NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60300-2

Deuxième édition
Second edition
2004-03

Gestion de la sûreté de fonctionnement –

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

Dependability management –

Part 2:
Guidelines for dependability management

© IEC 2004 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 XA

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 Système de gestion de la sûreté de fonctionnement 18
5 Responsabilité de la direction 20
5.1 Fonction directoriale en matière de sûreté de fonctionnement 20
5.2 Satisfaction des besoins du client en matière de sûreté de fonctionnement 22
5.3 Politique de sûreté de fonctionnement et implications réglementaires 22
5.4 Programmes de sûreté de fonctionnement 24
5.5 Représentant de la direction 24
5.6 Revue de direction 24
6 Management des ressources 24
6.1 Mise à disposition des ressources 24
6.2 Planification, développement et maintien des ressources 26
6.3 Sous-traitance 28
7 Réalisation du produit 28
7.1 Planification de la réalisation du produit 28
7.2 Adaptation des programmes de sûreté de fonctionnement 30
7.3 Application du plan de sûreté de fonctionnement 30
7.4 Gestion de la chaîne d'approvisionnement 32
8 Mesures, analyses et amélioration 32
8.1 Mesure de la sûreté de fonctionnement 32
8.2 Surveillance et assurance de la sûreté de fonctionnement 34
8.3 Estimation et analyse de la sûreté de fonctionnement 34
8.4 Utilisation des informations de sûreté de fonctionnement 34
8.5 Mesure des résultats 36
8.6 Amélioration de la sûreté de fonctionnement 38
Annexe A (informative) Eléments du programme de sûreté de fonctionnement et tâches des applications des systèmes, du matériel et du logiciel 42
Annexe B (informative) Phases du cycle de vie du produit 70
Annexe C (informative) Association des phases du cycle de vie du produit avec les éléments et les tâches applicables de la sûreté de fonctionnement 74
Annexe D (informative) Etapes de processus et normes relatives à la gestion de la sûreté de fonctionnement 78
Annexe E (informative) Questions pour la revue de gestion de la sûreté de fonctionnement 84
Annexe F (informative) Lignes directrices sur le processus d'ajustement 88
Annexe G (informative) Classification des normes relatives à la sûreté de fonctionnement selon les phases du cycle de vie pour lesquelles elles sont applicables 92
Bibliographie 100

Figure 1 – Etapes du processus de gestion de la sûreté de fonctionnement 18

CONTENTS

FOREWORD 5
INTRODUCTION 9
1 Scope 11
2 Normative references 11
3 Terms and definitions 11
4 Dependability management system 19
5 Management responsibility 21
5.1 Management function on dependability 21
5.2 Meeting customer dependability needs 23
5.3 Dependability policy and regulatory implications 23
5.4 Dependability programmes 25
5.5 Management representative 25
5.6 Management review 25
6 Resource management 25
6.1 Provision of resources 25
6.2 Resource planning, development and maintenance 27
6.3 Outsourcing 29
7 Product realization 29
7.1 Planning for product realization 29
7.2 Tailoring of dependability programmes 31
7.3 Application of dependability plan 31
7.4 Supply-chain management 33
8 Measurement, analysis and improvement 33
8.1 Dependability measurement 33
8.2 Dependability monitoring and assurance 35
8.3 Dependability assessment and analysis 35
8.4 Use of dependability information 35
8.5 Measurement of results 37
8.6 Dependability improvement 39

Annex A (informative) Dependability programme elements and tasks for systems, hardware and software applications 43
Annex B (informative) Product life cycle phases 71
Annex C (informative) Association of product life cycle phases with the applicable dependability elements and tasks 75
Annex D (informative) Process steps and standards for managing dependability 79
Annex E (informative) Questions for dependability management review 85
Annex F (informative) Guidelines for the tailoring process 89
Annex G (informative) Classification of dependability standards with the life cycle phases in which they are applicable 93
Bibliography 101

Figure 1 – Process steps for managing dependability 19

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

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

AVANT-PROPOS

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

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

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

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

Part 2: Guidelines for dependability management

FOREWORD

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

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

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

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

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

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/913/FDIS	56/934/RVD

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

La présente publication a été rédigée conformément aux Directives de l'ISO/CEI, Partie 2.

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

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

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

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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

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

Annex B defines the product life cycle phases.

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

Annex D presents process steps and standards for managing dependability.

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

Annex F provides guidelines for the tailoring process.

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

GESTION DE LA SÛRETE DE FONCTIONNEMENT –

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

1 Domaine d'application

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

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

2 Références normatives

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

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

CEI 61014, *Programmes de croissance de fiabilité*

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

DEPENDABILITY MANAGEMENT –

Part 2: Guidelines for dependability management

1 Scope

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

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

2 Normative references

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

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

IEC 61014, *Programmes for reliability growth*

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