEC would like to offer you the best quality standards possible. To make sure that we continue to meet your needs, your feedback is essential. Would you please take a minute to answer the questions overleaf and fax them to us at +41 22 919 03 00 or mail them to the address below. Thank you!

Customer Service Centre (CSC)

International Electrotechnical Commission
3, rue de Varembé
1211 Genève 20
Switzerland

or

Fax to: **IEC**/CSC at +41 22 919 03 00

Thank you for your contribution to the standards-making process.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 GENEVA 20
Switzerland

Q1 Please report on **ONE STANDARD** and **ONE STANDARD ONLY**. Enter the exact number of the standard: *(e.g. 60601-1-1)*

.....

Q2 Please tell us in what capacity(ies) you bought the standard *(tick all that apply).* I am the/a:

purchasing agent ❑
librarian ❑
researcher ❑
design engineer ❑
safety engineer ❑
testing engineer ❑
marketing specialist ❑
other.....

Q3 I work for/in/as a: *(tick all that apply)*

manufacturing ❑
consultant ❑
government ❑
test/certification facility ❑
public utility ❑
education ❑
military ❑
other.....

Q4 This standard will be used for: *(tick all that apply)*

general reference ❑
product research ❑
product design/development ❑
specifications ❑
tenders ❑
quality assessment ❑
certification ❑
technical documentation ❑
thesis ❑
manufacturing ❑
other.....

Q5 This standard meets my needs: *(tick one)*

not at all ❑
nearly ❑
fairly well ❑
exactly ❑

Q6 If you ticked NOT AT ALL in Question 5 the reason is: *(tick all that apply)*

standard is out of date ❑
standard is incomplete ❑
standard is too academic ❑
standard is too superficial ❑
title is misleading ❑
I made the wrong choice ❑
other .....

Q7 Please assess the standard in the following categories, using the numbers:
(1) unacceptable,
(2) below average,
(3) average,
(4) above average,
(5) exceptional,
(6) not applicable

timeliness.....
quality of writing.....
technical contents.....
logic of arrangement of contents .....
tables, charts, graphs, figures.....
other .....

Q8 I read/use the: *(tick one)*

French text only ❑
English text only ❑
both English and French texts ❑

Q9 Please share any comment on any aspect of the IEC that you would like us to know:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Enquête sur les normes

La CEI ambitionne de vous offrir les meilleures normes possibles. Pour nous assurer que nous continuons à répondre à votre attente, nous avons besoin de quelques renseignements de votre part. Nous vous demandons simplement de consacrer un instant pour répondre au questionnaire ci-après et de nous le retourner par fax au +41 22 919 03 00 ou par courrier à l'adresse ci-dessous. Merci !

Centre du Service Clientèle (CSC)

Commission Electrotechnique Internationale
3, rue de Varembé
1211 Genève 20
Suisse

ou

Télécopie: **CEI**/CSC +41 22 919 03 00

Nous vous remercions de la contribution que vous voudrez bien apporter ainsi à la Normalisation Internationale.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Centre du Service Clientèle (CSC)
Commission Electrotechnique Internationale
3, rue de Varembé
1211 GENÈVE 20
Suisse

Q1 Veuillez ne mentionner qu'**UNE SEULE NORME** et indiquer son numéro exact: (*ex. 60601-1-1)*

.....

Q2 En tant qu'acheteur de cette norme, quelle est votre fonction?
(cochez tout ce qui convient)
Je suis le/un:

agent d'un service d'achat ❑
bibliothécaire ❑
chercheur ❑
ingénieur concepteur ❑
ingénieur sécurité ❑
ingénieur d'essais ❑
spécialiste en marketing ❑
autre(s).....

Q3 Je travaille:
(cochez tout ce qui convient)

dans l'industrie ❑
comme consultant ❑
pour un gouvernement ❑
pour un organisme d'essais/ certification ❑
dans un service public ❑
dans l'enseignement ❑
comme militaire ❑
autre(s).....

Q4 Cette norme sera utilisée pour/comme
(cochez tout ce qui convient)

ouvrage de référence ❑
une recherche de produit ❑
une étude/développement de produit ❑
des spécifications ❑
des soumissions ❑
une évaluation de la qualité ❑
une certification ❑
une documentation technique ❑
une thèse ❑
la fabrication ❑
autre(s).....

Q5 Cette norme répond-elle à vos besoins:
(une seule réponse)

pas du tout ❑
à peu près ❑
assez bien ❑
parfaitement ❑

Q6 Si vous avez répondu PAS DU TOUT à Q5, c'est pour la/les raison(s) suivantes:
(cochez tout ce qui convient)

la norme a besoin d'être révisée ❑
la norme est incomplète ❑
la norme est trop théorique ❑
la norme est trop superficielle ❑
le titre est équivoque ❑
je n'ai pas fait le bon choix ❑
autre(s) .....

Q7 Veuillez évaluer chacun des critères ci-dessous en utilisant les chiffres
(1) inacceptable,
(2) au-dessous de la moyenne,
(3) moyen,
(4) au-dessus de la moyenne,
(5) exceptionnel,
(6) sans objet

publication en temps opportun .....
qualité de la rédaction.....
contenu technique .....
disposition logique du contenu .....
tableaux, diagrammes, graphiques, figures.....
autre(s) .....

Q8 Je lis/utilise: *(une seule réponse)*

uniquement le texte français ❑
uniquement le texte anglais ❑
les textes anglais et français ❑

Q9 Veuillez nous faire part de vos observations éventuelles sur la CEI:

.....
.....
.....
.....
.....
.....

ISBN 2-8318-7400-9

ICS 03.100.40; 03.120.01

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND