IEC 62628

Edition 1.0 2012-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Guidance on software aspects of dependability

Lignes directrices concernant la sûreté de fonctionnement du logiciel

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XB

ICS 03.120.01

ISBN 978-2-83220-303-3

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

® 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, definitions and abbreviations 7
3.1 Terms and definitions 7
3.2 Abbreviations 9
4 Overview of software aspects of dependability 9
4.1 Software and software systems 9
4.2 Software dependability and software organizations 10
4.3 Relationship between software and hardware dependability 10
4.4 Software and hardware interaction 11
5 Software dependability engineering and application 12
5.1 System life cycle framework 12
5.2 Software dependability project implementation 12
5.3 Software life cycle activities 13
5.4 Software dependability attributes 14
5.5 Software design environment 15
5.6 Establishing software requirements and dependability objectives 15
5.7 Classification of software faults 16
5.8 Strategy for software dependability implementation 17
5.8.1 Software fault avoidance 17
5.8.2 Software fault control 17
6 Methodology for software dependability applications 18
6.1 Software development practices for dependability achievement 18
6.2 Software dependability metrics and data collection 18
6.3 Software dependability assessment 19
6.3.1 Software dependability assessment process 19
6.3.2 System performance and dependability specification 20
6.3.3 Establishing software operational profile 21
6.3.4 Allocation of dependability attributes 21
6.3.5 Dependability analysis and evaluation 22
6.3.6 Software verification and software system validation 24
6.3.7 Software testing and measurement 25
6.3.8 Software reliability growth and forecasting 28
6.3.9 Software dependability information feedback 29
6.4 Software dependability improvement 29
6.4.1 Overview of software dependability improvement 29
6.4.2 Software complexity simplification 29
6.4.3 Software fault tolerance 30
6.4.4 Software interoperability 30
6.4.5 Software reuse 31
6.4.6 Software maintenance and enhancement 31
6.4.7 Software documentation 32
6.4.8 Automated tools 33
6.4.9 Technical support and user training 33

7 Software assurance 34
7.1 Overview of software assurance 34
7.2 Tailoring process 34
7.3 Technology influence on software assurance 34
7.4 Software assurance best practices 35
Annex A (informative) Categorization of software and software applications 37
Annex B (informative) Software system requirements and related dependability activities 39
Annex C (informative) Capability maturity model integration process 43
Annex D (informative) Classification of software defect attributes 46
Annex E (informative) Examples of software data metrics obtained from data collection 50
Annex F (informative) Example of combined hardware/software reliability functions 53
Annex G (informative) Summary of software reliability model metrics 55
Annex H (informative) Software reliability models selection and application 56
Bibliography 59

Figure 1 – Software life cycle activities 14
Figure F.1 – Block diagram for a monitoring control system 53

Table C.1 – Comparison of capability and maturity levels 43
Table D.1 – Classification of software defect attributes when a fault is found 46
Table D.2 – Classification of software defect attributes when a fault is fixed 47
Table D.3 – Design review/code inspection activity to triggers mapping 47
Table D.4 – Unit test activity to triggers mapping 48
Table D.5 – Function test activity to triggers mapping 48
Table D.6 – System test activity to triggers mapping 49
Table H.1 – Examples of software reliability models 57

INTERNATIONAL ELECTROTECHNICAL COMMISSION

GUIDANCE ON SOFTWARE ASPECTS OF 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 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 62628 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/1469/FDIS	56/1480/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 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

Software has widespread applications in today's products and systems. Examples include software applications in programmable control equipment, computer systems and communication networks. Over the years, many standards have been developed for software engineering, software process management, software quality and reliability assurance, but only a few standards have addressed the software issues from a dependability perspective.

Dependability is the ability of a system to perform as and when required to meet specific objectives under given conditions of use. The dependability of a system infers that the system is trustworthy and capable of performing the desired service upon demand to satisfy user needs. The increasing trends in software applications in the service industry have permeated in the rapid growth of Internet services and Web development. Standardized interfaces and protocols have enabled the use of third-party software functionality over the Internet to permit cross-platform, cross-provider, and cross-domain applications. Software has become a driving mechanism to realize complex system operations and enable the achievement of viable e-businesses for seamless integration and enterprise process management. Software design has assumed the primary function in data processing, safety monitoring, security protection and communication links in network services. This paradigm shift has put the global business communities in trust of a situation relying heavily on the software systems to sustain business operations. Software dependability plays a dominant role to influence the success in system performance and data integrity.

This International Standard provides current industry best practices and presents relevant methodology to facilitate the achievement of software dependability. It identifies the influence of management on software aspects of dependability and provides relevant technical processes to engineer software dependability into systems. The evolution of software technology and rapid adaptation of software applications in industry practices have created the need for practical software dependability standard for the global business environment. A structured approach is provided for guidance on the use of this standard.

The generic software dependability requirements and processes are presented in this standard. They form the basis for dependability applications for most software product development and software system implementation. Additional requirements are needed for mission critical, safety and security applications. Industry specific software qualification issues for reliability and quality conformance are not addressed in this standard.

This standard can also serve as guidance for dependability design of firmware. It does not however, address the implementation aspects of firmware with software contained or embedded in the hardware chips to realize their dedicated functions. Examples include application specific integrated circuit (ASIC) chips and microprocessor driven controller devices. These products are often designed and integrated as part of the physical hardware features to minimize their size and weight and facilitate real time applications such as those used in cell phones. Although the general dependability principles and practices described in this standard can be used to guide design and application of firmware, specific requirements are needed for their physical construction, device fabrication and embedded software product implementation. The physics of failure of application specific devices behaves differently as compared to software system failures.

This International Standard is not intended for conformity assessment or certification purposes.

GUIDANCE ON SOFTWARE ASPECTS OF DEPENDABILITY

1 Scope

This International Standard addresses the issues concerning software aspects of dependability and gives guidance on achievement of dependability in software performance influenced by management disciplines, design processes and application environments. It establishes a generic framework on software dependability requirements, provides a software dependability process for system life cycle applications, presents assurance criteria and methodology for software dependability design and implementation and provides practical approaches for performance evaluation and measurement of dependability characteristics in software systems.

This standard is applicable for guidance to software system developers and suppliers, system integrators, operators and maintainers and users of software systems who are concerned with practical approaches and application engineering to achieve dependability of software products and systems.

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.

IEC 60050-191, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

IEC 60300-3-15, *Dependability management – Part 3-15: Application guide – Engineering of system dependability*

SOMMAIRE

AVANT-PROPOS 64
INTRODUCTION 66
1 Domaine d'application 67
2 Références normatives 67
3 Termes, définitions et abréviations 67
3.1 Termes et définitions 67
3.2 Abréviations 69
4 Présentation de la sûreté de fonctionnement du logiciel 70
4.1 Logiciels et systèmes logiciels 70
4.2 Sûreté de fonctionnement du logiciel et organisations logicielles 70
4.3 Relation entre la sûreté de fonctionnement du logiciel et du matériel 71
4.4 Interaction du logiciel et du matériel 72
5 Ingénierie et application de la sûreté de fonctionnement du logiciel 73
5.1 Cadre du cycle de vie du système 73
5.2 Mise en œuvre du projet de sûreté de fonctionnement du logiciel 73
5.3 Activités du cycle de vie du logiciel 74
5.4 Attributs de sûreté de fonctionnement du logiciel 75
5.5 Environnement de conception du logiciel 76
5.6 Définition des exigences et objectifs de sûreté de fonctionnement du logiciel 77
5.7 Classification des défauts logiciels 78
5.8 Stratégie relative à la mise en œuvre de la sûreté de fonctionnement du logiciel 78
5.8.1 Evitement des défauts logiciels 78
5.8.2 Contrôle des défauts logiciels 79
6 Méthodologie relative aux applications de sûreté de fonctionnement du logiciel 80
6.1 Pratiques de développement de logiciels pour la réalisation de la sûreté de fonctionnement 80
6.2 Mesures de la sûreté de fonctionnement du logiciel et collecte de données 80
6.3 Evaluation de la sûreté de fonctionnement du logiciel 82
6.3.1 Processus d'évaluation de la sûreté de fonctionnement du logiciel 82
6.3.2 Spécification relative à la performance et à la sûreté de fonctionnement du système 82
6.3.3 Etablir le profil opérationnel du logiciel 83
6.3.4 Allocation d'attributs de sûreté de fonctionnement 84
6.3.5 Analyse et évaluation de la sûreté de fonctionnement 84
6.3.6 Vérification du logiciel et validation du système logiciel 87
6.3.7 Essai des logiciels et mesure 88
6.3.8 Croissance et prévision de la fiabilité logicielle 91
6.3.9 Retour d'informations sur la sûreté de fonctionnement du logiciel 92
6.4 Amélioration de la sûreté de fonctionnement du logiciel 93
6.4.1 Présentation de l'amélioration de la sûreté de fonctionnement du logiciel 93
6.4.2 Simplification de la complexité logicielle 93
6.4.3 Tolérance aux pannes du logiciel 93
6.4.4 Interopérabilité logicielle 94
6.4.5 Réutilisation du logiciel 94

6.4.6 Maintenance et amélioration du logiciel 95
6.4.7 Documentation relative au logiciel 96
6.4.8 Outils automatisés 97
6.4.9 Support technique et formation des utilisateurs 97
7 Assurance logicielle 98
7.1 Présentation de l'assurance logicielle 98
7.2 Processus de personnalisation 98
7.3 Influence technologique sur l'assurance logicielle 99
7.4 Pratiques d'excellence en matière d'assurance logicielle 100
Annexe A (informative) Classement des logiciels et applications logicielles 101
Annexe B (informative) Exigences relatives au système logiciel et activités de sûreté de fonctionnement associées 104
Annexe C (informative) Processus d'intégration du modèle d'évolution des capacités 108
Annexe D (informative) Classification des attributs des défauts logiciels 111
Annexe E (informative) Exemples de métriques de données logicielles obtenues à partir de la collecte de données 115
Annexe F (informative) Exemple de fonctions de fiabilité matérielle/logicielle combinées 118
Annexe G (informative) Résumé des métriques du modèle de fiabilité logicielle 120
Annexe H (informative) Sélection et application de modèles de fiabilité logicielle 121
Bibliographie 125

Figure 1 – Activités du cycle de vie du logiciel 75
Figure F.1 – Schéma de principe pour un système de contrôle de surveillance 118

Tableau C.1 – Comparaison des niveaux de capacité et de maturité 108
Tableau D.1 – Classification des attributs de défauts logiciels lorsqu'un défaut est détecté 111
Tableau D.2 – Classification des attributs de défauts logiciels lorsqu'un défaut est corrigé 112
Tableau D.3 – Allocation de l'activité «examen de conception/inspection de code» sur les déclencheurs 112
Tableau D.4 – Allocation de l'activité «Test de l'unité» sur les déclencheurs 113
Tableau D.5 – Allocation de l'activité «test de fonction» sur les déclencheurs 114
Tableau D.6 – Allocation de l'activité «test du système» sur les déclencheurs 114
Tableau H.1 – Exemples de modèles de fiabilité logicielle 122

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

LIGNES DIRECTRICES CONCERNANT LA SÛRETÉ DE FONCTIONNEMENT DU LOGICIEL

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 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 la CEI. La CEI 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 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 brevet. La CEI 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 CEI 62628 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
56/1469/FDIS	56/1480/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.

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 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 logiciels sont très répandus dans les produits et systèmes actuels, à titre d'exemples les applications logicielles dans les équipements de commande programmables, les systèmes informatiques et les réseaux de communication. Au cours des années, de nombreuses normes ont été développées en matière de génie logiciel, de gestion des processus logiciels, de qualité logicielle et de garantie de fiabilité, mais seules quelques normes traitent les questions logicielles d'un point de vue de la sûreté de fonctionnement.

La sûreté de fonctionnement est la capacité d'un système à fonctionner au moment voulu et tel que prévu de façon à satisfaire aux objectifs spécifiés dans des conditions d'utilisation données. La sûreté de fonctionnement d'un système suppose que le système est sûr et capable d'exécuter le service souhaité, sur demande, pour répondre aux besoins des utilisateurs. L'évolution croissante des applications logicielles dans l'industrie des services a entraîné un rapide développement des services Internet et du Web. Les interfaces et protocoles standardisés ont permis l'utilisation de logiciels-tiers sur Internet et par là-même, les applications inter-plates-formes, inter-fournisseurs et inter-domaines. Les logiciels sont devenus un moteur pour réaliser des opérations complexes et permettre la réalisation d'affaires électroniques viables pour une intégration sans fil et la gestion des processus d'affaires. La conception de logiciels a mis l'accent sur le traitement des données, la surveillance de la sécurité et les liens de communication dans les services de réseau. Ce changement de paradigme a mis le monde des affaires mondial dans une situation reposant fortement sur les systèmes logiciels pour soutenir les opérations financières. La sûreté de fonctionnement du logiciel joue un rôle dominant pour influencer le succès des performances d'un système et l'intégrité des données.

La présente Norme internationale présente les pratiques d'excellence actuelles et la méthodologie correspondante pour faciliter la réalisation de la sûreté de fonctionnement du logiciel. Elle identifie l'influence du management sur les aspects logiciels de la sûreté de fonctionnement et fournit les processus techniques correspondants à la sûreté de fonctionnement du logiciel dans les systèmes. L'évolution de la technologie logicielle et l'adaptation rapide des applications logicielles dans les pratiques industrielles ont créé le besoin d'une norme pratique relative à la sûreté de fonctionnement du logiciel pour le marché mondial des affaires. Une approche structurée est fournie afin de servir de lignes directrices pour l'utilisation de cette norme.

Les exigences et processus génériques en matière de sûreté de fonctionnement du logiciel sont présentés dans cette norme. Ils représentent la base des applications de sûreté de fonctionnement pour le développement de produits logiciels et la mise en œuvre de systèmes logiciels en grande partie. Des exigences supplémentaires sont requises pour les applications d'importance vitale, de sûreté et de sécurité. Les aspects liés à la qualification des logiciels spécifiques à l'industrie en termes de fiabilité et de qualité ne sont pas traités dans cette norme.

Cette norme peut également servir de lignes directrices pour la conception de la sûreté de fonctionnement de micro-logiciels. Elle ne porte cependant pas sur les aspects de mise en œuvre des micro-logiciels avec les logiciels contenus ou intégrés dans les puces matérielles pour réaliser leurs fonctions dédiées telles les puces à circuit intégré à application spécifique (ASIC) et les contrôleurs commandés par microprocesseur. Ces produits sont souvent conçus et intégrés dans le cadre des fonctionnalités matérielles physiques pour minimiser leur taille et leur poids et faciliter les applications en temps réel comme celles utilisées dans les téléphones cellulaires. Bien que les principes et pratiques de sûreté de fonctionnement générale, décrits dans cette norme, puissent faciliter la conception et l'application de micro-logiciels, des exigences spécifiques sont nécessaires pour leur construction physique, la fabrication des appareils et la mise en œuvre des produits logiciels intégrés. La physique de défaillance des appareils spécifiques à l'application se comporte différemment par rapport aux défaillances du système logiciel.

La présente Norme Internationale n'est pas conçue à des fins d'évaluation de la conformité ou de certification.

LIGNES DIRECTRICES CONCERNANT LA SÛRETÉ DE FONCTIONNEMENT DU LOGICIEL

1 Domaine d'application

La présente Norme internationale porte sur les problèmes concernant la sûreté de fonctionnement du logiciel et définit les lignes directrices pour la réalisation de la sûreté de fonctionnement dans les performances logicielles influencées par les disciplines de management, les processus de conception et les environnements d'application. Elle définit un cadre générique pour les exigences en matière de sûreté de fonctionnement du logiciel, fournit un processus de sûreté de fonctionnement du logiciel pour les applications du cycle de vie du système, présente les critères d'assurance et la méthodologie pour la conception et la mise en œuvre de la sûreté de fonctionnement du logiciel, et fournit des approches et mesures pratiques des caractéristiques de sûreté de fonctionnement dans les systèmes logiciels.

La présente norme s'applique aux développeurs et fournisseurs de systèmes logiciels, aux intégrateurs de systèmes, aux opérateurs et aux spécialistes de la maintenance, ainsi qu'aux utilisateurs de systèmes logiciels qui sont concernés par les approches pratiques et l'ingénierie d'application pour atteindre la sûreté de fonctionnement des produits et systèmes logiciels.

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).

CEI 60050-191, *Vocabulaire Electrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60300-3-15, *Gestion de la sûreté de fonctionnement – Partie 3-15: Guide d'application – Ingénierie de la sûreté de fonctionnement des systèmes*