NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
62347

Première édition
First edition
2006-11

Lignes directrices pour les spécifications de sûreté de fonctionnement des systèmes

Guidance on system dependability specifications

Numéro de référence
Reference number
CEI/IEC 62347:2006

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 (www.iec.ch/searchpub) 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 (www.iec.ch/online_news/justpub) 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 (www.iec.ch/searchpub) 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 (www.iec.ch/online_news/justpub) 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
62347

Première édition
First edition
2006-11

Lignes directrices pour les spécifications de sûreté de fonctionnement des systèmes

Guidance on system dependability specifications

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 V

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

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

LIGNES DIRECTRICES POUR LES SPÉCIFICATIONS DE SÛRETÉ DE FONCTIONNEMENT DES SYSTÈMES

AVANT-PROPOS

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

La Norme internationale CEI 62347 a été préparée par le comité d'étude 56 de la CEI : Sûreté de fonctionnement.

Le texte de cette norme est basé sur les documents suivants:

FDIS	Rapport de vote
56/1138/FDIS	56/1161/RVD

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

GUIDANCE ON SYSTEM DEPENDABILITY SPECIFICATIONS

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 62347 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/1138/FDIS	56/1161/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.

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

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

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

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

INTRODUCTION

Un système est une entité physique et/ou virtuelle. Il est parfois nécessaire de définir les frontières du système afin qu'il puisse être distingué ou séparé d'autres systèmes. Un système interagit avec ce qui l'entoure et avec l'environnement pour répondre à un besoin ou à un objet, ou pour atteindre un objectif défini. Ceci est accompli par l'interaction des éléments du système représentant les fonctions nécessaires pour atteindre l'objectif. La détermination des fonctions nécessaires pour atteindre l'objectif constitue le processus de développement d'une spécification d'un système. La conception détaillée d'un système commence seulement après que les fonctions ont été bien identifiées.

La complexité d'un système peut varier dans sa complexité, structuralement et fonctionnellement. Un système peut être constitué d'éléments matériels, logiciels et humains, ou de leurs combinaisons pour effectuer les fonctions nécessaires. Un système réalisant une seule fonction peut être un produit, comme une télévision ou un programme logiciel pour une commande d'éclairage. Un système de "home vidéo" ou un aéronef sont des exemples de systèmes réalisant plusieurs fonctions. Des systèmes individuels avec des frontières définies peuvent être joints à d'autres pour former un ensemble complexe de systèmes interactifs comme un réseau de distribution d'énergie ou un service de protocole internet.

La spécification du système établit l'enveloppe et les frontières du système. La structure du système est souvent un ensemble de liaisons entre sous-systèmes ou systèmes interactifs. La spécification du système est applicable à tout système sous la définition générique de système, sans tenir compte de sa hiérarchie. Elle ne remplace pas ni ne se substitue à une spécification produit qui fournit des détails spécifiques sur les exigences portant sur le produit.

La sûreté de fonctionnement d'un système implique que l'on puisse compter sur lui et qu'il soit capable de servir sur demande avec les attributs de performance souhaités. Ces attributs de performance peuvent être atteints par l'incorporation de la sûreté de fonctionnement dans les fonctions. La sûreté de fonctionnement suppose une sensibilisation à la confiance de l'utilisateur, acquise au cours d'expériences précédentes, par des résultats fiables par rapport aux attentes.

La présente Norme internationale détaille le rationnel fondant l'importance de l'introduction, par fonction, de la sûreté de fonctionnement dans la spécification du système. Elle présente une procédure pour déterminer les exigences de sûreté de fonctionnement d'un système. Le processus de détermination des fonctions nécessaires pour atteindre les objectifs de sûreté de fonctionnement est décrit pour le fonctionnement d'un système générique. Pour le fonctionnement d'un système spécifique, le concept d'un profil opérationnel est introduit afin d'établir les exigences fonctionnelles dans un environnement pertinent pour le fonctionnement d'un système spécifique. La présente Norme internationale est basée sur le modèle de système et sur les catégories de fonctions établis dans la série CEI 61069. Les processus techniques pertinents pour la définition et l'analyse des exigences du système sont ceux de l'ISO/CEI 15288. Les étapes de procédure et les processus pour déterminer la sûreté de fonctionnement sont présentés avec des exemples. La CEI 60300-1 et la CEI 60300-2 sont utilisées comme recommandations pour la gestion de la sûreté de fonctionnement. La présente Norme internationale étend le processus de spécification de la sûreté de fonctionnement afin de traiter les fonctions comme des pré-requis à la conception du système. Elle complète la CEI 60300-3-4 dans la spécification des exigences de la sûreté de fonctionnement pour les produits et les équipements. Le processus technique relatif à l'ingénierie de la sûreté de fonctionnement des systèmes est décrit dans la CEI 60300-3-15.

INTRODUCTION

A system is a physical and/or virtual entity. It is necessary sometimes to define a system's boundary so that it can be distinguished or separated from other systems. A system interacts with its surroundings or environment to fulfil a specific need or purpose, or to achieve a defined objective. This is accomplished through the interaction of the system's elements representing the necessary functions designed to meet the intended objective. Determining the functions needed to meet a specific objective represents the process of developing a system specification. Detailed system design begins only after the functions have been identified.

Systems may vary in their complexity structurally and functionally. A system can consist of hardware, software, and human elements, or a combination of any of these elements to perform the necessary functions. A system consisting of a single function can be a product, such as a television set or a software program for lighting controls. A system performing multiple functions can be a home theatre system or an aircraft. Individual systems with defined boundaries can be joined together to form a complex set of interacting systems such as a power distribution network or an internet protocol service.

System specification establishes the envelope and boundary for the system. System structure is often hierarchical linking subsystems and interacting systems. System specification is applicable to all systems under the generic definition of system irrespective of its hierarchy. It does not replace or substitute for use a product specification, which provides specific details of the product requirements.

The dependability of a system infers that the system is perceived to be trustworthy and has the ability to provide service upon demand as desirable performance attributes. Such performance attributes can be achieved through the incorporation of dependability into the functions. Dependability implies the awareness of user confidence acquired through prior experience of the system with reliable performance results in meeting user expectations.

This International Standard provides the rationale on the importance of dependability in system specification by functions. It presents a procedure for determining system dependability requirements. For generic system operation, the process of determining the functions needed to meet system dependability objective is described. For specific system operation, the concept of an operating profile is introduced to establish the requirements of functions in an environment relevant to the specific system operation. This International Standard is based on the system model and categorization of functions established in the IEC 61069 series. Relevant technical processes for the definition and analysis of system requirements are adopted from ISO/IEC 15288. The procedural steps and processes for determining system dependability requirements are presented with applicable examples. IEC 60300-1 and IEC 60300-2 are used to guide dependability management. This International Standard extends the dependability specification process to address functions as a prerequisite for system design. It complements IEC 60300-3-4 in specification of dependability requirements for products and equipment. The technical process for engineering dependability into systems is described in IEC 60300-3-15.

LIGNES DIRECTRICES POUR LES SPÉCIFICATIONS DE SÛRETÉ DE FONCTIONNEMENT DES SYSTÈMES

1 Domaine d'application

La présente Norme internationale apporte des recommandations pour la préparation des spécifications de sûreté de fonctionnement des systèmes. Elle fournit un processus pour l'évaluation des systèmes et présente une procédure pour déterminer les exigences de sûreté de fonctionnement des systèmes.

La présente Norme internationale n'est pas destinée à la certification ou à la réalisation de l'évaluation de la conformité dans un cadre contractuel. Elle n'est pas destinée à modifier des droits ou des obligations résultant d'exigences statutaires ou réglementaires applicables.

2 Références normatives

Les documents de référence suivants sont indispensables pour 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 de référence s'applique (y compris les éventuels amendements).

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

ISO/CEI 15288, *Ingénierie systèmes – Processus de cycle de vie des systèmes*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans la CEI 60050(191) ainsi que ceux qui suivent s'appliquent.

3.1
système
ensemble d'éléments liés ou interactifs

[ISO 9000:2005, 3.2.1]

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

- un objet défini exprimé en termes de fonctions prévues,
- des conditions établies de fonctionnement et/ou d'utilisation, et
- des frontières définies.

NOTE 2 La structure d'un système peut être hiérarchique.

[CEI 60300-1, 3.6]

NOTE 3 Pour certains systèmes, tels que les produits des technologies de l'information, les données constituent une partie importante des éléments du système.

3.2
profil opérationnel
ensemble complet des tâches à accomplir pour atteindre l'objectif d'un système spécifique

NOTE Un profil opérationnel est la séquence des tâches à effectuer par le système pour atteindre son objectif opérationnel. Le profil opérationnel représente un scénario de fonctionnement spécifique pour le système en fonctionnement.

GUIDANCE ON SYSTEM DEPENDABILITY SPECIFICATIONS

1 Scope

This International Standard gives guidance on the preparation of system dependability specifications. It provides a process for system evaluation and presents a procedure for determining system dependability requirements.

This International Standard is not intended for certification or to perform conformity assessment for contractual purposes. It is not intended to change any rights or obligations provided by applicable statutory or regulatory requirements.

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

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

3 Terms and definitions

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

3.1
system
set of interrelated or interacting elements

[ISO 9000:2005, 3.2.1]

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

- a defined purpose expressed in terms of intended functions;
- stated conditions of operation/use; and
- defined boundaries.

NOTE 2 The structure of a system may be hierarchical.

[IEC 60300-1, 3.6]

NOTE 3 For some systems, such as Information Technology products, data is an important part of the system elements.

3.2
operating profile
complete set of tasks to achieve a specific system objective

NOTE An operating profile is the sequence of tasks to be performed by the system to achieve its operational objective. The operating profile represents a specific operating scenario for the system in operation.

3.3
fonction
opération élémentaire effectuée par le système qui, lorsqu'elle est combinée à d'autres opérations élémentaires (fonctions du système), permet au système d'effectuer une tâche donnée

[CEI 61069-1, définition 2.2.5]

NOTE Pour certains systèmes, les informations et les données constituent une partie importante des éléments du système.

3.4
élément
combinaison de composants qui forme un bloc de base pour réaliser une fonction distincte

NOTE Un élément peut comprendre du matériel, du logiciel, de l'information et/ou des composantes humaines.

3.5
conditions influentes
ensemble de conditions créé par des éléments externes influents et/ou d'autres facteurs qui interagit avec la performance du système et affecte celle-ci.

NOTE Des conditions influentes peuvent aussi inclure des réglementations et des contraintes.

4 Concepts traitant de la sûreté de fonctionnement

4.1 Comprendre le système

4.1.1 Objet et objectif

Un système est conçu pour un objet. Un système peut avoir un objectif défini pour atteindre son objet. L'objet d'un "home vidéo" est de fournir un loisir similaire au cinéma dans un environnement domestique. Les objectifs peuvent comprendre la perception de l'utilisateur d'une vision d'une image claire et de la superbe qualité de son. La fiabilité et la sécurité de fonctionnement et la facilité d'installation et des mises à jour. Un système peut avoir un objectif spécifique pour réaliser une tâche dédiée, par exemple un avion transportant une cargaison pour atteindre une destination de livraison. Les objectifs d'un système peuvent inclure la complétude d'une séquence de tâche, par exemple la livraison de différentes charges utiles en différentes destinations. Définir le système afin d'atteindre son objectif ou des objectifs spécifiques est un pré-requis important pour spécifier les exigences du système.

Un système ayant de multiples fonctions et un scénario complexe de fonctionnement implique souvent des systèmes externes qui interagissent. Un système peut aussi évoluer dans le temps, ce qui entraînera des améliorations de sa capacité de performance pour répondre à des demandes de service en fonctionnement et à la concurrence.

4.1.2 Propriétés et caractéristiques du système

Un système possède un ensemble de propriétés spécialement assignées, sélectionnées et conçues dans le système pour atteindre ses objectifs. Les propriétés spécifiques du système sont utilisées pour développer les fonctions nécessaires pour réaliser les tâches. Ces propriétés représentent les caractéristiques spéciales ou des attributs inhérents au système. Ils peuvent être répartis en groupes majeurs comme cela est défini dans la série CEI 61069. Dans chaque groupe, il y a un ensemble de caractéristiques pertinentes et dominantes dans ce groupe. Les fonctions sont déduites de ces propriétés du système, au moyen d'éléments interactifs dans le système. Les éléments interactifs sont conçus pour apporter des caractéristiques spéciales capables de fournir les fonctions du système et de réaliser les tâches une fois que ces fonctions peuvent être réalisées. Les caractéristiques du système peuvent être qualitatives ou quantitatives. La Figure 1 donne un exemple des caractéristiques d'un système groupées dans diverses propriétés du système.

3.3
function
elementary operation performed by the system which, combined with other elementary operations (system functions), enables the system to perform a task

[IEC 61069-1, definition 2.2.5]

NOTE For some systems, information and data are important parts of the system elements.

3.4
element
combination of components that form the basic building block to perform a distinct function

NOTE An element may comprise hardware, software, information and/or human components.

3.5
influencing condition
condition set forth by external influencing elements and/or other factors that interact with and affect system performance

NOTE Influencing conditions may also include regulations and constraints.

4 Concepts dealing with system dependability

4.1 Understanding the system

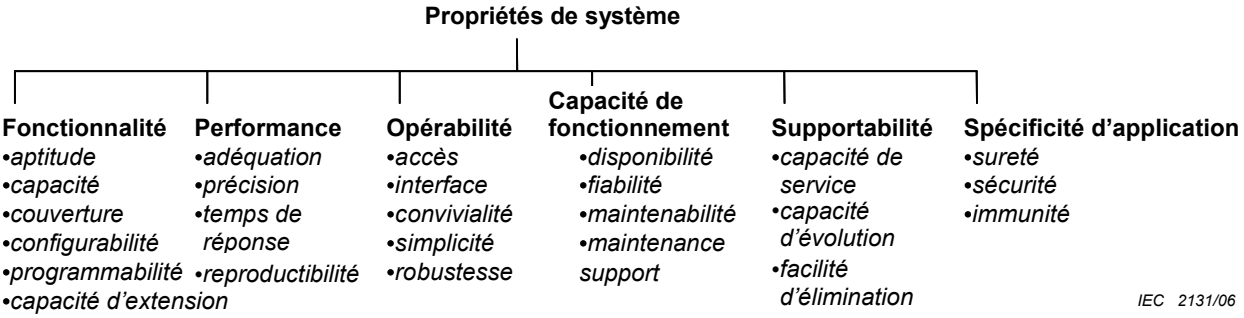
4.1.1 Purpose and objective

A system is designed for a purpose. A system must have a defined objective to achieve its purpose. The purpose of a home theatre system is to provide cinema-like entertainment in a home environment. The objectives may include users' perception of a clear picture vision and superb sound quality, reliability and safety in operation, and ease of installation and upgrade. A system may have a specific objective to perform a dedicated task, such as an aircraft carrying cargo to reach a delivery target. The objectives of a system may include the completion of a sequence of tasks, such as delivering different payloads to different destinations. Defining the system to meet its generic or specific objectives is an important prerequisite of specifying the system requirements.

A system with multiple functions and complex operating scenario often involves external interacting systems to achieve its objectives. A system may also evolve with time, resulting from enhancements of its performance capability, to sustain service demands in operation and for market competition.

4.1.2 System properties and characteristics

A system has a set of properties specifically assigned, selected or designed into the system to meet its intended objectives. Specific system properties are used to develop the needed functions to perform the tasks. These properties represent the special features or attributes inherent in the system. They may be categorized in major groupings as defined in IEC 61069 series. Under each group is a set of characteristics relevant to and dominant in that group. The functions are derived from those system properties by means of interacting elements within the system. The interacting elements are designed to provide specific characteristics capable of delivering the system functions and to carry out the tasks once these functions can be realized. System characteristics may be qualitative or quantitative. Figure 1 shows an example of the system characteristics grouped under various system properties.



NOTES **Fonctionnalité**: étendue sur laquelle le traitement, la surveillance et les fonctions de commande sont fournis.

Performance: étendue sur laquelle les fonctions fournies peuvent être exécutées dans des conditions opérationnelles et environnementales définies.

Opérabilité: étendue sur laquelle l'information peut être effectivement communiquée par une interface humaine et des protocoles établis.

Sûreté de fonctionnement: étendue sur laquelle le système peut s'appuyer pour réaliser ses fonctions attendues dans des conditions opérationnelles et environnementales définies, à un instant donné ou sur une durée donnée.

Supportabilité: étendue sur laquelle le système peut être soutenu et maintenu pour un fonctionnement continu.

Applications spécifiques: étendue sur laquelle le système peut être conçu pour un évitement de risque ou un confinement de risque, par exemple des mesures de sécurité en exploitation.

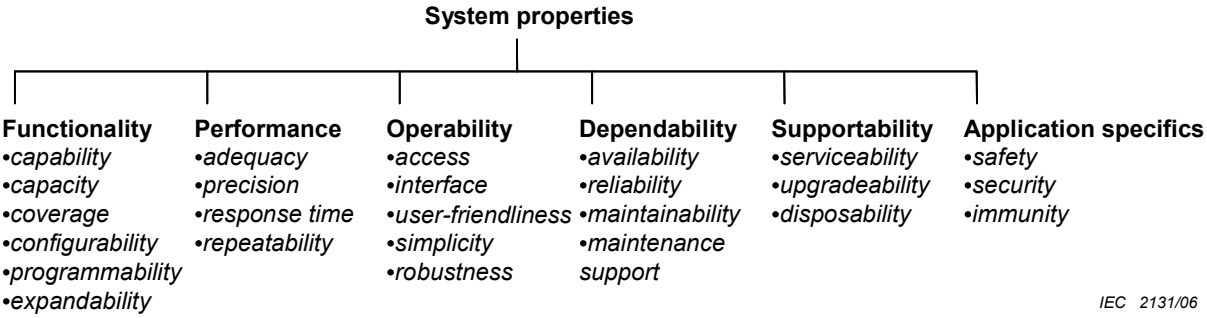
Figure 1 – Exemple de propriétés de système et de caractéristiques liées

4.1.3 Conditions influentes

Afin de déterminer quelles fonctions ont les caractéristiques sélectionnées appropriées pour atteindre un objectif spécifique, il est nécessaire de définir les conditions que le système est capable de tenir ou ses capacités à répondre aux demandes et la durée des tâches assignées. Il convient de considérer les domaines d'influence suivants affectant le système:

- les exigences des tâches imposées au système ;
- l'interface humaine avec le système ;
- le processus impliqué dans le fonctionnement du système ;
- l'environnement auquel le système est exposé ;
- les services de support disponibles pour le système ;
- les servitudes nécessaires au fonctionnement du système ;
- les systèmes externes interactifs ;
- les contraintes et réglementations.

Une spécification de sûreté de fonctionnement d'un système ne peut pas être établie isolément. Elle requiert en entrée des informations détaillées à l'étape de la planification du système, pour déterminer comment le système est prévu pour fonctionner pour la durée de vie entière. Ce travail est essentiel pour permettre l'identification et la sélection de la sûreté de fonctionnement et d'autres caractéristiques, et pour la justification des compromis de conception et pour l'optimisation du système.



NOTES **Functionality**: the extent to which the processing, monitoring and control functions are provided.

Performance: the extent to which the provided functions can be executed under defined operational and environmental conditions.

Operability: the extent to which information can be effectively communicated via the human interfaces and established protocols.

Dependability: the extent to which the system can be relied upon to perform its intended functions under defined operational and environmental conditions at a given instant of time or over a given time interval.

Supportability: the extent to which the system can be supported and maintained for continual operation.

Application specifics: the extent to which the system can be designed for risk avoidance and risk containment, such as security operational measures.

Figure 1 – Example of system properties and related characteristics

4.1.3 Influencing conditions

In order to determine which functions have the selected characteristics appropriate to achieving a specific objective, it is necessary to define the conditions that the system is capable of withstanding or meeting the demands and duration of the assigned tasks. The following areas of influence or domains affecting the system should be considered:

- task requirements imposed on the system;
- human interface with the system;
- process involved with system operation;
- environment to which the system is exposed;
- support services available for the system;
- utilities needed to operate the system;
- external interacting systems;
- constraints and regulations.

A system dependability specification cannot be completed in isolation. It requires the input of detailed information at the system planning stage to determine how the system is intended to perform for the entire duration of its defined life. This effort is essential to permit identification and selection of dependability and other relevant characteristics, and justification for design trade-off and system optimization.

4.1.4 Facteurs influents

Chaque condition influente peut être affectée par divers facteurs influençant son état. Par exemple, les exigences des tâches imposées au système peuvent être influencées par des facteurs associés à la nature et à la durée de la tâche; l'environnement du système peut être influencé par la température et l'humidité de l'ambiance autour du système. Les facteurs influents ne sont pas équivalents à l'étendue de leur influence. Certains facteurs sont plus dominants par leur présence tandis que d'autres peuvent être moins influents ou négligeables.

L'Annexe A donne des exemples typiques de facteurs influents sur des fonctions de systèmes, qui peuvent servir de critères d'évaluation des caractéristiques de la sûreté de fonctionnement d'un système.

4.1.5 Relations entre les propriétés d'un système et les conditions influentes

Etablir les relations entre les propriétés d'un système et les conditions influentes peut aider à identifier la pertinence et la criticité d'une condition externe spécifique influençant la conception d'une fonction. Le processus d'identification conduira à la sélection des propriétés spécifiques et des caractéristiques associées qui sont nécessaires à la fonction. Les caractéristiques sélectionnées ne sont pas spécifiques à la fonction. Les mêmes caractéristiques spécifiques peuvent être nécessaires dans la conception d'autres fonctions. L'importance de ces caractéristiques est déterminée par un processus itératif pour l'évaluation et les compromis de conception. Les résultats déduits de cette évaluation peuvent aider à déterminer la configuration du système et à établir les frontières appropriées du système dans la tenue des objectifs. Les informations et données pertinentes saisies lors de cette évaluation constitueront une base pour spécifier les caractéristiques importantes dans la conception des fonctions du système.

Les relations entre les propriétés d'un système et les conditions influentes peuvent être utilisées pour l'évaluation des propriétés du système. L'identification des fonctions est présentée à l'Annexe A pour faciliter la détermination des caractéristiques pertinentes de la sûreté de fonctionnement.

4.1.6 Réalisation des fonctions d'un système

Un système peut consister en toute combinaison de matériels, de logiciels et d'éléments humains. Les fonctions du système peuvent être réalisées par l'utilisation de matériels, et/ou de logiciels dans leur construction. Certaines fonctions peuvent impliquer l'intervention humaine pour réaliser les tâches qui leur sont assignées. Pour le développement d'un nouveau système, les fonctions du système peuvent être réalisées par l'ingénierie de conception et la production comme cela est décrit dans la CEI 60300-3-15 (à l'étude). Parfois, il peut être plus économique ou rapide de modifier une conception existante ou d'utiliser un produit du commerce (COTS pour "commercial-off-the-shelf") pour remplir la fonction nécessaire. Les systèmes évolutifs requièrent souvent des fonctions supplémentaires pour l'amélioration des capacités de performance et le retrait des fonctions obsolètes. Dans de tels cas, le travail d'ingénierie doit tenir compte des problèmes héréditaires comme cela est décrit à l'Annexe A.

4.2 Cycle de vie d'un système

Un système, quelque soit sa taille et sa complexité, progresse dans un cycle de vie de sa conception initiale jusqu'à son éventuel retrait. Le cycle de vie d'un système est généralement représenté par une séquence d'étapes discrètes. Chaque étape du cycle de vie d'un système peut de plus être représentée par des sous-étapes pour faciliter le planning, l'exploitation et le support. Un cycle de vie typique consiste en les étapes identifiables suivantes comme le montre la Figure 2.

4.1.4 Influencing factors

Each influencing condition can be affected by various factors influencing the status of its condition. For example, the task requirements imposed on the system could be influenced by factors associated with the nature and duration of the task; the system environment could be influenced by the temperature and humidity of the system ambience. Influencing factors are not equal to the extent of their influence. Some factors are more prominent or dominant in the extent of their influence while others may have less influence or be negligible.

Annex A provides typical examples of influencing factors on system functions to serve as criteria for evaluation of system dependability characteristics.

4.1.5 Relationships of system properties with influencing conditions

Establishing the relationships of system properties with influencing conditions can help identify the relevance and criticality of a specific external condition influencing the design of a function. The identification process will lead to the selection of specific properties and associated characteristics that are needed for the function. The selected characteristics are not exclusive to a specific function. The same characteristics may be needed in the design of other functions. The importance of these characteristics is determined by an iterative process for evaluation and design trade-off. The results derived from this evaluation can help determine the system configuration and establish the appropriate system boundaries in meeting the intended objective. The relevant information and data captured in this evaluation process will form the basis for specifying the important characteristics in the design of system functions.

The relationships of system properties with influencing conditions can be used as guidance for evaluation of system functions. The identification of functions is presented in Annex A to facilitate determination of relevant dependability characteristics.

4.1.6 Realization of system functions

A system can consist of any combination of hardware, software, and human elements. System functions can be realized by means of using hardware and/or software in their construction. Some functions may involve human intervention to achieve their assigned tasks. For new system development, system functions can be realized through engineering design and production as described in IEC 60300-3-15 (under consideration). Sometimes it may be more economical or expedient to modify an existing design or to utilize a commercial-off-the-shelf (COTS) product to serve as the needed function. Evolving systems often require additional functions for performance capability enhancement and removal of obsolete functions. In such a case, the engineering effort would have to deal with legacy issues as described in Annex A.

4.2 System life cycle

A system, irrespective of its size and complexity, follows a life cycle progression from its initial conception through to its eventual retirement. A system life cycle is generally represented by a sequence of discrete stages. Each system life cycle stage can be further represented by sub-stages to facilitate planning, operation and support. A typical system life cycle can consist of the following identifiable stages as shown in Figure 2.

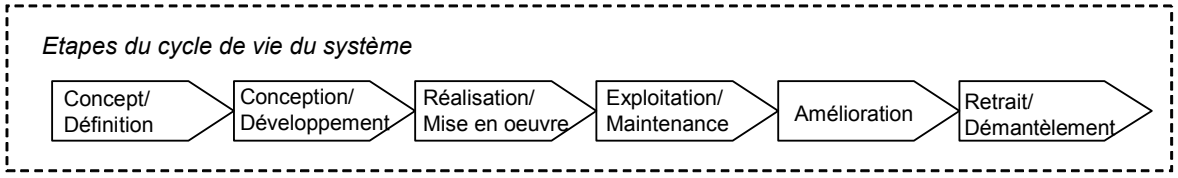


Figure 2 – Vue d'ensemble des étapes d'un cycle de vie

L'objectif de chaque étape du cycle de vie est présenté ci-dessous:

- *Concept/définition:* identifier les exigences du système et les spécifications de développement du système.
- *Conception/développement:* mener la conception préliminaire et développer des fonctions du système viables pour atteindre les objectifs de performance.
- *Réalisation/mise en oeuvre:* produire, sous-traiter ou acquérir les éléments du système sous forme de matériels et de logiciels pour un assemblage de sous-systèmes adapté aux interactions humaines comme requis dans le fonctionnement du système.
- *Exploitation/maintenance*: engager le système dans des dispositions de service opérationnel et atteindre le niveau exigé de capacité de performance du système.
- *Amélioration*: améliorer la performance du système avec des caractéristiques supplémentaires.
- *Retrait/démantèlement:* mettre fin à l'existence de l'entité système.

La description des étapes du cycle de vie d'un système dans la Figure 2 est présentée du point de vue de l'ingénierie des systèmes génériques. Il existe d'autres descriptions de cycle de vie de système. La CEI 60300-2 décrit les phases du cycle de vie d'un produit du point de vue de la gestion de projet. L'ISO/CEI 15288 fournit une description similaire du cycle de vie d'un produit du point de vue de l'ingénierie logicielle. Considérant qu'il y a certaines différences dans l'utilisation des termes présentés dans cette norme, leurs alignements sont plus évidents aux points de transition des étapes de leurs cycles de vie respectifs ou phases de projet.

Chaque étape possède ses propres objectifs spécifiques à atteindre par le processus de conception du système, par exemple, un accès limité à la maintenance pendant le fonctionnement du système, des pièces recyclables pour en faciliter l'élimination. Chaque étape requiert aussi différentes procédures internes et instructions de travail, ainsi que différentes conditions à respecter.

Définir les exigences du système et développer des solutions de systèmes pendant les étapes de conception/développement peut affecter des étapes postérieures lors du fonctionnement et/ou de la maintenance du système. Des décisions prises pour l'architecture du système et la sélection de la technologie dans la conception du système peuvent avoir des effets en production, en intégration de système et en travaux d'amélioration et contraindre le processus d'élimination.

La durée du cycle de vie d'un système est affectée par divers facteurs dépendant du type de système et de l'application, des technologies utilisées et des dispositions de support. Par exemple, le cycle de vie d'un véhicule motorisé peut être de 7 ans à 15 ans selon l'usure mécanique et la détérioration du châssis, tandis qu'un ordinateur personnel peut avoir une vie inférieure à 5 ans du fait de l'obsolescence des technologies. La durée de l'application est la durée de vie utile du système.

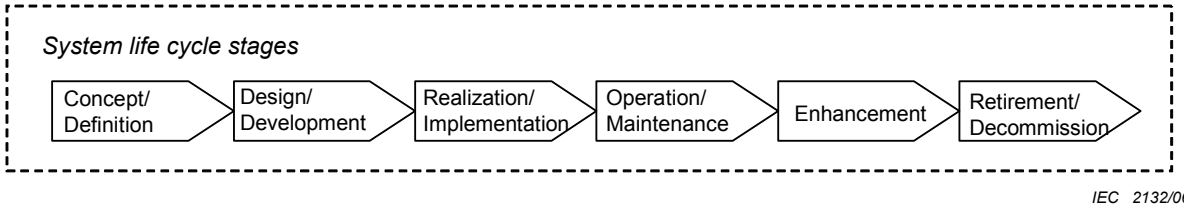


Figure 2 – Overview of system life cycle stages

The objective of each life cycle stage is presented as follows:

- *Concept/definition*: to identify system requirements and develop system specifications.
- *Design/development*: to conduct preliminary design and develop viable system functions to meet performance objectives.
- *Realization/implementation*: to produce, out-source or acquire the system elements in hardware and software forms for assembly of subsystems suitable for human interactions as needed in system operation.
- *Operation/maintenance*: to engage the system for provision of operational service and to sustain the prescribed level of system performance capability.
- *Enhancement*: to improve the system performance with additional features.
- *Retirement/decommission*: to end the existence of the system entity.

The description of system life cycle stages in Figure 2 is viewed from a generic systems engineering perspective. There are other system life cycle descriptions. IEC 60300-2 describes the product life cycle phases from a project management view. ISO/IEC 15288 provides a similar system life cycle description from a software engineering view. Whereas there are some differences in the use of terms presented in these standards, their alignments are noticeable at the transition points of their respective system life cycle stages or project phases.

Each stage has its own specific objectives to be met by the system design process, such as limited access to maintenance during system operation, recyclable parts for ease of disposal. Each stage also requires different internal procedures and work instructions, as well as requiring different contractual conditions to be met. Defining system requirements and developing system solutions during concept/definition and design/development stages can affect subsequent stages in system operation/maintenance. Decisions made for system architecture and technology selection in system design can have an effect on production, system integration and enhancement efforts, and constraining the disposal process.

The time duration of a system life cycle is affected by various factors depending on the system type and application, the technology used, and the support provision. For example, the life cycle of a motor vehicle may last from 7 to 15 years due to mechanical wear and chassis deterioration, whereas a personal computer may have a life-span of less than 5 years due to technology obsolescence. The time duration for application is the useful life of the system.

4.3 Fonctionnement du système

L'objectif premier de la conception d'un système et de l'application est l'atteinte des performances prévues en fonctionnement. L'étape de fonctionnement de la durée de vie du système représente la partie utile du cycle de vie du système. Pendant le fonctionnement, le système est surveillé, maintenu et soutenu comme le requièrent les objectifs opérationnels.

La plupart des fonctionnements de système suivent un schéma de fonctionnement générique d'utilisation moyenne reflétant l'application réelle. Au cours du fonctionnement, les fonctions sont nécessaires pour que les performances attendues du système soient disponibles en permanence ou sur demande en tenant les exigences de performance. Dans certains cas, il existe une période de garantie représentant une sous-étape pendant le fonctionnement initial du système. Pendant les périodes de garantie, la maintenance du système et le travail de support peuvent être plus intenses pour des motifs commerciaux ou contractuels, qu'après la période de garantie pour le reste de la partie utile du fonctionnement du système. La plupart des systèmes disponibles dans le commerce, par exemple des véhicules motorisés ou des systèmes "home vidéo", se conforment à un schéma générique de fonctionnement et de maintenance.

Cependant, il existe des systèmes conçus pour répondre à un objectif opérationnel dédié pour lesquels un profil opérationnel spécifique devra être établi.

La dégradation de la performance d'un système peut être représentée par une étape de fonctionnement séparée. Lors du fonctionnement normal d'un système, une performance dégradée qui n'affecte pas le fonctionnement de façon critique est tolérable dans des limites prédéterminées. Par exemple, quelques incidents isolés de d'interruption de ligne de client d'un commutateur de télécommunication, provoqués par des ruptures de lignes peu fréquentes dans des conditions atmosphériques mauvaises sont considérés normalement acceptables. Le client privé pourra tolérer ces événements rares si le service est rapidement restauré. Cependant, la fréquence des interruptions peut représenter dans des cas rares un scénario de performance dégradée. La dégradation aura un effet sur la qualité du service fourni par le système.

Il convient que les situations et réponses d'urgence soient traitées par des étapes séparées.

4.4 Profil opérationnel d'un système

Un profil opérationnel est la séquence des tâches que le système doit accomplir pour atteindre son objectif opérationnel. Le profil opérationnel représente un scénario de fonctionnement spécifique pour le système en exploitation. Par exemple, l'objectif d'un avion de ligne volant d'un point A à un point B est de fournir un service passager; un profil opérationnel peut être établi pour l'avion consistant à effectuer les tâches de décollage, de vol et d'atterrissage pendant son fonctionnement. Associées à chaque tâche spécifique, il existe des activités et des conditions spécifiques établies pour être effectuées par l'avion. Les critères sont établis à la fin ou au début de chaque tâche pour déterminer son succès avant de poursuivre ou d'abandonner l'opération ultérieure.

Les tâches dans le profil opérationnel peuvent aussi être atteintes par la mise en oeuvre de diverses fonctions conçues dans le système. Pour une perspective opérationnelle d'un système, certaines des fonctions sont critiques et elles peuvent nécessiter l'incorporation d'exigences spécifiques de sûreté de fonctionnement pour accomplir les tâches désignées. D'autres fonctions peuvent être non critiques; elles peuvent ne pas être nécessaires aux tâches désignées. Par exemple, les moteurs d'avion sont des fonctions critiques pour accomplir les tâches de décollage, de vol et d'atterrissage. Cependant les trains d'atterrissage sont utilisés uniquement pour le décollage et l'atterrissage. La fonction de train d'atterrissage n'est pas utilisée pendant le vol. Une analyse du profil opérationnel du système peut aider à déterminer les besoins d'application et les cycles de charge des fonctions spécifiques pendant le fonctionnement. La Figure 3 montre les relations entre, d'une part le profil opérationnel et le scénario opérationnel dans le fonctionnement du système et d'autre part, les étapes du cycle de vie.

4.3 System operation

The primary objective of a system design and application is aimed at achieving its intended performance during system operation. The operation stage of the system life cycle represents the useful life or service life of the system. During operation the system is monitored, maintained, and supported as needed to sustain operational objectives.

For most system operations, they follow a generic operating pattern of average usage reflecting the actual application. The functions during operation are needed to carry out the intended system performance all the time or to be available upon demand to meet performance requirements. In some cases, there is a warranty period representing a sub-stage during initial operation of the system. During guarantee and warranty periods, the system maintenance and support effort may be more intensive for business or contractual reasons than those normally applied after warranty for the remaining useful life of the system operation. Most commercially available systems, such as a motor vehicle or a home entertainment system, fit into this generic pattern for operation and maintenance.

However, there are systems designated for serving a dedicated operational objective where a specific operating profile will need to be established.

Degradation in system performance should be presented by a separate operation stage. Under normal system operation, degraded performance of system without affecting critical operation is tolerated up to a predetermined limit. For example, a few isolated outage incidents of subscriber lines of a telecommunications switching system due to infrequent lightning strikes in bad weather conditions is normally considered acceptable. The general public customers would tolerate such rare events subject to expedient restoration to full service within reasonable time. However, the occurrence of outages in such rare events still represents a degraded performance scenario. Degradation will have an effect on the quality of service provided by the system.

Emergency situations and responses should be treated as separate stages.

4.4 System operating profile

An operating profile is the sequence of tasks to be performed by the system to achieve its operational objective. The operating profile represents a specific operating scenario for the system in operation. For example, the objective of a commercial aircraft flying from point A to point B is to deliver passenger service; an operating profile can be stated for the aircraft to perform the tasks of take-off, flight, and landing during its specific operation. Associated with each specific task, there are specific activities and conditions set forth for the aircraft to perform. Criteria are established at the completion or start of each task to determine its success before continuation or to abort further operation.

The tasks in an operating profile can only be achieved through the implementation of various functions designed into the system. From a system's operational perspective, some of the functions are critical that may demand incorporation of specific dependability requirements to achieve the designated tasks. Other functions may be non-critical; they may not be needed for those designated tasks. For example, the aircraft engines are critical functions to carry out the tasks of take-off, flight, and landing. However, the landing gears are only used during take-off and landing. The landing gear function is not needed during flight. An analysis of the system operating profile may help determine the application needs and duty cycles of specific functions during operation. Figure 3 shows the relationships of operating profile and operating scenario in system operation to the system life cycle stages.

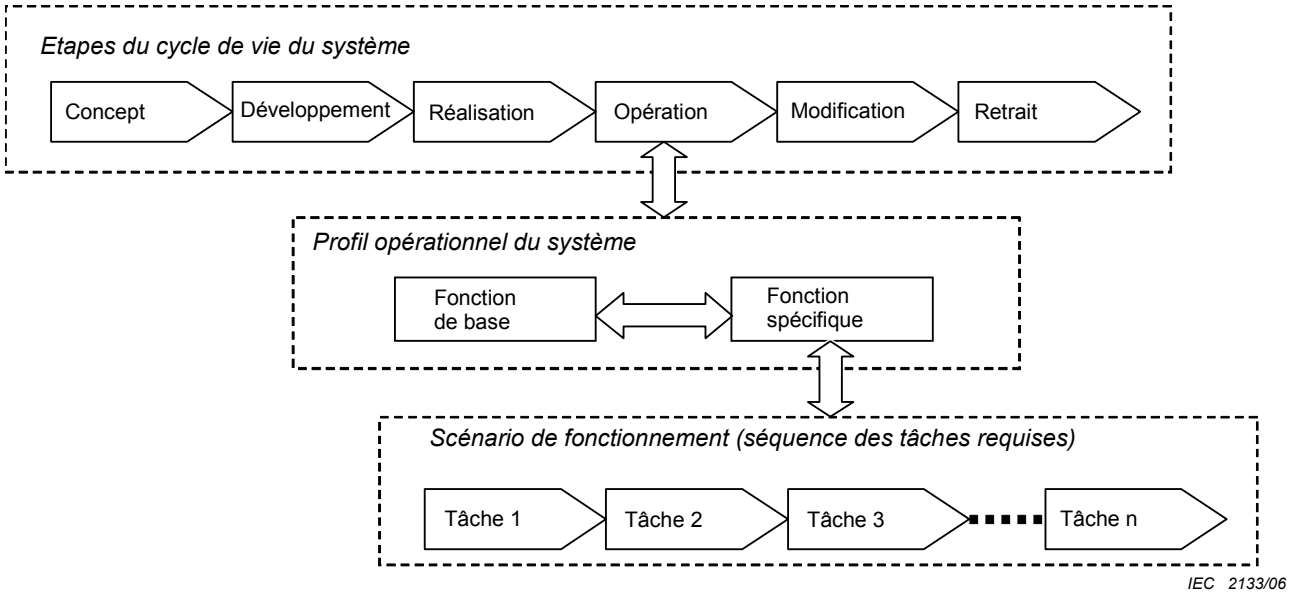


Figure 3 – Relations entre un profil opérationnel d'un système et un scénario de fonctionnement du système

4.5 Exigences de sûreté de fonctionnement

4.5.1 Exigences de sûreté de fonctionnement pour les fonctions systèmes

Pendant les étapes de définition et de conception du cycle de vie d'un système, l'objectif de la conception est focalisé sur la réalisation des fonctions pour la performance du système en fonctionnement. Les exigences de sûreté de fonctionnement pour les fonctions d'un système peuvent être déterminées seulement après que les fonctions ont été identifiées par le processus de conception du système. Pour la plupart des systèmes suivant un schéma fonctionnel générique, le système requiert que toutes les fonctions respectent les exigences de sûreté de fonctionnement pour maintenir le fonctionnement. C'est-à-dire qu'en fonctionnement, toutes les fonctions du système sont nécessaires pour atteindre la performance attendue du système en permanence ou sur demande.

Les exigences de sûreté de fonctionnement dans un fonctionnement spécifique peuvent requérir certaines fonctions clé sélectives pour accomplir les tâches. Ces fonctions clé sont critiques pour la performance réussie du système pendant le fonctionnement spécifique. Par exemple, la disponibilité du déploiement du train d'atterrissage pendant le décollage et l'atterrissage.

La procédure d'application pour spécifier la sûreté de fonctionnement d'un système est obtenue par différenciation entre les fonctions qui ont une influence sur la sûreté de fonctionnement du système, et celles qui n'en ont pas.

Pour développer les exigences pour la sûreté de fonctionnement d'un système, une description du profil opérationnel est nécessaire. Cela est fait par l'évaluation des fonctions pertinentes pour la sûreté de fonctionnement, qui implique une analyse des conditions influentes affectant les caractéristiques sélectionnées de sûreté de fonctionnement.

4.5.2 Caractéristiques de la sûreté de fonctionnement

Les concepts de la sûreté de fonctionnement sont décrits dans la CEI 60300-1 et définis dans la CEI 60050(191). Les caractéristiques de la sûreté de fonctionnement applicables à une spécification de système incluent:

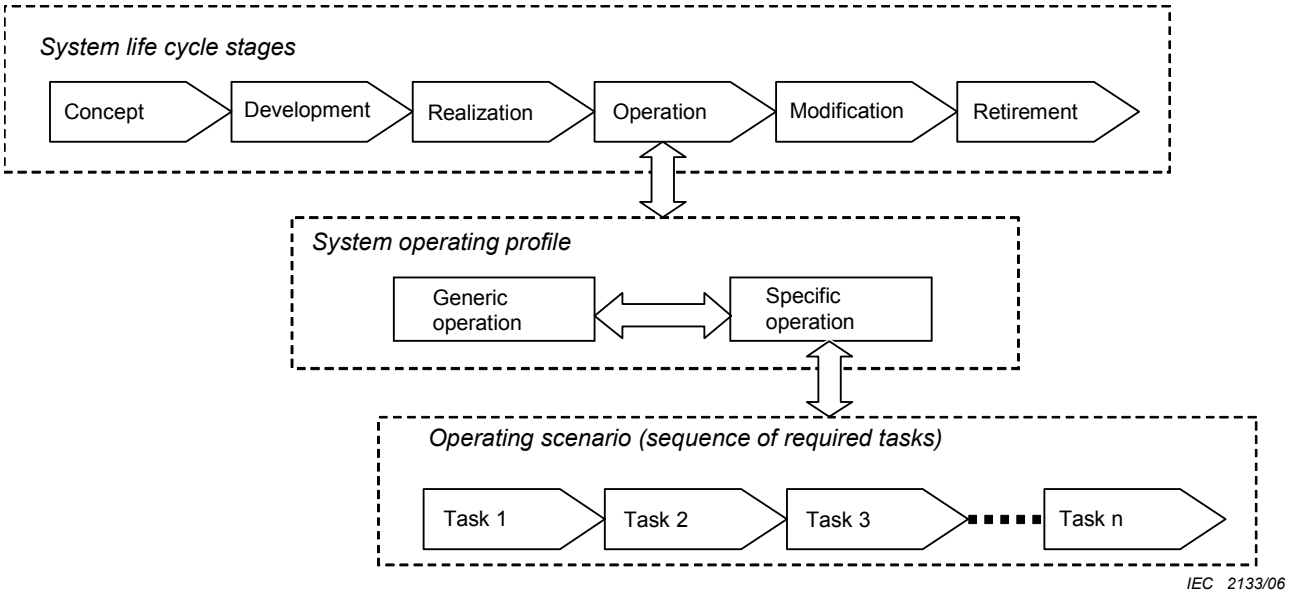


Figure 3 – Relationships of system operating profile and scenario in system operation

4.5 Dependability requirements

4.5.1 Dependability requirements for system functions

During the definition and design stages of the system life cycle, the design objective is focused on realizing the functions for system performance during operation. Dependability requirements for system functions can only be determined after the functions have been identified by the system design process. For most systems following a generic operating pattern, the system demands all functions to meet dependability requirements for sustained operation. That is, all system functions during operation are needed to carry out the intended system performance all the time or be available upon demand.

Dependability requirements in a specific operation may require certain selective key functions to complete the tasks. These key functions are critical to the successful performance of the system during the specific operation. For example, the availability of landing gear deployment during aircraft take-off and landing.

The application procedure for specifying system dependability is done by differentiating between those functions that do and those that do not influence system dependability.

To develop the requirements for specifying system dependability, a description of the operating profile is necessary. This is done through the evaluation of functions relevant to dependability, which involves an analysis of influencing conditions affecting the selected dependability characteristics.

4.5.2 System dependability characteristics

The dependability concepts are described in IEC 60300-1 and defined in IEC 60050(191). The dependability characteristics applicable to system specification include:

- la performance de disponibilité;
- la performance de fiabilité;
- la performance de maintenabilité;
- la performance du support de maintenance.

Du point de vue de l'application du système, l'efficacité du fonctionnement sur demande est un élément fort de la performance de disponibilité. La performance de fiabilité représente la longévité du fonctionnement du système sans aucun incident affectant une rupture du système ou une dégradation. La performance de maintenabilité est la facilité à accéder aux services de maintenance du système, la restauration ou le recouvrement du système sur site ou à distance. La performance du support de maintenance fournit la capacité organisationnelle et les ressources nécessaires pour maintenir un fonctionnement en continu du système.

4.5.3 Critères d'acceptation de la sûreté de fonctionnement du système

Pour les applications de la sûreté de fonctionnement d'un système, les critères d'acceptation incluent, sans y être limités:

- la démonstration de l'atteinte des objectifs de la sûreté de fonctionnement du système par une vérification progressive de la performance à diverses étapes du cycle de vie, en atteignant les exigences ciblées pour chaque étape ;
- la démonstration de la complétude réussie des cas d'essai pour simuler la performance de fonctionnement du système, les dysfonctionnements et les recouvrements ;
- l'apport de l'évidence objective de l'historique de la performance et de données portant sur des systèmes analogues en exploitation et relatives à l'atteinte des objectifs de sûreté de fonctionnement du système ;
- l'atteinte des durées "sans faute" établies pour l'acceptation pendant la mise en service du système et la période de garantie de fonctionnement du système ;
- les dispositions pour les règles de retour ou de remplacement, les incitations de garantie et l'extension des contrats de service de maintenance pour maintenir un fonctionnement en continu du système.

Etablir les critères d'acceptation de la sûreté de fonctionnement de systèmes complexes constitue souvent un processus de collaboration entre les parties contractantes. Des exemples vont de la mise en service d'un nouveau réseau de télécommunication aux services de maintenance d'un contrat de tierce-partie et à l'installation de systèmes applicatifs logiciels pour inventaire et réorganisation de stocks. La spécification de la sûreté de fonctionnement d'un système peut refléter la nature particulière du type d'affaire.

4.5.4 Vérification des fonctions du système

Un système peut consister en toute combinaison de matériels, de logiciels et d'éléments humains. Etant entendu qu'une telle combinaison d'éléments peut être démontrée par l'utilisation de critères établis pour l'acceptation de la sûreté de fonctionnement, des produits individuels matériels ou logiciels servant comme fonctions du système peuvent utiliser les approches pour la vérification et la validation telles que décrites dans la CEI 60300-3-4 pour le domaine de l'acceptation de produits et de spécifications. Pour les produits logiciels du commerce (COTS), il est essentiel d'en spécifier la taille et la durée d'exécution, les exigences d'interfaces et de protocoles pour faciliter la vérification de l'interopérabilité et l'intégration du système. Quand des éléments sont impliqués, soit servant indépendamment comme fonctions spécifiques du système ou soit intégrées comme partie du système, des exigences de compétences et de formation sont nécessaires pour la spécification des fonctions. Ceci est souvent démontré par la complétude des exigences de formation et la certification.

- availability performance;
- reliability performance;
- maintainability performance;
- maintenance support performance.

From a system application perspective, availability performance exhibits the efficacy of system operation upon demand. Reliability performance represents the longevity of system operation without any incidents affecting system outage or impairment. Maintainability performance is the ease of access for system maintenance services, on-site or remote system restoration and recovery. Maintenance support performance provides the needed organizational capability and resources to sustain continuity of system operation.

4.5.3 System dependability acceptance criteria

For system dependability applications, criteria for acceptance include, but are not limited to a combination of the following:

- demonstrating achievement of system dependability objective by means of progressive performance verification at various life cycle stages in meeting target requirements established for each stage;
- demonstrating successful completion of test cases to simulate system performance operation, malfunction and recovery;
- providing objective evidence of performance history and data of similar systems deployed in field operation in meeting system dependability objective;
- achievement of established failure-free time duration for acceptance during system commissioning and warranty period of system operation;
- provision of return or replacement policy, warranty incentives, and extension of maintenance service contracts to sustain continuity of system operation.

Establishing system dependability acceptance criteria for complex systems often constitutes a collaborative process between contracting parties. Examples include commissioning of a new telecommunications network, provision of third-party contract maintenance services, and installation of software application systems for inventory control and stock reordering. System dependability specification should reflect the particular nature of the business.

4.5.4 Dependability verification of system functions

A system can consist of any combination of hardware, software, and human elements. Whereas such combination of system elements may be demonstrated by using the criteria established for system dependability acceptance, individual hardware or software products serving as system functions may utilize the approaches for verification and validation as described in IEC 60300-3-4 for product acceptance and specification purposes. For COTS software products, it is essential to specify size and run time, interface and protocol requirements to facilitate interoperability verification and system integration. When human elements are involved, either independently serving as specific system functions or integrated as part of the system operation, skills and training requirements are needed for specification of functions. This is often demonstrated by completion of training requirements and certification.

5 Procédure pour spécifier la sûreté de fonctionnement d'un système

5.1 Processus de spécification d'un système

Le processus de spécification d'un système suppose que les entrées du marketing sont disponibles pour la définition du système et que les conditions associées pour définir l'objectif du système ont été fournies. Le point de départ du processus est l'identification du système et le développement des exigences nécessaires conduisant à la spécification par fonctions, de la sûreté de fonctionnement du système.

La Figure 4 donne une vue d'ensemble du processus de spécification d'un système. Elle identifie la séquence des activités du processus montrant les résultats des activités de sûreté de fonctionnement du système dans le processus de spécification du système. Les activités du processus dans l'*identification du système* en définissant ses exigences sont basées sur les besoins de l'utilisateur et les contraintes des applications du système. Les activités du processus dans *l'analyse des exigences* transforment la vision de l'utilisateur sur les applications du système en une vision technique pour l'ingénierie du système. Les activités du processus dans la *conception de l'architecture* synthétisent une solution qui satisfait aux exigences du système pour des scénarios de fonctionnement, en identifiant les fonctions nécessaires. Les activités du processus dans la *conception fonctionnelle* et l'*évaluation* déterminent les moyens pratiques de réalisation des fonctions pour faciliter les compromis de conception et l'optimisation. Les activités du processus dans la *documentation de la conception du système* fournissent les informations sur le système, y compris les données de sûreté de fonctionnement appropriées pour la conception du système. Le processus détaillé pour l'ingénierie de la sûreté de fonctionnement dans les systèmes est décrit dans la CEI 60300-3-15 (à l'étude).

5.2 Processus de spécification de la sûreté de fonctionnement d'un système

Il convient que la spécification de la sûreté de fonctionnement du système soit une partie intégrante du processus de spécification du système, ceci afin de faciliter le travail de conception du système. Les activités de sûreté de fonctionnement peuvent être conduites simultanément au processus d'ingénierie des systèmes afin d'assurer la coordination temporelle et les travaux en collaboration.

Une spécification de sûreté de fonctionnement d'un système est l'allocation des exigences de sûreté de fonctionnement à chaque fonction pertinente du système du point de vue de la sûreté de fonctionnement. La spécification de sûreté de fonctionnement peut varier avec la configuration du système, le mode de fonctionnement et les conditions influentes applicables. La spécification fournit un ensemble d'exigences clés de sûreté de fonctionnement des fonctions pertinentes du système et de caractéristiques liées pour initier la conception du système.

Du point de vue du système, les exigences du système détaillent la performance du système et la spécification du système prescrit les contenus du système. Les exigences sont requises essentiellement pour décrire la réalisation dans un accord contractuel. Une spécification représente un état précis des exigences. Pour d'autres propos, une spécification est généralement utilisée comme base pour établir une compréhension claire des exigences par les parties contractantes. Les exigences forment la base du contrat pour un accord commercial.

La CEI 60300-3-4 fournit des détails sur la spécification des exigences de sûreté de fonctionnement. Le processus décrit ici étend les applications pour inclure la spécification par fonctions pour des systèmes complexes et des systèmes interactifs.

La Figure 4 montre aussi les relations d'activités diverses de processus impliquées dans la spécification du système, y compris celles liées à l'évaluation de la sûreté de fonctionnement pour établir des valeurs pour les exigences de sûreté de fonctionnement.

5 Procedure for specifying system dependability

5.1 System specification process

The system specification process assumes that market input is available for system definition and that the associated conditions for completing the system objective have been provided. The starting point for the process is to identify the system and develop the necessary requirements leading to specifying system dependability by functions.

Figure 4 presents an overview of the system specification process. It identifies the sequence of process activities showing the outcomes of the system dependability activities in the system specification process. The process activities in *system identification* by defining its requirements are based on the users' needs and constraints of system applications. The process activities for *requirements analysis* transform the users' view on system applications into a technical view for engineering the system. The process activities in *architectural design* synthesize a solution that satisfies system requirements for operating scenarios by identifying the necessary functions. The *functional design and evaluation* process activities determine the practical means for realizing the functions to facilitate design trade-off and optimization. The process activities in *system design documentation* provide the system information, including dependability data, suitable for system design. A detailed process for engineering dependability into systems is described in IEC 60300-3-15 (under consideration).

5.2 System dependability specification process

Specifying system dependability should be an integral part of the system specification process to facilitate the system design effort. The dependability activities should be conducted concurrently with the systems engineering process to ensure timely coordination and collaborative effort.

A system dependability specification is the allocation of dependability requirements for each relevant function of the system from a dependability perspective. Dependability specification may vary with system configuration, mode of operation, and the applicable influencing conditions. The specification provides a set of key dependability requirements of relevant system functions and related characteristics for the initiation of system design.

From a system perspective, the system requirements detail the system's performance, and the system specification prescribes the system's contents. Requirements are an essential requisite for seeking fulfilment in a contract agreement. A specification represents a precise statement of the requirements. Among other purposes, a specification is generally used as the basis for establishing clear understanding of the requirements by the contracting parties. Requirements form the basis for the contract intent in reaching business agreements.

IEC 60300-3-4 provides details on specification of dependability requirements. The process described herein extends the applications to include specification by functions for complex systems and interacting systems.

Figure 4 also shows the relationships of various process activities involved in system specification, including those related to dependability assessment, to establish values for dependability requirements.

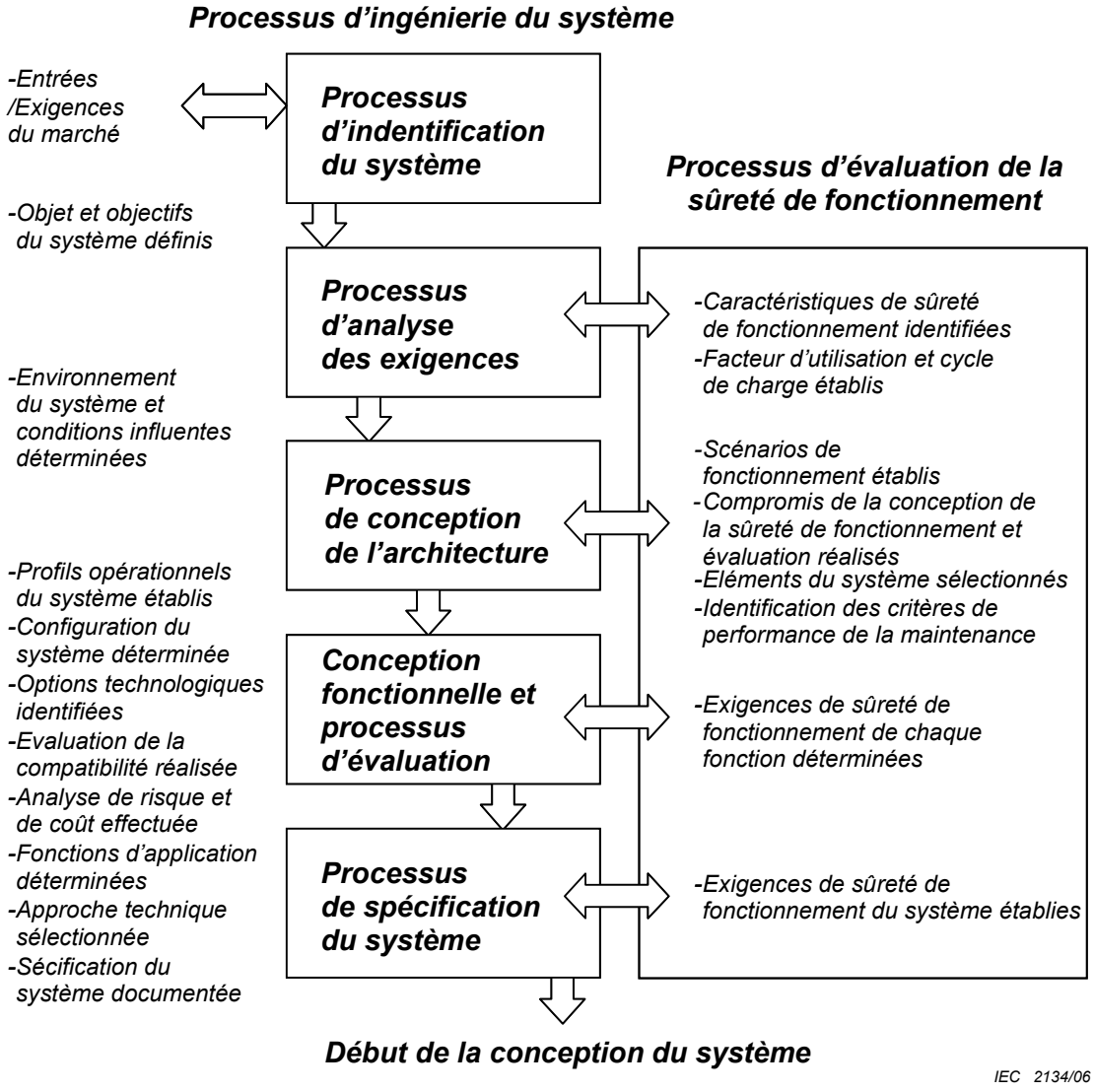


Figure 4 – Vue générale du processus de spécification d'un système

5.3 Détermination des valeurs de la sûreté de fonctionnement

La sûreté de fonctionnement est un terme collectif pour décrire la performance de disponibilité et ses facteurs influents: la performance de fiabilité, la performance de maintenabilité et la performance de support de maintenance. L'expression, « sûreté de fonctionnement » est utilisée pour des descriptions générales et non quantitatives. Pour caractériser la sûreté de fonctionnement, des mesures quantitatives sont utilisées pour assigner des valeurs à la disponibilité, à la fiabilité, à la maintenabilité et aux supports de maintenance. La détermination des valeurs des exigences de la sûreté de fonctionnement peut être obtenue en quantifiant les mesures applicables des caractéristiques pertinentes de la sûreté de fonctionnement. Les exemples suivants illustrent comment des valeurs de sûreté de fonctionnement sont interprétées en termes quantitatifs.

- Disponibilité: pourcentage de la durée utilisable pour le fonctionnement du système sur demande; fréquence de rupture et durée des temps d'arrêt
- Fiabilité: temps moyen entre défaillance; durée sans défaillance
- Maintenabilité: temps moyen avant restauration; temps de recouvrement

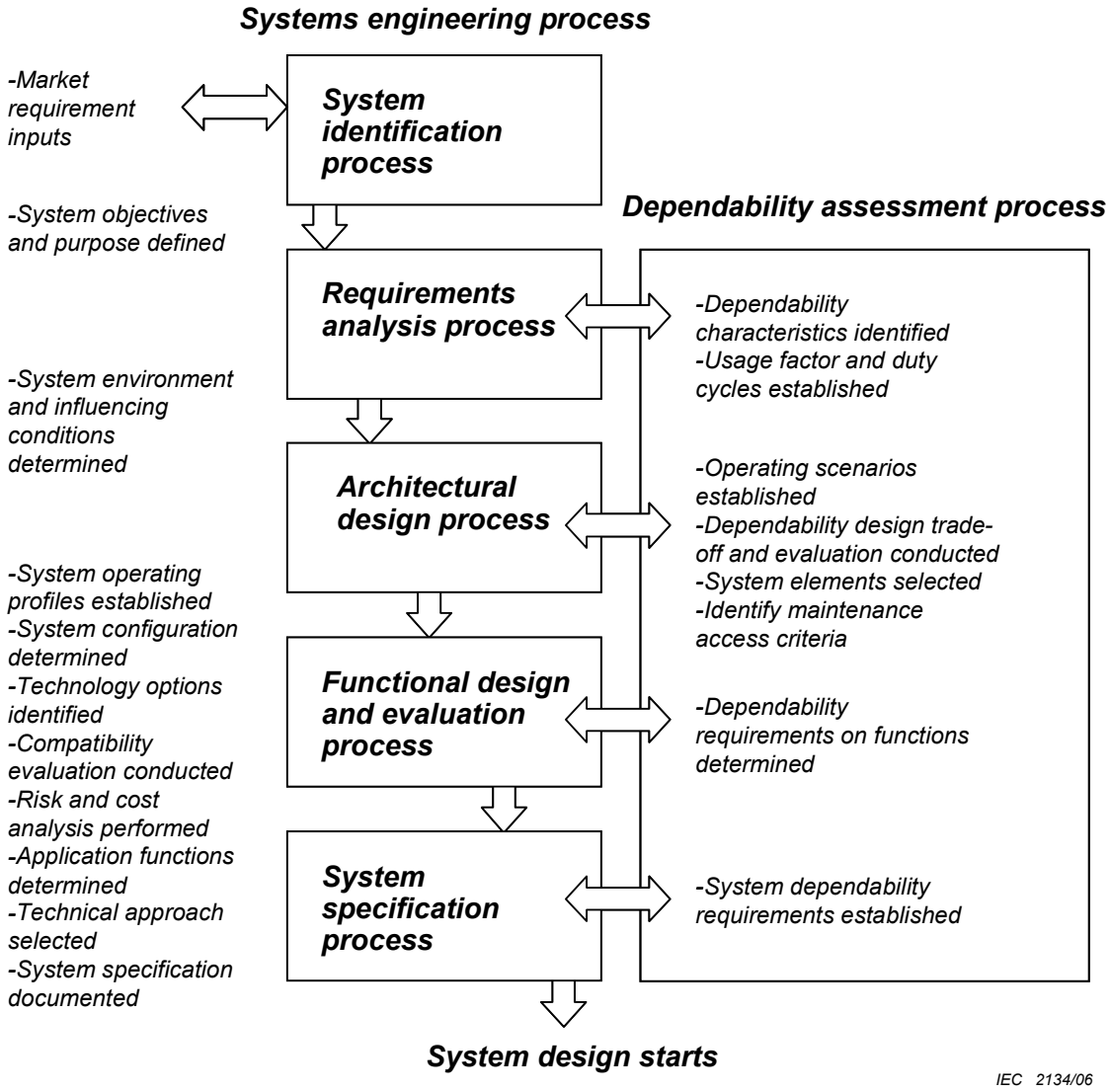


Figure 4 – Overview of system specification process

5.3 Determining dependability values

Dependability is a collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance. The term dependability is used for general descriptions and non-quantitative. To characterize dependability, quantitative measures are used to assign values for availability, reliability, maintainability and maintenance support. Determining the values for dependability requirements can be achieved by quantifying the applicable measures of the relevant dependability characteristics. The following examples illustrate how dependability values are interpreted in quantitative term or numerical form:

- availability: percentage uptime for the duration of system performance operation upon demand; outage frequency and downtime duration;
- reliability: mean-time-between-failures; failure-free duration;
- maintainability: mean-time-to-restore; recovery time;

- Support de maintenance: temps de réponse de la logistique; délai d'approvisionnement pour les pièces de rechange.

Pour le développement de nouveaux systèmes ou de fonctions nouvelles de système, les valeurs cibles de sûreté de fonctionnement sont habituellement déterminées avec les informations du marketing, l'analyse de la concurrence, les exigences des utilisateurs, les connaissances de base des applications technologiques et l'analyse des données de performance en exploitation. Pour les systèmes héréditaires, les valeurs cibles de sûreté de fonctionnement sont établies à partir de l'expérience en exploitation.

5.4 Etapes de procédure pour déterminer les exigences de sûreté de fonctionnement d'un système

5.4.1 Description des étapes de procédure

5.4.1.1 Généralités

La Figure 5 montre les étapes de procédure pour déterminer les exigences de sûreté de fonctionnement d'un système. Ce qui suit décrit le propos et le processus de chaque étape pour apporter des recommandations de procédure. L'Annexe B donne un exemple de développement de la spécification de la sûreté de fonctionnement d'un système.

- maintenance support: logistics delay time; turn-around time for spares provisioning.

For newly developed systems or system functions, the target dependability values are usually determined through market information, competitive analysis, customer requirements, technology application knowledge base, and analysis of field performance data. For legacy systems, the target dependability values are established from field performance experience.

5.4 Procedural steps for determining system dependability requirements

5.4.1 Description of procedural steps

5.4.1.1 General

Figure 5 shows the procedural steps for determining system dependability requirements. The following describes the purpose and process for each step to provide procedural guidance. Annex B shows an example on developing a system dependability specification.

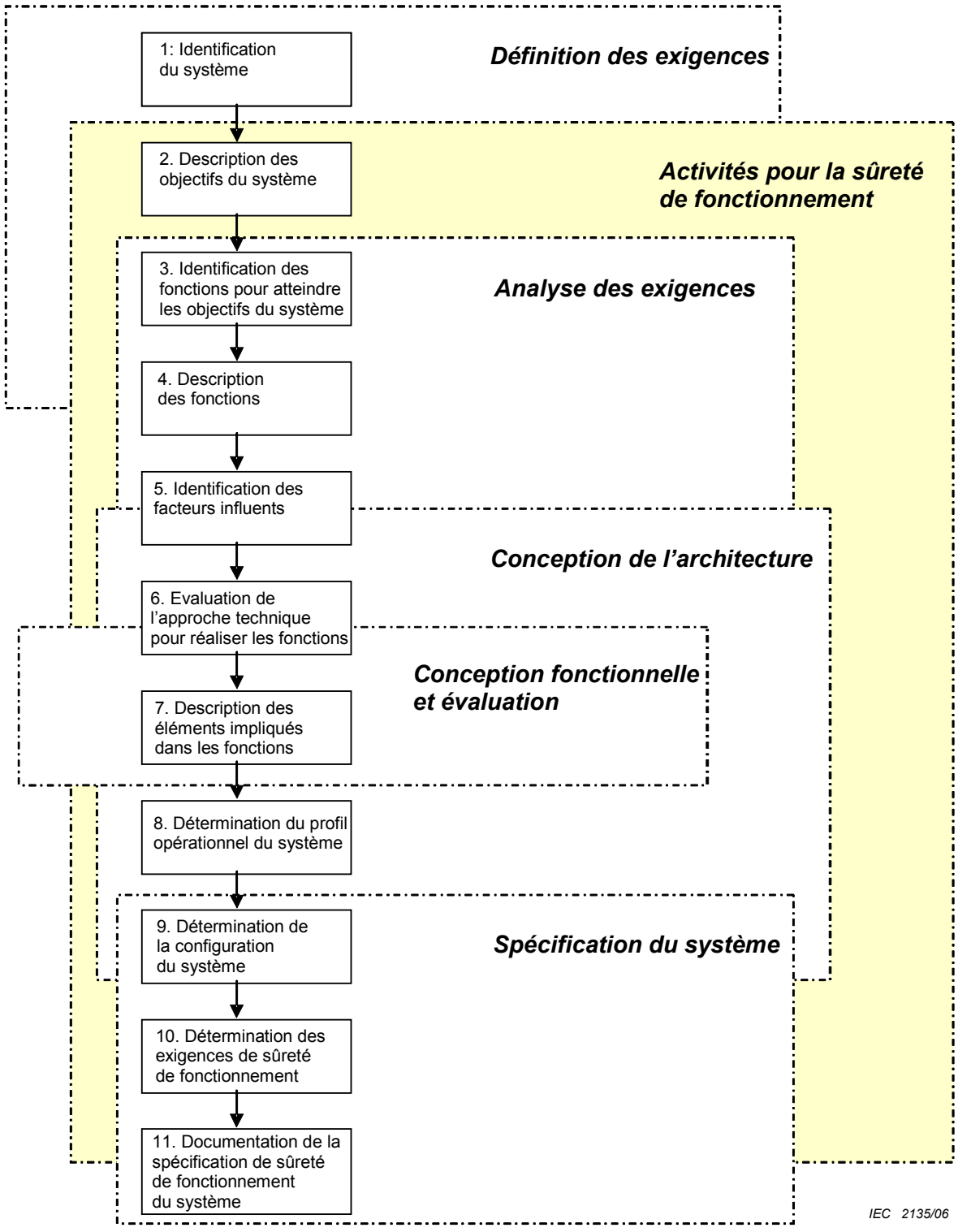


Figure 5 – Etapes pour déterminer les exigences de sûreté de fonctionnement d'un système

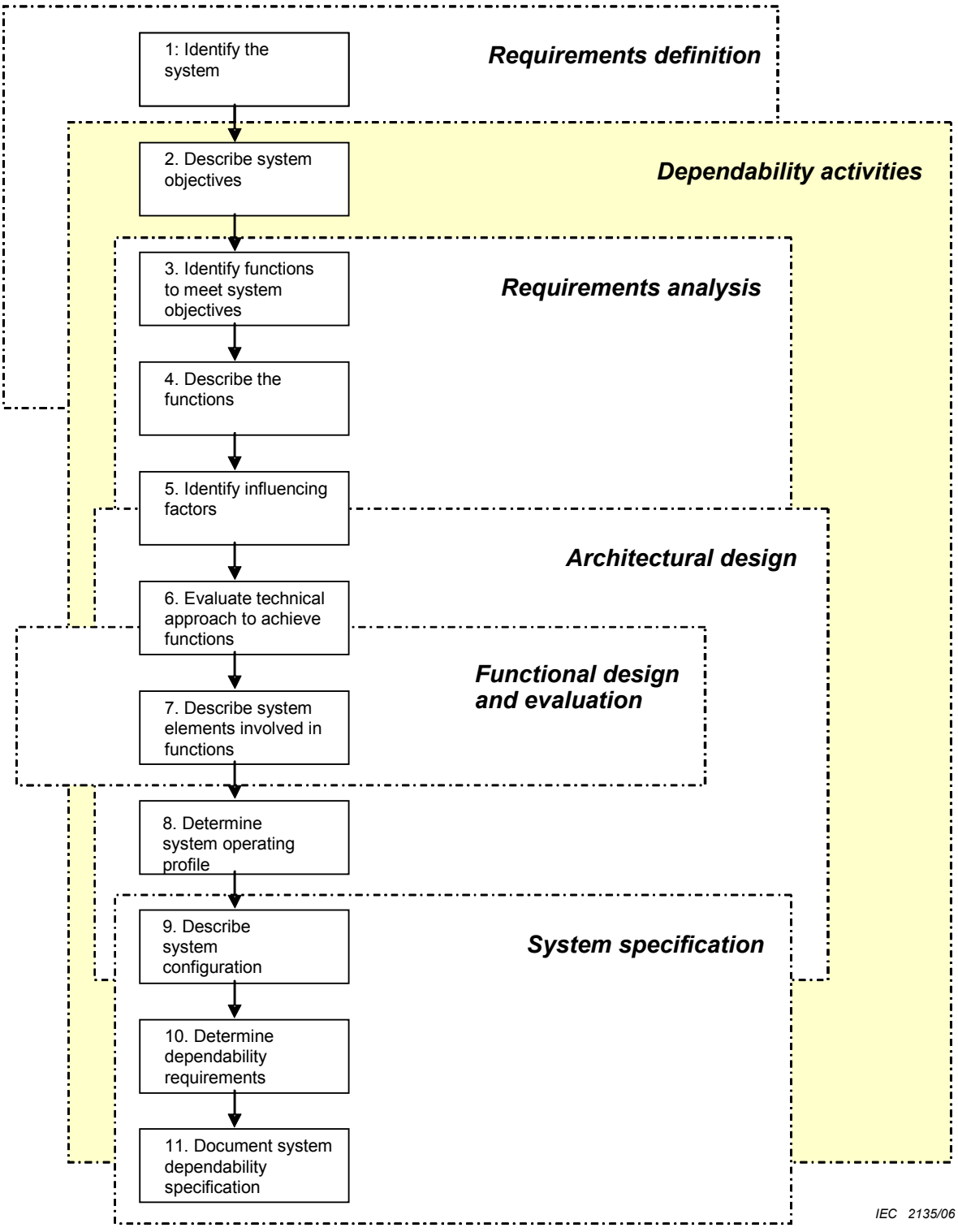


Figure 5 – Steps for determining system dependability requirements

5.4.1.2 Identifier le système

Il y a lieu que le système à l'étude soit identifié. Il convient que l'identification du système inclut le nom, le site d'exploitation et l'objet principal de l'application.

5.4.1.3 Décrire les objectifs du système

Il est recommandé que l'objet du système en termes d'application majeure soit établi et que l'objectif opérationnel soit l'obtention de la description du système.

5.4.1.4 Identifier les fonctions pour la tenue des objectifs d'un système

Il est recommandé que les fonctions clés nécessaires pour atteindre la performance du système soient identifiées. Il y a lieu que l'objet de chaque fonction soit établi du point de vue des exigences du système. Le cas échéant, il convient que les relations entre ces fonctions soient établies.

5.4.1.5 Décrire les fonctions

Il est recommnadé que chaque fonction identifiée nécessaire au système soit décrite pour fournir le champ d'application et l'objectif pour l'évaluation de la faisabilité de la réalisation de la fonction.

5.4.1.6 Identifier les conditions influentes

Il y a lieu que les facteurs influant affectant chaque fonction soient identifiés pour évaluer leur impact sur la performance du système. En utilisant l'Annexe A comme recommandations, les facteurs influant clés peuvent être identifiés à partir de la matrice de relations affectant les fonctions nécessaires au système.

5.4.1.7 Evaluer l'approche technique pour réaliser les fonctions

Il convient que l'approche technique pour la réalisation des fonctions soit évaluée. Il s'agit d'évaluer les moyens pratiques pour réaliser les fonctions dans les limites établies. L'approche technique traite de l'acquisition et du maintien des fonctions nécessaires pour maintenir le fonctionnement dans les contraintes de coût et de temps.

5.4.1.8 Décrire les éléments de système impliqués dans les fonctions

Il y a lieu que les éléments de système, consistant en des matériels, des logiciels et des interactions humaines impliquées dans les fonctions du système soient décrits. En régle générale, ceci est fait en tant que partie de l'ingénierie du système et du processus de conception déterminant les résultats pratiques et économiques dans la sélection et l'‘acquisition des fonctions.

5.4.1.9 Déterminer le profil opérationnel du système

Il convient que le profil opérationnel du système soit déterminé afin d'établir les différents scénarios de fonctionnement et la séquence des tâches nécessaires à la performance du système dans des conditions établies.

5.4.1.10 Décrire la configuration du système

Il convient que la configuration associée à chaque scénario de fonctionnement pour le profil opérationnel du système soit décrite. Il est recommnandé que les relations entre chaque fonction impliquée dans une configuration spécifique soient établies afin de faciliter les compromis de conception du système et l'évaluation. Lorsque des systèmes interactifs sont impliqués dans des opérations spécifiques, il convient qu'ils soient identifiés et que leurs frontières et interfaces soient aussi établies pour l'évaluation du système.

5.4.1.2 Identify the system

The system under consideration should be identified. System identification should include name, premise for use or operation, and primary purpose of application.

5.4.1.3 Describe system objectives

The purpose of the system in terms of its primary application should be stated. The operational objective to be achieved by the system should be described.

5.4.1.4 Identify the functions to meet system objectives

The key functions needed to achieve the system performance should be identified. The purpose of each function should be stated from a system requirements perspective. Where appropriate, the relationships of these functions should be established.

5.4.1.5 Describe the functions

Each identified function needed for the system should be described to provide a scope and objective for assessing the feasible realization of the function.

5.4.1.6 Identify influencing conditions

The influencing factors affecting each function should be identified to assess their impact on system performance. Using Annex A as guidance, key influencing factors can be identified from the matrix relationships affecting the functions needed by the system.

5.4.1.7 Evaluate the technical approach to realize the functions

The technical approach to realize the functions should be evaluated. This is to assess the practical means of achieving the functions within established limits. The technical approach deals with acquiring and maintaining the needed functions for sustained operation within cost and time constraints.

5.4.1.8 Describe the system elements involved in the functions

The system elements consisting of hardware, software, and human interactions involved in the functions for system operation should be described. This should be done as part of the systems engineering and design process to determine practical and cost-effective outcomes in the selection and acquisition of the functions.

5.4.1.9 Determine the system operating profile

The operating profile of the system should be determined to establish the different operating scenarios and the sequence of tasks needed for system performance under stated conditions.

5.4.1.10 Describe the system configuration

The system configuration associated with each operating scenario for the system operating profile should be described. The relationships of each function involved in a specific configuration should be established to facilitate system design trade-off and assessment. Where interacting systems are involved in specific operations, they should be identified and their boundaries and interfaces established for system evaluation.

5.4.1.11 Déterminer les exigences de sûreté de fonctionnement

Il est recommandé que les exigences de sûreté de fonctionnement des fonctions du système soient déterminées en établissant le scénario de fonctionnement du système et les exigences des fonctions spécifiques identifiées dans le processus d'évaluation. Il convient que chaque caractéristique de sûreté de fonctionnement associée à des fonctions clés soit traduite en un état d'évaluation quantitative dans la séquence événementielle spécifique du profil opérationnel. Quand cela est possible, il estrecommandé qu'une valeur quantitative soit assignée. Ce processus de caractérisation constitue la base pour la saisie de la spécification de sûreté de fonctionnement des fonctions du système dont le but est la satisfaction des objectifs de sûreté de fonctionnement.

5.4.1.12 Documentation de la spécification de sûreté de fonctionnement d'un système

Il y a lieu que la spécification de la sûreté de fonctionnement et les données pertinentes saisies soient documentées. Les exigences de sûreté de fonctionnement font partie de la spécification du système. Il convient que les informations portant sur la sûreté de fonctionnement soient enregistrées en vue d'une utilisation future comme entrées pour concevoir les fonctions applicables pour la tenue des exigences globales du système. La documentation servira aussi comme données de support pour faciliter la revue formelle de conception et la réalisation du produit, ainsi que la vérification du système et des modifications.

Il est recommandé que la documentation de la spécification de sûreté de fonctionnement du système inclut les données suivantes, comme faisant partie de la spécification du système:

- identification du système ;
- objectifs du système ;
- fonctions du système ;
- profil opérationnel du système ;
- maintenabilité du système et exigences d'accès à la maintenance ;
- configuration du système ;
- exigences de sûreté de fonctionnement pour chaque fonction ;
- un état sur la sûreté de fonctionnement du système.

5.4.1.11 Determine the dependability requirements

The dependability requirements of the system functions should be determined by establishing the system operating scenario and the requirements of the specific functions identified in the evaluation process. Each dependability characteristic associated with the key functions should be translated into a qualitative evaluation statement in the specific event sequence of the operating profile. Where possible a quantitative value should be assigned. This characterization process forms the basis for capturing the dependability specification of system functions to satisfy the dependability objectives.

5.4.1.12 Document system dependability specification

The system dependability specification and relevant data captured should be documented. Dependability requirements should form part of the system specification. The dependability information should be recorded for future use as input for designing the applicable functions to meet overall system requirements. The documentation will also serve as supporting data to facilitate design review and product realization, and for system verification and modification.

Documentation of the system dependability specification should comprise the following data as part of the system specification:

- system identification;
- system objectives;
- system functions;
- system operating profile;
- system maintainability and maintenance access requirements;
- system configuration;
- dependability requirements for each function;
- a statement on system dependability.

Annexe A
(informative)

Evaluation des caractéristiques de sûreté de fonctionnement

A.1 Exemples de facteurs influant sur la sûreté de fonctionnement du système

NOTE Les facteurs suivants sont disposés selon leur importance dans la plupart des situations.

A.1.1 Contraintes économiques

Les contraintes économiques résultent souvent de restrictions budgétaires, de limitations des dépenses ou de problèmes de planification ayant un impact sur l'avancement d'un développement de système et la réalisation d'un produit. Il convient que les contraintes économiques soient traitées comme des conditions influentes sur le processus de gestion de la sûreté de fonctionnement. Les premiers plannings traitant du coût de la conception, de la gestion de la chaîne d'approvisionnement et de l'analyse du coût du cycle de vie peuvent aider à identifier les domaines de problèmes potentiels, à mettre l'accent sur des évitements de coûts et pour créer des opportunités d'amélioration. L'analyse des risques du projet est souvent utilisée dans les exercices de planification pour déterminer la criticité de la situation, en permettant de tracer un enchaînement des actions.

A.1.2 Contraintes réglementaires

Les contraintes réglementaires peuvent être imposées par des services publics où des considérations de sécurité et d'impact sur l'environnement sont prépondérantes. La législation définit généralement un ensemble de méthodes, d'outils ou d'impositions techniques. Ces contraintes réglementaires constituent l'une des conditions influentes dans la stratégie d'évaluation de la conception d'un système et dans les plans de sûreté de fonctionnement.

> EXEMPLE: L'imposition d'un capot ou d'un couvercle sur un élément d'un système pour des raisons de sécurité peut modifier l'approche pour l'accès à cet élément. Comme conséquence, une modification dans la conception de la maintenabilité ou une modification du processus de support de maintenance peut être à introduire impérativement.

A.1.3 Type de fonctionnement de système

Le type de fonctionnement affecte le résultat des objectifs globaux du système. Le type de fonctionnement est lié à l'application du système, par exemple un système de transport urbain, ou un système de communication de nouveaux services de radiodiffusion. Il y a lieu que les caractéristiques de sûreté de fonctionnement associées à de tels systèmes soient évaluées en termes réglementaires, économiques, sociaux, techniques et autres domaines pertinents. Ce processus d'évaluation est lié à des prévisions positives. Par exemple, la prévision d'un réseau national réussi de distribution d'énergie est liée à la distribution effective de l'énergie électrique, facilitant ainsi les activités économiques du pays. Le résultat de l'évaluation peut créer le besoin d'un haut niveau de performance de fiabilité du système électrique. Le type de fonctionnement est en général lié à l'application du système, étant entendu que le mode de fonctionnement est lié au scénario de fonctionnement du système pour une tâche spécifique.

Annex A
(informative)

Evaluation of dependability characteristics

A.1 Examples of influencing factors on system dependability

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

A.1.1 Economic constraints

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

A.1.2 Regulatory constraints

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

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

A.1.3 Type of system operation

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

A.1.4 Criticité du fonctionnement

La criticité est le degré de gravité des conséquences possibles d'une défaillance du système. Les caractéristiques de sûreté de fonctionnement peuvent être évaluées en termes d'effets sur l'interaction humaine, l'impact économique, les conséquences environnementales, des contraintes anormales, un impact opérationnel et autres problèmes. Ce processus d'évaluation est lié à des considérations événementielles qui peuvent avoir un impact négatif. Par exemple, la maintenabilité d'un réseau national de distribution électrique est d'une grande importance, si l'on considère l'impact social et économique d'une rupture prolongée ou de la défaillance du système électrique national. Une situation de blackout peut survenir dans une cité du fait d'une utilisation excessive de l'électricité mettant le système de distribution électrique hors de ses capacités de fournitures aux heures de pointe.

A.1.5 Type d'utilisation

Un système peut avoir plusieurs type d'utilisation, comme:

- une utilisation unique ;
- une utilisation brève et une durée de stockage brève ;
- une utilisation brève et une durée de stockage prolongée ;
- une utilisation prolongée et une durée de stockage brève ;
- une utilisation prolongée avec maintenance ;
- une utilisation prolongée sans maintenance.

Le type d'utilisation du système affecte les caractéristiques de sûreté de fonctionnement.

- Pour une utilisation unique, la performance de sûreté de fonctionnement dépend du fonctionnement du système comme requis. Les caractéristiques incluent la disponibilité et la fiabilité. La maintenabilité et le support de maintenance sont pertinents uniquement pour le scénario de stockage.

  EXEMPLE: Il est recommandé qu'un lanceur spatial en stockage, maintenu en état de disponibilité atteigne une très grande fiabilité pendant son vol.

- Pour une utilisation brève et un stockage bref, le support de maintenance est d'une grande importance pour une performance de sûreté de fonctionnement réussie, du fait du temps restreint disponible pour maintenir le système.

  EXEMPLE: Il est recoomandé qu'un avion qui a un programme de support de maintenance très efficace puisse avoir un taux élevé d'opération de vol par rapport à la durée de la maintenance au sol.

- Pour une utilisation prolongée avec maintenance, la fiabilité, la maintenabilité et le support de maintenance sont d'égale importance. Les caractéristiques de sûreté de fonctionnement peuvent être optimisées pour le fonctionnement du système.

  EXEMPLE: Une centrale nucléaire est un exemple de ce type d'utilisation prolongée avec maintenance.

- Pour une utilisation prolongée sans maintenance, la fiabilité est d'une importance majeure et la maintenabilité est d'un intérêt mineur.

  EXEMPLE: Réparer un satellite en orbite est impraticable et la sûreté de fonctionnement du satellite dans l'espace est uniquement liée à sa haute performance de fiabilité.

A.1.4 Criticality of operation

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

A.1.5 Type of use

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

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

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

- For a one-shot use, dependability performance depends on the system functioning as required. Characteristics include availability and reliability. Maintainability and maintenance support are only relevant to the storage scenario.

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

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

  EXAMPLE: A plane that has a very efficient maintenance support programme should have a high flight operation to ground maintenance ratio.

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

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

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

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

A.1.6 Type d'utilisateurs

Il y a plusieurs types d'utilisateurs de compétence et de connaissances différentes qui peuvent intervenir dans le fonctionnement d'un système. Certains utilisateurs peuvent posséder une formation professionnelle avec une compétence et une connaissance élevée du fonctionnement du système. D'autres utilisateurs peuvent ne pas avoir acquis le même niveau de compétence et de connaissance pour faire fonctionner le même système. Cette condition influente peut affecter les caractéristiques de la sûreté de fonctionnement qui sont imposées à la conception du système pour prendre en compte différentes exigences relatives aux utilisateurs. Il convient qu'une attention particulière soit portée à l'étendue de l'interaction humaine avec le système lors de la conception des fonctions concernées, particulièrement pour un système possédant une interface ouverte au public.

EXEMPLE: Les exigences de maintenance varieront avec le niveau de compétence des utilisateurs du système. L'arrêt d'un système peut être une simple opération en appuyant sur un bouton, ou il peut exiger une procédure élaborée.

A.1.7 Sûreté de fonctionnement des systèmes interactifs

Un système peut être lié à un autre système, ou interagir avec de multiples systèmes afin d'atteindre son objectif. Dans ce cas, il est recommandé que leur dépendance soit définie dans la spécification de sûreté de fonctionnement, particulièrement dans les premiers et seconds rôles en relation avec le fonctionnement du système.

- Dépendance élevée: l'objet d'un système secondaire est de soutenir le système primaire dans son fonctionnement.
- Dépendance moyenne: un système est lié à d'autres systèmes mais ses fonctions sont indépendantes de ces systèmes.
- Dépendance faible: un système n'a pas de relation (à l'exception des sources d'énergie) avec d'autres systèmes. Il est capable de fonctionner seul.
- Dépendance temporaire gouvernée, par exemple, par l'initiation d'une routine logicielle sur commande pour réaliser un service spécial ou une action planifiée.

Pour un système à dépendance élevée, il est important d'intégrer la spécification de sûreté de fonctionnement du système secondaire comme faisant partie des exigences de sûreté de fonctionnement du système primaire.

EXEMPLE: La sûreté de fonctionnement d'un système d'alimentation de secours peut faire partie de la spécification de sûreté de fonctionnement de l'alimentation principale dans la spécification du système.

A.1.8 Structure ou configuration d'un système

Un système peut avoir différentes structures ou configurations consistant en une combinaison de divers éléments constituants. Par exemple:

Type 1: un système exclusivement matériel, sans logiciel ou élément humain impliqué ;

Type 2: un système exclusivement matériel, sans implication de logiciels mais avec une forte interaction humaine ;

Type 3: un système composé d'éléments matériels et logiciels, mais sans interaction humaine lors de son fonctionnement ;

Type 4: un système composé d'éléments matériels, logiciels et humains.

Pour un système de Type 1, les méthodes et outils classiques de sûreté de fonctionnement tels que recommandés dans la CEI 60300-3-4 sont pleinement applicables.

A.1.6 Type of users

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

EXAMPLE: Maintenance support requirements will vary with the skill level of the system's users. System shut-down could be a simple operation involving pressing a button, or it may require an elaborate procedure.

A.1.7 Dependency of interacting systems

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

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

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

EXAMPLE: Dependability of a back-up power supply should form part of the dependability specification of the main power supply in system specification.

A.1.8 Structure or configuration of a system

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

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

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

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

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

For a Type 1 system, classical dependability methods and tools as recommended in IEC 60300-3-4 are fully applicable.

Pour un système de Type 2, il convient que les études soient intégrées les approches des facteurs humains et particulièrement des bases de données de facteurs humains. Ces approches, pensées et définies pour certains secteurs industriels, ne sont pas actuellement normalisées.

Les systèmes de Type 3 et de Type 4 impliquent des éléments logiciels. Un logiciel dans sa forme stricte est déterministe, mais les logiciels en exploitation dans un système matériel avec des entrées réelles ne peuvent pas être évalués par les méthodes déterministes classiques. Il convient qu'une approche probabiliste soit utilisée pour évaluer le degré de confiance de la sûreté de fonctionnement dans la performance d'un système. L'identification des fonctions est similaire pour les éléments matériels et logiciels. Seule, la méthodologie pour l'évaluation de la sûreté de fonctionnement diffère dans son processus.

En pratique, la plupart des systèmes sont des combinaisons d'éléments personnalisés et d'éléments du commerce (COST).

A.1.9 Innovations techniques

Pour les systèmes fondés sur des nouvelles technologies, l'innovation implique la mise en oeuvre de nouvelles technologies ou l'utilisation de nouveaux procédés techniques pour la résolution de problèmes dans un système existant. Trois classes de systèmes sont identifiées:

- un système totalement nouveau utilisant une nouvelle technologie ;
- un système nouveau basé sur un système technologique existant et une technologie mature ;
- un système existant à modifier.

Pour un système totalement nouveau, l'absence de données provenant d'une expérience antérieure impose l'utilisation de méthodes formelles pour acquérir la confiance dans une conception détaillée avec une ingénierie de grande rigueur.

Pour un nouveau système basé sur un système technologique existant et une technologie mature, les méthodes de sûreté de fonctionnement classiques et les outils applicables au système existant peuvent être utilisés, mais il convient d'employer des procédés supplémentaires pour la vérification et la validation de la nouvelle configuration du système. Cela a pour but d'assurer la confiance dans la conception du nouveau système basé sur le système technologique existant et la technologie mature.

Pour un système existant qui est transformé en un système modifié, les méthodes classiques et les outils applicables de sûreté de fonctionnement peuvent être utilisés mais il est recommandé qu'ils soient vérifiés.

A.1.10 Nouveauté de fonctionnement

La nouveauté dans le fonctionnement fait référence à un nouvel état et à des objectifs opérationnels non explorés. Par exemple:

- établissement d'un objectif opérationnel totalement nouveau du nouveau système;
- extension du fonctionnement d'un système existant pour atteindre de nouveaux objectifs.

Pour un système complètement nouveau avec des objectifs opérationnels non explorés, l'absence d'une expérience antérieure impose une évaluation complète du profil opérationnel et de l'identification des tâches, incluant une évaluation de toutes les conditions influentes possibles rencontrées pendant le fonctionnement afin de définir les objectifs de sûreté de fonctionnement du système.

For a Type 2 system, the studies should integrate human factor approaches and specifically human factor databases. These approaches, though defined for some industrial sectors, are not yet standardized.

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

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

A.1.9 Technical novelty

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

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

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

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

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

A.1.10 Novelty of operation

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

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

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

Pour l'extension d'un système existant avec de nouveaux objectifs, les données issues de l'expérience antérieure peuvent être utilisées pour projeter l'extension de l'application du système. Un examen complet des modifications anticipées peut nécessiter d'être entrepris afin d'assurer que les ressources adéquates sont disponibles pour maintenir l'extension du système.

A.1.11 Problèmes héréditaires

Les problèmes héréditaires proviennent de l'infrastructure existante dans les grands systèmes complexes nécessitant une extension des services, une augmentation de capacité et une amélioration de performance. En ingénierie des systèmes, la définition de la plupart des exigences initiales et les travaux préliminaires de conception doivent traiter des problèmes héréditaires. Les problèmes héréditaires comprennent (mais ne sont pas limités à):

- la préservation des investissements dans l'infrastructure existante ;
- la résistance sociétale au changement et les contraintes règlementaires ;
- la couverture de l'assurance de l'existant par rapport aux nouvelles installations ;
- le redéploiement des ressources actuelles ;
- la formation nécessaire pour la transition des compétences ;
- les bénéfices du coût du cycle de vie et la justification pour les travaux d'amélioration.

Parfois, les ramifications des problèmes héréditaires sont de loin plus complexes et plus onéreuses pour l'extension d'un système existant que la construction d'un système complètement nouveau.

A.1.12 Complexité

Il y a lieu que la complexité d'un système soit évaluée du point de vue technique et du point de vue fonctionnel.

La complexité peut être évaluée en fonction du nombre d'interface entre les éléments ou les sous-systèmes et en fonction de son environnement, aussi bien qu'en fonction du nombre de configurations du système différentes possibles.

La complexité technique peut être évaluée en fonction du nombre de technologies différentes utilisées dans le système.

La complexité fonctionnelle est liée à la variété des principales caractéristiques du service ou des applications fonctionnelles du système.

A.1.13 Nombre de systèmes en exploitation

Le nombre de systèmes en exploitation peut influencer le choix des méthodes et des outils utilisés pour mettre en oeuvre la sûreté de fonctionnement. Si le nombre de systèmes identiques en exploitation est élevé, les données de l'expérience antérieure sont pertinentes et des données d'essai sont souvent disponibles. Un faible nombre de systèmes en exploitation peut conduire à une absence de données de retour d'expérience. Le choix des méthodes et des outils pour mettre en oeuvre la sûreté de fonctionnement peut être limité. Une démonstration de sûreté de fonctionnement peut être nécessaire pour vérification. Dans ce cas, des méthodes et outils probabilistes pour modéliser et simuler le système peuvent être utilisés.

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

A.1.11 Legacy issues

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

- preservation of investments in existing infrastructures;
- societal resistance to change and regulatory constraints;
- insurance coverage of existing versus new installations;
- re-deployment of current resources;
- training needs for skills transition;
- life cycle cost benefits and justification for enhancement efforts.

Sometimes the ramification of legacy issues is far more complex and costly in extending or upgrading an existing system rather than building a completely new system.

A.1.12 Complexity

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

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

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

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

A.1.13 Number of systems in use

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

A.2 Détermination des facteurs influents pertinents pour l'évaluation des fonctions d'un système

Le Tableau A.1 et le Tableau A.2 facilitent la détermination des facteurs influents affectant les caractéristiques des fonctions d'un système.

Tableau A.1 – Exemples de facteurs influents pour chaque condition influente

	Conditions influentes							
Facteurs influants	**Exigences de la tâche**	**Interaction humaine**	**Processus**	**Environ-nement**	**Service de support**	**Servitudes**	**Systèmes interactifs**	**Autres facteurs**
	Nature de la tâche	Commandes autorisées	Entrées/Sorties	Température	Maintenance	Alimentation	Frontières	Contraintes économiques
	Domaine	Interactions interdites	Modes	Humidité	Documen-tation	Fuel	Protocole	Contraintes règlementaires
	Durée	Interaction des définitions de rôles	Etapes	Vibration	Support technique	Energie	Interférences	Innovation technique
	Séquence	Formation	Cycles	Chocs	Pièces de rechange	Services publics	Sûreté de fonctionnement	Fonctionnement nouveau
	Mode de fonction-nement	Compé-tences	Protocole de défaillance	Pression	Outils spéciaux	Services privés		Complexité
	Démarrage	Interfaces		Rayonne-ment	Accès de maintenance	Communica-tions		Nombre de systèmes
	Fonction-nement normal			Contamina-tions	Niveaux de support			Degré de redondance
	Fonction-nement d'urgence			Stockage				
	Arrêt			Transports				

A.2 Determining relevant influencing factors for evaluation of system functions

Table A.1 and Table A.2 facilitate the determination of influencing factors affecting dependability characteristics of system functions.

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

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

Tableau A.2 – Relations entre les propriétés d'un système et les conditions influentes

Conditions influentes	Propriétés du système					
	Fonctionnalité	**Performance**	**Opérabilité**	**Sûreté de fonctionnement**	**Support**	**Applications spécifiques**
Exigences de la tâche	Identifier les fonctions pertinentes pour tenir les exigences des tâches	Identifier l'adéquation des fonctions à réaliser les tâches dans des conditions établies	Identifier les besoins opérationnels et les interfaces avec les fonctions	Identifier l'extension de fiabilité, de maintenabilité et de support de maintenance des fonctions	Identifier le service de logistique de support pour maintenir l'exécution des fonctions	Identifier les problèmes sanitaires et réglementaires imposés aux fonctions
Interaction humaine	Identifier l'implication de l'élément humain dans les fonctions	Identifier les compétences nécessaires pour la réalisation manuelle des fonctions	Identifier le degré de difficulté des opérations humaine dans les fonctions	Identifier la relation de l'intervention humaine affectant la performance de sûreté de fonctionnement des fonctions	Identifier les ressources humaines nécessaires au support des fonctions	Identifier les aspects humains dans l'application spécifique des fonctions
Processus	Identifier les procédures et las méthodes pour l'exécution des fonctions	Identifier la précision, la cohérence et la reproductibilité dans l'exécution des fonctions	Identifier la facilité d'utilisation et d'accès à l'exécution des fonctions	Identifier la disponibilité et la fiabilité de l'exécution des fonctions	Identifier l'extension des instructions des procédures et des travaux de maintenance pour maintenir l'exécution des fonctions	Identifier tout processus spécial nécessaire pour l'exécution des fonctions
Environnement	Identifier l'environnement dominant affectant la conception et l'exécution des fonctions	Identifier les limites opérationnelles ou les restrictions dans la performance des fonctions exposées à l'environnement	Identifier les limitations à l'accès et à l'utilisation des fonctions exposées à l'environnement	Identifier les effets sur la performance de la sûreté de fonctionnement des fonctions exposées à l'environnement	Identifier les limitations au support ou au service des fonctions exposées à l'environnement	Identifier toute précaution spéciale lors du fonctionnement dans un environnement extrême ou hostile
Services de support	Identifier le besoin des services de support pour maintenir l'exécution des opérations	Identifier les effets des services de support nécessaires pour maintenir l'exécution des fonctions	Identifier les effets des services de support pour l'amélioration de l'opérabilité des fonctions	Identifier les effets des services de support pour maintenir la performance de sûreté de fonctionnement des fonctions	Identifier tout service de support spécial pour la modification du système, la mise à niveau ou la destruction	Identifier tout service de support, spécial nécessaire pour les applications spécifiques
Servitudes	Identifier l'infrastructure pour l'exécution des fonctions	Identifier l'adéquation des servitudes pour maintenir l'exécution des fonctions	Identifier les effets des servitudes sur l'amélioration de l'opérabilité du système	Identifier les besoins et les effets des servitudes pour maintenir la performance de la sûreté de fonctionnement	Identifier toute source d'énergie spécifique fuel, etc. nécessaire pour soutenir le fonctionnement du système	Identifier tout outil spécifique nécessaire pour activer les systèmes nécessaires à l'application spécifique
Système interactif	Identifier l'influence des systèmes interactifs sur les fonctions	Identifier les effets du système interactif sur la performance des fonctions	Identifier l'incidence du système interactif sur l'opérabilité du système	Identifier les effets du système interactif sur la performance de la sûreté de fonctionnement	Identifier les frontières du système et l'incidence sur le support du système interactif	Identifier le système interactif pour l'application spécifique
Autres facteurs	Identifier les contraintes techniques et technologiques imposées aux fonctions	Identifier l'extension de l'utilisation et la complexité dans les applications affectant la performance de la fonction	Identifier les facteurs humains et sociaux affectant les fonctionnements normaux et spécifiques des fonctions	Identifier tout facteur spécial limitant ou restreignant le performance de la sûreté de fonctionnement	Identifier tout facteur spécial limitant ou restreignant le support du système	Identifier les contraintes économiques et règlementaires pour l'application spécifique

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

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

Annexe B
(informative)

Exemple de développement de spécification de sûreté de fonctionnement d'un système – Système de sécurité d'habitation individuelle

NOTE L'exemple suivant est utilisé comme illustration. La configuration du système et les procédures de fonctionnement sont typiques d'un système de sécurité d'habitation individuelle. Les données de sûreté de fonctionnement de cet exemple ne reflètent pas les résultats de performance du produit d'un constructeur spécifique ou du fonctionnement d'un service.

B.1 Etape 1: Identification du système

Un système de sécurité d'habitation individuelle est destiné à surveiller et commander dans un environnement domestique à l'aide d'alarmes déclenchées automatiquement en cas de danger ou d'intrusion et à alerter pour obtenir une protection. Un système de sécurité d'habitation individuelle est constitué de deux systèmes interactifs: un système autonome d'alarme d'habitation individuelle et un système séparé de service impliquant la police, les pompiers, les urgences médicales et d'autres services de protection et de sécurité.

B.2 Etape 2: Description des objectifs du système

Les objectifs du système sont:

a) détecter les risques de feu et de fumée et les intrusions dans l'habitation individuelle par un déclenchement d'alarme ;

b) alerter les autorités (c'est-à-dire la police, les pompiers, les urgences médicales, le prestataire de service de sécurité) pour obtenir une protection.

B.3 Etape 3: Identification des fonctions pour atteindre les objectifs

Un système de sécurité d'habitation individuelle possède les fonctions primaires suivantes:

a) Fonction de détection des risques de feu et de fumée ;

b) Fonction de commande pour traiter l'information ;

c) Fonction d'alarme pour alerter les occupants de l'habitation individuelle et les services de sécurité ;

d) Fonction de service de sécurité pour protéger l'habitation individuelle et les occupants d'un éventuel danger.

B.4 Etape 4: Description des fonctions

Les fonctions de détection, de commande et d'alarme sont nécessaires dans les locaux d'habitation individuelle. Ces trois fonctions basiques sont généralement intégrées dans un système d'alarme pour une installation dans une habitation individuelle. Cela répond au premier objectif du système de sécurité d'habitation individuelle.

a) La fonction de détection inclut:

- la détection de la présence du feu, de la fumée et des émissions d'oxyde de carbone à un niveau de risque dans l'habitation individuelle. Un moyen pratique de détection est de placer des dispositifs de surveillance tels que des capteurs en des endroits stratégiques dans les locaux ;

Annex B
(informative)

Example on developing a system dependability specification – Home security system

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

B.1 Step 1: Identify the system

The home security system is intended for monitoring and control in a home environment by setting alarms automatically in case of hazards or intrusion and alerting for security protection. A home security system consists of two interacting systems: a stand-alone home alarm system and a separate supporting security service system, involving the police, fire brigade, medical emergency, and other security protection services.

B.2 Step 2: Describe the system objectives

The objectives of the system are:

a) to detect fire and smoke hazards and intrusion in the home by setting alarm;

b) to alert the authorities (i.e. police, fire brigade, medical emergency, security service provider) for protection.

B.3 Step 3: Identify the functions to meet system objectives

A home security system has the following primary functions:

a) detection function for hazards and home intrusion;

b) control function for information processing;

c) alarm function to alert home occupants and security services;

d) security service function to protect home and occupants from possible harm.

B.4 Step 4: Describe the functions

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

a) Detection function includes:

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

- la détection d'intrusions, d'entrées forcées ou de la présence de personnes non autorisées dans les locaux. Un moyen pratique est de placer des capteurs de périmètre et des détecteurs de mouvements dans les endroits stratégiques dans l'habitation individuelle. Pour empêcher un cambriolage ou un accès non autorisé par des portes verrouillées et des fenêtres extérieures, des capteurs magnétiques, électriques et acoustiques peuvent être installés aux portes et aux fenêtres afin de détecter des entrées forcées et des bris de vitres de fenêtre.

b) La fonction de commande inclut:

- le traitement des signaux des capteurs pour activer l'alarme. Un moyen pratique pour le traitement des données est un processeur électronique avec un logiciel enfoui pour piloter l'unité de traitement ;
- la communication des données traitées à un affichage sur le panneau de commande pour une intervention humaine. La communication des données traitées et de l'affichage est réalisée au moyen de connexions câblées ou sans fil ;
- un convertisseur de tension fournit l'énergie électrique pour les fonctions du système. En cas de dysfonctionnement de l'alimentation principale ou de coupure, une batterie rechargeable peut être utilisée comme alimentation électrique de secours ;
- un contournement automatique peut être programmé pour commander les autorisations optionnelles d'enclenchement à distance. Quand il est programmé par un code autorisé, le système permet aux occupants de l'habitation individuelle de sortir dans un laps de temps prescrit (par exemple 90 s) avant la réactivation automatique du système. Le code autorisé est nécessaire pour pénétrer à nouveau dans les locaux dans un laps de temps prescrit sans que l'alarme soit activée pour une alerte pour un service de protection.

c) La fonction d'alarme inclut:

- la connexion directe par lignes téléphoniques pour alerter les services de sécurité sur une situation d'alarme ;
- la génération d'un son intense pendant une durée préétablie pour alerter les occupants. Ce peut être une sirène activée par le processeur, déclenchée par une situation d'alarme.

d) La fonction de service de sécurité inclut:

- l'activation d'une commande pour alerter le prestataire de services de sécurité pour les urgences. Cette activation peut utiliser la ligne d'appel téléphonique domestique entre le panneau de commande et le système de communication du prestataire de services de sécurité.

La fonction de service de sécurité requiert l'interaction du système d'alarme d'habitation individuelle avec d'autres systèmes fournis par le prestataire de services de sécurité. Il existe des protocoles et des procédures demandées par les réglementations pour répondre à un appel d'alarme. Différents prestataires de services de sécurité doivent activer leurs propres systèmes de sécurité pour se relier à l'habitation individuelle à protéger. Ceci répond au second objectif du système de sécurité d'une habitation individuelle.

Les effets combinés des systèmes interactifs (c'est-à-dire le système d'alarme d'habitation individuelle et le système de service de sécurité) conduisent à un système complet de sécurité d'habitation individuelle en répondant aux objectifs spécifiés du système.

B.5 Etape 5: Identifier les conditions influentes affectant les fonctions

En utilisant les Tableaux A.1 et A.2 comme lignes directrices, les facteurs d'influence peuvent être identifiés à partir d'une matrice de relations affectant les fonctions. Le processus d'identification consiste à se concentrer sur des facteurs ayant des impacts significatifs sur les fonctions du système, et qui ainsi affectent sa performance.

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

b) Control function includes:

- processing the detected signals from the sensors to activate the alarm. A practical means for processing data is an electronic processor with embedded firmware to drive the processing unit;
- communicating the processed data for display on the control panel for manual intervention. A practical means for communication of processed data and display is by wire-line or wireless connections to facilitate signal processing;
- power conversion providing electrical energy to operate the system functions. In case of main power failure or outage, a rechargeable battery can be used as back-up power supply;
- auto-bypassing can be programmed for control to permit optional home-away arming. When activated by an authorized code, the system allows home occupants to exit within a prescribed exit time (e.g. 90 s) before automatically reactivating the system. The authorized code is needed for re-entry to the home premises within prescribed time without activating the alarm to alert for protection service.

c) Alarm function includes:

- direct connection via telephone lines to alert security services of an alarm situation;
- generating loud sound for a preset duration to alert the occupants. This can be a siren activated by the processor triggered by an alarm situation.

d) Security service function includes:

- activating a command to alert the security service provider for emergencies. This can utilize the home telephone dial-up line connection between the control panel and the communication system of the security service provider.

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

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

B.5 Step 5: Identify the influencing conditions affecting the functions

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

Les facteurs clé influents suivants ont été identifiés pour la sélection ou la conception de chacune des fonctions nécessaires.

Détection
- type et coût des divers capteurs appropriés à fin de détection
- nombre de capteurs nécessaires pour une couverture totale ou partielle afin de réduire les expositions aux risques
- technologie et fiabilité des capteurs
- facilité d'installation des capteurs et de maintenance
- durée de vie attendue des capteurs

Commande
- conception spécifique ou utilisation d'unités de commande disponibles dans le commerce
- facilité d'utilisation et de programmation pour l'armement et le désarmement du système
- réglage du contournement automatique et du délai d'activation
- nombre de zones de détection disponibles pour la surveillance par le panneau de contrôle
- connexions aux capteurs, câblées ou sans fil
- durée de vie de la batterie de secours
- affichage des dysfonctionnements pour permettre un diagnostic du système
- communication pour alerter l'agence de services de sécurité pour obtenir une protection

Alarme
- intensité du signal sonore en activation
- consommation d'énergie du dispositif d'alarme sonore (par exemple, sirène)

Services de sécurité
- programme et coût du contrat de maintenance
- types de services de protection disponibles
- dispositions de surveillance (c'est-à-dire horaires)
- temps de réponse en cas d'alerte
- réglementation gouvernant les dispositions des services de sécurité
- conséquences des fausses alarmes

B.6 Etape 6: Evaluation de l'approche technique pour atteindre les fonctions requises

L'approche technique traite de l'acquisition et du maintien des fonctions requises pour maintenir le fonctionnement dans les contraintes de coût et de délai. La protection offerte par les prestataires de services de sécurité disponibles sur le marché constitue une partie essentielle du processus d'évaluation du système. Les aspects sociaux et économiques tels que l'impact sur la prévention des crimes et les effets sur l'environnement résultants de l'installation et de l'utilisation d'un système de protection d'habitation individuelle ne seront pas traités.

Les problèmes techniques clé incluent l'évaluation des fonctions nécessaires en termes de coût, de technologie et de services de protection.

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

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

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

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

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

B.6 Step 6: Evaluate the technical approach to achieve the needed functions

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

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

Détection La technologie est le principal moteur du coût de la détection. Les types de capteurs incluent les capteurs pour les fumées et les mouvements ainsi que les capteurs magnétiques et électriques d'une fiabilité prouvée qui peuvent répondre à la plupart des besoins de détections. Ces capteurs sont disponibles sous différentes formes et configurations à des coûts raisonnables mais ils requièrent des connexions par câblage direct dans les locaux de l'habitation. Cela affecte le coût non récurrent de l'installation. Des capteurs plus coûteux pour la détection des bris de vitres de fenêtre et des capteurs de surveillance sans fil sont disponibles pour des applications commerciales. Ces capteurs utilisent des technologies plus avancées à un prix qui ne peut être justifié pour une utilisation domestique. La technologie sans fil des capteurs de détection est plus susceptible de provoquer des interférences à l'origine de fausses alarmes. Cependant, les capteurs de nouvelles technologies sont plus adaptés aux grands immeubles, en facilitant l'installation, la modification et les services de maintenance.

Commande La conception de base de l'unité de commande est fiable, bon marché et disponible dans le commerce. L'unité de commande est le coeur du système d'alarme d'habitation, fournissant les caractéristiques fonctionnelles les plus communément nécessaires pour l'utilisation d'un système de surveillance d'habitation. La technologie sans fil incorporée dans la conception des nouveaux systèmes facilite l'installation et les services de maintenance mais au prix fort. La batterie de secours a une durée de vie de 3 ans à 5 ans. Du point de vue de l'utilisateur, il n'y a pas de différence de performance entre le système câblé et le système sans fil.

Alarme Tous les systèmes utilisent des dispositifs d'alarme similaires. Il n'y a pas d'écart de coût ou de différences de technologies.

Services de sécurité Les prestataires de services de sécurité peuvent offrir différents contrats de maintenance pour répondre à la demande des propriétaires d'habitation. Ces contrats sont en premier lieu basés sur la première installation du système, sur le principe de garantie, sur les services de support de maintenance ultérieurs et sur la durée du contrat. Il existe des variations mineures dans le coût et les termes contractuels du fait de la concurrence sur le marché de la surveillance d'habitation. Une analyse du coût du cycle de vie peut être appropriée pour justifier l'investissement dans une acquisition et le coût de possession sur la période de la durée de vie du système de sécurité d'habitation. Le matériel installé pour un système d'alarme d'habitation peut avoir une durée de vie attendue de 15 ans. Il convient qu'un contrôle régulier de maintenance et des essais de sécurité soient suivis.

B.7 Etape 7: Description du matériel, du logiciel et des éléments humains impliqués dans le fonctionnement du système

Matériel Tout le matériel d'un système d'alarme d'habitation peut être intégré et installé dans les locaux de l'habitation. Le système est automatisé. Il exige une attention minimale pour l'exécution de ses fonctions. La maintenance et les contrôles de sécurité sont des procédures simples.

Logiciel L'unité de commande du système contient un logiciel enfoui pour piloter les fonctions de traitement. Les codes de programmation et de modification de codes d'accès sont des instructions directes manuelles du système d'alarme d'habitation qui fournissent une procédure étape par étape pour la programmation.

Humain Le système d'alarme d'habitation est conçu pour assurer un test d'utilisation sous réglementation, pour le fonctionnement du système de sécurité d'habitation. Des accès conviviaux à l'affichage du panneau de commande facilitent les diagnostics et la communication pendant le fonctionnement normal quotidien.

Detection Technology is the main driver on detection cost. The types of sensors include smoke and motion sensors, magnetic and electrical sensors with proven reliability that can meet most detection needs. These sensors are available in various forms and configurations at reasonable cost but they require direct wiring connections at the home premises. This affects a one time installation cost. More expensive sensors for detection of window glass-breakage and wireless monitoring sensors are available for commercial applications. These sensors use more advanced technology at a premium price which cannot be cost justified for home use. Wireless technology for sensor detection is more susceptible to interference causing false alarm. However, new technology sensors are more suitable for large building complexes to facilitate installation, modification and maintenance services.

Control The basic design for the control unit is reliable, inexpensive, and commercially available. The control unit is the heart of the home alarm system providing most operating features commonly needed for home alarm use. Wireless technology incorporated in new system design facilitates installation and maintenance services, but at a premium price. Back-up battery has a life of 3 years to 5 years. From a home user perspective, there is no difference in performance between the wired system and the wireless system.

Alarm All systems are using similar alarm devices. There is no difference in cost or technology variation.

Security service Security service providers can offer various maintenance contracts to suit the home owner's needs. These contracts are based primarily on the initial installation of the system, the warranty schemes and subsequent maintenance support services and contract duration. There are some minor variations in cost and contract terms due to market competition in the home security business. A life cycle cost analysis would be appropriate to justify the investment of acquisition and ownership costs over the life period of the home security system. The hardware installed for the home alarm system should have a life expectancy of 15 years. Regular maintenance check and safety tests should be followed.

B.7 Step 7: Describe the hardware, software, and human elements involved in system operation

Hardware All system hardware for the home alarm system can be integrated and installed in the home premises. The system is automated. It requires minimal attention to its operating functions. Maintenance and safety checks are simple procedures.

Software The system control unit incorporates embedded firmware to drive its processing functions. Programming and changing access codes are straight forward. Instruction manual of the home alarm system provides step-by-step procedure for programming effort.

Human The home alarm system is designed to ensure fitness-for-use under safety regulations for home security system operation. User friendly access to the control panel display facilitates diagnosis and communication during daily normal mode of operation.

Quand une alarme est activée et se traduit par un mode de fonctionnement d'alerte de service de sécurité, un protocole normalisé est suivi par la réponse des agences de sécurité (c'est-à-dire, police, pompiers, urgences médicales, prestataire des services de sécurité) selon les procédures adéquates.

La procédure pour vérifier une fausse alarme est réalisée par un protocole normalisé initié par le prestataire de services de sécurité. Le propriétaire peut annuler la fausse alarme en entrant un mot de passe dans le panneau de commande. Le taux de fausses alarmes est très important dans un système de sécurité d'habitation.

B.8 Etape 8: Détermination du profil opérationnel du système

Différents scénarios peuvent être établis pour fournir un profil opérationnel spécifique pendant le mode d'alerte du service de sécurité. Ce qui suit constitue trois exemples typiques.

- Lorsqu'un système d'alarme d'habitation a détecté une situation anormale dans les locaux de l'habitation, que ce soit un danger réel ou une fausse alarme, seul le prestataire du service de sécurité est alerté pour répondre. Le protocole normal prend immédiatement la liaison téléphonique de l'habitation pour contacter l'occupant et demande l'identification correcte pour évaluer les causes probables de l'alerte. Si ceci échoue, le prestataire du service de sécurité appelle d'autres personnes par avance autorisées par le propriétaire pour évaluer la situation. Si ceci échoue aussi, la police est contactée pour lui rapporter l'incident. La police répond alors à une alarme d'urgence dans les locaux de l'habitation. Ceci est le mode normal de fonctionnement.

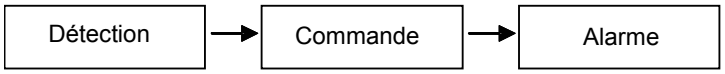
- Lorsque le bouton d'urgence du panneau de commande est activé par un occupant de l'habitation, la police, les pompiers, les urgences médicales et le prestataire du service de sécurité sont tous alertés en même temps. Ils vont répondre à l'alerte d'urgence pour apporter une protection en accord avec leurs procédures respectives. C'est le mode de fonctionnement d'urgence.

- Le mode de sécurité de fonctionnement est une extension du mode normal de fonctionnement par un engagement supplémentaire spécial des services de protection.

B.9 Etape 9: Description des configurations du système pour atteindre les objectifs du système

a) Pour le mode normal de fonctionnement

Pour le mode normal de fonctionnement, le système d'alarme d'habitation requiert la disponibilité de toutes les fonctions de détection, de commande et d'alarme, en permanence pour la performance de sûreté de fonctionnement du système d'alarme d'habitation. Dès la détection d'un danger ou d'une intrusion dans les locaux de l'habitation, la fonction de commande active immédiatement une alarme pour alerter les occupants de l'habitation et le prestataire du service de sécurité. La Figure B.1 donne la configuration du système pour un mode normal de fonctionnement.



-alerte les occupants de l'habitation
-alerte le prestataire du service de sécurité

IEC 2136/06

Figure B.1 – Configuration du système pour le mode normal de fonctionnement

When an alarm is activated resulting in a security service alert mode of operation, a standard protocol is followed by the responding security agencies (i.e. police, fire marshal, medical emergency, security service provider) according to their respective procedures.

Procedure for verifying a false alarm is done by standard protocol initiated by the security service provider. Home owner may cancel the false alarm by entering the assigned pass code to the control panel. The false alarm rate is very important for a home security system.

B.8 Step 8: Determine the operating profile of the system

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

- When the home alarm system has detected an abnormal situation at the home premises, whether it is an actual hazard detected or a false alarm, only the security service provider is alerted to respond. The normal protocol is interrupting immediately the home telephone connection to contact the occupant, and request proper identification to assess probable causes of the alert. Failing that, the security service provider will call other persons pre-authorized by the home owner to assess the situation. If not successful, the police will be contacted to report the incident. The police will respond to an emergency alarm at the home premises. This is the normal mode of operation.

- When the control panel panic button is activated by the home occupant, the police, fire marshal, and the security service provider are all alerted at the same time. They will respond to the emergency alert to provide protection at the home premises according to their respective procedures. This is the panic mode of operation.

- For security mode of operation, this is the extension of the normal mode of operation by engaging additional special protection services.

B.9 Step 9: Describe the system configurations to meet system objectives

a) For normal mode of operation

For normal mode of operation, the home alarm system requires the availability of all the functions for detection, control and alarm operating full time for system dependability performance. Under the home alarm system, upon detection of a hazard or an intrusion at the home premises, the control function immediately activates an alarm to alert the home occupants and the security service provider. Figure B.1 shows the system configuration for normal mode of operation.

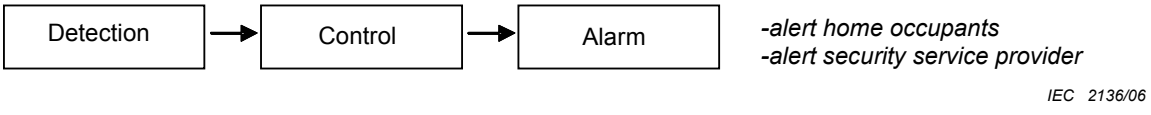


Figure B.1 – System configuration for normal mode of operation

b) Pour le mode de fonctionnement d'alerte du service de sécurité, avec le scénario d'urgence

Lorsque le bouton d'urgence est activé pour une quelconque raison, la police, les pompiers, les urgences médicales et le prestataire du service d'urgence sont alertés directement par le système d'alarme d'habitation. Le système d'alarme d'habitation fonctionne en permanence, mais la fonction de détection est contournée et l'alarme sonore reste silencieuse. Un scénario typique d'urgence est qu'un occupant appuie sur le bouton d'urgence pour indiquer une situation d'urgence. Des exemples incluent un risque d'incendie impossible à maîtriser, un intrus suspect proche des locaux d'habitation, ou une recherche immédiate d'assistance médicale. La Figure B.2 donne la configuration pour le fonctionnement en mode d'urgence.

Figure B.2 – Configuration du système pour le fonctionnement en mode d'urgence

c) Pour le mode de fonctionnement d'alerte du service de sécurité

Lorsque le prestataire du service de sécurité reçoit un signal d'alerte du système d'alarme d'habitation, un protocole spécifique est suivi. Le processus inclut la prise automatique de la ligne téléphonique pour appeler les occupants de l'habitation afin d'évaluer la situation. Si cela échoue, d'autres personnes autorisées par avance sont contactées. Si cela échoue aussi, la police est alertée pour une situation d'urgence dans les locaux de l'habitation. Le système d'alarme est disponible en permanence et il interagit avec les systèmes utilisés par le prestataire du service de sécurité. Ce qui suit constitue les éléments typiques de systèmes utilisés par le prestataire du service de sécurité du système.

- Elément humain impliquant le personnel effectuant les appels téléphoniques nécessaires. La disponibilité sur appel du personnel de sécurité est permanente 24 h par jour, 7 jours par semaine tout au long de l'année.
- Le service fourni par l'opérateur téléphonique aux abonnés. La disponibilité du service téléphonique est sans interruption tout au long de l'année.
- La police et les services d'urgence, habituellement utilisant des véhicules motorisés, mais parfois engageant un hélicoptère pour des services de transport d'urgence médicale. La disponibilité de ces moyens de transport est généralement exprimée en délai d'intervention sur site.

La Figure B.3 donne la configuration du système pour le mode de fonctionnement de service de sécurité.

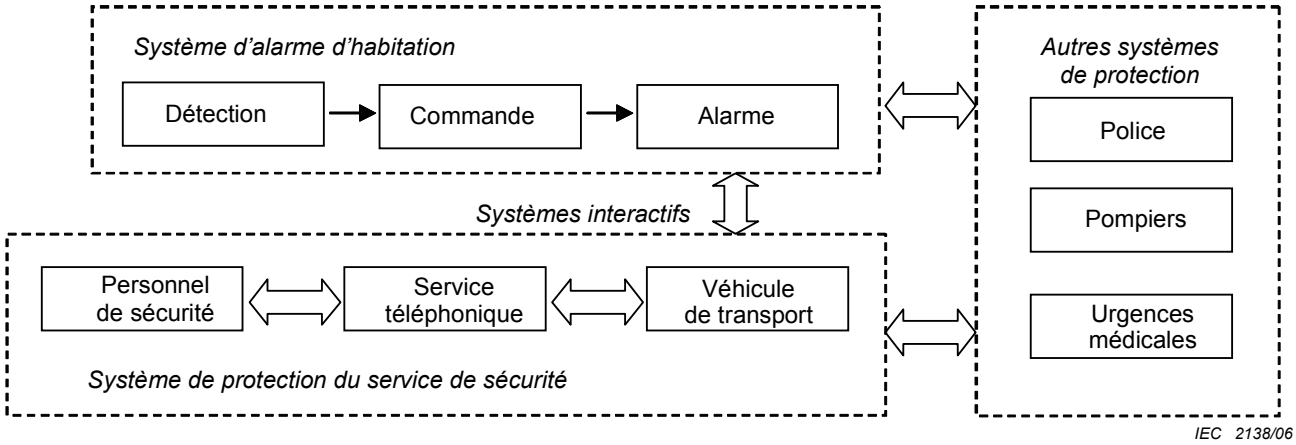


Figure B.3 – Configuration du système pour le mode de fonctionnement en service de sécurité

b) For security service alert mode of operation with panic scenario

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

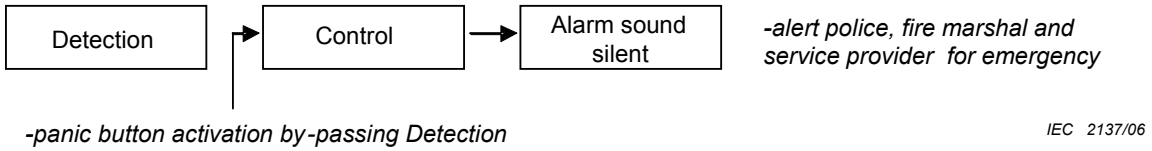


Figure B.2 – System configuration for panic mode of operation

c) For security service alert mode of operation with security service alert scenario

When the security service provider receivs an alert signal from the home alarm system, a specific protocol is followed. The process includes automatically interrupting the phone line and calling the home occupant to assess the situation. Failing that, other pre-authorized persons will be contacted. If not successful, the police will be alerted for an emergency situation at the home premises. The availability of the home alarm system is operating full time and interacting with the system or systems used by the security service provider. The following are typical system elements utilized by the security service provider.

- Human element involving the security attendant making the necessary phone calls. The availability of the security attendant on-call is continuous: 24 h per day and 7 days per week year-round service.
- The services provided by the telephone company to subscribers. The availability of the telephone service to subscribers is continuous throughout the year.
- The police and emergency cruisers, usually employing a motor vehicle, but sometimes engaging a helicopter for transporting emergency services for medical attention. The availability of these transportation means is usually considered in terms of response time to arrive at the scene.

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

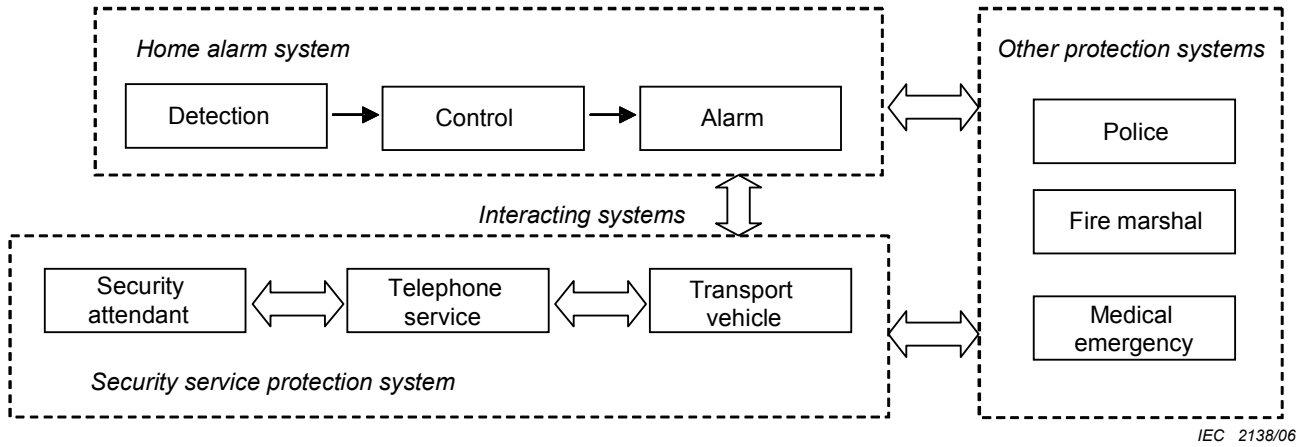


Figure B.3 – System configuration for security service mode of operation

B.10 Etape 10: Détermination des exigences de sûreté de fonctionnement

NOTE Les données présentées dans cet exemple sont uniquement pour illustration. Elles ne sont pas représentatives des données de sûreté de fonctionnement d'un quelconque système, produit ou service.

Les exigences de sûreté de fonctionnement des fonctions du système peuvent être déterminées en établissant le scénario de fonctionnement du système et les exigences pour les fonctions spécifiques peuvent l'être dans le processus d'évaluation. Ce qui suit résume les exigences de sûreté de fonctionnement de chaque fonction du système de sécurité d'habitation. Les valeurs numériques des fonctions représentant le système d'alarme d'habitation sont déterminées par les études de marché et des essais des produits de la concurrence, ainsi que par des évaluations de technologies et des études de capacité des éléments sélectionnés pour le système, tout en restant dans les contraintes économiques et règlementaires. Les valeurs numériques pour les fonctions identifiées dans le système de protection du service de sécurité sont déduites de leurs données respectives d'exploitation. Une série de modèle est utilisée pour déterminer la disponibilité globale du système.

Système d'alarme d'habitation

- Fonction de détection: 99,5 % de disponibilité; contrôle annuel de maintenance; durée de vie prévue: 15 ans.
- Fonction de commande: 99,9 % de disponibilité; contrôle mensuel du système de sécurité; durée de vie prévue: 20 ans.
- Fonction d'alarme: 99,9 % de disponibilité; contrôle annuel de maintenance; durée de vie prévue: 20 ans.

Système de protection du service de sécurité

- Fonction de personnel de sécurité: 99,7 % de disponibilité avec rotation de poste, 24 h sur 24, tout au long de l'année.
- Fonction de service téléphonique: 99,9997 % de disponibilité du service câblé.
- Fonction de véhicule de transport: 99,8 % de disponibilité avec des véhicules de redondance et d'autres moyens de transports avec un temps de réponse inférieur à 10 min.

B.11 Etape 11: Documentation de la spécification de sûreté de fonctionnement du système

Les exigences de sûreté de fonctionnement du système font partie de la spécification globale du système. Ce qui suit résume les données d'entrée pour documenter la spécification de sûreté de fonctionnement du système.

a) Identification du système

Un système de sécurité d'habitation avec un système d'alarme d'habitation installé dans les locaux de l'habitation soutenu par un système de service de sécurité à distance.

b) Objectifs du système

Détection automatique et alarme pour la protection d'habitation par des services de sécurité.

c) Profil opérationnel du système

- Fonctionnement en mode normal
- Fonctionnement en mode d'urgence
- Fonctionnement en mode de sécurité

B.10 Step 10: Determine the dependability requirements

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

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

Home alarm system

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

Security service protection system

- Security attendant function: 99,7 % availability with shift rotation 24 h year-round service alert.
- Telephone service function: 99,9997 % availability for wire-line service.
- Transport vehicle function: 99,8 % availability with redundant vehicles or other transportation means with a response time within 10 min.

B.11 Step 11: Documentation of system dependability specification

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

a) System identification

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

b) System objectives

Automated detection and alarm for home protection by security services.

c) System operating profile

- Normal mode of operation
- Panic mode of operation
- Security mode of operation

d) Exigences de maintenabilté du système et d'accès de maintenance

Le système est maintenu par un test de surveillance automatique intégré des fonctions clé et un contrôle mensuel manuel de sécurité effectué par le propriétaire de l'habitation à partir du panneau de contrôle afin de vérifier le fonctionnement du système de sécurité d'habitation.

e) Configuration du système

Se référer à l'Etape 9 pour la description des configurations du système pour chaque mode de fonctionnement.

f) Fonctions du système

- Fonctions de détection, de commande et d'alarme nécessaires pour le système d'alarme d'habitation.
- Personnel de sécurité, service téléphonique, fonctions de véhicules de transport nécessaire pour la protection de service de sécurité.

g) Exigences de sûreté de fonctionnement pour chaque fonction

(1) Système d'alarme d'habitation

- Fonction de détection: 99,5 % de disponibilité; contrôle annuel de maintenance; durée de vie prévue: 15 ans.
- Fonction de commande: 99,9 % de disponibilité; contrôle mensuel du système de sécurité; durée de vie prévue: 20 ans.
- Durée de vie prévue de la batterie de secours: 5 ans. Le remplacement tous les 3 ans est recommandé.
- Fonction d'alarme: 99,9 % de disponibilité; contrôle annuel de maintenance; durée de vie prévue: 20 ans.

(2) Système de protection de service de sécurité

- Fonction de personnel de sécurité: 99,7 % de disponibilité avec rotation de poste, 24 h sur 24, tout au long de l'année.
- Fonction de service téléphonique: 99,9997 % de disponibilité du service câblé.
- Fonction de véhicule de transport: 99,8 % de disponibilité avec des véhicules de redondance ou d'autres moyens de transports.

h) Une déclaration sur la sûreté de fonctionnement du système

(1) Disponibilité du système d'alarme: 99,3 %.

(2) Disponibilité du système de protection de service de sécurité: 99,5 %.

(3) Disponibilité du système de sécurité d'habitation: 98,8 %.

d) System maintainability and maintenance access requirements

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

e) System configurations

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

f) System functions

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

g) Dependability requirements for each function

(1) Home alarm system

- Detection function: 99,5 % availability; annual maintenance check, expected life 15 years.
- Control function: 99,9 % availability; monthly security system test, expected life 20 years.
- Expected life of back-up battery is 5 years. Recommended replacement every 3 years.
- Alarm function: 99,9 % availability; annual maintenance check, expected life 20 years.

(2) Security service protection system

- Security attendant function: 99,7 % availability with shift rotation 24 h year round service alert.
- Telephone service function: 99,9997 % availability for wire-line service.
- Transport vehicle function: 99,8 % availability with redundant vehicles or other transportation means.

h) A statement on system dependability

(1) Home alarm system availability: 99,3 %.

(2) Security service protection system availability: 99,5 %.

(3) Home security system availability: 98,8 %.

Bibliographie

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

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

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

CEI 60300-3-15[1], *Gestion de la sûreté de fonctionnement – Partie 3-15: Guide d'application – Recommandations pour l'ingénierie de la sûreté de fonctionnement des systèmes*

CEI 61069 (toutes les parties), *Mesure et commande dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation*

CEI 61069-1, *Mesure et commande dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 1: Considérations générales et méthodologie*

ISO 9000:2005, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

[1] A l'étude.

Bibliography

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

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

IEC 60300-3-4, *Dependability management – Part 3: Application guide – Section 4: Specification of dependability requirements*

IEC 60300-3-15[1)], *Dependability management – Part 15: Application guide – Section 15: Guidance to engineering of system dependability*

IEC 61069 (all parts), *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment*

IEC 61069-1, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 1: General considerations and methodology*

ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

———————

1) Under consideration.

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 2-8318-8907-3

ICS 03.120.01

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND