IEC 62960

Edition 1.0 2020-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Dependability reviews during the life cycle

Revues de la sûreté de fonctionnement au cours du cycle de vie

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.120.01

ISBN 978-2-8322-7977-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

DEPENDABILITY REVIEWS DURING THE LIFE CYCLE

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 62960 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
56/1874/FDIS	56/1878/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

Dependability is the ability to perform as and when required. Dependability has many attributes but is usually characterized in terms of reliability, maintainability, supportability (including maintenance and support) and availability. These attributes are subject to change over the life cycle and can benefit from regular review.

Benefits of dependability review throughout the life cycle include:

– discovering and mitigating or eliminating weaknesses in the early life cycle stages before they manifest as dependability problems in later stages;
– identifying and treating problems which might occur later in the life cycle, and providing feedback to prevent their recurrence and to adapt systems to changes in environment and other factors;
– providing assurance of dependability and of the systems and processes that aim to achieve dependability;
– continually improving the dependability of the system in order to maintain or improve a commercial advantage.

Systems are becoming increasingly complex and constantly changing. This raises specific problems that need attention. Systems are changing in the following ways. A system is often developed, and/or utilized, in organizations across national borders and industry sectors. Changes such as legislation affecting one country or industry sector may necessitate a change to the system. System requirements can also change over time as technology, environmental conditions and societal demands change.

Dependability reviews are mainly used for large systems, but even small products such as mobile phones are complicated systems that may require dependability reviews.

Organizations involved in different parts of the life cycle might not be able to share a common purpose. For example, an engineering design company during the development and realization stages may not be able to fully anticipate the needs of stakeholders at the utilization stage. More generally, it is becoming increasingly difficult to predict at some earlier stage potential dependability problems that can occur at a later life cycle stage. Dependability reviews carried out at appropriate points during the life cycle can assist in addressing all of the above issues.

This document provides guidance on dependability reviews as part of an organization’s technical review processes. It provides a coherent set of principles for dependability reviews which could be useful in addition to, and in support of, general monitoring and dependability assurance carried out by various organizations at different life cycle stages.

In many cases dependability aspects of a system are covered in other reviews such as design reviews or manufacturability reviews. In these cases, the procedures given in this document can be applied. The informative annexes can be used as checklists to cover all technical relevant aspects.

Dependability reviews described in this document are a key part of a dependability management system as described in IEC 60300-1.

DEPENDABILITY REVIEWS DURING THE LIFE CYCLE

1 Scope

This document provides guidance on a review methodology for dependability from a technical perspective that is applicable at all stages of a system life cycle. Its application can improve the dependability of a system throughout its life cycle by triggering appropriate actions at appropriate times to address potential dependability problems.

It provides guidance for developers, manufacturers, users and third-party independent reviewers such as consulting organizations.

This document describes a dependability review methodology focusing on:

– coherence of review activities across life cycle stages and their impact on dependability;
– stakeholder identification and how this affects dependability review activities;
– the relationships between different types of reviews;
– procedures for effective dependability reviews;
– examples of dependability review activities.

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)

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

REVUES DE LA SÛRETÉ DE FONCTIONNEMENT AU COURS DU CYCLE DE VIE

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 62960 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	Report on voting
56/1874/FDIS	56/1878/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

La sûreté de fonctionnement est la capacité à fonctionner correctement et au moment voulu. Elle possède de nombreux attributs, mais se caractérise généralement par la fiabilité, la maintenabilité, la supportabilité (y compris la maintenance et le soutien) et la disponibilité. Ces attributs sont appelés à évoluer au cours de leur cycle de vie et peuvent tirer parti de revues régulières.

Une revue de la sûreté de fonctionnement tout au long du cycle de vie comporte divers avantages:

– découvrir et réduire ou éliminer les faiblesses dès les premières phases du cycle de vie, avant qu'elles n'affectent la sûreté de fonctionnement au cours des phases ultérieures;
– identifier et traiter les problèmes pouvant survenir ultérieurement au cours du cycle de vie, et assurer un retour d'informations afin d'éviter leur récurrence et d'adapter les systèmes aux changements d'environnement et autres facteurs;
– fournir une assurance de la sûreté de fonctionnement ainsi que des systèmes et processus qui ont pour objet de garantir la sûreté de fonctionnement;
– améliorer de façon continue la sûreté de fonctionnement du système afin de préserver ou de renforcer un avantage commercial.

Les systèmes connaissent une évolution constante et se révèlent de plus en plus complexes. Cela soulève des problèmes spécifiques qui nécessitent une attention particulière. Les systèmes sont soumis à divers changements. Un système est souvent élaboré et/ou utilisé dans des organisations implantées au-delà des frontières nationales et dans divers secteurs d'activité. Les évolutions, notamment de la législation, qui affectent un pays ou un secteur industriel peuvent nécessiter une modification du système. Les exigences du système peuvent aussi changer au fil du temps, à mesure qu'évoluent la technologie, les conditions environnementales et les exigences sociétales.

Les revues de la sûreté de fonctionnement sont principalement appliquées aux systèmes de grande envergure, mais même les produits de petite taille, tels que les téléphones portables, constituent des systèmes complexes qui peuvent exiger des revues de la sûreté de fonctionnement.

Les organisations impliquées dans les différentes parties du cycle de vie peuvent ne pas être capables de partager un objectif commun. Pendant les phases de développement et de réalisation, par exemple, un bureau d'études peut ne pas être en mesure d'anticiper les besoins des parties prenantes à la phase d'utilisation. D'une manière plus générale, il devient de plus en plus difficile de prévoir au cours des premières phases certains problèmes de sûreté de fonctionnement potentiels pouvant se produire à une phase ultérieure du cycle de vie. La réalisation de revues de la sûreté de fonctionnement à des moments appropriés du cycle de vie peut aider à résoudre l'ensemble de ces problèmes.

Le présent document fournit des recommandations concernant les revues de la sûreté de fonctionnement entreprises dans le cadre des processus de revue technique d'une organisation. Il fournit un ensemble de principes cohérents applicables aux revues de la sûreté de fonctionnement, qui peuvent se révéler utiles en complément et en accompagnement du processus général de surveillance et d'assurance de sûreté de fonctionnement entrepris par différentes organisations à différentes étapes du cycle de vie.

Dans de nombreux cas, les aspects liés à la sûreté de fonctionnement d'un système sont traités dans le cadre d'autres revues, telles que les revues de conception ou de fabricabilité. Les procédures indiquées dans le présent document peuvent être appliquées dans ces cas de figure. Les annexes informatives peuvent être utilisées comme listes de vérification afin de couvrir tous les aspects techniques pertinents.

Les revues de la sûreté de fonctionnement décrites dans le présent document sont un élément essentiel du système de gestion de la sûreté de fonctionnement tel que défini dans l'IEC 60300-1.

REVUES DE LA SÛRETÉ DE FONCTIONNEMENT AU COURS DU CYCLE DE VIE

1 Domaine d'application

Le présent document fournit, sous un angle technique, des recommandations relatives à une méthodologie de revue de la sûreté de fonctionnement applicable à toutes les phases du cycle de vie d'un système. Son application permet d'améliorer la sûreté de fonctionnement d'un système tout au long de son cycle de vie, en déclenchant au moment opportun des mesures adéquates pour traiter les éventuels problèmes de sûreté de fonctionnement.

Il fournit des recommandations à l'attention des développeurs, des fabricants, des utilisateurs et des vérificateurs tiers indépendants, tels que des organismes de conseil.

Le présent document décrit une méthodologie de revue de la sûreté de fonctionnement portant sur:

– la cohérence des activités de revue au cours des différentes étapes du cycle de vie et leur impact sur la sûreté de fonctionnement;
– l'identification des parties prenantes et leurs effets sur les activités de revue de la sûreté de fonctionnement;
– les relations entre les différents types de revues;
– les procédures garantissant l'efficacité des revues de la sûreté de fonctionnement;
– des exemples d'activités réalisées dans le cadre de revues de la sûreté de fonctionnement.

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)