IEC 60300-1

Edition 4.0 2024-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Dependability management – Part 1: Managing dependability

Gestion de la sûreté de fonctionnement – Partie 1: Gérer la sureté de fonctionnement

IEC 60300-1:2024-06(en-fr)

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

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

IEC 60300-1

Edition 4.0 2024-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Dependability management – Part 1: Managing dependability

Gestion de la sûreté de fonctionnement – Partie 1: Gérer la sureté de fonctionnement

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 03.100.40, 03.120.01, 21.020

ISBN 978-2-8322-8320-2

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

DEPENDABILITY MANAGEMENT –

Part 1: Managing 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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 60300-1 has been prepared by IEC technical committee 56: Dependability. It is an International Standard.

This fourth edition cancels and replaces the third edition published in 2014. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) more guidance on integration of dependability activities into an existing management system;
b) greater detail on the activities required to establish and implement a programme of dependability activities;
c) changes to provide consistency with other dependability standards.

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

Draft	Report on voting
56/2031/FDIS	56/2044/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all parts in the IEC 60300 series, published under the general title *Dependability management*, can be found on the IEC website.

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

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The "colour inside" logo on the cover page of this document 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. A dependable item is one where there is justified confidence that it operates as desired and satisfies agreed stakeholder needs and expectations. Dependability has many attributes but is usually characterised in terms of reliability, maintainability and supportability, and the resulting availability. In some cases, attributes such as resilience, recoverability, durability, integrity, safety, security, and trustworthiness are included in, or overlap with, dependability.

The specification and verification of dependability attributes provide stakeholders with assurance that requirements will be met into the future and quality will be maintained over time. The dependability of a system, product or service influences the business strategies associated with its design, acquisition and use, and costs over its life cycle. The dependability of an organization's systems, products and services has a strong impact on the perception of the value and trustworthiness of the organization.

Dependability is managed as a key element of an organization's wider management system, particularly aspects relating to assets, quality and finance.

This document highlights the importance and benefits of managing dependability. It gives guidance on dependability activities and their integration into an existing management system and life cycle processes so that an efficient, effective and economical approach is achieved.

Dependability activities bring benefits whenever they are performed but greater benefit is achieved the sooner in the life cycle they are implemented.

This document is applicable to a broad range of industry sectors and organizations of any size. It applies to systems of systems, large unique systems, mass produced industrial and consumer products, software applications, components and services. These categories are not mutually exclusive. For example, many products and components are in themselves complex systems.

The document will be useful for:

- managers and technical personnel;
- those involved in deciding how their systems, products and services can be made dependable;
- organizations such as regulators who evaluate the dependability of systems, products and services;
- those (e.g. users or the public) who need justified confidence in systems, product and services that might affect them;
- developers of other dependability related standards.

This document is one of a suite of "top level" interrelated IEC dependability standards that provide managers and technical personnel with guidance on how to effectively plan and implement dependability activities. Other documents in the suite are:

– IEC 60300-3-4 which provides guidance on writing dependability requirements in specifications, and on the means of assuring the achievement of those requirements;

– IEC 60300-3-10 and IEC 60300-3-14 which provide guidance on how to identify and apply appropriate analysis and assurance techniques for maintainability (and maintenance) and supportability (and support) respectively;

– standards to cover reliability and availability, which are planned.

DEPENDABILITY MANAGEMENT –

Part 1: Managing dependability

1 Scope

This document provides guidance on:

- the meaning and significance of dependability from a business, technical and financial perspective;
- achieving dependability through suitable adaptation of organizational management systems such as those described in ISO 9001 (quality management) and ISO 55001 (asset management);
- the activities that are integrated into management systems and life cycle processes in order to achieve dependable systems, products and services;
- planning and implementing dependability activities throughout the life cycle to achieve and assure required outcomes, taking into account factors such as costs, safety, the environment, customer goodwill, brand and reputation.

This document is applicable to any type of system, both new and existing, to mass produced industrial or consumer products, to components and to services. This document addresses all elements of systems, products and services including hardware, software, data, processes, procedures, facilities, materials, and personnel required for operations and support.

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 60050-192:2015, *International Electrotechnical Vocabulary (IEV) – Part 192: Dependability* (available at www.electropedia.org)

3 Terms, definitions, and abbreviated terms

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 Terms and definitions

3.1.1
accountability
state of being answerable for decisions and activities to the organization's governing bodies, legal authorities and, more broadly, its stakeholders and society in general

Note 1 to entry: Accountability involves an obligation on management, the organization and individuals to be answerable for the impact of their decisions and activities on stakeholders, society and the environment. Accountability thus implies answerability to those affected and to society in general.

Note 2 to entry: Accountability implies that individuals, organizations and the community are responsible for their actions and can be required to justify them to others.

[SOURCE: ISO 26000:2010, 2.1, modified – "and society in general" has been added to the definition and notes to entry have been added.]

3.1.2
adaptability
ability to adjust to changed conditions or to be modified for a particular purpose or for a changed environment

3.1.3
assurance
grounds for justified confidence that a claim has been or will be achieved

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.1.1]

3.1.4
availability
ability to be in a state to perform as required under given conditions

Note 1 to entry: Availability depends upon the combined attributes of the reliability, maintainability, supportability and on the maintenance and support provided.

Note 2 to entry: Availability can also be affected by delays before it is recognised that maintenance or support are needed, for example fault detection time (192-06-18) and administrative delay (192-07-12).

Note 3 to entry: Given conditions include aspects that affect availability such as mode of operation, stress levels, environmental conditions and maintenance defined in the life profile.

Note 4 to entry: Availability may be quantified using measures defined in IEC 60050-192:2015, 192-08, *Availability related measures*.

[SOURCE: IEC 60050-192:2015, 192-01-23, modified – in the definition "of an item" has been deleted, "under given conditions" has been added, Note 1 to entry has been modified, and Notes 2 and 3 to entry have been added.]

3.1.5
business process
partially ordered set of inter-related enterprise activities that can be executed to achieve some desired end-result in pursuit of a given objective of an organization

Note 1 to entry: Business is interpreted broadly to mean those activities that are core to the purposes of the organization's existence whether the organization is public, private, for profit or not for profit.

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.445, modified – Note 1 to entry has been added.]

3.1.6
dependability
ability to perform as and when required

Note 1 to entry: A dependable item or service is one where there is justified confidence that it operates as desired and satisfies agreed stakeholder expectations.

Note 2 to entry: In most cases, the term dependability is used as an umbrella term to express its core attributes of reliability, maintainability, and supportability and the resulting availability. In some cases, attributes such as resilience, recoverability, durability, integrity, safety, security and trustworthiness are included in or overlap with dependability.

Note 3 to entry: In order to express the ability to perform, requirements in terms of functions to be performed, when the performance is to be achieved, and the life profile conditions, are specified by the customers, users or stakeholders.

Note 4 to entry: The attributes of dependability can be expressed qualitatively or quantitatively.

Note 5 to entry: It is also a common practice to use the term dependability in the context of a subject of study or discipline.

[SOURCE: IEC 60050-192:2015, 192-01-22, modified – "of an item" has been deleted, the notes have been deleted and new notes to entry have been added.]

3.1.7
dependability activity
set of cohesive tasks carried out to achieve a dependability related purpose

Note 1 to entry: A dependability activity can be mapped to a process view that uses a combination of life cycle processes, activities and tasks as defined in ISO/IEC/IEEE 15288.

3.1.8
dependability case
evidence-based, reasoned, traceable argument created to support the contention that a defined system does and/or will satisfy the dependability requirements

Note 1 to entry: A dependability case is an assurance case for dependability-related claims, see ISO/IEC/IEEE 15026-2.

[SOURCE: IEC 62741:2015, 3.1.1, modified – Note 1 to entry has been added.]

3.1.9
dependability plan
information item that presents a systematic course of action for achieving a declared purpose related to dependability including when, how and by whom specific tasks are to be performed

3.1.10
durability
ability to perform as required, under defined conditions of use and maintenance until a defined end state is reached

Note 1 to entry: The degree to which maintenance and repair are within the scope of durability will vary by product or product group.

Note 2 to entry: The end state can be based on technological, social or economic aspects.

Note 3 to entry: Durability can be expressed in units appropriate to the part or product concerned, e.g. calendar time, operating cycles, distance run, etc. or the probability of being able to achieve a given period of usage. The units should always be clearly stated.

Note 4 to entry: Durability as a measure relates to the longevity of the interval.

[SOURCE: IEC 60050-192:2015, 192-01-21, modified – "end of useful life" has been replaced with "defined end state", and notes to entry have been added.]

3.1.11
integrity
<in dependability> ability to prevent or withstand unauthorised modification

Note 1 to entry: Modification can involve hardware, software or data.

3.1.12
life profile
stresses and their levels, content, duration and sequence encountered during the life of an item

Note 1 to entry: Stresses can be internal (such as operating cycles) or external (such as environmental stress, input power level, or rate of service requests over a network).

Note 2 to entry: Life profile can be actual, expected or predicted.

3.1.13
maintainability
ability to be retained in, or restored to a state to perform as required, under given conditions

Note 1 to entry: Given conditions include location for maintenance, accessibility, maintenance procedures and maintenance resources as well as conditions defined in the life profile.

Note 2 to entry: Maintainability can be quantified using appropriate measures. See IEC 60050-192:2015, 192-07, *Maintainability and maintenance support measures*.

3.1.14
measurement
process of experimentally obtaining one or more values that can reasonably be attributed to a quantity

Note 1 to entry: Measurement does not apply to nominal properties.

Note 2 to entry: Measurement implies comparison of quantities, including counting of entities.

Note 3 to entry: Measurement presupposes a description of the quantity commensurate with the intended use of a measurement result, a measurement procedure, and a calibrated measuring system operating according to the specified measurement procedure, including the measurement conditions.

Note 4 to entry: The French word "mesure" has several meanings in everyday French language. It is for this reason that the French word "mesurage" has been introduced to describe the act of measurement. Nevertheless, the French word "mesure" occurs many times in forming terms, following current usage, and without ambiguity. Examples are: unité de mesure (unit of measurement), méthode de mesure (measurement method), instrument de mesure (measurement instrument). This does not mean that the use of the French word "mesurage" in place of "mesure" in such terms is not permissible when advantageous.

[SOURCE: ISO/IEC GUIDE 99:2007, 2.1, modified – Note 4 to entry has been added.]

3.1.15
need
prerequisite identified as necessary, to achieve an intended outcome, implied or stated, within a specific context of use

3.1.16
reliability
ability to perform as required, without failure, for a given interval under given conditions

Note 1 to entry: The interval can be expressed in units appropriate to the item concerned, for example calendar time, operating cycles, distance run, etc., and the units should always be clearly stated.

Note 2 to entry: Given conditions include aspects that affect reliability such as: mode of operation, stress levels, environmental conditions and maintenance.

Note 3 to entry: Reliability can be quantified using measures defined in IEC 60050-192:2015, 192-05, *Reliability related concepts: measures*.

[SOURCE: IEC 60050-192:2015, 192-01-24, modified – in the definition "of an item" and "time" have been deleted.]

3.1.17
requirement
<in dependability> statement which translates or expresses a need and its associated constraints and conditions

Note 1 to entry: Requirements exist at different levels in the system structure.

Note 2 to entry: A requirement is an expression of one or more particular needs in a very specific, precise and unambiguous manner.

Note 3 to entry: A requirement always relates to a system, software or service, or other item of interest.

Note 4 to entry: A requirement is a statement where evidence or assurance of compliance can be provided.

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.19, modified – Note 4 to entry has been added.]

3.1.18
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive or negative or both and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

[SOURCE: ISO 31000:2018, 3.1]

3.1.19
safety
freedom from unacceptable risk of physical injury or damage to the health of people or damage to property or the environment

3.1.20
security
protection against intentional subversion or forced failure

3.1.21
specification
<in dependability> information item that identifies the dependability requirements and goals of a system, product or service together with any supporting information

Note 1 to entry: Supporting information can include details of use, operating and environmental conditions, failure criteria and methods intended to be applied for assurance of compliance with requirements, including accept or reject criteria.

Note 2 to entry: ISO/IEC/IEEE 15289 defines a specification as an information item that identifies in a complete, precise and verifiable manner the requirements, design, behaviour or other expected characteristics of the system, service or process. The specification of dependability has a greater scope than that used in ISO/IEC/IEEE 15289.

3.1.22
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

EXAMPLE: End users, end user organizations, supporters, developers, producers, trainers, maintainers, disposers, acquirers, supplier organizations and regulatory bodies.

Note 1 to entry: Some stakeholders can have conflicting interests.

[SOURCE: ISO Guide 73:2009, 3.2.1.1, modified – example added and Note 1 to entry reworded.]

3.1.23
support
<in dependability> provision of resources to enable an item to continue to function as required

Note 1 to entry: Examples of resources are human effort, training, tools, jigs, test equipment, lifting equipment, materials, spare parts, facilities, documentation, information and information systems.

Note 2 to entry: Support is concerned with providing a quality resource to the correct location at the best time for the optimum cost, taking into account environmental, social and economic impacts.

3.1.24
supportability
ability of an item to be supported to perform as required with a defined life profile and given resources

3.1.25
system
combination of interacting parts that collectively has one or more purposes

Note 1 to entry: A system is sometimes considered as a product or as the service it provides.

Note 2 to entry: Parts can include the associated equipment, facilities, material, computer programs, firmware, technical documentation, other systems, services and personnel required.

3.1.26
usability
extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

[SOURCE: ISO 9241-210:2019, 3.13, modified – notes to entry omitted.]

3.1.27
useful life
interval from defined first use of an item until a defined end state is reached due to performance obsolescence or other factors

Note 1 to entry: The first use has to be defined. In this context, "first use" excludes testing activities prior to hand-over of the item to the end-user. The "first use" can commence after an initial period of early mortality.

Note 2 to entry: The end state has to be defined and can include safety margins that prevent the onset of failure or percentages of accumulated failures.

Note 3 to entry: The applicable interval is expressed in units appropriate to the item concerned, for example calendar time, operating cycles, distance run, etc. The units should be clearly stated.

Note 4 to entry: In some cases, the useful life of an item is more than that required by an organization in which case it will have residual value and could be repurposed.

3.2 Abbreviated terms

AI	Artificial intelligence
ASIL	Automotive safety integrity level
CMM	Capability maturity model
DRACAS	Data reporting, analysis and corrective action system
FMEA	Failure modes and effects analysis
FRACAS	Failure reporting, analysis, and corrective action system
HAZOP	Hazard and operability
IAS	International accounting standards
IFRS	International financial reporting standards
IOT	Internet of things
SIL	Safety integrity level

4 Key concepts and application of this document

4.1 Overview

Dependability is the ability to perform as and when required. The term applies equally well to items, products, processes and services, as well as to systems ranging from a simple component to a system of systems. A dependable system, product or service provides the user with assurance that requirements will be met into the future and quality maintained over time.

Clause 4 explains the concept of dependability and the attributes of systems, products and services that fall under the umbrella of dependability. The principles of dependability management and the benefits of devoting effort to it are described. The relationship between an organization's management system and dependability is discussed. The concept of a technical programme of dependability activities which is carried out through the life cycle is introduced.

4.2 Principles of dependability management

Dependability management encompasses a number of principles as follows.

- Holistic approach: Managing dependability integrates considerations of performance, cost, risk and compliance across the entire life of a system, product or service. It does so by taking a systems approach with continual optimization over the life.

- Assurance and accountability: Managing dependability establishes the grounds for justified confidence that claims relating to dependability have been, or will be, achieved. This satisfies the assurance and accountability requirements of the organization's management framework, which in turn fulfils the needs and expectations of stakeholders for assurance and accountability.
- Risk based: Managing dependability involves identifying factors that could cause systems, products and services, and the systems that support them, to fail or deviate from requirements. These risks represent a potential cost throughout the life of a system, product or service. Improving dependability represents an initial cost to the designer or manufacturer, but can result in a saving when considered across the life of the product. Deciding how much to invest to improve dependability at all stages of the life cycle is directly related to risk and value, and the amount of risk that the organization is willing to accept.
- Adaptability: Dependability activities and the systems to manage them need to be sufficiently flexible to be able to respond to changes in needs and context in a timely way. Adaptability can also be a desirable attribute of a system, product or service which can improve its maintainability and supportability and extend its useful life.
- Sustainability: For a system, product or service to meet the needs and expectations of stakeholders, economic, social and environmental issues need to be considered as well as technical excellence. For example as well as seeking to achieve a reliable, maintainable and supportable system, product or service, a dependable design should also aim to reduce energy consumption and environmental impacts and consider including re-usable components. A system, product or service that is reliable, maintainable and supportable is likely to have a longer life, use fewer resources, and produce less waste than one which does not have these attributes.
- Balance: Dependability is managed to achieve an appropriate balance of cost, risk and performance over the life of the system, product or service. A trade-off can also be required with requirements such as safety and security that can sometimes conflict with dependability, and with constraints such as contractual and legal requirements.

4.3 Benefits of managing dependability

Managing dependability is essential to managing the value that organizations or individuals derive from their assets. This value is often defined in terms of performance, cost and compliance as well as less tangible, but equally important elements such as brand, reputation, customer goodwill and trust.

Managing dependability provides benefit to an organization by:

- providing justified confidence that systems, products and services will provide value by performing as and when required;
- optimising life cycle costs and demonstrating affordable levels of dependability performance;
- achieving compliance with regulatory requirements or mandated standards;
- managing the risks of failure or degraded performance to achieve a balance of cost, risk and performance;
- providing transparency of decision making;
- underpinning the development of management systems, for example asset management systems and quality management systems, and providing objective evidence of the achievement of their intended outcomes. (Outcomes can include financial, safety, environmental and security outcomes as well as technical performance outcomes);
- improving design;
- optimising maintenance and support needs;
- reducing the need for unplanned maintenance activities that could expose staff to potential hazards;

- enabling informed decisions in a changing operational environment (including changes in requirements themselves);
- providing input to the design, implementation and ongoing improvement of maintenance and support;
- providing information so that mistakes of the past are not repeated, lessons are learnt and successes are built upon;
- improving an organization's resilience to adverse events and circumstances.

4.4 Attributes of dependability

The dependability of a system, product or service is specified and verified using a set of attributes. Where practicable these are quantified to facilitate providing assurance that requirements are met, and to unambiguously demonstrate improvements. Dependability has many attributes but is usually characterized in terms of reliability, maintainability, supportability and availability.

Reliability relates to the ability to provide a required function without failure for a given interval (time, operating cycles, distance, etc.). Reliability can be quantified as a probability of success (e.g. the probability of an item performing its intended function for a specified time period) or expressed through related measures, for example the failure rate. To specify reliability unambiguously it is necessary to define a point at which any particular function is said to have failed.

Maintainability relates to the ease and speed with which an item can be retained in, or restored to, a state to perform as required. It can be quantified as the probability that a given maintenance action, performed under stated conditions, can be completed in a specified time. "Retained in" refers to maintenance whilst a system is in an operational state (such as on-line maintenance or repairs to redundant components). "Restored to" refers to maintenance whilst the system is in a non-operational state such as planned down time servicing. Software differs from hardware in that it does not wear out and faults originate in the specification, design logic or coding process and can lie hidden until specific input conditions occur. Maintainability of software relates to the ease and speed with which software can be modified to change or add capabilities, to correct faults or defects, improve performance, or to adapt it to a different environment.

Supportability is concerned with identifying and quantifying:

- the support required for a defined item in a given context of use;
- the time to provide that support;
- the resourcing, cost and quality of that support;
- the quality of the delivered support.

Specifically, supportability is concerned with what is required for an item to continue to function as well as how to implement this requirement. The "what is required" element is inherent within the item design, but the way in which it is implemented is determined by the organization conducting the support.

Availability is the ability to be in a state to perform when called upon to do so. It is often quantified as the ratio of up time to total time. As reliability, maintainability and supportability are major contributors of up time and down time, availability is impacted by the trade-offs between these attributes.

EXAMPLE: A reliable item does not fail very often, an available item works when it is needed and a dependable item, as well as being available, performs correctly over time and is easy to maintain and support.

Factors such as cost, resources, the time available for dependability activities, and usage conditions influence the level of reliability, maintainability and supportability that can be achieved in practice.

Measures of reliability, maintainability, supportability and availability are discussed in IEC 62308, IEC 60300-3-10, IEC 60300-3-14 and IEC 61070 respectively. IEC 61703 explains the mathematical meaning of a range of dependability related measures and how they are established.

Measures of reliability, maintainability, supportability and availability are stochastic or statistical quantities, i.e. sufficient data need to be available to provide statistical validity (see IEC 60300-3-2 and IEC 60605-6). Verifying high reliability, or providing a high level of confidence for a dependability measure, requires a large number of tests which will not always be practicable, time feasible or cost effective to perform. The expected reliability in these circumstances can however be verified using results of reliability models (see IEC 60300-3-1).

Other attributes that can fall under the umbrella of dependability include the following.

- Durability, which is the ability to perform as required, under defined conditions of use, maintenance and repair until a defined end state is reached. It relates to the ability to continue to restore a system or product to a functioning condition until it is no longer needed.
- Recoverability, which is the ability to recover from failure without corrective maintenance (for example automatic re-initialization after software failure detection).
- Fault tolerance, which is the ability to continue functioning with certain faults present.
- Usability, which is the ability of a system, product or service to be used effectively and efficiently. Usability affects the performance of operators and maintainers and hence has an influence on the overall reliability and maintainability of an item. It includes for example learnability, operability, and prevention and protection mechanisms against errors. See IEC 62508.
- Testability, which is a design characteristic that determines the degree to which a system, product or service can be tested to determine one or more characteristics under stated conditions. Testability is discussed in IEC 60706-5.
- Operability, which is the ability of a system, product or service to operate safely and reliably to provide an intended result or function.
- Robustness, which is the ability of a system, product or service to function correctly in the presence of stressful inputs or environmental conditions.
- Resilience, which is the ability to adapt to change and return to functional capability within an acceptable time period after having been affected by stressful inputs or environmental conditions.
- Integrity, which is the ability to prevent or withstand unauthorized modification. This includes both non-malicious alteration (e.g. unexpected wear of hardware or the uncoordinated automatic update of software) and malicious or unauthorized alteration (e.g. malware infection or counterfeit components). For hardware, integrity refers to the ability of a system to sustain its form stability and robustness. For software and data the focus is on accuracy, completeness and security.

Often these attributes will affect reliability, maintainability and supportability and can be included in the measurement of those attributes. Guidance for writing dependability requirements in specifications, together with a means of assuring them, is provided by IEC 60300-3-4. Methods for specifying requirements and evaluating performance for some other quality attributes that can affect dependability more indirectly, such as learnability, error tolerance and error protection, are given in ISO/IEC 25023.

Safety, security and trustworthiness can overlap with dependability. Safety functions are required to be dependable to prevent harm to people, property and the environment. In some situations, a failure can lead to an unsafe situation, therefore improved reliability can enhance safety. In other cases safety requirements can result in increased maintenance and hence decrease availability. Dependable items require less maintenance and therefore avoid exposing staff to potential hazards during repair operations.

Security requires a system, product, or service to be available only to those authorized to use it (a combination of the attributes of availability and integrity) with the added requirement of confidentiality (absence of unauthorized disclosure). See Figure 1 (the lines with arrows in the figure indicate the attributes of dependability and of security.)

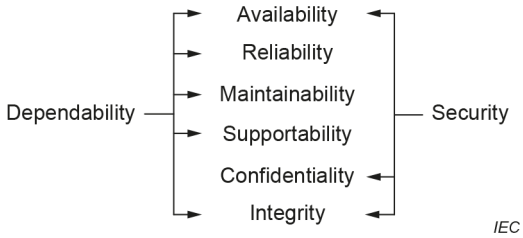


Figure 1 – Dependability and security attributes

Security and dependability are linked. Security can sometimes reduce dependability. For example access restriction to a system can reduce its maintainability. Poor dependability can also adversely affect security. For example poor maintainability of software can lead to a security breach. Trustworthiness is a concept that is applied in software intensive systems such as artificial intelligence (AI) and the internet of things (IOT). It is defined as the ability to meet stakeholders' expectations in a verifiable way. Trustworthiness characteristics include reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality, usability and accuracy (see e.g. ISO/IEC 30145-2).

It can be difficult to define quantitative measures for dependability attributes of AI and related technologies. The user's perception of a failure depends on their expectations of the system. The behaviour of the system changes as a result of interactions with the user so experiences differ from user to user. This means that failure to perform as required depends on the user's expertise, goals, mental models, and past experience in using the product as well as on the design of the algorithms and the data on which they are based. However qualitative analyses are still possible.

In general users, providers, operators, maintainers and others who interact with a system can have overlapping dependability requirements but with different objectives and usage expectations. This can result in differing needs and differing perceptions of dependability. A user perspective of overall dependability can in some circumstances be obtained using qualitative statements or an ordinal rating scale.

For an open system, such as a system of systems or a large system that operates for an extended period in a real world environment, the attributes of dependability have to be considered in the context where no single stakeholder has a full understanding of the system or its risks. Achieving and assuring dependability in this case relies on building consensus between stakeholders, achieving accountability and accommodating change. Since identifying and controlling risks is more difficult, it is particularly important that the system is able to respond effectively to failure. IEC 62853 provides guidance on dependability of open systems.

4.5 Relationship between an organization's management system and dependability

An organization's management system provides and documents the infrastructure needed to achieve the value and outcomes that are to be delivered. Within this management system, processes, activities and tasks are developed, documented and implemented to achieve specific objectives. ISO standards such as ISO 9001 and ISO 55001 describe the requirements of an organization's management system. Technical and financial standards provided by IEC, IFRS and IAS provide detailed guidance on the processes, activities and tasks. IEC TS 62775 shows how the IEC dependability suite of standards, systems engineering and the IFRS and IAS standards can support the requirements of asset management, as described by the ISO 5500x suite of standards.

Figure 2 shows the relationship between management system standards and dependability standards. Annex A lists dependability related standards from IEC.

The dependability of equipment, people, processes and services is central to the organization's ability to achieve its objectives. Therefore dependability management should be integrated into the management system of the organization. Dependability management is not a separate endeavour to the business, and dependability objectives should align with the business objectives. Dependability attributes are interlinked with other aspects of performance and functionality; hence dependability should be considered in conjunction with other organizational drivers such as cost, schedule, performance, risk and profitability.

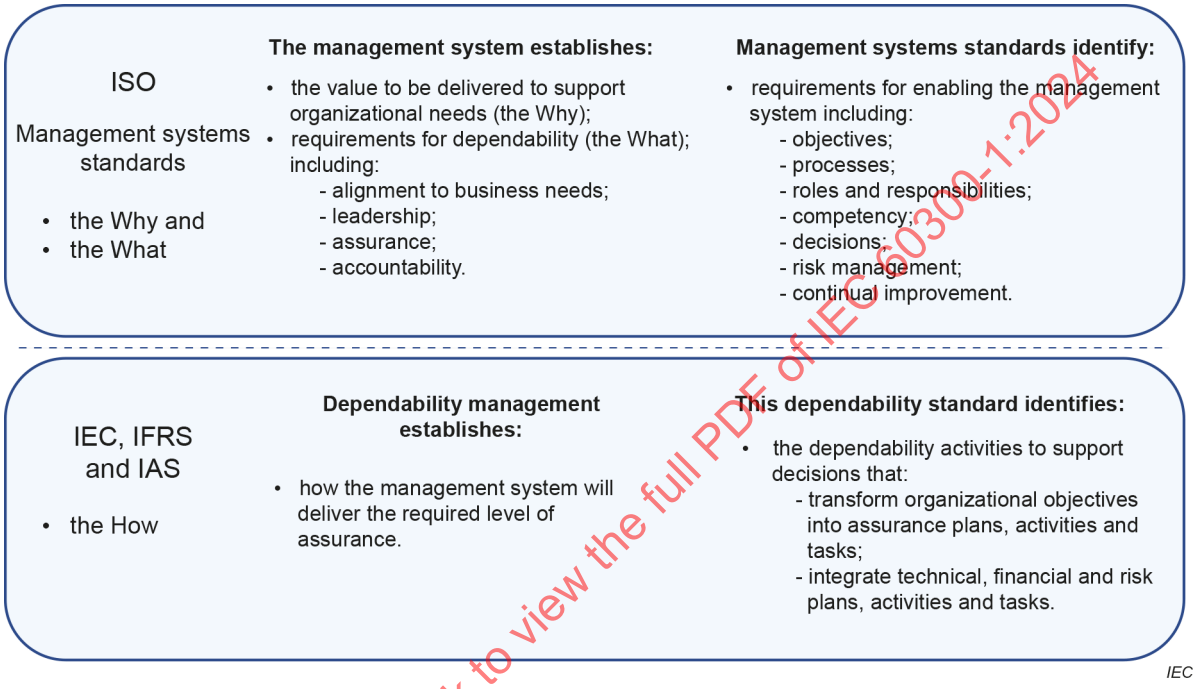


Figure 2 – Relationship between management system standards and dependability standards

Clause 5 describes how managing dependability can be incorporated into a management system that is assumed to conform to a management system standard with the harmonized structure of ISO/IEC Directives, Part 1, Consolidated ISO Supplement:2022, Annex SL.

4.6 Technical programmes for dependability

In order to achieve dependability objectives and targets and provide assurance that they have been, or will be, achieved, a customized set of coordinated dependability activities is carried out. Activities are broken down into individual tasks (and sometimes sub-tasks). These are usually documented in a plan which provides details of the objectives and the context and constraints. It identifies the tasks to be undertaken, the techniques, tools and resources required, responsibilities and accountabilities and how dependability activities and tasks will be integrated with other related activities.

NOTE A dependability activity can be a life cycle process, activity, task or process view as defined in ISO/IEC/IEEE 15288 (see Annex F).

Dependability activities can be organised as separate but closely coordinated programmes for reliability, maintainability, supportability, maintenance and support or a combination of these, or be fully integrated into other programmes. The arrangement chosen is determined by technical considerations and stakeholder needs and by the organization's business priorities and values. Programmes can be established on a project-by-project basis or can be organization wide, with flexibility to allow for variations between projects. Variables include the stakeholders of relevance, cost, schedule, quality trade-offs, the technical difficulty of the work and the knowledge and experience of the people involved.

Whatever organizational arrangements are put in place, dependability activities should be coordinated to achieve dependability objectives and integrated with related activities for the project as a whole. The customised selection of dependability activities and tasks for a particular context is sometimes referred to as a dependability programme. Clause 6 discusses the design of a programme of dependability activities.

4.7 Life cycle concept

A system or product, irrespective of its size and complexity, evolves from its initial conception through to its eventual retirement and disposal or re-use. It is generally useful to build a model of this progression to help manage the evolution of the system. Such models are termed life cycle models. A life cycle model is segmented by stages to facilitate planning, provisioning, operating and supporting the system or product of interest. Movement from one stage to another represents the major milestones where investment decisions and resource commitments can be made and incorporated into the management process.

NOTE The concept of a life cycle model, an abstract functional model of the actual life cycle of a system, is detailed in ISO/IEC/IEEE 24748-1.

Dependability activities bring benefits whenever they commence. However the greatest gains are achieved by starting them from the earliest stages of the life cycle because:

- incorporating stakeholders' needs and expectations for dependability from the start helps to maintain stakeholder satisfaction;
- it is cheaper and easier to design in reliability, availability, maintainability, and supportability and balance them from the earliest stages;
- rectifying problems relating to poor dependability once a system is in operation is often time consuming and costly. An investment in dependability during design activities in the early stages of the life cycle can repay itself in terms of the combined development, realization, utilization and retirement/re-use costs.

IEC 60300-3-3 describes life cycle costing and the relationships between dependability and cost.

There are many different formulations of the life cycle according to the nature, purpose, use and prevailing circumstances of the system or product. A simple generic life cycle model has the following stages:

– concept;
– development;
– realization (including manufacture, transport, acquisition and installation);
– utilization (including operation, maintenance, evolution and enhancement);
– retirement and re-use.

Some alternative life cycle models are described in Annex B.

It is possible that an organization will not have control of or interest in all stages or can require additional detail within a stage to account for the major decision points of relevance to them. For example, in some cases, where the operating stage is extensive, there are likely to be changes in context and usage and perhaps also in requirements. Managing change becomes particularly important. There will also inevitably be some failures and anomalies which will need to be investigated with results fed back to improve dependability. Changes, whether an evolution or significant enhancement, should be made in a controlled manner and the effects of design changes analysed for potential unwanted effects and interactions. Figure B.3 illustrates how change can be managed through the life cycle stages.

4.8 Dependability activity concept

A dependability activity is defined by its purpose, its outcomes and a list of tasks that together achieve the purpose and outcomes. Dependability activities can be considered in two groups:

- programme management activities;
- technical dependability activities.

Programme management activities are those needed to plan, implement, review and improve a set of technical activities that achieve dependability objectives and meet stakeholder needs.

The technical dependability activities described in this document are generic and likely to form some part of any programme. Each activity involves a number of tasks that are selected to achieve the purpose and outcomes of the dependability activity in the context concerned in a cost effective way. Clause 7 describes programme management activities and Clause 8 technical dependability activities.

NOTE In this document a dependability activity, and a task in a dependability activity do not have the same meaning as an activity and a task in ISO/IEC/IEEE 15288 (see 3.1.7). The relationship between the meaning in this document and that in ISO/IEC/IEEE 15288 is explained in Annex F.

5 Integrating dependability into an organization's management system

5.1 Overview

Clause 5 describes how dependability can be incorporated within the requirements of a management system that is assumed to conform to a management system standard that has the harmonized structure of ISO/IEC Directives, Part 1, Consolidated ISO Supplement:2022, Annex SL. Such standards include ISO 55001 (for asset management systems) and ISO 9001 (for quality management systems).

It is not intended that dependability management should be a separate management system. Figure 3 shows the elements of a management system and the dependability management aspects to be incorporated into it. The numbers in the arrows indicate the subclauses in this document where these dependability aspects are described.

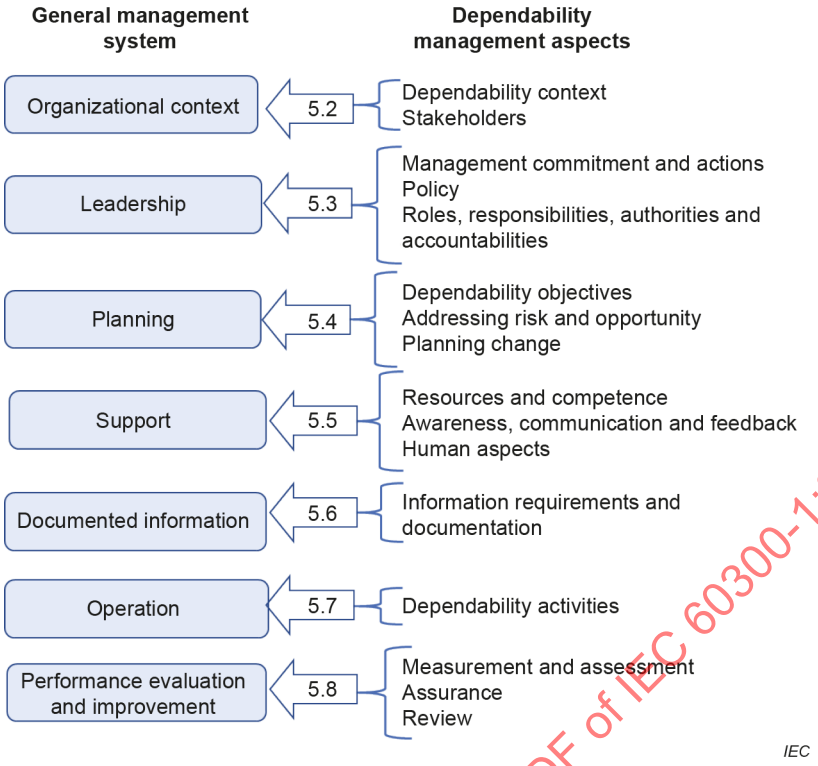


Figure 3 – Integration of dependability into a management system

5.2 Understanding the organization and its context

Organizational arrangements for managing dependability should take into account external and internal issues including the organization's objectives, threats, opportunities and risks.

Internal and external stakeholders with an interest in dependability should be identified and their needs and expectations determined (see Annex C). Stakeholders can change over time, therefore the organization should monitor, review and update information about stakeholders and their needs and expectations.

Dependability is affected by physical and psycho-social factors within the organization and by the performance of external organizations such as suppliers or service providers. Dependability requirements within the system of interest might be achieved, but if internal and external influences are not also understood and managed effectively stakeholder needs and expectations might not be met.

5.3 Leadership

Leaders should recognize the importance of dependability to achieving business objectives and demonstrate their commitment to dependability so that the importance of behaviours that promote dependability is transmitted clearly. They should communicate to external stakeholders the scope of management's accountability for dependability and their commitment to it, and should obtain external stakeholders' consent and confidence. High dependability can only be achieved where dependability is recognized as part of corporate strategy and accorded top management commitment and ongoing focus. Without this, dependability effort is liable to be compromised whenever time or cost pressures arise.

- Policy:

  Dependability should be referred to in an organization's policy statement. This helps to ensure that appropriate resources are provided, and that the work practices and actions of all staff achieve high quality and dependable outcomes. It also provides accountability to external stakeholders.

- Roles, responsibilities, authorities and accountabilities:

  Responsibilities, authorities and accountabilities for roles to manage dependability for different systems, products and services at relevant stages of the life cycle should be assigned. Often more than one organization is involved during the life of a system and some responsibilities and accountabilities need to be passed from one organization to another. Since organizational styles and procedures vary, the way dependability is managed needs to adapt to different situations. The results should be documented as agreements that clarify accountabilities for any failures.

  Roles, responsibilities and authorities can change with time. Clarity on accountabilities is also important in this case. In some business areas, such as medical equipment, aerospace and machines, regulatory rules specify strict requirements on accountability and independence.

5.4 Planning

- Defining dependability objectives and planning to achieve them:

  Dependability objectives that support the objectives of the organization should be defined, together with accountability for their achievement. Dependability objectives should be considered at organizational and project levels as well as at the level of the requirements of particular systems, products or services (see 7.2.3). Where more than one organization is involved, agreements on the objectives and plans should be recorded as the basis of dispute resolutions and for future improvement.

- Actions to address risks, threats and opportunities:

  When planning how to manage dependability, the organization should determine the threats, opportunities and risks that need to be addressed to give assurance that the dependability activities can achieve their intended outcomes. Subclause 7.2 describes planning a programme of dependability activities.

  Risks to the dependability of systems, products and services and to the effectiveness of dependability management activities should be identified and understood as part of the organization's risk management processes. Actions should be planned and implemented to address risks, threats and opportunities, taking into account how these can change with time (see 8.3). Managing risk starts from the earliest stages of a life cycle and continues through each stage. Information about risks should be passed from stage to stage and the understanding of risk refined as more information becomes available.

- Planning changes:

  Changes should be carried out in a planned manner, taking into account the potential impact on arrangements to manage dependability and on dependability outcomes. This includes considering how dependability will be affected by the availability of resources and the reallocation of responsibilities and authorities. The way dependability is managed needs to be adaptable so that dependability continues to be assured in the face of unplanned changes.

5.5 Support

- Resources and competence:

  The organization should provide the resources needed to achieve dependability objectives. Such resources include:

  – skilled and motivated personnel;
  – specialist expertise to carry out appropriate technical activities and analyses;
  – an information and knowledge management system;
  – infrastructure including equipment, buildings, hardware and software;
  – an appropriate social, psychological and physical environment so people can perform effectively;
  – resources to monitor and measure dependability;

– appropriate tools, including software tools and data, for analysis and simulation.

The resources necessary vary with the stage of the life cycle. For example, the development stage requires dependability design expertise and the realization stage can involve resources for detailed verification and testing.

NOTE Technical aspects of support are discussed in 8.6.

- Awareness, communication and feedback:

  Perceptions of dependability can vary depending on the stakeholder and over time. Effective communication and consultation with relevant stakeholders should therefore be maintained over time. Information should be provided in a way that is unambiguous, complete, comprehensible, verifiable, consistent, and traceable. The quality of dependability communication and feedback affects customer confidence, trust, satisfaction and loyalty, and regulators' approval as well as the quality of customer care service.

  Effective communication improves accuracy in incident reporting and data capture. This facilitates the choice of appropriate corrective and preventive actions.

  Relevant feedback can help establish performance trends, identify critical areas requiring attention and provide objective evidence for verification, validation and improvement. A dependability case (see IEC 62741) can be a valuable medium of dependability communication and stakeholder feedback. Stakeholder engagement is discussed in 8.2.

- Human aspects:

  People at all levels have a significant role to play in achieving dependability. Specific organizational factors that influence dependability performance include support for decision making and problem solving, communication, supervision, proceduralization and role clarity. Staff should be trained, motivated and given the appropriate resources to be able to perform their work dependably (see IEC 62508). The organization has the ability to support or impede the processes and behaviours that promote dependability. Therefore any approach to dependability should include a means for identifying and improving critical human factors.

5.6 Documented information

The organization should determine the information needed to manage dependability. The data collected should include those necessary to:

- provide confidence that processes have been carried out as intended;
- communicate with stakeholders;
- verify that dependability requirements are or will be met;
- validate that outcomes satisfy stakeholder needs and expectations;
- evaluate and improve dependability activities and their outcomes;
- provide a basis for accountability;
- improve the way dependability is managed.

If a clear purpose for data is not evident then the need to collect it should be questioned.

Examples of information and data relevant to dependability include:

– explicit agreements and accountabilities;
– dependability data from tests and in the field;
– results from dependability analyses;
– configuration control documents;
– information from or for acquirers and suppliers;
– data from DRACAS and FRACAS. Whether a data recording systems is referred to as DRACAS or FRACAS, both failures and successful periods of operation need to be recorded in order to quantify dependability and its contributory elements.

Ownership of dependability data should be defined and a means by which necessary information is communicated through the supply chain put in place. This can be the subject of explicit agreements. Dependability related data should be adequately protected (e.g. from loss of confidentiality, improper use or loss of integrity). A means to control dependability data and information and ensure that it is kept updated and is available when needed should be established as part of the organization's documented information systems. Data collection and interpretation are discussed in 8.5.

ISO/IEC/IEEE 15289 describes the purpose and content of information items that might be relevant.

5.7 Operation

The organization should implement and control dependability activities as outlined in Clause 7 and Clause 8 in order to achieve its desired outcomes.

5.8 Performance evaluation and improvement

The organization should plan and implement processes to monitor, measure, analyse and improve the effectiveness and efficiency of the way it manages dependability. This can be assisted by use of a dependability case (see IEC 62741).

Performance indicators and targets should be defined and performance assessed against them. This could involve:

- evaluating whether the organization's dependability policies and objectives are being met;
- reviewing the suitability of dependability policies and objectives;
- evaluating the dependability of systems, products and services against requirements;
- evaluating the efficiency of operation and effectiveness of dependability activities;
- assessing outcome measures such as customer satisfaction.

One method for self-assessment and improvement is through the use of a maturity matrix. A dependability maturity matrix is a checklist of desired characteristics of dependability management with various levels of achievement defined. It is used to assess current effectiveness and indicate what capabilities are needed next in order to improve performance. An example of dependability maturity matrix is provided in Annex D. Maturity models (also referred to as capability maturity models (CMMs)) can also be used by organizations to assess their software processes. CMM provides a benchmark against which to compare the software development processes that can be used as a predictor of product quality and to drive improvement.

Where possible, existing performance monitoring systems should be used to generate the information needed to improve dependability activities and outcomes. Examples of such systems include:

– DRACAS and FRACAS (see 8.6.3);
– a customer care and feedback system;
– a spares provisioning system;
– a maintenance and support system;
– a condition monitoring system;
– a quality control system.

Dependability aspects of the management system should be included in internal and external audits of the organization's management system and in management reviews.

The organization should identify and exploit opportunities for continual improvement and implement necessary actions to meet customer requirements and enhance stakeholder satisfaction.

6 Programme design

6.1 General

A coordinated set of dependability activities should be undertaken to meet the organization's objectives for dependability and stakeholder's needs. It should be customised to the organization and to the systems, products and services of interest. Clause 6 describes considerations for designing such a programme including coordination and integration with other activities, trade-offs and key success factors. Clause 7 describes how to plan, implement, review and improve a programme that is tailored to circumstances. Clause 8 describes technical dependability activities and tasks that can be included in the programme.

A plan should be developed for implementing the programme, with accountabilities, authorities and timelines defined (see 7.2). Human and organizational factors required to support the plan should be identified and incorporated into the programme. The people involved in implementing the plan at any stage in the life cycle should be aware of their responsibilities and accountabilities, and be adequately supported and competent.

6.2 Coordination and integration

Dependability can be managed as a separate programme by a dedicated organizational unit, be fully integrated into relevant areas, such as product development or manufacturing, or be a mixture of the two approaches. In some organizations the responsibility for dependability (like quality) rests with a separate department. (This is required for companies that approve their own products, for example for the European CE-marking system). For a large organization it can be worthwhile to set up a cross-departmental entity to serve the overall needs of the organization in an efficient manner. This helps eliminate duplication of effort and ensure consistency of dependability activities while enabling the highest level of expertise to be applied. In all cases the alignment of organizational structures, responsibilities, accountabilities, activities, resources and information is critical for efficient management.

It is generally more efficient to integrate dependability activities and tasks with those relating, for example, to scheduling, design, production, and operations and to develop an overall project plan. Coordination and integration are also important because it can be necessary to trade-off dependability against other stakeholder needs or organizational objectives.

Risks identified as part of the development of a dependability case or through the use of tools such as FMEA (see IEC 60812) should be integrated into the overall project risk management process. This provides better awareness of risks across a project, encourages a common view of the acceptability of risks and enables more efficient treatment strategies. Guidelines for managing risk in any context are provided by ISO 31000. IEC 31010 describes risk assessment techniques and how they are used and IEC 62198 provides guidance on managing risk in projects.

Coordination between different dependability activities within the same project, as well as between different projects, should be actively managed so that resources are used effectively. For example reliability, maintainability and supportability activities could use the same analysis tools and data sets (if for different purposes). Responsibility, authority and accountability for coordination should be assigned.

6.3 Trade-offs

A trade-off is a decision where one feature is diminished in return for gains in another. In dependability this can be because of limitations in resources or in the design. Trade-offs are made by considering the advantages and disadvantages of the characteristics being traded in the context concerned. Priorities that drive decisions about trade-offs and hence programme design should be agreed with relevant stakeholders.

Types of trade-off relevant to managing dependability include the following:

- Within a specific dependability attribute: For example, a high reliability can be achieved by designing a highly reliable item or by incorporating redundancy. Similarly, maintenance down time can be reduced by conducting preventive maintenance during operation or during a scheduled shut down.
- Between dependability attributes: For example the choice can be made between low reliability items that are cheap initially but are expensive to maintain, and high reliability items that can be expensive to design and construct but require little maintenance. Decisions relating to maintainability and maintenance influence the type of support (such as spare parts and maintenance skills) which affects supportability. The attributes of components can be combined in different ways to deliver the same overall availability.
- Between dependability and other criteria such as safety or performance: For example, the inclusion of safety features and safety systems can make an item so complex to use that its dependability is reduced. Other functional and non-functional requirements such as form, fit and function compatibility can also impact dependability.
- Between the effort put into the dependability programme (hence its costs and schedule), and the value added by it (e.g. improved stakeholder satisfaction, brand value and the overall savings from improved dependability): For systems and products with a long life, operational costs, particularly the cost of maintenance, can dominate life cycle costs. Additional effort spent in design can therefore produce significant cost savings later. However improved dependability can have to be traded off against meeting the project's schedule and budget. Decisions depend on the level of risk the organization is prepared to accept.

The trade-offs that are made should be explicit and decisions documented.

6.4 Tailoring a technical programme of dependability activities

The purpose of tailoring is to design a programme of dependability activities and tasks that achieve the specific dependability objectives within applicable constraints in a cost effective way. Examples of tailoring include:

- budget planning for the allocation of dependability resources or outsourcing in order to meet project delivery time scales;
- determining the activities and tasks that will provide on-going confidence that the dependability requirements will be achieved;
- deciding on the best approach to performing a particular activity in the particular context.

Programme design depends on:

a) objectives, including any specified requirements (see 7.2.3);
b) the nature of the system, product or service concerned;
c) the relevant life cycle stages;
d) the time frame adopted by the organization;
e) the engineering approach.

EXAMPLE The engineering approach in the design stage would consider whether the design was for:

- a brand new item;
- an item based upon previous item designs;
- a system utilising the latest off-the-shelf technology;
- a transitional service such as manual to automated or electronic driven to software driven.

In some cases a statement of work from a customer, agreements with other stakeholders and internal policies define the tasks that need to be performed.

Other approaches include:

– reviewing an existing programme and its activities and tasks to see where improvements can be made and tailoring it to the particular circumstances;

– use of a dependability case where structured arguments are made and evidence is provided to support the claim that a system meets its dependability requirements. The activities and tasks needed to provide the evidence in support of the claim represent those activities and tasks required to achieve and assure dependability (see IEC 62741).

Where an organization has an existing dependability programme, criteria and guidelines can be developed for tailoring this to specific circumstances. This could involve a set of activities which apply in all cases and to which additions are made, or a set of activities from which those required in a particular case are selected.

6.5 Key success factors

Key factors that contribute to the success of the programme include:

- incorporation of dependability considerations into decision-making from an early stage;
- a common understanding of the system or product, its dependability needs and the means of achieving them;
- clearly defined and agreed responsibilities and accountabilities for meeting dependability requirements;
- effective coordination and integration among the various organizational entities that will be involved;
- an understanding of the factors that affect the dependability and costs of a particular system, product or service;
- an understanding of trade-offs that need to be made.
- provision of adequate resources (including competent personnel) for the dependability activities and tasks to be undertaken;
- incorporation of tasks that support, analyse and improve human performance;
- effective collection and use of information and data;
- customization to organizational, stakeholder and project needs.

7 Programme management activities

7.1 Overview

Clause 7 describes the activities required to establish a programme of technical dependability activities, namely:

a) planning the programme to achieve objectives within the applicable context and constraints;

b) implementing the plan;

c) reviewing and improving the programme and plan;

d) providing assurance that dependability objectives are achieved;

e) achieving accountability.

The overall management system and structures that support dependability activities are discussed in Clause 5.

7.2 Plan dependability activities

7.2.1 Purpose

The purpose of planning is to select and coordinate a set of dependability activities that achieve the organization's objectives for dependability in a cost effective way and to integrate these into related project plans and processes.

7.2.2 Outcomes

As a result of planning:

a) the organization's objectives for dependability are defined;
b) a clear approach for achieving those objectives is articulated;
c) technical dependability activities, tasks and tools are selected;
d) entry and exit criteria for each dependability activity are established;
e) responsibilities and accountabilities for performing dependability tasks are defined and assigned to appropriate roles;
f) information and resource requirements for tasks are defined;
g) a schedule for the programme is developed;
h) a dependability plan is developed including provisions for change of the programme;
i) the dependability plan is integrated into the other relevant plans.

7.2.3 Tasks

The following tasks should be undertaken in accordance with organizational policies.

a) Identify the programme objectives. These can include:
   - achieving dependability objectives or requirements for a system, product or service;
   - providing evidence that dependability objectives or requirements have been achieved;
   - satisfying legal or contractual requirements;
   - managing life cycle costs;
   - improving efficiency;
   - improving the capability of the organization to support human performance, including workers and product users, so that the full capability of the technical systems is achieved;
   - increasing stakeholder confidence;
   - improving support;
   - achieving specific targets or milestones;
   - satisfying safety and environmental requirements.
b) Define the programme context. This can include:
   - defining the boundaries (open or closed) of the system, product or service under consideration;

     EXAMPLE 1 A supplier of consumer goods to a general market might specify the dependability characteristics of the hardware and software which they are supplying, whereas a user might wish also to include human operators and external utilities.

EXAMPLE 2 A supplier of a bank teller terminal might set the boundary to include only hardware and software, and then specify their dependability characteristics. On the other hand, a bank customer might wish also to include human operators and connected server services in the boundary and to know the overall dependability characteristics.

- identifying stakeholders;
- defining the life cycle model relevant to the situation and determining the specific life cycle stages that are applicable;
- identifying relevant characteristics of the system, product or service to which the programme applies, such as its features, functions, novelty and complexity and application environment;
- identifying the outputs or evidence required by relevant stakeholders.

c) Identify programme constraints. These can include:

- the budget;
- available time and resources;
- technological capability;
- expertise available;
- other resource requirements (e.g. personnel, organizational policy and infrastructure);
- acceptable risk;
- management time and focus;
- legal and contractual requirements.

d) Identify risks to programme objectives.

e) Identify the evidence necessary to provide assurance that the objectives are achieved.

NOTE 1 Identifying necessary evidence, and planning to obtain it, starts as soon as objectives are identified. Assurance that objectives are being, or have been, achieved is provided on an on-going basis.

f) Identify the technical dependability activities required to achieve the programme objectives and the tasks and tools needed to achieve the required outcomes.

g) Prioritize the dependability activities, tasks and tools, considering the objectives, constraints, context and risks.

NOTE 2 Multiple tools can be required to provide a single outcome.

h) Determine the minimum depth and detail required from each tool selected in order to achieve the desired aims with the necessary confidence. This will assist in allocating resources and optimizing cost.

i) Compare the time, capability and resources required to complete each task to the necessary depth with the resources available.

j) Assess whether the planned dependability effort adds value and modify the programme if not. This can involve a cost benefit analysis of each activity taking into account the cost of failures, life cycle costs of ownership and the costs of dependability activities.

k) Make decisions about trade-offs including the possibility of modifying objectives.

l) Select the dependability activities and tools which will provide the desired programme objectives within the given constraints.

m) Document the planning decisions and the details of how the dependability activities will be implemented. The dependability plan can be integrated into other plans, such as a quality plan or an overall project plan. It should state, as a minimum:

- the dependability objectives;
- the required dependability activities, tasks and tools, and the justification for their inclusion;
- the timing of dependability activities, the sequence, where relevant, and interactions between them, so they can be timed to give inputs to important development decisions;
- the evidence and outputs required;

- milestone events and the entry and exit criteria for each step, including the conditions under which activities and tasks require ongoing review or are considered complete;
- the estimated schedule and any dependencies between elements of the programme (the schedule can have to consider pressures from other business priorities and project plans);
- responsibilities and accountabilities;
- arrangements for dependability reviews.

n) Plan for monitoring changes in the programme context, for reviewing progress of the programme, and for triggering re-planning according to defined criteria.

7.3 Implement the plan

7.3.1 Purpose

The purpose of implementing the plan is to achieve dependability objectives in an efficient and cost effective way that complies with relevant contracts, regulations and standards and satisfies stakeholders.

7.3.2 Outcomes

As a result of implementing the plan:

a) organizational and stakeholder objectives with respect to dependability are met;

b) stakeholders are aware of their responsibilities and accountabilities, and accountability for dependability is achieved;

c) dependability is efficiently integrated into technical processes;

EXAMPLE Risk assessments relating to dependability can be combined with other project risk assessments and stakeholder engagement arrangements can be common across a wide range of issues.

d) people tasked with implementing the plan at any stage in the life cycle are competent and adequately supported in their roles;

e) the outcomes of technical activities (see Clause 8) are achieved;

f) assurance is provided that dependability objectives have been or will be met (see 7.5);

g) systems are established to collect, store and analyse dependability data.

7.3.3 Tasks

The following tasks can be involved in implementing a dependability plan.

a) Engage with stakeholders to establish their needs, expectations and requirements on an ongoing basis and to keep them informed as appropriate (see 8.2).

b) Provide information and training so that people are aware of their responsibilities and accountabilities and are competent to perform them.

c) Establish explicit agreements between stakeholders, including accountabilities for fulfilling them.

Explicit agreements among stakeholders and accountability for fulfilling them are particularly important for systems with extended operational life or with changing and difficult-to-define boundaries. For those open systems, activities focused on consensus building and accountability achievement are required. See IEC 62853.

d) Provide resources and support for dependability activities and the people involved in implementing them.

e) Document decisions and actions to provide traceability and accountability. A dependability case can be used for this purpose (see IEC 62741, ISO/IEC/IEEE 15026-2 and ISO/IEC/IEEE 15026-4).

f) Establish systems for monitoring the dependability of the system, product or service and the efficiency and effectiveness of dependability tasks.

7.4 Review and improve

7.4.1 Purpose

The purpose of reviewing dependability is to:

a) provide assurance that specific objectives from both technical and business perspectives are being met throughout the life cycle;
b) provide feedback on dependability deficiencies, deviations and risks;
c) improve the dependability of systems, products and services and of the workforce;
d) improve the way dependability is managed;
e) determine the status of projects;
f) assess the need for, and cost effectiveness of, dependability activities;
g) recognize change and the need to adapt.

7.4.2 Outcomes

As a result of undertaking reviews:

a) individual, organizational or technical weaknesses are identified and corrected early;
b) systems, products and services and the dependability programme are improved;
c) schedules and budgets are met;
d) risks are identified and treatments implemented effectively.

7.4.3 Tasks

The following tasks should be undertaken in accordance with applicable organizational policies.

a) Plan the scope and timing of reviews.

   Dependability is reviewed at each stage of the life cycle of a system, product or service, particularly when moving from one stage to another or when responsibility for a project is transferred. The scope can be:

   - technical, covering design and dependability performance aspects of a system, product or service or
   - management focussed, covering cost and scheduling aspects of a project or the dependability programme.

b) Identify stakeholders and involve them as appropriate.
c) Review requirements on a regular basis to account for changing stakeholder needs, operating conditions and new technologies.
d) Coordinate with, and participate in, other organizational and project reviews.

   EXAMPLE 1 Design reviews normally incorporate both dependability and performance aspects.

e) Identify targets.

   EXAMPLE 2 Targets can be dependability requirements, or project timelines and budgets, etc., relevant to dependability.

f) Collect evidence and information.
g) Prepare for and conduct meetings.
h) Assess the gap between required and actual performance.
i) Identify and monitor risks and areas of concern.
j) Analyse outcomes of review and recommend actions.

k) Check the effectiveness of changes made.

Dependability reviews that are carried out throughout the life cycle, including details of the tasks involved, are discussed in IEC 62960.

7.5 Providing assurance

7.5.1 Purpose

The purpose of dependability assurance is to give managers and other stakeholders justified confidence that their dependability objectives have been, or will be, achieved and that risks are controlled to an acceptable level. Assurance can relate to any aspect of dependability objectives (see 7.2.3).

NOTE This dependability activity is a version of the assurance process view provided in ISO/IEC/IEEE 15026-4 that is specific to the assurance of dependability.

7.5.2 Outcomes

As a result of providing assurance:

a) stakeholders unambiguously understand the claimed achievement of dependability objectives by an explicit statement of dependability performance;

b) it is verified that processes and systems, products and services conform to their requirements, standards and guidance and that defined procedures are followed;

c) a justified statement of dependability performance can be provided;

d) evidence and arguments are presented that provide stakeholders with the required level of confidence in the claimed achievement of dependability objectives;

e) stakeholders, including managers, have greater confidence that stakeholder needs, objectives, expectations and requirements, as well as business objectives, have been, or will be, achieved.

7.5.3 Tasks

The following tasks should be undertaken in accordance with applicable organizational policies.

a) Engage with stakeholders to establish their needs, expectations and requirements on an ongoing basis and to keep them informed as appropriate (see 8.2).

b) Provide evidence that risks of not achieving a dependability objective have been identified and addressed and opportunities to improve dependability have been exploited (see 8.3).

c) Provide evidence in the form of analysis that demonstrates that dependability can be achieved when direct measurement is impracticable or not appropriate (see 8.4).

d) Collect and evaluate data relating to dependability performance of the system, product or service or its components, in use or under test conditions (see 8.5).

e) Verify that requirements are, or will be, achieved and that any non-compliances have been corrected using evidence from b), c) and d) above.

f) Verify that procedures are followed through inspection, review and audit, etc.

g) Validate that systems, products and services meet stakeholder needs and expectations.

h) Provide evidence that support is provided to sustain the performance of people and the capability of the system, enabling it to adapt to changing needs (see 8.6).

Progressive assurance that dependability requirements are being met or will be satisfied throughout the life cycle of a system can be provided through a dependability case (see IEC 62741). This provides:

- a set of claims that formulate the contention that dependability is achieved;
- a reasoned auditable argument supporting the set of claims;

- evidence that risks have been treated and the claim has been or will be achieved.

NOTE 1 Progressive assurance means that assurance tasks are carried out through the life cycle and results provided at project milestones. This reduces the risk of finding out only at the end of a project that the evidence is inadequate.

NOTE 2 The dependability activities and tasks necessary to provide evidence relating to a dependability claim also define the necessary dependability activities and tasks of a dependability programme.

7.6 Achieving accountability

7.6.1 Purpose

The purpose of the accountability achievement activity is to establish the relationship between a noncompliance with an explicit agreement and its implications for stakeholders and society in general. This includes ensuring that accountable stakeholders will fulfil their obligation to provide agreed remedies for damage caused by noncompliance, so as to gain confidence and trust in the system among non-accountable stakeholders and general public.

NOTE 1 Explicit agreements can include the acquisition contract on the system, specified system requirements, assurance of identified dependability claims or a specified dependability programme. They can involve external and internal stakeholders and the general public (via, e.g. regulations).

NOTE 2 IEC 62853 provides a more detailed instance of this dependability activity as the accountability achievement process view.

7.6.2 Outcomes

As a result of achieving accountability:

a) for any noncompliance with explicit agreements, including a system failure, the affected stakeholders and, if relevant, the general public are able to identify the accountable stakeholders;

b) the affected stakeholders and, if relevant, the general public are provided with adequate information and agreed remedies by the accountable stakeholders;

c) information on readiness for a) and b) is available at any time, even before an event occurs, such that:

   - all stakeholders are aware of their accountability;
   - all stakeholders and general public have confidence in what will happen if the system fails or noncompliance with explicit agreements occurs.

NOTE Accountability achievement crucially complements dependability assurance in providing confidence and trust in the system. Confidence in what happens when dependability claims do not hold has significance independently of the required level of confidence in dependability claims, providing a possibility of trade-off between the two.

7.6.3 Tasks

The following tasks should be undertaken in accordance with applicable organizational policies:

a) for each potential noncompliance with explicit agreements:

   - identify key decisions in the system life cycle and dependability activities that can cause the non-compliance;
   - identify the accountable stakeholder for each key decision;
   - assess the impacts of noncompliance on the non-accountable stakeholders and general public;
   - agree on the implications of non-compliance for the accountable stakeholders and also for the non-accountable stakeholders and general public, including remedies the accountable stakeholders will be obliged to provide;

b) monitor, assess and feed back to the accountable stakeholders, the anticipated and unanticipated outcomes of key decisions, including noncompliance and its actual impacts;

c) enable the accountable stakeholders to promptly provide adequate information and the agreed remedies to the non-accountable stakeholders and general public when a noncompliance occurs;

d) communicate to all stakeholders and, where relevant, the general public how a), b) and c) are implemented.

8 Technical dependability activities

8.1 Overview

Clause 8 describes the technical dependability activities that aim to achieve dependability requirements and provide assurance that they have been or will be achieved. These are:

- stakeholder engagement (including consensus building and consultation);
- managing opportunities, threats and risks to dependability objectives;
- analysis of dependability attributes (including mathematical and statistical analysis, modelling, simulation and prediction of dependability attributes and life cycle costs);
- dependability assessment (including collection and evaluation of information and data);

  NOTE Information and data include operating and test data relating to a system, product or service and information and data to support dependability and project management.

- maintenance, support and improvement.

Annex E provides examples of tasks and tools that can be applicable at each life cycle stage.

Annex F explains how these dependability activities can be related to the system life cycle processes provided in ISO/IEC/IEEE 15288.

Activities relevant to maintainability and supportability programmes are also covered in IEC 60300-3-10 and IEC 60300-3-14.

8.2 Stakeholder engagement, consensus building and communication

8.2.1 Purpose

The purpose of engaging with stakeholders in the context of dependability is to:

a) achieve and maintain positive relationships with internal and external stakeholders;

b) understand stakeholder needs and expectations so that dependability requirements can be articulated and achieved, and their achievement trusted;

c) establish the basis of accountability through explicit agreements;

d) establish and promote a common understanding of the system that enables dependability problems that are not anticipated in explicit agreements to be resolved;

e) provide input to identifying risks so they can be treated as early as reasonably practicable;

f) enable dependability activities to be efficiently integrated into projects and into business and technical processes;

g) enhance the performance of the workforce so that the technical capabilities of the system and products can be fully realized and human dependability problems can be resolved;

h) receive feedback from stakeholders to assist improvement.

Stakeholder engagement should commence at the first available opportunity and be ongoing throughout the life cycle. Stakeholders that can be relevant in a particular context are detailed in Annex C.

8.2.2 Outcomes

As a result of engaging with stakeholders:

a) positive relationships are established with managers, project managers, customers, suppliers, regulators, etc., as appropriate;

b) managers and staff are aware of the importance of dependability and motivated and supported to achieve it;

c) there is a common understanding between relevant stakeholders of the purpose of the system, product or service, of its constraints and dependability requirements, and of responsibilities, accountabilities and authorities;

d) stakeholder needs and expectations are understood and translated into verifiable requirements;

e) dependability requirements and data are effectively communicated to appropriate stakeholders through different stages of the life cycle;

f) explicit agreements are formulated and maintained that include agreements on accountability of each stakeholder in the event of non-compliance;

g) traceability of dependability requirements to stakeholders and their needs is established;

h) stakeholders are assured that their dependability expectations are being met;

i) risks of not achieving dependability requirements are identified and treated as early as reasonably practicable;

j) failures and successes are reported and understood so dependability can be improved;

k) key decisions and agreements are recorded together with the rationale for them so that accountability can be traced and lessons learned when decisions turn out to be faulty;

l) weaknesses in workforce or organizational performance, which might impair dependability, are identified and mitigated so that technical capabilities can be fully realized.

8.2.3 Tasks

The following tasks should be undertaken in accordance with applicable organization policies and outcomes required.

a) Identify internal and external stakeholders and assess and document their interest and influence.

NOTE 1 Stakeholders can change over time, for example when ownership changes, when moving between stages of the life cycle or when there is a long utilization stage.

b) Identify those stakeholders that should be involved in particular dependability tasks, such as risk assessment or verification, and those to whom results should be communicated.

c) Develop communication plans.

d) Develop a policy on managing changes to agreements.

e) Engage with stakeholders in accordance with the communication plans.

f) Agree on an arbitration process to resolve conflicts when consensus cannot be reached.

g) Elicit and document stakeholder's needs, expectations and accountabilities for dependability. Consideration should be given to the following:

- the stakeholder's intended use of, or interaction with, the system, product or service and its operating environment and life profile;
- any accountabilities stakeholders have with regard to the system, product or service and its management, use or support;
- stakeholder needs, wants and expectations with regard to reliability, availability, maintainability, supportability and any other dependability related requirements;
- any constraints which will influence how dependability is managed;
- how relevant dependability attributes can be measured or otherwise assured.

h) Analyse stakeholder expectations and identify and resolve any conflicts.

i) Establish and maintain explicit agreements, and record accounts of negotiations and the rationale for decisions taken.

j) Communicate information associated with dependability to relevant stakeholders on a timely basis.

k) Obtain feedback on dependability issues for problem resolution and continual improvement.

l) Periodically review stakeholders and communication plans and update as necessary.

NOTE 2 IEC 62853 provides the consensus building process view, which details that part of the dependability activity concerning consensus building.

8.3 Managing opportunities, threats and risks

8.3.1 Purpose

The purpose of managing opportunities, threats and risks in the context of dependability is to:

a) achieve dependability objectives and improve decision making by understanding and managing the effects of uncertainty on those objectives;

NOTE Dependability objectives include achieving the requirements of the system, product or service and any other organizational objectives that could affect or be affected by dependability activities, for example objectives relating to safety, to the environment or to customer satisfaction.

b) understand how failures might occur so as to prevent failures or mitigate their effects;

c) exploit opportunities to improve dependability and dependability activities;

d) set priorities (of, for example, dependability objectives and activities) on the basis of risk;

e) provide assurance by demonstrating that risks to dependability have been controlled.

8.3.2 Outcomes

As a result of managing risk, threats and opportunities:

a) risks to the dependability of systems, products and services and to dependability activities are identified, understood and controlled;

b) the efficiency of a programme of dependability activities is improved as activities are directed to best manage risk;

c) opportunities to improve dependability and dependability activities are exploited;

d) decisions are based on a good understanding of opportunities, threats and risks, and are justifiable and traceable;

e) human actions and organizational processes, as well as systems, products and services fail less and are more dependable;

f) the uncertainty in data is understood and where appropriate quantified;

g) there is an understanding of how systems can fail, enabling designs to be improved and cost effective maintenance and support programmes to be implemented;

h) change, and the need for enhancement, are identified and managed effectively;

i) preparation is made for potential failures, including generic responses to failures that have not been recognized in advance;

j) information about risks is available to those that need it;

k) assurance is provided that risks are managed commensurate with the organization's appetite for risk.

8.3.3 Tasks

The following tasks should be undertaken as appropriate to the context.

a) Identify stakeholders who should be involved in activities to assess risks, and those who should be kept informed.

b) Establish a mechanism to communicate and consult about risks and their treatment to appropriate stakeholders.

c) Determine the scope, context and timing of risk management tasks and how they should be included within the scope of the organization's other risk management activities.

d) Decide how acceptable risk will be defined.

e) Identify opportunities, threats and risks and take them into consideration in decisions made at each life cycle stage. Tools for identifying risks include failure modes and effects analysis (IEC 60812), HAZOP (IEC 61882) and other tools as described in IEC 31010.

f) Analyse risk by looking at causes, consequences and the controls already in place. Where appropriate determine the probability that particular consequences will occur. Tools such as fault tree analysis (IEC 61025) and event tree analysis (IEC 62502) can be used (see also IEC 31010).

NOTE 1 Tools used for dependability analysis can also be used to analyse risk more generally.

g) Coordinate risk management activities and the use of risk assessment tools to avoid duplication of effort.

h) Identify opportunities and analyse them by comparing expected benefits and the risks of either pursuing or not pursuing the opportunity.

i) Apply the understanding of risks in the design of the programme through each life cycle stage.

j) Plan and implement actions based on the understanding gained from risk analysis so that unacceptable risks are treated.

k) Allocate responsibilities, authorities and accountabilities for actions relating to risks and the risk management framework.

l) Monitor the status of risks and their treatments.

m) Analyse direct and underlying causes of failures so that lessons can be learnt and failures prevented (see IEC 62740).

n) Monitor changes in the environment, context and purpose, etc., and analyse how they affect risk.

o) Monitor anticipated and unanticipated outcomes from decisions, and relay results in a timely manner to improve failure response and accountability achievement.

p) Collect, analyse, store, review and update information on risk, through the life cycle.

q) Follow up recommended actions relating to risk, threats and opportunities.

NOTE 2 Guidance on the risk management principles, framework and process is given in ISO 31000. Managing risk in projects is discussed in IEC 62198 and risk assessment tools in IEC 31010.

8.4 Dependability analysis

8.4.1 Purpose

The purpose of dependability analysis is to provide a technical understanding of the system, product or service and factors affecting its dependability and life cycle costs. This can be used:

- as an input to decisions;
- to model and predict dependability outcomes of a design;
- to achieve and improve dependability in a cost effective way;
- to verify that requirements are being or can be met.

Analyses are also performed as part of managing opportunities, threat and risks (8.3), dependability assessment (8.5) and to verify safety, for example safety integrity level (SIL) for systems that include electronic safety related items (see the IEC 61508 series) and automotive safety integrity level (ASIL) for cars (see the ISO 26262 series).

8.4.2 Outcomes

As a result of dependability analysis:

a) a technical understanding of the system, product or service and its operating environment is obtained;

b) common characteristics and worst case constraints of the operating environment are identified;

c) dependability, cost and risk characteristics of design options are predicted and compared;

d) a cost effective design is selected that can be demonstrated to achieve requirements within specified conditions and constraints;

e) assurance is provided to stakeholders that their needs and requirements for dependability have been or will be met;

f) the system is designed with consideration of its eventual retirement taking into account the circular economy and the need to minimise environmental impact;

g) potential failure modes are identified so they can be prevented or their effects mitigated;

h) cost implications of decisions relating to dependability are understood;

i) factors affecting reliability, maintainability, supportability and other dependability related attributes such as availability, operability, usability, durability, etc., are understood and trade-off decisions made;

j) the roles of hardware, software and people in a system are optimized so that their performance does not impair the overall capabilities of the system;

k) systems and products are retired in a way that is safe, secure, environmentally sound and in line with legislation and standards.

8.4.3 Tasks

Dependability analysis can include the following tasks.

a) Map design characteristics to the end user environment to assist in defining requirements or selecting design options.

NOTE 1 Factors to consider can include electromagnetic compatibility, thermal conditions and mechanical stresses.

b) Predict values for dependability attributes.

c) Undertake an iterative process of analysis and improvement as the design progresses to improve dependability.

d) Perform regression analysis to verify that changes have not affected the existing functionality of a system, product or service.

e) Undertake life cycle cost analysis to optimize dependability performance within given life cycle cost constraints (see IEC 60300-3-3).

f) Conduct trade-off analyses.

g) Analyse potential failure modes, causes and effects in order to improve designs, plan maintenance and support programmes and plan failure response (IEC 60812).

NOTE 2 Techniques used for root cause analysis can also be used proactively to identify failure modes and causes (see IEC 62740).

h) Analyse the dependability of the system by modelling stress conditions and corrupted or illegal data inputs.

i) Analyse the effect of human performance on dependability activities and dependability attributes of the system, product or service. Where relevant, develop programmes to improve human error rate (IEC 62508).

j) Analyse processes used in manufacture, delivery and installation to minimize impact on dependability. Process FMEA can be used (see IEC 60812).

k) Analyse design changes and enhancements for safety and operability issues (see IEC 61882) and check intended improvements will be achieved.

l) Analyse systems prior to retirement for potential second hand use or for re-use of modules, components and materials (see IEC 62309). Consider means of safe transfer or deletion of data.

NOTE 3 The systems analysis process (ISO/IEC/IEEE 15288) provides generic tasks that apply for any analysis task. A comparison of the two approaches is given in Annex F.

Analyses relevant to reliability, maintainability and supportability are discussed in IEC 62308, IEC 62508, IEC 60300-3-1, IEC 60300-3-10 and IEC 60300-3-14.

8.5 Dependability assessment

8.5.1 Purpose

The purpose of dependability assessment is to:

r) determine dependability characteristics of a system, product or service;

s) verify that the dependability of people, systems, products, services and processes meets requirements;

t) validate that dependability meets stakeholder needs;

u) detect and remove defects;

v) monitor dependability as improvement strategies are implemented to meet business needs (e.g. to enhance dependability performance, reduce costs and improve timeliness of product releases);

w) learn from operational data and tests to improve design;

x) improve the way dependability activities are carried out;

y) assess the dependability aspects of a project;

z) provide information for dependability reviews (see IEC 62960).

NOTE ISO/IEC/IEEE 15288 describes the project assessment and control life cycle process that can be applied to assess dependability aspects of a project.

8.5.2 Outcomes

As a result of dependability assessment:

a) performance measures are available;

b) information needs and data collection methods are identified;

c) information and data are collected, verified and stored;

d) data are analysed and the results interpreted and reported;

e) dependability characteristics for the system, product or service are known and quantified where possible;

f) desired dependability characteristics are achieved, verified and validated;

g) information and data are available, enabling dependability and its management to be improved;

h) traceability of results is established;

i) stakeholders are provided with the data they need in the format and within the time scales required;

j) project and dependability objectives are achieved.

8.5.3 Tasks

Dependability assessment can include the following tasks.

a) Identify the problem or question that requires assessment.

b) Determine stakeholder needs and requirements and the form of output required.

c) Determine how dependability attributes will be measured or otherwise verified and the data required.

d) Determine the inputs and associated data required to perform the assessment.

e) Determine test conditions, data requirements and test methods (see IEC 60300-3-5).

f) Determine resources available and constraints (e.g. time, funding, samples, personnel, tools and facilities). It is important that test results are ready to provide input to critical decisions. This can influence the design of the test procedure.

g) Determine the source of data and how and when data will be collected (e.g. from simulations and models, from tests in a simulated environment, from observations during normal operation or from manufacturers data, etc.).

NOTE 1 Data from suppliers of components and modules, or from field observations and tests of similar systems, products and services can be used to predict and improve dependability during design (see IEC 62308).

NOTE 2 IEC 60300-3-2 provides guidance on the collection of data from the field.

h) Integrate dependability assessment into relevant processes.

i) Collect information and data. This can involve measuring dependability attributes, monitoring the performance of systems, products and services to check that performance is not degraded over time, surveys, observations and tests (see Annex G).

j) Interpret data.

k) Compare actual dependability characteristics with those desired, implement improvements and conduct regression tests as required (see IEC 61014).

l) Record data in such a way that traceability can be achieved between product changes and cost and performance outcomes.

m) Store data so it can be used for future reference.

n) Communicate outcomes to stakeholders as appropriate.

Techniques for reliability testing are discussed in IEC 60300-3-5 and for maintainability testing in IEC 60300-3-10. Software testing techniques are covered in ISO/IEC/IEEE 29119-4.

8.6 Maintenance, support and improvement

8.6.1 Purpose

The purpose of maintenance, support and improvement in the context of dependability is to:

o) sustain the performance of the system, product or service;

p) manage life cycle costs;

q) enable systems, products and services to continue to meet dependability objectives during operation in a cost effective way;

r) manage information necessary for ongoing operation and for future improvement, (including data on faults and failures);

s) minimize harm and disruption from failures;

t) maintain fit for purpose status of the system or product despite changes in requirements, environments, objectives and purpose;

u) manage obsolescence (see IEC 62402);

v) support and enhance the capability of the stakeholders (e.g. workers or users) to operate the system or use the product;

w) improve the dependability of systems, products and services and the efficiency and effectiveness of dependability activities.

8.6.2 Outcomes

As a result of the maintenance, support and improvement activity:

a) systems, products and their components are designed so that they are safely and reliably operable, maintainable, testable and re-useable;

b) user requirements for maintainability and for availability during operation are achieved and assured;

c) maintenance programmes are planned and implemented;

d) support is organized and operates effectively;

e) people are supported to perform their roles effectively and efficiently;

f) risks to maintenance and support arrangements are identified and treated;

g) the effects of failures are minimized;

h) the system, product or service performs as required despite changes in requirements, environments objectives and purpose;

i) improvements are implemented through a controlled process;

j) all changes to software and hardware are known and tracked at all times.

8.6.3 Tasks

Maintenance, support and improvement can include the following tasks.

a) Provide input to the design team regarding maintainability and supportability.

b) Identify potential failure modes, mechanisms and effects as input to defining a maintenance programme (see IEC 60812).

c) Incorporate human aspects into design for usability, maintainability and supportability.

d) Define a maintenance and support strategy (see IEC 60300-3-12).

e) Define an initial maintenance programme during design and develop it continuously through the life cycle (see IEC 60300-3-10 and IEC 60300-3-11).

f) Plan maintenance and support, including resource needs, skill levels and schedules to achieve an affordable, operable, supportable and sustainable solution.

g) Specify external support services needed and develop agreements (see IEC 60300-3-16).

h) Identify, analyse and treat risks to maintenance and support programmes including those associated with the contractual arrangements and the supply chain.

i) Manage spare parts (see IEC 62550).

j) Perform maintenance and organise maintenance support.

k) Collect and review data concerning maintenance and support and compare with maintainability and supportability specifications and requirements.

l) Establish a system for reporting failures and successes (FRACAS or DRACAS) and collect data related to successes, failures and non-conformances during tests and in the field (see IEC 60300-3-2 and IEC 60300-3-5).

NOTE 1 For failures of systems in operation, the observed failures relate only to the operating conditions when the failure occurred.

NOTE 2 Failure analysis during accelerated testing and stress testing can be used to identify failure modes that could also occur in use. (See IEC 62506 and the IEC 61163 series.)

m) Provide input to decisions regarding evolution and enhancement.

n) Control and track modifications to the system's design including hardware, firmware, software and documentation.

o) Manage contractors and suppliers.

p) Manage obsolescence (see IEC 62402).

q) Provide information concerning the cost and practicalities of maintenance and support (including considerations of obsolescence) to assist in decisions about retirement.

r) Evaluate and apply life extension methods such as update, upgrade or refurbishment.

s) Identify items that can be suitable for re-use and provide relevant data concerning their condition.

Further information on maintenance and maintainability tasks is provided in IEC 60300-3-10 and on support and supportability in IEC 60300-3-14. Integrated logistic support is covered in IEC 60300-3-12.

Annex A
(informative)

IEC standards related to dependability

Table A.1 – Classification of dependability standards by topic and life cycle stage

Classification	Life cycle stage				
	Conc.	Dev.	Real.	O/M.	Retir.
Fundamentals					
IEC 60500-192, *International Electrotechnical Vocabulary – Part 192: Dependability*	✓	✓	✓	✓	✓
IEC 61703, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms*	✓	✓	✓	✓	✓
High level standards – Process standards					
IEC 60300-1, *Dependability management – Part 1: Managing dependability*	✓	✓	✓	✓	✓
IEC 62853, *Open systems dependability*	✓	✓	✓	✓	✓
IEC 62508, *Guidance on human aspects of dependability*	✓	✓	✓	✓	✓
IEC 60300-3-3, *Dependability management – Part 3-3: Application guide – Life cycle costing*	✓	✓	✓	✓	✓
IEC 62402, *Obsolescence management*	✓	✓	✓	✓	✓
IEC 62741, *Demonstration of dependability requirements – The dependability case*	✓	✓	✓	✓	✓
IEC TS 62775, *Application guidelines – Technical and financial processes for implementing asset management systems*	✓	✓	✓	✓	✓
IEC 62960, *Dependability reviews during the life cycle*	✓	✓	✓	✓	✓
Documentation and data					
IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*			✓	✓	
IEC 60300-3-4, *Dependability management – Part 3-4: Application guide – Specification of dependability requirements*	✓	✓			
Software, communications and open systems					
IEC 61907, *Communication network dependability engineering*	✓	✓	✓	✓	
IEC 62673, *Methodology for communication network dependability assessment and assurance*	✓	✓	✓	✓	✓
IEC 62628, *Guidance on software aspects of dependability*	✓	✓	✓	✓	✓
Discipline based standards – Programme level					
IEC 60300-3-10, *Dependability management – Part 3-10: Application guide – Maintainability and maintenance*[1]	✓	✓	✓	✓	✓
IEC 60300-3-14, *Dependability management – Part 3-14: Application guide – Supportability and support*[2]	✓	✓	✓	✓	✓
Reliability					
IEC 61014, *Programmes for reliability growth*		✓	✓	✓	
IEC 61709, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*		✓			

[1] Under preparation. Stage at the time of publication: IEC CDV 60300-3-10:2024.

[2] Under preparation. Stage at the time of publication: IEC FDIS 60300-3-14:2024.

Classification	Life cycle stage				
	Conc.	Dev.	Real.	O/M.	Retir.
IEC 62308, *Equipment reliability – Reliability assessment methods*		✓	✓		
Maintenance and maintainability					
IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*		✓	✓	✓	
IEC 60706-2, *Maintainability of equipment – Part 2: Maintainability requirements and studies during the design and development phase*	✓	✓			
IEC 60706-3, *Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data*		✓	✓	✓	
IEC 60706-5, *Maintainability of equipment – Part 5: Testability and diagnostic testing*		✓	✓	✓	
IEC 62309, *Dependability of products containing reused parts – Requirements for functionality and tests*	✓	✓			✓
Supportability and support					
IEC 60300-3-12, *Dependability management – Part 3-12: Application guide – Integrated logistic support*		✓	✓	✓	
IEC 60300-3-16, *Dependability management – Part 3-16: Application guide – Guidelines for specification of maintenance support services*	✓	✓			
IEC 62550, *Spare parts provisioning*		✓	✓	✓	
Dependability and risk modelling and analysis					
IEC 31010, *Risk management – Risk assessment techniques*	✓	✓	✓	✓	✓
IEC 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*	✓	✓	✓	✓	
IEC 60812, *Failure modes and effects analysis (FMEA and FMECA)*	✓	✓	✓	✓	
IEC 61025, *Fault tree analysis*	✓	✓	✓	✓	
IEC 61078, *Reliability block diagrams*	✓	✓		✓	
IEC 61165, *Application of Markov techniques*		✓			
IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*	✓	✓		✓	
IEC 62198, *Managing risk in projects – Application guidelines*	✓	✓	✓	✓	✓
IEC 62502, *Analysis techniques for dependability – Event tree analysis (ETA)*		✓		✓	
IEC 62508, *Guidance on human aspects of dependability*	✓	✓	✓	✓	✓
IEC 62740, *Root cause analysis (RCA)*		✓	✓	✓	
IEC 62551, *Analysis techniques for dependability – Petri net techniques*		✓		✓	
IEC TR 63039, *Probabilistic risk analysis of technological systems – Estimation of final event rate at a given initial state*	✓	✓			

Classification	Life cycle stage				
	Conc.	Dev.	Real.	O/M.	Retir.
Reliability testing and statistical analysis					
IEC 60300-3-5, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*		✓	✓	✓	
IEC 60605-2, *Equipment reliability testing – Part 2: Design of test cycles*		✓	✓		
IEC 62506, *Methods for product accelerated testing*		✓	✓		
IEC 60605-4, *Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals*		✓	✓	✓	
IEC 60605-6, *Equipment reliability testing – Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity*		✓	✓	✓	
IEC 61070, *Compliance test procedures for steady-state availability*		✓	✓	✓	
IEC 61123, *Reliability testing – Compliance test plans for success ratio*		✓	✓		
IEC 61124, *Reliability testing – Compliance tests for constant failure rate and constant failure intensity*		✓	✓		
IEC 61649, *Weibull analysis*		✓	✓		
IEC 61650, *Reliability data analysis techniques – Procedures for comparison of two constant failure rates and two constant failure (event) intensities*		✓	✓		
IEC 61710, *Power law model – Goodness-of-fit tests and estimation methods*		✓	✓		
Screening					
IEC 61163-1, *Reliability stress screening – Part 1: Repairable assemblies manufactured in lots*			✓	✓	
IEC 61163-2, *Reliability stress screening – Part 2: Components*			✓	✓	

Key – Abbreviations used in table

Conc. Concept

Dev. Development

Real. Realization

O./M. Operation and maintenance

Retir. Retirement

✓ indicates life cycle stage for which the standard is relevant

Annex B
(informative)

Life cycle models

B.1 Generic life cycle

A simple generic life cycle model that is generally applicable and which can form the basis from which more specific models can be derived is illustrated in Figure B.1. The details of the stages and the transitions between them will be context specific and defined by the particular milestones applicable to the situation or project concerned. A key aspect of any life cycle model is that each stage has entry criteria that have to be met before effort in that stage begins and each stage is required to meet exit criteria before it is considered to be complete. Not all stages are necessarily relevant to all contexts. Table B.1 describes the purpose of these stages and typical dependability outputs.

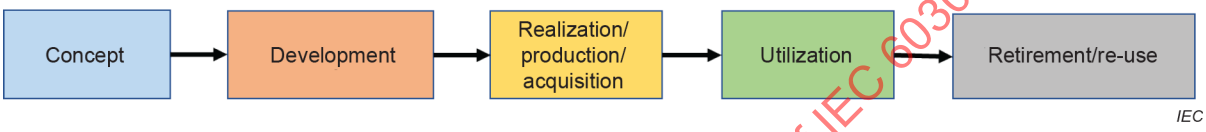


Figure B.1 – Generic life cycle model

Table B.1 – Stages of generic model, their purpose and outputs

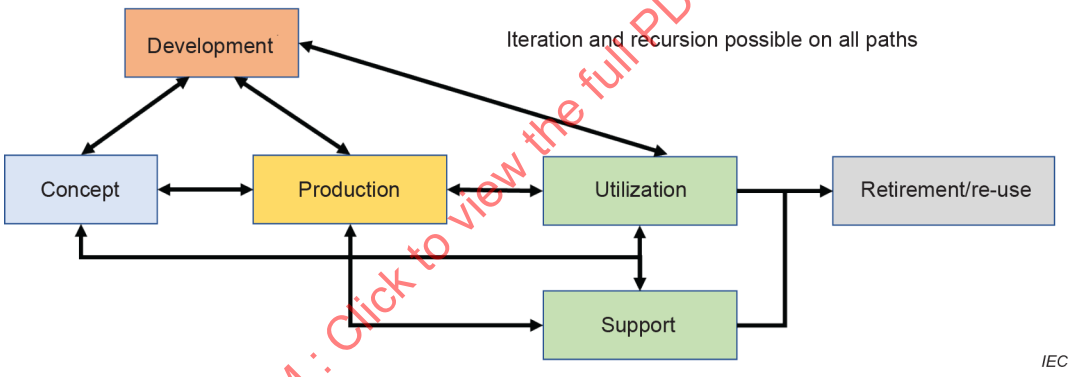
Stage	Purpose	Dependability outputs
Concept	Identify stakeholder needs Explore concepts Propose viable solutions	Specified requirements that meet user's needs Conceptual design(s) that meet requirements Preliminary risks identified for ongoing consideration Evidence that requirements and constraints can be met by the conceptual design Initial life cycle cost estimates Agreements including on conceptual design and maintenance and support policies
Development	Refine requirements Create solution description Build systems or products Verify and validate that needs and requirements are satisfied	A design verified and validated by tests, analysis and simulation Refined outcomes and life cycle cost estimates Prototype where relevant Evidence that the system, product or service meets or will meet dependability requirements and is cost effective Plans for realization
Realization (production, acquisition and installation)	Produce or acquire system Verify and validate that needs and requirements are satisfied	Functioning tested system that meets specifications Documentation relating to operation, maintenance and support Agreements relating to acceptance, operation and maintenance

Stage	Purpose	Dependability outputs
Utilization (including evolution and enhancement)	Operate to satisfy users' needs Maintain and support system or product to provide sustained capability Accommodate changing needs	Systems, products and services that meet user needs on an ongoing basis Dependability data, for example field data
Retirement or re-use	Store, archive or dispose of system Achieve sustainable, environmentally sound end of use	Safe and acceptable closure Re-use of system, products or parts and materials Data and experiences for future projects

B.2 Alternative life cycle models

B.2.1 Life cycle model with multiple progressions

In practice the stages often overlap and iterations between the stages can occur. Stages do not necessarily occur one after another in a time sequence. Figure B.2 provides an example of such a life cycle. In this example support is added as a separate stage and realization is considered from the point of view of a producer. Development can continue to occur during the concept, production and utilization stage. The figure also shows that when the system needs to be enhanced it returns from utilization and support back to the concept stage.



Source: Reproduced from ISO/IEC/IEEE 24748-1:2018, Figure 6.

Figure B.2 – Life cycle model with some of the possible progressions

B.2.2 Managing change through the life cycle

During utilization changes can be needed, for example to improve dependability, to respond to failures, or to adapt to changing needs. Figure B.3 illustrates how the need for change that is recognised from analysing data during utilization is fed back into different life cycle stages.

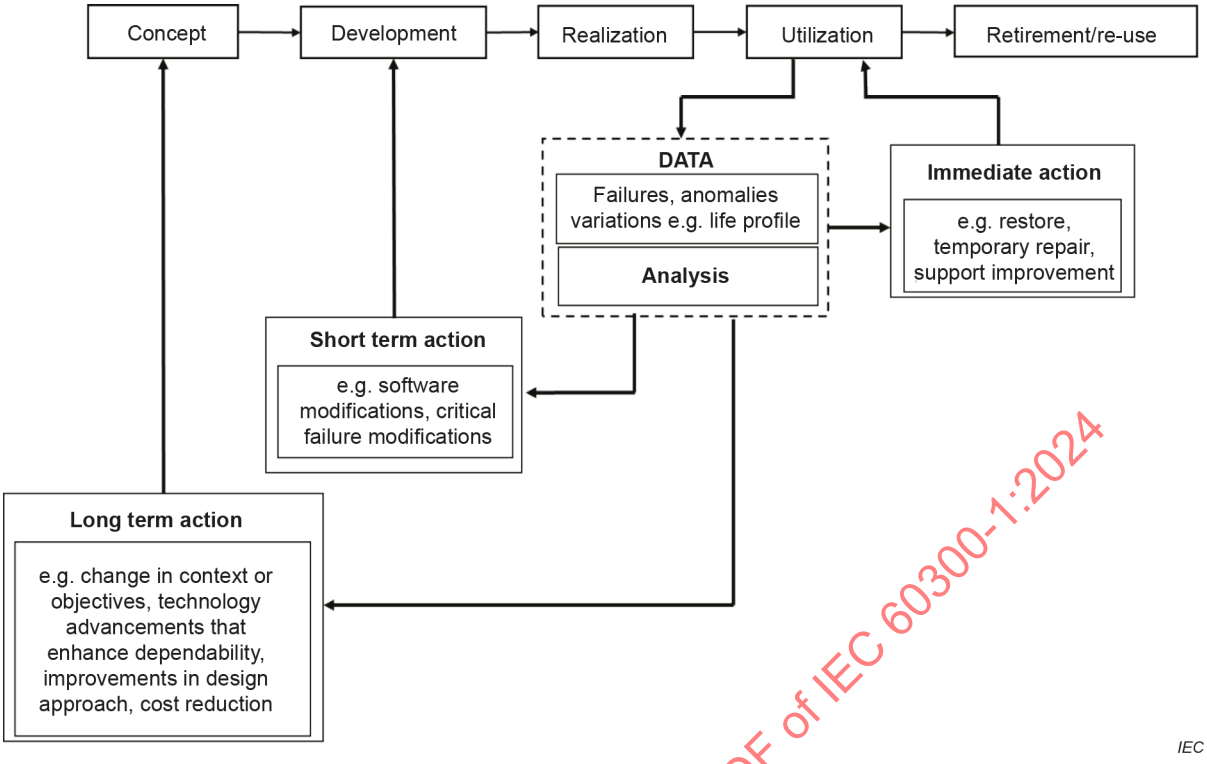


Figure B.3 – Managing change through the life cycle

B.2.3 Hardware

The hardware life cycle can vary for different types of item. Components or simple systems such as electronics can be designed and manufactured as products for consumer use. More complex hardware systems might be designed with some items being acquired and others manufactured. The result is that there are often multiple organizations involved, each considering a different life cycle (see Figure B.4).

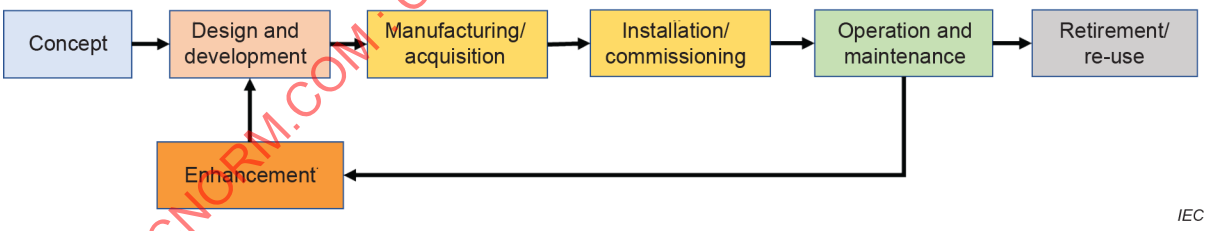


Figure B.4 – Example of hardware life cycle model

B.2.4 Software (see Figure B.5)

Software can be embedded into hardware or can be separate. During development it is tested and verified to ensure proper functionality, and validated against user needs. Software is not manufactured but does have to be built, compiled and distributed to users. During the utilization stage, errors or failures that are encountered are normally rectified through software maintenance, support and improvement. Major enhancements are handled through a separate enhancement stage that includes regression tests. For software, changes in requirements and environments are more frequent and the need for enhancement is greater than for hardware. One reason is that software interacts with a more complex, wider ranging environment (e.g. with humans, through the internet). Another is that, when a combined hardware-software system needs to change, software is expected to absorb most of the change because of perceived ease of modification compared with hardware.

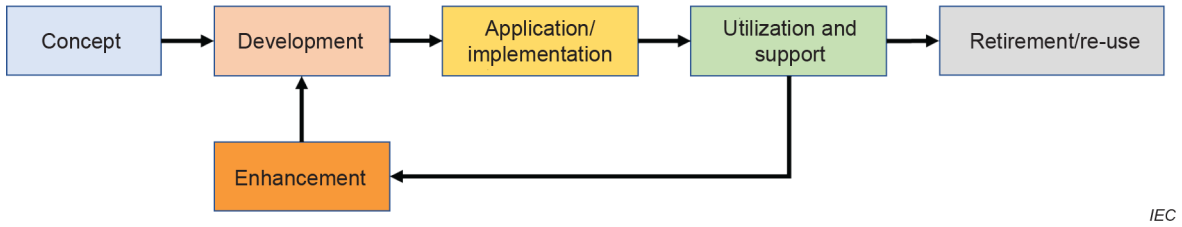


Figure B.5 – Example of software life cycle model

B.2.5 Services

The requirement for a service can be obtained either by setting it up internally or by outsourcing (or a combination of the two approaches) (see Figure B.6).

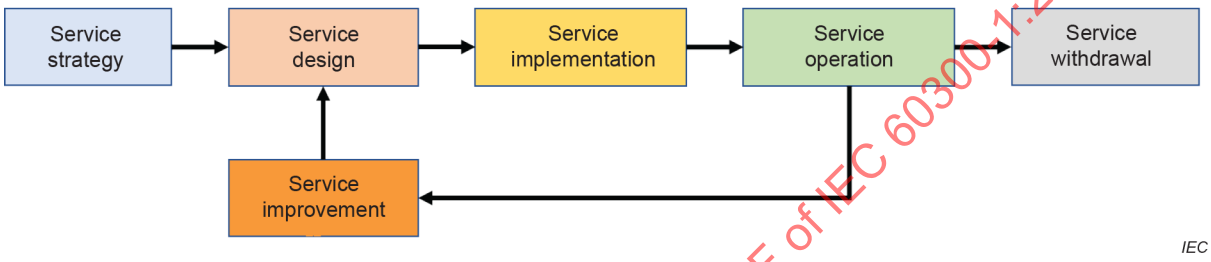


Figure B.6 – Example of service life cycle model

B.2.6 Open systems

As systems become more complex and interlinked, boundaries become difficult to define and no one fully understands all aspects of the system. Information management, communication, clearly defined accountability and local autonomy become critical to the dependability of the system (see IEC 62853). Figure B.7 shows a simplified life cycle model that can be used when considering such systems. As well as incorporating the need for change this model incorporates a consensus building stage, an accountability achievement stage and a failure response stage.

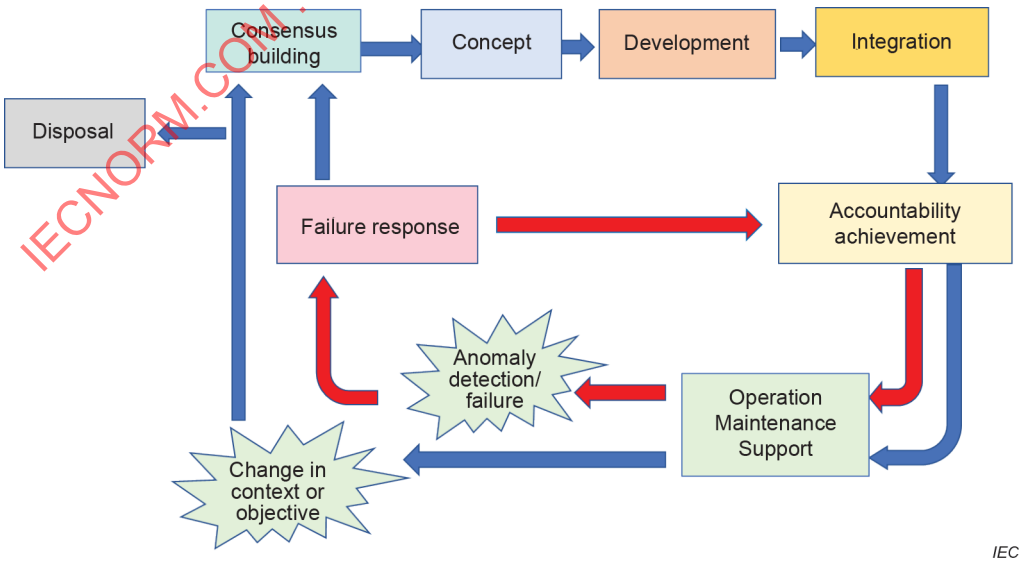


Figure B.7 – Simplified life cycle model for an open system

Annex C
(informative)

Stakeholders

C.1 General

A stakeholder is anyone who can affect, is affected by, or perceives themselves to be affected by an organization's actions, objectives or policies. For dependability, this includes users and operators who depend on systems, products or services to perform as and when required, those that manufacture, sell or acquire as well as those responsible for ensuring that dependability can be achieved.

Stakeholders and their level of involvement vary with the type of system, product or service concerned. For a pervasive system, or any system in a networked environment, the totality of stakeholders can be hard to ascertain and stakeholders might not even be aware of each other. Society in general might have to be considered as a stakeholder in some cases.

Stakeholders can change substantially over the life of a system, product or service as its application, requirements and utilization change.

C.2 Users of systems, products and services

Users will be impacted by the reliability and availability of a system, product or service, and by the need for maintenance and support. The impact depends on the nature and importance of the application. A cell phone used for normal communication between family members or general use is less critical than if it is being used by an emergency service such as fire fighters or ambulance services.

Users can include consumers, the public, government, military, private organizations, public utilities and public or private organizations providing transportation such as airlines, ferries, railways and buses.

C.3 Managers

The role of managers in dependability is to ensure that adequate resources are applied to dependability activities. Top management is responsible for overall strategy and planning and for approving financial resources to manage dependability. The first level of management (e.g. supervisors, project leaders) has a more direct role in hiring staff, ensuring dependability activities are carried out effectively and reporting results to higher level management and stakeholders.

Managers can be involved in approving decisions such as trade-offs between dependability and other factors such as performance, cost and risk.

C.4 The workforce

The workforce contributes to system performance and dependability outcomes at all stages of the life cycle.

C.5 Specialists

The role of specialists is to apply their expertise to specify, design, achieve and maintain dependability. Specialists include reliability, maintainability, supportability and maintenance personnel as well as specialists from other disciplines that are relevant to a particular project. For example a human factors expert can be involved in achieving a useable and accessible design and organizational arrangements that support dependability.

C.6 Others

Dependability standards can be used in regulations or contracts, in which case stakeholders can be national and international standards organizations, governments, regulators, organizations being regulated and organizations using dependability standards in contracts.

Some stakeholders for dependability exist in academic and industry-based research institutions where expertise is available to develop new or improved methods, tools and techniques.

Members of the public can be stakeholders as users of systems, products or services or because they are affected by them.

C.7 Stakeholders through the life cycle

C.7.1 Concept – Specification

Stakeholders involved at the concept stage include targeted end users, design or system engineers, specialists responsible for reliability, maintainability and supportability, staff responsible for purchasing and procurement, and in some cases regulatory authorities.

C.7.2 Development

The stakeholders during the initial design or during enhancement of a system or product include representatives of the various disciplines responsible for the design and specialists providing input such as statisticians, ergonomists, software designers and maintenance staff. Future users and maintainers are also stakeholders in the design and can provide significant input. Other stakeholders at this stage can include regulatory authorities, subcontractors and suppliers.

C.7.3 Realization (including manufacture, transport acquisition and installation)

The main role for dependability during the realization stage of the life cycle (which includes manufacturing, acquisition and installation) is to verify that required dependability attributes will be achieved. This can include acceptance testing, verification of maintainability and maintenance support resources and availability testing. Quality assurance and quality control activities for both manufactured and purchased systems and products also provide assurance that dependability requirements can be achieved.

As well as end users and those involved with assembly, installation and commissioning, stakeholders can include regulators, quality assurance and control staff and, in some cases, members of the public.

C.7.4 Operation or use of items

Stakeholders who operate or control items, such as the pilot in an aircraft or an operator in a process plant, have an important role in ensuring that items are operated safely and within their design and operating constraints. This also applies to consumer products where the way they are used can affect their dependability. For example, an excessively hard driving style can lead to increased loading and premature failure of the transmission and other vehicle units.

Stakeholders during operation include users of consumer items, system operators or field engineers, those who use a system or product to supply a service and customer support personnel.

C.7.5 Maintenance

Maintenance involves technical staff who perform corrective or preventive maintenance and those responsible for support such as spare parts. Others include those involved in monitoring or testing of machinery and staff performing software maintenance. Stakeholders also include anyone, internal or external, who is impacted by down time, and external stakeholders such as suppliers and contractors.

C.7.6 Obsolescence, retirement and re-use

Stakeholders can be involved in planning for obsolescence and for in-life extension activities such as update, upgrade or refurbishment and subsequently for actions when items have been deemed to be obsolete (see IEC 62402).

When systems, products or their components are retired, some stakeholders might have to find a replacement and others might be involved in decommissioning, dismantling or abandonment. Some items might be re-used and thus can have to be re-evaluated from a dependability point of view. Affected stakeholders could be users and operators of a system or product, managers, maintenance support personnel, manufacturers and spare parts providers, users of second hand parts and society and future generations affected by the environmental impact of disposal.

Annex D
(informative)

Dependability maturity assessment

Maturity models are used by organizations to describe and assess their processes. Four or five levels or stages are defined, from ad-hoc to optimised processes. Verifiable indicators are specified for each stage against a range of dimensions. These can be used to develop a maturity questionnaire from which areas for improvement can be identified. Table D.1 provides an example of some indicators to assess the maturity of dependability management.

Table D.1 – Example of dependability maturity matrix

Dimensions	Stage 1 – Immature	Stage 2	Stage 3	Stage 4 – Mature
Organizational context (see 5.2)	Organizational context not understood Stakeholders and their requirements unknown	Primary dependability objectives are identified from the organizational context, however they are established in isolation from market conditions and external stakeholder needs Dependability requirements are not updated with changing organizational context Operational profiles for assets are established, however remain fixed for the life of the asset, regardless of a changing organizational context	Organizational context is established and is periodically assessed for changes Current market conditions are considered Dependability requirements are derived from organizational context with some consideration towards balancing risk, cost and performance Operational profiles for assets are established and are updated based on major organizational context changes Primary stakeholder dependability requirements are known Stakeholder management is informal	Organizational context is known and continuously under surveillance Current and expected future market conditions are considered when deriving dependability requirements Desired balance of risk, cost and performance is known Stakeholder requirements are known and actively managed Changes to the dependability context are readily identified and initiate resultant changes in operational profiles, dependability plans, arrangements and operational aspects

Dimensions	Stage 1 – Immature	Stage 2	Stage 3	Stage 4 – Mature
Leadership	Leadership team has little understanding of the benefit of dependability management Dependability management is not integrated into policy There are no organizational arrangements focused on dependability	Leadership team regards dependability as a separate activity Warranty costs are to be minimized	Leadership team recognizes dependability as an investment, but it is not related to business Objectives (cost, schedule and performance)	Leadership team believes dependability management is essential to achieving business objectives Dependability aspects are integrated into policy with clear guidelines on how dependability objectives will be achieved Internal and external relationships, authorities, responsibilities and reporting are effective in achieving dependability requirements New dependability tools and techniques are monitored and integrated into business plans where appropriate
Planning	Dependability objectives are unknown There is no planning to achieve dependability objectives	Tests are planned but results are usually too late to influence design and manufacturing	Dependability objectives are mostly known Dependability activities are included in business plans, however are not tailored to the context Funding is often wasted by conducting dependability activities which do not provide value	Dependability objectives are known Required dependability activities are included in business plans and are tailored depending on the context Funding is not wasted on dependability activities which will not support achievement of business objectives Technical and financial risks are known and risk management strategies are in place Contingency plans are developed and activated as necessary
Support	No dependability understanding throughout the organization No dependability specialists or roles No funding allocated to dependability activities No dependability training offered within organization	Dependability specialist roles are established, but in isolation from other company activities	Dependability specialists participate in projects, but not at decision level	Organization appoints dependability specialists that participate in decisions All employees, including leadership team, have understanding of dependability concepts and objectives Dependability training is supported by management, with different levels targeted at various roles within the organization Funding is allocated to dependability activities as required There is an established information record system which supports the efficient storage, retrieval and update of dependability plans, processes and related data

Dimensions	Stage 1 – Immature	Stage 2	Stage 3	Stage 4 – Mature
Operation	Few dependability activities are conducted, if any	Dependability characteristics are assessed and predicted using point estimates	Risk is assessed using qualitative measures Dependability characteristics are predicted and assessed	Dependability activities are integrated into business processes and conducted routinely Dependability characteristics are considered and controlled through all phases of the life cycle Dependability characteristics are predicted and assessed using distributions and confidence intervals Risk is assessed using qualitative and quantitative measures Engineering changes are conducted to improve balance of risk, cost and performance Supplier dependability is monitored
Performance evaluation	Data collection is sporadic and untargeted Cost of poor dependability is unknown	Costs due to lack of dependability are recorded	Proactive activities and costs of dependability trade-off are recognized	Data required to measure and predict risk, cost and performance are routinely collected Predictions are compared to realized values in order to improve future predictions Effect of corrective actions is monitored
Improvement	Dependability improvement not actively sought	Improvement is focussed on reducing warranty costs	Dependability problems are reduced before manufacturing and acceptance tests	Outcomes from performance evaluation are fed back into all phases of the life cycle and business areas Designs are updated to improve dependability characteristics Asset management strategies are adjusted to reach desired dependability characteristics in utilization phase Dependability training is adapted based on business improvement needs

Annex E
(informative)

Dependability through the life cycle

Table E.1 – Examples of dependability focus relevant to each life cycle stage

Stage	Outcomes or project tasks	Dependability focus
Concept	Commence dialogue with stakeholders Understand stakeholder and market needs and context of use and constraints Identify necessary trades with respect to objectives Translate stakeholder needs into the requirements of the system Determine how technical and quality requirements are to be measured Obtain agreements with stakeholders Develop technical design specifications Review organization's capability to undertake the work Identify feasible design or purchasing solutions Allocate functions between hardware, software and people Identify potential partnerships and supplier requirements Identify risks that need to be addressed in design	Define boundaries of system of interest and operating environment Define scope of dependability programme for the system Identify needs and expectations of stakeholders and translate to verifiable dependability requirements Establish acceptance criteria and verification methods Identify constraints that can affect dependability (e.g. human factors, regulations) Identify design implications of retirement or re-use Identify need for trade-offs, for example between reliability and safety, or reliability and maintainability Allocate dependability targets to subsystems Assess risks of alternative technologies and design options Collect relevant data, for example field performance history of similar systems Identify applicable maintenance and support policies and practices Predict dependability implications of design concepts Establish supply chain management plan Commence preparation of dependability plan Obtain agreements relating to dependability

Stage	Outcomes or project tasks	Dependability focus
Development	Plan system design and integration of modules Plan and execute selected design solution(s) Source components Develop engineering models Construct prototypes Assess and treat risks of selected design Verify and validate design	Influence design to enhance dependability Identify impact of interfaces on dependability Undertake trade-off studies Establish test plan Obtain data for reliability of components or subsystems as input to characterising reliability Undertake detailed failure analysis and check failure modes are adequately controlled Identify and assess risks including risks during realization, operation and retirement Plan maintenance and support Analyse life cycle costs Plan obsolescence management Undertake simulations, analysis and tests related to dependability attributes Estimate dependability attributes and compare with requirements Develop and test prototypes or subsystems Apply modelling and probabilistic approaches to predict and improve dependability as design progresses Plan failure response and recovery strategies Provide assurance concerning dependability Review and improve dependability

Stage	Outcomes or project tasks	Dependability focus
Realization (the make and buy decisions for manufacture or purchase)	Source supplies Manufacture or purchase product Install and integrate into existing systems Undertake tests and analysis Validate performance Demonstrate performance is achieved Obtain acceptance Prepare documentation	Control quality of manufacture Ensure conformance to established processes Predict, analyse and measure dependability as appropriate to verify requirements are met Test to check that manufacturing and installation processes are preserving the design dependability characteristics Test for early failures Set up maintenance agreements Plan spare parts provisioning Prepare documents relating to operation, maintenance and support Assess and monitor risks under actual conditions Address any non-conformances
Utilization	Operate, maintain and support system Provide training Measure and monitor performance Quality assurance Identify changes that could affect performance Undertake stakeholder satisfaction surveys Manage risk Recommend design or procedural changes for continual improvement	Assess risks of utilization in more detail Sustain performance through maintenance and support Verify dependability targets through analysis and test Monitor dependability achievement Collect data on in service dependability Analyse any failures and non-conformances and respond to them Monitor changes that might affect dependability Analyse dependability implications of change and adapt as required. Perform regression tests
Enhancement	Consult with stakeholders Identify objectives of enhancement and the changes needed Evaluate need for change and resulting benefits Identify risks of change and not changing and incorporate in cost-benefit analysis of the change	Evaluate implications of planned change for dependability Repeat relevant activities that can be influenced by the change (e.g. FMEA or tests) Determine reliability growth for design changes and new software versions Perform regression tests
Retirement and re-use	Communicate with stakeholders Implement retirement strategy Re-use items as appropriate	Archive dependability data as required Identify dependability issues of recycle and re-use of components Record learnings

Annex F
(informative)

Comparison of approach of ISO/IEC/IEEE 15288 with that of IEC 60300-1

F.1 Overview

This annex compares the approach taken in this document with that of ISO/IEC/IEEE 15288 to assist those who are more familiar with the life cycle process approach or wish to apply both standards.

F.2 Concept of system life cycle processes

ISO/IEC/IEEE 15288 describes a set of system life cycle processes together with activities and tasks to achieve the defined purpose of each process (see Figure F.1). Each life cycle process can be undertaken at any stage in a life cycle model. Processes, activities and tasks are selected to fit a particular context.

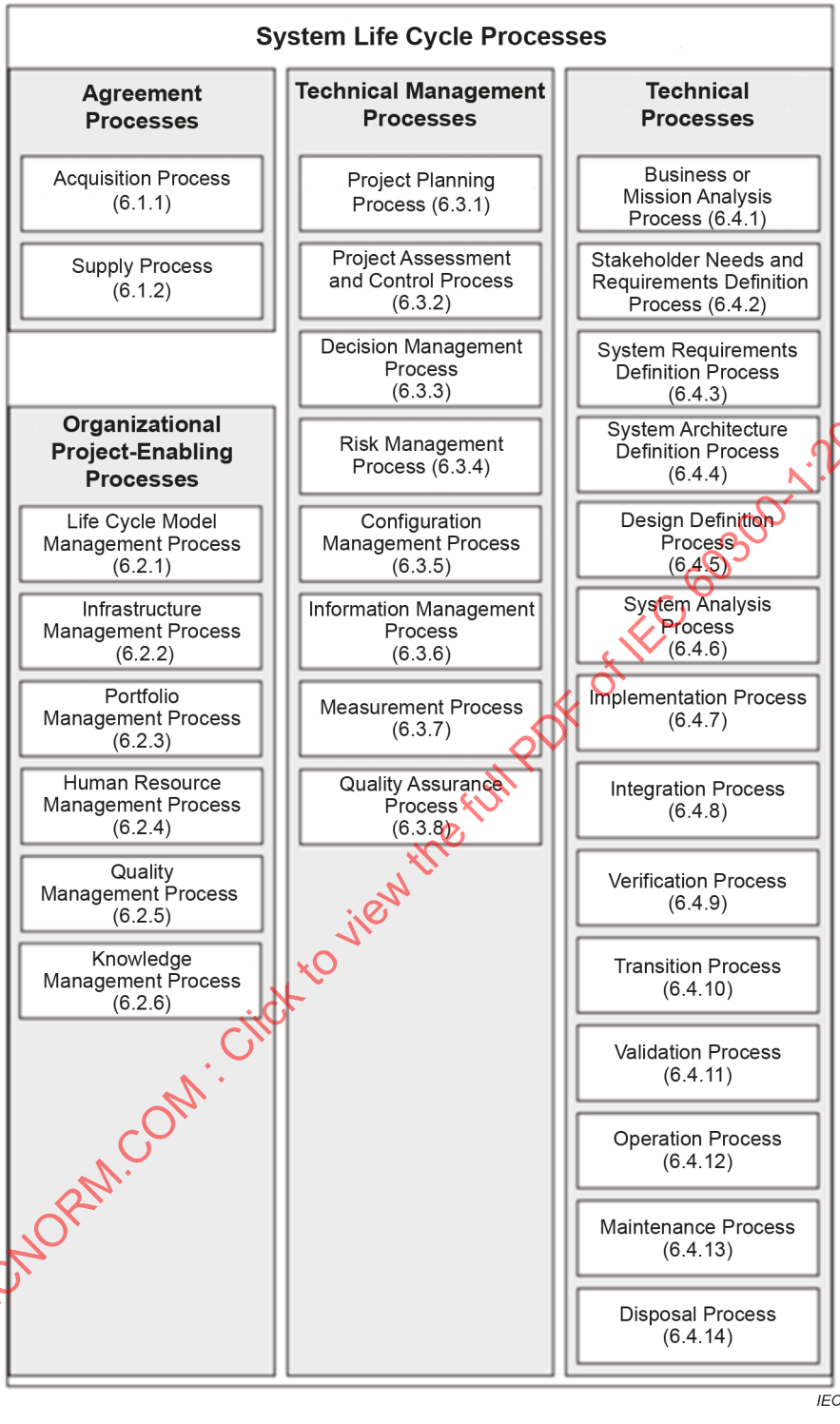
The dependability activities described in this document are also undertaken at any stage in a life cycle model. They form a set of dependability activities that are likely to be found in any dependability programme.

The tasks of the dependability activities in this document are equivalent to, or specialized instances of, tasks within the activities of different life cycle processes within ISO/IEC/IEEE 15288. To that extent each dependability activity can be considered to be a process view as defined in ISO/IEC/IEEE 15288 and described in more detail in ISO/IEC/IEEE 24748-1. The process view name, purpose and outcomes, are equivalent to the name, purpose and outcomes of the dependability activities of Clause 7 and Clause 8. For example the life cycle processes from which activities and tasks can be selected to fulfil the purpose and outcomes for the dependability activity of the "dependability" analysis (see 8.4 and Table F.1) include the following:

- systems analysis processes;
- project assessment and control process;
- risk management process;
- information management process.

The system life cycle processes of ISO/IEC/IEEE 15288 are provided in a general context without focussing on any attribute, while the dependability activities of this document focus on dependability. The tasks of a dependability activity in this document are thus described more specifically for the dependability context and objectives with a higher level of detail than is appropriate for the general level. For example ISO/IEC/IEEE 15288 describes the tasks for undertaking any analysis process including analyses relating to dependability. These tasks apply to how analysis is undertaken. This document defines the particular analyses that can be needed within a dependability programme to achieve dependability objectives and describes what analyses can be undertaken. This is illustrated in Table F.1.

IEC dependability standards provide the tools and application details that enable dependability tasks to be undertaken. More detailed mapping between ISO/IEC/IEEE 15288, the ISO 55000 series (asset management) and dependability standards is given in IEC TS 62775.



NOTE The subclauses referenced in Figure F.1 refer to the subclause numbers in ISO/IEC/IEEE 15288:2023.

SOURCE: Reproduced from ISO/IEC/IEEE 15288:2023, Figure 4.

Figure F.1 – System life cycle processes according to ISO/IEC/IEEE 15288

Table F.1 – Comparison of approach of ISO/IEC/IEEE 15288 and IEC 60300-1

Analysis activity according to IEC 60300-1	System analysis process according to ISO/IEC/IEEE 15288
Outcomes	**Outcomes**
A technical understanding of the product or system is obtained	System analyses needed are identified
Dependability, cost and risk characteristics of design options are predicted and compared	System analysis assumptions and results are validated
A cost effective design is selected that can be demonstrated to achieve requirements	Systems analysis results are provided for decisions or technical assessment needs
Assurance is provided that stakeholder needs and requirements for dependability are met	Enabling systems or services needed for system analysis are available
The system is designed with consideration of its eventual retirement	Traceability of the system analysis results is established
Potential failure modes are identified so they can be prevented or their effects mitigated	
Cost implications of decisions relating to dependability are understood	
Factors affecting reliability, maintainability and supportability and other dependability related attributes are understood and trade-off decisions made	
The roles of hardware, software and people in the system are optimized	
Systems are retired in a way that is safe, environmentally sound and in line with legislation and standards	

Analysis activity according to IEC 60300-1	System analysis process according to ISO/IEC/IEEE 15288
Tasks for analysis activity in IEC 60300-1	**Tasks for the activities "*Prepare for system analysis*" and "*Perform system analysis*" according to ISO/IEC/IEEE15288:2023, 6.4.6.3**
Predict values for dependability attributes	Define system analysis strategy
Undertake an iterative process of analysis and improvement as the design progresses	Identify problem that requires analysis
Perform regression analysis to verify that changes have not affected existing functionality	Identify stakeholders of the system analysis
Undertake life cycle cost analysis to optimize dependability within cost constraints	Define scope objectives and level of fidelity of the system analysis
Conduct trade-off analyses	Select the system analysis methods
Analyse failure modes, causes and effects in order to improve designs and plan maintenance and support programmes and failure response	Identify and plan for necessary enabling systems or services needed to support systems analysis
Analyse the system, product or service by modelling stress conditions and corrupted or illegal data inputs	Obtain or acquire access to enabling systems or services to be used
Analyse the effect of human performance upon the dependability programme	Identify and validate assumptions
Analyse processes used in manufacture, delivery and installation	Plan for and collect data and inputs need for analysis
Analyse design changes for safety and operability and to check intended improvements will be achieved	Apply selected analysis methods to perform the required system analysis
Analyse causes of failures including organizational failures (see IEC 62740)	Review the analysis results for quality and validity
Analyse system prior to retirement for potential re-use	Establish conclusions and recommendations
	Record the results of system analysis
	Maintain traceability of system analysis results
	Provide key artefacts that have been selected for baselines

Annex G
(informative)

Testing

G.1 General

A test is a procedure carried out to determine one or more characteristics. Tests can be carried out at any stage of the life cycle, however it has been proven that testing as early as possible can save time and reduce overall development costs.

Testing by inserting correct inputs to obtain a correct output is only part of the test. Observing the effects of incorrect inputs and from this changing the design can have great benefit later in the life cycle.

Testing requires the following factors to be considered:

- the purpose and objectives of the test (see 8.4.1);
- the type of tests and test conditions needed to fulfil those objectives;
- the time by which test results are required in order to influence decisions;
- the quality and quantity of input data needed;
- the quality and quantity of output data required to satisfy the goal;
- the level of progressive data required to be stored.

G.2 Purpose and objectives of tests

In general tests are carried out to:

- support verification and validation;
- to compare the dependability of products or product designs;
- to monitor on-going performance;
- to discover and eliminate weaknesses and hence improve performance and reduce costs.

G.3 Test conditions

Tests can be carried out under controlled conditions (e.g. in a laboratory) or can be carried out during operation.

When collecting data from a system during operation the following needs to be considered:

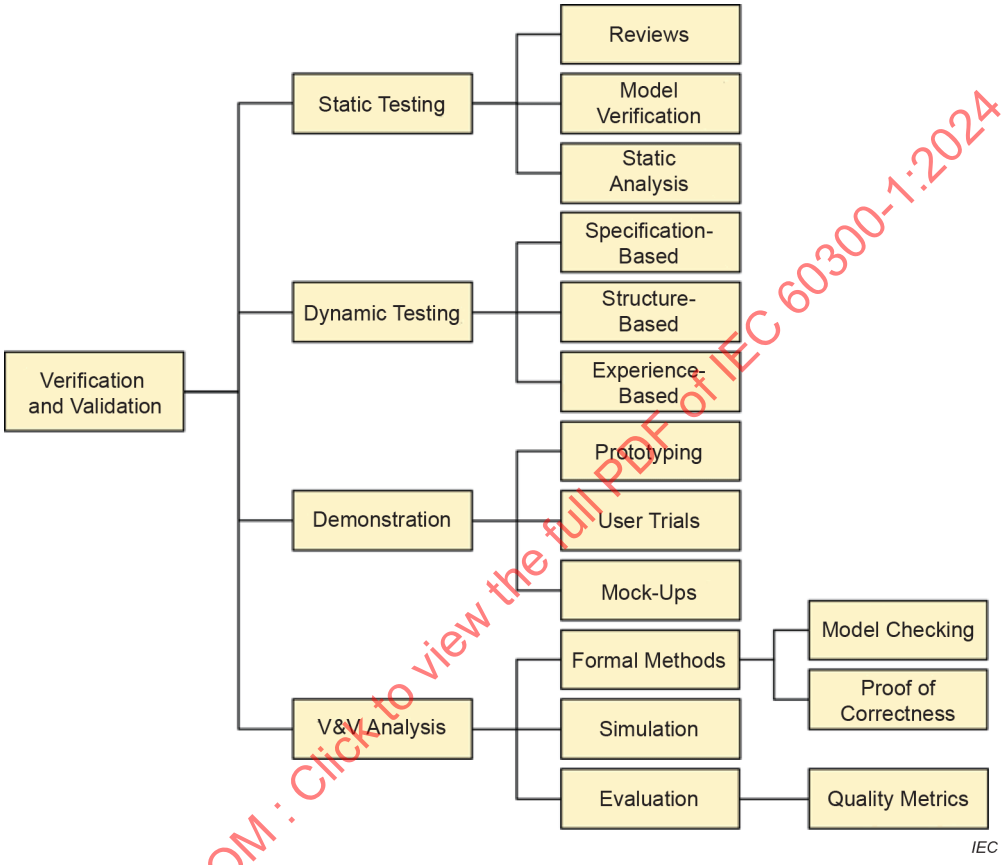
- the conditions and limitations of field data (e.g. the extent to which actual conditions match those assumed during design);
- how much contextual information is required;
- how incomplete data is addressed.

  For example data can be collected from customer surveys, warranty data or systems and products which are returned to the manufacturer for repair. Such data should be analysed with great care to give information that applies across the population of products. They are nevertheless crucial for monitoring the performance of a product under actual conditions of use;
- how changes to the design baselines, maintenance and manufacturing practices over time are accounted for.

Guidelines for planning and performing reliability tests are described in IEC 60300-3-5 and tests for availability in IEC 61070.

G.4 Types of test

ISO/IEC/IEEE 29119-1 describes types of tests carried out to support verification and validation of software (see Figure G.1). A similar categorization can also be applied to any system, product or service.



SOURCE: Reproduced from ISO/IEC/IEEE 29119-1:2022, Figure 1.

Figure G.1 – Verification and validation methods or practices

Testing encompasses hardware, software, products and services. Static testing of software is the evaluation of a test item where no execution of the code takes place. The test item can take the form of documentation or source code. Static testing can be performed anywhere in the life cycle.

Software static testing includes reviews and static analysis. Reviews and example review types relevant to software are described in ISO/IEC 20246. Static analysis involves the use of software tools to detect anomalies in program code or documents without execution of the code (e.g. a compiler, a cyclomatic complexity analyser, or a security analyser for code).

For systems, products and services other than software, static tests can be carried out to ensure that the relevant design rules have been correctly followed. For example this could involve checking that designers' calculations have complied with accepted practice or that models used in analysis are valid. A similar approach occurs in manufacturing. For example a "bed of nails" test is used to check that the components in a circuit board are the correct components and are in the correct orientation.

Dynamic testing in software involves confirming the functioning of the software by executing the code and running test cases or simulating an operational load, for example overload/surge tests. Dynamic testing can thus only occur in the parts of the life cycle when an executable test item is available. Three test design-techniques are defined and fully described in ISO/IEC/IEEE 29119-4. These depend on whether the basis for the choice of test cases is the specification (e.g. requirements or user needs), the structure (e.g. the source code) or the knowledge and experience of the tester. These classes of test design techniques are complementary and their combined application typically results in more effective testing.

For other systems, products and services dynamic tests are carried out to confirm functions. This usually starts with small items and increases in complexity as these are integrated to produce a system. In the early stages, it can be necessary to develop pseudo interfaces to enable the testing of the item's functions and it is important that the functions and interfaces for the small item are clearly defined.

If the system, product or service fails a test it can be necessary to carry out diagnostic tests or debugging to identify the cause of the fault. After correcting a fault, previous tests can have to be repeated (regression testing). Testing can also cover maintainability functions and operator functions, such as testing with "What if" scenarios.

Tests can be simple or highly complex. For example a drop test can involve dropping an item from a fixed height and inspecting for signs of damage. Alternatively, it can involve testing to establish that all individual components continue to function correctly.

G.5 Data quality and quantity

The quality and quantity of input data is an important consideration, but the axiom "more is better" is not always the best approach as it can become a time-consuming process. In some cases it might not be possible to cover all possible eventualities and in these cases, certain extreme events can be considered and special tests developed. For example, to prove by dynamic testing that a software item meets all requirements under all given circumstances would require all possible combinations of input values in all possible states to be tested. This is impractical so test cases are selected. The selection of test cases highly influences the risk of the item failing, so selection should take account of the risks involved. Test case testing should be supplemented by tests with simulated or actual operational load, for example beta-tests.

For high reliability hardware items the failure rate can be extremely low under normal working conditions and the time to demonstrate reliability to the required level of confidence can be impracticably long. In this case action can be taken to force the item to fail within a convenient time period. Increased failure rates are achieved by applying controlled stress, for example accelerated testing aims to subject a hardware product to stresses that would produce the cumulative damage expected over its operating life (see IEC 62506).

Stress testing can also be applied to software where the objective is to evaluate the test item's behaviour under conditions of loading above that anticipated or with resources below minimum specified requirements.

The quality and quantity of output data will depend on the purpose and objective of the test. For example, when an item has been manufactured, it is tested to confirm that all functions are operational (this is not the same as validating that all functions meet stakeholder needs). While the item is in operation functions selected through reliability centred maintenance analysis might be periodically tested as part of failure finding or condition monitoring (see IEC 60300-3-11)

The level of progressive data relates to the amount of data that is progressively stored whilst the system continues to operate or sometimes to the amount of data stored as the system undergoes testing. An example is the flight recorder carried by all aircraft which is recovered after an accident to help establish the cause. During development progressive data collection can be used to help locate the cause of a failure.

During operation measures and test protocols are defined that will provide insight into performance levels. Data is collected to confirm whether dependability requirements continue to be met within acceptable limits and to detect any changes that can indicate, for example, wear out or the presence of latent faults.

Bibliography

IEC 31010, *Risk management – Risk assessment techniques*

IEC 60050-192:2015, *International Electrotechnical Vocabulary (IEV) – Part 192: Dependability* (available at www.electropedia.org)

IEC 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60300-3-3, *Dependability management – Part 3-3: Application guide –. Life cycle costing*

IEC 60300-3-4, *Dependability management – Part 3-4: Application guide –Specification of dependability requirements*

IEC 60300-3-5, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

IEC 60300-3-10, *Dependability management – Part 3-10: Application guide – Maintainability and maintenance*

IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

IEC 60300-3-12, *Dependability management – Part 3-12: Application guide – Integrated logistic support*

IEC 60300-3-14:–, *Dependability management – Part 3-14: Application guide – Supportability and support*

IEC 60300-3-16, *Dependability management – Part 3-16: Application guide – Guidelines for specification of maintenance support services*

IEC 60605 (all parts), *Equipment reliability testing*

IEC 60605-2, *Equipment reliability testing – Part 2: Design of test cycles*

IEC 60605-4, *Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals*

IEC 60605-6, *Equipment reliability testing – Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity*

IEC 60706-2, *Maintainability of equipment – Part 2: Maintainability requirements and studies during the design and development phase*

IEC 60706-3, *Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data*

IEC 60706-5, *Maintainability of equipment – Part 5: Testability and diagnostic testing*

IEC 60812, *Failure modes and effects analysis (FMEA and FMECA)*

IEC 61014, *Programmes for reliability growth*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61070, *Compliance test procedures for steady state availability*

IEC 61078, *Reliability block diagrams*

IEC 61123, *Reliability testing – Compliance test plans for success ratio*

IEC 61124, *Reliability testing – Compliance tests for constant failure rate and constant failure intensity*

IEC 61163-1, *Reliability stress screening – Part 1: Repairable assemblies manufactured in lots*

IEC 61163-2, *Reliability stress screening – Part 2: Components*

IEC 61165, *Application of Markov techniques*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61649, *Weibull analysis*

IEC 61650, *Reliability data analysis techniques – Procedures for comparison of two constant failure rates and two constant failure (event) intensities*

IEC 61703, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms*

IEC 61709, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*

IEC 61710, *Power law model – Goodness-of-fit tests and estimation methods*

IEC 61709, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*

IEC 61710, *Power law model – Goodness-of-fit tests and estimation methods*

IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

IEC 61907, *Communication network dependability engineering*

IEC 62198, *Managing risk in projects – Application guidelines*

IEC 62308, *Equipment reliability – Reliability assessment methods*

IEC 62309, *Dependability of products containing reused parts – Requirements for functionality and tests*

IEC 62402, *Obsolescence management*

IEC 62502, *Analysis techniques for dependability – Event tree analysis (ETA)*

IEC 62506, *Methods for product accelerated testing*

IEC 62508, *Guidance on human aspects of dependability*

IEC 62550, *Spare parts provisioning*

IEC 62551, *Analysis techniques for dependability – Petri net techniques*

IEC 62628, *Guidance on software aspects of dependability*

IEC 62673, *Methodology for communication network dependability assessment and assurance*

IEC 62740, *Root cause analysis (RCA)*

IEC 62741:2015, *Demonstration of dependability requirements – The dependability case*

IEC TS 62775, *Application guidelines – Technical and financial processes for implementing asset management systems*

IEC 62853, *Open systems dependability*

IEC 62960, *Dependability reviews during the life cycle*

IEC TR 63039, *Probabilistic risk analysis of technological systems – Estimation of final event rate at a given initial state*

IEC 80001-1, *Application of risk management for IT-networks incorporating medical devices – Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software*

ISO/IEC Directives Part 1:2022, *Consolidated ISO Supplement – Procedure for the technical work – Procedures specific to ISO*

ISO Guide 73:2009, *Risk management – Vocabulary*

ISO Guide 82:2019, *Guidelines for addressing sustainability in standards*

ISO Guide 99:2007, *International vocabulary of metrology – Basic and general concepts and associated terms (VIM)*

ISO 9001, *Quality management systems – Requirements*

ISO 9241-210:2019, *Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems*

ISO 15489-1, *Information and documentation – Records management – Part 1: Concepts and principles*

ISO/IEC/IEEE 14764, *Software engineering – Software life cycle processes – Maintenance*

ISO/IEC/IEEE 15026 (all parts), *Systems and software engineering – Systems and software assurance*

ISO/IEC/IEEE 15026-1:2019, *Systems and software engineering – Systems and software assurance – Part 1: Concepts and vocabulary*

ISO/IEC/IEEE 15026-2, *Systems and software engineering – Systems and software assurance – Part 2: Assurance case*

ISO/IEC/IEEE 15026-4, *Systems and software engineering – Systems and software assurance – Part 4: Assurance in the life cycle*

ISO/IEC/IEEE 15288:2023, *Systems and software engineering – System life cycle processes*

ISO/IEC/IEEE 15289, *Systems and software engineering – Contents of life cycle information items (documentation)*

ISO/IEC 20246, *Software and systems engineering – Work product reviews*

ISO 20815, *Petroleum, petrochemical and natural gas industries – Production assurance and reliability management*

ISO/IEC/IEEE 24748-1, *Systems and software engineering – Life cycle management – Part 1: Guidelines for life cycle management*

ISO/IEC/IEEE 24765:2017, *Systems and software engineering – Vocabulary*

ISO/IEC 25010, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*

ISO/IEC 25023, *Systems and software engineering – System and software Quality Requirements and Evaluation (SQuaRE) – Measurement of system and software product quality*

ISO/IEC 25064, *Systems and software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Common Industry Format (CIF) for usability: User needs report*

ISO/IEC/IEEE 29119 (all parts), *Software and systems engineering – Software testing*

ISO/IEC/IEEE 29119-1:2022, *Software and systems engineering – Software testing – Part 1: General concepts*

ISO/IEC/IEEE 29119-4, *Software and systems engineering – Software testing – Part 4: Test techniques*

ISO/IEC/IEEE 29148:2018, *Systems and software engineering – Life cycle processes – Requirements engineering*

ISO 26000:2010, *Guidance on social responsibility*

ISO 26262 (all parts), *Road vehicles – Functional safety*

ISO/IEC 30145-2:2020 *Information technology – Smart City ICT reference framework – Part 2: Smart city knowledge management framework*

ISO 31000, *Risk management – Guidelines*

ISO 55001, *Asset management – Management systems – Requirements*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 1: Gérer la sûreté de fonctionnement

AVANT-PROPOS

1) La Commission Électrotechnique 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. À 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'IEC attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'IEC ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de propriété revendiqué à cet égard. À la date de publication du présent document, l'IEC n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse https://patents.iec.ch. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevet.

L'IEC 60300-1 a été établie par le comité d'études 56 de l'IEC: Sûreté de fonctionnement. Il s'agit d'une Norme internationale.

Cette quatrième édition annule et remplace la troisième édition parue en 2014. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) davantage de recommandations sur l'intégration des activités de sûreté de fonctionnement dans un système de gestion existant;
b) plus de détails sur les activités exigées pour établir et mettre en œuvre un programme d'activités de sûreté de fonctionnement;
c) modifications visant à assurer la cohérence avec d'autres normes de sûreté de fonctionnement.

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

Projet	Rapport de vote
56/2031/FDIS	56/2044/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

La version française de cette norme n'a pas été soumise au vote.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications.

Une liste de toutes les parties de la série IEC 60300, publiées sous le titre général *Gestion de la sûreté de fonctionnement*, se trouve sur le site Web de l'IEC.

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 webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera:

- reconduit,
- supprimé, ou
- révisé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de ce document 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 l'aptitude à fonctionner quand et tel qu'exigé. Une entité fiable est une entité en laquelle il existe une confiance légitime qu'elle fonctionne comme souhaité et satisfait aux besoins et attentes convenus des parties prenantes. La sûreté de fonctionnement comporte de nombreux attributs, mais elle est généralement caractérisée en matière de fiabilité, de maintenabilité et de supportabilité, ainsi que la disponibilité résultante. Dans certains cas, des attributs tels que la résilience, la récupérabilité, la durabilité, l'intégrité, la sécurité, la sûreté et la véracité sont inclus dans la sûreté de fonctionnement ou la recoupe.

La spécification et la vérification des attributs de sûreté de fonctionnement donnent aux parties prenantes l'assurance que les exigences seront satisfaites à l'avenir et que la qualité sera maintenue au fil du temps. La sûreté de fonctionnement d'un système, produit ou service influence les stratégies d'entreprise associées à sa conception, son acquisition et son utilisation, ainsi que ses coûts du cycle de vie. La sûreté de fonctionnement des systèmes, produits et services d'un organisme a un fort impact sur la perception de la valeur et de la véracité de l'organisme.

La sûreté de fonctionnement est gérée comme élément clé des systèmes de gestion plus larges d'un organisme, en particulier les aspects relatifs aux biens, à la qualité et à la finance.

Le présent document souligne l'importance et les avantages de la gestion de la sûreté de fonctionnement. Il donne des recommandations sur les activités de sûreté de fonctionnement et sur l'intégration de celles-ci dans un système de gestion et des processus du cycle de vie existants, afin d'obtenir une approche significative, efficace et économique.

Les activités de sûreté de fonctionnement procurent des avantages chaque fois qu'elles sont réalisées, mais plus leur mise en œuvre est précoce dans le cycle de vie, plus les avantages sont importants.

Le présent document est applicable à un large éventail de secteurs professionnels et d'organismes de toute taille. Il s'applique aux systèmes de systèmes, aux grands systèmes uniques, aux produits industriels et de consommation fabriqués en série, aux applications logicielles, aux composants et aux services. Ces catégories ne sont pas mutuellement exclusives. Par exemple, de nombreux produits et composants sont eux-mêmes des systèmes complexes.

Le document est utile pour:

- les responsables et le personnel technique;
- les personnes qui participent à la détermination de la façon dont leurs systèmes, produits et services peuvent être rendus fiables;
- des organismes tels que des organismes de réglementation qui évaluent la sûreté de fonctionnement des systèmes, produits et services;
- les personnes (par exemple les utilisateurs ou le public) qui ont besoin d'une confiance légitime dans les systèmes, produits et services susceptibles de les affecter;
- les normalisateurs d'autres normes relatives à la sûreté de fonctionnement.

Le présent document fait partie d'une série de normes de sûreté de fonctionnement de l'IEC reliées de niveau supérieur qui fournissent aux responsables et au personnel technique des recommandations sur la façon de planifier et de mettre en œuvre efficacement les activités de sûreté de fonctionnement. Les autres documents de la série sont:

– l'IEC 60300-3-4 qui fournit des recommandations sur l'élaboration d'exigences de sûreté de fonctionnement dans les spécifications, et sur les moyens d'assurer la réalisation de ces exigences;
– l'IEC 60300-3-10 et l'IEC 60300-3-14 qui fournissent respectivement des recommandations sur la manière d'identifier et d'appliquer les techniques d'analyse et d'assurance appropriées pour la maintenabilité (et la maintenance) et la supportabilité (et le soutien) respectivement;
– des normes couvrant la fiabilité et la disponibilité sont prévues.

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 1: Gérer la sûreté de fonctionnement

1 Domaine d'application

Le présent document fournit des recommandations sur:

- la signification et l'importance de la sûreté de fonctionnement du point de vue commercial, technique et financier;
- l'obtention de la sûreté de fonctionnement par une adaptation appropriée des systèmes de management organisationnel, tels que ceux décrits dans la série ISO 9001 (management de la qualité) et dans la série ISO 55001 (gestion d'actifs);
- les activités qui sont intégrées dans les systèmes de management et les processus du cycle de vie afin d'obtenir des systèmes, produits et services fiables;
- la planification et la mise en œuvre d'activités de sûreté de fonctionnement tout au long du cycle de vie afin d'obtenir et d'assurer les résultats exigés, en tenant compte de facteurs tels que les coûts, la sécurité, l'environnement, la clientèle, la marque et la réputation.

Le présent document est applicable à tout type de système, neuf et existant, aux produits industriels ou de consommation fabriqués en série, aux composants et aux services. Le présent document traite de tous les éléments des systèmes, produits et services, y compris le matériel, les logiciels, les données, les processus, les procédures, les installations, les matériaux et le personnel exigé pour les opérations et le soutien.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils 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 60050-192:2015, *Vocabulaire Électrotechnique International (IEV) – Partie 192: Sûreté de fonctionnement* (disponible à l'adresse http://www.electropedia.org)

3 Termes, définitions et termes abrégés

Pour les besoins du présent document, les termes et les définitions de l'IEC 60050-192, ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/;
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp.

3.1 Termes et définitions

3.1.1
redevabilité
état consistant, pour un organisme, à être en mesure de répondre de ses décisions et activités à ses organes directeurs, ses autorités constituées et, plus largement, à ses parties prenantes et la société en général

Note 1 à l'article: la redevabilité implique, pour la direction, l'organisme et les individus, l'obligation de pouvoir répondre de l'impact de leurs décisions et activités sur les parties prenantes, la société et l'environnement. La redevabilité implique donc le fait d'être comptable envers la société en général.

Note 2 à l'article: La redevabilité implique que les personnes, les organisations et la communauté sont responsables de leurs actions et peuvent être tenues de les justifier à d'autres.

[SOURCE: ISO 26000:2010, 2.1, modifié – ajout de "et la société en général" à la définition et ajout des notes à l'article.]

3.1.2
adaptabilité
aptitude à s'adapter à des conditions changeantes ou à être modifié pour un objet particulier ou un environnement modifié

3.1.3
assurance
justifications pour une confiance légitime dans le fait que des performances ont été réalisées, le sont ou le seront

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.1.1]

3.1.4
disponibilité
aptitude à être en état de fonctionner tel que requis dans des conditions données

Note 1 à l'article: La disponibilité dépend des attributs combinés de fiabilité, de maintenabilité, de supportabilité, ainsi que de la maintenance et du soutien fournis.

Note 2 à l'article: La disponibilité peut également être affectée par des retards avant qu'il ne soit reconnu que la maintenance ou le soutien sont nécessaires, par exemple le temps de détection de pannes (192-06-18) et le délai administratif (192-07-12).

Note 3 à l'article: Les conditions données incluent les aspects ayant un impact sur la disponibilité, tels que le mode de fonctionnement, les niveaux de contrainte, les conditions environnementales et la maintenance définis dans le profil de cycle de vie.

Note 4 à l'article: La disponibilité peut être quantifiée à l'aide de mesures définies dans l'IEC 60050-192:2015, 192-08, *Mesures liées à la disponibilité*.

[SOURCE: IEC 60050-192:2015, 192-01-23, modifié – suppression de "d'une entité" et ajout de "dans des conditions données" dans la définition, modification de la Note 1 à l'article et ajout des Notes 2 et 3 à l'article.]

3.1.5
processus métier
ensemble partiellement ordonné d'activités d'entreprise interdépendantes qui peuvent être exécutées pour atteindre un résultat final souhaité en vue de la réalisation d'un objectif donné d'un organisme

Note 1 à l'article: Le terme "métier" est interprété au sens large, c'est-à-dire comme se référant aux activités liées à la finalité de l'organisme, que ce dernier soit public, privé, à but lucratif ou non lucratif.

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.445, modifié – ajout de la Note 1 à l'article.]

3.1.6
sûreté de fonctionnement
aptitude à fonctionner quand et tel que requis

Note 1 à l'article: Une entité ou un service fiable est celui pour lequel il existe une confiance légitime qu'il fonctionne comme souhaité et satisfait aux attentes convenues des parties prenantes.

Note 2 à l'article: Dans la plupart des cas, le terme de sûreté de fonctionnement est utilisé comme terme générique pour exprimer ses attributs centraux de fiabilité, de maintenabilité et de supportabilité, ainsi que la disponibilité résultante. Dans certains cas, des attributs tels que la résilience, la récupérabilité, la durabilité, l'intégrité, la sécurité, la sûreté et la véracité sont inclus dans la sûreté de fonctionnement ou la recoupe.

Note 3 à l'article: Afin d'exprimer la capacité d'exécution, les exigences en termes de fonctions à accomplir, lorsque la performance est à atteindre, et les conditions du profil de cycle de vie sont spécifiées par les clients, les utilisateurs ou les parties prenantes.

Note 4 à l'article: Les attributs de sûreté de fonctionnement peuvent être exprimés de manière qualitative ou quantitative.

Note 5 à l'article: Il est également courant d'utiliser le terme "sûreté de fonctionnement" dans le contexte d'un sujet d'étude ou de discipline.

[SOURCE: IEC 60050-192:2015, 192-01-22, modifié – suppression de "d'une entité", suppression des notes et ajout de nouvelles notes à l'article.]

3.1.7
activité de sûreté de fonctionnement
ensemble de tâches cohésives réalisées pour atteindre un objet lié à la sûreté de fonctionnement

Note 1 à l'article: Une activité de sûreté de fonctionnement peut être mise en correspondance avec une vision de processus qui utilise une combinaison de processus du cycle de vie, d'activités et de tâches dans la terminologie de l'ISO/IEC/IEEE 15288.

3.1.8
étude de sûreté de fonctionnement
argument basé sur des preuves, raisonné et traçable créé pour soutenir l'affirmation selon laquelle un système défini satisfait et/ou satisfera aux exigences de sûreté de fonctionnement

Note 1 à l'article: Une étude de sûreté de fonctionnement est un argumentaire pour les affirmations relatives à la sûreté de fonctionnement, voir ISO/IEC/IEEE 15026-2.

[SOURCE: IEC 62741:2015, 3.1.1, modifié – ajout de la Note 1 à l'article.]

3.1.9
plan de sûreté de fonctionnement
entité d'information qui présente une conduite systématique pour atteindre un objet déclaré relatif à la sûreté de fonctionnement, ainsi que le moment auquel des tâches spécifiques sont à exécuter, la manière de le faire et les personnes qui en sont chargées

3.1.10
durabilité
aptitude à fonctionner tel que requis, dans des conditions données d'utilisation et de maintenance, jusqu'à l'état final défini

Note 1 à l'article: Le degré dans lequel la maintenance et la réparation entrent dans le domaine d'application de la durabilité varie en fonction du produit ou de la catégorie de produits.

Note 2 à l'article: L'état final peut être basé sur des aspects technologiques, sociaux ou économiques.

Note 3 à l'article: La durabilité peut être exprimée en unités appropriées à la pièce ou au produit concerné, par exemple le temps calendaire, les cycles de fonctionnement, la distance parcourue, etc. ou la probabilité de pouvoir atteindre une période d'utilisation donnée. Il convient de toujours énoncer clairement les unités.

Note 4 à l'article: La durabilité en tant que mesure se rapporte à la longévité de l'intervalle.

[SOURCE: IEC 60050-192:2015, 192-01-21, modifié – remplacement de "la fin de la vie utile" par "l'état final défini", et ajout des notes à l'article.]

3.1.11
intégrité
<en sûreté de fonctionnement> aptitude à empêcher ou à résister à une modification non autorisée

Note 1 à l'article: La modification peut concerner le matériel, les logiciels ou les données.

3.1.12
profil de cycle de vie
contraintes et leurs niveaux, contenu, durée et ordre, rencontrés pendant le cycle de vie d'une entité

Note 1 à l'article: Les contraintes peuvent être internes (telles que cycles de fonctionnement) ou externes (telles que contrainte environnementale, niveau de puissance d'entrée ou le taux de demandes de service sur un réseau).

Note 2 à l'article: Le profil de cycle de vie peut être réel, attendu ou prévu.

3.1.13
maintenabilité
aptitude à être maintenu ou rétabli dans un état permettant de fonctionner tel que requis, dans des conditions données

Note 1 à l'article: Les conditions données incluent notamment l'emplacement de maintenance, l'accessibilité, les procédures de maintenance et les ressources de maintenance, ainsi que celles définies dans le profil de cycle de vie.

Note 2 à l'article: La maintenabilité peut être quantifiée à l'aide de mesures appropriées. voir IEC 60050-192:2015, 192-07, *Maintenabilité et logistique de maintenance: mesures*.

3.1.14
mesurage
mesure
processus consistant à obtenir expérimentalement une ou plusieurs valeurs que l'on peut raisonnablement attribuer à une grandeur

Note 1 à l'article: Les mesurages ne s'appliquent pas aux propriétés qualitatives.

Note 2 à l'article: Un mesurage implique la comparaison de grandeurs, y compris le comptage d'entités.

Note 3 à l'article: Un mesurage suppose une description de la grandeur compatible avec l'usage prévu d'un résultat de mesure, une procédure de mesure et un système de mesure étalonné fonctionnant selon la procédure de mesure spécifiée, incluant les conditions de mesure.

Note 4 à l'article: Le mot "mesure" a, dans la langue française courante, plusieurs significations. C'est la raison pour laquelle le mot "mesurage" a été introduit pour qualifier l'action de mesurer. Le mot "mesure" intervient cependant à de nombreuses reprises pour former des termes de ce Vocabulaire, suivant en cela l'usage courant et sans ambiguïté. En voici quelques exemples: unité de mesure, méthode de mesure, instrument de mesure. Cela ne

signifie pas que l'utilisation du mot "mesurage" au lieu de "mesure" pour ces termes ne soit pas admissible si elle s'avère avantageuse.

[SOURCE: ISO/IEC GUIDE 99:2007, 2.1, modifié – ajout de la Note 4 à l'article.]

3.1.15
besoin
prérequis identifié comme nécessaire pour obtenir un résultat visé, implicite ou explicite dans un contexte d'utilisation donné

3.1.16
fiabilité
aptitude à fonctionner tel que requis, sans défaillance, pendant un intervalle donné et dans des conditions données

Note 1 à l'article: L'intervalle peut être exprimé en unités appropriées à l'entité concernée, par exemple, temps calendaire, cycles de fonctionnement, distance parcourue, etc. Il convient de toujours énoncer clairement les unités.

Note 2 à l'article: Les conditions données incluent les aspects ayant un impact sur la fiabilité, tels que: le mode de fonctionnement, les niveaux de contrainte, les conditions environnementales et la maintenance.

Note 3 à l'article: La fiabilité peut être quantifiée à l'aide de mesures définies dans l'IEC 60050-192:2015, 192-05, *Concepts liés à la fiabilité: mesures*.

[SOURCE: IEC 60050-192:2015, 192-01-24, modifié – suppression de "d'une entité" et "de temps" dans la définition.]

3.1.17
exigence
<en sûreté de fonctionnement> déclaration qui traduit ou exprime un besoin et ses contraintes et conditions qui y sont associées

Note 1 à l'article: Les exigences se retrouvent à différents niveaux de la structure du système.

Note 2 à l'article: Une exigence est l'expression d'un ou plusieurs besoins particuliers d'une manière très spécifique, précise et explicite.

Note 3 à l'article: Une exigence se rapporte toujours à un système, un logiciel ou un service, ou toute autre entité considérée.

Note 4 à l'article: Une exigence est une déclaration pour laquelle une preuve ou une assurance de conformité peut être fournie.

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.19, modifié – ajout de la Note 4 à l'article.]

3.1.18
risque
effet de l'incertitude sur les objectifs

Note 1 à l'article: Un effet est un écart par rapport à un attendu. Il peut être positif, négatif ou les deux à la fois, et traiter, créer ou entraîner des opportunités et des menaces.

Note 2 à l'article: Les objectifs peuvent avoir différents aspects, être de catégories différentes, et peuvent concerner différents niveaux.

Note 3 à l'article: Un risque est généralement exprimé en termes de sources de risque, événements potentiels avec leurs conséquences et leur vraisemblance.

[SOURCE: ISO 31000:2018, 3.1]

3.1.19
sécurité
absence de risque inacceptable d'une blessure physique ou d'une atteinte à la santé des personnes ou de dommages sur les biens ou l'environnement

3.1.20
sûreté
protection contre les subversions intentionnelles ou la défaillance forcée

3.1.21
spécification
<en sûreté de fonctionnement> information qui définit les exigences de sûreté de fonctionnement et les objectifs d'un système, produit ou service, ainsi que toute information complémentaire

Note 1 à l'article: Les informations complémentaires peuvent inclure des informations d'utilisation, des conditions de fonctionnement et environnementales, des critères de défaillance et les méthodes prévues pour l'assurance de la conformité aux exigences, y compris les critères d'acceptation ou de rejet.

Note 2 à l'article: L'ISO/IEC/IEEE 15289 définit une spécification comme une information qui définit de manière exhaustive, précise et vérifiable les exigences, la conception, le comportement ou d'autres caractéristiques prévues du système, du service ou du processus. La spécification de la sûreté de fonctionnement a un domaine d'application plus large que celui utilisé dans l'ISO/IEC/IEEE 15289.

3.1.22
partie prenante
personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité

EXEMPLE: Utilisateurs finals, organismes utilisateurs finals, logisticiens, développeurs, producteurs, formateurs, techniciens d'entretien, agents chargés de la mise au rebut, acquéreurs, organismes fournisseurs et organismes de réglementation.

Note 1 à l'article: Certaines parties prenantes peuvent avoir des intérêts contraires.

[SOURCE: ISO Guide 73:2009, 3.2.1.1, modifié – ajout de l'exemple et reformulation de la Note 1 à l'article.]

3.1.23
soutien
<en sûreté de fonctionnement> mise à disposition des ressources permettant à une entité de continuer à fonctionner tel que requis

Note 1 à l'article: Des exemples de ressources sont l'effort humain, la formation, les outils, les gabarits, les équipements d'essai, les matériels de levage, les matériaux, les pièces de rechange, les installations, la documentation, les informations et les systèmes d'information.

Note 2 à l'article: Le soutien vise à fournir une ressource de qualité au bon emplacement, au meilleur moment et au coût optimal, en tenant compte des impacts environnementaux, sociaux et économiques.

3.1.24
supportabilité
aptitude d'une entité à être maintenue pour fonctionner tel que requis avec un profil de cycle de vie défini et des ressources données

3.1.25
système
combinaison de parties en interaction qui ont collectivement un ou plusieurs objets

Note 1 à l'article: Un système est parfois considéré comme un produit ou comme le service qu'il fournit.

Note 2 à l'article: Les parties peuvent inclure l'équipement associé, les installations, le matériel, les programmes informatiques, les micrologiciels, la documentation technique, d'autres systèmes, les services et le personnel exigés.

3.1.26
utilisabilité
degré selon lequel un système, un produit ou un service peut être utilisé, par des utilisateurs spécifiés, pour atteindre des buts définis avec efficacité, efficience et satisfaction, dans un contexte d'utilisation spécifié

[SOURCE: ISO 9241-210:2019, 3.13, modifié – omission des notes à l'article.]

3.1.27
vie utile
intervalle entre la première utilisation définie d'une entité et un état final défini, atteint en raison de l'obsolescence des performances ou d'autres facteurs

Note 1 à l'article: La première utilisation doit être définie. La première utilisation exclut, dans ce contexte, les essais préalables à la livraison de l'entité à l'utilisateur final. La première utilisation peut commencer après une période initiale de mortalité précoce.

Note 2 à l'article: L'état final est à définir et peut inclure des marges de sécurité qui empêchent l'apparition d'une défaillance ou des pourcentages de défaillances accumulées.

Note 3 à l'article: L'intervalle applicable est exprimé en unités appropriées à l'entité concernée, par exemple, temps calendaire, cycles de fonctionnement, distance parcourue, etc. Il convient d'énoncer clairement les unités.

Note 4 à l'article: Dans certains cas, la vie utile d'une entité est plus longue que celle exigée par l'organisme, auquel cas elle a une valeur résiduelle et peut être réutilisé.

3.2 Termes abrégés

AI	Intelligence artificielle
ASIL	Automotive Safety Integrity Level (niveau d'intégrité de sécurité automobile)
CMM	Capability Maturity Model (modèle d'évolution des capacités)
DRACAS	Data Reporting, Analysis and Corrective Action System (système d'enregistrement des données et de mesures correctives)
AMDE	Analyse des modes de défaillance et de leurs effets
LTIAC	Logique de traitement des incidents et actions correctives
HAZOP	HAZard and Operability studies (études de danger et d'exploitabilité)
IAS	International Accounting Standards (normes comptables internationales)
IFRS	International Financial Reporting Standards (normes internationales d'information financière)
IdO	Internet des objets
SIL	Safety Integrity Level (niveau d'intégrité de sécurité)

4 Concepts clés et application du présent document

4.1 Vue d'ensemble

La sûreté de fonctionnement est l'aptitude à fonctionner quand et tel qu'exigé. Le terme s'applique également aux entités, produits, processus et services, ainsi qu'aux systèmes allant d'un composant simple à un système de systèmes. Un système, produit ou service fiable donne à l'utilisateur l'assurance que les exigences seront satisfaites à l'avenir et la qualité maintenue au fil du temps.

L'Article 4 explique le concept de sûreté de fonctionnement et les attributs des systèmes, produits et services qui relèvent du domaine de la sûreté de fonctionnement. Les principes de gestion de la sûreté de fonctionnement et les avantages d'y consacrer des efforts sont décrits. La relation entre le système de gestion d'un organisme et la sûreté de fonctionnement est abordée. Le concept d'un programme technique d'activités de sûreté de fonctionnement réalisé tout au long du cycle de vie est présenté.

4.2 Principes de gestion de la sûreté de fonctionnement

La gestion de la sûreté de fonctionnement englobe les principes suivants.

- Approche holistique: la gestion de la sûreté de fonctionnement intègre des considérations de performance, de coût, de risque et de conformité tout au long du cycle de vie d'un

système, produit ou service. Elle le fait en adoptant une approche des systèmes avec une optimisation continue tout au long du cycle de vie.

- Assurance et redevabilité: la gestion de la sûreté de fonctionnement fournit les justifications permettant d'éprouver une confiance légitime dans la réalisation des affirmations relatives à la sûreté de fonctionnement, actuelle ou future. Cela satisfait aux exigences d'assurance et de redevabilité du cadre de management de l'organisme, qui satisfait à son tour aux besoins et aux attentes des parties prenantes en matière d'assurance et de redevabilité.
- Basé sur le risque: la gestion de la sûreté de fonctionnement implique l'identification de facteurs susceptibles de provoquer des défaillances ou des divergences par rapport aux exigences des produits et services des systèmes, ainsi que des systèmes qui les prennent en charge. Ces risques représentent un coût potentiel tout au long du cycle de vie d'un système, produit ou service. L'amélioration de la sûreté de fonctionnement représente un coût initial pour le concepteur ou le fabricant, mais peut entraîner une économie lorsqu'elle est considérée sur toute la durée de vie du produit. La détermination du montant à investir pour améliorer la sûreté de fonctionnement à toutes les étapes du cycle de vie est directement liée au risque et à la valeur, ainsi qu'au niveau de risque que l'organisme est disposé à accepter.
- Adaptabilité: il est nécessaire que les activités de sûreté de fonctionnement, et les systèmes pour les gérer, soient suffisamment souples pour répondre en temps opportun aux changements des besoins et du contexte. L'adaptabilité peut également être un attribut souhaitable d'un système, produit ou service qui peut améliorer sa maintenabilité et sa supportabilité, et prolonger sa durée de vie utile.
- Durabilité: pour qu'un système, produit ou service satisfasse aux besoins et aux attentes des parties prenantes, il est nécessaire de prendre en compte les aspects économiques, sociaux et environnementaux, ainsi que l'excellence technique. Par exemple, en essayant d'obtenir un système, un produit ou un service fiable, maintenable et soutenable, il convient qu'une conception fiable vise également à réduire la consommation d'énergie et les impacts sur l'environnement et envisage l'inclusion de composants réutilisables. Un système, produit ou service fiable, maintenable et soutenable est susceptible d'avoir une durée de vie plus longue, d'utiliser moins de ressources et de produire moins de déchets qu'un autre qui n'a pas ces attributs.

- Équilibre: la sûreté de fonctionnement est gérée de manière à obtenir un équilibre approprié entre le coût, le risque et la performance tout au long du cycle de vie du système, produit ou service. Un compromis peut également être exigé avec des exigences, telles que la sécurité et la sûreté, qui peuvent parfois être contradictoires avec la sûreté de fonctionnement et avec des contraintes telles que des exigences contractuelles et légales.

4.3 Avantages de la gestion de la sûreté de fonctionnement

La gestion de la sûreté de fonctionnement est essentielle à la gestion de la valeur que les organismes ou les particuliers tirent de leurs actifs. Cette valeur est souvent définie en matière de performance, de coût et de conformité, ainsi que d'éléments moins concrets, mais tout aussi importants tels que la marque, la réputation, la clientèle et la confiance.

La gestion de la sûreté de fonctionnement est avantageuse pour un organisme, car elle:

- donne une confiance justifiée dans le fait que les systèmes, produits et services apporteront une valeur ajoutée en fonctionnant quand et tel qu'exigé;
- optimise les coûts du cycle de vie et présente des niveaux de performances de sûreté de fonctionnement à un prix raisonnable;
- obtient la conformité aux exigences réglementaires ou aux normes imposées;
- gère les risques de défaillance ou de dégradation des performances de manière à obtenir un équilibre entre coût, risque et performance;
- assure la transparence de la prise de décision;
- étaye le développement de systèmes de gestion, par exemple les systèmes de gestion d'actifs et les systèmes de management de la qualité, et fournit des preuves tangibles de l'obtention de leurs résultats prévus (les résultats peuvent inclure les résultats financiers, la sécurité, l'environnement et la sûreté, ainsi que les résultats de performance technique);
- améliore la conception;
- optimise les besoins en maintenance et en soutien;
- réduit la nécessité d'activités de maintenance non programmées susceptibles d'exposer le personnel à des dangers potentiels;
- permet de prendre des décisions éclairées dans un environnement opérationnel changeant (y compris les modifications des exigences proprement dites);
- fournit des éléments d'informations nécessaires à la conception, à la mise en œuvre et à l'amélioration continue de la maintenance et du soutien;
- fournit des informations de sorte que les erreurs du passé ne se reproduisent pas, que des leçons en soient tirées et que les succès soient mis à profit;
- améliore la résilience d'un organisme aux événements et circonstances défavorables.

4.4 Attributs de la sûreté de fonctionnement

La sûreté de fonctionnement d'un système, produit ou service est spécifiée et vérifiée à l'aide d'un ensemble d'attributs. Dans la mesure du possible, ceux-ci sont quantifiés pour assurer que les exigences sont satisfaites et pour démontrer les améliorations sans ambiguïté. La sûreté de fonctionnement comporte de nombreux attributs, mais elle est généralement caractérisée en matière de fiabilité, de maintenabilité, de supportabilité et de disponibilité.

La fiabilité se rapporte à la capacité de fournir une fonction exigée sans défaillance pendant un intervalle donné (temps, cycles de fonctionnement, distance, etc.). La fiabilité peut être quantifiée comme une probabilité de succès (par exemple la probabilité qu'une entité s'acquitte de sa fonction prévue pendant une période de temps spécifiée) ou exprimée au moyen de mesures connexes, par exemple le taux de défaillance. Pour spécifier la fiabilité sans ambiguïté, il est nécessaire de définir un point auquel une fonction particulière est considérée comme défaillante.

La maintenabilité se rapporte à la facilité et à la rapidité avec lesquelles une entité peut être maintenue ou rétablie dans un état permettant de fonctionner tel qu'exigé. Elle peut être quantifiée comme la probabilité qu'une action de maintenance donnée, réalisée dans des conditions déclarées, puisse être accomplie dans un délai spécifié. Le terme "maintenue dans" fait référence à la maintenance lorsqu'un système est dans un état opérationnel (par exemple maintenance en ligne ou réparation de composants redondants). Le terme "rétablie" fait référence à la maintenance lorsqu'un système est dans un état non opérationnel, tel que l'entretien planifié du temps d'indisponibilité. Le logiciel diffère du matériel en ce sens qu'il ne s'use pas et que les défauts proviennent de la spécification, de la logique de conception ou du processus de codage et peuvent être cachés jusqu'à ce que des conditions d'entrée spécifiques se produisent. La maintenabilité du logiciel se rapporte à la facilité et à la rapidité avec lesquelles un logiciel peut être modifié pour changer ou ajouter des capacités, corriger des défauts ou des pannes, améliorer les performances ou l'adapter à un environnement différent.

La supportabilité concerne l'identification et la quantification:

- du soutien exigé pour une entité définie dans un contexte d'utilisation donné;
- du temps pour fournir ce soutien;
- des ressources, du coût et de la qualité de ce soutien;
- de la qualité du soutien fourni.

Plus précisément, la supportabilité est concernée par ce qui est exigé pour qu'une entité continue à fonctionner, ainsi que par la façon de mettre en œuvre cette exigence. L'élément "ce qui est exigé" est inhérent à la conception de l'entité, mais la manière dont il est mis en œuvre est déterminée par l'organisme qui gère le soutien.

La disponibilité est la capacité à être en état de fonctionner lorsque cela est nécessaire. Elle est souvent définie comme le rapport entre le temps de disponibilité et le temps total. Étant donné que la fiabilité, la maintenabilité et la supportabilité constituent des facteurs qui contribuent de manière significative au temps de disponibilité et au temps d'indisponibilité, la disponibilité est influencée par les compromis entre ces attributs.

EXEMPLE: Une entité fiable ne tombe pas très souvent en panne, une entité disponible fonctionne quand cela est nécessaire et une entité fiable, en plus d'être disponible, fonctionne correctement dans le temps et est facile à maintenir et à soutenir.

Des facteurs tels que le coût, les ressources, le temps disponible pour les activités de sûreté de fonctionnement et les conditions d'utilisation influencent le niveau de fiabilité, de maintenabilité et de supportabilité qui peut être obtenu en pratique.

Les mesures de fiabilité, de maintenabilité, de supportabilité et de disponibilité sont abordées respectivement dans l'IEC 62308, l'IEC 60300-3-10, l'IEC 60300-3-14 et l'IEC 61070. L'IEC 61703 explique la signification mathématique d'une série de mesures relatives à la sûreté de fonctionnement et la manière dont elles sont établies.

Les mesures de fiabilité, de maintenabilité, de supportabilité et de disponibilité sont des quantités de nature stochastique ou statistique, c'est-à-dire qu'il est nécessaire de disposer de suffisamment de données pour assurer une validité statistique (voir IEC 60300-3-2 et l'IEC 60605-6). La vérification d'une fiabilité élevée ou la fourniture d'un niveau de confiance élevé pour une mesure de sûreté de fonctionnement exige un grand nombre d'essais qui ne sont pas toujours faisables, réalisables dans le temps ou rentables. La fiabilité prévisionnelle dans ces conditions peut cependant être vérifiée à l'aide des résultats des modèles de fiabilité (voir IEC 60300-3-1).

Les autres attributs qui peuvent relever du domaine de la sûreté de fonctionnement sont les suivants.

- Durabilité, qui est l'aptitude à fonctionner tel qu'exigé, dans des conditions données d'utilisation, de maintenance et de réparation, jusqu'à l'état final défini. Elle est liée à la capacité de continuer à rétablir un système ou un produit dans une condition de fonctionnement jusqu'à ce qu'il ne soit plus nécessaire.
- La récupérabilité, qui est la capacité à se remettre d'une défaillance, sans recourir à la maintenance corrective (par exemple réinitialisation automatique du logiciel après détection d'une défaillance logicielle).
- La tolérance aux pannes, qui est l'aptitude à continuer à fonctionner malgré la présence de certaines pannes.
- L'utilisabilité, qui est l'aptitude d'un système, d'un produit ou d'un service à être utilisé de manière effective et efficace. L'utilisabilité affecte les performances des opérateurs et des techniciens d'entretien et a donc une influence sur la fiabilité et la maintenabilité globales d'une entité. Elle inclut par exemple l'apprenabilité, l'exploitabilité et les mécanismes de prévention et de protection contre les erreurs, voir IEC 62508.
- La testabilité, qui est une caractéristique de conception qui détermine le degré auquel un système, produit ou service peut être contrôlé pour déterminer une ou plusieurs caractéristiques dans des conditions indiquées. La testabilité est abordée dans l'IEC 60706-5.
- L'exploitabilité, qui est la capacité d'un système, produit ou service d'être utilisé ou exploité de façon sûre et fiable pour fournir un résultat ou une fonction prévus.
- La robustesse, qui est la capacité d'un système, produit ou service pour fonctionner correctement en présence d'entrées contraignantes ou de conditions d'environnement.
- La résilience, qui est la capacité à s'adapter au changement et à retrouver sa capacité fonctionnelle dans un délai acceptable après avoir été affecté par des entrées ou des conditions d'environnement contraignantes.
- L'intégrité, qui est la capacité d'empêcher ou de résister à une modification non autorisée. Elle inclut à la fois l'altération non malveillante (par exemple usure inattendue du matériel ou mise à jour automatique non coordonnée du logiciel) et l'altération malveillante ou non autorisée (par exemple contamination par des logiciels malveillants ou des composants contrefaits). Pour le matériel, l'intégrité est l'aptitude d'un système à maintenir la stabilité de sa forme et sa robustesse. Pour les logiciels et les données, elle concerne l'exactitude, l'exhaustivité et la sûreté.

Souvent, ces attributs affectent la fiabilité, la maintenabilité et la supportabilité et peuvent être inclus dans le mesurage de ces attributs. L'IEC 60300-3-4 fournit des recommandations sur l'élaboration d'exigences de sûreté de fonctionnement dans les spécifications, et sur les moyens d'assurer la réalisation de ces exigences. L'ISO/IEC 25023 fournit les méthodes pour spécifier les exigences et évaluer les performances de certains autres attributs de qualité qui peuvent affecter plus indirectement la sûreté de fonctionnement, tels que l'apprenabilité, la tolérance à l'erreur et la protection contre les erreurs.

La sécurité, la sûreté et la véracité peuvent se recouper avec la sûreté de fonctionnement. Il est exigé que les fonctions de sécurité soient fiables pour empêcher les dommages corporels et matériels, ainsi qu'à l'environnement. Dans certaines situations, une défaillance peut conduire à une situation dangereuse; par conséquent, une fiabilité améliorée peut améliorer la sécurité. Dans d'autres cas, les exigences de sécurité peuvent entraîner une augmentation de la maintenance et donc réduire la disponibilité. Les entités fiables exigent moins d'entretien et évitent donc d'exposer le personnel à des dangers potentiels lors des opérations de réparation.

La sûreté exige qu'un système, produit ou service soit disponible uniquement pour les personnes autorisées à l'utiliser (combinaison des attributs de disponibilité et d'intégrité) avec l'exigence supplémentaire de confidentialité (absence de divulgation non autorisée). Voir Figure 1 (les traits avec flèches à la figure indiquent les attributs de sûreté de fonctionnement et de sûreté).

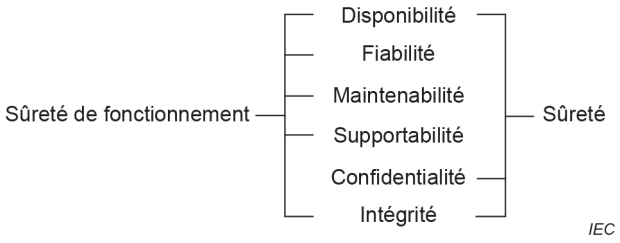


Figure 1 – Attributs de sûreté de fonctionnement et de sûreté

La sûreté et la sûreté de fonctionnement sont liées. La sûreté peut parfois réduire la sûreté de fonctionnement. Par exemple, une restriction d'accès à un système peut réduire sa maintenabilité. Une mauvaise sûreté de fonctionnement peut nuire à la sûreté. Par exemple, une mauvaise maintenabilité du logiciel peut entraîner une violation de sûreté. La véracité est un concept qui est appliqué dans des systèmes fortement axés sur des logiciels, tels que l'intelligence artificielle (IA) et l'Internet des objets (IdO). C'est la capacité à satisfaire aux attentes des parties prenantes de manière vérifiable. Les caractéristiques de véracité comprennent la fiabilité, la disponibilité, la résilience, la sûreté, la protection de la vie privée, la sécurité, la redevabilité, la transparence, l'intégrité, l'authenticité, la qualité, l'utilisabilité et l'exactitude (voir par exemple l'ISO/IEC 30145-2).

Il peut être difficile de définir des mesures quantitatives pour les attributs de sûreté de fonctionnement de l'IA et des technologies connexes. La perception d'une défaillance par l'utilisateur dépend de ses attentes vis-à-vis du système. Le comportement du système change en fonction des interactions avec l'utilisateur, de sorte que les expériences diffèrent d'un utilisateur à l'autre. Cela signifie que le défaut d'exécution tel qu'exigé dépend de l'expertise, des objectifs, des modèles mentaux et de l'expérience passée de l'utilisateur dans l'utilisation du produit, ainsi que de la conception des algorithmes et des données sur lesquelles ceux-ci sont basés. Cependant, des analyses qualitatives restent possibles.

En général, les utilisateurs, les fournisseurs, les opérateurs, les techniciens d'entretien et ceux qui interagissent avec un système peuvent avoir des exigences de sûreté de fonctionnement qui coïncident, mais des objectifs d'application et des attentes d'utilisation qui diffèrent. Cela peut entraîner des besoins différents et des perceptions différentes de la sûreté de fonctionnement. Une perspective utilisateur de la sûreté de fonctionnement globale peut dans certains cas être obtenue à l'aide de déclarations qualitatives ou d'une échelle d'appréciation ordinale.

Pour un système ouvert, tel qu'un système de systèmes ou un gros système qui fonctionne pendant une période prolongée dans un environnement réel, les attributs de sûreté de fonctionnement sont à envisager dans un contexte où aucune partie prenante n'a une compréhension exhaustive du système et de ses risques. L'obtention et l'assurance de la sûreté de fonctionnement dans ce cas reposent sur l'établissement d'un consensus entre les parties prenantes, la garantie de la redevabilité et l'adaptation au changement. Étant donné que l'identification et le contrôle des risques sont plus difficiles, il est particulièrement important que le système soit en mesure de répondre efficacement à la défaillance. L'IEC 62853 fournit des recommandations sur la sûreté de fonctionnement des systèmes ouverts.

4.5 Relation entre le système de gestion d'un organisme et la sûreté de fonctionnement

Le système de gestion d'un organisme fournit et documente l'infrastructure nécessaire pour obtenir la valeur et les résultats à fournir. Au sein de ce système de gestion, les processus, les activités et les tâches sont développés, documentés et mis en œuvre pour atteindre des objectifs spécifiques. Les normes ISO telles que l'ISO 9001 et l'ISO 55001 décrivent les exigences du système de management d'un organisme. Les normes techniques et financières fournies par l'IEC, l'IFRS et l'IAS fournissent des recommandations détaillées sur les processus, activités et tâches. L'IEC TS 62775 montre comment la suite de normes de sûreté de fonctionnement de l'IEC, l'ingénierie des systèmes et les normes IFRS et IAS peuvent déterminer les exigences de gestion d'actifs, telles que décrites par la suite de normes ISO 5500x.

La Figure 2 représente la relation entre les normes de systèmes de management et les normes de sûreté de fonctionnement. L'Annexe A énumère les normes relatives à la sûreté de fonctionnement provenant de l'IEC.

La sûreté de fonctionnement des équipements, des personnes, des processus et des services est essentielle à la capacité de l'organisme à atteindre ses objectifs. Il convient donc d'intégrer la gestion de la sûreté de fonctionnement dans le système de management de l'organisme. La gestion de la sûreté de fonctionnement ne constitue pas un effort distinct pour l'entreprise et il convient que les objectifs de sûreté de fonctionnement s'alignent sur les objectifs commerciaux. Les attributs de sûreté de fonctionnement sont interconnectés avec d'autres aspects de performance et de fonctionnalité; il convient donc de tenir compte de la sûreté de fonctionnement conjointement avec d'autres facteurs organisationnels tels que le coût, le calendrier, la performance, le risque et la rentabilité.

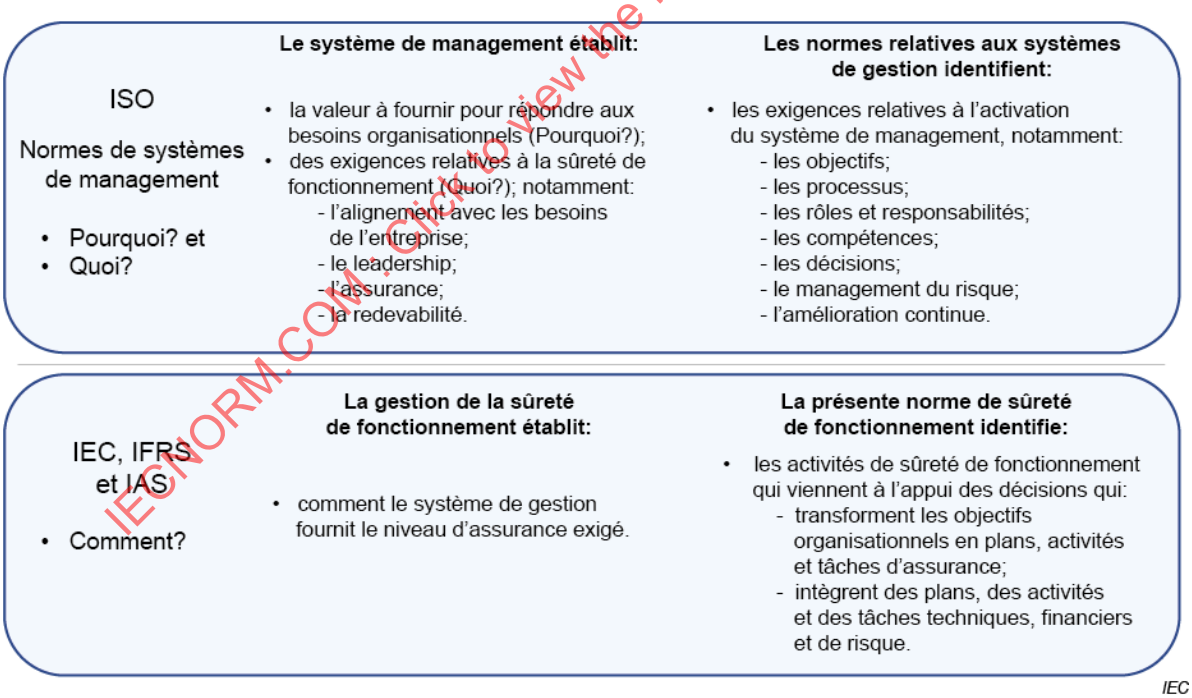


Figure 2 – Rapport entre les normes de systèmes de management et les normes de sûreté de fonctionnement

L'Article 5 décrit comment la gestion de la sûreté de fonctionnement peut être incorporée à un système de management présumé être conforme à une norme de système de management ayant la structure harmonisée des Directives ISO/IEC, Partie 1, Supplément ISO consolidé:2022, Annexe SL.

4.6 Programmes techniques de sûreté de fonctionnement

Afin d'atteindre les objectifs et les cibles de sûreté de fonctionnement et de fournir l'assurance qu'ils ont été ou seront réalisés, un ensemble d'activités de sûreté de fonctionnement coordonnées est réalisé sur mesure. Les activités sont réparties en tâches individuelles (et parfois sous-tâches). Celles-ci sont généralement documentées dans un plan qui donne des détails sur les objectifs, le contexte et les contraintes. Il identifie les tâches à entreprendre, les techniques, les outils et les ressources exigés, les responsabilités et les redevabilités, ainsi que la manière dont les activités et les tâches de sûreté de fonctionnement sont intégrées à d'autres activités connexes.

NOTE Une activité de sûreté de fonctionnement peut être un processus de cycle de vie, une activité, une tâche ou une vue de processus tel que défini dans l'ISO/IEC/IEEE 15288 (voir Annexe F).

Les activités de sûreté de fonctionnement peuvent être organisées sous la forme de programmes distincts, mais étroitement coordonnés pour la fiabilité, la maintenabilité, la supportabilité, la maintenance et le soutien, ou une combinaison de ces capacités, ou bien être pleinement intégrées dans d'autres programmes. La disposition choisie est déterminée par des considérations techniques et les besoins des parties prenantes, ainsi que par les priorités et les valeurs de l'entreprise. Les programmes peuvent être établis projet par projet ou peuvent être à l'échelle de l'organisme, avec une souplesse permettant des variations entre les projets. Les variables comprennent les parties prenantes comme la pertinence, le coût, le calendrier, les compromis sur la qualité et la difficulté technique du travail, ainsi que les connaissances et l'expérience des personnes concernées.

Quelles que soient les dispositions organisationnelles mises en place, il convient que les activités de sûreté de fonctionnement soient coordonnées pour atteindre les objectifs de sûreté de fonctionnement et intégrées aux activités connexes pour l'ensemble du projet. La sélection personnalisée des activités et tâches de sûreté de fonctionnement pour un contexte particulier est parfois appelée programme de sûreté de fonctionnement. L'Article 6 traite de la conception d'un programme d'activités de sûreté de fonctionnement.

4.7 Concept de cycle de vie

Un système ou un produit, quelles que soient sa taille et sa complexité, évolue depuis sa conception initiale jusqu'à sa mise au rebut et à son élimination ou sa réutilisation éventuelle. Il est généralement utile de construire un modèle de cette progression pour aider à gérer l'évolution du système. Ces modèles sont appelés modèles de cycle de vie. Un modèle de cycle de vie est divisé en étapes pour faciliter la planification, l'approvisionnement, l'exploitation et le soutien du système ou du produit considéré. Le passage d'une étape à l'autre représente les principaux repères dans lesquels les décisions d'investissement et les engagements des ressources peuvent être pris et incorporés dans le processus de gestion.

NOTE Le concept d'un modèle de cycle de vie, modèle fonctionnel abstrait du cycle de vie réel d'un système, est décrit en détail dans l'ISO/IEC/IEEE 24748-1.

Les activités de sûreté de fonctionnement procurent des avantages dès le début. Cependant, les plus grands gains sont obtenus en entreprenant ces activités dès les premières étapes du cycle de vie, car:

- la prise en compte des besoins et des attentes des parties prenantes en matière de sûreté de fonctionnement dès le début aide à maintenir la satisfaction des parties prenantes;
- la conception de la fiabilité, de la disponibilité, de la maintenabilité et de la supportabilité, ainsi que leur équilibre, sont moins onéreux et plus faciles dès les premières étapes;
- la rectification de problèmes liés à une faible sûreté de fonctionnement une fois qu'un système est en exploitation est souvent chronophage et onéreuse. Un investissement en sûreté de fonctionnement pendant les activités de conception dès les premières étapes du cycle de vie peut être payant par rapport aux coûts combinés de développement, de réalisation, d'utilisation et de mise au rebut et réutilisation.

L'IEC 60300-3-3 décrit l'évaluation du coût du cycle de vie et les relations entre la sûreté de fonctionnement et le coût.

Il existe de nombreuses formules différentes de cycle de vie en fonction de la nature, de l'objet, de l'utilisation et des circonstances prédominantes du système ou du produit. Un modèle de cycle de vie générique simple comporte les étapes suivantes:

– concept;
– développement;
– réalisation (y compris fabrication, transport, acquisition et installation);
– utilisation (y compris exploitation, maintenance, évolution et amélioration);
– mise au rebut et réutilisation.

L'Annexe B décrit d'autres modèles de cycle de vie.

Il est possible qu'un organisme n'ait pas de contrôle ou d'intérêt à toutes les étapes ou puisse exiger des détails supplémentaires au sein d'une étape pour tenir compte des principaux points de décision qui leur sont pertinents. Par exemple, dans certains cas, si l'étape d'exploitation est étendue, il est probable qu'il y ait des changements de contexte et d'utilisation, et peut-être aussi d'exigences. La gestion du changement devient particulièrement importante. Il y aura également inévitablement certaines défaillances et anomalies qu'il sera nécessaire d'étudier avec les résultats restitués afin d'améliorer la sûreté de fonctionnement. Il convient d'effectuer des modifications, qu'il s'agisse d'une évolution ou d'une amélioration significative, d'une manière contrôlée et d'analyser les effets des modifications de conception pour déceler d'éventuels effets et interactions indésirables. La Figure B.3 représente comment la modification peut être gérée tout au long des étapes du cycle de vie.

4.8 Concept d'activité de sûreté de fonctionnement

Une activité de sûreté de fonctionnement est définie par son objet, ses résultats et une liste de tâches qui, ensemble, atteignent l'objet et les résultats. Les activités de sûreté de fonctionnement peuvent être prises en compte en deux groupes:

- les activités de gestion de programme;
- les activités techniques de sûreté de fonctionnement.

Les activités de gestion de programme sont celles qui sont nécessaires à la planification, à la mise en œuvre, à la revue et à l'amélioration d'un ensemble d'activités techniques qui atteignent les objectifs de sûreté de fonctionnement et satisfont aux besoins des parties prenantes.

Les activités techniques de sûreté de fonctionnement décrites dans le présent document sont génériques et susceptibles de faire partie intégrante d'un programme quelconque. Chaque activité implique un certain nombre de tâches qui sont choisies pour atteindre l'objet et les résultats de l'activité de sûreté de fonctionnement dans le contexte concerné de manière rentable. L'Article 7 décrit les activités de gestion de programme et l'Article 8 les activités techniques de sûreté de fonctionnement.

NOTE Dans le présent document, une activité de sûreté de fonctionnement et une tâche dans une activité de sûreté de fonctionnement n'ont pas la même signification qu'une activité et une tâche selon l'ISO/IEC/IEEE 15288 (voir 3.1.7). L'Annexe F explique la relation entre la signification selon le présent document et celle selon l'ISO/IEC/IEEE 15288.

5 Intégration de la sûreté de fonctionnement dans le système de gestion d'un organisme

5.1 Vue d'ensemble

L'Article 5 décrit comment la sûreté de fonctionnement peut être incorporée dans les exigences d'un système de management présumé être conforme à une norme de système de management ayant la structure harmonisée des Directives ISO/ IEC, Partie 1, Supplément ISO consolidé:2022, Annexe SL. Ces normes comprennent l'ISO 55001 (pour les systèmes de gestion d'actifs) et l'ISO 9001 (pour les systèmes de management de la qualité).

Il n'est pas prévu que la gestion de la sûreté de fonctionnement soit un système de gestion distinct. La Figure 3 représente les éléments d'un système de gestion et les aspects de gestion de la sûreté de fonctionnement à intégrer dans ce système. Les nombres dans les flèches indiquent les paragraphes du présent document dans lesquels ces aspects de sûreté de fonctionnement sont décrits.

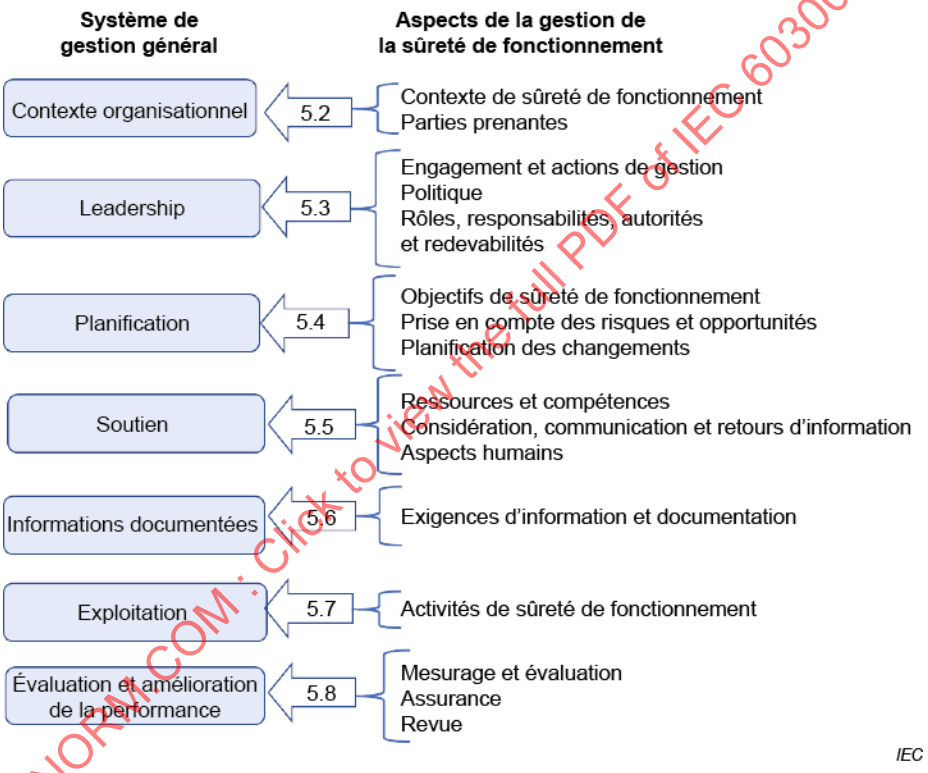


Figure 3 – Intégration de la sûreté de fonctionnement dans un système de gestion

5.2 Compréhension de l'organisme et de son contexte

Il convient que les dispositions organisationnelles concernant la gestion de la sûreté de fonctionnement tiennent compte des enjeux externes et internes, y compris les objectifs, les menaces, les opportunités et les risques de l'organisme.

Il convient d'identifier les parties prenantes internes et externes concernées par la sûreté de fonctionnement et de déterminer leurs besoins et leurs attentes (voir Annexe C). Les parties prenantes pouvant changer avec le temps, il convient que l'organisme surveille, examine et mette à jour les informations relatives aux parties prenantes, ainsi qu'à leurs besoins et à leurs attentes.

La sûreté de fonctionnement est affectée par des facteurs physiques et psychosociaux au sein de l'organisme et par les performances d'organismes externes telles que les fournisseurs ou les fournisseurs de services. Les exigences de sûreté de fonctionnement au sein du système considéré peuvent être satisfaites, mais si les influences internes et externes ne sont pas également comprises et gérées efficacement, les besoins et les attentes des parties prenantes peuvent ne pas être satisfaits.

5.3 Leadership

Il convient que les responsables reconnaissent l'importance de la sûreté de fonctionnement dans la réalisation des objectifs commerciaux et démontrent leur engagement envers la sûreté de fonctionnement, de sorte que l'importance des comportements qui favorisent la sûreté de fonctionnement soit clairement transmise. Il convient qu'ils communiquent aux parties prenantes externes le domaine d'application de la redevabilité de la direction en ce qui concerne la sûreté de fonctionnement et leur engagement vis-à-vis de celle-ci, et il convient d'obtenir le consentement et la confiance des parties prenantes externes. Une sûreté de fonctionnement élevée peut uniquement être obtenue si la sûreté de fonctionnement est reconnue comme faisant partie intégrante de la stratégie d'entreprise et si elle fait l'objet d'un engagement et une priorité permanente de la haute direction. Sans cela, l'effort de sûreté de fonctionnement est susceptible d'être compromis chaque fois que des contraintes de temps ou de coût apparaissent.

- Politique:

  Il convient de faire référence à la sûreté de fonctionnement dans la déclaration de politique d'un organisme. Cela permet de s'assurer que des ressources appropriées sont fournies et que les pratiques de travail et les actions de l'ensemble du personnel permettent d'obtenir des résultats fiables et de haute qualité. Elle assure également la redevabilité des parties prenantes externes.

- Rôles, responsabilités, autorités et redevabilités:

  Il convient d'attribuer des responsabilités, des autorités et des redevabilités pour les rôles de gestion de la sûreté de fonctionnement pour différents systèmes, produits et services aux étapes pertinentes du cycle de vie. Souvent, plusieurs organismes sont impliqués tout au long du cycle de vie d'un système et il est nécessaire de transférer certaines responsabilités et redevabilités d'un organisme à l'autre. Dans la mesure où les styles et les procédures organisationnels varient, il est nécessaire d'adapter la gestion de la sûreté de fonctionnement aux différentes situations. Il convient de documenter les résultats sous forme d'accords qui clarifient les redevabilités pour toute défaillance.

  Les rôles, les responsabilités et les autorités peuvent varier avec le temps. La clarté des redevabilités est également importante dans ce cas. Dans certains domaines d'activité, tels que les appareils médicaux, l'industrie aérospatiale et les machines, des dispositions réglementaires spécifient des exigences strictes relatives à la redevabilité et à l'indépendance.

5.4 Planification

- Définition des objectifs de sûreté de fonctionnement et planification des actions pour les atteindre:

  Il convient de définir les objectifs de sûreté de fonctionnement qui viennent à l'appui des objectifs de l'organisme, ainsi que la redevabilité de leur réalisation. Il convient de tenir compte des objectifs de sûreté de fonctionnement au niveau de l'organisme et du projet, ainsi qu'au niveau des exigences des systèmes, produits ou services particuliers (voir 7.2.3). Lorsque plusieurs organismes sont impliqués, il convient que les accords relatifs aux objectifs et aux plans soient consignés comme la base des résolutions de litiges et pour une amélioration future.

- Actions pour traiter les risques, les menaces et les opportunités:

  Lors de la planification de la gestion de la sûreté de fonctionnement, il convient que l'organisme détermine les menaces, les opportunités et les risques qu'il est nécessaire de traiter pour donner l'assurance que les activités de sûreté de fonctionnement peuvent obtenir leurs résultats prévus. Le paragraphe 7.2 décrit la planification d'un programme d'activités de sûreté de fonctionnement.

  Il convient d'identifier et de comprendre les risques pour la sûreté de fonctionnement des systèmes, produits et services et pour l'efficacité des activités de gestion de la sûreté de fonctionnement dans le cadre des processus de management du risque de l'organisme. Il convient de planifier et de mettre en œuvre des actions pour traiter les risques, les menaces et les opportunités, en tenant compte de la manière dont ceux-ci peuvent varier avec le temps (voir 8.3). La gestion du risque commence aux premières étapes d'un cycle de vie et se poursuit à chaque étape. Il convient de transmettre des informations sur les risques d'une étape à l'autre et de mieux comprendre le risque au fil de la disponibilité des informations.

- Planification des changements:

  Il convient que les changements soient réalisés de manière planifiée, en tenant compte de l'impact potentiel sur les dispositions de gestion de la sûreté de fonctionnement et des résultats de la sûreté de fonctionnement. Cela inclut l'étude de la manière dont la sûreté de fonctionnement est affectée par la disponibilité des ressources et la réattribution des responsabilités et des autorités. Il est nécessaire que la gestion de la sûreté de fonctionnement soit adaptable de sorte que la sûreté de fonctionnement continue d'être assurée face à des changements imprévus.

5.5 Soutien

- Ressources et compétences:

  Il convient que l'organisme fournisse les ressources nécessaires pour atteindre les objectifs de sûreté de fonctionnement. Ces ressources sont les suivantes:

  – un personnel qualifié et motivé;
  – l'expertise des spécialistes permettant de mener les activités et les analyses techniques appropriées;
  – un système de gestion de l'information et des connaissances;
  – les infrastructures, notamment les équipements, les bâtiments, le matériel et les logiciels;
  – un environnement social, psychologique et physique approprié pour que les personnes puissent travailler efficacement;
  – des ressources pour surveiller et mesurer la sûreté de fonctionnement;
  – des outils appropriés, y compris les outils logiciels et les données pour l'analyse et la simulation.

  Les ressources nécessaires varient selon les étapes du cycle de vie. Par exemple, l'étape de développement exige une expertise en conception de la sûreté de fonctionnement et l'étape de réalisation peut impliquer des ressources pour une vérification et des essais détaillés.

  NOTE Les aspects techniques du soutien sont abordés en 8.6.

- Considération, communication et retours d'information:

  Les perceptions de la sûreté de fonctionnement peuvent varier en fonction des parties prenantes et au fil du temps. Il convient de maintenir de bonnes communication et consultation avec les parties prenantes concernées au fil du temps. Il convient de fournir des informations non ambiguës, complètes, compréhensibles, vérifiables, cohérentes et traçables. La qualité de la communication et des retours d'information de sûreté de fonctionnement a une incidence sur la confiance, la satisfaction et la fidélité du client, sur l'approbation des organismes de réglementation, ainsi que sur la qualité du service d'assistance à la clientèle.

  Une communication efficace améliore l'exactitude des rapports d'incident et de la capture des données. Elle facilite le choix des actions correctives et préventives appropriées.

  Les retours d'information pertinents peuvent contribuer à établir des tendances de performance, à identifier les domaines critiques nécessitant une attention et à fournir des preuves objectives pour la vérification, la validation et l'amélioration. Une étude de sûreté de fonctionnement (voir IEC 62741) peut constituer un moyen utile de communication de sûreté de fonctionnement et de retours d'information des parties prenantes. L'engagement des parties prenantes est traité en 8.2.

- Aspects humains:

  Les personnes à tous les niveaux jouent un rôle important dans l'obtention de la sûreté de fonctionnement. Les facteurs organisationnels spécifiques qui influencent les performances de sûreté de fonctionnement comprennent l'assistance à la prise de décision et à la résolution de problèmes, la communication, la supervision, la procéduralisation et la clarté des rôles. Il convient que le personnel soit formé, motivé et doté des ressources appropriées pour pouvoir accomplir son travail de manière fiable (voir IEC 62508). L'organisme a la capacité de soutenir ou d'entraver les processus et les comportements qui favorisent la sûreté de fonctionnement. Il convient par conséquent que toute approche de la sûreté de fonctionnement comporte un moyen d'identifier et d'améliorer les facteurs humains critiques.

5.6 Informations documentées

Il convient que l'organisme détermine les informations nécessaires à la gestion de la sûreté de fonctionnement. Il convient que les données recueillies incluent celles qui sont nécessaires pour:

- assurer la confiance que les processus ont été réalisés comme prévu;
- communiquer avec les parties prenantes;
- vérifier que les exigences de sûreté de fonctionnement sont ou seront satisfaites;
- valider que les résultats satisfont aux besoins et aux attentes des parties prenantes;
- évaluer et améliorer les activités de sûreté de fonctionnement et leurs résultats;
- constituer une base pour la redevabilité;
- améliorer la gestion de la sûreté de fonctionnement.

Si les données n'ont pas d'objet clair et évident, il convient de s'interroger sur la nécessité de les recueillir.

Ci-après des exemples d'informations et de données pertinentes pour la sûreté de fonctionnement:

– des accords et redevabilités explicites;
– des données de sûreté de fonctionnement dans des conditions d'essais et d'exploitation;
– les résultats des analyses de sûreté de fonctionnement;
– des documents de contrôle de configuration;
– des informations issues des acquéreurs et des fournisseurs ou destinées à ceux-ci;
– données issues du DRACAS et de la LTIAC. Qu'un système d'enregistrement de données soit appelé DRACAS ou LTIAC, il est nécessaire d'enregistrer les défaillances et les périodes d'exploitation réussies afin de quantifier la sûreté de fonctionnement et ses éléments contributifs.

Il convient de définir la propriété des données de sûreté de fonctionnement et de définir un moyen permettant de communiquer les informations nécessaires dans la chaîne d'approvisionnement mise en place. Cela peut faire l'objet d'accords explicites. Il convient que les données relatives à la sûreté de fonctionnement soient convenablement protégées (par exemple de toute perte de confidentialité, d'une utilisation inappropriée ou d'une perte d'intégrité). Il convient d'établir un moyen de contrôler les données et les informations de sûreté de fonctionnement et de s'assurer qu'elles sont mises à jour et disponibles si nécessaire, dans le cadre des systèmes d'information documentés de l'organisme. Le recueil et l'interprétation des données sont abordés en 8.5.

L'ISO/IEC/IEEE 15289 décrit l'objet et le contenu des entités d'information qui peuvent être pertinentes.

5.7 Exploitation

Il convient que l'organisme mette en œuvre et contrôle les activités de sûreté de fonctionnement comme indiqué à l'Article 7 et à l'Article 8 afin d'obtenir les résultats souhaités.

5.8 Évaluation et amélioration de la performance

Il convient que l'organisme planifie et mette en œuvre des processus visant à surveiller, mesurer, analyser et améliorer l'efficacité et l'efficience de la manière dont il gère la sûreté de fonctionnement. Cela peut être facilité par l'utilisation d'une étude de sûreté de fonctionnement (voir IEC 62741).

Il convient que les indicateurs de performance et les cibles soient définis et évalués par rapport à celui-ci. Il peut inclure:

- l'évaluation de la réalisation des politiques et des objectifs de sûreté de fonctionnement de l'organisme;
- la revue de la pertinence des politiques et des objectifs de sûreté de fonctionnement;
- l'évaluation de la sûreté de fonctionnement des systèmes, produits et services par rapport aux exigences;
- l'évaluation de l'efficacité de l'exploitation et l'efficacité des activités de sûreté de fonctionnement;
- l'évaluation des mesures des résultats telles que la satisfaction du client.

L'utilisation d'une matrice de maturité constitue une méthode d'auto-évaluation et d'amélioration. Une matrice de maturité de sûreté de fonctionnement est une liste de contrôle des caractéristiques souhaitées de la gestion de la sûreté de fonctionnement avec différents niveaux de réussite définis. Elle est utilisée pour évaluer l'efficacité actuelle et indiquer les capacités nécessaires à l'amélioration des performances. L'Annexe D fournit un exemple de matrice de maturité de sûreté de fonctionnement. Les modèles de maturité [également appelés modèles d'évolution des capacités (CMM)] peuvent également être utilisés par les organismes pour évaluer leurs processus logiciels. Les CMM fournissent une référence par rapport à laquelle comparer les processus de développement de logiciels; ils peuvent être utilisés comme un indicateur prévisionnel de la qualité du produit et pour favoriser l'amélioration.

Dans la mesure du possible, il convient d'utiliser les systèmes existants de surveillance des performances pour générer les informations nécessaires pour améliorer les activités et les résultats de sûreté de fonctionnement. De tels systèmes prévoient notamment:

– DRACAS et LTIAC (voir 8.6.3);
– un système d'assistance à la clientèle et de retour d'information;
– un système d'approvisionnement de pièces de rechange;
– un système de maintenance et de soutien;
– un système de surveillance des conditions;
– un système de management de la qualité.

Il convient que les aspects de la sûreté de fonctionnement du système de gestion soient inclus dans les audits internes et externes du système de gestion de l'organisme et dans les revues de gestion.

Il convient que l'organisme identifie et exploite les opportunités d'amélioration continue et mette en œuvre les actions nécessaires pour satisfaire aux exigences du client et améliorer la satisfaction des parties prenantes.

6 Conception du programme

6.1 Généralités

Il convient d'effectuer un ensemble coordonné d'activités de sûreté de fonctionnement afin de satisfaire aux objectifs de l'organisme en matière de sûreté de fonctionnement et de besoins des parties prenantes. Il convient qu'il soit adapté à l'organisme et aux systèmes, produits et services considérés. L'Article 6 décrit les considérations relatives à la conception d'un tel programme, y compris la coordination et l'intégration avec d'autres activités, les compromis et les facteurs clés de réussite. L'Article 7 décrit la façon de planifier, de mettre en œuvre, d'examiner et d'améliorer un programme adapté aux circonstances. L'Article 8 décrit les activités et les tâches techniques de sûreté de fonctionnement qui peuvent être incluses dans le programme.

Il convient d'élaborer un plan pour la mise en œuvre du programme, avec des redevabilités, des autorités et des intervalles de temps définis (voir 7.2). Il convient d'identifier et d'intégrer dans le programme les facteurs humains et organisationnels exigés. Il convient que les personnes impliquées dans la mise en œuvre du plan à n'importe quelle étape du cycle de vie soient conscientes de leurs responsabilités et de leurs redevabilités, et qu'elles soient suffisamment soutenues et compétentes.

6.2 Coordination et intégration

La sûreté de fonctionnement peut être gérée en tant que programme distinct par une unité organisationnelle dédiée, être pleinement intégrée dans des domaines pertinents, tels que la mise au point ou la fabrication de produits, ou bien être une combinaison des deux approches. Dans certains organismes, la responsabilité de la sûreté de fonctionnement (comme la qualité) incombe à un service distinct (cela est exigé pour les entreprises qui approuvent leurs propres produits, par exemple pour le système européen de marquage CE). Pour un grand organisme, il peut être utile de mettre en place une entité interservices destinée à répondre aux besoins globaux de l'organisme de manière efficace. Cela permet d'éviter de dupliquer les efforts et assure la cohérence des activités de sûreté de fonctionnement tout en permettant l'application du niveau d'expertise le plus élevé. Dans tous les cas, l'alignement des structures organisationnelles, des responsabilités, des redevabilités, des activités, des ressources et de l'information est essentiel pour une gestion efficace.

Il est généralement plus efficace d'intégrer les activités et les tâches de sûreté de fonctionnement à celles relatives par exemple à la planification, à la conception, à la production, aux opérations et d'élaborer un plan de projet global. La coordination et l'intégration sont également importantes, car il peut être nécessaire de sacrifier la sûreté de fonctionnement pour d'autres besoins des parties prenantes ou objectifs organisationnels.

Il convient d'intégrer les risques identifiés dans le cadre du développement d'une étude de sûreté de fonctionnement ou par l'utilisation d'outils tels que l'AMDE (voir IEC 60812) dans le processus général de management du risque lié à un projet. Cela procure une meilleure connaissance des risques d'un projet, encourage une vision commune de l'acceptabilité des risques et permet des stratégies de traitement plus efficaces. L'ISO 31000 fournit des lignes directrices relatives à la gestion des risques dans tous les contextes. L'IEC 31010 décrit les techniques d'appréciation du risque et la manière dont elles sont utilisées, et l'IEC 62198 fournit des recommandations relatives à la gestion du risque dans les projets.

Il convient de gérer activement la coordination entre différentes activités de sûreté de fonctionnement dans le cadre d'un même projet, ainsi qu'entre différents projets, de manière à ce que les ressources soient utilisées efficacement. Par exemple, les activités de fiabilité, de maintenabilité et de supportabilité peuvent utiliser les mêmes outils d'analyse et les mêmes ensembles de données (si c'est pour des objets différents). Il convient d'attribuer la responsabilité, l'autorité et la redevabilité de la coordination.

6.3 Compromis

Un compromis est une décision dans laquelle une fonctionnalité est réduite en contrepartie de gains dans une autre. Dans la sûreté de fonctionnement, cela peut être dû à des limitations de ressources ou de conception. Les compromis sont effectués en tenant compte des avantages et des inconvénients des caractéristiques qui font l'objet du compromis dans le contexte concerné. Il convient que les priorités qui orientent les décisions concernant les compromis et par conséquent la conception du programme soient convenues avec les parties prenantes concernées.

Les types de compromis applicables à la gestion de la sûreté de fonctionnement sont les suivants:

- au sein d'un attribut de sûreté de fonctionnement spécifique: par exemple une fiabilité élevée peut être obtenue en concevant une entité très fiable ou en incorporant une redondance. De même, le temps d'indisponibilité due à la maintenance peut être réduit en effectuant une maintenance préventive pendant l'exploitation ou pendant un arrêt planifié;

- entre attributs de sûreté de fonctionnement: par exemple le choix peut être fait entre des entités de faible fiabilité qui sont initialement bon marché, mais coûteuses à maintenir, et des entités de fiabilité élevée qui peuvent coûter cher à la conception et à la construction, mais qui exigent peu d'entretien. Les décisions relatives à la maintenabilité et à la maintenance influencent le type de soutien (tels que les pièces de rechange et les compétences de maintenance) qui affecte la supportabilité. Les attributs des composants peuvent être combinés de différentes manières pour offrir la même disponibilité globale;
- entre la sûreté de fonctionnement et d'autres critères tels que la sécurité ou les performances: par exemple l'inclusion de fonctionnalités de sécurité et de systèmes de sécurité peut rendre une entité si complexe à utiliser que sa sûreté de fonctionnement est réduite. D'autres exigences fonctionnelles et non fonctionnelles, telles que la compatibilité de forme, de conformité et de fonction, peuvent également avoir un impact sur la sûreté de fonctionnement;
- entre l'effort mis dans le programme de sûreté de fonctionnement (et donc ses coûts et son calendrier) et la valeur ajoutée (par exemple amélioration de la satisfaction des parties prenantes, de la valeur de marque, et des économies globales résultant de l'amélioration de la sûreté de fonctionnement): pour les systèmes et les produits ayant une longue durée de vie, les coûts d'exploitation, en particulier le coût de maintenance, peuvent être prédominants dans les coûts du cycle de vie. L'effort supplémentaire nécessaire à la conception peut donc permettre de réaliser des économies significatives par la suite. Cependant, une meilleure sûreté de fonctionnement peut devoir faire l'objet d'un compromis afin de respecter le calendrier et le budget du projet. Les décisions dépendent du niveau de risque que l'organisme est prêt à accepter.

Il convient que les compromis qui sont effectués soient explicites et que les décisions soient documentées.

6.4 Personnalisation d'un programme technique d'activités de sûreté de fonctionnement

L'objet de la personnalisation est de concevoir un programme d'activités et de tâches de sûreté de fonctionnement qui obtiennent les objectifs de sûreté de fonctionnement spécifiques dans les contraintes applicables de manière rentable. Exemples de personnalisation:

- planification du budget pour l'affectation des ressources de sûreté de fonctionnement ou la sous-traitance afin de satisfaire au calendrier de réalisation du projet;
- détermination des activités et des tâches qui permettent d'assurer en permanence que les exigences de sûreté de fonctionnement sont satisfaites;
- décision de la meilleure approche pour réaliser une activité particulière dans le contexte particulier.

La conception du programme dépend:

a) des objectifs, notamment de toutes les exigences spécifiées (voir 7.2.3);

b) de la nature du système, produit ou service concerné;

c) des étapes pertinentes du cycle de vie;

d) du délai adopté par l'organisme;

e) de l'approche technique.

EXEMPLE L'approche technique lors de l'étape de conception examine si la conception concerne:

- une entité neuve;
- une entité basée sur des conceptions d'entités précédentes;
- un système utilisant la dernière technologie standard;
- un service de transition tel que "manuel" à "automatisé" ou "à commande électronique" vers "à commande logicielle".

Dans certains cas, une déclaration de travail provenant d'un client, les accords avec d'autres parties prenantes et les politiques internes définissent les tâches à accomplir.

D'autres approches peuvent être:

– la revue d'un programme existant, de ses activités et de ses tâches afin de déterminer où des améliorations peuvent être apportées et l'adapter aux circonstances particulières;

– l'utilisation d'une étude de sûreté de fonctionnement dans laquelle des arguments structurés sont présentés et les preuves sont fournies pour étayer l'affirmation selon laquelle un système satisfait à ses exigences de sûreté de fonctionnement. Les activités et les tâches nécessaires pour fournir les preuves à l'appui de l'allégation représentent les activités et les tâches exigées pour atteindre et assurer la sûreté de fonctionnement (voir IEC 62741).

Lorsqu'un organisme dispose d'un programme de sûreté de fonctionnement existant, des critères et des lignes directrices peuvent être élaborés pour l'adapter à des circonstances spécifiques. Cela peut impliquer un ensemble d'activités qui s'appliquent dans tous les cas et auxquelles des ajouts sont effectués, ou un ensemble d'activités parmi lesquelles celles exigées dans un cas particulier sont choisies.

6.5 Facteurs clés de réussite

Les facteurs clés qui contribuent à la réussite du programme sont les suivants:

- l'intégration des considérations de sûreté de fonctionnement dans la prise de décision dès les premières étapes;
- une compréhension commune du système ou du produit, de ses besoins de sûreté de fonctionnement et des moyens de les obtenir;
- une définition et un accord clairs sur les responsabilités et les redevabilités pour satisfaire aux exigences de sûreté de fonctionnement;
- une coordination et une intégration efficaces entre les différentes entités organisationnelles qui sont impliquées;
- une compréhension des facteurs qui affectent la sûreté de fonctionnement et les coûts d'un système, produit ou service particulier;
- la compréhension des compromis qu'il est nécessaire de faire;
- la fourniture de ressources appropriées (y compris le personnel compétent) pour les activités et les tâches de sûreté de fonctionnement à entreprendre;
- l'intégration de tâches qui soutiennent, analysent et améliorent les performances humaines;
- le recueil et l'utilisation efficaces d'informations et de données;
- l'adaptation aux besoins de l'organisme, des parties prenantes et du projet.

7 Activités de gestion de programme

7.1 Vue d'ensemble

L'Article 7 décrit les activités exigées pour établir un programme d'activités de sûreté de fonctionnement technique, à savoir:

a) la planification du programme pour atteindre les objectifs dans le contexte et les contraintes applicables;

b) la mise en œuvre du plan;

c) la révision et l'amélioration du programme et du plan;

d) l'assurance de la réalisation des objectifs de sûreté de fonctionnement;

e) la garantie de la redevabilité.

Le système de management global et les structures qui soutiennent les activités de sûreté de fonctionnement sont traités à l'Article 5.

7.2 Planifier les activités de sûreté de fonctionnement

7.2.1 Objet

L'objet de la planification est de choisir et coordonner un ensemble d'activités de sûreté de fonctionnement qui atteignent les objectifs de sûreté de fonctionnement de l'organisme d'une manière rentable et d'intégrer celles-ci dans les plans et les processus de projets connexes.

7.2.2 Résultats

Résultat de la planification:

a) définition des objectifs de l'organisme en matière de sûreté de fonctionnement;
b) énoncé d'une approche claire pour l'obtention de ces objectifs;
c) sélection des activités, tâches et outils techniques de sûreté de fonctionnement;
d) établissement des critères d'entrée et de sortie pour chaque activité de sûreté de fonctionnement;
e) définition et attribution à des rôles appropriés des responsabilités et des redevabilités relatives à l'exécution des tâches de sûreté de fonctionnement;
f) définition des exigences d'information et de ressources pour les tâches;
g) élaboration d'un calendrier pour le programme;
h) élaboration d'un plan de sûreté de fonctionnement comprenant des dispositions relatives à la modification du programme;
i) intégration du plan de sûreté de fonctionnement aux autres plans pertinents.

7.2.3 Tâches

Il convient d'entreprendre les tâches suivantes conformément aux politiques organisationnelles.

a) Identifier les objectifs du programme. Elles peuvent inclure:
   - l'obtention des objectifs ou la satisfaction aux exigences de sûreté de fonctionnement d'un système, produit ou service;
   - la démonstration que les objectifs ont été atteints ou les exigences satisfaites en matière de sûreté de fonctionnement;
   - la satisfaction aux exigences légales ou contractuelles;
   - la gestion des coûts du cycle de vie;
   - l'amélioration de l'efficacité;
   - l'amélioration de la capacité de l'organisme à soutenir les performances humaines, notamment celles des travailleurs et des utilisateurs de produits, de manière à atteindre la pleine capacité des systèmes techniques;
   - le renforcement de la confiance des parties prenantes;
   - l'amélioration du soutien;
   - l'obtention d'objectifs ou de jalons spécifiques;
   - la satisfaction aux exigences de sécurité et d'environnement.
b) Définir le contexte du programme. Il peut inclure:
   - la définition des limites (ouvertes ou fermées) du système, produit ou service étudié;

     EXEMPLE 1 Un fournisseur de biens de consommation sur un marché général peut spécifier les caractéristiques de sûreté de fonctionnement matérielles et logicielles qu'il fournit, alors qu'un utilisateur pourrait également inclure des opérateurs humains et des services publics externes.

     EXEMPLE 2 Un fournisseur d'un terminal de guichet bancaire peut fixer la limite de manière à n'inclure que le matériel et les logiciels, puis spécifier leurs caractéristiques de sûreté de fonctionnement. D'un autre côté, un client d'une banque peut également souhaiter inclure des opérateurs humains et des services de serveur connecté à la limite et connaître les caractéristiques globales de sûreté de fonctionnement.

- l'identification des parties prenantes;
- la définition du modèle de cycle de vie correspondant à la situation et la détermination des étapes spécifiques du cycle de vie applicables;
- l'identification des caractéristiques pertinentes du système, produit ou service auquel le programme s'applique, telles que ses fonctionnalités, fonctions, innovations, complexité et environnement d'application;
- l'identification des résultats ou des preuves exigés par les parties prenantes concernées.

c) Identifier les contraintes du programme. Elles peuvent inclure:

- le budget;
- le temps et les ressources disponibles;
- la capacité technologique;
- l'expertise disponible;
- d'autres exigences de ressources (par exemple personnel, politique organisationnelle et infrastructure);
- le risque acceptable;
- le temps de gestion et les priorités;
- les exigences légales et contractuelles.

d) Identifier les risques pour les objectifs du programme.

e) Identifier les preuves nécessaires pour fournir l'assurance que les objectifs sont atteints.

NOTE 1 L'identification des preuves nécessaires et la planification de leur obtention commencent dès que les objectifs sont identifiés. L'assurance que les objectifs sont ou ont été atteints est fournie de manière continue.

f) Identifier les activités techniques de sûreté de fonctionnement exigées pour atteindre les objectifs du programme, ainsi que les tâches et les outils nécessaires pour atteindre les résultats exigés.

g) Hiérarchiser les tâches et les outils des activités de sûreté de fonctionnement, en tenant compte des objectifs, des contraintes, du contexte et des risques.

NOTE 2 Plusieurs outils peuvent être exigés pour fournir un résultat unique.

h) Déterminer la profondeur et le détail minimal exigés à partir de chaque outil sélectionné afin d'atteindre les objectifs souhaités avec la confiance nécessaire. Cela facilite l'affectation des ressources et l'optimisation des coûts.

i) Comparer le temps, la capacité et les ressources exigés pour accomplir chaque tâche à la profondeur nécessaire avec les ressources disponibles.

j) Évaluer si l'effort de sûreté de fonctionnement planifié ajoute de la valeur et modifier le programme dans le cas contraire. Cela peut impliquer une analyse coûts-bénéfices de chaque activité en tenant compte du coût des défaillances, des coûts de possession tout au long du cycle de vie et des coûts des activités de sûreté de fonctionnement.

k) Prendre des décisions concernant les compromis, y compris la possibilité de modifier les objectifs.

l) Choisir les activités et les outils de sûreté de fonctionnement qui fourniront les objectifs du programme souhaités avec les contraintes données.

m) Documenter les décisions de planification et les détails de mise en œuvre des activités de sûreté de fonctionnement. Le plan de sûreté de fonctionnement peut être intégré à d'autres plans, tels qu'un plan qualité ou un plan de projet global. Il convient qu'il indique, au minimum:

- les objectifs de sûreté de fonctionnement;
- les activités, tâches et outils de sûreté de fonctionnement exigés, ainsi que la justification de leur inclusion;
- le calendrier des activités de sûreté de fonctionnement, leur ordre d'exécution, le cas échéant, et les interactions entre elles, de sorte qu'elles puissent être programmées de manière à apporter des éléments d'informations nécessaires à la prise de décisions importantes pour le développement;
- les preuves et les résultats exigés;
- les événements marquants et les critères d'entrée et de sortie pour chaque étape, y compris les conditions dans lesquelles les activités et les tâches exigent une revue en cours ou sont considérés comme terminés;
- le calendrier estimé et les dépendances entre les éléments du programme (le calendrier peut avoir à tenir compte des pressions exercées par d'autres priorités commerciales et des plans de projets);
- les responsabilités et les redevabilités;
- les dispositions pour les revues de la sûreté de fonctionnement.

n) Planifier la surveillance des changements dans le contexte du programme, la revue de l'avancement du programme et le déclenchement d'une nouvelle planification selon les critères définis.

7.3 Mise en œuvre du plan

7.3.1 Objet

L'objet de la mise en œuvre du plan est d'atteindre les objectifs de sûreté de fonctionnement d'une manière efficace et rentable, conforme aux contrats, réglementations et normes applicables, et satisfaisant aux parties prenantes.

7.3.2 Résultats

Résultat de la mise en œuvre du plan:

a) les objectifs de l'organisme et des parties prenantes en ce qui concerne la sûreté de fonctionnement sont atteints;

b) les parties prenantes sont conscientes de leurs responsabilités et de leurs redevabilités, et la redevabilité de la sûreté de fonctionnement est assurée;

c) la sûreté de fonctionnement est efficacement intégrée aux processus techniques;

EXEMPLE Les évaluations des risques relatives à la sûreté de fonctionnement peuvent être combinées à d'autres appréciations du risque lié au projet, et les dispositions d'engagement des parties prenantes peuvent être communes sur un large éventail de questions.

d) les personnes chargées de mettre en œuvre le plan à n'importe quelle étape du cycle de vie sont compétentes et adéquatement soutenues dans leurs rôles;

e) les résultats des activités techniques (voir Article 8) sont obtenus;

f) il est assuré que les objectifs de sûreté de fonctionnement ont été ou seront atteints (voir 7.5);

g) des systèmes sont établis pour recueillir, stocker et analyser des données de sûreté de fonctionnement.

7.3.3 Tâches

Les tâches suivantes peuvent être associées à la mise en œuvre d'un plan de sûreté de fonctionnement:

a) s'engager auprès des parties prenantes pour établir de manière continue leurs besoins, leurs attentes et leurs exigences et les tenir informées, suivant le cas (voir 8.2);

b) fournir des informations et des formations afin que les personnes soient conscientes de leurs responsabilités et redevabilités et qu'elles aient les compétences pour les exécuter;

c) établir des accords explicites entre les parties prenantes, y compris les redevabilités pour les honorer.

   Les accords explicites entre les parties prenantes et la redevabilité pour les honorer sont particulièrement importants pour les systèmes ayant une durée de vie opérationnelle étendue ou avec des limites changeantes et difficiles à définir. Pour ces systèmes ouverts, des activités centrées sur la recherche d'un consensus et l'établissement de la redevabilité sont exigées (voir IEC 62853);

d) fournir les ressources et le soutien pour les activités de sûreté de fonctionnement et les personnes impliquées dans leur mise en œuvre;

e) documenter les décisions et les actions visant à assurer la traçabilité et la redevabilité. Une étude de sûreté de fonctionnement peut être utilisée à cet effet (voir IEC 62741, ISO/IEC/IEEE 15026-2 et ISO/IEC/IEEE 15026-4);

f) établir des systèmes de surveillance de la sûreté de fonctionnement du système, du produit ou du service et de l'efficacité et de l'efficience des tâches de sûreté de fonctionnement.

7.4 Revue et amélioration

7.4.1 Objet

L'objet de la revue de la sûreté de fonctionnement est:

a) d'assurer la satisfaction des objectifs spécifiques provenant de perspectives techniques et commerciales tout au long du cycle de vie;

b) de fournir des retours d'information sur les carences de sûreté de fonctionnement, les écarts et les risques;

c) d'améliorer la sûreté de fonctionnement des systèmes, produits et services, ainsi que de la main-d'œuvre;

d) d'améliorer la gestion de la sûreté de fonctionnement;

e) de déterminer le statut des projets;

f) d'évaluer la nécessité et le rapport coût-efficacité des activités de sûreté de fonctionnement;

g) de reconnaître le changement et la nécessité de s'y adapter.

7.4.2 Résultats

Résultat des revues menées:

a) identification et correction des faiblesses individuelles, organisationnelles ou techniques à un stade précoce;

b) amélioration des systèmes, produits et services, ainsi que du programme de sûreté de fonctionnement;

c) respect des calendriers et budgets;

d) identification des risques et mise en œuvre efficace des traitements.

7.4.3 Tâches

Il convient que les tâches suivantes soient entreprises conformément aux politiques organisationnelles applicables.

a) Planifier le domaine d'application et le calendrier des revues.

La sûreté de fonctionnement est revue à chaque étape du cycle de vie d'un système, produit ou service, en particulier lors du passage d'une étape à l'autre ou lorsque la responsabilité d'un projet est transférée. Le domaine d'application peut être:

- technique, en couvrant les aspects relatifs à la conception et aux performances de sûreté de fonctionnement d'un système, produit ou service; ou
- axé sur la gestion, en couvrant les aspects relatifs aux coûts et à la planification d'un projet ou le programme de sûreté de fonctionnement.

b) Identifier les parties prenantes et les impliquer, le cas échéant.

c) Revoir régulièrement les exigences afin de tenir compte de l'évolution des besoins des parties prenantes, des conditions de fonctionnement et des nouvelles technologies.

d) Coordonner et participer à d'autres revues organisationnelles et de projets.

EXEMPLE 1 Les revues de conception intègrent normalement à la fois des aspects liés à la sûreté de fonctionnement et aux performances.

e) Identifier les cibles.

EXEMPLE 2 Les cibles peuvent être des exigences de sûreté de fonctionnement, des calendriers et des budgets du projet, etc., applicables à la sûreté de fonctionnement.

f) Recueillir des preuves et des informations.

g) Préparer et tenir des réunions.

h) Évaluer l'écart entre les exigences et les performances réelles.

i) Identifier et surveiller les risques et les secteurs critiques.

j) Analyser les résultats des revues et recommander des actions.

k) Vérifier l'efficacité des modifications apportées.

Les revues de sûreté de fonctionnement qui sont effectuées tout au long du cycle de vie, y compris la description détaillée des tâches concernées, sont abordées dans l'IEC 62960.

7.5 Assurance

7.5.1 Objet

L'objet de l'assurance de la sûreté de fonctionnement est de donner aux responsables et aux autres parties prenantes une confiance légitime dans le fait que leurs objectifs de sûreté de fonctionnement ont été ou seront atteints et que les risques sont contrôlés à un niveau acceptable. L'assurance peut se rapporter à n'importe quel aspect des objectifs de sûreté de fonctionnement (voir 7.2.3).

NOTE Cette activité de sûreté de fonctionnement est une version de la vue du processus d'assurance fournie dans l'ISO/IEC/IEEE 15026-4 qui est spécifique à l'assurance de la sûreté de fonctionnement.

7.5.2 Résultats

Résultat de l'assurance:

a) les parties prenantes comprennent sans ambiguïté la réalisation déclarée des objectifs de sûreté de fonctionnement par une déclaration explicite des performances de sûreté de fonctionnement;

b) il est vérifié que les processus et les systèmes, produits et services sont conformes à leurs exigences, normes et recommandations, et que les procédures définies sont suivies;

c) une déclaration justifiée des performances de sûreté de fonctionnement peut être fournie;

d) des preuves et des arguments sont présentés pour fournir aux parties prenantes le niveau de confiance exigé dans la réalisation revendiquée des objectifs de sûreté de fonctionnement;

e) les parties prenantes, notamment les responsables, sont davantage convaincues que leurs besoins, leurs objectifs, leurs attentes et leurs exigences, ainsi que les objectifs commerciaux, ont été ou seront obtenus.

7.5.3 Tâches

Il convient que les tâches suivantes soient entreprises conformément aux politiques organisationnelles applicables:

a) s'engager auprès des parties prenantes pour établir de manière continue leurs besoins, leurs attentes et leurs exigences et les tenir informées, suivant le cas (voir 8.2);

b) fournir la preuve que les risques de non-obtention d'un objectif de sûreté de fonctionnement ont été identifiés et traités et que les opportunités d'amélioration de la sûreté de fonctionnement ont été exploitées (voir 8.3);

c) fournir la preuve sous forme d'analyse démontrant que la sûreté de fonctionnement peut être obtenue lorsque le mesurage direct est impossible ou non approprié (voir 8.4);

d) recueillir et évaluer les données relatives aux performances de sûreté de fonctionnement du système, produit ou service, ou de ses composants, dans des conditions d'utilisation ou d'essai (voir 8.5);

e) vérifier que les exigences sont ou seront satisfaites et que toute non-conformité a été corrigée en utilisant les preuves de b), c) et d) ci-dessus;

f) vérifier que les procédures sont suivies par l'examen, la revue et l'audit, etc.;

g) valider que les systèmes, produits et services répondent aux besoins et aux attentes des parties prenantes;

h) fournir la preuve que le soutien est assuré pour maintenir les performances des personnes et la capacité du système de s'adapter à l'évolution des besoins (voir 8.6).

L'assurance progressive que les exigences de sûreté de fonctionnement sont ou seront satisfaites tout au long du cycle de vie d'un système peut être fournie dans une étude de sûreté de fonctionnement (voir IEC 62741). Celui-ci fournit:

- un ensemble d'affirmations qui formulent l'affirmation générale selon laquelle la sûreté de fonctionnement est atteinte;
- un argument raisonné et auditable qui étaye l'ensemble d'affirmations;
- la preuve que les risques ont été traités et que l'affirmation a été ou sera obtenue.

NOTE 1 L'assurance progressive signifie que les tâches d'assurance sont réalisées tout au long du cycle de vie et les résultats fournis lors des étapes importantes du projet. Cela réduit le risque de découvrir seulement à la fin d'un projet que les preuves sont insuffisantes.

NOTE 2 Les activités et tâches de sûreté de fonctionnement nécessaires pour fournir des preuves relatives à une affirmation de la sûreté de fonctionnement définissent également les activités et tâches de sûreté de fonctionnement nécessaires d'un programme de sûreté de fonctionnement.

7.6 Garantie de la redevabilité

7.6.1 Objet

L'objet de l'activité d'établissement de la redevabilité est d'établir la relation entre une non-conformité à un accord explicite et ses conséquences pour les parties prenantes et la société en général. Cela inclut de s'assurer que les parties prenantes redevables s'acquittent de leur obligation de fournir des solutions convenues pour les dommages causés par la non-conformité, de façon à acquérir la confiance dans le système des parties prenantes non redevables et du grand public.

NOTE 1 Les accords explicites peuvent inclure le contrat d'acquisition sur le système, les exigences spécifiées du système, l'assurance d'affirmations de la sûreté de fonctionnement identifiées ou un programme de sûreté de fonctionnement spécifié. Elles peuvent impliquer des parties prenantes externes et internes, ainsi que le grand public (par l'intermédiaire par exemple de réglementations).

NOTE 2 L'IEC 62853 fournit un exemple plus détaillé de cette activité de sûreté de fonctionnement comme vue du processus d'établissement de la redevabilité.

7.6.2 Résultats

Résultat de la garantie de la redevabilité:

a) pour toute non-conformité à des accords explicites, y compris une défaillance du système, les parties prenantes concernées et, le cas échéant, le grand public sont en mesure d'identifier les parties prenantes redevables;

b) les parties prenantes concernées et, le cas échéant, le grand public reçoivent des informations adéquates et des solutions convenues par les parties prenantes redevables;

c) des informations sur l'état de préparation pour a) et b) sont disponibles à tout moment, même avant qu'un événement ne se produise, de sorte que:

- toutes les parties prenantes sont conscientes de leur redevabilité;
- toutes les parties prenantes et le grand public ont confiance dans les conséquences d'une défaillance du système ou d'une non-conformité à des accords explicites.

NOTE L'établissement de la redevabilité complète de manière cruciale l'assurance de la sûreté de fonctionnement en assurant la confiance dans le système. La confiance dans les conséquences d'une non-conformité aux affirmations de la sûreté de fonctionnement est importante, indépendamment du niveau de confiance exigé dans les affirmations de la sûreté de fonctionnement, ce qui offre une possibilité de compromis entre les deux.

7.6.3 Tâches

Il convient que les tâches suivantes soient entreprises conformément aux politiques organisationnelles applicables:

a) pour chaque non-conformité potentielle à des accords explicites:

- identifier les décisions clés dans le cycle de vie du système et les activités de sûreté de fonctionnement susceptibles de provoquer la non-conformité;
- identifier la partie prenante redevable pour chaque décision clé;
- évaluer les impacts de la non-conformité sur les parties prenantes non redevables et le grand public;
- convenir des implications de la non-conformité pour les parties prenantes redevables, ainsi que pour les parties prenantes non redevables et le grand public, y compris les solutions que les parties prenantes redevables seront tenues de fournir;

b) surveiller, évaluer et retransmettre aux parties prenantes redevables les résultats attendus et imprévus des décisions clés, y compris la non-conformité et ses impacts réels;

c) permettre aux parties prenantes redevables de fournir rapidement des informations adéquates et les solutions convenues aux parties prenantes non redevables et au public en cas de non-conformité;

d) communiquer à toutes les parties prenantes et, le cas échéant, au grand public comment a), b) et c) sont mis en œuvre.

8 Activités techniques de sûreté de fonctionnement

8.1 Vue d'ensemble

L'Article 8 décrit les activités techniques de sûreté de fonctionnement qui visent à satisfaire aux exigences de sûreté de fonctionnement et donnent l'assurance qu'elles ont été ou seront réalisées. Elles sont:

- l'engagement des parties prenantes (y compris la recherche d'un consensus et la consultation);
- la gestion des opportunités, des menaces et des risques pour les objectifs de sûreté de fonctionnement;
- l'analyse des attributs de sûreté de fonctionnement (y compris l'analyse mathématique et statistique, la modélisation, la simulation et la prévision des attributs de sûreté de fonctionnement et des coûts du cycle de vie);
- l'évaluation de la sûreté de fonctionnement (y compris le recueil et l'évaluation des informations et des données);

  NOTE Les informations et les données comprennent les données d'exploitation et d'essai relatives à un système, produit ou service, ainsi qu'aux informations et aux données pour prendre en charge la sûreté de fonctionnement et la gestion de projet.

- la maintenance, le soutien et l'amélioration.

L'Annexe E fournit des exemples de tâches et d'outils qui peuvent s'appliquer à chaque étape du cycle de vie.

L'Annexe F explique comment ces activités de sûreté de fonctionnement peuvent être liées aux processus du cycle de vie du système fournis dans l'ISO/IEC/IEEE 15288.

Les activités relatives aux programmes de maintenabilité et de supportabilité sont également couvertes dans l'IEC 60300-3-10 et l'IEC 60300-3-14.

8.2 Engagement des parties prenantes, recherche d'un consensus et communication

8.2.1 Objet

L'objet de l'engagement avec les parties prenantes dans le contexte de la sûreté de fonctionnement est:

a) d'établir et de maintenir des relations positives avec les parties prenantes internes et externes;

b) de comprendre les besoins et les attentes des parties prenantes de manière à ce que les exigences de sûreté de fonctionnement puissent être énoncées et atteintes, et que leur réalisation soit fiable;

c) d'établir la base de la redevabilité par le biais d'accords explicites;

d) d'établir et promouvoir une compréhension commune du système permettant de résoudre les problèmes de sûreté de fonctionnement qui ne sont pas prévus dans les accords explicites;

e) de fournir des éléments d'informations nécessaires à l'identification des risques de sorte qu'ils puissent être traités le plus tôt possible;

f) de permettre l'intégration efficace des activités de sûreté de fonctionnement dans les projets et dans les processus commerciaux et techniques;

g) d'améliorer les performances de la main-d'œuvre de sorte que les capacités techniques du système et des produits puissent être pleinement exploitées et que les problèmes de sûreté de fonctionnement liés aux facteurs humains puissent être résolus;

h) de recevoir les retours d'information des parties prenantes pour faciliter l'amélioration.

Il convient que l'engagement des parties prenantes commence à la première occasion et se poursuive tout au long du cycle de vie. Les parties prenantes qui peuvent être pertinentes dans un contexte particulier sont détaillées à l'Annexe C.

8.2.2 Résultats

Résultat de l'engagement auprès des parties prenantes:

a) des relations positives sont établies avec les gestionnaires, les responsables de projets, les clients, les fournisseurs, les organismes de réglementation, etc., suivant le cas;

b) les responsables et le personnel sont conscients de l'importance de la sûreté de fonctionnement et sont encouragés et soutenus pour l'obtenir;

c) il existe une compréhension commune entre les parties prenantes concernées de l'objet du système, produit ou service, de ses contraintes et de ses exigences de sûreté de fonctionnement, ainsi que des responsabilités, des redevabilités et des autorités;

d) les besoins et les attentes des parties prenantes sont compris et convertis en exigences vérifiables;

e) les exigences et les données de sûreté de fonctionnement sont communiquées efficacement aux parties prenantes appropriées au cours des différentes étapes du cycle de vie;

f) des accords explicites sont formulés et maintenus, y compris des accords sur la redevabilité de chaque partie prenante en cas de non-conformité;

g) la traçabilité des exigences de sûreté de fonctionnement pour les parties prenantes et leurs besoins est établie;

h) les parties prenantes sont assurées que leurs attentes en matière de sûreté de fonctionnement sont satisfaites;

i) les risques de non-respect des exigences de sûreté de fonctionnement sont identifiés et traités le plus tôt possible;

j) les échecs et réussites sont consignés et compris de sorte que la sûreté de fonctionnement puisse être améliorée;

k) les décisions et accords clés sont consignés accompagnés de leur justification, de sorte que la redevabilité puisse être tracée et les connaissances acquises lorsque les décisions s'avèrent défaillantes;

l) les déficiences de performance de la main-d'œuvre ou de l'organisme, susceptibles d'affecter la sûreté de fonctionnement, sont identifiées et atténuées de sorte que les capacités techniques puissent être pleinement réalisées.

8.2.3 Tâches

Il convient que les tâches suivantes soient exécutées conformément aux politiques applicables de l'organisme et aux résultats exigés:

a) identifier les parties prenantes internes et externes et évaluer et documenter leur intérêt et leur influence;

NOTE 1 Les parties prenantes peuvent varier avec le temps, par exemple lors de changements de propriété ou de déplacement de celle-ci entre les étapes du cycle de vie ou lors d'une longue étape d'utilisation.

b) identifier les parties prenantes qu'il convient d'impliquer dans des tâches particulières de sûreté de fonctionnement, telles que l'appréciation ou la vérification du risque, et celles auxquelles il convient de communiquer les résultats;

c) développer des plans de communication;

d) élaborer une politique de gestion du changement d'accords;

e) s'engager auprès des parties prenantes conformément aux plans de communication;

f) convenir d'un processus d'arbitrage pour résoudre les conflits lorsqu'un consensus ne peut pas être atteint;

g) obtenir et documenter les besoins, les attentes et les redevabilités des parties prenantes en matière de sûreté de fonctionnement. Il convient de tenir compte des éléments suivants:

- l'utilisation ou l'interaction prévue par les parties prenantes avec le système, produit ou service, ainsi que son environnement d'exploitation et profil de cycle de vie;
- toutes les redevabilités des parties prenantes en ce qui concerne le système, produit ou service et sa gestion, son utilisation ou son soutien;
- les besoins, les souhaits et les attentes des parties prenantes en ce qui concerne la fiabilité, la disponibilité, la maintenabilité, la supportabilité, ainsi que toute autre exigence relative à la sûreté de fonctionnement;
- toute contrainte qui influence la gestion de la sûreté de fonctionnement;
- la manière dont les attributs de sûreté de fonctionnement peuvent être mesurées ou assurées;

h) analyser les attentes des parties prenantes et identifier et résoudre tout conflit;

i) établir et maintenir des accords explicites, consigner les comptes rendus des négociations et justifier les décisions prises;

j) communiquer les informations associées à la sûreté de fonctionnement aux parties prenantes concernées en temps opportun;

k) obtenir des retours d'information sur les problèmes de sûreté de fonctionnement pour la résolution de problème et l'amélioration continue;

l) examiner périodiquement les parties prenantes et les plans de communication et les mettre à jour si nécessaire.

NOTE 2 L'IEC 62853 fournit la vue de processus de recherche d'un consensus, qui détaille la partie de cette activité de sûreté de fonctionnement concernant la recherche d'un consensus.

8.3 Gestion des opportunités, des menaces et des risques

8.3.1 Objet

L'objet de la gestion des opportunités, des menaces et des risques dans le contexte de la sûreté de fonctionnement est:

a) d'atteindre les objectifs de sûreté de fonctionnement et d'améliorer la prise de décision par la compréhension et la gestion des effets de l'incertitude sur ces objectifs;

NOTE Les objectifs de sûreté de fonctionnement comprennent la satisfaction des exigences du système, produit ou service et tout autre objectif organisationnel susceptible d'affecter ou d'être affecté par des activités de sûreté de fonctionnement, par exemple les objectifs relatifs à la sécurité, à l'environnement ou à la satisfaction du client.

b) de comprendre la manière dont les défaillances peuvent se produire afin de les prévenir ou d'en atténuer les effets;

c) d'exploiter les opportunités d'améliorer la sûreté de fonctionnement et les activités de sûreté de fonctionnement;

d) d'établir des priorités (par exemple objectifs et activités de sûreté de fonctionnement) en fonction du risque;

e) de fournir de l'assurance en démontrant que les risques pour la sûreté de fonctionnement ont été contrôlés.

8.3.2 Résultats

Résultat de la gestion des risques, des menaces et des opportunités:

a) les risques pour la sûreté de fonctionnement des systèmes, produits et services, ainsi que pour les activités de sûreté de fonctionnement sont identifiés, compris et contrôlés;

b) l'efficacité d'un programme d'activités de sûreté de fonctionnement est améliorée à mesure que les activités sont orientées vers la meilleure gestion des risques;

c) les possibilités d'améliorer la sûreté de fonctionnement et les activités de sûreté de fonctionnement sont exploitées;

d) les décisions sont basées sur une bonne compréhension des opportunités, des menaces et des risques, et sont justifiables et traçables;

e) les actions humaines et les processus organisationnels, ainsi que les systèmes, produits et services font l'objet de moins de défaillances et sont plus fiables;

f) l'incertitude des données est comprise et, le cas échéant, quantifiée;

g) la compréhension de la manière dont les systèmes peuvent être défaillants permet d'améliorer les conceptions et de mettre en œuvre des programmes de maintenance et d'assistance rentables;

h) les modifications, et la nécessité d'améliorations, sont identifiées et gérées efficacement;

i) la préparation est faite pour les défaillances potentielles, y compris les réponses génériques aux défaillances qui n'ont pas été reconnues à l'avance;

j) des informations sur les risques sont disponibles pour ceux qui en ont besoin;

k) il est assuré que les risques sont gérés en fonction de la disposition de l'organisme à prendre des risques.

8.3.3 Tâches

Il convient que les tâches suivantes soient réalisées suivant le contexte:

a) identifier les parties prenantes qu'il convient d'impliquer dans des activités d'évaluation des risques et celles qu'il convient de tenir informées;

b) établir un mécanisme de communication et de consultation sur les risques et leur traitement avec les parties prenantes appropriées;

c) déterminer le domaine d'application, le contexte et la temporisation des tâches de management du risque et la manière qu'il convient de les inclure dans le domaine d'application des autres activités de management du risque de l'organisme;

d) décider de la manière dont le risque acceptable sera défini;

e) identifier les opportunités, les menaces et les risques et les prendre en compte dans les décisions prises à chaque étape du cycle de vie. Les outils d'identification des risques comprennent l'analyse des modes de défaillance et de leurs effets (IEC 60812), les études HAZOP (IEC 61882) et d'autres outils décrits dans l'IEC 31010;

f) analyser les risques en examinant les causes, les conséquences et les contrôles déjà mis en œuvre. Le cas échéant, déterminer la probabilité d'apparition de conséquences particulières. Des outils tels que l'analyse par arbre de panne (IEC 61025) et l'analyse par arbre d'événement (IEC 62502) peuvent être utilisés (voir également l'IEC 31010);

NOTE 1 Les outils utilisés pour l'analyse de la sûreté de fonctionnement peuvent également être utilisés pour analyser le risque de manière plus générale.

g) coordonner les activités de management du risque et l'utilisation d'outils d'appréciation du risque pour éviter la duplication des efforts;

h) identifier les opportunités et les analyser en comparant les avantages escomptés et les risques liés au fait de saisir ou non l'opportunité;

i) appliquer la compréhension des risques dans la conception du programme au cours de chaque étape de cycle de vie;

j) planifier et mettre en œuvre des actions fondées sur la compréhension tirée de l'analyse des risques afin de traiter les risques inacceptables;

k) attribuer les responsabilités, les autorités et les redevabilités pour les actions liées aux risques et au cadre organisationnel du management du risque;

l) surveiller le statut des risques et de leurs traitements;

m) analyser les causes directes et sous-jacentes des défaillances afin de pouvoir en tirer des leçons et prévenir les défaillances (voir IEC 62740);

n) surveiller les changements d'environnement, de contexte et d'objet, etc., et analyser leur incidence sur le risque;

o) surveiller les résultats attendus et imprévus des décisions, et relayer les résultats en temps opportun afin d'améliorer la réponse aux défaillances et l'établissement de la redevabilité;

p) recueillir, analyser, stocker, passer en revue et mettre à jour les informations relatives aux risques, tout au long du cycle de vie;

q) assurer le suivi des actions recommandées relatives aux risques, aux menaces et aux opportunités.

NOTE 2 L'ISO 31000 fournit des recommandations sur les principes, le cadre et le processus de management du risque. Le management du risque dans les projets est traité dans l'IEC 62198 et les outils d'appréciation du risque dans l'IEC 31010.

8.4 Analyse de la sûreté de fonctionnement

8.4.1 Objet

L'objet de l'analyse de la sûreté de fonctionnement est de fournir une compréhension technique du système, produit ou service, ainsi que des facteurs affectant sa sûreté de fonctionnement et ses coûts de cycle de vie. Elle peut être utilisée:

- comme élément d'informations nécessaire à la prise de décision;
- pour modéliser et prévoir les résultats de la sûreté de fonctionnement d'une conception;
- pour atteindre et améliorer la sûreté de fonctionnement de manière rentable;
- pour vérifier que les exigences sont ou peuvent être satisfaites.

Les analyses sont également réalisées dans le cadre de la gestion des opportunités, des dangers et des risques (8.3), de l'évaluation de la sûreté de fonctionnement (8.5) et de la vérification de la sécurité, par exemple le niveau d'intégrité de sécurité (SIL) pour les systèmes électroniques relatifs à la sécurité (voir la série IEC 61508) et le niveau d'intégrité de sécurité automobile (ASIL) pour les véhicules (voir la série ISO 26262).

8.4.2 Résultats

Résultat de l'analyse de la sûreté de fonctionnement:

a) une compréhension technique du système, produit ou service et de son environnement d'exploitation est obtenue;

b) les caractéristiques communes et les contraintes les plus défavorables de l'environnement d'exploitation sont identifiées;

c) les caractéristiques de la sûreté de fonctionnement, de coût et de risque des options de conception sont prévues et comparées;

d) une conception rentable est sélectionnée dont la satisfaction aux exigences peut être démontrée dans des conditions et des contraintes spécifiées;

e) les parties prenantes sont assurées que leurs besoins et exigences de sûreté de fonctionnement ont été ou seront satisfaits;

f) le système est conçu en tenant compte de sa mise au rebut éventuelle en tenant compte de l'économie circulaire et de la nécessité de réduire au minimum l'impact environnemental;

g) les modes de défaillance potentiels sont identifiés de sorte qu'ils puissent être évités ou que leurs effets soient atténués;

h) les implications en matière de coût des décisions relatives à la sûreté de fonctionnement sont comprises;

i) les facteurs affectant la fiabilité, la maintenabilité, la supportabilité, ainsi que d'autres attributs liés à la sûreté de fonctionnement tels que la disponibilité, l'exploitabilité, l'utilisabilité, la supportabilité, etc., sont compris et des décisions d'arbitrage sont prises;

j) les rôles du matériel, des logiciels et des personnes dans un système sont optimisés de sorte que leurs performances ne compromettent pas les capacités globales du système;

k) les systèmes et les produits sont mis au rebut d'une manière sûre, sécurisée, écologique et conforme à la législation et aux normes.

8.4.3 Tâches

L'analyse de la sûreté de fonctionnement peut inclure les tâches suivantes:

a) mettre en correspondance les caractéristiques de conception avec l'environnement de l'utilisateur final pour contribuer à définir des exigences ou à choisir des options de conception;

NOTE 1 Les facteurs à prendre en compte peuvent inclure la compatibilité électromagnétique, les conditions thermiques et les contraintes mécaniques.

b) prévoir les valeurs des attributs de sûreté de fonctionnement;

c) entreprendre un processus itératif d'analyse et d'amélioration à mesure que la conception progresse pour améliorer la sûreté de fonctionnement;

d) effectuer une analyse de régression pour vérifier que les modifications n'ont pas affecté la fonctionnalité existante d'un service, produit ou système;

e) réaliser une analyse du coût du cycle de vie afin d'optimiser les performances de sûreté de fonctionnement tout en respectant les contraintes de coût du cycle de vie données (voir IEC 60300-3-3);

f) effectuer des analyses de compromis;

g) analyser les modes de défaillance potentiels, les causes et les effets afin d'améliorer les conceptions, planifier les programmes de maintenance et de soutien et planifier la réponse aux défaillances (IEC 60812);

NOTE 2 Les techniques utilisées pour l'analyse des causes profondes peuvent également être utilisées de manière proactive pour identifier les modes et causes de défaillance (voir IEC 62740).

h) analyser la sûreté de fonctionnement du système en modélisant les conditions de contraintes et la saisie de données corrompues ou illégales;

i) analyser l'effet des performances humaines sur les activités de sûreté de fonctionnement et les attributs de sûreté de fonctionnement du système, produit ou service. Le cas échéant, développer des programmes visant à améliorer le taux d'erreur humaine (IEC 62508);

j) analyser les processus utilisés dans la fabrication, la livraison et l'installation afin de réduire le plus possible l'impact sur la sûreté de fonctionnement. L'AMDE des processus peut être utilisée (voir IEC 60812);

k) analyser les modifications et les améliorations de conception pour les questions de sécurité et d'exploitabilité (voir IEC 61882) et vérifier la réalisation des améliorations prévues;

l) analyser les systèmes préalablement à leur mise au rebut en vue d'un éventuel réemploi ou d'une réutilisation de modules, composants et matériaux (voir IEC 62309). Prévoir des moyens de transfert ou de suppression sécurisés de données.

NOTE 3 Le processus d'analyse des systèmes (ISO/IEC/IEEE 15288) fournit des tâches génériques qui s'appliquent à toute tâche d'analyse. L'Annexe F fournit une comparaison des deux approches.

L'IEC 62308, l'IEC 62508, l'IEC 60300-3-1, l'IEC 60300-3-10 et l'IEC 60300-3-14 abordent les analyses relatives respectivement à la fiabilité, à la maintenabilité et à la supportabilité.

8.5 Évaluation de la sûreté de fonctionnement

8.5.1 Objet

L'évaluation de la sûreté de fonctionnement a pour objet de:

a) déterminer les caractéristiques de sûreté de fonctionnement d'un système, produit ou service;

b) vérifier que la sûreté de fonctionnement des personnes, des systèmes, des produits, des services et des processus satisfait aux exigences;

c) valider que la sûreté de fonctionnement satisfait aux besoins des parties prenantes;

d) détecter et éliminer les défauts;

e) surveiller la sûreté de fonctionnement à mesure de la mise en œuvre de stratégies d'amélioration afin de satisfaire aux besoins de l'entreprise (par exemple améliorer les performances de sûreté de fonctionnement, réduire les coûts et améliorer l'opportunité des lancements de produits);

f) tirer parti des données d'exploitation et des essais pour améliorer la conception;

g) améliorer la manière dont les activités de sûreté de fonctionnement sont réalisées;

h) évaluer les aspects de sûreté de fonctionnement d'un projet;

i) fournir des informations relatives aux revues de sûreté de fonctionnement (voir IEC 62960).

NOTE L'ISO/IEC/IEEE 15288 décrit le Processus d'évaluation et de contrôle du projet tout au long du cycle de vie qui peut être appliqué pour évaluer les aspects de sûreté de fonctionnement d'un projet.

8.5.2 Résultats

Résultat de l'évaluation de la sûreté de fonctionnement:

a) les mesures de performance sont disponibles;

b) les besoins d'information et les méthodes de recueil de données sont identifiés;

c) les informations et les données sont recueillies, vérifiées et stockées;

d) les données sont analysées et les résultats sont interprétés et consignés;

e) les caractéristiques de sûreté de fonctionnement du système, produit ou service sont connues et quantifiées si possible;

f) les caractéristiques de sûreté de fonctionnement souhaitées sont obtenues, vérifiées et validées;

g) les informations et les données sont disponibles, permettant d'améliorer la sûreté de fonctionnement et sa gestion;

h) la traçabilité des résultats est établie;

i) les parties prenantes reçoivent les données dont elles ont besoin dans le format et les délais exigés;

j) les objectifs du projet et de la sûreté de fonctionnement sont atteints.

8.5.3 Tâches

L'évaluation de la sûreté de fonctionnement peut inclure les tâches suivantes.

a) Identifier le problème ou la question qui exige une évaluation.

b) Déterminer les besoins et les exigences des parties prenantes et le format des données de sortie exigé.

c) Déterminer la façon de mesurer ou de vérifier les attributs de sûreté de fonctionnement et les données exigées.

d) Déterminer les éléments d'informations et les données associées exigés pour réaliser l'évaluation.

e) Déterminer les conditions d'essai, les exigences de données et les méthodes d'essai (voir IEC 60300-3-5).

f) Déterminer les ressources disponibles et les contraintes (par exemple temps, fonds, échantillons, personnel, outils et installations). Il est important que les résultats des essais soient disponibles pour fournir des éléments d'informations nécessaires à la prise de décisions critiques. Ils peuvent avoir une incidence sur la conception de la procédure d'essai.

g) Déterminer la source des données et la manière et le moment où elles sont recueillies (par exemple à partir de simulations et de modèles, à partir d'essais dans un environnement simulé, à partir d'observations en fonctionnement normal ou à partir de données du fabricant, etc.).

NOTE 1 Les données provenant des fournisseurs de composants et de modules, ou d'observations sur le terrain et d'essais de systèmes, de produits et de services similaires peuvent être utilisées pour prédire et améliorer la sûreté de fonctionnement pendant la conception (voir IEC 62308).

NOTE 2 L'IEC 60300-3-2 fournit des recommandations pour recueillir des données de sûreté de fonctionnement dans des conditions d'exploitation.

h) Intégrer l'évaluation de la sûreté de fonctionnement dans les processus pertinents.

i) Recueillir des informations et des données. Cela peut impliquer la mesure des attributs de sûreté de fonctionnement, la surveillance des performances des systèmes, produits et services pour vérifier que les performances ne sont pas dégradées au fil du temps, des enquêtes, des observations et des essais (voir Annexe G).

j) Interpréter les données.

k) Comparer les caractéristiques réelles de sûreté de fonctionnement à celles souhaitées, mettre en œuvre des améliorations et réaliser des essais de non-régression, tel qu'exigé (voir IEC 61014).

l) Consigner les données de telle sorte que la traçabilité puisse être obtenue entre les variations de produit et les résultats de coût et de performance.

m) Stocker les données de sorte qu'elles puissent être utilisées pour une référence ultérieure.

n) Communiquer les résultats aux parties prenantes, le cas échéant.

Les techniques des essais de fiabilité sont abordées dans l'IEC 60300-3-5 et celles des essais de maintenabilité dans l'IEC 60300-3-10. Les techniques des essais logiciels sont couvertes par l'ISO/IEC/IEEE 29119-4.

8.6 Maintenance, soutien et amélioration

8.6.1 Objet

L'objet de la maintenance, du soutien et de l'amélioration dans le contexte de la sûreté de fonctionnement est de:

a) maintenir les performances du système, produit ou service;

b) gérer les coûts du cycle de vie;

c) permettre aux systèmes, produits et services de continuer à atteindre les objectifs de sûreté de fonctionnement pendant l'exploitation d'une manière rentable;

d) gérer les informations nécessaires à l'exploitation en continu et à l'amélioration future (y compris les données relatives aux défauts et aux défaillances);

e) réduire le plus possible les dommages et les perturbations dus aux défaillances;

f) maintenir le statut d'applicabilité du système ou du produit en dépit des modifications des exigences, des environnements, des objectifs et de l'objet;

g) gérer l'obsolescence (voir IEC 62402);

h) soutenir et améliorer la capacité des parties prenantes (par exemple des travailleurs ou des utilisateurs) à exploiter le système ou à utiliser le produit;

i) améliorer la sûreté de fonctionnement des systèmes, produits et services, ainsi que l'efficacité et l'efficience des activités de sûreté de fonctionnement.

8.6.2 Résultats

Résultat de l'activité de maintenance, de soutien et d'amélioration:

a) les systèmes, les produits et leurs composants sont conçus de telle sorte qu'ils soient exploitables de façon sûre et fiable, qu'ils soient maintenables, contrôlables et réutilisables;

b) les exigences de l'utilisateur relatives à la maintenabilité et à la disponibilité pendant l'exploitation sont satisfaites et assurées;

c) les programmes de maintenance sont planifiés et mis en œuvre;

d) le soutien est organisé et remplit son rôle efficacement;

e) les personnes sont soutenues afin de remplir leurs rôles de manière efficace et efficiente;

f) les risques pour la maintenance et les dispositions de soutien sont identifiés et traités;

g) les effets des défaillances sont réduits le plus possible;

h) le système, produit ou service fonctionne tel qu'exigé, en dépit des modifications apportées aux exigences, aux objectifs d'environnement et à l'objet;

i) les améliorations sont mises en œuvre par le biais d'un processus contrôlé;

j) toutes les modifications apportées aux logiciels et au matériel sont connues et tracées à tout moment.

8.6.3 Tâches

La maintenance, le soutien et l'amélioration peuvent inclure les tâches suivantes.

a) Fournir des éléments d'informations à l'équipe de conception en ce qui concerne la maintenabilité et la supportabilité.

b) Identifier les modes, mécanismes et effets potentiels des défaillances comme éléments d'informations nécessaires à la définition d'un programme de maintenance (voir IEC 60812);

c) Intégrer les facteurs humains dans la conception pour assurer l'utilisabilité, la maintenabilité et la supportabilité.

d) Définir une stratégie de maintenance et de soutien (voir IEC 60300-3-12).

e) Définir un programme initial de maintenance pendant la conception et le développer continuellement tout au long du cycle de vie (voir IEC 60300-3-10 et l'IEC 60300-3-11).

f) Planifier la maintenance et le soutien, y compris les besoins en ressources, les niveaux de compétences et les calendriers pour obtenir une solution abordable, exploitable, soutenable et durable.

g) Spécifier les services de soutien externes nécessaires et élaborer des accords (voir IEC 60300-3-16).

h) Identifier, analyser et traiter les risques pour les programmes de maintenance et de soutien, y compris ceux associés aux dispositions contractuelles et à la chaîne d'approvisionnement.

i) Gérer les pièces de rechange (voir IEC 62550).

j) Réaliser la maintenance et organiser la logistique de maintenance.

k) Recueillir et revoir les données relatives à la maintenance et au soutien et les comparer avec les spécifications et exigences de maintenabilité et de supportabilité.

l) Mettre en place un système de compte rendu des échecs et des succès (LTIAC ou DRACAS) et recueillir des données relatives aux réussites, aux échecs et aux non-conformités pendant les essais et sur le terrain (voir IEC 60300-3-2 et l'IEC 60300-3-5).

NOTE 1 Pour les défaillances des systèmes en exploitation, les défaillances observées sont uniquement reliées aux conditions d'exploitation au moment où la défaillance a eu lieu.

NOTE 2 L'analyse de défaillance au cours des essais accélérés et des essais de contraintes peut être utilisée pour identifier les modes de défaillance susceptibles de se produire également en cours d'utilisation (voir IEC 62506 et série IEC 61163).

m) Fournir des éléments d'informations nécessaires à la prise de décisions relatives à l'évolution et à l'amélioration.

n) Contrôler et tracer les modifications de la conception du système, concernant le matériel, les micrologiciels, les logiciels et la documentation.

o) Gérer les sous-traitants et les fournisseurs.

p) Gérer l'obsolescence (voir IEC 62402).

q) Fournir des informations concernant les coûts et les aspects pratiques de la maintenance et du soutien (y compris les considérations d'obsolescence) pour contribuer à prendre des décisions relatives à la mise au rebut.

r) Evaluer et appliquer des méthodes d'allongement de la durée de vie telles que mises à jour, mises à niveau ou remises à neuf.

s) Identifier les entités susceptibles d'être réutilisées et fournir des données pertinentes concernant leur état.

L'IEC 60300-3-10 fournit de plus amples informations concernant les tâches de maintenance et de maintenabilité et l'IEC 60300-3-14 sur le soutien et la supportabilité. Le soutien logistique intégré est couvert par l'IEC 60300-3-12.

Annexe A
(informative)

Normes IEC relatives à la sûreté de fonctionnement

Tableau A.1 – Classification des normes de sûreté de fonctionnement par sujet et par étape du cycle de vie

Classification	Étape du cycle de vie				
	Conc.	Dév.	Réal.	E/M	Rebut
Principes essentiels					
IEC 60500-192, *Vocabulaire Électrotechnique International – Partie 192: Sûreté de fonctionnement*	✓	✓	✓	✓	✓
IEC 61703, *Expressions mathématiques pour les termes de fiabilité, de disponibilité, de maintenabilité et de logistique de maintenance*	✓	✓	✓	✓	✓
Normes de niveau supérieur – normes de processus					
IEC 60300-1, *Gestion de la sûreté de fonctionnement – Partie 1: Gérer la sûreté de fonctionnement*	✓	✓	✓	✓	✓
IEC 62853, *Sûreté de fonctionnement des systèmes ouverts*	✓	✓	✓	✓	✓
IEC 62508, *Lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement*	✓	✓	✓	✓	✓
IEC 60300-3-3, *Gestion de la sûreté de fonctionnement – Partie 3-3: Guide d'application – Évaluation du coût du cycle de vie*	✓	✓	✓	✓	✓
IEC 62402, *Gestion de l'obsolescence*	✓	✓	✓	✓	✓
IEC 62741, *Démonstration des exigences de sûreté de fonctionnement – Argumentaire dans le cadre de la sûreté de fonctionnement*	✓	✓	✓	✓	✓
IEC/TS 62775, *Application guidelines – Technical and financial processes for implementing asset management systems* (disponible en anglais seulement)	✓	✓	✓	✓	✓
IEC 62960, *Revues de la sûreté de fonctionnement au cours du cycle de vie*	✓	✓	✓	✓	✓
Documentation et données					
IEC 60300-3-2, *Gestion de la sûreté de fonctionnement – Partie 3-2: Guide d'application – Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation*			✓	✓	
IEC 60300-3-4, *Gestion de la sûreté de fonctionnement – Partie 3-4: Guide d'application – Spécification d'exigences de sûreté de fonctionnement*	✓	✓			
Logiciels, communications et systèmes ouverts					
IEC 61907, *Ingénierie de la sûreté de fonctionnement des réseaux de communication*	✓	✓	✓	✓	
IEC 62673, *Méthodologie pour l'évaluation et l'assurance de la sûreté de fonctionnement d'un réseau de communication*	✓	✓	✓	✓	✓
IEC 62628, *Lignes directrices concernant la sûreté de fonctionnement du logiciel*	✓	✓	✓	✓	✓
Normes basées sur une discipline – niveau de programme					
IEC 60300-3-10, *Gestion de la sûreté de fonctionnement – Partie 3-10: Guide d'application – Maintenabilité et maintenance*[1]	✓	✓	✓	✓	✓

[1] En préparation. Stade au moment de la publication: IEC CDV 60300-3-10:2024.

Classification	Étape du cycle de vie				
	Conc.	Dév.	Réal.	E/M	Rebut
IEC 60300-3-14, *Gestion de la sûreté de fonctionnement – Partie 3-14: Guide d'application – Supportabilité et soutien*[2]	✓	✓	✓	✓	✓
Fiabilité					
IEC 61014, *Programmes de croissance de fiabilité*		✓	✓	✓	
IEC 61709, *Composants électriques – Fiabilité – Conditions de référence pour les taux de défaillance et modèles de contraintes pour la conversion*		✓			
IEC 62308, *Fiabilité de l'équipement – Méthodes d'évaluation de la fiabilité*		✓	✓		
Maintenance et maintenabilité					
IEC 60300-3-11, *Gestion de la sûreté de fonctionnement – Partie 3-11: Guide d'application – Maintenance basée sur la fiabilité*		✓	✓	✓	
IEC 60706-2, *Maintenabilité de matériel – Partie 2: Exigences et études de maintenabilité pendant la phase de conception et de développement*	✓	✓			
IEC 60706-3, *Maintenabilité de matériel – Partie 3: Vérification et recueil, analyse et présentation de données*		✓	✓	✓	
IEC 60706-5, *Maintenabilité de matériel – Partie 5: Testabilité et tests pour diagnostic*		✓	✓	✓	
IEC 62309, *Sûreté de fonctionnement des produits contenant des composants réutilisés – Exigences pour la fonctionnalité et les essais*	✓	✓			✓
Supportabilité et soutien					
IEC 60300-3-12, *Gestion de la sûreté de fonctionnement – Partie 3-12: Guide d'application – Soutien logistique intégré*		✓	✓	✓	
IEC 60300-3-16, *Gestion de la sûreté de fonctionnement – Partie 3-16: Guide d'application – Lignes directrices pour la spécification des services de support de maintenance*	✓	✓			
IEC 62550, *Approvisionnement en pièces de rechange*		✓	✓	✓	
Sûreté de fonctionnement et modélisation et analyse des risques					
IEC 31010, *Management du risque – Techniques d'appréciation du risque*	✓	✓	✓	✓	✓
IEC 60300-3-1, *Gestion de la sûreté de fonctionnement – Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique*	✓	✓	✓	✓	
IEC 60812, *Analyse des modes de défaillance et de leurs effets (AMDE et AMDEC)*	✓	✓	✓	✓	
IEC 61025, *Analyse par arbre de panne (AAP)*	✓	✓	✓	✓	
IEC 61078, *Diagrammes de fiabilité*	✓	✓		✓	
IEC 61165, *Applications des techniques de Markov*		✓			
IEC 61882, *Études de danger et d'exploitabilité (études HAZOP) – Guide d'application*	✓	✓		✓	
IEC 62198, *Managing risk in projects – Application guidelines*	✓	✓	✓	✓	✓
IEC 62502, *Techniques d'analyse de la sûreté de fonctionnement – Analyse par arbre d'événement (AAE)*		✓		✓	
IEC 62508, *Lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement*	✓	✓	✓	✓	✓
IEC 62740, *Analyse de cause initiale (RCA)*		✓	✓	✓	

[2] En préparation. Stade au moment de la publication: IEC FDIS 60300-3-14:2024.

Classification	Étape du cycle de vie				
	Conc.	Dév.	Réal.	E/M	Rebut
IEC 62551, *Techniques d'analyse de sûreté de fonctionnement – Techniques des réseaux de Petri*		✓		✓	
IEC/TR 63039, *Probabilistic risk analysis of technological systems – Estimation of final event rate at a given initial state* (disponible en anglais seulement)	✓	✓			
Essais de fiabilité et analyse statistique					
IEC 60300-3-5, *Gestion de la sûreté de fonctionnement – Partie 3-5: Guide d'application – Conditions des essais de fiabilité et principes des essais statistiques*		✓	✓	✓	
IEC 60605-2, *Essais de fiabilité des équipements – Partie 2: Conception des cycles d'essai*		✓	✓		
IEC 62506, *Méthodes d'essais accélérés de produits*		✓	✓		
IEC 60605-4, *Essai de fiabilité des équipements – Partie 4: Méthodes statistiques de distribution exponentielle – Estimateurs ponctuels, intervalles de confiance, intervalles de prédiction et intervalles de tolérance*		✓	✓	✓	
IEC 60605-6, *Essais de fiabilité des équipements – Partie 6: Tests pour la validité et l'estimation du taux de défaillance constant et de l'intensité de défaillance constante*		✓	✓	✓	
IEC 61070, *Procédures d'essai de conformité pour la disponibilité en régime établi*		✓	✓	✓	
IEC 61123, *Essais de fiabilité – Plans d'essai de conformité pour une proportion de succès*		✓	✓		
IEC 61124, *Essais de fiabilité – Plan d'essais de conformité d'un taux de défaillance constant et d'une intensité de défaillance constante*		✓	✓		
IEC 61649, *Analyse de Weibull*		✓	✓		
IEC 61650, *Techniques d'analyse des données de fiabilité – Procédures pour la comparaison de deux taux de défaillance constants et de deux intensités de défaillance (événements) constantes*		✓	✓		
IEC 61710, *Modèle de loi en puissance – Essais d'adéquation et méthodes d'estimation des paramètres*		✓	✓		
Déverminage					
IEC 61163-1, *Déverminage sous contraintes – Partie 1: Assemblages réparables fabriqués en lots*			✓	✓	
IEC 61163-2, *Déverminage sous contraintes – Partie 2: Composants*			✓	✓	
Légende – Abréviations utilisées dans le tableau Conc. Concept Dév. Développement Réal. Réalisation E/M Exploitation et maintenance Rebut Mise au rebut ✓ indique l'étape du cycle de vie pour laquelle la norme est pertinente					