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

IEC 62960:2020-03(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

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)

3 Terms and definitions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-192 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
dependability management
coordinated activities to direct and control an organization with regard to dependability

Note 1 to entry: Dependability management is part of an organization's overall management.

[SOURCE: IEC 60300-1:2014, 3.1.4]

3.1.2
dependability plan
set of scheduled activities that when carried out are aimed to achieve dependability objectives and targets for an item

[SOURCE: IEC 60300-1:2014, 3.1.6, modified – "that when carried out are aimed" added.]

3.1.3
dependability review
review which focuses on the dependability aspects of an item, system or process being reviewed

Note 1 to entry: A dependability review can be a standalone review or a part of a review covering wider aspects.

3.1.4
design review
planned and documented review of an existing or proposed design

Note 1 to entry: Objectives include evaluation of the design's capability to fulfil the specified requirements, identification for any actual or potential deficiencies, proposing enhancements.

Note 2 to entry: A design review by itself is not sufficient to ensure proper design.

Note 3 to entry: The design can be for a product or process.

Note 4 to entry: The design review can be achieved by means of a meeting or other documented process.

3.1.5
gap analysis
method to compare what is achieved with what is required in order to identify differences and make improvements

3.1.6
item
subject being considered

Note 1 to entry: The item may be an individual part, component, device, functional unit, equipment, subsystem, or system.

Note 2 to entry: The item may consist of hardware, software, people or any combination thereof.

Note 3 to entry: The item often comprises elements that may each be individually considered.

[SOURCE: IEC 60050-192:2015, 192-01-01, modified – Note 3 modified by omission of internal references and Notes 4 and 5 deleted.]

3.1.7
life cycle
series of identifiable stages through which an item goes, from its conception to disposal

EXAMPLE A typical system life cycle consists of: concept and definition; design and development; construction, installation and commissioning; operation and maintenance; mid-life upgrading, or life extension and decommissioning and disposal.

Note 1 to entry: The stages identified will vary with the application.

[SOURCE: IEC 60050-192:2015, 192-01-09]

3.1.8
management
coordinated activities to direct and control an organization

Note 1 to entry: Management can include establishing policies and objectives and processes to achieve these objectives.

Note 2 to entry: The word "management" sometimes refers to people, i.e. a person or group of people with authority and responsibility for the conduct and control of an organization. When "management" is used in this sense, it should always be used with some form of qualifier to avoid confusion with the concept of "management" as a set of activities defined above. For example, "management shall…" is deprecated whereas "top management shall…" is acceptable. Otherwise different words should be adopted to convey the concept when related to people, e.g. managerial or managers.

[SOURCE: ISO 9000:2015, 3.3.3]

3.1.9
project
unique process, consisting of a set of coordinated and controlled activities with start and finish dates, undertaken to achieve an objective conforming to specific requirements, including the constraints of time, cost and resources

Note 1 to entry: The project's organization is normally temporary and established for the lifetime of the project.

Note 2 to entry: The complexity of the interactions among project activities is not necessarily related to the project size.

[SOURCE: ISO 9000:2015, 3.4.2, modified – Notes 1 to 3 deleted.]

3.1.10
project milestone
specific and predetermined point in a project at which certain deliverables are expected to have been attained, or at which a measurable amount of progress is to be expected

3.1.11
project review
review of the project output

3.1.12
review
activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

[SOURCE: ISO Guide 73:2009, 3.8.2.2, modified – Note deleted.]

3.1.13
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Note 1 to entry: This definition is more general than that given in IEC/ISO/IEEE 15288:2015.

[SOURCE: IEC 60300-1:2014, 3.1.5, modified – Note 1 added.]

3.1.14
status review
review of the overall project status with respect to established objectives

Note 1 to entry: The status review consists of a technical part where status information is gathered and structured and a management part where the status is determined and appropriate decisions are taken.

3.1.15
system
<in dependability> set of interrelated items that collectively fulfil a requirement

Note 1 to entry: A system is considered to have a defined real or abstract boundary.

Note 2 to entry: External resources (from outside the system boundary) may be required for the system to operate.

Note 3 to entry: A system structure may be hierarchical, e.g. system, subsystem, component, etc.

Note 4 to entry: Conditions of use and maintenance should be expressed or implied within the requirement.

[SOURCE: IEC 60050-192:2015, 192-01-03]

3.1.16
team
two or more persons working together with a set of complementary skills required to complete a task

Note 1 to entry: A member of the team is appointed as the team leader.

Note 2 to entry: The team can include persons-in-training.

3.1.17
team review
review of the team output

EXAMPLE Mechanical team, electronic team or software team as input to the technical part of the status review.

3.1.18
technical review
review of technical aspects of a process or a work product by a team of technically-qualified personnel that examines the suitability of the work product for its intended use and identifies risks and discrepancies from specifications and standards

Note 1 to entry: Subjects whose technical aspects may be reviewed include application of new technology, product line diversification, make-buy decisions, timeline for new product introduction and review of the suitability/adequacy of the technical specification.

[SOURCE: ISO/IEC 20246:2017, 3.18, modified – "formal peer review" replaced with "review of technical aspects of a process", "risks" added and Note 1 replaced.]

3.2 Abbreviated terms

COTS	commercial-off-the-shelf
FMEA	modes and effects analysis
FTA	fault tree analysis
MMH	maintenance man-hours
MTBF	mean operating time between failures
MTTF	mean time to first failure
MTTR	mean time to restoration
PoF	physics of failure
RTM	requirements traceability matrix

4 Introducing dependability reviews

4.1 General

Dependability reviews are key activities in the dependability plan. The persons in charge of dependability reviews have the responsibility for ensuring that dependability reviews are carried out during the life cycle.

Reviews involve investigating the current situation in order to compare it with what is expected or required. Reviews identify discrepancies, risks and potential problems, analyse them and recommend improvements.

Dependability reviews comprise a coherent set of reviews for different aspects of dependability. These reviews are performed repeatedly throughout the life cycle, continually providing follow-up actions and assessment of their effectiveness.

Dependability reviews can be performed from various perspectives, such as:

– the dependability attributes of an item including reliability, maintainability, supportability and availability;
– other time related characteristics of an item such as durability and recoverability;
– dependability related functions such as safety and security;
– cost efficiency, including both life cycle cost and the short term cost;
– activities carried out to achieve or assess dependability outcomes;
– effectiveness of dependability processes;
– accountability of, and to, various stakeholders for potential failures;
– adaptation to changes in requirements, environments, objectives and/or purpose of the system.

A dependability review provides assurance that dependability is achieved throughout the life cycle either by demonstrating that requirements are met or by identifying problems and making improvements. A dependability review can be used to provide evidence that a dependability claim is satisfied as part of a dependability case (IEC 62741 [3][1] gives guidance on the content of a dependability case and establishes general principles for its preparation).

Systematic dependability reviews across the system life cycle enable agile corrective redirection of effort with less waste. This is particularly beneficial given the current trends for increasing system complexity, tightening development time and prolonged operational life.

Some environments or conditions for the trends include:

– ubiquitous network connection to any range of systems controlled by others;
– frequent changes in the system's context such as user expectation and competitions in the market;
– inability to discard the old and start anew due to, for example cost consideration and preferences for "circular economy".

Dependability reviews help identify, predict and correct problems as they arise in the system life cycle while they are small enough to be addressed.

There are various types of dependability reviews. The type of dependability review performed at a life cycle stage should be appropriate to that life cycle stage. This is best managed and documented through the dependability plan. Dependability review activities during the life cycle are described in Clause 5.

A review can be internal where the review team involves people closely involved with the subject under review or it can be external where the review team involves only independent people. In this case the team which is the subject of the review provides evidence to the external review team.

Management problems such as accountability and changes in business objectives have consequences for dependability. Such problems can therefore form part of a dependability review. In this case both technical experts and managers can be involved.

---

[1] Numbers in square brackets refer to the Bibliography.

Dependability reviews can be categorized as technical reviews or management reviews. The principles of this document can be applied equally to all types of review. However, this document focuses on technical reviews. The management part of reviews in the status review is not covered. Both technical reviews and management reviews take place at each stage of the life cycle, often as an integral part of other reviews rather than as a standalone activity. Subclauses 4.2 and 4.3 describe technical reviews and status reviews.

4.2 Technical reviews

Technical reviews identify and analyse potential problems and opportunities, and recommend actions for improvement. They also provide assurance that processes are operating effectively and requirements are met.

Technical reviews can include design reviews, operation reviews, maintenance reviews, risk reviews or reviews of other technical aspects of an item or process. They may focus on dependability or dependability may be considered as part of a wider performance review.

Technical reviews of dependability can involve:

– reviews of the achieved or predicted dependability of an item where the objective is to improve dependability of the item itself by evaluating dependability measures and by exploring opportunities for improvement;

– reviews of the processes and activities planned to achieve dependability in order to learn lessons and improve future processes and activities.

Participants should have a technical understanding of the system under review and of the reliability, maintenance and supportability disciplines.

The participants should include experts who are independent from the design of the system and have necessary skills to analyse how items, systems and processes could fail. Participation of such experts is most important for securing independence and quality of the review. Participants might include, for example, quality professionals, reliability professionals, ergonomics professionals, safety analysts and test personnel.

Management should normally not participate in a technical review. The customer or user of the system or process may participate in a technical review.

Each technical review should designate a chair of the meeting (the facilitator), who can assign a secretary to assist the review.

4.3 Status reviews

The purpose of a status review is to provide the management group, and sometimes the customer, with information about how a project is progressing, and in some cases, to authorize the continuation of a project to the next phase in the project plan. Some status reviews are held at project milestones and are referred to as "milestone reviews". Some milestone reviews also include a decision on whether, or not the project can proceed and may be referred to as "gate reviews". In some cases a stage payment is dependent on the result of the status review.

A status review of dependability starts with a phase where information and evidence related to dependability are collected and structured. The structured information is then presented to management for review and decisions.

The team for a status review should include people that have the authority to devote resources to the project and remove obstacles. The participants in the technical part of the status review are typically the chair, the secretary, the project leaders and the team leaders for the different project teams. Once consensus on the status of the technical problems has been reached, the status review can proceed to the management phase, where usually the programme manager, the management and, possibly, the customer participate. Care should be taken so that serious problems reported by the team leaders in the project review are not presented as tasks for the next project phase without reporting their potential impact if left unsolved.