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

© IEC 2006 Droits de reproduction réservés — Copyright - all rights reserved

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

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

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

AVANT-PROPOS 4
INTRODUCTION 8

1 Domaine d'application 10
2 Références normatives 10
3 Termes et définitions 10
4 Concepts traitant de la sûreté de fonctionnement 12
4.1 Comprendre le système 12
4.2 Cycle de vie d'un système 16
4.3 Fonctionnement du système 20
4.4 Profil opérationnel d'un système 20
4.5 Exigences de sûreté de fonctionnement 22
5 Procédure pour spécifier la sûreté de fonctionnement d'un système 26
5.1 Processus de spécification d'un système 26
5.2 Processus de spécification de la sûreté de fonctionnement d'un système 26
5.3 Détermination des valeurs de la sûreté de fonctionnement 28
5.4 Etapes de procédure pour déterminer les exigences de sûreté de fonctionnement d'un système 30

Annexe A (informative) Evaluation des caractéristiques de sûreté de fonctionnement 38
Annexe B (informative) Exemple de développement de spécification de sûreté de fonctionnement d'un système – Système de sécurité d'habitation individuelle 52

Bibliographie 68

Figure 1 – Un exemple de propriétés de système et de caractéristiques liées 14
Figure 2 – Vue d'ensemble des étapes d'un cycle de vie 18
Figure 3 – Relations entre un profil opérationnel d'un système et un scénario de fonctionnement du système 22
Figure 4 – Vue générale du processus de spécification d'un système 28
Figure 5 – Etapes pour déterminer les exigences de sûreté de fonctionnement d'un système 32
Figure B.1 – Configuration du système pour le mode normal de fonctionnement 60
Figure B.2 – Configuration du système pour le fonctionnement en mode d'urgence 62
Figure B.3 – Configuration du système pour le mode de fonctionnement en service de sécurité 62

Tableau A.1 – Exemples de facteurs influents pour chaque condition influente 48
Tableau A.2 – Relations entre les propriétés d'un système et les conditions influentes 50

CONTENTS

FOREWORD 5
INTRODUCTION 9

1 Scope 11
2 Normative references 11
3 Terms and definitions 11
4 Concepts dealing with system dependability 13
4.1 Understanding the system 13
4.2 System life cycle 17
4.3 System operation 21
4.4 System operating profile 21
4.5 Dependability requirements 23
5 Procedure for specifying system dependability 27
5.1 System specification process 27
5.2 System dependability specification process 27
5.3 Determining dependability values 29
5.4 Procedural steps for determining system dependability requirements 31

Annex A (informative) Evaluation of dependability characteristics 39
Annex B (informative) An example on developing a system dependability specification – A home security system 53

Bibliography 69

Figure 1 – An example of system properties and related characteristics 15
Figure 2 – Overview of system life cycle stages 19
Figure 3 – Relationships of system operating profile and scenario in system operation 23
Figure 4 – Overview of system specification process 29
Figure 5 – Steps for determining system dependability requirements 33
Figure B.1 – System configuration for normal mode of operation 61
Figure B.2 – System configuration for panic mode of operation 63
Figure B.3 – System configuration for security service mode of operation 63

Table A.1 – Examples of influencing factors under each influencing condition 49
Table A.2 – Relationship of system properties with influencing conditions 51

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*

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*