IEC 60300-3-15

Edition 1.0 2009-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Dependability management – Part 3-15: Application guide – Engineering of system dependability

Gestion de la sûreté de fonctionnement – Partie 3-15: Guide d'application – Ingénierie de la sûreté de fonctionnement des systèmes

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XA
CODE PRIX

ICS 03.120.01

ISBN 978-2-88910-099-6

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 7
2 Normative references 7
3 Terms and definitions 7
4 System dependability engineering and applications 8
4.1 Overview of system dependability engineering 8
4.2 System dependability attributes and performance characteristics 9
5 Managing system dependability 10
5.1 Dependability management 10
5.2 System dependability projects 10
5.3 Tailoring to meet project needs 11
5.4 Dependability assurance 11
6 Realization of system dependability 11
6.1 Process for engineering dependability into systems 11
6.1.1 Purpose of dependability process 11
6.1.2 System life cycle and processes 11
6.1.3 Process applications through the system life cycle 12
6.2 Achievement of system dependability 14
6.2.1 Purpose of system dependability achievements 14
6.2.2 Criteria for system dependability achievements 14
6.2.3 Methodology for system dependability achievements 15
6.2.4 Realization of system functions 16
6.2.5 Approaches to determine achievement of system dependability 17
6.2.6 Objective evidence of achievements 18
6.3 Assessment of system dependability 18
6.3.1 Purpose of system dependability assessments 18
6.3.2 Types of assessments 18
6.3.3 Methodology for system dependability assessments 20
6.3.4 Assessment value and implications 21
6.4 Measurement of system dependability 21
6.4.1 Purpose of system dependability measurements 21
6.4.2 Classification of system dependability measurements 22
6.4.3 Sources of measurements 23
6.4.4 Enabling systems for dependability measurements 23
6.4.5 Interpretation of dependability measurements 24
Annex A (informative) System life cycle processes and applications 25
Annex B (informative) Methods and tools for system dependability development and assurance 35
Annex C (informative) Guidance on system application environment 42
Annex D (informative) Checklists for System Dependability Engineering 47
Bibliography 54

Figure 1 – An overview of a system life cycle 12
Figure 2 – An example of a process model 13

Figure A.1 – An overview of system life cycle processes 25
Figure C.1 – Environmental requirements definition process 43
Figure C.2 – Mapping system application environments to exposures 44

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

Part 3-15: Application guide – Engineering of system dependability

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 should 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 should 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 should not be held responsible for identifying any or all such patent rights.

International Standard IEC 60300-3-15 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/1315/FDIS	56/1321/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.

A list of all parts of the IEC 60300 series, under the general title *Dependability management*, can be found on the IEC website.

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

Systems are growing in complexity in today's application environments. System dependability has become an important performance attribute that affects the business strategies in system acquisition and the cost-effectiveness in system ownership and operations. The overall dependability of a system is the combined result of complex interactions of system elements, application environments, human-machine interfaces, deployment of support services and other influencing factors.

This part of IEC 60300 gives guidance on the engineering of the overall system to achieve its dependability objectives. The engineering approach in this standard represents the application of appropriate scientific knowledge and relevant technical disciplines for realizing the required dependability for the system of interest.

The four main aspects for engineering dependability concerning systems are addressed in terms of

– process,
– achievement,
– assessment, and
– measurement.

The engineering disciplines consist of technical processes that are applicable to the various stages of the system life cycle. Specific technical processes described in this part of IEC 60300 are supported by a sequence of relevant process activities to achieve the objectives of each system life cycle stage.

This part of IEC 60300 is applicable to generic systems with interacting system functions consisting of hardware, software and human elements to achieve system performance objectives. In many cases a function can be realized by commercial off-the-shelf products. A system can link to other systems to form a network. The boundaries separating a product from a system, and a system from a network, can be distinguished by defining the application of the entity. For example, a digital timer as a product can be used to synchronize the operation of a computer; the computer as a system can be linked with other computers in a business office for communications as a local area network. The application environment is applicable to all kinds of systems. Examples of applicable systems include control systems for power generation, fault-tolerant computing systems and systems for provision of maintenance support services.

Guidance on dependability engineering is provided for generic systems. It does not classify systems for special applications. The majority of systems in use are generally repairable throughout their life cycle operation for economic reasons and practical applications. Non-repairable systems such as communication satellites, remote sensing/monitoring equipment, and one-shot devices are considered as application-specific systems. They require further identification of specific application environment, operational conditions and additional information on unique performance characteristics to achieve their mission success objectives. Non-repairable subsystems and components are considered as throwaway items. The selection of applicable processes for engineering dependability into a specific system is carried out through the project tailoring and dependability management process.

This part of IEC 60300 forms part of the framework standards on system aspects of dependability to support IEC 60300-1 and IEC 60300-2 on dependability management. References are made to project management activities applicable to systems. They include identification of dependability elements and tasks relevant to the system and guidelines for dependability management reviews and tailoring of dependability projects.

DEPENDABILITY MANAGEMENT –

Part 3-15: Application guide – Engineering of system dependability

1 Scope

This part of IEC 60300 provides guidance for an engineering system's dependability and describes a process for realization of system dependability through the system life cycle.

This standard is applicable to new system development and for enhancement of existing systems involving interactions of system functions consisting of hardware, software and human elements.

This standard also applies to providers of subsystems and suppliers of products that seek system information and criteria for system integration. Methods and tools are provided for system dependability assessment and verification of results for achievement of dependability objectives.

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

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

SOMMAIRE

AVANT-PROPOS 58
INTRODUCTION 60
1 Domaine d'application 62
2 Références normatives 62
3 Termes et définitions 62
4 Ingénierie de la sûreté de fonctionnement des systèmes et applications 63
4.1 Vue d'ensemble de l'ingénierie de la sûreté de fonctionnement des systèmes 63
4.2 Attributs et caractéristiques d'aptitude à la fonction de sûreté de fonctionnement des systèmes 64
5 Gestion de la sûreté de fonctionnement des systèmes 65
5.1 Gestion de la sûreté de fonctionnement 65
5.2 Projets de sûreté de fonctionnement des systèmes 66
5.3 Adaptation afin de satisfaire aux besoins d'un projet 66
5.4 Assurance de la de sûreté de fonctionnement 67
6 Réalisation de la sûreté de fonctionnement des systèmes 67
6.1 Processus d'ingénierie de la sûreté de fonctionnement des systèmes 67
6.1.1 Objet du processus de sûreté de fonctionnement 67
6.1.2 Cycle de vie des systèmes et processus 67
6.1.3 Applications de processus au cours du cycle de vie d'un système 69
6.2 Réalisation de la sûreté de fonctionnement d'un système 70
6.2.1 Objet de la réalisation de la sûreté de fonctionnement d'un système 70
6.2.2 Critères de réalisation de la sûreté de fonctionnement d'un système 70
6.2.3 Méthodologie pour la réalisation de la sûreté de fonctionnement des systèmes 72
6.2.4 Réalisation des fonctions d'un système 73
6.2.5 Approches pour déterminer la réalisation de la sûreté de fonctionnement d'un système 74
6.2.6 Preuves tangibles des réalisations 75
6.3 Evaluation de la sûreté de fonctionnement d'un système 75
6.3.1 Objet des évaluations de la sûreté de fonctionnement d'un système 75
6.3.2 Types d'évaluation 76
6.3.3 Méthodologie pour l'évaluation de la sûreté de fonctionnement du système 78
6.3.4 Valeur de l'évaluation et implications 79
6.4 Mesure de la sûreté de fonctionnement d'un système 79
6.4.1 Objet des mesures de la sûreté de fonctionnement d'un système 79
6.4.2 Classification des mesures de la sûreté de fonctionnement d'un système 80
6.4.3 Sources de mesures 81
6.4.4 Systèmes d'activation pour les mesures de la sûreté de fonctionnement 81
6.4.5 Interprétation des mesures de la sûreté de fonctionnement 82
Annexe A (informative) Processus du cycle de vie des systèmes et applications 84
Annexe B (informative) Méthodes et outils pour le développement et l'assurance de la sûreté de fonctionnement d'un système 95
Annexe C (informative) Guide sur l'environnement d'application d'un système 103

Annexe D (informative) Listes de contrôle applicables à l'ingénierie de la sûreté de fonctionnement d'un système 109
Bibliographie 118

Figure 1 – Présentation du cycle de vie d'un système 68
Figure 2 – Exemple de modèle de processus 69
Figure A.1 – Présentation générale des processus du cycle de vie d'un système 84
Figure C.1 – Processus de définition des exigences environnementales 104
Figure C.2 – Cartographie des environnements d'application d'un système aux expositions 105

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

_____

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 3-15: Guide d'application – Ingénierie de la 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 tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 60300-3-15 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1315/FDIS	56/1321/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.

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

Une liste de toutes les parties de la série CEI 60300, sous le titre général *Gestion de la sûreté de fonctionnement*, est disponible sur le site web de la CEI.

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.

INTRODUCTION

Les systèmes utilisés dans les environnements d'application actuels sont de plus en plus complexes. La sûreté de fonctionnement constitue désormais un attribut d'aptitude à la fonction important affectant les stratégies d'entreprise en termes d'acquisition de systèmes et de rentabilité en termes de propriété et d'exploitation de ces derniers. La sûreté de fonctionnement globale d'un système résulte de l'association d'interactions complexes entre éléments de systèmes, environnements d'application, interfaces homme-machines, de la mise en œuvre de services d'assistance et d'autres facteurs influents.

Cette partie de la CEI 60300 donne des lignes directrices pour l'ingénierie d'un système global, pour l'atteinte des objectifs en matière de sûreté de fonctionnement. L'approche technique décrite dans la présente norme est la mise en application de connaissances scientifiques appropriées et de disciplines techniques pertinentes permettant de réaliser la sûreté de fonctionnement requise pour le système étudié.

Les quatre principaux aspects de la sûreté de fonctionnement d'ingénierie des systèmes sont traités en termes

– de processus,
– de réalisation,
– d'évaluation et
– de mesure.

Les disciplines techniques consistent en des processus techniques applicables aux différentes étapes du cycle de vie d'un système. Une séquence d'activités de processus pertinentes vient à l'appui des processus techniques spécifiques décrits dans la présente partie de la CEI 60300, afin d'atteindre les objectifs de chaque étape du cycle de vie d'un système.

La présente partie de la CEI 60300 s'applique aux systèmes génériques ayant des fonctions système interactives et consistant en des éléments matériels, logiciels et humains permettant d'atteindre les objectifs d'aptitude à la fonction desdits systèmes. Dans de nombreux cas, une fonction peut être réalisée par des produits du commerce. Un système peut être associé à d'autres systèmes pour former un réseau. Les limites qui séparent un produit d'un système et un système d'un réseau, peuvent être différenciées par la définition de l'application de l'entité. Par exemple, une horloge numérique peut être utilisée en tant que produit pour la synchronisation du fonctionnement d'un ordinateur; un ordinateur peut, en tant que système, être associé à d'autres ordinateurs dans un bureau à des fins de communications sous forme de réseau local d'entreprise. La prise en considération de l'environnement d'application vaut pour tous les types de systèmes. Les systèmes de commande pour la production d'énergie, les ordinateurs tolérants aux pannes et les systèmes de prestation de services de logistique de maintenance sont des exemples de systèmes.

Des lignes directrices portant sur l'ingénierie de la sûreté de fonctionnement sont données pour les systèmes génériques. Elles ne classent pas les systèmes en fonction d'applications spéciales. La majorité des systèmes utilisés peuvent généralement être réparés tout au long de leur cycle de vie selon des considérations économiques et d'applications pratiques. Les systèmes non réparables tels que les satellites de communication, les matériels de télédétection/télésurveillance et les dispositifs à mission unique sont considérés comme des systèmes spécifiques à une application. Pour atteindre leurs objectifs, ils requièrent une identification propre de l'environnement d'application spécifique, des conditions d'exploitation et d'informations supplémentaires relatives à des caractéristiques uniques d'aptitude à la fonction. Les sous-systèmes et composants non réparables sont considérés comme des articles jetables. La sélection de processus applicables à ingénierie de la sûreté de fonctionnement dans un système spécifique est menée au moyen d'une adaptation du projet et du processus de la gestion de la sûreté de fonctionnement.

La présente partie de la CEI 60300 fait partie intégrante du jeu de normes traitant des aspects système de la sûreté de fonctionnement et venant à l'appui de la CEI 60300-1 et de la CEI 60300-2 en matière de gestion de la sûreté de fonctionnement. Il y est fait référence aux activités de gestion de projet applicables aux systèmes. Elle traite de l'identification des éléments de la sûreté de fonctionnement et des tâches appropriées au système, ainsi que des lignes directrices pour les revues de gestion de la sûreté de fonctionnement et l'adaptation des projets de sûreté de fonctionnement.

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 3-15: Guide d'application – Ingénierie de la sûreté de fonctionnement des systèmes

1 Domaine d'application

La présente partie de la CEI 60300 donnent des lignes directrices pour l'ingénierie de la sûreté de fonctionnement des systèmes et elle décrit un processus de réalisation de la sûreté de fonctionnement tout au long du cycle de vie des systèmes.

Cette norme s'applique au développement de nouveaux systèmes et à l'amélioration de systèmes existants impliquant des interactions de fonctions système et consistant en des éléments matériels, logiciels et humains.

Cette norme s'applique également aux fournisseurs de sous-systèmes et de produits qui recherchent des informations relatives aux systèmes et des critères relatifs à l'intégration des systèmes. Des méthodes et des outils sont donnés pour évaluer la sûreté de fonctionnement des systèmes et la vérifier des résultats afin d'atteindre les objectifs de sûreté de fonctionnement.

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 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*