IEC 60300-1

Edition 3.0 2014-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Dependability management – Part 1: Guidance for management and application

Gestion de la sûreté de fonctionnement – Partie 1: Lignes directrices pour la gestion et l'application

IEC 60300-1:2014-05 (en-fr)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

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

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

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

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 It also gives information on projects, replaced and withdrawn publications.

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

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 55 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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

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

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

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

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

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

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 14 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
Plus de 55 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

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

IEC 60300-1

Edition 3.0 2014-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Dependability management – Part 1: Guidance for management and application

Gestion de la sûreté de fonctionnement – Partie 1: Lignes directrices pour la gestion et l'application

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

X

ICS 03.100.40, 03.120.01, 21.020

ISBN 978-2-8322-1777-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

DEPENDABILITY MANAGEMENT –

Part 1: Guidance for management and application

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

This bilingual version (2014-08) corresponds to the English version, published in 2014-05.

This third edition cancels and replaces the second edition published in 2003 and constitutes a technical revision.

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

a) an updating of definitions to reflect IEC 60050-191:2014;
b) an enhanced description of dependability and its attributes;
c) a more generic approach to dependability management;
d) revised guidelines for application of dependability management;

e) a more generic approach to the life cycle;

f) a framework for dependability standards.

In addition, this third edition cancels and replaces the second edition of document IEC 60300-2 published in 2004.

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

FDIS	Report on voting
56/1550/FDIS	56/1556/RVD

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

The French version of this standard has not been voted upon.

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

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 publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

INTRODUCTION

This part of IEC 60300 describes the processes involved in managing dependability within an organization and establishes a framework for managing dependability activities for the purpose of achieving dependability performance.

Dependability is the ability of an item to perform as and when required. Dependability is a term used to describe the time-dependent characteristics associated with the performance of an item. Dependability includes characteristics such as availability, reliability, maintainability and supportability under given conditions of use and maintenance support requirements. Dependability describes the extent to which something can be trusted to behave as expected.

Dependability creates trust and confidence and affects the ability of an organization to meet its objectives. It is achieved by effective planning and implementation of dependability activities throughout the life cycle of items.

Dependability has a strong impact on the user's perception of the value of an item developed or provided by an organization. Poor dependability will affect an organization's capability to deliver its objectives and reduce its reputation.

Dependability management provides a systematic approach for addressing dependability and related issues from an organizational and business perspective. Dependability is often driven by technology and requires the integration of innovation with legacy products. Achieving dependability throughout the life cycle process can be influenced by market dynamics, global economics and resource distributions, changing customer needs, and a competitive environment. Strategies need to adapt to anticipated changes to sustain viability in business operations. Dependability management focuses on the needs of stakeholders in optimizing dependability to enhance organizational objectives and return-on-investments.

This standard is written specifically for application to technological products, systems, processes and services, which are referred to in this standard by the general term "item". However, much of the guidance provided is generic and can be adapted for application in various non-technological applications. In addition, the potential side effects on safety, environment and other factors should be identified, analysed and managed when optimizing dependability.

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

DEPENDABILITY MANAGEMENT –

Part 1: Guidance for management and application

1 Scope

This part of IEC 60300 establishes a framework for dependability management. It provides guidance on dependability management of products, systems, processes or services involving hardware, software and human aspects or any integrated combinations of these elements. It presents guidance on planning and implementation of dependability activities and technical processes throughout the life cycle taking into account other requirements such as those relating to safety and the environment.

This standard gives guidelines for management and their technical personnel to assist them to optimize dependability.

This standard is not intended for the purpose of certification.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

None.

3 Terms, definitions and abbreviations

For the purposes of this document, the following terms and definitions apply.

3.1 Terms and definitions

3.1.1
availability <of an item>
ability to be in a state to perform as required

Note 1 to entry: Availability depends upon the combined characteristics of the reliability, recoverability and maintainability of the item, and in some cases, on the maintenance support performance.

Note 2 to entry: Availability may be quantified using appropriate performance measures.

[SOURCE: IEC 60050-191:2014 [1][1], 191-41-23]

3.1.2
dependability <of an item>
ability to perform as and when required

Note 1 to entry: Dependability includes availability, reliability, recoverability, maintainability, and maintenance support performance, and, in some cases, other characteristics such as durability, safety and security.

---

1 Numbers in brackets refer to the bibliography.

Note 2 to entry: Dependability is used as a collective term for the time-related quality characteristics of an item.

[SOURCE: IEC 60050-191:2014, 191-41-22]

3.1.3
dependability case
evidence-based, reasoned, traceable argument created to support the contention that a defined system will satisfy the dependability requirements

3.1.4
dependability management
coordinated activities to direct and control an organization with regard to dependability

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

3.1.5
dependability management system
set of interrelated or interacting elements of an organization to establish dependability-related policies and objectives and the processes to achieve those dependability objectives

Note 1 to entry: Systems for managing dependability are part of the overall management system and not usually a separate management system.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning, procedures and processes.

3.1.6
dependability plan
set of scheduled activities to achieve dependability objectives and targets for an item

3.1.7
dependability programme
coordinated set of plans that describe the activities that lead to cost-effective achievement of dependability objectives and targets and the way they are resourced

3.1.8
item
subject being considered

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

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

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

[SOURCE: IEC 60050-191:2014, 191-41-01]

3.1.9
life cycle
series of identifiable stages through which an item goes, from its conception to disposal

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

Note1 to entry: The stages identified will vary with application.

[SOURCE: IEC 60050-191:2014, 191-41-09]

3.1.10
maintainability <of an item>
ability to be retained in, or restored to a state to perform as required, under given conditions of use and maintenance

Note 1 to entry: Given conditions would include aspects that affect maintainability, such as: location for maintenance, accessibility, maintenance procedures and maintenance resources.

Note 2 to entry: Maintainability may be quantified using appropriate measures.

[SOURCE: IEC 60050-191:2014, 191-41-27]

3.1.11
maintenance support
provision of resources to maintain an item

Note 1 to entry: Resources include human resources, support equipment, materials and spare parts, maintenance facilities, documentation and information, and maintenance information systems.

[SOURCE: IEC 60050-191:2014, 191-41-28]

3.1.12
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited, to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: For organizations with more than one operating unit, a single unit may be defined as an organization.

3.1.13
reliability <of an item>
ability to perform as required, without failure, for a given time interval, under given conditions

Note 1 to entry: The time interval duration may be expressed in units appropriate to the item concerned, e.g. 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 may be quantified using appropriate measures.

[SOURCE: IEC 60050-191:2014, 191-41-24]

3.1.14
requirement
need or expectation that is stated, generally implied or obligatory

[SOURCE: ISO 9000:2005, 3.1.2]

3.1.15
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

3.1.16
supportability <of an item>
ability to be supported to sustain the required availability with a defined operational profile and logistic and maintenance resources

Note 1 to entry: Supportability complements the inherent reliability and maintainability of the item, combined with factors external to the item that affect the relative ease of providing the required maintenance and logistic support.

[SOURCE: IEC 60050-191:2014, 191-41-31, note 1 has been modified]

3.1.17
system <in dependability>
set of interrelated items that collectively fulfil a requirement

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

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

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

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

[SOURCE: IEC 60050-191:2014, 191-41-03]

3.1.18
tailoring <process>
process to adapt, adjust or alter an organization's set of established processes and activities to fulfil, satisfy or meet requirements as they apply to dependability

3.2 Abbreviations

COTS	Commercial-off-the-shelf
FMEA	Failure modes and effects analysis
FRACAS	Failure recording, analysis and corrective action system
FTA	Fault tree analysis
HSE	Health, safety and environment
MTBF	Mean time between failure
HAZOP	Hazard and operability studies
RCM	Reliability centred maintenance

4 Dependability management

4.1 Understanding dependability

Dependability is the ability of an item to perform as and when required. Dependability is thus the ability to fulfil the requirements and expectations of an item consistently over time. Dependability creates value in that the item retains its performance characteristics, operates as desired, and satisfies customer needs and expectations.

Management of dependability is a key element of an organization's wider management systems in particular those for assets, finance and quality. Dependability management encompasses the planning and application of organizational arrangements, processes and associated methods and techniques to achieve the organization's performance and product objectives.

Dependability is improved by systematically reducing the frequency of outages, product failures, service downtimes, and other undesired events and minimizing their effects. This is achieved by actions such as improving design, eliminating root causes of failure, simplifying complex processes, mitigating anomalies, promoting fault tolerance in design and fitness for use, advocating fault avoidance and error prevention, managing maintenance activities and making commitments to build trust and integrity to ensure user confidence throughout the life cycle. Early consideration of dependability in the life cycle is crucial since rectifying a design

that causes poor dependability will often be more difficult, time consuming and costly at a later time.

Figure 1 illustrates the relationship of dependability to the needs of stakeholders and the requirements of an item. Depending on context, stakeholders can include users, owners, customers, government agencies, businesses and organizations responsible for ensuring dependability requirements are met.

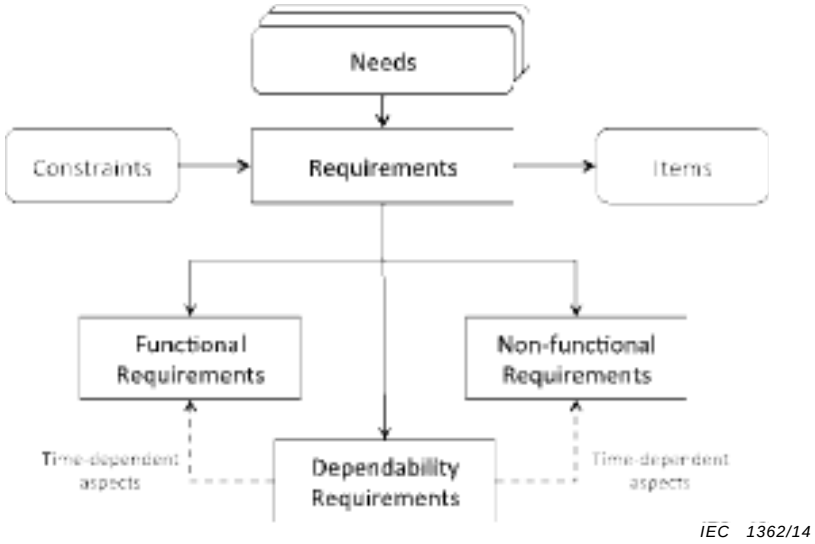


Figure 1 – Relationship of dependability to the needs and requirements of an item (product, system, process or service)

Requirements are determined from the needs of stakeholders and from constraints such as the conditions of use, resources and legislation. They include functional requirements, which define what the item is required to do, and non-functional requirements, which specify additional attributes. Examples of functional requirements are capacity and power output and examples of non-functional requirements are safety, environmental sustainability and efficiency. Dependability requirements, which define the time-dependent ability to achieve dependability performance in these requirements consist of characteristics such as reliability, availability, maintainability and supportability.

Functional and non-functional requirements and dependability requirements are inter-related. A dependability requirement can only exist if there is a functional or non-functional requirement that has to be satisfied. There can be competing objectives between desirable requirements, such as safety or oil/gas production and dependability, and therefore trade-offs may be necessary. There can also be constraints related to cost, availability of item components or resources, or fixed timelines that could cause a compromise between functionality and dependability.

The perception of the ability to perform as and when required can vary for different stakeholders. Users, providers, operators, maintainers and others who interact with an item can have overlapping dependability requirements but with different application objectives and usage expectations. This can result in differing perceptions of dependability which might need to be considered while defining requirements.

Dependability includes objectively measureable characteristics, such as reliability, availability and maintainability, and more subjective judgements of trustworthiness relating to the functions required by particular stakeholders. The ability to measure the attainment of performance objectives is a fundamental consideration in setting the requirements.

Dependability includes both the ability to meet functional and non-functional requirements under normal and expected conditions, and the ability to adapt to unexpected changes in requirements, assumptions and circumstances to recover from external system failures.

4.2 Benefits of dependability management

Managing dependability results in benefits such as

- meeting stakeholder requirements and objectives,
- achieving expected service levels,
- maintaining production or manufacturing capacity through increased availability,
- improving safety when potential detrimental consequences are identified and dealt with appropriately,
- reducing environmental impact when detrimental consequences are identified and dealt with appropriately,
- increasing life and durability and reducing life cycle costs, and
- improving quality.

4.3 Challenges of managing dependability

Dependability needs to be addressed during the entire life cycle of an item. Early consideration and implementation of relevant dependability activities will better ensure that dependability requirements are achieved.

There can be complications when multiple organizations are involved, mid-life upgrading occurs, or the item's dependability is influenced by interconnected and external systems.

Items are often integrated to operate with legacy items that are in different stages of the life cycle, with older generation technologies and methods of design. Dependability management needs to ensure interoperability and dependability of the integrated items through interface specifications to ensure dependable performance.

Systems are becoming more complex and can exhibit the characteristics of "open systems", "systems of systems" or "unbounded or weakly bounded systems". The systems can be managed by different parties that have different objectives and can be at different stages of the life cycle. This, together with the scale and complexity of the system makes it difficult for any stakeholder to comprehend the system as a whole and changes are thus less predictable and controllable. For that reason, it is crucial for stakeholders to understand and agree on the boundaries of their responsibilities and to assign accountability for implementation. Planning for dependability needs to take into account the potential for major failures and changes outside respective boundaries as well as inside.

5 System for managing dependability

5.1 Overview

The purpose of a system for managing dependability is to direct and control an organization with regard to dependability, coordinating with other disciplines to provide an efficient and integrated effort to achieve objectives. Organizational policies and objectives may include dependability policies and objectives, which then lead to a dependability management system that can effectively implement them.

Figure 2 shows dependability management as a part of a generic management system. The dependability management system results in a dependability programme which feeds into organizational plans and activities.

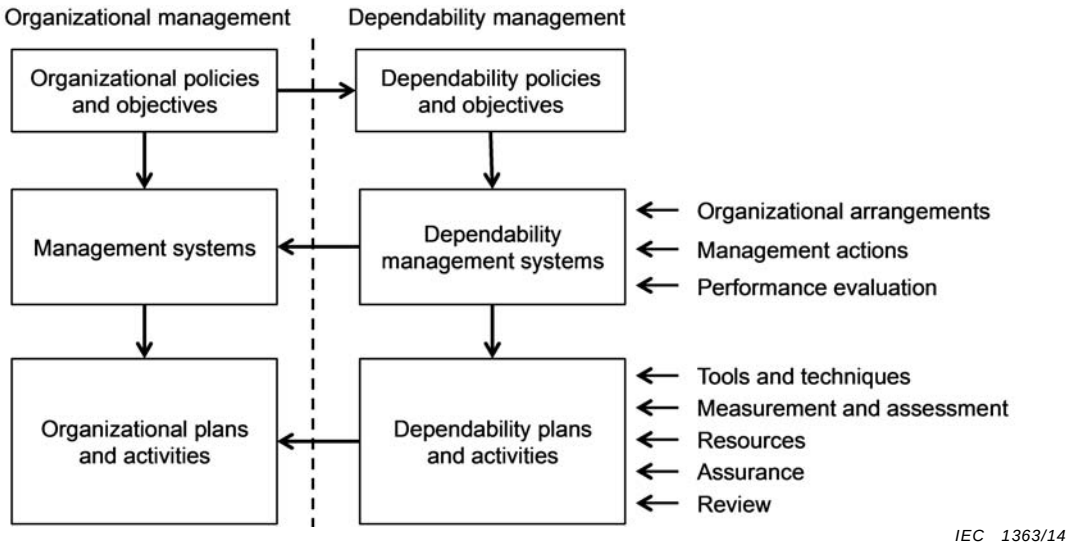


Figure 2 – Dependability management systems

A dependability management system consists of three elements:

- organizational arrangements to implement dependability policies and objectives;
- dependability activities that are implemented in the dependability programme;
- performance evaluation arrangements.

5.2 Organizational arrangements

Establishing organizational arrangements focuses on the management structure needed to facilitate effective implementation of the dependability policies. Dependability management should be integrated by the management systems of an organization in order to enable effective decision-making and influence technical direction. In particular, dependability engineering should be closely integrated into engineering projects for design and process improvements. Annex A describes the incorporation of dependability activities in the organizational operations, strategies and processes to achieve long-term goals and on-going project objectives.

Dependability policies and objectives need to be aligned with organizational policies and objectives and those of stakeholders comprising both technical and business perspectives. Organizational arrangements for managing dependability should take into consideration the organization's context, its objectives and the strategies to achieve them, and its risks and opportunities.

Dependability management systems do not always require a complex organizational infrastructure and reporting hierarchy to be effective. Dependability activities either can be managed by a separate organizational unit with close coordination, be fully integrated into other relevant areas, or be a mixture of the two approaches. The alignment of organizational structure, responsibilities, procedures, activities, resources and information is critical to efficient and effective direction and control of dependability. There should be dependability management involvement in planning, review, auditing, verification and validation of on-going project activities.

Where functions such as design, maintenance and logistic support are outsourced, the responsibility for dependability aspects of outsourcing should be specified, monitored and controlled.

One of the challenges with managing dependability over the life cycle is that often more than one organization is involved. Over the life cycle, certain responsibilities may need to be

passed from one organization to another. Since organizational styles and procedures vary, the management of dependability needs to adapt to different situations.

A means to manage and control dependability data and information should be established as a part of the organization's management information systems. This is to provide management insights on historical data and dependability-related performance records, enabling measurement of dependability status and improvements.

5.3 Management actions

Effective dependability management helps to ensure that dependability requirements are met in conjunction with functional and non-functional requirements.

Management actions should address the following:

- provide leadership through management commitment, policy direction and establishment of roles, responsibilities and authority;
- provide operational planning and control to achieve dependability objectives and manage risks;
- involve stakeholders by identifying dependability requirements and issues, communication of dependability programme status, conflict resolution and trade-offs, and securing and maintaining agreements and accountability;
- coordinate different organizational functions that are involved in dependability activities with assigned dependability responsibility for the coordination of management and technical effort;
- manage risks to dependability objectives and targets;
- provide and manage resources including acquisition of capital equipment, staff training and deployment, outsourcing and sub-contracting of dependability technical work;
- manage the technical activities needed during an item's life cycle to achieve dependability;
- manage knowledge and information through the capture and dissemination of relevant dependability data and knowledge, including maintenance of a dependability performance data base;
- undertake performance evaluations through monitoring, measuring analysis and evaluation, audit and assurance and management review;
- ensure sustained improvement via the planning and control of enhancement activities and appropriate reviews of progress.

Dependability related issues and technical concerns should be brought to management attention at review meetings for resolution, decisions and priority setting of task assignments.

5.4 Performance evaluation

Performance of organizational arrangements and processes is evaluated to assure relevant stakeholders that dependability management activities are being carried out well and will achieve the required dependability performance.

The organization should define performance indicators and targets for the dependability management system and monitor measure, analyse and improve performance against these indicators and targets.

This could involve

- evaluating the operation and effectiveness of dependability processes, activities and procedures,
- evaluating whether the organization's dependability policies and objectives are being met,

- reviewing the suitability of the dependability policies objectives and programme,
- assessing the dependability performance of items, and
- monitoring agreements and responsibilities.

6 Application of dependability management

6.1 Tailoring a dependability programme

The basic elements of a dependability programme are as follows:

- dependability plans, which define the activities, techniques and resources required to achieve dependability of items;
- methods for measurement and assessment;
- assurance and review (see Figure 2).

Management accountable for the resulting dependability of an item should tailor these elements to fulfil the dependability objectives for that specific situation or project. Tailoring applies to any stage of the life cycle but important tailoring occurs during the initial design-related parts of the life cycle. It might not be necessary to tailor activities in all cases, for example, for manufacturers who develop and produce similar products.

The general tailoring of the dependability programme involves the following:

- identification of the organizational context, including policy and infrastructure;
- consideration of regulatory requirements or standards;
- identification of item related characteristics such as its features and functions, past history of similar items, their intended end use and anticipated application environments;
- analysis of objectives and requirements;
- determination of the specific life cycle stages or phases that are applicable;
- assessing risks;
- selection of dependability activities relevant to the specific life cycle stages or phases identified;
- selection of tools and technical activities needed to achieve dependability;
- selection of techniques for measurement and assessment;
- definition of the capability and resources needed and actually available for implementation;
- prioritization and allocation of resources;
- planning reviews and assurance;
- documentation of the rationale in formalizing the tailoring decisions as part of the organizational or project plan.

If the magnitude of the programme dictates the need for each functional area to have its own plan, these dependability activities can be documented in their own separate plans.

Tailoring criteria and guidelines describe

- how the organization’s dependability activities are used within project processes,
- which mandatory and legal requirements need to be satisfied,
- which options may be exercised as well as the criteria for selecting from these options, and
- how to make decisions about which dependability procedures should be performed.

Tailoring needs to take into account the nature of the organization and the dependability tasks that need to be managed. The organization could vary from a technical consultancy to a multinational conglomerate requiring appropriate dependability management of diverse disciplines, organization and specialization. Management approaches often seek technology transfer, knowledge infusion, or expert consultancy to deal with critical short-term technical gaps.

The tailoring of dependability activities includes consideration of the organization's technical and administrative processes with their constraints and influencing factors, which include, but are not limited to the following:

- customer requirements;
- regulatory requirements;
- safety requirements;
- delivery targets;
- allowable budgets;
- available resources;
- technical capability;
- environmental impact;
- novelty of technology involvement;
- provision of sustainable services.

The outcome of tailoring activities form the basis of a dependability plan of activities and resources for that particular project. The depth and detail of the plan should enable measurement for management tracking and costing purposes. Tailored plans should, along with other plans such as those relating to safety, scheduling, integration, production, operations and maintenance, build the backbone of the overall project plan. Integration into this overall project plan can require further tailoring to accommodate project time and cost limitations. This can incur a trade-off of predicted product dependability against project timing and cost.

The provision of flexibility through tailoring should be balanced with the need to ensure appropriate consistency in the dependability activities across the organization. Flexibility is needed to address contextual variables such as the nature of the customer, cost, schedule, quality trade-offs, and technical difficulty of the work as well as the depth of experience of the people implementing the process. Tailoring criteria can allow for use of a standard process with no tailoring or an approach where only exceptions are noted from a standard process.

6.2 Analysis of objectives and requirements

Requirements are defined to satisfy the needs and objectives of stakeholders. Requirements can be divided into two interrelated groups, functional and non-functional requirements, both of which could include dependability requirements (see Figure 1). Annex C describes how dependability requirements can be defined.

Since perceptions of dependability can vary depending on the stakeholder, it is important to ensure there is good communication and consultation between all relevant stakeholders when defining requirements and how they will be assessed.

When there is a contract between a customer and a provider, they need to agree on the way dependability is to be measured and how it will be decided that dependability targets have been achieved.

6.3 Risk management

Risks should be identified considering both potential failures to achieve requirements and opportunities for enhanced performance. Risks to dependability and to functional and non-functional objectives such as those concerning safety or the environment need to be considered and trade-offs could be required.

Failure to meet requirements and objectives can arise as a result of

- failures of or within an item, which can be identified by reference to past data and methods including root cause analysis of failures or by procedures such as FTA or FMEA,
- failure in support for the item such as in maintenance or maintenance support, and
- changes in requirements, assumptions and circumstances from outside the dependability system and sometimes outside the organization.

Where practicable and cost beneficial, adverse consequences should be prevented or reduced. Arrangements should be made to monitor external circumstances critical to dependability to obtain early warning of changes. The need for an item to be able to recover from and adapt to risks should be taken into account in defining requirements and the activities and plans to achieve them.

6.4 Implementation of dependability activities through the life cycle

Dependability activities occur throughout the life cycle of an item and are normally incorporated as part of engineering processes at every life cycle stage, even when the different stages of the life cycle overlap. The transitions between life cycle stages often entail different technical resources, diverse enabling systems and support criteria.

The activities required for each stage of the life cycle can be different. Dependability activities should be organized and managed as part of engineering or other programmes or projects for maximum effectiveness.

Annex B maps dependability activities to a generic life cycle; it should be recognized that life cycle stages can be simpler or more complex, depending on specific circumstances.

6.5 Selection of dependability tools and technical activities

There is a broad range of technical activities and tools to facilitate achievement of dependability management objectives such as reliability analysis and testing, maintenance and logistic support management, customer care services, failure analysis and corrective action systems. Dependability tools vary with the stage of the life cycle.

For example, at the design and development stage, techniques such as HAZOP, FMEA or FTA can be applied. Those techniques aim to identify and prevent faults, failures or undesired events before they have been observed in real operation.

During implementation and utilization, reliability improvement by a growth programme should be part of an overall reliability activity in the development of an item, particularly for a design that uses novel or unproven techniques, components or a substantial content of software. In such a case, the programme can expose, over a period of time, many types of weaknesses having design-related causes. Reliability growth is achieved by learning about the deficiencies of the design through testing and taking action to eliminate or minimize the effect of these deficiencies. Various statistical models can be used to develop a planned growth curve that sets realistic interim reliability goals to be attained during the testing and indicates that sufficient progress is being made in order to reach the final goal or requirement.

Root cause analysis is another dependability tool that consists of any systematic process to identify the causes of a fault, failure or undesired event that have been observed in operation or during testing with the aim of preventing similar or related failures from occurring. It is

performed with the understanding that failures are best resolved by eliminating the primary or root causes rather than addressing the immediately obvious symptom. It is typically applied in response to a repeated failure or a failure with significant consequences.

Annex D presents the structure for dependability standards to support dependability management and guide the application of methods and tools. Information on specific and current dependability standards is provided on the IEC/TC56 Website [2] to facilitate dependability applications.

6.6 Resources

The resources to achieve dependability of an item include

- someone to take responsibility for the dependability of an item either as a prime responsibility or possibly as part of another role,
- expertise to carry out the appropriate technical activities and analyses,
- an information management system such as a dependability knowledge database (either stand-alone or part of a logistic support system), and
- appropriate dependability analysis software.

The resources necessary can vary with the stage of the life cycle. For example, the design and development stage requires dependability design expertise and the use of dependability analysis techniques, which often require software programs and dependability data. The realization stage can involve resources for detailed testing. During utilization of the item, resources might be needed for data gathering and assessment and performance of maintenance and support activities.

6.7 Measurement and assessment

The measurement process involves:

- identifying the type and objectives of the measurements of dependability attributes that are needed under contractual and operational requirements or for specific conditions such as product evaluation;
- determining the relevant data and the nature of the data sources for measurements;
- utilizing effective enabling systems to facilitate the measurement process such as deployment of data collection systems, failure reporting, analysis and corrective action systems, survey questionnaires, or other support schemes;
- interpreting the measurement results to establish performance trends, identify critical issues and recommend management actions with rationales and justifications;
- documenting the measurement findings for record retention, quality audits and objective evidence.

Dependability is assessed in different ways according to the stage in the life cycle:

- forecasted at the design stage by using probabilistic assessment and modelling methods;
- estimated at the realization stage by, for example, accelerated reliability and durability testing;
- measured and analysed at the utilization stage using statistical and other methods.

The dependability characteristic that is measured depends on whether a user or organizational perspective is taken and on the applicable performance requirements. For example, for a transportation service, the user (passenger) will be concerned with accessibility of the service (availability of space and conformance to the posted schedule), dependability of service (on-time arrival) and integrity (properly maintained seating and facilities). From an organizational perspective, dependability can also be assessed by means

of an effectiveness measure such as customer satisfaction, reliability of the service and maintenance cost.

The characteristics that constitute dependability can be measured either qualitatively or quantitatively. Qualitative assessment could be done descriptively or by using ranking methods.

Examples of qualitative methods are as follows:

- An assessment by an expert providing explanations on the item and providing a score (such as 5 ‘stars’). In certain cases, the attributes are weighted to incorporate levels of importance before an overall score is established. By comparing various scores from different experts, an objective assessment can be achieved. Making judgments based on the scores of a single expert should be treated with caution.
- An assessment derived from the general public providing an individual score and associated justifications for a particular item. These scores are accumulated within a database to establish an overall ranking for the item compared with other similar items.
- In these cases, the method of ranking needs to be understood as well as the potential biases of the individuals providing the score before the accuracy of the ranking can be acknowledged.

A quantitative value of dependability performance is derived from observed or estimated data. Dependability characteristics can be quantified in different ways such as instantaneous and operational measures of availability or reliability derived from direct and indirect measures of items during testing, operation or maintenance. For example, they can be measured by times of failures, operating time to first failure, duration of intervals of up time and down time and effort expended on maintenance activities.

Since high reliability or availability is difficult and time-consuming to verify by testing, even when using accelerated testing, the reliability of the item might need to be verified by analysis methods. If it is not possible to test the entire item, tests could be made on the component and module level. However, the final measure of the performance of the item is not normally feasible until it is in operation.

Dependability parameters of an item should be predicted, forecast or measured under defined stressing conditions such as the exposure to various environmental conditions that will occur during utilization. Some typical natural environment stressing conditions are storage and operating temperatures, humidity and solar loading. Cultural, organizational or political rules and human involvement can also have dependability impacts.

6.8 Assurance of dependability

Assurance is the process to ensure the item conforms to established requirements and standards. Assurance establishes the grounds for justified confidence that dependability-related performance achievement claims will be, are or have been achieved. The objective of assurance is to gain the trust of stakeholders that item dependability can be achieved. There are generic approaches to assuring item dependability, which serve different purposes and have varying degrees of engineering rigour. In practice, a combination of these three approaches is likely to be used.

a) Dependability assurance is demonstrated by actual utilization in an application environment over a scheduled time period. This could involve a formal demonstration or actual performance during the warranty or operating period.

b) Dependability is inferred by applying statistical methods to data of the dependability of constituent items.

c) Evidence of correct implementation of required dependability activities and tools is provided.

A means of achieving progressive assurance that dependability requirements are being met, or will be satisfied throughout the life cycle of the item, is by use of a dependability case. The framework for establishing a dependability case for assurance includes

- a reasoned auditable argument to support the contention that a defined item satisfies the dependability requirements,
- a summary of evidence and arguments to support the claims for dependability achievement, and
- progressive assurance throughout the life cycle of the item as part of the evaluation.

The dependability case provides a focal point for determining uncertainties and managing related risks. Thereby, assurance has become a key factor for the life cycle activities that plan, design, achieve, demonstrate, sustain and monitor the dependability-related performance during operation.

Where possible, existing performance monitoring systems should be used to generate the information needed for improving dependability activities and outcomes.

Typical examples include

- a failure recording, analysis and corrective action system (FRACAS),
- a customer care and feedback system,
- a maintenance and logistic support system,
- an incident reporting and fault management system,
- a health monitoring system, and
- a quality management system.

6.9 Reviewing dependability outcomes and activities

Dependability outcomes and activities should be reviewed throughout the life cycle. The purpose of dependability reviews is to ensure that specific objectives from both technical and business perspectives are being met throughout the life cycle. The reviews provide feedback on dependability deficiencies and deviations at one life cycle stage for correction and mitigation at other stages, as well as improving the way dependability is managed. The reviews should consider both activities and outcomes and should set a course of action from a technical perspective to achieve objectives and manage risks, for example, at critical design points to prevent the propagation of errors and inadequate design decisions.

Dependability reviews are conducted in conjunction with other management reviews with broader scope to address dependability management issues such as those associated with the organization’s policies, administration, operation or customer services. For example, project management reviews should be enhanced to include dependability aspects.

Dependability managers should participate in various capacities at review meetings and contribute accordingly to issues of dependability interest and impact requiring management attention and follow-up actions. A typical dependability review checklist is shown in Annex E. The checklist is provided to assist a dependability review at major decision points during the life cycle. The checklist can be used by the supplier and the customer for tailoring purposes to meet their specific application needs.

The checklist is aligned with the life cycle as identified in Annex B.

Reviews cover a broad range of review activities over the life cycle of an item. Typical reviews conducted at various levels of management which should incorporate dependability components could include:

- operations review to determine the health and operational status of an organization, a subsidiary division, a manufacturing plant, or a service facility;
- project review to determine work progress status, project schedules and milestones commitments, resource availability, outsourcing needs, supplier coordination, and identify problems requiring management actions;
- technical review to evaluate application of new technology, product line diversification, make-buy decisions, and timeline for new product introduction;
- design review to evaluate technical development achievements, dependability assessments, design weaknesses for improvement, product qualification, manufacturability, functional design, operability in the environment of application and service support needs, and final design approval prior to design release to production;
- component application review to check operating conditions of components and COTS items against data sheets and test results and for special requirements of use, handling and assembly processes;
- production review to determine resource requirements and delivery schedules, production capacity and throughput, outsourcing and subcontracting of production work, tooling, assembly fabrication, material control and testing activities;
- risk review to determine whether risks have changed and whether the risk management process is effective;
- service review to determine customers' service needs, scheduled and unscheduled maintenance activities, third-party service provisions, logistic support, inventory holdings and depot locations;
- customer satisfaction review to address user concerns and improvement strategies;
- supplier review to ascertain supplies quality, delivery schedule commitments, ordering process efficiency, multiple sourcing and supply-chain management;
- quality review to determine non-conformance status, assurance effectiveness and quality performance trends, identify areas for improvements and recommend management actions;
- verification and validation review to ensure proper verification and validation processes have been carried out;
- product release review releasing the product for delivery and/or customer acceptance;
- regulation review to determine if applicable health, safety and environmental rules have been identified and are properly implemented.

Dependability components in those reviews have to work together as a whole. Each of those reviews typically involves several life cycle stages and activities and feedback from one review can trigger activities affecting other reviews.

All reviews are part of the assurance process. The reviews of dependability ensure that all critical issues have been assessed and resolved. The review records could be used as objective evidence to support the dependability assurance process in a wider review of assurance processes.

Annex A
(informative)

Organizational arrangements of a dependability management system

A.1 Organizational structures

In order to achieve their objectives effectively, organizations are usually structured into entities or business units with several levels of hierarchies. Each of these entities has responsibility for managing certain activities with assigned resources to accomplish their tasks. Unless objectives are very simple and easy to achieve, activities are normally divided into multiple groups for efficiency based on factors such as common skill sets or physical location requirements. Groups have leaders to manage activities, often with several layers of management. In many organizations, dependability is a very important requirement that needs to be met and the organizational structure should accommodate these specific requirements.

Some organizations exist for a certain time period in order to achieve a specific objective as is common with situations such as product development, and design and construction of facilities. In other cases, an organization can exist for a longer time period. In both situations, dependability requirements will need to be accommodated in the organizational structure.

In organizations where business or technology is fast-moving, new organizational structures are appearing. Typical examples include new partnerships to promote communications networks, cross-regional and national jurisdictions in transportation and distribution, and specialized one-stop manufacturing services where different organizations collaborate by agreements to work together worldwide. Facilities can be established, transported and duplicated in almost any country where human resources, security and a level playing field can be established and sustained. Some vertically integrated organizations have also engaged in matrix management and participative organizational structures to retain expertise for strategic deployment. Organizations can then expand beyond standard corporate management and can include collaborations of government, industry and academic institutions or complex systems where no one stakeholder fully understands the system.

A.2 Organization of dependability activities

There are different possible approaches to structuring an organization to enable dependability objectives to be met successfully. Since overall requirements are a combination of functional, non-functional and dependability requirements, they require close coordination of activities and should be seen as an integrated set of activities within an organization. In general, dependability activities should be included within an organizational structure under one of the following general scenarios.

- Dependability activities are fully integrated into the organizational structure with dependability resources embedded into an organizational entity, for example, where every employee is responsible for the dependability aspects of his or her activities. Often one or more persons are assigned as facilitators for such activities.
- Dependability activities are sufficiently time-consuming and important that one or more organizational entities will be needed to complete dependability activities as would be appropriate for the design, construction and commissioning of a major facility. These entities will still function in close coordination with other entities.
- For a large organization with multiple product lines or many large facilities to operate, it can be worthwhile to set up a major organizational entity to serve the overall needs of the organization in an efficient manner. This can eliminate duplication of effort and ensure consistency of dependability activities while at the same time enabling the highest level of expertise to be applied. In some cases, a separate dependability organization is required

by regulatory authorities, e.g. type approval within the fields of telecommunication, medical equipment and aerospace.

- With any of these scenarios, specific activities can be outsourced, either because they are very specialized or their duration is short.

Key factors that contribute to successful achievement of dependability requirements from an organizational perspective include

- defining a single overall responsibility for meeting dependability requirements and coordinating shared responsibilities among the various organizational entities that are involved,
- supplying and enabling expertise and competence of dependability resources to carry out activities,
- managing information associated with dependability and related functional requirements,
- coordination between internal and external groups involved with dependability activities, and
- incorporating dependability requirements in decision-making and fully understanding trade-offs that can be made between functional and dependability requirements and project-related factors such as schedule and cost.

Annex B
(informative)

Activities of a dependability management system

B.1 Dependability activities within the life cycle

A variety of dependability activities are needed as items are created or acquired, used or operated, enhanced and finally retired or disposed. This series of identifiable stages is known as the life cycle and forms the basis for dependability activities.

For the purpose of this annex, a generic life cycle has been used that should be generally applicable to all items. Note that these stages often overlap in their timing.

a) Concept

The concept stage is the initial visioning stage for an item. It can entail activities to identify market or other needs, define/identify the general operational use environment and timeline, human aspects the regulatory requirements (such as traceability, safety, environment, sustainability, retirement and waste disposal) and other constraints. From this, functional and non-functional requirements and the preliminary dependability requirements can be defined and analysed and feasible design or purchasing solutions identified from broad technical specifications. Potential needs for trade-off such as between safety and dependability should be identified at this stage. Modelling and probabilistic approaches can be used to achieve high-level dependability predictions in order to select the preliminary architecture and the maintenance and supportability policies, which are likely to meet the regulatory and dependability requirements. Risk assessment during the concept stage should focus on the feasibility of concept design and technology selection for project implementation. Selection of design options is based on the best practical engineering approaches to achieve requirements and manage risks within the constraints imposed.

b) Development

The development stage follows the initial concept once its feasibility has been verified. The focus is to plan and execute selected engineering design solutions for the realization of item functions. This is transcribed into an appropriate design and development effort including designing system architecture, engineering modelling and prototype construction and testing. Interfaces between system and subsystem elements are identified and a systematic evaluation of the integrated item functions and its interactions with external environments is conducted to validate the final configuration. Risks associated with the selected design are assessed in more detail and treatments specified. Planning for supportability maintenance access, operational procedures and assurance as well as support processes should be well established prior to item realization. Relevant modeling and probabilistic approaches can be used at this stage to achieve detailed dependability predictions in order to consolidate the architecture and the maintenance and supportability policies selected at the conceptual stage, and to verify that the regulatory and dependability requirements are likely to be met.

c) Realization

The realization stage implements make-buy decisions for the acquisition, and/or manufacturing of the final item and its components. The realization efforts deal with activities such as technology development, tooling, manufacturing, packaging and supply sourcing to ensure the complete transformation from the design to the specified item or its subsystem components. The realized items or components can comprise a combination of hardware and software functions. Realization includes component and module simulations, analyses and tests including integration tests as well as activities such as assembly of components, integration of item functions, verification of subsystems, and installation of the item. Acceptance procedures should be established with the customer

with possible trials in the actual operating environment prior to commissioning. Validation should be a part of the trial to provide objective evidence of conformance to specifications.

d) Utilization

The utilization stage is when the item is deployed for delivery of functionality or service with support for its operational capability by means of maintenance. The process activities include operating and maintaining the item in accordance with performance requirements, training for operators and maintainers to maintain skills competency, customer interface to establish a service relationship, and record keeping on item performance status and reporting failure incidents to initiate timely corrective and preventive actions. The item performance should be monitored and checked on a regular basis to ensure that dependability, regulatory and quality of service objectives are met. Data collection and sampling can be used to estimate service dependability. Risk assessment during operation and maintenance can deal with issues that arise due to changing conditions.

e) Enhancement

The enhancement stage might be needed to improve item performance with added features to meet growing user demands, extend operating life or address obsolescence. The process activities can include hardware or software upgrades or additions, maintenance improvements, simplifying procedures to improve operational efficiency or obsolescence management. At this stage relevant modeling and probabilistic approaches can be used to assess the impact of the possible enhancements and select the best solutions. Risk assessment during the enhancement stage often looks at cost versus benefits and return-on-investment.

f) Retirement

The retirement stage occurs at the end of the life of the item. Upon termination of the use of an item, it can be disassembled, redeployed for other uses, disposed for reuse of materials and components or, in some cases, abandoned in situ (such as a pipeline). This should be considered from the conceptual stage. For complex items, a strategy for decommissioning could be established to formalize planning and implementation of the decommissioning process to meet regulatory requirements. For other items, there could be regulatory rules concerning their return and reuse or disposal.

Dependability activities are often considered in the context of the life cycle as shown in Figure B.1.

Variations of these generic life cycle stages can result in more specific life cycle stages such as:

- product: concept and definition, design and development, manufacturing and installation, operation and maintenance, mid-life upgrading or life extension, and decommissioning and disposal;
- facility: concept and definition, design and development, construction and commissioning, operation and maintenance, mid-life upgrading, or life extension, and decommissioning and disposal;
- hardware: concept, design, fabrication and manufacturing, installation/commissioning, operation/maintenance, modification, disposal;
- software: concept, development, application, operation and maintenance, enhancement, retirement.

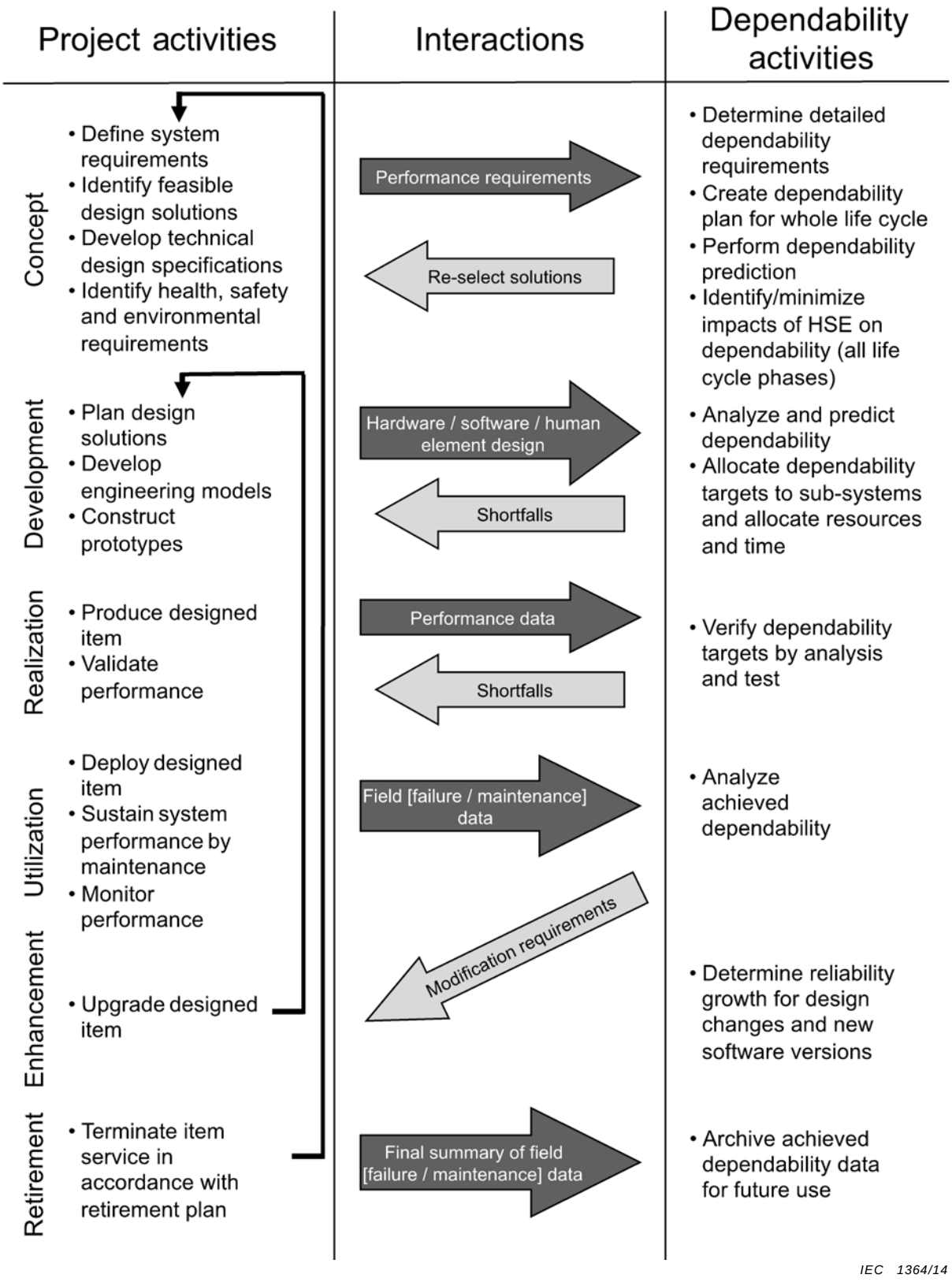


Figure B.1 – Dependability activities and the life cycle

B.2 Dependability life cycle activities

The following tables provide typical examples of activities with an impact on dependability objectives that could be part of a life cycle. This list is not exhaustive and should be modified or tailored to meet specific requirements.

Table B.1 – Activities during the concept stage

Dependability objectives	Dependability strategies	Activities with impact on dependability
1. Define item requirements	a. Identify market needs or other opportunities	• Conduct market or other surveys and research studies to assess customer/user needs • Identify regulatory requirements related to new initiatives • Determine competitive leverage on dependability values • Identify scope of market or other needs and assess risk of new initiatives • Establish the context
	b. Establish dependability policies and incentives for implementation	• Determine timing for new venture initiation and define innovation objectives • Formulate strategic plans for new item development and acquisition tactics • Rationalize resource commitments to support new initiatives and on-going programme portfolios • Plan achievement targets • Establish project tailoring criteria • Document policies and mission statement • Determine development tools and procedures
2. Analyse item performance requirements	a. Identify technical approaches and feasibility for item realization	• Conduct requirements analysis • Determine item boundaries, operating functions and performance characteristics from the set of defined performance requirements • Achieve probabilistic evaluations in order to establish feasible solutions and define the preliminary architectures • Identify the organization's capability to undertake the work • Identify risks • Evaluate trade-offs which can be required between desired functionality and dependability requirements • Determine resource requirements and evaluate allocation plan for specific project tailoring • Determine technical and quality measures for design guidance and to enable dependability assessments
	b. Identify potential partnership and supplier requirements	• Determine feasibility of supply-chain and joint venture collaboration • Determine outsourcing requirements

Dependability objectives	Dependability strategies	Activities with impact on dependability
3. Establish high level design criteria	a. Identify appropriate logical architectural design options	• Establish item configuration • Partition item functions • Select technologies for design and choice of hardware/software for realization of functions • Formulate make/buy decisions of item functions • Formulate solution to meet item requirements • Establish means for verification and integration of item functions
	b. Establish design requirements for evaluation	• Formalize the design process and how trade-offs will be handled • Identify design composition of hardware/software elements for each function • Incorporate test functions for performance verification • Establish human factors design criteria • Establish dependability design criteria • Perform dependability prediction • Establish environmental design criteria • Establish ergonomics design and interface criteria • Establish electro-magnetic compatibility design criteria • Establish safety, security and reliability design criteria • Establish hardware design guidelines • Establish software design guidelines • Simulate item performance at functional level to determine fault coverage and item recovery strategy • Verify performance limits, robustness and interoperability of item functions to meet architectural design requirements • Analyse and minimize the impact of health, safety and environmental requirements and potential detrimental effects on dependability
	c. Document item specifications	• Incorporate dependability requirements in item specifications

Table B.2 – Activities during development stage

Dependability objectives	Dependability strategies	Activities with impact on dependability
1. Design and develop the item	a. Initiate item design	• Establish item dependability programme • Establish quality assurance programme • Establish configuration management plan and design change procedures • Achieve probabilistic evaluations in order to assess the forecasted dependability values • Determine risk assessment requirements • Establish test plan and item acceptance criteria • Establish item monitoring, diagnostic schemes, incidents reporting and data management system • Establish suppliers' dependability programmes • Analyse and minimize the impact of health, safety and environmental requirements and potential detrimental effects on dependability
	b. Initiate full scale item development	• Formalize dependability requirements for system, subsystems and functions • Implement project tailoring plan • Achieve probabilistic evaluations in order to verify that the dependability targets are likely to be reached • Develop software test and diagnostic programme • Establish dependability acceptance criteria and reliability growth programmes • Establish item maintenance and logistics support programme • Conduct risk assessments • Monitor and collaborate with material outsourcing and contracting external development efforts • Develop spares provisioning programme • Define warranty conditions • Establish training programmes

Table B.3 – Activities during the realization stage

Dependability objectives	Dependability strategies	Activities with impact on dependability
1. Item or module realization	a. Initiate production or acquisition of hardware assemblies and functions	• Implement item dependability programme • Implement quality assurance programme • Implement failure reporting, analysis, data collection and feedback system • Establish configuration management plan and design change procedures • Establish test plan and item acceptance criteria • Establish item monitoring, diagnostic schemes, incidents reporting and data management system • Implement suppliers' dependability programmes
	b. Initiate software module functions and item development	• Implement software reliability assurance programme • Implement software test and diagnostic programme • Implement software module qualification and evaluation plan for acceptance
2. Item implementation	a. Item integration	• Execute integration plan • Coordinate outsourcing and support programmes • Implement configuration management plan and design change procedures • Prepare and perform analysis and tests of components and modules • Prepare plans for and perform item acceptance analysis and testing • Perform required changes for reliability growth • Prepare item acceptance plan • Prepare verification and validation plans and procedures
	b. Item verification/ validation	• Implement verification/validation plan • Document verification/validation test results • Conduct failure analysis and recommend preventive/corrective actions for improvement
	c. Item installation and acceptance	• Execute installation plan • Document installation records and procedures • Conduct item acceptance and generate acceptance report • Implement warranty schemes if applicable • Establish shared supportability and reporting schemes with customer maintainers on item installed on customer premises • Customer sign-off for item acceptance to initiate official item operation and full-scale deployment • Resolve warranty issues with customers • Analyse and minimize the impact of health, safety and environmental requirements and potential detrimental effects on dependability • For consumer products, release to mass production, distribution and sale

Table B.4 – Activities during the utilization stage

Dependability objectives	Dependability strategies	Activities with impact on dependability
1. Item operation and maintenance	a. Implement operation strategy	• Monitor item performance • Implement reliability growth programme • Implement field data collection system for information about in-service dependability • Conduct customer satisfaction survey • Analyse and minimize the impact of health, safety and environmental requirements and potential detrimental effects on dependability
	b. Implement supportability strategy	• Provide customer care service • Monitor item maintenance efforts • Analyse failure trends and maintenance service records • Recommend design or procedural changes for continual improvement • Determine quality of service and provide customer value

Table B.5 – Activities during the enhancement stage

Dependability objectives	Dependability strategies	Activities with impact on dependability
1. Item enhancement	a. Implement item enhancement strategy	• Identify new feature and enhancement requirements • Evaluate the need for change and resulting benefits • Conduct risk and value assessments • Analyse the impact on health, safety and environmental requirements • Implement enhancement efforts • Evaluate impact on dependability-related performance like stability and robustness due to changes with added new features • Conduct customer satisfaction survey resulting from change reactions

Table B.6 – Activities during the retirement stage

Dependability objectives	Dependability strategies	Activities with impact on dependability
1. Item retirement	a. Implement item retirement strategy	• Execute item retirement/decommissioning plan • Implement reuse of components, data and materials from disposed items • Ensure that health, safety and environmental requirements are met • Implement waste treatment on disposal items • Notify customers on service termination • Provide information on new or alternative service provision • Conduct customer satisfaction survey due to termination of service

Annex C
(informative)

Defining requirements of an item

C.1 Requirements from an application perspective

The dependability requirements together with the functional and non-functional requirements define the performance requirements of the item.

The dependability requirements are an integral part of the overall requirements and relate to how the functional and non-functional requirements can be achieved from a time-related performance perspective, where time is a general term for a variety of measures such as calendar time, operating time, number of demands and number of operating cycles.

There is a wide variance in how performance requirements are established and implemented for different applications.

The requirements can be determined by identifying the needs of stakeholders taking into account aspects such as

- knowledge of similar items and performance data,
- relevant technology and application limitations,
- information on operating environment and usage scenario,
- established standards and relevant specifications, and
- users' experiences and complaints.

The dependability requirements take into account aspects such as

- expected length of uninterrupted operation,
- maximum allowable failure rate during operation,
- time to first failure or time to wearout,
- minimum expected availability/effectiveness of the item,
- required maintainability,
- the capability and availability of maintenance and support needs,
- expected total life of the item,
- safety requirements, and
- cost constraints.

The requirements can be derived from this set of inputs and translated into technical specifications that will include qualitative or quantitative requirements of expected performance.

Performance and dependability requirements are very closely linked and should not be seen as separate characteristics of performance. Trade-offs can occur between them to achieve a combined solution. For example, a specified level of power output could require shorter maintenance intervals that might be unacceptable from an operational point of view. Cost constraints will impact both performance and dependability requirements.

The following two examples serve to illustrate how performance and dependability requirements can be defined for two scenarios and the methods that can be used as part of

the dependability programme for this item: in the first case, requirements are defined by both provider and user and, in the second case requirements are defined mainly by the provider based on their understanding of user expectations but without specific user input.

C.2 Examples of performance requirements that include dependability

C.2.1 Requirements determined by both provider and user

In many industrial and other applications, performance requirements are determined by both provider and user. The example given here is that of a motor-driven oil pump in pipeline service, transporting crude oil, which has been processed to remove entrained gas and lighter liquids but which still contains some contaminants. The overall function of the pump is to provide dependable pumping capacity, safely and with minimum environmental impact. The constraints in terms of conditions of use and operational environment are tropical climate with ambient temperatures normally below 40 °C, but with high humidity. Required maintenance will be determined by a risk-based approach such as RCM that will include both normal preventive maintenance tasks and condition monitoring.

The primary functional requirement for the pump is to provide a flow capacity that is defined by a specified head (pressure increase) at a certain flow with an associated efficiency. The expected operating range is between 80 % and 120 % of the rated design flow. These fundamental performance requirements are derived from the process requirements of the pumping facility and its location in the pipeline system. Non-functional requirements consist of extensive safety and environmental features to minimize potential impact to employees and the public.

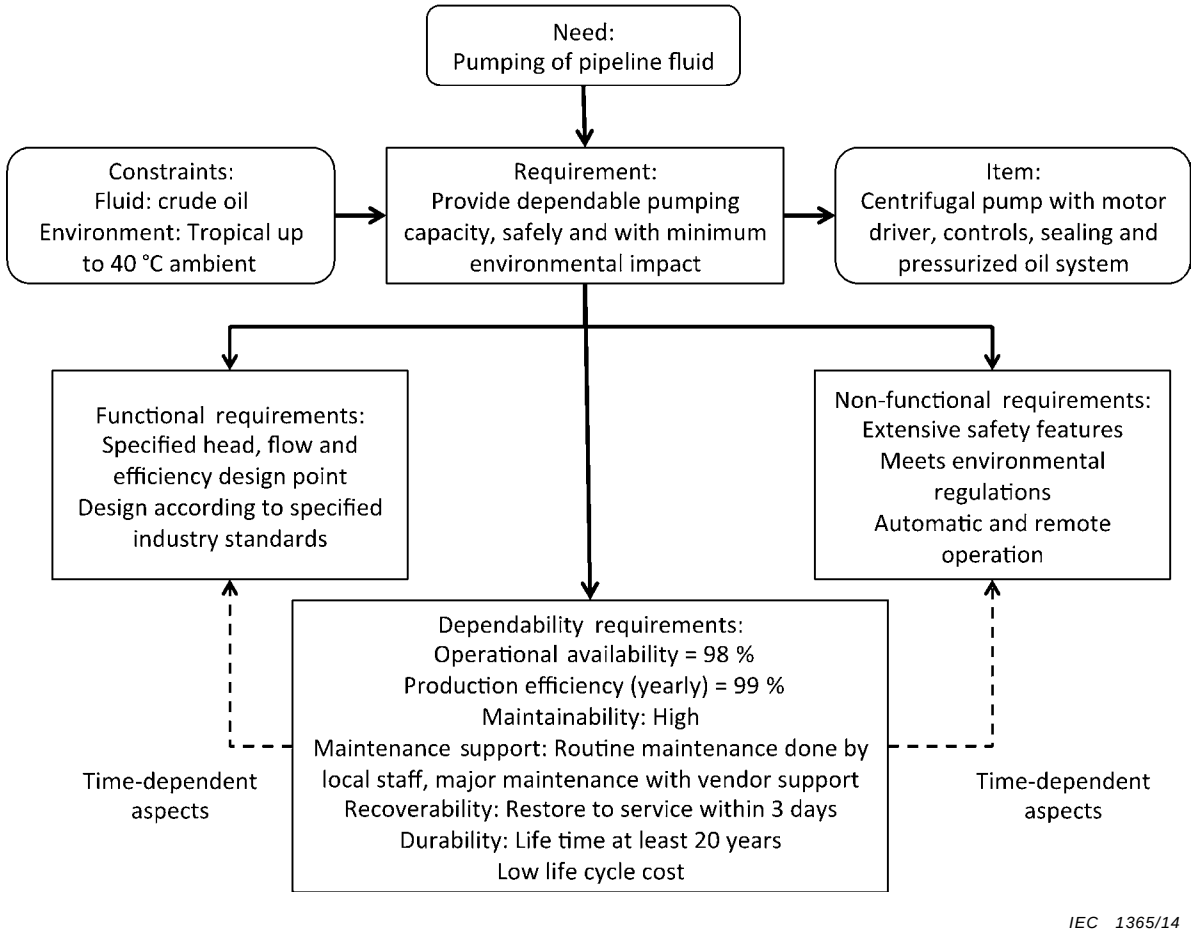
The pump unit has a software-based control system supported by instrumentation and remote control from a centralized facility. To minimize environmental impact, the mechanical seals use a nitrogen buffer fluid. Safety protection is built into the control system with fire monitoring and protection devices. A number of available design standards are followed including ones for petroleum pumps, sealing systems and machinery protection systems. Safety concerns are addressed by local and national safety standards.

In this case, all of the main dependability characteristics are applicable. A target of 99 % for production efficiency (i.e. the expected production of the system is an average over 1 year of the rated design flow) between yearly maintenance activities is established. In order to predict that this level of reliability is achievable, a reliability block diagram, consisting of the major blocks of the pump-motor system, is produced. Data on the reliability of individual equipment or blocks using MTBF is obtained from both industry reliability databases and estimates from the vendor. It is compared to practical results from actual maintenance history for similar equipment already in operation for verification and validation.

High availability is required due to the nature of the pipeline system and downtime is to be minimized with an operational availability of 98 % considered to be achievable over a time period associated with a major maintenance cycle. The final availability over a 5-year period is estimated from the reliability data and the maintenance records including a major overhaul.

Additional dependability characteristics are maintainability and durability. To recover quickly from a failure requires high maintainability and careful supportability planning. Down time due to a major failure usually takes 3 days, requiring the pump to be dismantled. For durability, a minimum life of 20 years is necessary with a low life cycle cost compared to similar equipment. A life cycle cost analysis is carried out based on the initial purchase and installation cost and also the anticipated operating and maintenance costs, which will depend on the selection of an acceptable support solution.

The relationship between the functional, non-functional and dependability requirements is illustrated in Figure C.1.



NOTE This is only an illustrative example to clarify the interrelationships between these concepts.

Figure C.1 – Example showing the relationship between the functional, non-functional and dependability requirements for a motor-driven pipeline pump

The decision-making process for performance requirements is largely standardized for this type of product and application. Reliability and availability prediction techniques for the components of the pump-motor system can be used by individual vendors but this is not as common for the final packaged system. Life cycle costs are estimated but sometimes do not include all life cycle costs. The lifetime of components can be estimated using Weibull analysis. Costs of preventive maintenance compared with maintenance on failure can be estimated. Often the cost of lost production due to an unscheduled outage is much larger than the cost of preventive maintenance. Users that acquire a complete understanding of dependability requirements are normally better able to manage the operation and maintenance phase of the life cycle.

C.2.2 Requirements determined by provider only

Acquiring a family car is a common decision process. The cost of owning and operating it is a major target objective but other performance requirements will influence the final cost and selection of a vehicle. There are quite a few options available to a buyer within a certain price range and the final selection is not always based on a rational evaluation of performance and dependability requirements. However, with the exception of some flexibility provided by options available to the customer, the fundamental performance requirements are fixed for each vehicle.

There are certain features of the car representing potential requirements that are essential to the customer. The selection criteria are based on the value of these features from the

customer's budget viewpoint. The conditions of use are defined by the driving environment such as type of roads, ambient temperature and possible rain or snow conditions.

The desirable functional and non-functional features for selection include

- size and capacity, both number and type of passengers and other carrying requirements,
- fuel economy,
- ease of driving and parking,
- safety protection such as crashworthiness,
- construction quality,
- initial purchase cost,
- operating and maintenance costs, and
- optional features.

The desirable dependability characteristics are mainly reliability, maintainability and supportability. Availability is not usually a major concern as long as maintenance support services are located close to the user but durability can be very important if the objective is to own the vehicle for a long time. The resultant dependability requirements for selection include

- reliability,
- maintainability,
- supportability,
- location and accessibility of maintenance support services, and
- durability.

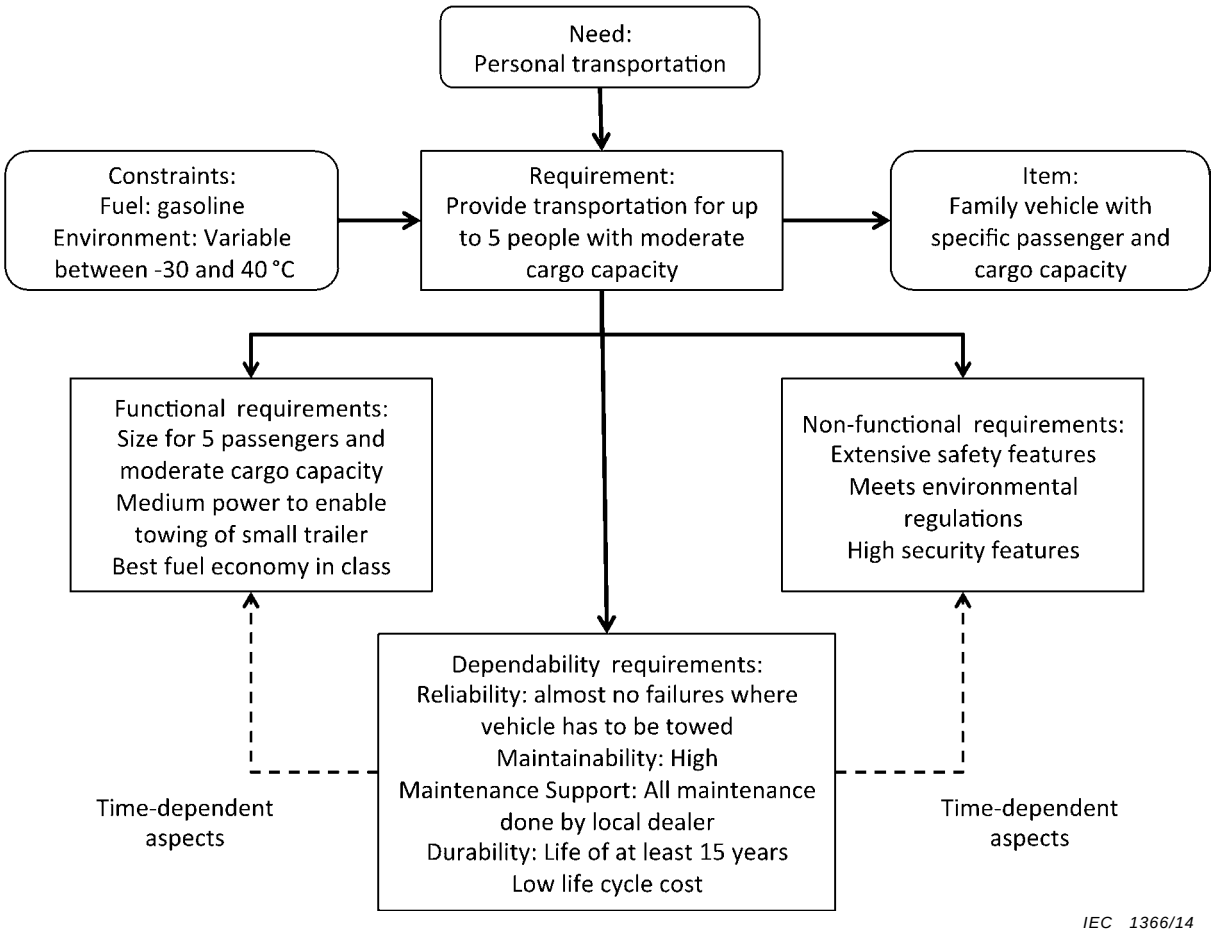
These features represent a set of performance requirements for the car under consideration by the user. There are interrelationships between the performance and dependability requirements, for example, maintainability will clearly influence maintenance costs and manufacturing quality will be related to durability. There are also requirements which compete and where trade-offs will need to be made. For example, while quality of build, reliability and safety are probably related, these are likely to conflict with a requirement for a low initial purchase cost.

The objective is to set a priority of importance pertaining to the relevant requirements identified which can be done by means of a decision matrix.

In this example the customer is faced with a set of options that fulfil the performance requirements to various degrees but none completely fulfil all requirements. One method by which a decision can be made is for the customer to weight the relative importance of their requirements, then to score each option according to how it achieves each requirement. The final choice is the option that achieves the highest total weighted score.

Although the individual user has no direct input to the performance requirements, manufacturers of personal vehicles will use various means such as customer surveys and quality function deployment to guide their selection of performance requirements and expectations for the target user market at which they are aiming.

A graphical representation of this example is shown in Figure C.2.



NOTE This is only an illustrative example to clarify the interrelationships between these concepts.

Figure C.2 – Example showing the relationship between the functional, non-functional and dependability requirements for a family car

Annex D
(informative)

Structure of dependability standards

D.1 Structure

The structure of IEC/TC56 standards is shown in Figure D.1.

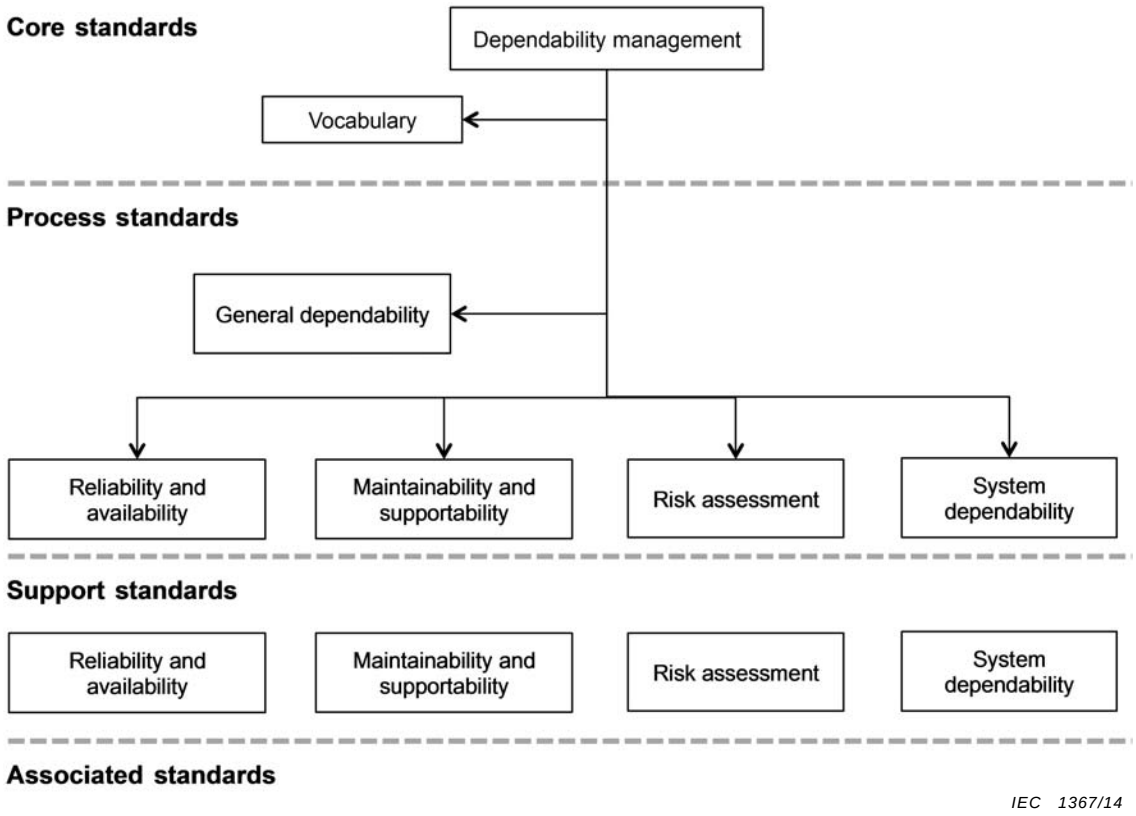


Figure D.1 – Framework for dependability standards

The dependability standards are structured into four levels to facilitate dependability applications and project implementation.

D.2 Core standards

Core standards provide guidance on overall management of dependability and present the standard framework for dependability application. In support of dependability management, the vocabulary contains the basic definitions relevant to dependability. Individual dependability standards can contain specific definitions applicable primarily to that standard.

D.3 Process standards

Process standards focus on the application processes of the major aspects of dependability to facilitate implementation of dependability for projects and achievement of other organizational objectives.

Process standards can be of a general nature, be associated with the dependability characteristics or relate to risk assessment and system aspects of dependability. Their purpose is to assist with the processes associated with implementation of dependability methods and techniques.

General dependability covers subjects such as life cycle costing and dependability specifications.

D.4 Support standards

Support standards are focused primarily on the specific methods and techniques for the process groupings.

Standards on reliability and availability deal with modeling and analysis, statistical analysis methods, reliability testing and screening and reliability growth.

Maintainability standards cover maintainability studies, testability and verification while supportability is concerned with aspects related to maintenance and maintenance management, reliability centered maintenance, maintenance support agreements and integrated logistic support.

Risk assessment standards provide support for tools that analyse risk such as FMEA and HAZOP as well as project risk.

System aspects consist of guidance for engineering and specification of dependability related to systems and networks. It also includes human and software reliability.

D.5 Associated standards

Associated standards include those standards which are not generated by IEC/TC 56, but are currently included within the list of standards on the TC 56 website for reference purposes.

The standard framework which presents the list of dependability standards and guidance on selection of standards for dependability project implementation, can be found on the IEC/TC 56 website [2].

Annex E
(informative)

Checklist for review of dependability

E.1 Introductory remark

The following checklists are examples of the dependability related issues that could be necessary for review by management to ensure that dependability objectives are being met. The lists should be tailored for individual circumstances with the agreement of both management and staff responsible for carrying out dependability activities. The checklists in the example are somewhat general and can require additional specific criteria to enable proper review.

E.2 Concept

E.2.1 Requirements definition

a) The dependability objectives established are suitable to meet market needs and user applications.

b) The extent of market scope and strategy for new initiatives are identified including customer use conditions and market operating conditions e.g. climatic conditions.

c) The dependability value, competitive leverage, incentives and application constraints are determined.

d) The timing for new product introduction and achievement targets are identified.

e) The tailoring criteria are established and applicable activities are identified.

f) The information on the proposed new system is adequate to initiate requirements analysis.

g) Stakeholder input into requirements and design to satisfy requirements has been obtained.

h) Risks that need to be taken into account in design have been identified.

E.2.2 Requirements analysis

a) The requirements analysis of the system boundaries, operating functions and performance characteristics and technology limitations has been conducted and determined.

b) The resource availability, technical capability, and new investment needs are identified.

c) The technical approaches and feasibility for system realization are identified.

d) The potential partnership and supplier requirements are identified.

e) The requirements analysis results and rationale can be justified for resource investments to initiate high-level concept design of the new system.

f) Risks of different options are assessed and taken into account in design selection.

g) Requirements for health, safety and the environment have been identified.

E.2.3 High-level architectural design

a) The architectural design criteria, possible item configuration and options are identified.

b) The technology selection for the design of item functions for realization is identified.

c) The forecasted probabilistic evaluations are consistent with the dependability targets.

d) The make/buy decision criteria are established.

e) The means for verification and integration of item functions have been established.

f) The criteria for hardware/software design functions have been established.

g) The criteria for environmental and ergonomic designs have been established.

h) The criteria for evaluation of item functions have been established.

i) The interoperability of system functions and performance limits has been verified to meet item requirements.

j) The dependability requirements in item specifications are incorporated as guidance for design and COTS acquisition.

k) The new item concept and architectural design options are identified and verified with associated constraints to justify initiation of formal item design with documented specifications.

l) Risks to performance associated with different designs are evaluated.

E.3 Development

E.3.1 Item design

a) The dependability plan for the design of the item and its components is established.

b) The quality assurance plan and item configuration management process are established.

c) The forecasted probabilistic evaluations are consistent with the dependability targets.

d) Test plans and acceptance criteria are established and simulation and tests have been performed.

e) The item monitoring and control, incidents reporting and data management systems have been established.

f) Component application has been reviewed with suppliers.

g) The suppliers' dependability programmes have been established.

h) The item design is verified and support programmes established for full-scale development.

E.3.2 Full-scale system development

a) The tailoring process for various item and functional development projects is implemented and the responsibility to each part of the project assigned, including dependability inputs to the design process.

b) The verification that the forecasted probabilistic evaluations are consistent with the dependability targets has been performed.

c) The item verification and validation plans have been developed.

d) The dependability acceptance criteria and reliability growth programmes have been established.

e) Design has been modified and reliability estimated.

f) Revision control of development documentation has been implemented.

g) Risks to functional and non-functional objectives and to dependability requirements have been assessed and treatment plans specified.

h) The item maintenance and logistics support programmes are established.

i) The outsourcing programmes are established.

j) The spares provisioning programme is developed.

k) The training programmes are established.

l) The warranty criteria for system service support are established.

m) The item is fully developed and ready for production and construction.

n) Software specifications and flow charts have been finished and approved.

o) The development of software module functions and subsystems has been initiated.

p) Requirements for health, safety and the environment have been analysed and the impact on dependability has been minimised.

E.4 Realization

E.4.1 Item realization

a) The production of hardware assemblies and functions has been initiated.

b) The suppliers' dependability programmes are implemented.

c) The item functions and subsystem verification and validation plans are implemented.

d) The failure reporting, analysis and data collection systems are implemented.

e) The training programmes are developed.

f) The item is produced, constructed and realized and ready for implementation.

E.4.2 Item implementation

a) The system integration plan is implemented.

b) Actions specified to treat risks have been implemented.

c) The item verification and validation plans are implemented.

d) The item qualification and acceptance plans are implemented.

e) The item installation plan is implemented.

f) The warranty plan is implemented.

g) The training programmes for system operation and customer care services are initiated.

h) The required design changes for fulfilling the dependability requirements have been implemented and verified.

i) The item is ready for release to operation.

E.5 Utilization

a) Maintenance and support programmes are implemented.

b) Risks are reassessed in the light of actual conditions.

c) The item performance and service maintenance are monitored and controlled.

d) The training programmes for operators and maintainers are implemented.

e) The field data collection system is implemented.

f) The design change and configuration controls are implemented.

g) The customer satisfaction survey is implemented.

h) The item performance data are analysed for continual improvement.

i) The item continues to sustain operational dependability-related performance.

E.6 Enhancement

a) The new item features and enhancement needs are identified.

b) The risk consequences, in particular with regards to health, safety and environmental requirements, and value of enhancement are analysed.

c) The enhancement programmes and improvement time frame are determined.

d) The decision for enhancement programmes is executed.

e) The customer satisfaction survey resulting from the enhancement programmes is monitored to determine enhancement value.

E.7 Retirement

a) The decommissioning and disposal strategy is planned and initiated.

b) The impact of service termination is determined.

c) The schedule and timing for service termination and the new or alternative service provisions have been notified to customers.

d) The customer satisfaction survey resulting from termination of the old service and the use of the new service is monitored.

e) Required data has been transferred.

Bibliography

[1] IEC 60050-191:2014, *International Electrotechnical Vocabulary – Part 191: Dependability*

[2] IEC/TC 56 website, http://tc56.iec.ch

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 1: Lignes directrices pour la gestion et l'application

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 60300-1 a été établie par le comité d'études 56 de l'IEC: Sûreté de fonctionnement.

Cette troisième édition annule et remplace la deuxième édition parue en 2003. Cette édition constitue une révision technique.

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

a) des définitions actualisées selon la toute dernière version du IEC 60050-191:2014;
b) une meilleure description de la sûreté de fonctionnement et de ses attributs;
c) une approche plus générique de la gestion de la sûreté de fonctionnement;

d) des lignes directrices révisées pour l'application de la gestion de la sûreté de fonctionnement;

e) une approche plus générique du cycle de vie;

f) un cadre pour les normes de sûreté de fonctionnement.

En plus, cette troisième édition annule et remplace la deuxième édition du document IEC 60300-2 qui a été publié en 2004.

La présente version bilingue (2014-08) correspond à la version anglaise monolingue publiée en 2014-05.

Le text anglais de cette norme est issu des documents 56/1550/FDIS et 56/1556/RVD.

Le rapport de vote 56/1556/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 60300, publiées sous le titre général *Gestion de la sûreté de fonctionnement*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

La présente partie de l'IEC 60300 décrit les processus impliqués dans la gestion de la sûreté de fonctionnement au sein d'un organisme et établit un cadre pour la gestion des activités de sûreté de fonctionnement, dans le but d'obtenir les performances de sûreté de fonctionnement.

La sûreté de fonctionnement est la capacité d'une entité à fonctionner correctement et au moment voulu. La sûreté de fonctionnement est un terme utilisé pour décrire les caractéristiques liées au temps et associées aux performances d'une entité. La sûreté de fonctionnement inclut des caractéristiques telles que la disponibilité, la fiabilité, la maintenabilité et la supportabilité pour des conditions d'utilisation et des exigences de logistique de maintenance données. La sûreté de fonctionnement décrit dans quelle mesure il est possible d'avoir confiance en la capacité d'une entité à se comporter comme prévu.

La sûreté de fonctionnement génère de la confiance et influence la capacité d'un organisme à atteindre ses objectifs. La sûreté de fonctionnement est obtenue en planifiant et en mettant en œuvre les activités de sûreté de fonctionnement tout au long du cycle de vie des entités.

La sûreté de fonctionnement a un impact important sur la perception de l'utilisateur sur la valeur d'une entité conçue ou fournie par un organisme. Une faible sûreté de fonctionnement affectera la capacité d'un organisme à atteindre ses objectifs ainsi que sa réputation.

La gestion de la sûreté de fonctionnement apporte une approche systématique permettant de traiter la sûreté de fonctionnement et les enjeux associés d'un point de vue organisationnel et commercial. La sûreté de fonctionnement est souvent orientée par la technologie et requiert l'intégration de l'innovation dans les produits existants. L'obtention de la sûreté de fonctionnement tout au long du processus de cycle de vie peut être influencée par les dynamiques des marchés, l'économie mondiale et les distributions des ressources, les modifications des besoins des consommateurs et un environnement compétitif. Les stratégies doivent s'adapter aux modifications prévues pour maintenir la viabilité des opérations commerciales. La gestion de la sûreté de fonctionnement se concentre sur les besoins des parties prenantes en optimisant la sûreté de fonctionnement afin d'améliorer les objectifs organisationnels et les retours sur investissement.

La présente norme est spécifiquement destinée à s'appliquer aux produits, aux systèmes, aux processus et aux services technologiques, qui sont désignés par le terme général "entité" dans la présente norme. Cependant, la plupart des lignes directrices fournies sont génériques et peuvent être adaptées pour être appliquées dans différentes applications non technologiques. De plus, lors de l'optimisation de la sûreté de fonctionnement, il convient d'identifier, d'analyser et de gérer les effets secondaires potentiels sur la sécurité, l'environnement et les autres facteurs.

La présente norme s'adresse aux utilisateurs, aux propriétaires, aux clients et aux organismes impliqués et chargés de garantir la conformité aux exigences de sûreté de fonctionnement. Les organismes comprennent tous types et tailles d'entreprises, d'institutions publiques ou privées tels que les administrations publiques, les entreprises commerciales et les associations à but non lucratif.

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 1: Lignes directrices pour la gestion et l'application

1 Domaine d'application

La présente partie de l'IEC 60300 établit un cadre pour la gestion de la sûreté de fonctionnement. Elle donne des lignes directrices sur la gestion de la sûreté de fonctionnement des produits, des systèmes, des processus ou des services impliquant des aspects matériels, logiciels et humains ou toute combinaison intégrant ces éléments. Elle présente des lignes directrices sur la planification et la mise en œuvre des activités de sûreté de fonctionnement et des processus techniques tout au long du cycle de vie, en prenant en compte les autres exigences telles que celles relatives à la sécurité et à l'environnement.

La présente norme donne des lignes directrices qui aident les directeurs et leur personnel technique à optimiser la sûreté de fonctionnement.

La présente norme n'a pas pour objectif la certification.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

Aucune.

3 Termes, définitions et abréviations

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1 Termes et définitions

3.1.1
disponibilité (caractéristiques d'une entité)
aptitude à être en état de fonctionner tel que demandé

Note 1 à l'article: La disponibilité dépend des caractéristiques combinées de la fiabilité, de la récupérabilité et de la maintenabilité de l'entité et, dans certains cas, des performances de la logistique de maintenance.

Note 2 à l'article: La disponibilité peut être quantifiée à l'aide de mesures de performances appropriées.

[SOURCE: IEC 60050-191:2014 [1][1], 191-41-23]

3.1.2
sûreté de fonctionnement (d'une entité)
aptitude à fonctionner tel que demandé et au moment voulu

[1] Les références entre crochets se rapportent à la Bibliographie.

Note 1 à l'article: La sûreté de fonctionnement comprend la disponibilité, la fiabilité, la récupérabilité, la maintenabilité et les performances de la logistique de maintenance et, dans certains cas, d'autres caractéristiques comme la durabilité, la sécurité et la sûreté.

Note 2 à l'article: "Sûreté de fonctionnement" est utilisé comme terme collectif pour les caractéristiques qualitatives d'une entité qui sont relatives au temps.

[SOURCE: IEC 60050-191:2014, 191-41-22]

3.1.3
dossier de sûreté de fonctionnement
argumentation factuelle, rationnelle et traçable produite pour supporter l'affirmation selon laquelle un système défini satisfera aux exigences de sûreté de fonctionnement

3.1.4
gestion de la sûreté de fonctionnement
activités coordonnées destinées à orienter et contrôler un organisme en matière de sûreté de fonctionnement

Note 1 à l'article: La gestion de la sûreté de fonctionnement fait partie du système de management global d'un organisme.

3.1.5
système de gestion de la sûreté de fonctionnement
ensemble d'éléments reliés ou interagissant d'un organisme destiné à établir des politiques et des objectifs relatifs à la sûreté de fonctionnement et des processus permettant d'atteindre ces objectifs de sûreté de fonctionnement

Note 1 à l'article: Les systèmes de gestion de la sûreté de fonctionnement font partie du système de management global et ne sont généralement pas un système de management séparé.

Note 2 à l'article: Les éléments du système comprennent la structure, les rôles et les responsabilités, la planification, les procédures et les processus au sein de l'organisme.

3.1.6
plan de sûreté de fonctionnement
ensemble d'activités planifiées permettant d'atteindre les objectifs de sûreté de fonctionnement d'une entité

3.1.7
programme de sûreté de fonctionnement
ensemble coordonné de plans décrivant les activités qui conduisent à la réalisation des objectifs de sûreté de fonctionnement économiquement rentables et la façon dont ils sont approvisionnés en ressources

3.1.8
entité
sujet à l'étude

Note 1 à l'article: Il peut s'agir d'un élément, composant, dispositif, unité fonctionnelle, équipement, sous-système ou système.

Note 2 à l'article: L'entité peut être constituée de matériel, de logiciel, de personnel ou une combinaison de ces éléments.

Note 3 à l'article: L'entité est souvent constituée d'éléments que l'on peut considérer individuellement.

[SOURCE: IEC 60050-191:2014, 191-41-01]

3.1.9
cycle de vie
série d'étapes identifiables que traverse une entité, de sa conception à sa mise au rebut

Note 1 à l'article: Les étapes identifiées varieront en fonction de l'application.

EXEMPLE Le cycle de vie classique d'un système est composé des phases suivantes: concept et définition; conception et développement; fabrication et mise en service; exploitation et maintenance; rénovation à mi-vie ou prolongation de la durée de vie, mise hors service et mise au rebut.

[SOURCE: IEC 60050-191:2014, 191-41-09]

3.1.10
maintenabilité (caractéristique d'une entité)
aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut fonctionner tel que demandé, dans des conditions données d'utilisation et de maintenance

Note 1 à l'article: Les conditions données incluent les aspects ayant un impact sur la maintenabilité, tels que: l'emplacement de maintenance, l'accessibilité, les procédures de maintenance et les ressources de maintenance.

Note 2 à l'article: La maintenabilité peut être quantifiée à l'aide de mesures de performances appropriées.

[SOURCE: IEC 60050-191:2014, 191-41-27]

3.1.11
logistique de maintenance
mise à disposition de ressources pour maintenir une entité

Note 1 à l'article: Les ressources comprennent les ressources humaines, les équipements de soutien, les ressources matérielles et les pièces de rechange, les installations de maintenance, la documentation, les informations et les systèmes d'informations de maintenance.

[SOURCE: IEC 60050-191:2014, 191-41-28]

3.1.12
organisme
personne ou groupe de personnes ayant ses propres fonctions avec des responsabilités, des liaisons hiérarchiques et des relations lui permettant d'atteindre ses objectifs

Note 1 à l'article: Le concept d'organisme comprend, sans toutefois s'y limiter: les entreprises individuelles les compagnies, les sociétés, les firmes, les entreprises, les autorités, les partenariats, les organisations caritatives ou les institutions, ou partie de celles-ci, à responsabilité limitée ou d'un autre statut, de droit public ou privé.

Note 2 à l'article: Dans le cas des organismes comprenant plusieurs unités de fonctionnement, une seule unité peut être définie comme un organisme.

3.1.13
fiabilité (caractéristique d'une entité)
aptitude d'une entité à fonctionner tel que demandée, sans défaillance, pendant un intervalle de temps donné, dans des conditions données

Note 1 à l'article: La durée de l'intervalle de temps peut être exprimée en unités adaptées à l'entité concernée, par exemple, en durée calendaire, en cycles de fonctionnement, en distance parcourue, etc., et il convient de toujours indiquer clairement les unités.

Note 2 à l'article: Les conditions données incluent des aspects qui affectent la fiabilité, comme: 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 de performances appropriées.

[SOURCE: IEC 60050-191:2014, 191-41-24]

3.1.14
exigence
besoin ou attente formulés, habituellement implicites ou imposés

[SOURCE: ISO 9000:2005, 3.1.2]

3.1.15
partie prenante
personne ou organisme qui peut affecter, être affecté(e) ou se sentir affecté(e) par une décision ou une activité

3.1.16
supportabilité (d'une entité)
aptitude à pouvoir assurer la disponibilité requise avec un profil opérationnel défini et avec des ressources logistiques et de maintenance

Note 1 à l'article: La supportabilité complète la fiabilité et la maintenabilité inhérentes à l'entité, combinées à des facteurs externes à l'entité, qui ont un impact sur la facilité relative d'assurer la maintenance et le soutien logistique requis.

[SOURCE: IEC 60050-191:2014, 191-41-31, avec modification de la note 1]

3.1.17
système (en sûreté de fonctionnement)
ensemble d'entités interdépendantes qui satisfont collectivement à une exigence

Note 1 à l'article: On considère qu'un système possède une limite définie réelle ou abstraite.

Note 2 à l'article: Des ressources externes (à la limite du système) peuvent être exigées pour permettre au système de fonctionner.

Note 3 à l'article: Une structure de système peut être hiérarchique, par exemple, un système, un sous-système, un composant, etc.

Note 4 à l'article: Il convient d'indiquer ou d'inclure dans l'exigence les conditions d'utilisation et de maintenance.

[SOURCE: IEC 60050-191:2014, 191-41-03]

3.1.18
adaptation (processus)
processus permettant d'adapter, d'ajuster ou de modifier au sein de l'organisme un ensemble de processus et d'activités établis afin de réaliser, satisfaire ou remplir des exigences s'appliquant à la sûreté de fonctionnement

3.2 Abréviations

COTS	Commercial-off-the-shelf (Produits du commerce)
AMDE	Analyse des modes de défaillance et de leurs effets
FRACAS	Failure recording, analysis and corrective action system (Système de compte-rendu des défaillances, d'analyse et d'action corrective)
AAP	Analyse par arbre de panne
HSE	Health, safety and environment (Santé, sécurité et environnement)
MTBF	Moyenne des temps de bon fonctionnement
HAZOP	Hazard and operability studies (Études de danger et d'exploitabilité)
RCM	Reliability centred maintenance (Maintenance basée sur la fiabilité)

4 Gestion de la sûreté de fonctionnement

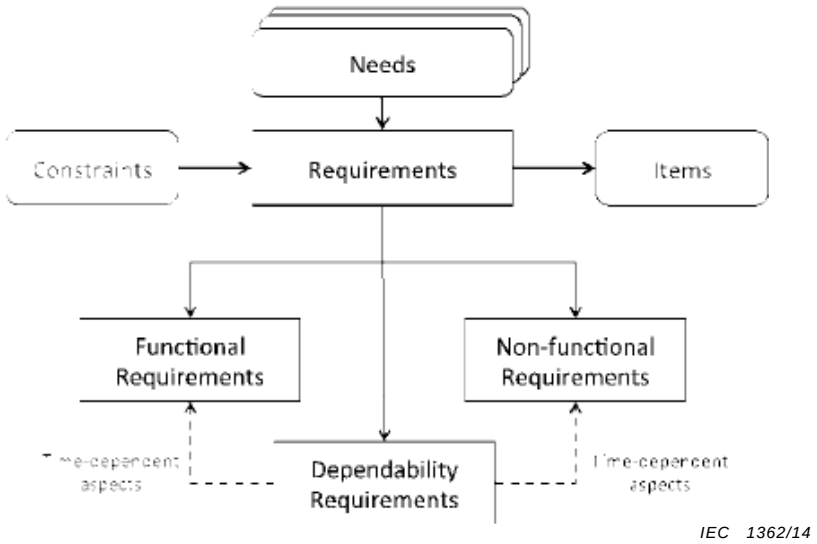
4.1 Comprendre la sûreté de fonctionnement

La sûreté de fonctionnement est la capacité d'une entité à fonctionner correctement et au moment voulu. La sûreté de fonctionnement est donc la capacité à satisfaire aux exigences et aux attentes d'une entité de manière constante. La sûreté de fonctionnement crée de la valeur dans la mesure où l'entité conserve ses caractéristiques de performances, fonctionne comme souhaité et satisfait aux besoins et attentes du client.

La gestion de la sûreté de fonctionnement est un élément clé des systèmes de gestion plus larges d'un organisme, en particulier les systèmes relatifs aux biens, à la finance et à la qualité. La gestion de la sûreté de fonctionnement comprend la planification et l'application des dispositions organisationnelles, des processus et des méthodes et techniques associées, permettant d'atteindre les performances de l'organisme et les objectifs des produits.

La sûreté de fonctionnement est améliorée en réduisant systématiquement la fréquence des indisponibilités, des défaillances des produits, des temps d'indisponibilité et autres événements non désirés et en minimisant leurs effets. Ceci est obtenu par des actions telles que l'amélioration de la conception, l'élimination des causes premières de défaillance, la simplification des processus complexes, l'atténuation des anomalies, la promotion de la tolérance aux pannes dans la conception et l'aptitude à l'emploi, la recommandation de l'évitement des pannes et de la prévention des erreurs, la gestion des activités de maintenance et la prise d'engagements, afin d'augmenter la confiance et l'intégrité qui permettent de garantir la confiance de l'utilisateur tout au long du cycle de vie. Prendre en compte la sûreté de fonctionnement dès les premières phases du cycle de vie est capital, dans la mesure où rectifier ultérieurement une conception qui provoque une faible sûreté de fonctionnement sera souvent plus difficile, chronophage et onéreux.

La Figure 1 illustre la relation entre la sûreté de fonctionnement et les besoins des parties prenantes et les exigences d'une entité. Selon le contexte, les parties prenantes peuvent être des utilisateurs, des propriétaires, des clients, des administrations publiques, des entreprises et des organisations en charge de garantir la satisfaction aux exigences de sûreté de fonctionnement.



Légende

Anglais	Français
Needs	Besoins
Constraints	Contraintes
Requirements	Exigences
Items	Entités
Functional requirements	Exigences fonctionnelles
Non-functional requirements	Exigences non fonctionnelles
Time dependent aspects	Aspects dépendants du temps
Dependability requirements	Exigences de sûreté de fonctionnement

Figure 1 – Relation entre la sûreté de fonctionnement et les besoins et les exigences d'une entité (produit, système, processus ou service)

Les exigences sont déterminées à partir des besoins des parties prenantes et des contraintes comme les conditions d'utilisation, les ressources et la législation. Elles comprennent des exigences fonctionnelles qui définissent ce qu'il est exigé d'une entité, et des exigences non fonctionnelles qui spécifient les attributs supplémentaires. Les exigences fonctionnelles sont par exemple la capacité et la puissance fournie et les exigences non fonctionnelles sont par exemple la sécurité, la durabilité et l'efficacité environnementales. Les exigences de sûreté de fonctionnement, qui définissent l'aptitude liée au temps permettant d'obtenir les performances de sûreté de fonctionnement correspondant à ces exigences, comprennent des caractéristiques comme la fiabilité, la disponibilité, la maintenabilité et la supportabilité.

Les exigences fonctionnelles et non fonctionnelles et les exigences de sûreté de fonctionnement sont interdépendantes. Une exigence de sûreté de fonctionnement ne peut exister que si une exigence fonctionnelle ou non fonctionnelle est à satisfaire. Il peut y avoir des objectifs en contradiction entre les exigences souhaitées comme la sécurité ou la production de pétrole/gaz et la sûreté de fonctionnement et des compromis peuvent donc être nécessaires. Il peut aussi exister des contraintes liées au coût, à la disponibilité des composants ou des ressources de l'entité, ou des calendriers fixes susceptibles de nécessiter un compromis entre la fonctionnalité et la sûreté de fonctionnement.

La perception de la capacité à fonctionner correctement et au moment voulu peut varier selon les différentes parties prenantes. Les utilisateurs, les fournisseurs, les opérateurs, les personnes responsables de la maintenance et ceux qui interagissent avec une entité peuvent avoir des exigences de sûreté de fonctionnement qui coïncident, mais des objectifs d'application et des attentes d'utilisation qui diffèrent. Cela peut avoir pour résultat des perceptions différentes de la sûreté de fonctionnement qu'il pourrait être nécessaire de prendre en compte lors de la définition des exigences.

La sûreté de fonctionnement inclut des caractéristiques objectivement mesurables comme la fiabilité, la disponibilité et la maintenabilité, ainsi que des jugements plus subjectifs de la véracité concernant les fonctions exigées par les parties prenantes spécifiques. La capacité à mesurer la réalisation des objectifs de performances est une considération fondamentale dans la détermination des exigences.

La sûreté de fonctionnement inclut à la fois l'aptitude à satisfaire aux exigences fonctionnelles et non fonctionnelles dans des conditions normales et attendues, et l'aptitude à s'adapter aux changements inattendus des exigences, des hypothèses et des circonstances, pour restaurer l'entité suite à des défaillances externes du système.

4.2 Avantages de la gestion de la sûreté de fonctionnement

La gestion de la sûreté de fonctionnement présente les avantages suivants:

- satisfaire aux exigences et aux objectifs des parties prenantes,
- obtenir des niveaux attendus de service,
- maintenir la capacité de production ou de fabrication au moyen d'une disponibilité accrue,
- améliorer la sécurité lorsque des conséquences nuisibles potentielles sont identifiées et traitées de façon adéquate,
- réduire l'impact sur l'environnement lorsque des conséquences nuisibles potentielles sont identifiées et traitées de façon adéquate,
- augmenter la durée de vie et la durabilité, et réduire les coûts du cycle de vie, et
- améliorer la qualité.

4.3 Enjeux relatifs à la gestion de la sûreté de fonctionnement

Il est nécessaire de traiter la sûreté de fonctionnement tout au long du cycle de vie d'une entité. Prendre en compte et mettre en œuvre les activités pertinentes de sûreté de fonctionnement dès les premières phases du cycle de vie permettra de mieux garantir la réalisation des exigences de sûreté de fonctionnement.

Il peut y avoir des complications lorsque plusieurs organismes sont impliqués, lors d'une rénovation à mi-vie, ou lorsque la sûreté de fonctionnement de l'entité est influencée par des systèmes interconnectés et externes.

Les entités sont souvent intégrées pour fonctionner avec des entités existantes qui se trouvent à différentes phases du cycle de vie, avec des technologies et des méthodes de conception qui sont plus anciennes. La gestion de la sûreté de fonctionnement nécessite d'assurer l'interopérabilité et la sûreté de fonctionnement des entités intégrées au moyen des spécifications d'interface pour garantir des performances fiables.

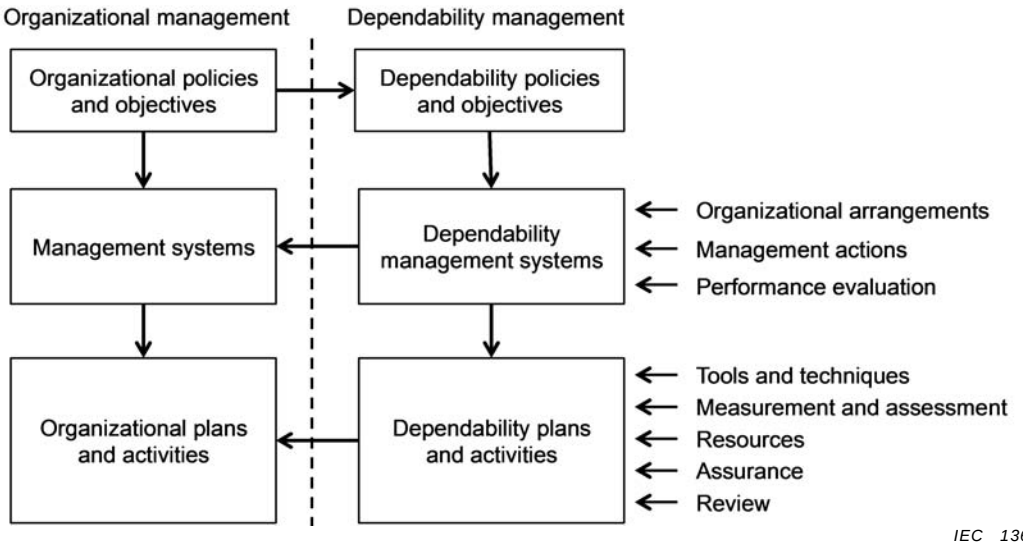
Les systèmes deviennent plus complexes et peuvent présenter les caractéristiques de "systèmes ouverts", "systèmes de systèmes" ou de "systèmes non limités ou faiblement limités". Les systèmes peuvent être gérés par différentes parties qui ont différents objectifs et qui peuvent se trouver à différentes phases du cycle de vie. Ceci, associé à l'étendue et à la complexité du système, complique la compréhension du système dans son ensemble pour les parties prenantes; les changements sont donc moins prévisibles et contrôlables. Pour cette raison, il est capital pour les parties prenantes de comprendre et de convenir des limites de leurs responsabilités, ainsi que d'attribuer la responsabilisation de la mise en œuvre. La planification de la sûreté de fonctionnement nécessite de prendre en compte la possibilité de défaillances et de changements majeurs au sein et hors des limites respectives.

5 Système de gestion de la sûreté de fonctionnement

5.1 Présentation générale

Un système de gestion de la sûreté de fonctionnement est destiné à orienter et contrôler un organisme en matière de sûreté de fonctionnement, en coordination avec d'autres disciplines, afin de fournir un effort efficace et intégré permettant d'atteindre les objectifs. Les politiques et les objectifs organisationnels peuvent inclure des politiques et des objectifs de sûreté de fonctionnement, qui aboutissent ensuite à un système de gestion de la sûreté de fonctionnement qui peut les mettre en œuvre de manière efficace.

La Figure 2 montre l'intégration de la gestion de la sûreté de fonctionnement dans un système générique de management. Le système de gestion de la sûreté de fonctionnement donne lieu à un programme de sûreté de fonctionnement qui entretient les plans et les activités organisationnels.



Légende

Anglais	Français
Organizational management	Gestion organisationnelle

Anglais	Français
Organizational policies and objectives	Politiques et objectifs organisationnels
Management systems	Systèmes de management
Organisational plans and activities	Plans et activités organisationnels
Dependability management	Gestion de la sûreté de fonctionnement
Dependability policies and objectives	Politiques et objectifs de sûreté de fonctionnement
Dependability management systems	Systèmes de gestion de la sûreté de fonctionnement
Dependability plans and activities	Plans et activités de sûreté de fonctionnement
Organisational arrangements	Dispositions organisationnelles
Management actions	Actions de gestion
Performance evaluation	Évaluation des performances
Activities	Activités
Tools and techniques	Outils et techniques
Measurement and assessment	Mesure et évaluation
Resources	Ressources
Assurance	Assurance
Review	Revue

Figure 2 – Systèmes de gestion de la sûreté de fonctionnement

Un système de gestion de la sûreté de fonctionnement comprend trois éléments:

- des dispositions organisationnelles destinées à mettre en œuvre les politiques et objectifs de sûreté de fonctionnement;
- des activités de sûreté de fonctionnement mises en œuvre dans le programme de sûreté de fonctionnement;
- des dispositions d'évaluation des performances.

5.2 Dispositions organisationnelles

L'établissement des dispositions organisationnelles consiste à déterminer la structure de management nécessaire pour faciliter la mise en œuvre efficace des politiques de sûreté de fonctionnement. Il convient que les systèmes de management d'un organisme intègrent la gestion de la sûreté de fonctionnement afin d'assurer l'efficacité des prises de décision et d'influencer l'orientation technique. Il convient notamment que l'ingénierie de la sûreté de fonctionnement soit étroitement intégrée aux projets d'ingénierie pour en améliorer la conception et les processus. L'Annexe A décrit l'intégration des activités de sûreté de fonctionnement dans les opérations, les stratégies et les processus organisationnels, afin d'atteindre les objectifs longs termes et ceux des projets en cours.

Il est nécessaire d'aligner les politiques et les objectifs de sûreté de fonctionnement sur les politiques et les objectifs organisationnels et sur ceux des parties prenantes incluant les deux perspectives technique et commercial. Il convient que les dispositions organisationnelles concernant la gestion de la sûreté de fonctionnement tiennent compte du contexte de l'organisme, de ses objectifs et des stratégies choisies pour les atteindre, ainsi que des risques et des opportunités qui y sont associés.

Les systèmes de gestion de la sûreté de fonctionnement n'exigent pas toujours d'une infrastructure organisationnelle complexe et un rapport hiérarchique pour être efficace. Les activités de sûreté de fonctionnement peuvent être gérées par une unité organisationnelle séparée avec une étroite coordination, être entièrement intégrées dans d'autres domaines pertinents, ou un mixte de ces deux approches. L'alignement de la structure organisationnelle, des responsabilités, des procédures, des activités, des ressources et des informations est capital pour une orientation et un contrôle efficaces et efficients de la sûreté de fonctionnement. Il convient que la gestion de la sûreté de fonctionnement soit impliquée

dans les activités de planification, de revue, d'audit, de vérification et de validation des projets en cours.

Lorsque des fonctions comme la conception, la maintenance et la logistique de maintenance sont externalisées, il convient de spécifier, de surveiller et de contrôler la responsabilité des aspects de sûreté de fonctionnement de l'externalisation.

L'un des enjeux de la gestion de la sûreté de fonctionnement au cours du cycle de vie réside dans le fait qu'il existe souvent plusieurs organismes impliqués. Au cours du cycle de vie, il peut être nécessaire de transférer certaines responsabilités d'un organisme à un autre. Dans la mesure où les styles et les procédures organisationnelles varient, il est nécessaire que la gestion de la sûreté de fonctionnement s'adapte aux différentes situations.

Il convient d'établir un moyen de gérer et de contrôler les données et les informations de sûreté de fonctionnement au sein des systèmes d'information de gestion de l'organisme. Cela permet de fournir à la direction des informations sur les données historiques et les enregistrements relatifs à la sûreté de fonctionnement, permettant ainsi de mesurer l'état et les améliorations de la sûreté de fonctionnement.

5.3 Actions de gestion

Une gestion efficace de la sûreté de fonctionnement permet de garantir que les exigences de sûreté de fonctionnement sont satisfaites, comme les exigences fonctionnelles et non fonctionnelles.

Il convient que les actions de gestion comprennent les actions suivantes:

- donner des directives par le biais de l'engagement de la direction, l'orientation de la politique et l'établissement des rôles, des responsabilités et de l'autorité;
- prévoir la planification et le contrôle opérationnels pour atteindre les objectifs de sûreté de fonctionnement et gérer les risques;
- impliquer les parties prenantes en identifiant les exigences et les enjeux de la sûreté de fonctionnement, en communiquant l'état du programme de sûreté de fonctionnement, les conflits résolus et les compromis, et en garantissant et en maintenant les accords et les responsabilités;
- coordonner les différentes fonctions organisationnelles qui sont impliquées dans les activités de sûreté de fonctionnement avec une responsabilité assignée de sûreté de fonctionnement pour la coordination de l'effort technique et de gestion;
- gérer les risques par rapport aux objectifs et cibles de sûreté de fonctionnement;
- fournir et gérer les ressources y compris l'acquisition de biens d'équipement, la formation des équipes et sa répartition, l'externalisation et la sous-traitance des tâches techniques de sûreté de fonctionnement;
- gérer les activités techniques nécessaires au cours du cycle de vie d'une entité afin d'obtenir la sûreté de fonctionnement;
- gérer les connaissances et les informations par la saisie et la diffusion des données et des connaissances pertinentes de sûreté de fonctionnement, notamment la maintenance d'une base de données des performances de sûreté de fonctionnement;
- évaluer les performances en réalisant les opérations de surveillance, d'analyse de mesure et d'évaluation, d'audit, d'assurance et de revue de direction;
- assurer l'amélioration continue au moyen de la planification et du contrôle des activités d'amélioration et des revues appropriées d'avancement.

Il convient que l'attention de la direction soit attirée sur les enjeux relatifs à la sûreté de fonctionnement et les préoccupations techniques, lors des réunions de revue de direction pour résoudre, décider et fixer les priorités des affectations des tâches.

5.4 Évaluation des performances

On évalue les performances des dispositions et des processus organisationnels pour garantir aux parties prenantes concernées que les activités de gestion de la sûreté de fonctionnement sont correctement effectuées et qu'elles réaliseront les performances exigées de sûreté de fonctionnement.

Il convient que l'organisme définisse les indicateurs et les objectifs de performances pour le système de gestion de la sûreté de fonctionnement et qu'il surveille les mesures, analyse et améliore les performances par rapport à ces indicateurs et à ces objectifs.

Cela peut inclure

- l'évaluation du fonctionnement et de l'efficacité des processus, des activités et des procédures de sûreté de fonctionnement,
- l'évaluation si les politiques et les objectifs de sûreté de fonctionnement de l'organisme sont atteints,
- la revue de la pertinence du programme, des politiques et des objectifs de sûreté de fonctionnement,
- l'évaluation des performances de sûreté de fonctionnement des entités, et
- la surveillance des accords et des responsabilités.

6 Application de la gestion de la sûreté de fonctionnement

6.1 Adaptation d'un programme de sûreté de fonctionnement

Les éléments de base d'un programme de sûreté de fonctionnement sont les suivants:

- des plans de sûreté de fonctionnement qui définissent les activités, les techniques et les ressources exigées pour obtenir la sûreté de fonctionnement des entités;
- des méthodes de mesure et d'évaluation;
- des procédures d'assurance et de revue (voir Figure 2).

Il convient que la direction responsable de la sûreté de fonctionnement résultante d'une entité adapte ces éléments pour remplir les objectifs de sûreté de fonctionnement pour cette situation ou ce projet en particulier. L'adaptation s'applique à toute phase du cycle de vie, mais une adaptation importante a lieu au cours des phases initiales de conception du cycle de vie. Il pourrait ne pas être nécessaire d'adapter ces activités dans tous les cas, par exemple, lorsque des fabricants développent et produisent des produits similaires.

L'adaptation générale du programme de sûreté de fonctionnement comprend les points suivants:

- l'identification du contexte organisationnel, notamment la politique et l'infrastructure;
- la prise en compte des exigences réglementaires ou des normes;
- l'identification des caractéristiques relatives à l'entité comme ses propriétés et ses fonctions, l'historique d'entités similaires, l'usage final prévu et les environnements d'application envisagés;
- l'analyse des objectifs et des exigences;
- la détermination des étapes ou des phases spécifiques du cycle de vie qui sont applicables;
- l'évaluation des risques;
- la sélection des activités de sûreté de fonctionnement qui sont pertinentes pour les étapes ou les phases spécifiques identifiées du cycle de vie;

- la sélection des outils et des activités techniques nécessaires pour réaliser la sûreté de fonctionnement;
- la sélection des techniques de mesure et d'évaluation;
- la définition de la capacité et des ressources nécessaires et réellement disponibles pour la mise en œuvre;
- la priorisation et l'affectation des ressources;
- la planification des revues et de l'assurance;
- la documentation des justifications de la formalisation des décisions d'adaptation dans le cadre du plan d'organisation ou de projet.

Si l'étendue du programme impose la nécessité d'un plan propre à chaque domaine fonctionnel, chaque plan séparé peut documenter ces activités de sûreté de fonctionnement.

Les critères et les lignes directrices d'adaptation décrivent les points suivants:

- la façon dont les activités de sûreté de fonctionnement d'un organisme sont utilisées dans les processus de projet,
- les exigences obligatoires et légales qu'il faut satisfaire,
- les options qui peuvent être appliquées et les critères de sélection entre ces options, et
- la façon dont il faut décider des procédures de sûreté de fonctionnement qu'il convient d'exécuter.

L'adaptation nécessite de prendre en compte la nature des tâches d'organisation et de sûreté de fonctionnement qu'il est nécessaire de gérer. L'organisme peut varier d'un cabinet de conseil technique, jusqu'à un conglomérat multinational exigeant une gestion appropriée de la sûreté de fonctionnement des différentes disciplines, organisations et spécialisations. Les approches de gestion recherchent souvent le transfert de technologie, l'apport de connaissances ou les conseils d'expert comme moyens de pallier les lacunes techniques critiques à court terme.

L'adaptation des activités de sûreté de fonctionnement inclut la prise en compte des processus techniques et administratifs de l'organisme, ainsi que les contraintes et les facteurs d'influence qui comprennent, sans toutefois s'y limiter, les éléments suivants:

- les exigences de la clientèle;
- les exigences réglementaires;
- les exigences de sécurité;
- les objectifs de livraison;
- les budgets possibles;
- les ressources disponibles;
- la capacité technique;
- l'impact sur l'environnement;
- l'innovation de l'implication technologique;
- la mise à disposition de services durables.

Le résultat des activités d'adaptation constitue la base d'un plan de sûreté de fonctionnement pour les activités et les ressources du projet considéré. Il convient que l'étendue et le niveau de détail de ce plan permettent d'effectuer des mesures en termes de suivi de gestion et d'estimation des coûts. Il convient que le plan de projet global soit constitué par les plans adaptés, ainsi que par d'autres plans comme ceux relatifs à la sécurité, à la planification, à l'intégration, à la production, aux opérations et à la maintenance, constitue la base de l'ensemble du plan projet. L'intégration à ce plan de projet global peut exiger plus d'adaptation afin d'ajuster le temps de projet et les limites de coûts. Cela peut entraîner un

compromis entre la sûreté de fonctionnement prévue du produit d'un côté et la planification et le coût du projet de l'autre.

Il convient que l'apport de flexibilité par l'adaptation soit équilibré par la nécessité de garantir une cohérence appropriée dans les activités de sûreté de fonctionnement d'un bout à l'autre de l'organisme. La flexibilité est nécessaire pour faire face aux variables contextuelles comme la nature de la clientèle, le coût, la programmation, les compromis sur la qualité et la difficulté technique du travail, ainsi que le degré d'expérience des personnes mettant en œuvre le processus. Les critères d'adaptation peuvent tenir compte de l'utilisation d'un processus normalisé sans adaptation ou d'une approche présentant seulement quelques différences par rapport à un processus normalisé.

6.2 Analyse des objectifs et des exigences

Les exigences sont définies pour satisfaire les besoins et les objectifs des parties prenantes. Les exigences peuvent être divisées en deux groupes interdépendants, les exigences fonctionnelles et non fonctionnelles, et ces deux groupes peuvent comprendre des exigences de sûreté de fonctionnement (voir Figure 1). L'Annexe C décrit comment les exigences de sûreté de fonctionnement peuvent être définies.

Dans la mesure où les perceptions de la sûreté de fonctionnement peuvent varier selon la partie prenante, il est important de s'assurer que toutes les parties prenantes concernées communiquent et se consultent correctement au moment de définir les exigences et la façon dont elles seront évaluées.

Lorsqu'un contrat lie un client et un fournisseur, il est nécessaire que ceux-ci se mettent d'accord sur la façon dont il faut mesurer la sûreté de fonctionnement et sur la façon dont il sera décidé que les objectifs de sûreté de fonctionnement ont été atteints.

6.3 Gestion des risques

Il convient d'identifier les risques en prenant en compte les incapacités potentielles à satisfaire aux exigences, ainsi que les opportunités d'améliorer les performances. Il est nécessaire de tenir compte des risques menaçant la sûreté de fonctionnement et les objectifs fonctionnels et non fonctionnels, comme ceux relatifs à la sécurité ou à l'environnement, et des compromis pourraient être exigés.

L'incapacité à satisfaire aux exigences et aux objectifs peut résulter

- de défaillances d'une unité ou au sein d'une entité. Ces défaillances peuvent être identifiées par des références à des données historiques et à des méthodes, notamment l'analyse de cause première de défaillance, ou par des procédures comme l'analyse AAP ou AMDE,
- de défaillances du soutien apporté à l'entité, comme la maintenance ou la logistique de maintenance, et
- de modifications des exigences, des hypothèses et des circonstances externes au système de sûreté de fonctionnement et parfois externes à l'organisme.

Dans toute la mesure du possible et si cela est rentable, il convient de prévenir ou de réduire les conséquences négatives. Il convient de prendre des dispositions pour surveiller les circonstances externes représentant une menace pour la sûreté de fonctionnement, de façon à être rapidement averti des changements. Lors de la définition des exigences et des activités et des plans permettant de les satisfaire, il convient de prendre en compte la nécessité pour une entité d'être capable de se récupérer et de s'adapter aux risques.

6.4 Mise en œuvre des activités de sûreté de fonctionnement tout au long du cycle de vie

Les activités de sûreté de fonctionnement se produisent tout au long du cycle de vie d'une entité et sont normalement intégrées aux processus d'ingénierie à toutes les phases du cycle de vie, même lorsque les différentes phases du cycle de vie se chevauchent. Les transitions entre les phases du cycle de vie impliquent souvent différentes ressources techniques, divers systèmes d'activation et critères de soutien.

Les activités exigées pour chaque phase du cycle de vie peuvent être différentes. Pour une efficacité maximale, il convient d'organiser et de gérer les activités de sûreté de fonctionnement comme faisant partie de l'ingénierie ou d'autres programmes ou projets.

L'Annexe B décrit les activités de sûreté de fonctionnement au cours d'un cycle de vie générique; il convient de reconnaître que les phases du cycle de vie peuvent être plus simples ou plus complexes selon les circonstances particulières.

6.5 Sélection des outils et des activités techniques de sûreté de fonctionnement

Il existe une large gamme d'activités et d'outils techniques permettant de faciliter la réalisation des objectifs de gestion de la sûreté de fonctionnement, comme l'analyse et les essais de fiabilité, la logistique de maintenance et la gestion du soutien logistique, les services d'assistance à la clientèle, l'analyse des défaillances et les systèmes d'action corrective. Les outils de sûreté de fonctionnement varient suivant les phases du cycle de vie.

Par exemple, à la phase de conception et de développement, des techniques comme HAZOP, AMDE ou AAP peuvent être appliquées. Ces techniques ont pour but d'identifier et de prévenir les pannes, les défaillances ou les événements non désirés avant de les observer en fonctionnement réel.

Lors de la mise en œuvre et de l'utilisation, il convient que l'amélioration de la fiabilité réalisée au moyen d'un programme de croissance fasse partie d'une activité globale de fiabilité dans le développement d'une entité, particulièrement pour une conception qui utilise des techniques, des composants nouveaux ou non éprouvés, ou un contenu important de logiciel. Dans un tel cas, le programme peut présenter, pendant un intervalle de temps donné, de nombreux types de défauts dont les causes sont relatives à la conception. La croissance de la fiabilité est obtenue en acquérant des connaissances sur les déficiences de la conception au moyen d'essais et d'actions permettant d'éliminer ou d'atténuer les effets de ces déficiences. Différents modèles statistiques peuvent être utilisés pour développer une courbe de croissance planifiée qui fixe des objectifs de fiabilité intermédiaires réalistes à atteindre au cours des essais et qui indique que les progrès réalisés sont suffisants pour atteindre l'objectif final ou l'exigence finale.

L'analyse de cause première est un autre outil de sûreté de fonctionnement qui correspond à tout processus systématique permettant d'identifier les causes d'une panne, d'une défaillance ou d'un événement non désiré observé en fonctionnement ou pendant les essais, avec l'objectif de prévenir des défaillances similaires ou connexes. Cette analyse est effectuée en admettant que les défaillances se résolvent mieux en éliminant les causes premières plutôt qu'en traitant le symptôme immédiatement détecté. Elle est généralement appliquée en réponse à une défaillance répétée ou à une défaillance ayant des conséquences significatives.

L'Annexe D présente la structure des normes de sûreté de fonctionnement pour soutenir la gestion de la sûreté de fonctionnement et guider l'application des méthodes et des outils. Le site web [2] de l'IEC/TC56 fournit des informations sur les normes spécifiques et actuelles relatives à la sûreté de fonctionnement, afin de faciliter les applications de sûreté de fonctionnement.

6.6 Ressources

Les ressources qui permettent de réaliser la sûreté de fonctionnement d'une entité comprennent

- une personne en charge de la sûreté de fonctionnement d'une entité, soit comme responsabilité principale, soit comme responsabilité intégrée à un autre rôle,
- l'expertise permettant de mener les activités et les analyses techniques appropriées,
- un système de gestion d'informations, comme une base de données des connaissances sur la sûreté de fonctionnement (soit autonome, soit intégrée à un système de soutien logistique), et
- un logiciel approprié d'analyse de la sûreté de fonctionnement.

Les ressources nécessaires peuvent varier suivant les phases du cycle de vie. Par exemple, la phase de conception et de développement exige une expertise relative à la sûreté de fonctionnement de la conception et l'utilisation de techniques d'analyse de la sûreté de fonctionnement, qui elles-mêmes exigent souvent des programmes logiciels et des données de sûreté de fonctionnement. La phase de réalisation peut impliquer des ressources destinées aux essais détaillés. Lors de l'utilisation d'une entité, des ressources pourraient être nécessaires pour collecter et évaluer les données et la performance des activités de maintenance et de soutien.

6.7 Mesure et évaluation

Le processus de mesure implique:

- l'identification du type et des objectifs de mesure des attributs de sûreté de fonctionnement qui sont nécessaires pour des exigences contractuelles et opérationnelles ou pour des conditions spécifiques, comme l'évaluation de produit;
- la détermination des données pertinentes et de la nature des sources de données pour les mesures;
- l'utilisation de systèmes efficaces permettant de faciliter le processus de mesure, tels que la mise en place de systèmes de collecte de données, les rapports des défaillances, les systèmes d'analyse et d'actions correctives, les questionnaires d'enquête ou d'autres projet de soutien;
- l'interprétation des résultats de mesure afin d'établir des tendances de performance, d'identifier les questions critiques et de recommander des actions de gestion avec la logique et justification;
- la documentation des résultats issus des mesures pour la conservation des rapports, les audits qualité et les preuves tangibles.

La sûreté de fonctionnement est évaluée de différentes façons, selon la phase du cycle de vie:

- prévue lors de la phase de conception en utilisant une évaluation probabiliste et des méthodes de modélisation;
- estimée lors de la phase de réalisation, par exemple au moyen d'essais accélérés de fiabilité et de durabilité;
- mesurée et analysée lors de la phase d'utilisation à l'aide de méthodes statistiques ou d'autres méthodes.

La caractéristique de sûreté de fonctionnement qui est mesurée dépend si on regarde la perspective de l'utilisateur ou de l'organisation, ainsi que des exigences de performance applicables. Par exemple, dans le cas d'un service de transports, l'utilisateur (le passager) sera concerné par l'accessibilité du service (disponibilité de l'espace et respect de l'horaire affiché), la sûreté de fonctionnement du service (arrivée à l'heure) et l'intégrité (places assises et installations convenablement entretenues). D'un point de vue organisationnel, la

sûreté de fonctionnement peut également être évaluée par une mesure de l'efficacité, telle que la satisfaction du client, la fiabilité du service et les coûts de maintenance.

Les caractéristiques qui constituent la sûreté de fonctionnement peuvent être mesurées soit qualitativement, soit quantitativement. L'évaluation qualitative peut être effectuée de façon descriptive ou à l'aide de méthodes de classement.

Des exemples de méthodes qualitatives sont les suivants:

- Une évaluation par un expert qui donne des explications sur l'entité et qui attribue une note (par exemple 5 "étoiles"). Dans certains cas, les attributs sont pondérés afin d'incorporer des niveaux d'importance avant d'attribuer une note globale. En comparant les différentes notes attribuées par les experts, une évaluation objective peut être réalisée. Il convient d'être prudent si l'on rend des jugements sur la base de notes attribuées par un seul expert.
- Une évaluation obtenue auprès du public qui fournit une note individuelle et des justifications associées pour une entité particulière. Ces notes sont cumulées dans une base de données pour établir un classement global de l'entité comparée à d'autres entités similaires.
- Dans de tels cas, il est nécessaire de comprendre la méthode de classement, ainsi que les partis pris potentiels des individus attribuant la note avant que la justesse du classement puisse être reconnue.

Une valeur quantitative des performances de sûreté de fonctionnement est déduite des données observées ou estimées. Les caractéristiques de sûreté de fonctionnement peuvent être quantifiées de différentes façons, telles que les mesures instantanées et opérationnelles de disponibilité ou de fiabilité déduites de mesures directes et indirectes des entités réalisées au cours des essais, en fonctionnement ou en maintenance. Par exemple, ces caractéristiques peuvent être mesurées en durée des défaillances, en durée de fonctionnement avant la première défaillance, en durée des temps de disponibilité et d'indisponibilité, et en efforts consacrés aux activités de maintenance.

Dans la mesure où la vérification d'un niveau élevé de fiabilité ou de disponibilité au moyen d'essais est difficile et chronophage, même au moyen d'essais accélérés, la fiabilité de l'entité pourrait avoir besoin d'être vérifiée au moyen de méthodes d'analyse. S'il n'est pas possible de tester la totalité de l'entité, des tests peuvent être réalisés au niveau du composant et du module. Cependant, la mesure finale des performances de l'entité n'est normalement pas réalisable avant que l'entité soit en service.

Il convient de prévoir ou de mesurer les paramètres de sûreté de fonctionnement d'une entité dans des conditions définies de contrainte comme l'exposition à différentes conditions environnementales qui se produiront pendant utilisation. Certaines conditions de contraintes environnementales naturelles typiques sont les températures de fonctionnement et de stockage, l'humidité et la charge solaire. Les règles culturelles, organisationnelles ou politiques et l'implication humaine peuvent aussi influencer la sûreté de fonctionnement.

6.8 Assurance de la sûreté de fonctionnement

L'assurance est le processus permettant d'assurer la conformité de l'entité aux exigences et aux normes définies. L'assurance fournit les justifications permettant d'avoir une confiance légitime dans le fait que les performances relatives à la sûreté de fonctionnement ont été réalisées, le sont ou le seront. L'objectif de l'assurance est de gagner la confiance des parties prenantes sur le fait que la sûreté de fonctionnement de l'entité peut être obtenue. Il existe des approches génériques permettant d'assurer la sûreté de fonctionnement de l'entité et qui ont différents objectifs et différents degrés de rigueur dans la conception. En pratique, une combinaison de ces trois approches est susceptible d'être utilisée.

a) L'assurance de la sûreté de fonctionnement est démontrée par l'utilisation réelle de l'entité dans un environnement d'application pendant un intervalle de temps programmé.

Cela peut impliquer une démonstration formelle ou la réalisation réelle pendant la période couverte par la garantie ou la période de fonctionnement.

b) La sûreté de fonctionnement est déduite en appliquant des méthodes statistiques aux données de la sûreté de fonctionnement des entités constitutives.

c) La preuve de la mise en œuvre correcte des activités et des outils exigés de sûreté de fonctionnement est fournie.

L'utilisation d'un dossier de sûreté de fonctionnement fournit un moyen de s'assurer progressivement que les exigences de sûreté de fonctionnement sont ou seront satisfaites tout au long du cycle de vie de l'entité. Le cadre permettant d'établir un dossier de sûreté de fonctionnement pour l'assurance comprend

- une argumentation rationnelle auditable supportant l'affirmation selon laquelle une entité définie satisfait aux exigences de sûreté de fonctionnement,
- un résumé des preuves et argumentations venant à l'appui des revendications de réalisation de la sûreté de fonctionnement, et
- l'assurance progressive tout au long du cycle de vie de l'entité en tant que partie de l'évaluation.

Le dossier de sûreté de fonctionnement fournit un point focal permettant de déterminer les incertitudes et les risques relatifs à la gestion. Ainsi, l'assurance est devenue un facteur clé des activités du cycle de vie qui prévoient, conçoivent, réalisent, démontrent, soutiennent et surveillent les performances en service liées à la sûreté de fonctionnement.

Dans toute la mesure du possible, il convient d'utiliser les systèmes existants de surveillance des performances pour générer les informations nécessaires à l'amélioration des activités et des résultats de sûreté de fonctionnement.

Les exemples typiques comprennent

- un système de compte-rendu des défaillances, d'analyse et d'action corrective (FRACAS),
- un système d'assistance à la clientèle et de retour d'information,
- un système de logistique de maintenance et de soutien logistique,
- un système de compte-rendu des incidents et de gestion des pannes,
- un système de surveillance de la santé, et
- un système de management de la qualité.

6.9 Revue des résultats et des activités de sûreté de fonctionnement

Il convient que les résultats et les activités de sûreté de fonctionnement fassent l'objet d'une revue tout au long du cycle de vie. Le but des revues de sûreté de fonctionnement est d'assurer que les objectifs spécifiques provenant de perspectives techniques et commerciales sont satisfaits tout au long du cycle de vie. Les revues fournissent des retours d'information sur les déficiences et les écarts de sûreté de fonctionnement observés lors d'une phase du cycle de vie en vue de leur correction et de leur réduction lors des autres phases, ainsi que pour améliorer le processus de gestion de la sûreté de fonctionnement. Il convient que les revues prennent en compte à la fois les activités et les résultats et qu'elles définissent une conduite d'un point de vue technique, afin d'atteindre les objectifs et de gérer les risques, par exemple, à des points de conception critiques afin d'éviter la propagation d'erreurs et de décisions inadaptées en matière de conception.

Les revues de sûreté de fonctionnement sont effectuées conjointement à d'autres revues de direction dont le domaine d'application est plus vaste, afin de faire face aux enjeux de gestion de la sûreté de fonctionnement comme ceux associés aux politiques, à l'administration, au fonctionnement ou au service client de l'organisme. Par exemple, il convient de renforcer les revues de direction de projet afin d'inclure les aspects de sûreté de fonctionnement.

Il convient que les responsables de la sûreté de fonctionnement participent à plusieurs titres aux réunions de revue et qu'ils contribuent en conséquence aux enjeux relatifs à la sûreté de fonctionnement dont les impacts exigent l'attention de la direction et des actions de suivi. L'Annexe E montre un exemple représentatif de liste de contrôle de revue de sûreté de fonctionnement. Cette liste de contrôle est destinée à appuyer la revue de sûreté de fonctionnement au moment des prises de décision majeures du cycle de vie. La liste de contrôle peut être utilisée par le fournisseur et le client à des fins d'adaptation afin de satisfaire aux besoins spécifiques de l'application concernée.

La liste de contrôle est alignée sur le cycle de vie, comme le montre l'Annexe B.

Les revues couvrent une grande variété d'activités de revue au cours du cycle de vie d'une entité. Il convient que les revues typiques menées à différents niveaux de gestion puissent inclure des composants de sûreté de fonctionnement:

- une revue des opérations destinée à déterminer l'état de santé et de fonctionnement d'un organisme, d'une subdivision, d'un site de production ou d'une infrastructure de service;
- une revue de projet destinée à déterminer l'état d'avancement du travail, le calendrier du projet et les engagements aux étapes importantes, la disponibilité des ressources, les besoins en externalisation, la coordination des fournisseurs et l'identification des problèmes exigeant des actions de la part de la direction;
- une revue technique destinée à évaluer l'application d'une nouvelle technologie, la diversification de la gamme de produits, les décisions «développer ou acheter», et le calendrier du lancement de nouveaux produits;
- une revue de conception destinée à évaluer les réalisations de développement technique, les évaluations de sûreté de fonctionnement, les faiblesses de conception à améliorer, la qualification de produit, l'aptitude à la fabrication, la conception fonctionnelle, l'exploitabilité dans l'environnement de l'application et les besoins en logistique de service, et l'approbation de la conception finale, avant la mise à disposition pour la production;
- une revue des composants destinée à vérifier les conditions de fonctionnement des composants et des COTS par rapport aux fiches techniques et aux résultats des essais et par rapport à des exigences particulières d'utilisation, de manipulation et de processus d'assemblage;
- une revue de production destinée à déterminer les exigences de ressource et les calendriers de livraison, la capacité de production et le flux, l'externalisation et la sous-traitance de tâches de production, l'outillage, l'assemblage, le contrôle du matériel et les activités d'essai;
- une revue des risques destinée à déterminer si les risques ont changé et si le processus de gestion des risques est efficace;
- une revue de service destinée à déterminer les besoins en service de la clientèle, les activités de maintenance programmées et non programmées, l'apport de services par des tiers, le soutien logistique, les coûts de possession du stock et l'emplacement des entrepôts;
- une revue de satisfaction du client destinée à répondre aux préoccupations des utilisateurs et à élaborer des stratégies d'amélioration;
- une revue de fournisseur destinée à vérifier la qualité des fournitures, les engagements de délai de livraison, l'efficacité du processus de commande, l'approvisionnement multiple en fournitures et la gestion de la chaîne d'approvisionnement;
- une revue de qualité destinée à déterminer l'état de non-conformité, l'efficacité de l'assurance et les tendances de performance de la qualité, à identifier les domaines d'amélioration et à préconiser des actions de gestion;
- une revue de vérification et de validation afin de s'assurer de la réalisation de processus de vérification et de validation appropriés;

- une revue de lancement de produit mettant à disposition le produit pour la livraison et/ou l'acceptation du client;
- une revue des règlements destinée à déterminer si les règles applicables de santé, de sécurité et d'environnement ont été identifiées et sont correctement mises en œuvre.

Il faut que les composants de sûreté de fonctionnement de ces revues travaillent ensemble comme un ensemble unique. Chacune de ces revues implique généralement plusieurs phases et activités du cycle de vie et le retour d'informations d'une revue peut déclencher des activités qui affectent d'autres revues.

Toutes les revues font partie intégrante du processus d'assurance. Les revues de sûreté de fonctionnement garantissent que tous les enjeux critiques ont été évalués et résolus. Les enregistrements des revues peuvent être utilisés comme preuves tangibles destinées à venir à l'appui du processus d'assurance de la sûreté de fonctionnement dans une revue plus large des processus d'assurance.

Annexe A
(informative)

Dispositions organisationnelles d'un système de gestion de la sûreté de fonctionnement

A.1 Structures organisationnelles

Afin d'atteindre leurs objectifs de manière efficace, les organismes sont généralement structurés en entités ou en unités d'exploitation avec plusieurs niveaux hiérarchiques. Chacune de ces entités a pour responsabilité la gestion de certaines activités avec des ressources assignées pour accomplir leurs tâches. À moins que les objectifs ne soient très simples et faciles à atteindre, les activités sont normalement divisées en plusieurs groupes pour plus d'efficacité, sur la base de facteurs comme des ensembles communs de compétences ou des exigences d'emplacement physique. Au sein des groupes, des responsables gèrent les activités, avec souvent plusieurs niveaux hiérarchiques. Dans de nombreux organismes, la sûreté de fonctionnement est une exigence très importante qu'il est nécessaire de satisfaire et il convient que la structure organisationnelle adapte ces exigences spécifiques.

Certains organismes existent pendant un certain temps afin d'atteindre un objectif spécifique comme cela est souvent le cas par exemple pour le développement de produit, et la conception et la construction d'infrastructures. Dans d'autres cas, un organisme peut exister pendant un intervalle de temps plus long. Dans les deux situations, il sera nécessaire que les exigences de sûreté de fonctionnement soient adaptées à la structure organisationnelle.

Dans des organismes où l'activité ou la technologie change rapidement, de nouvelles structures organisationnelles apparaissent. On peut citer comme exemples typiques les nouveaux partenariats destinés à favoriser des réseaux de communications, des juridictions nationales et interrégionales dans le domaine des transports et de la distribution, et les services de fabrication spécialisés tout-en-un auxquels différents organismes collaborent en passant des accords pour travailler ensemble à l'échelle mondiale. Des infrastructures peuvent être établies, transportées et dupliquées dans presque n'importe quel pays où les ressources humaines, la sécurité et des règles équitables peuvent être établies et conservées. Certains organismes verticalement intégrés se sont aussi engagés dans une organisation matricielle et des structures organisationnelles participatives afin de conserver l'expertise pour le déploiement stratégique. Les organismes peuvent ensuite s'étendre au-delà de la gestion d'entreprise normalisée et inclure des collaborations avec le gouvernement, le secteur industriel et les institutions académiques ou des systèmes complexes pour lesquels aucune partie prenante ne comprend parfaitement le système.

A.2 Organisation des activités de sûreté de fonctionnement

Il existe différentes approches possibles de structuration d'un organisme permettant d'atteindre avec succès les objectifs de sûreté de fonctionnement. Dans la mesure où les exigences globales sont une combinaison des exigences fonctionnelles, non fonctionnelles et de sûreté de fonctionnement, elles réclament une coordination étroite des activités et il convient de les considérer comme un ensemble intégré d'activités au sein d'un organisme. De façon générale, il convient d'inclure les activités de sûreté de fonctionnement dans une structure organisationnelle correspondant à l'un des scénarii généraux suivants.

- Les activités de sûreté de fonctionnement sont entièrement intégrées à la structure organisationnelle, des ressources de sûreté de fonctionnement étant incluses dans une entité organisationnelle, par exemple, lorsque chaque employé est responsable des aspects de sûreté de fonctionnement de ses activités. Une ou plusieurs personnes sont souvent désignées pour faciliter ces activités.

- Les activités de sûreté de fonctionnement sont suffisamment chronophages et capitales qu'une ou plusieurs entités organisationnelles seront nécessaires pour mener les activités de sûreté de fonctionnement de façon adaptée à la conception, la construction et la mise en service d'une installation majeure. Ces entités continueront à travailler en étroite coordination avec les autres entités.
- Pour un grand organisme possédant plusieurs gammes de produits ou de nombreuses installations de grande taille à gérer, il peut être utile de mettre en place une entité organisationnelle majeure destinée à répondre aux besoins globaux de l'organisme de manière efficace. Cela peut éviter de dupliquer les efforts et cela garantit la cohérence des activités de sûreté de fonctionnement tout en rendant possible l'application du niveau d'expertise le plus élevé. Dans certains cas, les autorités de réglementation exigent une organisation séparée de sûreté de fonctionnement, par exemple l'homologation dans les domaines des télécommunications, des appareils médicaux et de l'industrie aérospatiale.
- Dans chacun de ces scénarii, des activités spécifiques peuvent être externalisées, soit parce qu'elles sont très spécialisées soit de courte durée.

Les facteurs clés qui contribuent au succès de la réalisation des exigences de sûreté de fonctionnement d'un point de vue organisationnel comprennent :

- la définition d'une responsabilité globale unique pour la satisfaction aux exigences de sûreté de fonctionnement et la coordination des responsabilités partagées entre les différentes entités organisationnelles qui sont impliquées,
- l'apport et la promotion de l'expertise et de la compétence des ressources de sûreté de fonctionnement pour permettre de mener à bien les activités,
- la gestion des informations associées à la sûreté de fonctionnement et aux exigences fonctionnelles correspondantes,
- la coordination entre les groupes internes et externes impliqués dans les activités de sûreté de fonctionnement, et
- l'intégration des exigences de sûreté de fonctionnement dans la prise de décisions et la compréhension complète des compromis qui peuvent être réalisés entre les exigences fonctionnelles et de sûreté de fonctionnement et les facteurs relatifs au projet comme le calendrier et les coûts.

Annexe B
(informative)

Activités d'un système de gestion de la sûreté de fonctionnement

B.1 Activités de sûreté de fonctionnement dans le cycle de vie

Différentes activités de sûreté de fonctionnement sont nécessaires à mesure que des entités sont créées ou acquises, utilisées ou exploitées, améliorées et enfin retirées ou mises au rebut. Cette série de phases identifiables est appelée cycle de vie et constitue la base des activités de sûreté de fonctionnement.

Pour les besoins de la présente annexe, un cycle de vie générique a été utilisé qu'il convient d'appliquer de façon générale à toutes les entités. Le déroulement de ces phases fait qu'elles se chevauchent souvent.

a) Concept

La phase de concept est la phase donnant une première vision de l'entité. Elle peut comprendre des activités servant à identifier les besoins du marché ou autres, à définir/identifier l'environnement opérationnel d'utilisation, le calendrier, les aspects humains, les exigences réglementaires (comme la traçabilité, la sécurité, l'environnement, la durabilité, la mise au rebut et l'élimination des déchets) et les autres contraintes. À partir de ces éléments, les exigences fonctionnelles et non fonctionnelles et les exigences préliminaires de sûreté de fonctionnement peuvent être définies et analysées et une conception réalisable ou des solutions achetées peuvent être identifiées à partir de spécifications techniques générales. C'est à cette étape qu'il convient d'identifier les besoins potentiels de compromis, par exemple entre la sécurité et la sûreté de fonctionnement. Des approches de modélisation et probabilistes peuvent être utilisées pour obtenir des prévisions de sûreté de fonctionnement de haut niveau afin de sélectionner l'architecture préliminaire et les politiques de maintenance et de supportabilité, susceptibles de satisfaire aux exigences réglementaires et de sûreté de fonctionnement. Il convient de centrer l'évaluation des risques au cours de la phase de concept sur la faisabilité de la conception et la sélection des technologies pour la mise en œuvre du projet. La sélection entre les différentes options de conception est basée sur les approches des meilleures pratiques d'ingénierie permettant de satisfaire aux exigences et de gérer les risques en respectant les contraintes imposées.

b) Développement

La phase de développement fait suite à la celle du concept initial, une fois que sa faisabilité a été vérifiée. Le but est de planifier et de réaliser les solutions de conception d'ingénierie sélectionnées pour la réalisation des fonctions de l'entité. Cette étape se traduit par un effort approprié consacré à la conception et au développement comprenant la conception de l'architecture système, l'ingénierie de modélisation, la construction de prototypes et les essais. Les interfaces entre les éléments du système et du sous-système sont identifiées et une évaluation systématique des fonctions des entités intégrées et des interactions avec des milieux externes est menée pour valider la configuration finale. Les risques associés à la conception sélectionnée sont évalués plus en détail et les traitements sont spécifiés. Il convient que la planification de l'accès à la maintenance pour la supportabilité, les procédures opérationnelles et l'assurance, ainsi que les processus de soutien soient bien établis avant la réalisation de l'entité. Les approches de modélisation et probabilistes pertinentes peuvent être utilisées au cours de cette phase afin d'obtenir des prévisions détaillées de sûreté de fonctionnement, ce qui permet de consolider l'architecture et les politiques de maintenance et de supportabilité sélectionnées lors de la phase de conception et de vérifier que les exigences réglementaires et de sûreté de fonctionnement sont susceptibles d'être satisfaites.

c) Réalisation

La phase de réalisation met en œuvre les décisions «développer ou acheter» pour l'acquisition, et/ou la fabrication de l'entité finale et de ses composants. Les efforts de réalisation portent sur des activités telles que le développement technologique, l'outillage, la fabrication, le conditionnement et l'approvisionnement en fournitures de manière à assurer la transformation complète depuis la conception jusqu'à l'entité spécifiée ou les composants de ses sous-systèmes. Les entités ou les composants réalisés peuvent comprendre la combinaison de fonctions matérielles et logicielles. La réalisation comprend des simulations de composant et de module, des analyses et des essais, notamment des essais d'intégration, ainsi que des activités comme l'assemblage de composants, l'intégration des fonctions de l'entité, la vérification des sous-systèmes et l'installation de l'entité. Il convient d'établir les procédures de réception en collaboration avec le client, et d'inclure éventuellement des essais dans l'environnement d'exploitation réel avant la mise en service. Il convient que la validation fasse partie intégrante de l'essai afin de fournir les preuves tangibles de la conformité aux spécifications.

d) Utilisation

La phase d'utilisation correspond à la mise en place de l'entité pour délivrer la fonctionnalité ou le service avec le support des moyens de maintenance pour sa capacité opérationnelle. Les activités de processus incluent l'exploitation et le maintien de l'entité conformément aux exigences de performance, la formation des opérateurs et des spécialistes de la maintenance afin de pérenniser les compétences, l'interface client destinée à établir une relation de service, et le compte-rendu sur l'état de performance de l'entité et les rapports des incidents de type défaillance afin de déclencher les actions correctives et préventives au moment opportun. Il convient de contrôler et de vérifier les performances de l'entité de manière régulière afin de s'assurer du respect des objectifs en matière de sûreté de fonctionnement, de réglementation et de qualité de service. La collecte et l'échantillonnage de données peuvent être utilisés pour estimer la sûreté de fonctionnement du service. L'appréciation des risques en service et pendant les activités de maintenance peut traiter les problèmes qui surgissent à cause des conditions changeantes.

e) Amélioration

La phase d'amélioration peut être nécessaire pour améliorer les performances de l'entité par l'ajout de fonctionnalités afin de satisfaire aux demandes croissantes des utilisateurs, d'allonger la durée de vie d'exploitation ou de corriger l'obsolescence. Les activités de processus peuvent inclure les mises à jour ou les ajouts de matériel ou de logiciel, des améliorations de maintenance, la simplification des procédures afin d'améliorer l'efficacité opérationnelle ou la gestion de l'obsolescence. Au cours de cette phase, les approches de modélisation et probabilistes peuvent être utilisées afin d'évaluer l'impact des améliorations possibles et de sélectionner les meilleures solutions. L'appréciation des risques au cours de la phase d'amélioration évalue souvent les coûts par rapport aux bénéfices et le retour sur investissement.

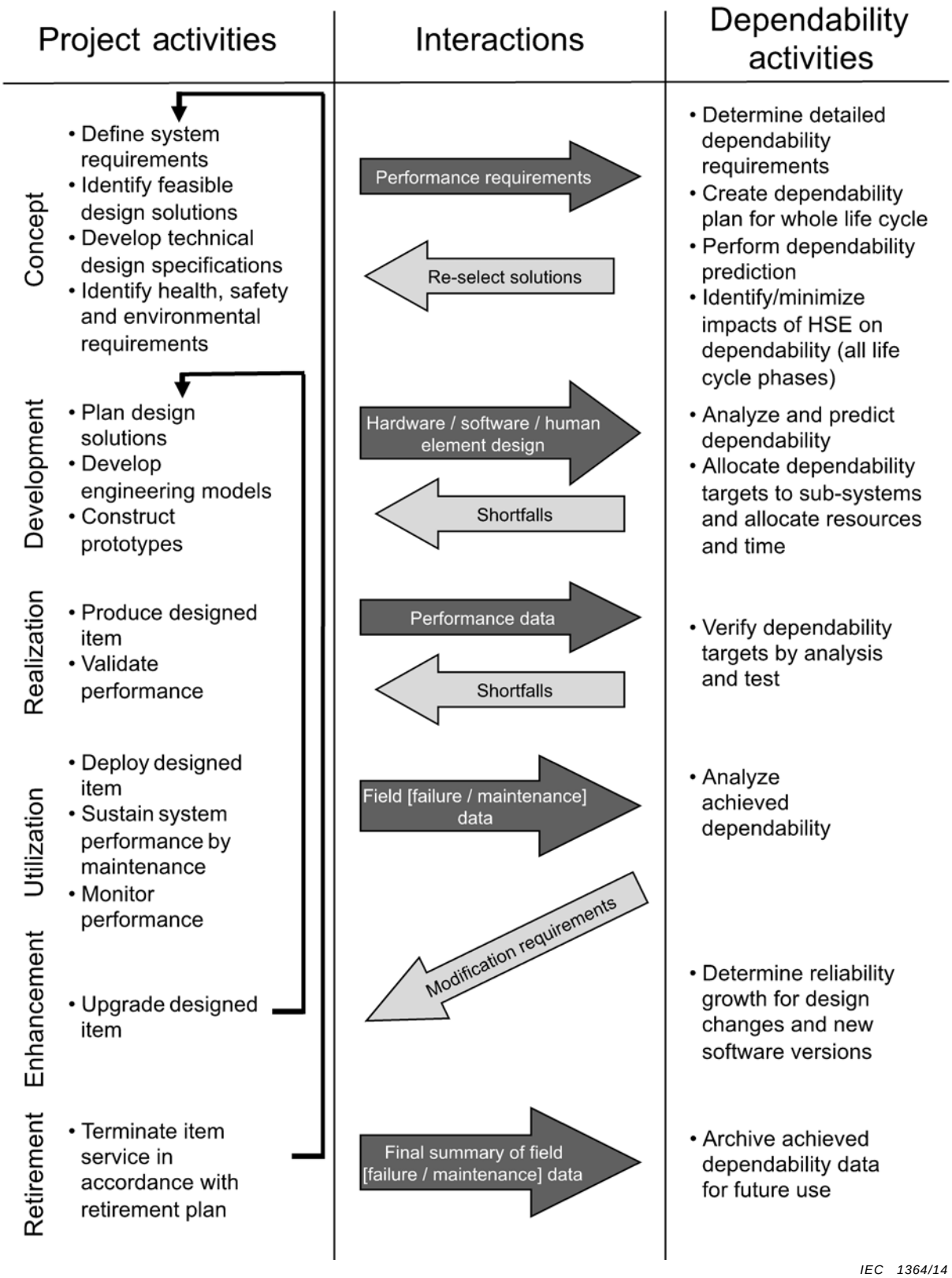
f) Mise au rebut

La phase de mise au rebut a lieu à la fin de la vie de l'entité. Au terme du service d'une entité, elle peut être démontée, réinstallée pour d'autres utilisations, détruite pour réutilisation des matériaux et des composants ou, dans certains cas, abandonnée sur place (par exemple un gazoduc). Il convient de prendre cela en compte dès la phase de conception. Pour les entités complexes, une stratégie de mise hors service pourrait être établie afin de formaliser le calendrier et la mise en œuvre du processus de mise hors service, de manière à satisfaire aux exigences réglementaires. Pour d'autres entités, des dispositions réglementaires peuvent exister concernant la reprise et la réutilisation ou la destruction.

Les activités de sûreté de fonctionnement sont souvent observées dans le contexte du cycle de vie, comme illustré à la Figure B.1.

Les variations de ces phases génériques d'un cycle de vie peuvent générer des phases plus spécifiques, comme:

- produit: concept et définition; conception et développement; construction et mise en service; exploitation et maintenance; rénovation à mi-vie ou prolongation de la durée de vie et mise hors service et destruction;
- infrastructure: concept et définition; conception et développement; construction et mise en service; exploitation et maintenance; rénovation à mi-vie ou prolongation de la durée de vie et mise hors service et destruction;
- matériel: concept, conception, fabrication et construction, installation/mise en service, exploitation/maintenance, modification, élimination;
- logiciel: concept, développement, application, exploitation et maintenance, amélioration, mise au rebut.



Légende

Anglais	Français
Project activities	Activités du projet
Concept	Concept

Anglais	Français
Define system requirements	Définir les exigences système
Identify feasible design solutions	Identifier les solutions avec des conceptions faisables
Develop technical design specifications	Élaborer des spécifications techniques de conception
Identify health, safety and environmental requirements	Identifier les exigences relatives à la santé, la sécurité et l'environnement
Development	Développement
Plan design solutions	Planifier les solutions de conception
Develop engineering models	Élaborer les modèles technologiques
Construct prototypes	Construire les prototypes
Realization	Réalisation/mise en œuvre
Produce designed item	Produire l'entité conçue
Validate performance	Valider les performances
Utilization	Utilisation
Deploy designed item	Mettre en place l'entité conçue
Sustain system performance by maintenance	Maintenir les performances système grâce à la maintenance
Monitor performance	Surveiller les performances
Enhancement	Amélioration
Upgrade designed item	Mettre à jour l'entité conçue
Retirement	Mise au rebut
Terminate item service in accordance with retirement plan	Mettre fin au service d'une entité, conformément au plan de mise au rebut
Interactions	Interactions
Performance requirements	Exigences de performances
Re-select solutions	Resélectionner les solutions
Hardware/software/human element design	Conception d'un élément matériel/logiciel/humain
Shortfalls	Déficiences
Performance data	Données relatives aux performances
Field [failure / maintenance] data	Données d'exploitation [défaillance / maintenance]
Modification requirements	Exigences de modification
Final summary of field (failure/maintenance) data	Résumé final des données d'exploitation [défaillance / maintenance]
Dependability activities	Activités de sûreté de fonctionnement
Determine detailed dependability requirements	Déterminer les exigences détaillées de sûreté de fonctionnement
Create dependability plan for whole life cycle	Concevoir un plan de sûreté de fonctionnement pour tout le cycle de vie
Perform dependability prediction	Effectuer la prévision de sûreté de fonctionnement
Identify/minimize impacts of HSE on dependability (all life cycle phases)	Identifier/minimiser les impacts du HSE sur la sûreté de fonctionnement (toutes les phases du cycle de vie)
Analyze and predict dependability	Analyser et prévoir la sûreté de fonctionnement
Allocate dependability targets to sub-systems and allocate resources and time	Attribuer des objectifs de sûreté de fonctionnement aux sous-systèmes et attribuer des ressources et du temps
Verify dependability targets by analysis and test	Vérifier les objectifs de sûreté de fonctionnement au moyen d'une analyse et d'essais

Anglais	Français
Analyze achieved dependability	Analyser la sûreté de fonctionnement obtenue
Determine reliability growth for design changes and new software versions	Déterminer la croissance de fiabilité pour les modifications de conception et les nouvelles versions logicielles
Archive achieved dependability data for future use	Archiver les données relatives à la sûreté de fonctionnement obtenue pour une utilisation ultérieure

Figure B.1 – Activités de sûreté de fonctionnement et cycle de vie

B.2 Activités de sûreté de fonctionnement au cours du cycle de vie

Les tableaux suivants donnent des exemples typiques d'activités ayant un impact sur les objectifs de sûreté de fonctionnement qui peuvent faire partie d'un cycle de vie. Cette liste n'est pas exhaustive et il convient de la modifier ou de l'adapter aux exigences spécifiques.

Tableau B.1 – Activités au cours de la phase de conception

Objectifs de sûreté de fonctionnement	Stratégies de sûreté de fonctionnement	Activités avec un impact sur la sûreté de fonctionnement
1. Définir les exigences de l'entité	a. Identifier les besoins du marché ou d'autres débouchés	• Mener des enquêtes de marché ou autres et des recherches pour évaluer les besoins des clients/utilisateurs • Identifier les exigences réglementaires relatives aux nouvelles initiatives • Déterminer le levier concurrentiel sur les valeurs de sûreté de fonctionnement • Identifier le domaine d'application du marché ou les autres besoins et évaluer les risques liés aux nouvelles initiatives • Déterminer le contexte
	b. Établir les politiques de sûreté de fonctionnement et les incitations pour la mise en œuvre	• Déterminer le moment pour l'initialisation d'un nouveau projet et définir les objectifs d'innovation • Formuler des plans stratégiques pour des tactiques de développement et d'acquisition de nouvelles entités • Rationaliser l'engagement des ressources pour soutenir les nouvelles initiatives et les portefeuilles de programmes en cours • Planifier les objectifs de réalisation • Définir les critères d'adaptation du projet • Documenter la déclaration des politiques et des missions • Déterminer des outils et des procédures de développement

Objectifs de sûreté de fonctionnement	Stratégies de sûreté de fonctionnement	Activités avec un impact sur la sûreté de fonctionnement
2. Analyser les exigences de performances de l'entité	a. Identifier les approches techniques et la faisabilité de la réalisation de l'entité	• Mener une analyse des exigences • Déterminer les limites de l'entité, ses fonctions d'exploitation et ses caractéristiques de performance en fonction de l'ensemble des exigences définies de performance • Obtenir les évaluations probabilistes afin de trouver des solutions réalisables et définir les architectures préliminaires • Identifier la capacité de l'organisme à entreprendre le projet • Identifier les risques • Évaluer les compromis qui peuvent être exigés entre les exigences fonctionnelles et celles de sûreté de fonctionnement • Déterminer les exigences de ressource et évaluer le plan d'attribution pour l'adaptation spécifique du projet. • Déterminer les mesures techniques et qualitatives pour les lignes directrices relatives à la conception et pour permettre les évaluations de sûreté de fonctionnement
	b. Identifier le partenariat potentiel et les exigences du fournisseur	• Déterminer la faisabilité de la chaîne d'approvisionnement et de la collaboration avec d'autres entreprises • Déterminer les exigences d'externalisation

Objectifs de sûreté de fonctionnement	Stratégies de sûreté de fonctionnement	Activités avec un impact sur la sûreté de fonctionnement
3. Établir des critères de conception de haut niveau	a. Identifier les options appropriées de conception d'architecture logique	• Établir la configuration de l'entité • Séparer les fonctions de l'entité • Sélectionner les technologies pour la conception et le choix du matériel/logiciel pour la réalisation des fonctions • Formuler les décisions de fabriquer ou d'acheter les fonctions de l'entité • Formuler des solutions pour satisfaire aux exigences de l'entité • Établir des moyens de vérification et d'intégration des fonctions de l'entité
	b. Établir des exigences de conception pour l'évaluation	• Formaliser le processus de conception et la façon dont les compromis seront gérés • Identifier la composition de conception des éléments matériel/logiciel pour chaque fonction • Incorporer des fonctions d'essai pour la vérification des performances • Définir les critères de conception pour les facteurs humains • Définir les critères de conception pour la sûreté de fonctionnement • Effectuer des prévisions de sûreté de fonctionnement • Définir les critères de conception pour l'environnement • Définir les critères de conception et d'interface ergonomiques • Définir les critères de conception de compatibilité électromagnétique • Définir les critères de conception de sécurité, de sûreté et de fiabilité • Établir les lignes directrices de conception matérielle • Établir les lignes directrices de conception logicielle • Simuler les performances des entités au niveau fonctionnel pour déterminer la stratégie de couverture des pannes et de restauration de l'entité • Vérifier les limites des performances, la robustesse et l'interopérabilité des fonctions de l'entité afin de satisfaire aux exigences de conception architecturale • Analyser et minimiser l'impact des exigences relatives à la santé, à la sécurité et à l'environnement et leurs effets potentiellement néfastes sur la sûreté de fonctionnement
	c. Documenter les spécifications de l'entité	• Incorporer les exigences de sûreté de fonctionnement dans les spécifications relatives à l'entité

Tableau B.2 – Activités au cours de la phase de développement

Objectifs de sûreté de fonctionnement	Stratégies de sûreté de fonctionnement	Activités avec un impact sur la sûreté de fonctionnement
1. Concevoir et développer l'entité	a. Initier la conception de l'entité	• Élaborer un programme de sûreté de fonctionnement pour l'entité • Élaborer un programme d'assurance qualité • Élaborer un plan de gestion de configuration et des procédures de modification de la conception • Obtenir des évaluations probabilistes afin d'évaluer les valeurs prévisionnelles de la sûreté de fonctionnement • Déterminer les exigences d'appréciation des risques • Etablir un plan d'essai et des critères d'acceptation pour l'entité • Établir un système de surveillance des entités, de programmes de diagnostic, de compte-rendu des incidents et de gestion des données • Établir des programmes de sûreté de fonctionnement pour les fournisseurs • Analyser et minimiser l'impact des exigences relatives à la santé, à la sécurité et à l'environnement et leurs effets potentiellement néfastes sur la sûreté de fonctionnement
	b. Initier le développement grandeur nature de l'entité	• Formaliser les exigences de sûreté de fonctionnement pour le système, les sous-systèmes et les fonctions • Mettre en œuvre un plan d'adaptation du projet • Obtenir des évaluations probabilistes afin de vérifier que les objectifs de sûreté de fonctionnement sont susceptibles d'être atteints • Développer un programme d'essai et de diagnostic logiciel • Déterminer des critères d'acceptation de sûreté de fonctionnement et des programmes de croissance de la fiabilité • Établir un programme de maintenance et de soutien logistique de l'entité • Mener des évaluations des risques • Surveiller et favoriser les efforts de d'externalisation matérielle et de sous-traitance externe • Développer un programme d'approvisionnement en pièces de rechange • Définir des conditions de garantie • Établir des programmes de formation

Tableau B.3 – Activités au cours de la phase de réalisation

Objectifs de sûreté de fonctionnement	Stratégies de sûreté de fonctionnement	Activités avec un impact sur la sûreté de fonctionnement
1. Réalisation de l'entité ou du module	a. Initier la production ou l'acquisition des sous-ensembles des fonctions du matériel	• Mettre en œuvre un programme de sûreté de fonctionnement pour l'entité • Mettre en œuvre un programme d'assurance de la qualité • Mettre en œuvre un système de compte-rendu des défaillances, d'analyse, de collecte des données et de retour d'information • Élaborer un plan de gestion de configuration et des procédures de modification de la conception • Définir un plan d'essai et des critères d'acceptation pour l'entité • Établir un système de surveillance des entités, de programmes de diagnostic, de compte-rendu des incidents et de gestion des données • Mettre en œuvre des programmes de sûreté de fonctionnement pour les fournisseurs
	b. Initier les fonctions du module logiciel et le développement de l'entité	• Mettre en œuvre un programme d'assurance de la fiabilité logicielle • Mettre en œuvre un programme d'essai et de diagnostic logiciel • Mettre en œuvre un plan de qualification et d'évaluation du module logiciel pour acceptation
2. Mise en œuvre de l'entité	a. Intégration de l'entité	• Exécuter le plan d'intégration • Coordonner les programmes d'externalisation et de soutien • Mettre en œuvre le plan de gestion de la configuration et les procédures de modification de conception • Préparer et effectuer l'analyse et les essais des composants et des modules • Préparer les plans pour l'analyse et les essais d'acceptation de l'entité et les exécuter • Effectuer les modifications exigées pour la croissance de la fiabilité • Préparer le plan d'acceptation de l'entité • Préparer les plans et les procédures de vérification et de validation
	b. Vérification/ validation de l'entité	• Mettre en œuvre le plan de vérification/validation • Documenter les résultats des essais de vérification/validation • Mener l'analyse des défaillances et recommander des actions préventives/correctives à des fins d'amélioration
	c. Installation et acceptation de l'entité	• Exécuter le plan d'installation • Documenter les enregistrements et les procédures d'installation • Mener l'acceptation de l'entité et générer le rapport d'acceptation • Mettre en œuvre des programmes de garantie le cas échéant • Établir des programmes partagés de supportabilité et de compte-rendu avec les spécialistes de la maintenance du client pour l'entité installée dans les locaux du client • Approbation du client pour l'acceptation de l'entité dans le but d'initier l'exploitation officielle de l'entité et l'application grandeur nature • Résoudre les questions de garantie avec les clients • Analyser et minimiser l'impact des exigences relatives à la santé, à la sécurité et à l'environnement et leurs effets potentiellement néfastes sur la sûreté de fonctionnement • Pour les produits de consommation, libération du produit selon une production en série, ainsi qu'une distribution et une vente intensives

Tableau B.4 – Activités au cours de la phase d'utilisation

Objectifs de sûreté de fonctionnement	Stratégies de sûreté de fonctionnement	Activités avec un impact sur la sûreté de fonctionnement
1. Exploitation et maintenance de l'entité	a. Mettre en œuvre la stratégie d'exploitation	• Surveiller les performances de l'entité • Mettre en œuvre le programme de croissance de la fiabilité • Mettre en œuvre le système de collecte des données d'exploitation pour obtenir des informations sur la sûreté de fonctionnement en exploitation • Mener une étude de satisfaction du client • Analyser et minimiser l'impact des exigences relatives à la santé, à la sécurité et à l'environnement et leurs effets potentiellement néfastes sur la sûreté de fonctionnement
	b. Mettre en œuvre la stratégie de supportabilité	• Proposer un service d'assistance à la clientèle • Surveiller les efforts de maintenance de l'entité • Analyser les tendances de défaillance et les enregistrements de service de maintenance • Recommander les modifications de conception ou de procédure pour une amélioration continue • Déterminer la qualité de service et fournir une plus-value au client

Tableau B.5 – Activités au cours de la phase d'amélioration

Objectifs de sûreté de fonctionnement	Stratégies de sûreté de fonctionnement	Activités avec un impact sur la sûreté de fonctionnement
1. Amélioration de l'entité	a. Mettre en œuvre une stratégie d'amélioration de l'entité	• Identifier les exigences de nouvelles fonctionnalités et d'amélioration • Évaluer la nécessité des modifications et les avantages qui en découlent • Mener des évaluations des risques et de la valeur • Analyser l'impact sur les exigences relatives à la santé, à la sécurité et à l'environnement • Mettre en œuvre les efforts d'amélioration • Évaluer l'impact sur les performances relatives à la sûreté de fonctionnement, comme la stabilité et la robustesse dues aux modifications comportant de nouvelles fonctionnalités • Mener une enquête de satisfaction client en prenant en compte les réactions aux modifications

Tableau B.6 – Activités au cours de la phase de mise au rebut

Objectifs de sûreté de fonctionnement	Stratégies de sûreté de fonctionnement	Activités avec un impact sur la sûreté de fonctionnement
1. Mise au rebut de l'entité	a. Mettre en œuvre la stratégie de mise au rebut de l'entité	• Exécuter le plan de mise au rebut/mise hors service de l'entité • Mettre en œuvre la réutilisation des composants, des données et des matériels des entités éliminées • Garantir la satisfaction aux exigences relatives à la santé, à la sécurité et à l'environnement • Appliquer le traitement des déchets pour les articles non recyclables/réutilisables • Notifier la fin du service aux clients • Fournir des informations sur la prestation d'un nouveau service ou d'un service alternatif • Mener une enquête de satisfaction client suite à la fin du service

Annexe C
(informative)

Définition des exigences pour une entité

C.1 Exigences du point de vue de l'application

Les exigences de sûreté de fonctionnement et les exigences fonctionnelles et non fonctionnelles définissent les exigences de performance de l'entité.

Les exigences de sûreté de fonctionnement font partie intégrante de l'ensemble des exigences et se rapportent à la façon dont les exigences fonctionnelles et non fonctionnelles peuvent être satisfaites du point de vue de la performance liée à la durée; la durée étant ici un terme général pour différentes mesures comme la durée calendaire, la durée de fonctionnement, le nombre de sollicitations et le nombre de cycles de fonctionnement.

La façon dont les exigences de performances sont établies et appliquées pour les différentes applications peut fortement varier.

Les exigences peuvent être déterminées en identifiant les besoins des parties prenantes tout en prenant en compte des aspects comme

- la connaissance d'entités similaires et les données de performances,
- la technologie pertinente et les limites d'application,
- les informations sur l'environnement de fonctionnement et le scénario d'usage,
- les normes établies et les spécifications pertinentes, et
- les expériences des utilisateurs et leurs réclamations.

Les exigences de sûreté de fonctionnement prennent en compte des aspects comme

- la durée prévue de fonctionnement ininterrompu,
- le taux de défaillance maximal acceptable en fonctionnement,
- la durée de fonctionnement avant la première défaillance ou avant l'usure,
- la disponibilité/efficacité minimale attendue de l'entité,
- la maintenabilité exigée,
- la capacité et la disponibilité des besoins en maintenance et en soutien,
- la durée de vie attendue de l'entité,
- les exigences de sécurité, et
- les contraintes de coûts.

Les exigences peuvent être déterminées à partir de cet ensemble d'éléments d'entrée et traduites en spécifications techniques qui comprendront des exigences qualitatives ou quantitatives des performances attendues.

Les exigences de performance et de sûreté de fonctionnement sont étroitement liées et il convient de ne pas les considérer comme des caractéristiques distinctes de performance. Il peut y avoir des compromis entre ces exigences pour obtenir une solution combinée. Par exemple, un niveau spécifié de sortie de puissance peut exiger des intervalles de maintenance plus réduits qui peuvent être inacceptables d'un point de vue opérationnel. Des contraintes de coûts influenceront à la fois les exigences de performance et de sûreté de fonctionnement.

Les deux exemples suivants illustrent la façon dont les exigences de performance et de sûreté de fonctionnement peuvent être définies pour les deux scénarii, ainsi que les méthodes qui peuvent être utilisées dans le programme de sûreté de fonctionnement pour cette entité: dans le premier cas, les exigences sont définies à la fois par le fournisseur et l'utilisateur et dans le second cas, les exigences sont définies principalement par le fournisseur sur la base de sa compréhension des attentes de l'utilisateur, mais sans éléments d'entrée apportés par l'utilisateur.

C.2 Exemples d'exigences de performance comprenant la sûreté de fonctionnement

C.2.1 Exigences déterminées par le fournisseur et l'utilisateur

Dans de nombreuses applications, notamment industrielles, les exigences de performance sont déterminées à la fois par le fournisseur et l'utilisateur. L'exemple donné ici est celui d'une pompe à huile à moteur dans un oléoduc, transportant du pétrole brut qui a été traité pour éliminer le gaz entraîné et les liquides plus légers, mais qui contient encore des contaminants. La fonction globale de la pompe est de fournir une capacité de pompage fiable, en toute sécurité et avec un impact environnemental minimal. Les contraintes en termes de conditions d'utilisation et d'environnement opérationnel sont celles d'un climat tropical avec des températures ambiantes normalement inférieures à 40 °C, mais avec une forte humidité. La maintenance exigée sera déterminée au moyen d'une approche basée sur le risque, comme la RCM qui comprendra à la fois des tâches de maintenance préventive et la surveillance des conditions.

L'exigence fonctionnelle primaire pour la pompe est de fournir un débit qui est défini par une charge spécifiée (augmentation de la pression) pour un certain débit avec une efficacité associée. La plage de fonctionnement prévue est comprise entre 80 % et 120 % du débit prévu par conception. Ces exigences fondamentales de performance sont déterminées à partir du processus des exigences de l'infrastructure de pompage et son emplacement dans l'oléoduc. Les exigences non fonctionnelles comprennent des dispositifs important de sécurité et d'environnement permettant de minimiser l'impact potentiel sur les employés et le public.

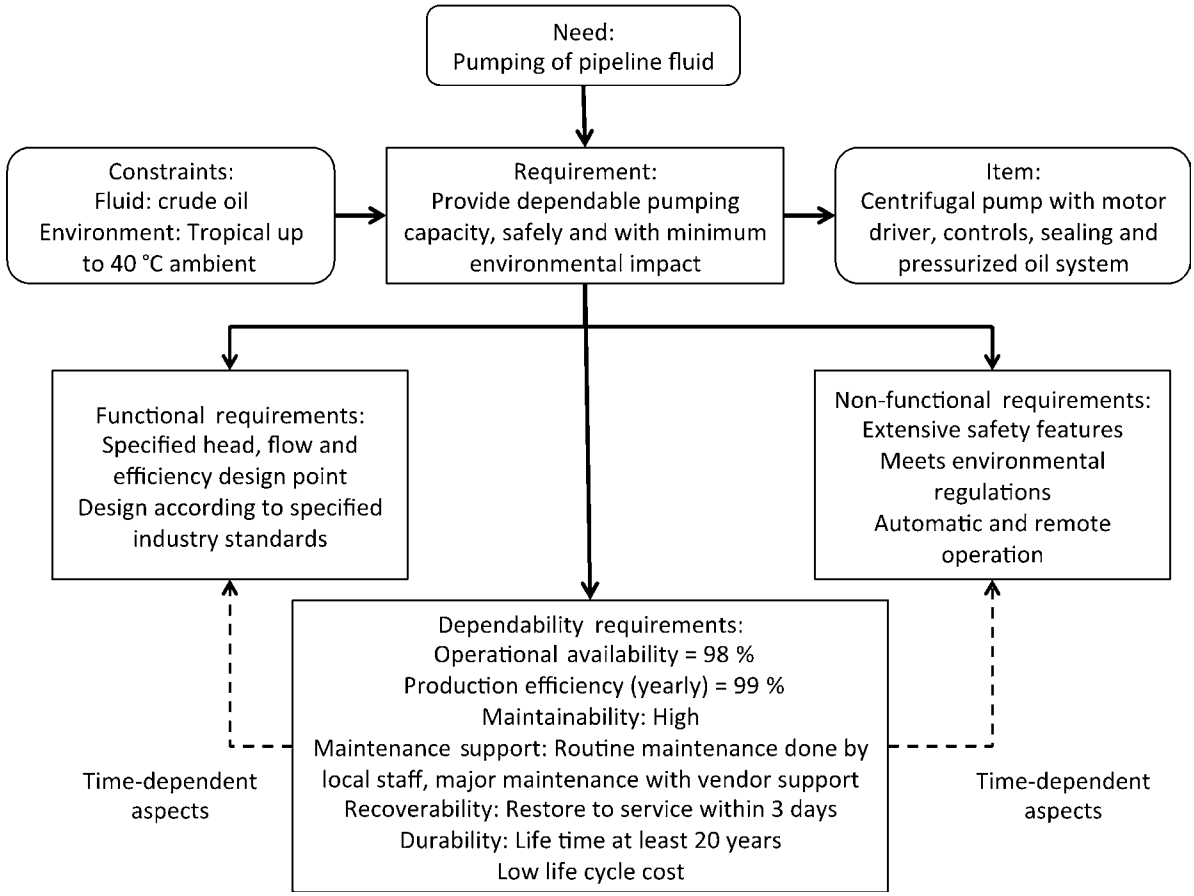
L'unité de pompage comprend un système de contrôle logiciel soutenu par instrumentation et par contrôle à distance depuis une infrastructure centralisée. Afin de minimiser l'impact environnemental, les joints mécaniques utilisent un tampon d'azote liquide. Une protection de sécurité est construite dans le système de contrôle avec des dispositifs de surveillance et de protection contre le feu. Plusieurs normes disponibles de conception sont respectées, notamment celles relatives aux pompes pétrolières, aux systèmes d'étanchéité et aux systèmes de protection des machines. Les enjeux de sécurité sont couverts par les normes de sécurité locales et nationales.

Dans ce cas, toutes les principales caractéristiques de sûreté de fonctionnement s'appliquent. On fixe un objectif de 99 % pour l'efficacité de la production (par exemple, la production prévue du système est une moyenne sur 1 an du débit prévu par conception) entre les activités annuelles de maintenance. Afin de prévoir si le niveau de fiabilité est atteignable, on produit un diagramme de fiabilité, constitué des principaux blocs du groupe électropompe. Les données sur la fiabilité de l'équipement ou des blocs individuels utilisant le MTBF sont obtenues à partir des bases de données de fiabilité du secteur et des estimations du fournisseur. Ces données sont comparées aux résultats pratiques issus de l'historique des activités réelles de maintenance sur des équipements similaires déjà en fonctionnement, à des fins de vérification et de validation.

Une disponibilité élevée est exigée en raison de la nature de l'oléoduc et le temps d'indisponibilité est à réduire avec une disponibilité d'exploitation de 98 % considérée comme atteignable en un intervalle de temps associé à un cycle majeur de travaux de maintenance. La disponibilité finale sur une période de 5 ans est estimée à partir des données de fiabilité et des enregistrements de maintenance, y compris une révision générale.

La maintenabilité et la durabilité sont d'autres caractéristiques de sûreté de fonctionnement. Restaurer rapidement une entité après une défaillance exige une maintenabilité élevée et une planification minutieuse de la supportabilité. Un temps d'indisponibilité dû à une défaillance majeure dure généralement 3 jours, ce qui exige que la pompe soit démontée. Pour la durabilité, une durée de vie minimale de 20 ans est nécessaire avec un coût de cycle de vie faible comparé à celui d'un équipement similaire. Une analyse des coûts du cycle de vie est effectuée sur la base du prix d'achat initial et du coût d'installation initial et les coûts d'exploitation et de maintenance anticipés dépendent aussi de la sélection d'une solution acceptable de soutien.

La Figure C.1 illustre la relation entre les exigences fonctionnelles et non fonctionnelles et de sûreté de fonctionnement.



Légende

Anglais	Français
Need: Pumping of pipeline fluid	Besoins: Pompage du fluide de l'oléoduc
Constraints: Fluid: crude oil Environment: Tropical up to 40 °C ambient	Contraintes: Fluide: pétrole brut Environnement: tropical jusqu'à une température ambiante de 40 °C
Requirement: Provide dependable pumping capacity, safety and with minimum environmental impact	Exigence: Fournir une capacité de pompage fiable, en toute sécurité et avec un impact minimal sur l'environnement
Item: Centrifugal pump with motor driver, controls, sealing and pressurized oil system	Entité: Pompe centrifuge à moteur, commandes, système d'étanchéité et de pétrole sous pression

Anglais	Français
Functional requirements: Specified head, flow and efficiency design point Design according to specified industry standards	Exigences fonctionnelles: Charge spécifiée, débit et point nominal d'efficacité Conception conforme aux normes industrielles spécifiées
Non-functional requirements: Extensive safety features Meets environmental regulations Automatic and remote operation	Exigences non fonctionnelles: Fonctionnalités complètes de sécurité Satisfaction aux règlements environnementaux Fonctionnement automatique et à distance
Dependability requirements: Operational availability = 98 % Production efficiency (yearly) = 99 % Maintainability: high Maintenance support: routine maintenance done by local staff, major maintenance with vendor support Recoverability: restore to service within 3 days Durability: life time at least 20 years Low life cycle cost	Exigences de sûreté de fonctionnement: Disponibilité d'exploitation = 98 % Efficacité de production (annuelle) = 99 % Maintenabilité: élevée Logistique de maintenance: maintenance de routine effectuée par le personnel local, gros travaux de maintenance avec soutien du fournisseur Récupérabilité: remise en service en 3 jours Durabilité: durée de vie minimale de 20 ans Coûts faibles du cycle de vie
Time-dependent aspects	Aspects liés au temps

NOTE Il s'agit uniquement d'un exemple illustratif permettant de clarifier les interdépendances entre ces concepts.

Figure C.1 – Exemple illustrant la relation entre les exigences fonctionnelles, non fonctionnelles et de sûreté de fonctionnement pour une pompe à moteur d'oléoduc

Le processus décisionnel pour les exigences de performance est fortement normalisé pour ce type de produit et d'application. Des techniques de prévision de la fiabilité et de la disponibilité pour les composants du groupe électropompe peuvent être utilisées par des fournisseurs individuels mais c'est moins commun pour le système final conditionné. Les coûts du cycle de vie sont estimés mais parfois ils n'incluent pas tous les coûts du cycle de vie. La durée de vie des composants peut être estimée à l'aide de l'analyse de Weibull. On peut estimer les coûts de maintenance préventive en les comparant à la maintenance après défaillance. Le coût de la perte de production en raison d'une indisponibilité non programmée est souvent bien plus élevé que le coût de la maintenance préventive. Les utilisateurs qui acquièrent une compréhension complète des exigences de sûreté de fonctionnement sont normalement plus à même de gérer la phase d'exploitation et de maintenance du cycle de vie.

C.2.2 Exigences déterminées uniquement par le fournisseur

L'achat d'une voiture familiale est un processus de décision collectif. Les coûts générés par la possession et l'exploitation d'une voiture représentent un objectif majeur, mais d'autres exigences de performance influencent le coût et le choix finaux d'un véhicule. Au sein d'une gamme de prix définie, un acheteur dispose de plusieurs options et le choix final n'est pas toujours fondé sur une évaluation rationnelle des exigences de performance et de sûreté de fonctionnement. Cependant, à l'exception de la flexibilité apportée au client par les options disponibles, les exigences fondamentales de performance sont fixées pour chaque véhicule.

Certaines propriétés de la voiture représentent de potentielles exigences essentielles pour le client. Les critères de sélection sont fondés sur la valeur de ces propriétés du point de vue du budget du client. Les conditions d'utilisation sont définies par l'environnement de conduite, comme le type de route, la température ambiante et les éventuelles conditions de pluie ou de neige.

Les propriétés fonctionnelles et non fonctionnelles souhaitables qui influencent le choix du client comprennent

- la taille et la capacité, le nombre et le type de passagers ainsi que d'autres exigences de volume,
- l'économie de carburant,

- la facilité à conduire et à se garer,
- la protection de sécurité comme la résistance à l'impact,
- la qualité de construction,
- le prix initial d'achat,
- les coûts d'exploitation et de maintenance, et
- les fonctionnalités optionnelles.

Les caractéristiques souhaitables de sûreté de fonctionnement sont principalement la fiabilité, la maintenabilité et la supportabilité. La disponibilité n'est généralement pas une préoccupation majeure tant que les services de logistique de maintenance sont situés à proximité de l'utilisateur, mais la durabilité peut être très importante si l'objectif est de conserver le véhicule pendant longtemps. Les exigences résultantes de sûreté de fonctionnement qui influencent le choix comprennent

- la fiabilité,
- la maintenabilité,
- la supportabilité
- l'emplacement et l'accessibilité des services de logistique de maintenance, et
- la durabilité.

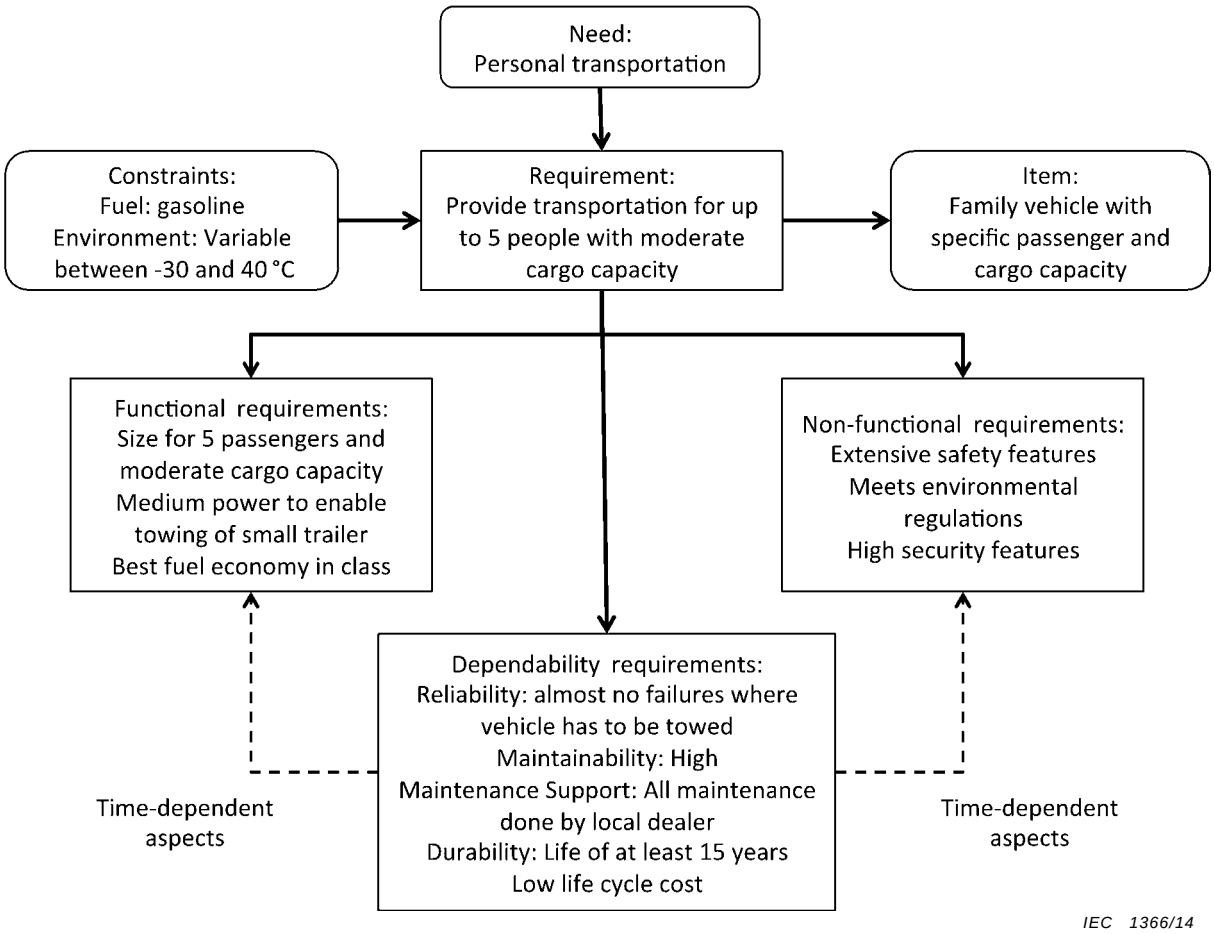
Ces propriétés représentent un ensemble d'exigences de performance propres au véhicule et prises en considération par l'utilisateur. Il existe des interdépendances entre les exigences de performance et de sûreté de fonctionnement, par exemple, la maintenabilité influence clairement les coûts de maintenance et la qualité de construction est liée à la durabilité. Il existe aussi des exigences qui sont contradictoires et pour lesquelles des compromis sont nécessaires. Par exemple, la qualité de construction, la fiabilité et la sécurité sont probablement liées, mais il est probable qu'elles soient en contradiction avec une exigence de faible prix d'achat initial.

L'objectif est de définir une priorité d'importance relative aux exigences pertinentes identifiées; cela peut être réalisé au moyen d'une matrice de décision.

Dans cet exemple, le client est confronté à un ensemble d'options qui satisfont aux exigences de performance à différents degrés, mais qui ne satisfont pas à toutes les exigences. Une méthode de prise de décision peut consister en une évaluation par le client de l'importance relative de ses exigences, puis l'attribution d'une note à chaque option selon le niveau de satisfaction à l'exigence. L'option finalement choisie est celle qui a la note pondérée totale la plus élevée.

Bien que les éléments d'entrée apportés par l'utilisateur individuel ne soient pas directement intégrés aux exigences de performance, les fabricants de véhicules personnels utilisent différents moyens comme les sondages auprès de la clientèle et le déploiement des fonctions qualité pour guider leur sélection des exigences de performance et leurs attentes pour le marché des utilisateurs cibles qu'ils visent.

La Figure C.2 montre une représentation graphique de cet exemple.



Légende

Anglais	Français
Need: Personal transportation	Besoins: Transport privé
Constraints: Fuel: gasoline Environment: Variable between –30 °C and 40 °C	Contraintes: Carburant: essence Environnement: varie entre –30 °C et 40 °C
Requirement: Provide transportation for up to 5 people with moderate cargo capacity	Exigence: Transporter jusqu'à 5 personnes avec une capacité de chargement modérée
Item: Family vehicle with specific passenger and cargo capacity	Entité: Véhicule familial avec passager et capacité de chargement spécifiques
Functional requirements: Size for 5 passengers and moderate cargo capacity Medium power to enable towing of small trailer Best fuel economy in class	Exigences fonctionnelles: Taille pour 5 passagers et capacité de chargement modérée Puissance moyenne permettant de tracter une petite remorque Modèle le plus économique en carburant dans la gamme
Non-functional requirements: Extensive safety features Meets environmental regulations High security features	Exigences non fonctionnelles: Fonctionnalités complètes de sécurité Satisfaction aux règlements environnementaux Fonctionnalités élevées de sécurité

Anglais	Français
Dependability requirements: Reliability: almost no failures where vehicle has to be towed Maintainability: High Maintenance support: all maintenance done by local dealer Durability: life of at least 15 years Low life cycle cost	Exigences de sûreté de fonctionnement: Fiabilité: quasiment aucune défaillance lorsque le véhicule est à remorquer Maintenabilité: élevée Logistique de maintenance: toutes les activités de maintenance sont effectuées par le concessionnaire local Durabilité: durée de vie d'au moins 15 ans Coût faible du cycle de vie
Time-dependent aspects	Aspects liés au temps

NOTE Il s'agit uniquement d'un exemple illustratif permettant de clarifier les interdépendances entre ces concepts.

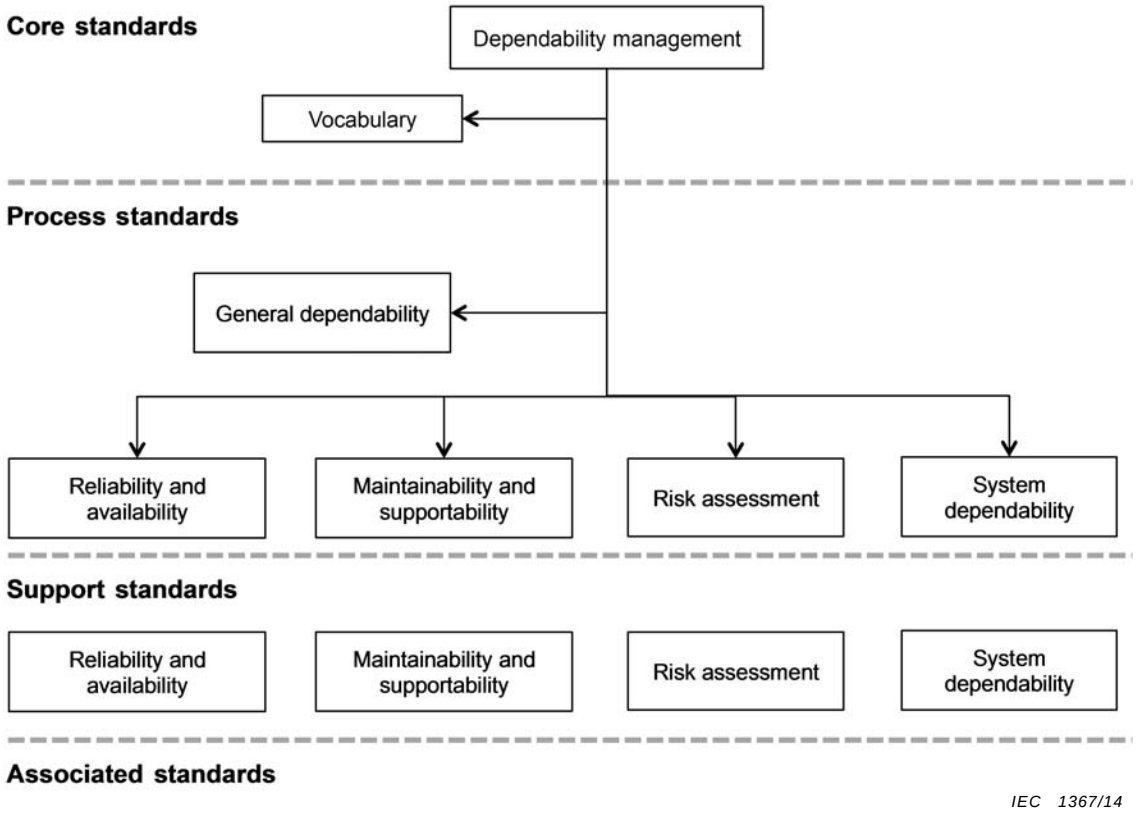
Figure C.2 – Exemple illustrant la relation entre les exigences fonctionnelles, non fonctionnelles et de sûreté de fonctionnement pour une voiture familiale

Annexe D
(informative)

Structure des normes de sûreté de fonctionnement

D.1 Structure

La Figure D.1 illustre la structure des normes IEC/TC56.



Légende

Anglais	Français
Core standards	Normes principales
Dependability management	Gestion de la sûreté de fonctionnement
Vocabulary	Vocabulaire
Process standards	Normes de processus
General dependability	Sûreté de fonctionnement générale
Reliability and availability	Fiabilité et disponibilité
Maintainability and supportability	Maintenabilité et supportabilité
Risk assessment	Appréciation des risques
System dependability	Sûreté de fonctionnement du système
Support standards	Normes de soutien
Associated standards	Normes connexes

Figure D.1 – Cadre pour les normes de sûreté de fonctionnement

Les normes de sûreté de fonctionnement sont structurées en quatre niveaux afin de faciliter les applications de sûreté de fonctionnement et la mise en œuvre du projet.

D.2 Normes principales

Elles donnent des lignes directrices sur la gestion globale de la sûreté de fonctionnement et présentent le cadre normalisé pour l'application de la sûreté de fonctionnement. Pour venir à l'appui de la gestion de la sûreté de fonctionnement, le vocabulaire comprend les définitions de base pertinentes pour la sûreté de fonctionnement. Les normes individuelles de sûreté de fonctionnement peuvent comprendre des définitions spécifiques applicables en premier lieu à la norme considérée.

D.3 Normes de processus

Elles concernent principalement les processus d'application des aspects majeurs de la sûreté de fonctionnement afin de faciliter la mise en œuvre de la sûreté de fonctionnement pour les projets et la réalisation des autres objectifs organisationnels.

Les normes de processus peuvent être de nature générale, être associées aux caractéristiques de sûreté de fonctionnement ou traiter de l'évaluation des risques et des aspects de sûreté de fonctionnement du système. Leur but est de fournir une aide pour les processus associés à la mise en œuvre des méthodes et techniques de sûreté de fonctionnement.

La sûreté de fonctionnement générale couvre des sujets comme les coûts du cycle de vie et les spécifications de la sûreté de fonctionnement.

D.4 Normes de soutien

Elles concernent essentiellement les méthodes et techniques spécifiques pour les groupements de processus.

Les normes sur la fiabilité et la disponibilité traitent de la modélisation et de l'analyse, des méthodes d'analyse statistique, des essais et de la protection de fiabilité, ainsi que de la croissance de la fiabilité.

Les normes de maintenabilité couvrent les études de maintenabilité, de testabilité et de vérification alors que la supportabilité traite des aspects relatifs à la maintenance et à la gestion de la maintenance, à la maintenance basée sur la fiabilité, aux accords de logistique de maintenance et au soutien logistique intégré.

Les normes d'évaluation des risques apportent un soutien aux outils qui analysent le risque comme AMDE et HAZOP ainsi que les risques liés au projet.

Les aspects du système consistent en des lignes directrices pour l'ingénierie et la spécification de la sûreté de fonctionnement relative aux systèmes et aux réseaux. Ceci comprend aussi la fiabilité humaine et logicielle.

D.5 Normes connexes

Elles comprennent les normes qui ne sont pas produites par l'IEC/TC 56, mais qui sont actuellement incluses pour référence dans la liste des normes sur le site web du TC 56.

Le cadre normalisé qui présente la liste des normes et des lignes directrices relatives à la sûreté de fonctionnement sur la sélection des normes pour la mise en œuvre du projet de sûreté de fonctionnement est disponible sur le site web [2] de l'IEC/TC 56.

Annexe E
(informative)

Liste de contrôle pour la revue de sûreté de fonctionnement

E.1 Remarque préliminaire

Les listes de contrôle suivantes sont des exemples des enjeux relatifs à la sûreté de fonctionnement pour lesquels une revue par la direction peut être nécessaire pour s'assurer que les objectifs de sûreté de fonctionnement sont atteints. Il convient d'adapter ces listes aux circonstances individuelles avec l'accord de la direction et du personnel responsable des activités de sûreté de fonctionnement. Les exemples de listes de contrôle sont plutôt généraux et peuvent exiger l'ajout de critères spécifiques pour réaliser une revue correcte.

E.2 Concept

E.2.1 Définition des exigences

a) Les objectifs de sûreté de fonctionnement établis sont adaptés aux besoins du marché et aux applications de l'utilisateur.

b) L'étendue du domaine d'application du marché et la stratégie pour les nouvelles initiatives sont identifiées, notamment les conditions d'utilisation du client et les conditions d'exploitation du marché, par exemple les conditions climatiques.

c) On détermine la valeur de sûreté de fonctionnement, le levier concurrentiel, les incitations et les contraintes d'application.

d) On identifie le calendrier de l'introduction d'un nouveau produit et les objectifs à atteindre.

e) On établit les critères d'adaptation et les activités applicables.

f) Les informations sur le nouveau système proposé sont acceptables pour initier une analyse des exigences.

g) Des éléments d'entrée relatifs aux exigences ont été obtenus auprès des parties prenantes et la conception permet de satisfaire à ces exigences.

h) Les risques qu'il est nécessaire de prendre en compte lors de la conception ont été identifiés.

E.2.2 Analyse des exigences

a) L'analyse des exigences des limites du système, des fonctions d'exploitation, des caractéristiques de performance et des limites technologiques a été menée et déterminée.

b) La disponibilité des ressources, la capacité technique et les nouveaux besoins d'investissement sont identifiés.

c) Les approches techniques et la faisabilité de la réalisation du système sont identifiées.

d) Le partenariat potentiel et les exigences du fournisseur sont identifiés.

e) Les résultats d'analyse des exigences et les raisons peuvent être justifiés pour les investissements de ressource afin d'initier la conception de concept de haut niveau du nouveau système.

f) Les risques des différentes options sont évalués et pris en compte dans la sélection de la conception.

g) Les exigences relatives à la santé, à la sécurité et à l'environnement ont été identifiées.

E.2.3 Conception architecturale de haut niveau

a) Les critères de conception architecturale, la configuration possible de l'entité et les options sont identifiés.

b) La sélection de technologie pour la conception des fonctions de l'entité pour la réalisation est identifiée.

c) Les évaluations probabilistes prévues sont cohérentes avec les objectifs de sûreté de fonctionnement.

d) Les critères de décision Fabriquer ou Acheter sont établis.

e) Les moyens de vérification et d'intégration des fonctions de l'entité ont été établis.

f) Les critères pour la conception des fonctions matérielles/logicielles ont été établis.

g) Les critères pour les conceptions prenant en compte l'environnement et l'ergonomie ont été établis.

h) Les critères pour l'évaluation des fonctions de l'entité ont été établis.

i) L'interopérabilité des fonctions du système et des limites de performance a été vérifiée pour satisfaire aux exigences de l'entité.

j) Les exigences de sûreté de fonctionnement dans les spécifications de l'entité sont incorporées comme lignes directrices pour la conception et l'acquisition de COTS.

k) La conception de la nouvelle entité et les options de conception architecturale sont identifiées et vérifiées avec des contraintes associées destinées à justifier l'initiation de la conception formelle de l'entité avec des spécifications documentées.

l) Les risques de performance associés aux différentes conceptions sont évalués.

E.3 Développement

E.3.1 Conception de l'entité

a) On établit le plan de sûreté de fonctionnement pour la conception de l'entité et ses composants.

b) On établit le plan d'assurance qualité et le processus de gestion de la configuration de l'entité.

c) Les évaluations probabilistes prévues sont cohérentes avec les objectifs de sûreté de fonctionnement.

d) Les plans d'essai et les critères d'acceptation sont établis et la simulation et les essais ont été effectués.

e) La surveillance et le contrôle de l'entité, le compte-rendu des incidents et les systèmes de gestion des données ont été établis.

f) L'application des composants a été revue avec les fournisseurs.

g) Les programmes de sûreté de fonctionnement des fournisseurs ont été établis.

h) La conception de l'entité est vérifiée et les programmes de soutien établis pour le développement grandeur nature.

E.3.2 Développement grandeur nature du système

a) Le processus d'adaptation pour différents projets de développement fonctionnels et d'entité est mis en œuvre et la responsabilité de chaque partie du projet est attribuée, notamment les éléments d'entrée de sûreté de fonctionnement pour le processus de conception.

b) On a vérifié la cohérence des évaluations probabilistes prévues avec les objectifs de sûreté de fonctionnement.

c) Les plans de vérification et de validation de l'entité ont été élaborés.

d) Les critères d'acceptation de la sûreté de fonctionnement et les programmes de croissance de la fiabilité ont été établis.

e) La conception a été modifiée et la fiabilité estimée.

f) Le contrôle de révision de la documentation de développement a été mis en œuvre.

g) Les risques menaçant les objectifs fonctionnels et non fonctionnels et les exigences de sûreté de fonctionnement ont été évalués et des plans de traitement spécifiés.

h) La maintenance de l'entité et les programmes de soutien logistique sont établis.

i) Les programmes d'externalisation sont établis.

j) Le programme d'approvisionnement en pièces de rechange est développé.

k) Les programmes de formation sont établis.

l) Les critères de garantie pour la logistique de service du système sont établis.

m) L'entité est entièrement développée et prête pour la production et la construction.

n) Les spécifications logicielles et les organigrammes ont été terminés et approuvés.

o) Le développement des fonctions du module logiciel et des sous-systèmes a été initié.

p) Les exigences relatives à la santé, à la sécurité et à l'environnement ont été analysées et l'impact sur la sûreté de fonctionnement a été minimisé.

E.4 Réalisation

E.4.1 Réalisation de l'entité

a) La production d'assemblages et de fonctions du matériel a été initiée.

b) Les programmes de sûreté de fonctionnement des fournisseurs sont mis en œuvre.

c) Les fonctions de l'entité et les plans de vérification et de validation du sous-système sont mis en œuvre.

d) Les systèmes de compte-rendu de défaillance, d'analyse et de collecte des données sont mis en œuvre.

e) Les programmes de formation sont développés.

f) L'entité est produite, construite, réalisée et prête à être mise en œuvre.

E.4.2 Mise en œuvre de l'entité

a) Le plan d'intégration du système est mis en œuvre.

b) Des actions spécifiées destinées à traiter les risques ont été mises en œuvre

c) Les plans de vérification et de validation de l'entité sont mis en œuvre.

d) Les plans de qualification et d'acceptation de l'entité sont mis en œuvre.

e) Le plan d'installation de l'entité est mis en œuvre.

f) Le plan de garantie est mis en œuvre.

g) Les programmes de formation pour l'exploitation du système et les services d'assistance à la clientèle sont initiés.

h) Les modifications exigées de conception destinées à satisfaire aux exigences de sûreté de fonctionnement ont été mises en œuvre et vérifiées.

i) L'entité est prête pour la mise en service.

E.5 Utilisation

a) Les programmes de maintenance et de soutien sont mis en œuvre.

b) Les risques sont réévalués à la lumière des conditions réelles.

c) Les performances de l'entité et les services de maintenance sont surveillées et contrôlées.

d) Les programmes de formation des opérateurs et des agents de maintenance sont mis en œuvre.

e) Le système de collecte des données d'exploitation est mis en œuvre.

f) La gestion de modification de la conception et la gestion de configuration sont mises en œuvre.

g) L'enquête de satisfaction client est mise en œuvre.

h) Les données de performance de l'entité sont analysées à des fins d'amélioration continue.

i) L'entité continue à maintenir les performances opérationnelles relatives à la sûreté de fonctionnement.

E.6 Amélioration

a) Les nouvelles fonctionnalités de l'entité et les besoins d'amélioration sont identifiés.

b) Les conséquences des risques, en particulier en ce qui concerne les exigences relatives à la santé, à la sécurité et à l'environnement, et la valeur d'amélioration sont analysées.

c) Les programmes d'amélioration et le cadre temporel d'amélioration sont déterminés.

d) La décision des programmes d'amélioration est mise à exécution.

e) L'enquête de satisfaction client résultant des programmes d'amélioration est surveillée afin de déterminer la valeur d'amélioration.

E.7 Mise au rebut

a) La stratégie de mise hors service et de destruction est planifiée et initiée.

b) L'impact de la fin du service est déterminé.

c) Les clients ont été notifiés du calendrier et de la date de fin de service ainsi que des offres de services nouveaux ou alternatifs.

d) L'enquête de satisfaction client résultant de la fin de l'ancien service et de l'utilisation du nouveau service est surveillée.

e) Les données exigées ont été transférées.

Bibliographie

[1] IEC 60050-191:2014, *Vocabulaire Électrotechnique International – Partie 191: Sûreté de fonctionnement*

[2] Site web IEC/TC 56, http://tc56.iec.ch

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch