IEC 62853

Edition 1.0 2018-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Open systems dependability

Sûreté de fonctionnement des systèmes ouverts

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.100.40; 03.120.01; 21.020

ISBN 978-2-8322-5789-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

OPEN SYSTEMS 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 62853 has been prepared by IEC technical committee 56: Dependability.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
56/1772/FDIS	56/1776/RVD

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

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

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under “http://webstore.iec.ch” in the data related to the specific document. At this date, the document will be

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- withdrawn,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

IMPORTANT – The ‘colour inside’ logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Open systems are systems whose boundaries, functions and structure change over time and which are recognized and described differently from various points of view. The dependability of open systems is a key attribute for the life cycle of a system that operates for an extended period of time in a real-world environment. Open systems dependability is the ability of open systems to accommodate changes in purpose, objectives, environment and actual performance and to continuously maintain accountability from stakeholders, in order to provide expected services as and when required. The attributes of dependability, including availability, reliability, maintainability and supportability, are the same for open systems as conventional systems but they have to be considered in the context that no single stakeholder has a full understanding of the system or its risks.

For open systems, security is especially important since the systems are much exposed to attack by malware. Since an open system changes continuously through its life, the design process, e.g. modelled by the spiral product development model, will to some extent continue during the whole lifetime of the system.

This document elaborates on IEC 60300-1 by providing additional guidance for dependability management of open systems.

This document provides guidance on open systems dependability by using the four process views, each of which selects and combines system life cycle processes, activities and tasks of ISO/IEC/IEEE 15288: 2015.

- Change Accommodation process view;
- Accountability Achievement process view;
- Failure Response process view;
- Consensus Building process view.

A dependability case that assures these process views is crucial for stakeholders to understand and agree on the boundaries of their responsibilities, to assign accountability for implementation and to duly manage changes in achieving open systems dependability.

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

OPEN SYSTEMS DEPENDABILITY

1 Scope

This document provides guidance in relation to a set of requirements placed upon system life cycles in order for an open system to achieve open systems dependability.

This document elaborates on IEC 60300-1 by providing details of the changes needed to accommodate the characteristics of open systems. It defines process views based on ISO/IEC/IEEE 15288:2015, which identifies the set of system life cycle processes.

This document is applicable to life cycles of products, systems, processes or services involving hardware, software and human aspects or any integrated combinations of these elements.

For open systems, security is especially important since the systems are particularly exposed to attack.

This document can be used to improve the dependability of open systems and to provide assurance that the process views specific to open systems achieve their expected outcomes. It helps an organization define the activities and tasks that need to be undertaken to achieve dependability objectives in an open system, including dependability related communication, dependability assessment and evaluation of dependability throughout system life cycles.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050-192, *International Electrotechnical Vocabulary – Part 192: Dependability* (available at http://www.electropedia.org/)

IEC 60300-1, *Dependability management – Part 1: Guidance for management and application*

ISO/IEC/IEEE 15288:2015, *Systems and software engineering – System life cycle processes*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÛRETÉ DE FONCTIONNEMENT DES SYSTÈMES OUVERTS

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 62853 a été établie par le comité d'études 56 de l'IEC: Sûreté de fonctionnement.

Le texte de cette norme internationale est issu des documents suivants:

FDIS	Rapport de vote
56/1772/FDIS	56/1776/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 internationale.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de ce document 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 au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "*colour inside*" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Les systèmes ouverts sont des systèmes dont les frontières, les fonctions et la structure changent avec le temps et qui sont envisagés et décrits différemment selon le point de vue. La sûreté de fonctionnement des systèmes ouverts est un attribut clé du cycle de vie d'un système qui fonctionne pendant une période prolongée dans un environnement réel. La sûreté de fonctionnement des systèmes ouverts est la capacité des systèmes ouverts à s'adapter aux changements apportés à leur objet, leurs objectifs, leur environnement et leurs performances réelles et à maintenir la redevabilité continue des parties prenantes de manière à fournir les services attendus au moment requis et lorsque cela est exigé. Les attributs de la sûreté de fonctionnement, tels que la disponibilité, la fiabilité, la maintenabilité et la supportabilité, sont les mêmes pour les systèmes ouverts que pour les systèmes conventionnels, mais ils doivent être envisagés dans un contexte où aucune partie prenante ne comprend pleinement le système et ses risques.

La sécurité des systèmes ouverts est particulièrement importante, car ces systèmes sont fortement exposés aux attaques des logiciels malveillants. Etant donné qu'un système ouvert évolue continuellement au cours de sa vie, le processus de conception (éventuellement modélisé par le modèle en spirale de développement de produits) se poursuivra, dans une certaine mesure, pendant toute sa durée de vie.

Le présent document précise l'IEC 60300-1 en fournissant des recommandations supplémentaires sur la gestion de la sûreté de fonctionnement des systèmes ouverts.

Le présent document contient des recommandations sur la sûreté de fonctionnement des systèmes ouverts qui s'appuient sur les quatre vues de processus, dont chacune sélectionne et combine des processus, activités et tâches du cycle de vie du système décrits dans l'ISO/IEC/IEEE 15288: 2015.

- vue de processus d'adaptation aux changements;
- vue de processus d'établissement de la redevabilité;
- vue de processus de réponse aux défaillances;
- vue de processus de recherche d'un consensus.

Il est crucial de réaliser une étude de sûreté de fonctionnement à l'appui de ces vues de processus pour que les parties prenantes comprennent et s'accordent sur les limites de leurs responsabilités, attribuent la redevabilité relative à la mise en œuvre et gèrent dûment les changements nécessaires à l'assurance de la sûreté de fonctionnement des systèmes ouverts.

Le présent document s'adresse aux utilisateurs, aux propriétaires, aux clients et aux organismes impliqués dans la conformité aux exigences de sûreté de fonctionnement des systèmes ouverts, et chargés de la garantir. On entend par "organismes" les entreprises, et institutions publiques ou privées de tous types et de toutes tailles, telles que les administrations publiques, les entreprises commerciales et les associations à but non lucratif.

SÛRETÉ DE FONCTIONNEMENT DES SYSTÈMES OUVERTS

1 Domaine d'application

Le présent document fournit des recommandations relatives à un ensemble d'exigences portant sur les cycles de vie des systèmes et visant à assurer la sûreté de fonctionnement des systèmes ouverts.

Le présent document précise l'IEC 60300-1 en fournissant des détails sur les changements nécessaires pour s'adapter aux caractéristiques des systèmes ouverts. Il définit les vues de processus basées sur l'ISO/IEC/IEEE 15288:2015, qui identifie l'ensemble des processus du cycle de vie du système.

Le présent document est applicable au cycle de vie des produits, des systèmes, des processus ou des services impliquant des aspects matériels, logiciels et humains ou toute combinaison intégrant ces éléments.

La sécurité des systèmes ouverts est particulièrement importante, car ces systèmes sont fortement exposés aux attaques des logiciels malveillants.

Le présent document peut être utilisé pour améliorer la sûreté de fonctionnement des systèmes ouverts et pour garantir que les vues de processus spécifiques aux systèmes ouverts donnent les résultats escomptés. Il aide les organismes à définir les activités et les tâches qui doivent être entreprises pour atteindre les objectifs de sûreté de fonctionnement dans un système ouvert, y compris en matière de communication relative à la sûreté de fonctionnement, ainsi que d'appréciation et d'évaluation de la sûreté de fonctionnement tout au long du cycle de vie du système.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences 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).

IEC 60050-192, *Vocabulaire électrotechnique international – Partie 192: Sûreté de fonctionnement* (disponible à l'adresse http://www.electropedia.org/)

IEC 60300-1, *Gestion de la sûreté de fonctionnement – Partie 1: Lignes directrices pour la gestion et l'application*

ISO/IEC/IEEE 15288:2015, *Systems and software engineering – System life cycle processes* (disponible en anglais seulement)