IEC 60300-1

Edition 3.0 2014-05

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

## Dependability management – Part 1: Guidance for management and application

## Gestion de la sûreté de fonctionnement – Partie 1: Lignes directrices pour la gestion et l'application

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

X

ICS 03.100.40, 03.120.01, 21.020

ISBN 978-2-8322-1777-1

# CONTENTS

FOREWORD....4
INTRODUCTION....6
1 Scope....7
2 Normative references....7
3 Terms, definitions and abbreviations....7
3.1 Terms and definitions....7
3.2 Abbreviations....10
4 Dependability management....10
4.1 Understanding dependability....10
4.2 Benefits of dependability management....12
4.3 Challenges of managing dependability....12
5 System for managing dependability....12
5.1 Overview....12
5.2 Organizational arrangements....13
5.3 Management actions....14
5.4 Performance evaluation....14
6 Application of dependability management....15
6.1 Tailoring a dependability programme....15
6.2 Analysis of objectives and requirements....16
6.3 Risk management....17
6.4 Implementation of dependability activities through the life cycle....17
6.5 Selection of dependability tools and technical activities....17
6.6 Resources....18
6.7 Measurement and assessment....18
6.8 Assurance of dependability....19
6.9 Reviewing dependability outcomes and activities....20
Annex A (informative) Organizational arrangements of a dependability management system....22
A.1 Organizational structures....22
A.2 Organization of dependability activities....22
Annex B (informative) Activities of a dependability management system....24
B.1 Dependability activities within the life cycle....24
B.2 Dependability life cycle activities....27
Annex C (informative) Defining requirements of an item....32
C.1 Requirements from an application perspective....32
C.2 Examples of performance requirements that include dependability....33
C.2.1 Requirements determined by both provider and user....33
C.2.2 Requirements determined by provider only....34
Annex D (informative) Structure of dependability standards....37
D.1 Structure....37
D.2 Core standards....37
D.3 Process standards....37
D.4 Support standards....38
D.5 Associated standards....38

Annex E (informative) Checklist for review of dependability ..... 39
E.1 Introductory remark ..... 39
E.2 Concept ..... 39
E.2.1 Requirements definition ..... 39
E.2.2 Requirements analysis ..... 39
E.2.3 High-level architectural design ..... 39
E.3 Development ..... 40
E.3.1 Item design ..... 40
E.3.2 Full-scale system development ..... 40
E.4 Realization ..... 41
E.4.1 Item realization ..... 41
E.4.2 Item implementation ..... 41
E.5 Utilization ..... 41
E.6 Enhancement ..... 41
E.7 Retirement ..... 42
Bibliography ..... 43

Figure 1 – Relationship of dependability to the needs and requirements of an item (product, system, process or service) ..... 11
Figure 2 – Dependability management systems ..... 13
Figure B.1 – Dependability activities and the life cycle ..... 26
Figure C.1 – Example showing the relationship between the functional, non-functional and dependability requirements for a motor-driven pipeline pump ..... 34
Figure C.2 – Example showing the relationship between the functional, non-functional and dependability requirements for a family car ..... 36
Figure D.1 – Framework for dependability standards ..... 37

Table B.1 – Activities during the concept stage ..... 27
Table B.2 – Activities during development stage ..... 29
Table B.3 – Activities during the realization stage ..... 30
Table B.4 – Activities during the utilization stage ..... 31
Table B.5 – Activities during the enhancement stage ..... 31
Table B.6 – Activities during the retirement stage ..... 31

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

# DEPENDABILITY MANAGEMENT –

## Part 1: Guidance for management and application

## 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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
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 60300-1 has been prepared by IEC technical committee 56: Dependability.

This bilingual version (2014-08) corresponds to the English version, published in 2014-05.

This third edition cancels and replaces the second edition published in 2003 and constitutes a technical revision.

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

a) an updating of definitions to reflect IEC 60050-191:2014;

b) an enhanced description of dependability and its attributes;

c) a more generic approach to dependability management;

d) revised guidelines for application of dependability management;

e) a more generic approach to the life cycle;

f) a framework for dependability standards.

In addition, this third edition cancels and replaces the second edition of document IEC 60300-2 published in 2004.

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

| FDIS | Report on voting |
|---|---|
| 56/1550/FDIS | 56/1556/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.

The French version of this standard has not been voted upon.

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

A list of all parts in the IEC 60300 series, published 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 stability 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

This part of IEC 60300 describes the processes involved in managing dependability within an organization and establishes a framework for managing dependability activities for the purpose of achieving dependability performance.

Dependability is the ability of an item to perform as and when required. Dependability is a term used to describe the time-dependent characteristics associated with the performance of an item. Dependability includes characteristics such as availability, reliability, maintainability and supportability under given conditions of use and maintenance support requirements. Dependability describes the extent to which something can be trusted to behave as expected.

Dependability creates trust and confidence and affects the ability of an organization to meet its objectives. It is achieved by effective planning and implementation of dependability activities throughout the life cycle of items.

Dependability has a strong impact on the user's perception of the value of an item developed or provided by an organization. Poor dependability will affect an organization's capability to deliver its objectives and reduce its reputation.

Dependability management provides a systematic approach for addressing dependability and related issues from an organizational and business perspective. Dependability is often driven by technology and requires the integration of innovation with legacy products. Achieving dependability throughout the life cycle process can be influenced by market dynamics, global economics and resource distributions, changing customer needs, and a competitive environment. Strategies need to adapt to anticipated changes to sustain viability in business operations. Dependability management focuses on the needs of stakeholders in optimizing dependability to enhance organizational objectives and return-on-investments.

This standard is written specifically for application to technological products, systems, processes and services, which are referred to in this standard by the general term "item". However, much of the guidance provided is generic and can be adapted for application in various non-technological applications. In addition, the potential side effects on safety, environment and other factors should be identified, analysed and managed when optimizing dependability.

The intended audience for this standard ranges from users, owners and customers to organizations involved in and responsible for ensuring dependability requirements are being met. Organizations include all types and sizes of corporations, public and private institutions such as in government agencies, business enterprises, and non-profit associations.

# DEPENDABILITY MANAGEMENT –

# Part 1: Guidance for management and application

## 1 Scope

This part of IEC 60300 establishes a framework for dependability management. It provides guidance on dependability management of products, systems, processes or services involving hardware, software and human aspects or any integrated combinations of these elements. It presents guidance on planning and implementation of dependability activities and technical processes throughout the life cycle taking into account other requirements such as those relating to safety and the environment.

This standard gives guidelines for management and their technical personnel to assist them to optimize dependability.

This standard is not intended for the purpose of certification.

## 2 Normative references

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

None.

# SOMMAIRE

AVANT-PROPOS ..... 46
INTRODUCTION ..... 48
1 Domaine d'application ..... 49
2 Références normatives ..... 49
3 Termes, définitions et abréviations ..... 49
3.1 Termes et définitions ..... 49
3.2 Abréviations ..... 52
4 Gestion de la sûreté de fonctionnement ..... 52
4.1 Comprendre la sûreté de fonctionnement ..... 52
4.2 Avantages de la gestion de la sûreté de fonctionnement ..... 54
4.3 Enjeux relatifs à la gestion de la sûreté de fonctionnement ..... 54
5 Système de gestion de la sûreté de fonctionnement ..... 55
5.1 Présentation générale ..... 55
5.2 Dispositions organisationnelles ..... 56
5.3 Actions de gestion ..... 57
5.4 Évaluation des performances ..... 58
6 Application de la gestion de la sûreté de fonctionnement ..... 58
6.1 Adaptation d'un programme de sûreté de fonctionnement ..... 58
6.2 Analyse des objectifs et des exigences ..... 60
6.3 Gestion des risques ..... 60
6.4 Mise en œuvre des activités de sûreté de fonctionnement tout au long du cycle de vie ..... 61
6.5 Sélection des outils et des activités techniques de sûreté de fonctionnement ..... 61
6.6 Ressources ..... 62
6.7 Mesure et évaluation ..... 62
6.8 Assurance de la sûreté de fonctionnement ..... 63
6.9 Revue des résultats et des activités de sûreté de fonctionnement ..... 64
Annexe A (informative) Dispositions organisationnelles d'un système de gestion de la sûreté de fonctionnement ..... 67
A.1 Structures organisationnelles ..... 67
A.2 Organisation des activités de sûreté de fonctionnement ..... 67
Annexe B (informative) Activités d'un système de gestion de la sûreté de fonctionnement ..... 69
B.1 Activités de sûreté de fonctionnement dans le cycle de vie ..... 69
B.2 Activités de sûreté de fonctionnement au cours du cycle de vie ..... 74
Annexe C (informative) Définition des exigences pour une entité ..... 80
C.1 Exigences du point de vue de l'application ..... 80
C.2 Exemples d'exigences de performance comprenant la sûreté de fonctionnement ..... 81
C.2.1 Exigences déterminées par le fournisseur et l'utilisateur ..... 81
C.2.2 Exigences déterminées uniquement par le fournisseur ..... 83
Annexe D (informative) Structure des normes de sûreté de fonctionnement ..... 87
D.1 Structure ..... 87
D.2 Normes principales ..... 88
D.3 Normes de processus ..... 88

D.4 Normes de soutien ..... 88
D.5 Normes connexes ..... 88
Annexe E (informative) Liste de contrôle pour la revue de sûreté de fonctionnement ..... 89
E.1 Remarque préliminaire ..... 89
E.2 Concept ..... 89
E.2.1 Définition des exigences ..... 89
E.2.2 Analyse des exigences ..... 89
E.2.3 Conception architecturale de haut niveau ..... 89
E.3 Développement ..... 90
E.3.1 Conception de l'entité ..... 90
E.3.2 Développement grandeur nature du système ..... 90
E.4 Réalisation ..... 91
E.4.1 Réalisation de l'entité ..... 91
E.4.2 Mise en œuvre de l'entité ..... 91
E.5 Utilisation ..... 91
E.6 Amélioration ..... 92
E.7 Mise au rebut ..... 92
Bibliographie ..... 93

Figure 1 – Relation entre la sûreté de fonctionnement et les besoins et les exigences d'une entité (produit, système, processus ou service) ..... 53
Figure 2 – Systèmes de gestion de la sûreté de fonctionnement ..... 56
Figure B.1 – Activités de sûreté de fonctionnement et cycle de vie ..... 74
Figure C.1 – Exemple illustrant la relation entre les exigences fonctionnelles, non fonctionnelles et de sûreté de fonctionnement pour une pompe à moteur d'oléoduc ..... 83
Figure C.2 – Exemple illustrant la relation entre les exigences fonctionnelles, non fonctionnelles et de sûreté de fonctionnement pour une voiture familiale ..... 86
Figure D.1 – Cadre pour les normes de sûreté de fonctionnement ..... 87

Tableau B.1 – Activités au cours de la phase de conception ..... 74
Tableau B.2 – Activités au cours de la phase de développement ..... 77
Tableau B.3 – Activités au cours de la phase de réalisation ..... 78
Tableau B.4 – Activités au cours de la phase d'utilisation ..... 79
Tableau B.5 – Activités au cours de la phase d'amélioration ..... 79
Tableau B.6 – Activités au cours de la phase de mise au rebut ..... 79

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

# GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

## Partie 1: Lignes directrices pour la gestion et l'application

## AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC 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, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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 l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 60300-1 a été établie par le comité d'études 56 de l'IEC: Sûreté de fonctionnement.

Cette troisième édition annule et remplace la deuxième édition parue en 2003. Cette édition constitue une révision technique.

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

a) des définitions actualisées selon la toute dernière version du IEC 60050-191:2014;
b) une meilleure description de la sûreté de fonctionnement et de ses attributs;
c) une approche plus générique de la gestion de la sûreté de fonctionnement;

d) des lignes directrices révisées pour l'application de la gestion de la sûreté de fonctionnement;

e) une approche plus générique du cycle de vie;

f) un cadre pour les normes de sûreté de fonctionnement.

En plus, cette troisième édition annule et remplace la deuxième édition du document IEC 60300-2 qui a été publié en 2004.

La présente version bilingue (2014-08) correspond à la version anglaise monolingue publiée en 2014-05.

Le text anglais de cette norme est issu des documents 56/1550/FDIS et 56/1556/RVD.

Le rapport de vote 56/1556/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

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

Une liste de toutes les parties de la série IEC 60300, publiées sous le titre général *Gestion de la sûreté de fonctionnement*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC 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

La présente partie de l'IEC 60300 décrit les processus impliqués dans la gestion de la sûreté de fonctionnement au sein d'un organisme et établit un cadre pour la gestion des activités de sûreté de fonctionnement, dans le but d'obtenir les performances de sûreté de fonctionnement.

La sûreté de fonctionnement est la capacité d'une entité à fonctionner correctement et au moment voulu. La sûreté de fonctionnement est un terme utilisé pour décrire les caractéristiques liées au temps et associées aux performances d'une entité. La sûreté de fonctionnement inclut des caractéristiques telles que la disponibilité, la fiabilité, la maintenabilité et la supportabilité pour des conditions d'utilisation et des exigences de logistique de maintenance données. La sûreté de fonctionnement décrit dans quelle mesure il est possible d'avoir confiance en la capacité d'une entité à se comporter comme prévu.

La sûreté de fonctionnement génère de la confiance et influence la capacité d'un organisme à atteindre ses objectifs. La sûreté de fonctionnement est obtenue en planifiant et en mettant en œuvre les activités de sûreté de fonctionnement tout au long du cycle de vie des entités.

La sûreté de fonctionnement a un impact important sur la perception de l'utilisateur sur la valeur d'une entité conçue ou fournie par un organisme. Une faible sûreté de fonctionnement affectera la capacité d'un organisme à atteindre ses objectifs ainsi que sa réputation.

La gestion de la sûreté de fonctionnement apporte une approche systématique permettant de traiter la sûreté de fonctionnement et les enjeux associés d'un point de vue organisationnel et commercial. La sûreté de fonctionnement est souvent orientée par la technologie et requiert l'intégration de l'innovation dans les produits existants. L'obtention de la sûreté de fonctionnement tout au long du processus de cycle de vie peut être influencée par les dynamiques des marchés, l'économie mondiale et les distributions des ressources, les modifications des besoins des consommateurs et un environnement compétitif. Les stratégies doivent s'adapter aux modifications prévues pour maintenir la viabilité des opérations commerciales. La gestion de la sûreté de fonctionnement se concentre sur les besoins des parties prenantes en optimisant la sûreté de fonctionnement afin d'améliorer les objectifs organisationnels et les retours sur investissement.

La présente norme est spécifiquement destinée à s'appliquer aux produits, aux systèmes, aux processus et aux services technologiques, qui sont désignés par le terme général "entité" dans la présente norme. Cependant, la plupart des lignes directrices fournies sont génériques et peuvent être adaptées pour être appliquées dans différentes applications non technologiques. De plus, lors de l'optimisation de la sûreté de fonctionnement, il convient d'identifier, d'analyser et de gérer les effets secondaires potentiels sur la sécurité, l'environnement et les autres facteurs.

La présente norme s'adresse aux utilisateurs, aux propriétaires, aux clients et aux organismes impliqués et chargés de garantir la conformité aux exigences de sûreté de fonctionnement. Les organismes comprennent tous types et tailles d'entreprises, d'institutions publiques ou privées tels que les administrations publiques, les entreprises commerciales et les associations à but non lucratif.

# GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

# Partie 1: Lignes directrices pour la gestion et l'application

## 1 Domaine d'application

La présente partie de l'IEC 60300 établit un cadre pour la gestion de la sûreté de fonctionnement. Elle donne des lignes directrices sur la gestion de la sûreté de fonctionnement des produits, des systèmes, des processus ou des services impliquant des aspects matériels, logiciels et humains ou toute combinaison intégrant ces éléments. Elle présente des lignes directrices sur la planification et la mise en œuvre des activités de sûreté de fonctionnement et des processus techniques tout au long du cycle de vie, en prenant en compte les autres exigences telles que celles relatives à la sécurité et à l'environnement.

La présente norme donne des lignes directrices qui aident les directeurs et leur personnel technique à optimiser la sûreté de fonctionnement.

La présente norme n'a pas pour objectif la certification.

## 2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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).

Aucune.