This is a preview - click here to buy the full publication

IEC 62741

Edition 1.0 2015-02

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

## Demonstration of dependability requirements – The dependability case

## Démonstration des exigences de sûreté de fonctionnement – Argumentaire dans le cadre de la sûreté de fonctionnement

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.120.01; 21.020

ISBN 978-2-8322-2247-8

**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

This is a preview - click here to buy the full publication



# CONTENTS

This is a preview - click here to buy the full publication

This is a preview - click here to buy the full publication



INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

# DEMONSTRATION OF DEPENDABILITY REQUIREMENTS – THE DEPENDABILITY CASE

## 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 62741 has been prepared by IEC technical committee 56: Dependability.

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

| FDIS | Report on voting |
|---|---|
| 56/1591/FDIS | 56/1609/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.

This is a preview - click here to buy the full publication



The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website 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.

This is a preview - click here to buy the full publication



# INTRODUCTION

Dependability is the ability to perform as and when required. Acceptable levels of dependability are therefore essential for continued performance and optimized life cycle costs.

In order to achieve dependability of a system, dependability requirements should be established, the risks of not meeting them identified and a suitable set of activities developed to meet and demonstrate the requirements and manage the risks. A dependability case provides a convenient and convincing means of recording the output of these activities in a single location and presenting an argument, supported by evidence, that risks have been treated and that the necessary dependability has been or will be achieved and will continue to be achieved over time. It serves as the main means of communication on dependability among customers, suppliers and other stakeholders and promotes cooperation among them. This is essential for dependability achievement and providing assurance as part of the customer/supplier relationship.

Preparing a dependability case can also improve dependability through the actions taken to prepare and develop the argument within the dependability case. It can improve the cost effectiveness of a dependability programme because if an activity does not provide evidence to support the case, this may indicate that the activity is not necessary.

The activities required for the achievement of dependability depend on the nature and development state of the system and are likely to vary significantly from one project to another.

Throughout this International Standard, the term "dependability" includes all aspects of reliability, availability, maintainability and supportability, as well as other attributes such as usability, testability and durability. In addition, dependability of a system includes all aspects of that system, including components, processes, hardware, software and the interfaces between them.

This standard is intended as guidance: the guidelines are not prescriptive in nature, they are generic, they should be tailored to the specific objectives and are not exhaustive.

This standard does not address safety or the environment.

This is a preview - click here to buy the full publication



# DEMONSTRATION OF DEPENDABILITY REQUIREMENTS – THE DEPENDABILITY CASE

## 1 Scope

This International Standard gives guidance on the content and application of a dependability case and establishes general principles for the preparation of a dependability case.

This standard is written in a basic project context where a customer orders a system that meets dependability requirements from a supplier and then manages the system until its retirement. The methods provided in this standard may be modified and adapted to other situations as needed.

The dependability case is normally produced by the customer and supplier but can also be used and updated by other organizations. For example, certification bodies and regulators may examine the submitted case to support their decisions and users of the system may update/expand the case, particularly where they use the system for a different purpose.

## 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 60050-192, *International Electrotechnical Vocabulary – Part 192: Dependability* [1]

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

ISO 31000, *Risk management – Principles and guidelines*

---

1 To be published.

This is a preview - click here to buy the full publication



# SOMMAIRE

This is a preview - click here to buy the full publication

This is a preview - click here to buy the full publication



COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

# DÉMONSTRATION DES EXIGENCES DE SÛRETÉ DE FONCTIONNEMENT – ARGUMENTAIRE DANS LE CADRE DE LA SÛRETÉ DE FONCTIONNEMENT

## 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 62741 a été établie par le comité d'études 56 de l'IEC: Sûreté de fonctionnement.

Le texte de cette norme est issu des documents suivants:

| FDIS | Rapport de vote |
|---|---|
| 56/1591/FDIS | 56/1609/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/IEC, Partie 2.

This is a preview - click here to buy the full publication



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.

This is a preview - click here to buy the full publication



# INTRODUCTION

La sûreté de fonctionnement est la capacité d'exécuter comme exigé et lorsque cela est exigé. Les niveaux acceptables de sûreté de fonctionnement sont ainsi essentiels pour une performance continue et des coûts du cycle de vie optimisés.

Afin d'atteindre la sûreté de fonctionnement d'un système, il convient d'établir les exigences en la matière, d'identifier les risques de non-satisfaction, et de développer un ensemble adapté d'activités pour satisfaire aux exigences, démontrer les exigences et gérer les risques. Une étude de sûreté de fonctionnement fournit un moyen pratique et convaincant d'enregistrer le résultat de ces activités dans un seul endroit et de présenter un argument, étayé par des preuves, que les risques ont été traités et que la sûreté de fonctionnement nécessaire a été ou sera atteinte ou continuera d'être atteinte dans le temps. Elle sert de moyen principal de communication sur la sûreté de fonctionnement entre clients, fournisseurs et autres acteurs et favorise la coopération entre eux. Cela est essentiel pour assurer la sûreté de fonctionnement et fournir l'assurance dans le cadre de la relation client/fournisseur.

La préparation d'une étude de sûreté de fonctionnement peut améliorer la sûreté de fonctionnement par le biais des actions prises pour préparer et développer l'argument dans l'étude de sûreté de fonctionnement. Elle peut améliorer le rapport coût-efficacité d'un programme de sûreté de fonctionnement car si une activité ne fournit pas la preuve qu'elle étaie l'étude, ceci peut indiquer que l'activité n'est pas nécessaire.

Les activités exigées pour la réalisation de la sûreté de fonctionnement dépendent de la nature et de l'état de développement du système et sont susceptibles de varier fortement d'un projet à l'autre.

Tout au long de la présente Norme internationale, le terme "sûreté de fonctionnement" inclut tous les aspects liés à la fiabilité, la disponibilité, la maintenabilité et l'aptitude au soutien, ainsi que d'autres attributs tels que l'aptitude à l'utilisation, la testabilité et la durabilité. De plus, la sûreté de fonctionnement d'un système inclut tous les aspects de ce système, y compris les composants, processus, matériels, logiciels et les interfaces entre eux.

La présente norme fait office de lignes directrices, lesquelles n'étant pas prescriptives par nature, mais étant génériques. Il convient qu'elles soient adaptées aux objectifs spécifiques et qu'elles ne soient pas exhaustives.

La présente norme n'aborde pas les questions liées à la sécurité ou l'environnement.

This is a preview - click here to buy the full publication



# DÉMONSTRATION DES EXIGENCES DE SÛRETÉ DE FONCTIONNEMENT – ARGUMENTAIRE DANS LE CADRE DE LA SÛRETÉ DE FONCTIONNEMENT

## 1 Domaine d'application

La présente Norme internationale fournit des lignes directrices concernant le contenu et l'application d'une étude de sûreté de fonctionnement et établit les principes généraux pour la préparation d'une étude de sûreté de fonctionnement.

La présente norme est rédigée dans le cadre d'un projet de base où un client commande un système qui satisfait aux exigences de sûreté de fonctionnement d'un fournisseur et gère alors le système jusqu'à sa mise hors service. Les méthodes fournies dans cette norme peuvent être modifiées et adaptées aux autres situations, si nécessaire.

L'étude de sûreté de fonctionnement est normalement produite par le client et le fournisseur et peut également être utilisée et mise à jour par d'autres organisations. Par exemple, les organismes de certification et législateurs peuvent examiner l'étude soumise pour étayer leurs décisions et les utilisateurs du système peuvent mettre à jour/développer l'étude, notamment lorsqu'ils utilisent le système à une autre fin.

## 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).

IEC 60050-192, *Vocabulaire électrotechnique international – Partie 192: Sûreté de fonctionnement* [1]

IEC 60300-1, *Gestion de la sûreté de fonctionnement – Partie 1: gestion du programme de sûreté de fonctionnement*

ISO 31000, *Management du risque – Principes et lignes directrices*

---

1 A publier.