

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Dependability reviews during the life cycle

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

IECNORM.COM : Click to view the full PDF of IEC 62960:2020



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2020 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

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

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

About the IEC

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

About IEC publications

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

IEC publications search - webstore.iec.ch/advsearchform

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

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

Electropedia - www.electropedia.org

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

IEC Glossary - std.iec.ch/glossary

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

A propos de l'IEC

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

A propos des publications IEC

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

Recherche de publications IEC -

webstore.iec.ch/advsearchform

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

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

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

Electropedia - www.electropedia.org

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

Glossaire IEC - std.iec.ch/glossary

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

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Dependability reviews during the life cycle

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.120.01

ISBN 978-2-8322-7977-9

Warning! Make sure that you obtained this publication from an authorized distributor. Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.
--

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	8
2 Normative references	8
3 Terms and definitions	8
3.1 Terms and definitions.....	8
3.2 Abbreviated terms.....	11
4 Introducing dependability reviews	11
4.1 General.....	11
4.2 Technical reviews	13
4.3 Status reviews	13
4.4 Overview of the dependability review method.....	14
4.4.1 Overview	14
4.4.2 Identifying stakeholders.....	14
4.4.3 Identifying what the requirements are	15
4.4.4 Capturing information on actual performance.....	15
4.4.5 Assessing the gap between requirements and actual performance	15
4.4.6 Identifying risks and areas of concern.....	15
4.4.7 Recommending actions.....	16
4.5 Planning for and timing of dependability reviews.....	16
4.6 Levels of dependability reviews.....	17
4.6.1 Overview	17
4.6.2 Team reviews	18
4.6.3 Project reviews	18
4.6.4 Status reviews	19
5 Dependability review activities during the life cycle.....	19
5.1 General.....	19
5.2 Concept stage.....	20
5.3 Development stage	20
5.3.1 Overview	20
5.3.2 Design reviews	21
5.4 Realization stage	22
5.5 Utilization stage	23
5.6 Enhancement stage	23
5.7 Retirement stage	24
6 Implementing the dependability review process	24
6.1 General.....	24
6.2 Planning of the review.....	24
6.3 Selection of the review team	25
6.4 Preparation of the input package	25
6.5 Meeting notification and agenda	25
6.6 Conducting a review meeting	26
6.6.1 General	26
6.6.2 Meeting protocol.....	26
6.6.3 Action points.....	27
6.6.4 Recommendations	27

6.6.5	Rejected action points and recommendations	27
6.6.6	Meeting conclusion	27
6.7	Preparing and distributing review minutes	27
6.7.1	General	27
6.7.2	Minutes	28
6.8	Actions and recommendations from a review	28
6.9	Follow-up and completion of action points and recommendations	29
Annex A (informative)	Examples of an input package for a review	30
A.1	Concept stage	30
A.2	Development stage	30
A.3	Realization stage	30
A.4	Utilization stage	31
A.5	Enhancement stage	31
A.6	Retirement stage	32
Annex B (informative)	Examples of objectives for dependability reviews during the life cycle	33
B.1	General	33
B.2	Concept stage	33
B.3	Development stage	33
B.3.1	Conceptual design review	33
B.3.2	Detail design review	33
B.3.3	Final design review	34
B.4	Realization stage	34
B.5	Utilization stage	35
B.5.1	Operation	35
B.5.2	Maintenance	35
B.6	Enhancement stage	35
B.7	Retirement stage	36
Annex C (informative)	Considerations during dependability reviews through the life cycle	37
C.1	General	37
C.2	Examples of dependability review considerations in the concept stage	37
C.3	Examples of dependability review considerations in the development stage	38
C.4	Examples of dependability review considerations in the realization stage	39
C.5	Examples of dependability review considerations in the utilization stage	40
C.6	Examples of dependability review considerations in the enhancement stage	41
C.7	Examples of dependability review considerations in the retirement stage	42
Annex D (informative)	Functions and responsibilities of some key persons for a technical review	43
D.1	General	43
D.2	Chair	43
D.3	Secretary	44
D.4	Relevant specialists	44
D.5	Project or team manager and members	45
D.6	Customers and users	45
Annex E (informative)	Dependability topics for a review	46
E.1	General	46
E.2	Reliability	46
E.3	Maintainability	46

E.4	Maintenance	47
E.5	Maintenance support.....	47
E.6	Availability	47
E.7	Quality assurance	48
E.8	Environmental effects	49
E.9	Product safety	50
E.10	Human factors	50
E.11	Legal matters	51
E.12	Durability	52
E.13	Security	52
E.14	Property damage	52
E.15	Accountability	53
Bibliography		54
Figure 1 – Flow of reviews during a life cycle stage		18
Figure 2 – Implementing the review process		24

IECNORM.COM : Click to view the full PDF of IEC 62960:2020

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY REVIEWS DURING THE LIFE CYCLE

FOREWORD

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

International Standard IEC 62960 has been prepared by IEC technical committee 56: Dependability.

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

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

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

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

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

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

IECNORM.COM : Click to view the full PDF of IEC 62960:2020

INTRODUCTION

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

Benefits of dependability review throughout the life cycle include:

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

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

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

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

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

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

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

DEPENDABILITY REVIEWS DURING THE LIFE CYCLE

1 Scope

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

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

This document describes a dependability review methodology focusing on:

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050-192, *International electrotechnical vocabulary – Part 192: Dependability* (available at <http://www.electropedia.org>)

3 Terms and definitions

3.1 Terms and definitions

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

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

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

3.1.1

dependability management

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

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

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

3.1.2**dependability plan**

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

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

3.1.3**dependability review**

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

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

3.1.4**design review**

planned and documented review of an existing or proposed design

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

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

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

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

3.1.5**gap analysis**

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

3.1.6**item**

subject being considered

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

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

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

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

3.1.7**life cycle**

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

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

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

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

3.1.8**management**

coordinated activities to direct and control an organization

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

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

[SOURCE: ISO 9000:2015, 3.3.3]

3.1.9

project

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

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

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

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

3.1.10

project milestone

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

3.1.11

project review

review of the project output

3.1.12

review

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

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

3.1.13

stakeholder

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

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

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

3.1.14

status review

review of the overall project status with respect to established objectives

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

3.1.15

system

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

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

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

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

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

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

3.1.16

team

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

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

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

3.1.17

team review

review of the team output

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

3.1.18

technical review

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

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

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

3.2 Abbreviated terms

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

4 Introducing dependability reviews

4.1 General

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

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

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

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

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

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

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

Some environments or conditions for the trends include:

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

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

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

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

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

¹ Numbers in square brackets refer to the Bibliography.

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

4.2 Technical reviews

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

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

Technical reviews of dependability can involve:

- reviews of the achieved or predicted dependability of an item where the objective is to improve dependability of the item itself by evaluating dependability measures and by exploring opportunities for improvement;
- reviews of the processes and activities planned to achieve dependability in order to learn lessons and improve future processes and activities.

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

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

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

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

4.3 Status reviews

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

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

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

4.4 Overview of the dependability review method

4.4.1 Overview

Dependability can be reviewed as a separate issue or as part of other reviews. In either case the dependability review should involve the following stages:

- identifying stakeholders;
- identifying what the requirements are;
- capturing information on actual performance;
- assessing the gap between requirements and actual performance;
- identifying risks and areas of concern;
- recommending actions.

If changes are introduced, their effectiveness should be checked, and a judgment should be made about whether any additional action or actions are required.

4.4.2 Identifying stakeholders

It is important for persons or organizations developing and operating systems to clearly recognize who their stakeholders are, since their ultimate aim is to satisfy the needs of these stakeholders. Stakeholders should therefore be identified and means of communication with them established. For some systems, it is relatively easy to identify stakeholders and they do not change through the lifecycle. For other systems, it may be difficult to identify all stakeholders at the outset and to fully determine their needs. For example stakeholders may change when a system enters the utilization stage or when a developed item is sold to a different person or organization. They can also change when a system enters the retirement stage.

When determining who are relevant stakeholders, the following should be considered:

- a) Stakeholders include those who may be affected by the system or by the system failure, for example, through wrongful information disclosure or malfunction caused by human error or misuse.
- b) Some of the stakeholder requirements which, for example can cause development failures and delivery delay, might be known during development and should be identified and considered in the reviews.
- c) Once the relevant stakeholders have been identified, the key stakeholders should be identified from this list. A risk-based approach should be followed to determine which stakeholders are key. The criteria for determining which stakeholders are considered as key, will be variable, depending on the identified success criteria for the system, as well as the degree of importance and influence that each stakeholder has.
- d) The list of stakeholders may change when the system enters the utilization or retirement stages. For example:
 - 1) A developed item may be sold to a different person or a different organization assumed during the development or realization stages.
 - 2) A developed item may be utilized by different persons or the same organization internally.

4.4.3 Identifying what the requirements are

In order to meet dependability objectives and achieve the dependability expected by stakeholders it is sensible to specify an achievable goal with measureable targets and activities together with an appropriate course of action during the life cycle. These become the requirements against which reviews are carried out. The goal may relate to both the functionality required from the system and the desired performance. Stakeholders or organizations who are interested in the system's dependability might have differing agendas and may or may not be different through the life cycle. Therefore, it can be necessary to revisit targets and goals at each stage and change them if necessary. New plans are then generated and executed on a stage by stage basis to achieve the targets and the results reviewed from a dependability perspective. The relative level of importance of stakeholders, to the project's perceived success can vary. This therefore may influence the contents of the plans, in line with relative importance.

A dependability goal should be clarified against the details of the system specification and the project plan. The goal can take into account technical opportunities, risks, the sufficiency of each life cycle stage and relevant requirements from the result of market research.

4.4.4 Capturing information on actual performance

Sufficient evidence should be gathered about what actually occurs or exists to enable reliable conclusions to be drawn during the review. Evidence includes information for comparison with each requirement, target and deliverable that is within the scope of the review. This may include test results calculations, simulations, and other analyses. Any problems encountered in areas of concern or features that might affect risks should be ascertained. Annex A provides details of some information that can be collected. This will minimize uncertainty in the output of the review.

If the evidence is insufficient, being incomplete or not of adequate quality, or the understanding and analysis of the evidence is incomplete, the results of the review are likely to be unreliable or incomplete. In this case, action should be taken to either obtain more or better evidence, or to improve understanding.

Evidence that has been collected for a dependability case can also be used as evidence in a dependability review. Similarly evidence from a review can form part of a dependability case.

IEC 62741 [3] gives guidance on the content and application of a dependability case and establishes general principles for its preparation. It is written in a basic project context where a customer orders a system that meets dependability requirements from a supplier and then manages the system until its retirement. The methods provided in this document may be modified and adapted to other situations as needed. The information is normally defined and produced in cooperation between customer and supplier but can also be used and updated by other organizations. For example, certification bodies and regulators may examine the submitted case to support their decisions and users of the system may update/expand the case, particularly where they use the system for a different purpose.

4.4.5 Assessing the gap between requirements and actual performance

Gaps between the actual result and that expected or required should be identified, the significance of any deviation should be evaluated, possible corrective actions identified and a decision made about whether a corrective action is required.

This may involve analysis of the causes of deviations. Techniques such as root cause analysis described in IEC 62740 [7] can be used.

4.4.6 Identifying risks and areas of concern

The review may also identify areas of concern and potential future problems, review previously identified risks and assess new risks. Techniques such as those described in IEC 31010 [13] can be used.

In addition, risks to dependability are likely to be identified in risk assessments carried out at each stage of the life cycle in contexts other than a dependability review. Equally the output of risk reviews will provide information on the progress of treatments for dependability risks. This information should be incorporated into dependability reviews as appropriate.

4.4.7 Recommending actions

Depending on the scope and objectives the outcome of the review may be:

- confirmation that requirements have been met;
- approval to progress to the next project stage;
- recommendations for improvements;
- actions to address issues and risks.

Where the team makes recommendations for change, depending on review scope, they might also follow through with implementation. In some cases the team identifies alternative solutions to problems for consideration by others, with the responsibility for implementing actions and checking their outcome lying with people outside the review team.

Recommendations should be checked to see that they do not introduce additional problems.

4.5 Planning for and timing of dependability reviews

Dependability reviews can continually improve the dependability of a system as part of "Plan-Do-Check-Act" described in ISO/IEC 27000 [19]. For example, there may be a need to continually improve the dependability of an item for example in order to maintain commercial advantage, or continual improvement in security controls may be necessary simply to maintain current levels of security. A "Plan-Do-Check-Act" process may be applied within a single stage of the life cycle or during multiple stages of the life cycle.

Dependability reviews occur at each stage of the life cycle, particularly when moving from one phase to another or when responsibility for a project is transferred. A critical point for planning the timing of status reviews is at the concept stage. This is usually carried out in support of a submission for authorization to proceed with a project or to enable a quotation to be submitted to a client. Risks should be identified and assessed as input to decisions about the dependability reviews required at later life cycle stages.

Ideally technical reviews should be conducted before taking a decision that can prove costly, time consuming or difficult to reverse. This should take into account the identified risks for the design and/or project. In this way, any changes arising from a dependability review can be made with less impact on schedule or cost. Additionally, cost, schedule and performance improvements can be more readily adopted if reviews are conducted before making a significant commitment such as at a major point of the design process.

Other triggers for a dependability review include the following.

- Detection of failures

Unanticipated failures can indicate that the environment and/or the system has changed and that the assumptions previously made are no longer valid. Dependability reviews should identify the changes that caused the failures and formulate possible adaptations. After failures, dependability reviews should assess the adequacy of actions and the need to prevent recurrence.
- Change in market requirements

The rapid technological changes, such as are typically found in software and information technology, can not only create new markets but also introduce new previously unanticipated requirements, for example the market requirement for a mobile phone might not be voice communications, but a mobile computing terminal. A change in market requirements for whatever reason can bring additional dependability requirements such as

security improvement or changes in support needs. Performing dependability reviews during the life cycle can clarify the new requirements for dependability and consequently changes in market requirements can be managed. Dependability reviews that are based on market trends and customer satisfaction can be performed for both marketing and dependability purposes.

- **Competitive system specifications**

It can be difficult to maintain the competitiveness of systems through the life cycle if the system specification and dependability performance are unchanged, as systems with similar or alternative specifications can be released by competitors. Therefore, reviews against competitor system specifications to achieve the objectives during the life cycle may be required. Such reviews can lead to system improvements, renewals or revised strategies.

- **Technical innovation**

Technical innovation can place demands on systems for improved dependability. It can create opportunities for new products or enable new methods to be applied that improve the dependability of existing products. A demand for rapid release of new and innovative products to the market applies pressures on achieving dependability. Reviews of dependability are essential to achieving change in a dependable way and providing assurance that new products are dependable.

- **Societal demand for dependability**

Dependability activities through the life cycle, including dependability planning, design review, reliability growth, maintenance, obsolescence management and disposal of modern systems, will be subject to societal pressures. Dependability reviews can include continual research into the demands of society and how they are changing. The societal demand for dependability in each system may not be the same since the stakeholder demands of the system are different depending on the type of system. In addition, different characteristics such as reliability, maintainability, availability, safety and security might be important. If appropriate, a checklist on societal demand can be created, the results of which can be reflected in the dependability plan and the activities of the dependability review.

Dependability reviews should be carried out both to address detected problems caused by these changes and also to identify potential future problems (risks).

The fact that these changes occur throughout the system life cycle gives rise to concerns about requisites such as accountability. These concerns are addressed not just in reviews triggered directly by the changes but through the organization of dependability reviews spanning the whole system life cycle. These problems may also result in a need for change to the dependability plan.

The size and complexity of the system will influence the nature, timing and number of reviews, such as whether it is:

- a simple design or a minor upgrade;
- a system involving multiple systems;
- a complex system.

Dependability review meetings are independent of those meetings undertaken as a part of the ongoing scheduling, development and maintenance of the system.

4.6 Levels of dependability reviews

4.6.1 Overview

Dependability reviews can be categorized according to the level of the review, which is determined from the participants and their level of involvement with the day to day subject of the review. These reviews are carried out at all life cycle stages and can be carried out at team, project and status level. They are carried out in a hierarchy with team reviews feeding into project reviews feeding into status reviews.

Figure 1 shows the relationship between team reviews, project reviews and status reviews during a life cycle stage.

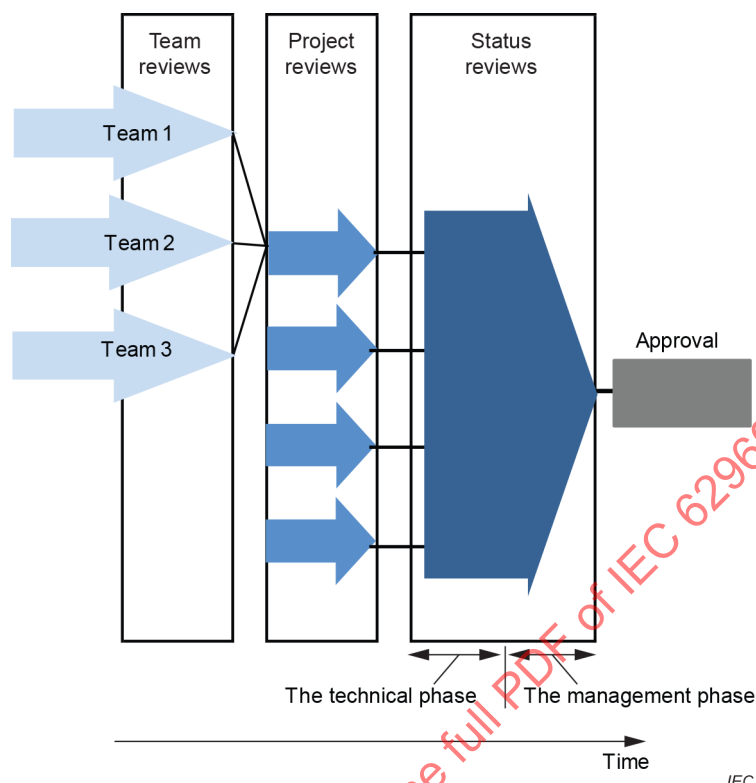


Figure 1 – Flow of reviews during a life cycle stage

4.6.2 Team reviews

The purpose of a team review is to undertake a technical review of the output of the team focused on the team's particular role, for example on electronics, mechanics or software. The participants in a team review are a team leader and at least one team member. The team leader has the role of the chair of the team review. The team leader may choose not to assign a secretary. The team leader uses information on what has been achieved and information from a gap analysis to identify what needs to be done by the team and develops task lists to determine the appropriate people for the actions and the estimated timeline. Members of the team then review their task lists and try to anticipate any problems or delays. The team is then in a position to give mutual assistance as soon as the need arises.

The content of a team review may be a part of a project review and conclusions from the team review can be input to the project review.

4.6.3 Project reviews

Project reviews are checks on the technical status of an individual project in an overall programme and includes input from team reviews. The project may be of any size and a project review may occur at any time during the life cycle. A project may be large, as would be common during the development phase, or could be small, which might apply during the utilization phase to review item reliability. Project reviews serve to evaluate what has been achieved relative to the project plan. Timelines should be reviewed and key progress deliverables monitored, using proper project management tools and proven techniques. The participants of a project review are a project leader and project members. The project leader has the role of the chair of the project review. The project leader may choose not to assign a secretary. Project reviews may be informal with the project leader or mentor, or formal with the project champion or the project sponsor. In either case, however, the project leader needs to manage the review to ensure that the required benefits are achieved. Each person involved in the project shall contribute in

accordance with their impact on the project's needs and outputs to ensure that the project review is successful. The conclusion from the project review can then be the technical input to a status review.

4.6.4 Status reviews

Status reviews consider the overall status of a project. The purpose is normally to make management aware of how a project is progressing and, in some cases, to discuss technical risks and authorize the continuation of the project to the next phase in the project plan. However, there is a possibility that the project might be modified or even stopped after a status review.

A status review has two phases, a technical phase that considers the technical status of the project and a management phase where the management group evaluates the technical status and takes decisions concerning cost, schedule, risks, opportunities and performance. This document only discusses the technical part of the status review.

The input to status reviews includes the results of any previous reviews including any recommendations, any corrective actions and an update on their implementation. The status of all potential problems should be listed with a time schedule and a responsible person for each problem not solved or otherwise closed.

Where a project review identifies problems, the technical phase of a status review should consider planned and implemented solutions and planned activities as well as the remaining technological risks in the project. Ideally, the technical part of the status review would not identify problems that have not been previously identified and analysed. Where an identified problem has not yet been analysed, a plan for the analysis with the responsible person and due date for the output should be presented together with an evaluation of the potential impact on the project.

The status review can also involve

- analysing the impact on the dependability plan and updating it accordingly;
- checking if a review of the entire plan is required as a result of the action;
- authorizing/obtaining resources and implementing change.

5 Dependability review activities during the life cycle

5.1 General

Life cycles vary according to the nature, purpose, use and prevailing circumstances of a system. The life cycle may be described generally as consisting of the following stages:

- concept;
- development;
- realization;
- utilization;
- enhancement;
- retirement.

Dependability is typically reviewed at every stage and often reviews need to be repeated within a single stage depending on the review result.

The result of the review affects the decision on whether to continue this loop or to exit from it. When continuing the loop, the review result is fed back to the activities carried out in the stage, revised output is produced, and the output is reviewed again taking into account the previous review result. When exiting the loop, the review result is forwarded to the activity succeeding the loop, which may be in the next life cycle stage.

Some dependability reviews are performed in more open-ended contexts with the goal to produce review results that improve future activities and products of the organization. The review result from the retirement stage, often containing "lessons learned", is recorded as the organizational knowledge, utilized in its projects portfolio management, and forwarded to the concept stage of the life cycle of the new item when relevant.

The type of dependability review carried out should be appropriate to the life cycle stage. This is best managed and documented through the dependability plan. If a problem is discovered through the review at any stage, it is important to investigate the root cause of the problem at the same stage, make improvements, and confirm the result with a technical review. The results of reviews carried out at one life cycle stage should where relevant be passed on to the next stage.

The manager should consider the conditions and constraints imposed by a particular life cycle stage in the scheduling of dependability reviews and the optimum number of reviews should be determined to optimize return on time spent. Only a few organizations or projects will have a need for all types of dependability reviews at all life cycle stages.

Subclauses 5.2 to 5.7 below outline the purpose of each life cycle stage, the dependability reviews which might be carried out during that stage and the particular issues which might occur. Examples of objectives of reviews for each life cycle stage are provided in Annex B. Annex C gives a generic list of review considerations that could be used during actual dependability reviews from different perspectives over the life cycle.

5.2 Concept stage

The concept stage is the initial visioning stage for an item and defines requirements, technical parameters and constraints. Ideas are generated and translated into technically and economically feasible concepts. A preferred option is selected, taking into account potential trade-offs and risks. The output from this stage is an initial concept design for the selected option and a preliminary project plan including a dependability plan.

Review activities involve:

- checking the concept design against customer needs, expectations and constraints;
- reviewing the feasibility of the proposed design;
- reviewing the feasibility of the project plan;
- improving the concept where necessary;
- deciding whether to commit resources to full development.

The reviews should include broad expectations for dependability and their impact on the design, operation and maintenance of the item. In particular, status reviews should be carried out at the end of the concept stage to ensure that the concept taken forward to the development stage meet the customer needs, expectations and constraints. Risks, including risks of failure to meet requirements are identified and reviewed at each subsequent stage.

Outputs from this stage should be reviewed later in the life cycle when more information has become available.

5.3 Development stage

5.3.1 Overview

The development stage follows the initial concept stage once its feasibility has been verified. The focus is to plan and execute selected engineering design solutions. Detailed engineering design of the selected solutions is then undertaken.

In the detailed design stage, properties of all components are specified and drawings and other documentation such as operating instructions are produced. Maintenance and logistic support needs are defined.

Risks associated with the selected design are assessed in more detail and treatments specified. Relevant modelling and probabilistic approaches can be used at this stage to achieve detailed dependability predictions. Prototypes (where relevant) are tested.

5.3.2 Design reviews

Design reviews are an example of technical reviews which look particularly at the design of an item or system and verify that the design requirements have been met as well as stimulating improvement in the design.

Generally, a series of reviews is carried out during the concept and development stages in the form of formal design reviews. A design review assesses the design against input requirements, identifies risks, opportunities for improvement and guides the design manager towards appropriate action. It accelerates maturing of the product by reducing the time needed to stabilize design details and allows product realization to proceed without frequent interruptions. Design reviews can also stimulate early product improvement.

Properly implemented, design reviews enhance the potential for delivering a product of the required dependability, quality, performance and safety with potential for reduction in costs and delivery schedule.

The feasibility of achieving the required dependability could be dependent on the approach taken in the design of the item such as whether:

- it is a customized design based upon selection from a range of proven components and materials;
- the design involves the use of unproven components, materials or subcontractors;
- the design involves the interpolation of existing experience;
- the design involves extrapolation from existing experience;
- it is a completely new design or the application of unproven technology.

If the design includes the need for a prototype, a review of the results of prototype testing could be critical in deciding the activities needed to ensure a reliable final design. In extreme cases, it could even result in a decision, in a status review, to abandon the project.

Design reviews are held when there is a draft design or process to analyse, preferably early enough to allow for the introduction of changes. The cost to correct deficiencies in a design and the potential consequences increase as the design nears completion. Also, as the design progresses towards completion, so the flexibility to implement a change to correct a deficiency or to optimize the design decreases.

Objectives of design reviews can include

- assessing whether the proposed solution meets the design input requirements that may include, but are not limited to: specified general performance requirements, dependability, life cycle costs, safety, endurance, environment, electromagnetic compatibility and human factors;
- assessing whether the proposed solution is the most robust, efficient and effective solution to achieve the product requirements;
- providing recommendations as required for achieving the design input requirements;
- assessing the status of the design in terms of the completeness of the drawings and specifications;
- assessing the evidence to support the verification of the design performance;

- assessing the status of the component application 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;
- proposing improvements;
- assessing whether the product and its elements can be safely and economically disposed of;
- checking components are to be used within their specified ratings.

Generally, design reviews should be held as follows:

- prior to acceptance of the order for the design to ensure that the scope of work is established together with all the parameters that need to be met for an acceptable design;
- prior to detail design to ensure that the members of the design team have first-hand detailed knowledge of all requirements. Interface provisions should be established and a list of defining documentation scheduled for submission and approval between the parties;
- at suitable points during detail design to review all interface provisions and agree on the test procedures for verifying that the design meets contract and stakeholder requirements;
- immediately prior to the handover to the realization stage.

Dependability review meetings are independent of those meetings undertaken as a part of the ongoing scheduling, development and maintenance of the system.

Care should be taken to prevent the design review from dictating the ultimate design and development of the system. Many decisions can affect the dependability of the system or process under review. If each decision is subjected to an independent review, the review team would, in essence, become the designer or developer with the potential for increased development time and costs. Conversely, if the first dependability review occurred only just before realization or utilization, its benefit could be questionable as there may be little opportunity to influence the situation without a significant time and/or cost penalty.

Design reviews may be internal or external. For an external review, there will be an independent review team who receives presentations and information from those responsible for the design. The typical composition of an external review team is described in 6.3.

5.4 Realization stage

The realization stage implements make-buy decisions for the acquisition and/or manufacturing of the final item and its components. Realization includes component and module simulations, analysis and tests (including integration tests) followed by installation of the item. There may be trials in the actual factory and/or operating environment prior to commissioning.

Reviews can involve a comparison of actual operating conditions, user characteristics and assumptions, against those assumed in the design, in order to help identify problems that might arise. The dependability performance achieved is reviewed against specifications to provide objective evidence of conformance. Plans for operation such as maintenance plans that were created during the development stage are reviewed to make sure that tasks are achievable and satisfy the design intent.

Reviews where dependability may be considered include:

- a supplier review to ascertain suppliers' quality, delivery schedule commitments, order processing capacity, efficiency, sourcing policy and supply-chain management;
- a quality review to determine non-conformance status, assurance effectiveness and quality performance trends and to identify areas for improvement and recommend management actions;
- a verification and validation review to ensure proper verification and validation processes have been carried out;

- a 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. Dependability problems are often a major component of downtime, that affect item availability and therefore production;
- a product release review prior to releasing the product for delivery and/or customer acceptance;
- a product release information review to ensure that the process for correct storage, installation, integration, commissioning and maintenance are available.

5.5 Utilization stage

In the utilization stage, the item is deployed to perform the function(s) or service(s) for which it was designed. Activities include operating and maintaining the item in accordance with performance requirements, training operators, training maintainers and keeping records of performance and of failure incidents to initiate timely corrective actions.

Risk assessment during operation and maintenance can deal with problems that arise due to changing conditions. Reliability, availability, maintainability and supportability can be monitored with longer term field testing possible and the results reviewed both to identify the need for design changes and to improve maintenance and maintenance support programmes.

Dependability reviews during utilization can take various forms such as:

- an operations review to determine the health and operational status of a plant or a service facility;
- a reliability review of actual against expected performance and its impact on availability;
- a maintenance and support review to evaluate the maintenance support and logistics performance of critical items including cost and clarify whether they are achieving the required availability and functionality;
- a service review to determine customers' service needs, scheduled and unscheduled maintenance activities, third-party service provisions, maintenance support, inventory holdings and depot locations;
- a risk review to determine whether risks have changed and whether the risk management process is effective;
- a customer satisfaction review to address user concerns and improvement strategies where dependability could be a significant focus.

For items with a long life, objectives, stakeholders and requirements can change through the utilization phase. Periodic reviews should be carried out to check for changes so that activities and their outputs continue to achieve objectives.

5.6 Enhancement stage

The enhancement stage might be needed to improve item performance to meet growing user demands, extend operating life or address obsolescence (see IEC 62402 [6]). Activities can include hardware or software upgrades or additions, maintenance improvements, simplifying procedures to improve operational efficiency or obsolescence management. At this stage, relevant modelling and probabilistic approaches can be used to assess the impact of possible enhancements and select the best solutions. Risk assessment during the enhancement stage often looks at cost versus benefits and return-on-investment as well as the technical impact of proposed changes.

A review is generally carried out in order to identify and assess the improvements that need to be implemented. Depending on the extent of the changes, design reviews as described in 5.3.2 may be required during the design of upgrades.

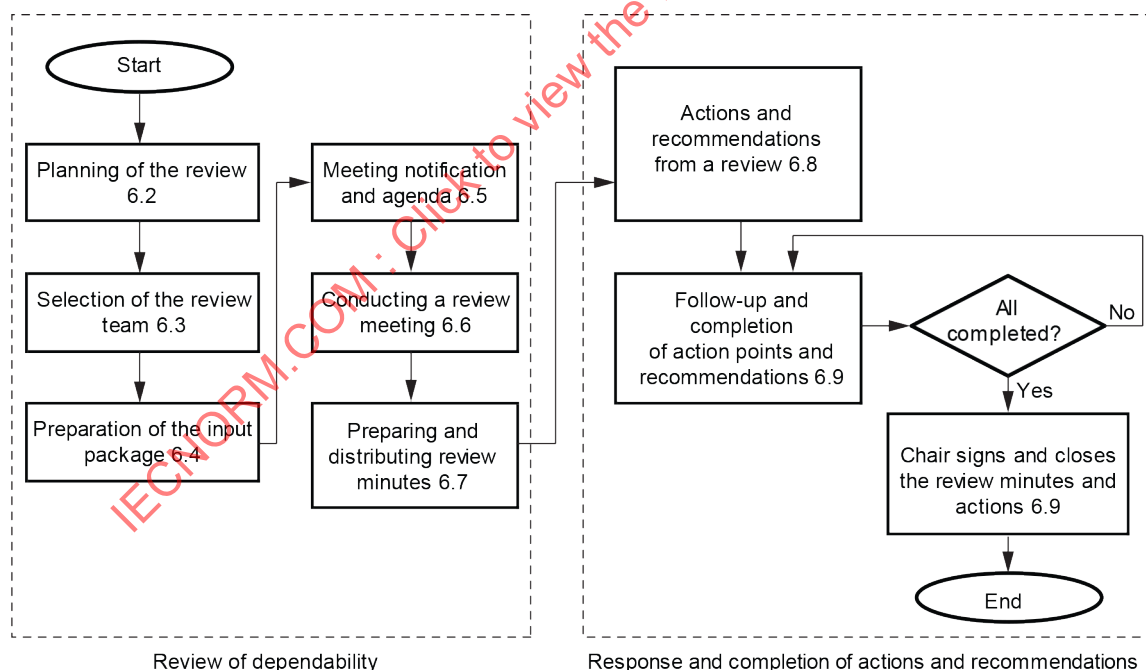
5.7 Retirement stage

The retirement stage occurs at the end of an item's useful life. 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). Actions to be taken for retirement or disposal should have been considered during the concept stage. Retirement plans developed earlier in the life cycle should be reviewed before implementation to take account of actual circumstances. 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. It may be useful to review lessons learnt over the life cycle if similar projects or items are to be considered. A requirement to mothball/preserve the system for a defined period before its ultimate disposal will require suitable preservation activities to be determined and then applied during the relevant period. The results of the reviews at the retirement stage, including lessons learnt should be recorded as the organizational knowledge and used as input to the concept stage of a new project when relevant.

6 Implementing the dependability review process

6.1 General

Dependability reviews require careful planning, organization and reporting. Clause 6 provides a framework for implementation of the review process and is applicable to most reviews and not just dependability reviews. Specific details will depend on the subject of the review and the type of review being carried out. This clause is based upon a review involving a structured review meeting. The process for a review is outlined in Figure 2.



NOTE Numbers refer to the applicable clause in this standard.

IEC

Figure 2 – Implementing the review process

6.2 Planning of the review

Planning starts with defining the purpose of the review, whether it is to be internal or external and the review scope, including whether the review team should make recommendations for solutions to any problems identified or whether the purpose of the review is purely a gap analysis.

The specific objectives depend on the type of review being undertaken and the product, system or process under review. Clear explanations by the chair of objectives and scope of each dependability review will focus attention on the specific areas to be covered and minimize misplaced comments.

6.3 Selection of the review team

Depending on whether the review is internal or performed by an external review team, the conduct of the review and the stances taken by the individuals can vary.

An internal review allows a team or a project team to pause, consider progress and to ensure that activities and outputs are meeting expectations. An external review is more formal and provides an independent assessment to give assurance to the team or the project team itself, to management or to external stakeholders regarding the dependability of an item and the activities being undertaken to achieve it.

The members of the review team can normally include:

- the chair;
- the secretary;
- relevant specialists, not involved in development of the system under review;
- the project or team manager and team members as necessary to present the project or type of review and answer questions.

In some cases, customers or users may also be on the team.

Where the purpose of a review is to approve transition from one stage to another the review team may include those with authority to give this approval.

The project or team manager or those directly involved would not normally chair the reviews and an independent chair should be appointed so that greater benefit can be obtained.

In selecting the review team, care should be taken to avoid conflict of interests, groupthink or vested interests.

The review may include people with specialist knowledge and experience from different spheres. The composition should be such that the participants, collectively, cover a sufficiently wide and detailed field of knowledge to permit consideration of all pertinent aspects of the review. Care should be taken to keep the team to a workable size. Annex D describes the functions and responsibilities of some key persons for a technical review.

6.4 Preparation of the input package

Information should be collected relevant to the review to be undertaken. Examples of the types of information that the input package should contain are provided in Annex E.

6.5 Meeting notification and agenda

The secretary, in conjunction with the chair, should prepare a notification and agenda for the meeting and circulate them to participants and, as applicable, their supervisors, sufficiently in advance of the review to allow participants to prepare for the meeting.

The notification and agenda should state the following:

- date, time and venue of the meeting;
- scope and objectives for the review meeting;
- project name and identification number (if applicable);

- participants and their functions;
- type and duration of the dependability review;
- team or section of the project under review, if appropriate;
- dependability topics to be discussed (see Annex E);
- persons who will make presentations;
- reference documents and contents of any attached input data package.

6.6 Conducting a review meeting

6.6.1 General

If the members are not experienced in reviews, an orientation session should be conducted explaining the general objectives, philosophy and practice.

The introductory comments should set a constructive tone and climate. The chair should review the objectives of the meeting and relate them to the overall objectives and procedures for the review process. The chair should stress the need to ask questions and to avoid negative and personally oriented comments.

Questions that imply pre-judgment should also be avoided.

Review participants should feel free to question their peers. They should not see their responsibility as being solely to ask why something was done in a particular way.

Whenever necessary, the review participants should be assured that all questions raised, subsequent investigations requested, and opinions expressed do not reflect on anyone's personality, ability or integrity. The entire team, under the direction of the chair, should ensure that the review remains proactive, objective and impartial both amongst the team itself and with reference to other involved teams.

The review participants in a technical review should always remember that they serve in an advisory capacity and that their prime purpose is to assist those responsible for the system's design, operation or maintenance in achieving the optimum result. A technical review team would normally provide only recommendations for a solution to any deficiencies identified.

6.6.2 Meeting protocol

The applicable manager and other members representing the responsible team or project may present, as required, aspects of the system's dependability which are under review in a team or project review.

The chair should ensure that the presentation and questioning proceed systematically and that minutes are taken.

The review process is one of constructive questions and answers. Derogatory questions or actions should not be permitted, nor should there be a flat refusal to discuss a topic unless there are specific problems of commercial confidentiality or national security involved. Questions should be framed in terms of requests for information or inquiry as to reasons for team or project decisions.

Review participants can submit questions to the chair in advance to allow for a prepared action. These questions can be considered as complex or minor. To facilitate the progress of the meeting, minor questions should if possible be closed before the start of the meeting. These questions (and answers if known) would then be a part of the meetings input package.

Typographical errors, or minor editorial matters relating to the input data themselves should not be discussed at a review. The secretary should arrange for correction of these as needed. Any substantive corrections should be discussed with review participants.

The review process should not confer approval or disapproval of the team or project documents reviewed.

6.6.3 Action points

Whenever an action is required, the task, the name of the person or persons assigned to undertake the task and the date for response should be recorded in the meeting minutes. Actions should be SMART (Specific, Measurable, Achievable, Realistic and Time-bound).

As a result of action points identified and recommendations made, matters that the chair should consider may include, but are not limited to, the following:

- changes in the system's design concepts, specifications, plans and schedules;
- impact on safety or environmental requirements, system quality, dependability, manufacturing, installation, operation and maintenance procedures, support options and costs.

As the status of the review team is advisory, the team or project manager determines the actual response to any action points.

The responsibility for follow up on the actions and their effects should be defined.

6.6.4 Recommendations

All recommendations should be described in detail in the meeting minutes and related to the original discussion. The reasons for a recommendation should be recorded wherever possible. Recommendations are not the same as action points but actions could result at a later date.

6.6.5 Rejected action points and recommendations

Where there are action points from previous reviews that have not been completed or recommendations that have been rejected, the reasons for inaction or rejection should be explained and documented in the review minutes.

6.6.6 Meeting conclusion

At the conclusion of the meeting the chair should summarize the actions and recommendations arising from the review to ensure a common understanding and agreement by the team.

6.7 Preparing and distributing review minutes

6.7.1 General

The purpose of review meeting minutes is:

- to provide a means for follow-up of actions and recommendations;
- to add to the organization's corporate knowledge and experience.

A record of the state of a design or the status of a project at a point in time adds to the history of the system or project. This can be useful when planning similar designs and projects in the future. A record of the development history of a design or project can also be useful in protecting patent and other property rights or protecting the system and its processes against subsequent inquiry and legal proceedings.

The minutes and supporting documents should be sent to the review members and others as appropriate. These documents should be retained in accordance with the document control procedures for the organization.

As well as the review participants, the review meeting minutes should be sent to the project or team manager, members of the dependability team and others as appropriate.

6.7.2 Minutes

The secretary is responsible for recording important problems, questions and answers, action points and recommendations. Verbatim statements should be discouraged. Sufficient information should be recorded to permit the preparation of a final set of minutes in the required degree of detail.

For the review process to be effective, the subjects and results of discussions during each review need to be documented. This will allow continuity and follow-up until such time as dependability decisions have been made and tasks completed. Sufficient documentation should be contained in the meeting minutes so that successive reviews avoid repeated coverage of the same problems and avoid significant loss of insight or understanding of relevant problems. If continuity and follow-up are achieved, successive review effort can be focused on more relevant problems.

Information contained in the minutes should include the following:

- a copy of the meeting's notification and agenda;
- the list of attendees and their roles;
- identification of the system or process being reviewed including the specific revision status of the reference documents;
- a summary of the findings, an abbreviated schedule of action points and, where appropriate, details of the review;
- pertinent questions and responses;
- a copy of any checklist used, and as appropriate, the answers to questions;
- the list of action points for unresolved questions;
- if an action was assigned, the person to whom responsibility for the action is given;
- if action points were assigned, dates for completion of the action points;
- the list of recommendations;
- from a status review the list of project actions or recommendations requiring priority;
- from a status review the status or disposition of action points and recommendations from previous meetings;
- the list of reference documents.

6.8 Actions and recommendations from a review

Although the review may generate many recommendations, the team or project manager is bound only to review all the recommendations and can reject those that they consider to be not feasible. For example, many recommendations may be wise and of general benefit to the team or project but it is possible that some will, on further examination, prove to be undesirable or impractical.

The person responsible for determining the response to each action and recommendation should consider the desirability and practicality of recommendation of the review team and respond in a timely manner and should:

- provide a response to each of the meeting's actions and recommendations within an agreed time frame;

- take action to resolve any difference of understanding;
- formally advise the chair when actions and recommendations have been addressed and closed if this is appropriate to the organizational arrangement in which the dependability review is held.

6.9 Follow-up and completion of action points and recommendations

The review process is not complete until all action points and recommendations arising from it have been addressed and completed as determined.

Responsibilities and authorities should be allocated for completing the action points, a budget should be provided and time scales specified. This includes defining who has overall responsibility for ensuring actions are completed and closing out the dependability review meeting's action list in the agreed time frame.

When all arising actions and recommendations have been completed, the actions and recommendations list from the minutes of the review should be signed and closed. This should then be lodged with the organization's appropriate manager responsible for dependability activities, in accordance with the organization's procedures.

IECNORM.COM : Click to view the full PDF of IEC 62960:2020

Annex A (informative)

Examples of an input package for a review

A.1 Concept stage

At the concept stage, the input data package should include some or all of the following:

- original requirements: these could include the customer's request for quotes, specifications, standards, regulatory and industry requirements;
- anticipated customer needs and expectations, developed and supported by market surveys and competitors' activities;
- conceptual design assumptions;
- general dependability objectives and requirements;
- reliability database if any exists;
- stakeholder requirements, interface requirements and any modifications that may exist;
- anticipated risks to achieving dependability requirements.

A.2 Development stage

At the development stage, the input data package should include some or all of the following:

- dependability plan;
- documented design assumptions;
- design trade-off studies and analyses;
- a list of any questions from the review team on the design to be reviewed;
- reliability, maintainability and availability allocations and predictions;
- planned maintenance and logistics support;
- designer's proposals and alternative considerations including drawings and calculations;
- information and data on similar systems;
- competitive system data;
- cost estimates and trade-off rationale;
- specifications and drawings;
- results of prototyping;
- reliability database if any exists;
- stakeholder requirements, interface requirements and any modifications that may exist;
- life cycle targets and cost data;
- certification/quality assurance activity requirements;
- project risk management plan/register.

A.3 Realization stage

At the realization stage, the input data package should include some or all of the following:

- manufacturing, tooling and productivity studies;
- status of manufacturing process;

- status of make/buy decisions;
- status of supplier dependability and quality programmes;
- performance test reports, analyses and requirements;
- quality control analyses of processes and supplies;
- inspection reports;
- quality reports for purchased or supplied items;
- reliability database if any exists;
- stakeholder requirements, interface requirements and any modifications that may exist;
- status of installation progress;
- certification/quality assurance activity requirements.

A.4 Utilization stage

At the utilization stage, the input data package should include some or all of the following:

- availability and downtime data linked to production or operations;
- field failure or malfunction and non-conformance reports and trends;
- supportability data for elements of maintenance support such as downtime due to delays in providing resources such as spare parts, skilled manpower and support equipment;
- maintenance costs;
- safety incidents related to system or equipment failure;
- results and recommendations from root cause analyses;
- current maintenance tasks;
- spare parts availability, especially for critical items;
- comparison between expected and actual reliability;
- comparison between expected and actual maintainability;
- reliability database if any exists;
- stakeholder requirements, interface requirements and any modifications that may exist;
- comparison between expected and actual supportability;
- project risk management plan/register.

A.5 Enhancement stage

At the enhancement stage, the input data package will be similar to that for the development phase and should include some or all of the following:

- documented design assumptions;
- design trade-off studies and analyses;
- a list of any questions from the review team on the design to be reviewed;
- reliability, maintainability and availability allocations and predictions;
- planned maintenance and logistics support;
- designer's proposals and alternative considerations including drawings and calculations;
- cost estimates and trade-off rationale;
- reliability database if any exists;
- stakeholder requirements, interface requirements and any modifications that may exist;

- specifications and drawings;
- project risk management plan/register.

A.6 Retirement stage

At the retirement stage, the input data package should include some or all of the following:

- any requirement for interim mothballing/preservation;
- the decommissioning and disposal strategy;
- influence on the environment for disposal of items;
- impact of service termination;
- reliability database if any exists;
- stakeholder requirements, interface requirements and any modifications that may exist;
- schedule and timing for service termination and the new or alternative service provisions;
- project risk management plan/register.

IECNORM.COM : Click to view the full PDF of IEC 62960:2020

Annex B

(informative)

Examples of objectives for dependability reviews during the life cycle

B.1 General

Annex B lists possible objectives to be addressed in dependability reviews at different life cycle stages. The life cycle used is a generic one and the actual application may require a modified set of stages. Some of the bullets below are associated with technical reviews and others with management reviews.

NOTE Annex E lists specific topics around the basic attributes of dependability and associated matters.

B.2 Concept stage

The objectives for a concept review may include the need to:

- assess whether customer requirements have been identified and clarified where necessary;
- assess whether applicable regulatory requirements have been identified;
- assess whether other required technical requirements have been included in the design inputs;
- assess whether organizational and technical interfaces have been identified;
- assess whether risks associated with the design have been assessed.

B.3 Development stage

B.3.1 Conceptual design review

The objectives for a conceptual design review may include the need to:

- interpret, evaluate and agree on customer's requirements, needs, and expectations and on the requirements for the product;
- establish mandatory requirements including regulatory and code requirements, as well as desirable and optional characteristics;
- assess the communication among the members of the project team responsible for design, sales, manufacture, testing, inspection, installation, operation, maintenance, disposal etc.;
- review conditions and technology currently available to satisfy customer, market, environmental and safety requirements;
- review performance, operation and liability information, from the organization's field records on similar products, or from industry;
- review development and design plans and schedules;
- evaluate proposed concepts for the design.

B.3.2 Detail design review

The objectives for a detail design review may include the need to:

- verify that the proposed design continues to satisfy product input requirements;
- confirm that actions and recommendations from previous review(s) have been assessed, addressed and closed;
- examine results of analyses, calculations and tests;

- evaluate the proposed product for cost effectiveness;
- ensure that the product will perform as expected;
- assess whether the proposed product can be manufactured, inspected, assembled with adequate tolerances, stored, shipped and installed reliably and, where relevant, disposed of, all safely, legally and cost effectively;
- review the supporting documentation showing the detail experience and data used in the development of the product;
- evaluate the system design, partitioning of functions (e.g. a reliability block diagram – see IEC 61078 [11]) and the interfaces between modules;
- review component application 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;
- establish a hierarchical ladder of characteristics such as cost, performance, physical parameters, dependability, environmental constraints, delivery requirements and contract incentives from which trade-off decisions can be made to establish mandatory, desirable and optional characteristics.

B.3.3 Final design review

The objectives for a final design review may include the need to:

- verify that the final design contains design input requirements;
- confirm that actions and recommendations from the previous review(s) have been assessed, addressed and closed;
- assess whether any lessons learnt from other projects/designs which were adopted were effective in improving the design;
- review any lessons learnt from other projects/designs which were not adopted, confirm the reasons and what mitigations were put in place to address the issues;
- ensure that detailed analyses, calculations and tests were carried out and that documentation for manufacturing, safety, installation, operation and maintenance of the product was produced in useable form;
- evaluate the final design for life cycle cost-effectiveness;
- verify that the final design can be manufactured, inspected, assembled with adequate tolerances, stored, delivered and installed reliably and where relevant, disposed of, all safely, legally and cost effectively and that it will perform as expected;
- ensure delivery compatibility, quality and dependability of purchased components;
- review supporting documentation showing detailed experience and data used for the design;
- assess the status of the drawing set, software codes and design specifications for completeness and applicability to the intended product or process;
- verify that adequate study was conducted before adoption and incorporation into the design of the accepted recommendations from previous design reviews;
- take into account the lessons learnt for the future design, record reasons or mitigating measures for any identified items that have not been incorporated.

B.4 Realization stage

The objectives for a realization review may include the need to:

- ascertain suppliers' quality, delivery schedule commitments, order processing efficiency, multiple sourcing policy and supply-chain management;
- review risks associated with utilization in the light of actual operating conditions;

- determine quality non-conformance status, assurance effectiveness and quality performance trends, and to identify areas for improvement and recommend management actions;
- ensure proper verification and validation processes, and if appropriate, certification and/or quality assurance activities have been carried out;
- review achieved dependability performance against specifications to provide objective evidence of conformance to specifications;
- review maintenance plans that were created during the development phase to make sure that tasks are achievable and satisfy the design intent.

B.5 Utilization stage

B.5.1 Operation

The objectives for an operation review may include the need to:

- monitor reliability, availability and related dependability problems, all of which aimed to identify the need for design changes;
- monitor failures and non-conformances and trends in dependability measures;
- review production 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;
- determine the health and operational status of an organization, a subsidiary division, a manufacturing plant or a service facility;
- compare actual reliability against expected performance and its impact on availability;
- review customer satisfaction to address user concerns and improvement strategies where dependability could be a significant focus.

B.5.2 Maintenance

The objectives for a maintenance review may include the need to:

- monitor reliability, maintainability, supportability and availability as dependability characteristics and trends to identify the need for design changes to improve maintenance and logistic support programmes;
- evaluate maintenance support and logistics performance of critical items including cost;
- perform a service review to determine customers' service needs, scheduled and unscheduled maintenance activities, third-party service provisions, logistic support, inventory holdings and depot locations.

B.6 Enhancement stage

The objectives for an enhancement review may include the need to:

- consider the value or need for a mid-life enhancement based upon commercial, technical, production, operational feedback, regulatory or code changes;
- check the extent to which the improved design addresses all the issues that lead to a decision to enhance the design;
- check the enhanced design does not introduce new risks;
- ensure the impact of design and other changes do not adversely affect dependability;
- carry out reviews that may be similar to those performed for the development stage.

B.7 Retirement stage

The objectives for a retirement review may include the need to:

- consider the possibility of recycling all or some of the system;
- ensure that disposal and abandonment actions taken meet regulatory and other requirements;
- consider plans that have been made in previous life cycle stages for obsolescence and retirement actions;
- review plans made for decommissioning;
- consider, and if appropriate, apply any required mothballing/preservation activities prior to final disposal;
- learn lessons such that the design of similar items in the future can be improved.

IECNORM.COM : Click to view the full PDF of IEC 62960:2020

Annex C (informative)

Considerations during dependability reviews through the life cycle

C.1 General

The following are general considerations during dependability reviews with examples of dependability related problems that could be reviewed. Some of the points below are associated with technical reviews and others with management reviews. The lists should be tailored to individual circumstances with the agreement of both management and the staff responsible for carrying out dependability activities. The checklists in the examples are general and can require additional specific criteria to enable proper review.

C.2 Examples of dependability review considerations in the concept stage

In the concept stage, the dependability review will normally consider whether the concept is feasible and particularly whether the dependability requirements can be achieved. This could be evaluated based on rational data and analyses by considering the following:

- dependability objectives established are suitable to meet market needs and user applications;
- the extent of market scope and strategy for new initiatives is identified including customer use conditions and market operating conditions, for example climatic conditions;
- the dependability target, competitive leverage, incentives and application constraints are determined;
- the proposed timing for new product introduction and achievement targets is identified;
- tailoring criteria are established and applicable activities are identified;
- information on the proposed new system is adequate to initiate requirements analysis;
- stakeholder input into requirements and design to satisfy requirements has been obtained;
- reliability, maintainability, supportability and availability targets as appropriate are derived from verifiable data and can be quantified or otherwise unambiguously specified;
- risks that need to be taken into account in design have been identified.

It is also important that the following factors are clear:

- the requirements analysis of the system boundaries, operating functions and performance characteristics and technology limitations have been conducted and documented;
- the resource availability, technical capability and new investment needs are identified;
- the technical approaches and feasibility for system realization are identified;
- the potential partnership and supplier requirements are identified;
- the requirements analysis results and rationale can be justified for resource investments to initiate high-level concept design of the new system;
- risks seen from different viewpoints are assessed and taken into account in design selection;
- the significance of the elements of the requirement analysis including system boundaries, the resource availability, the potential partnership and the resource investment as well as the rationale are clear;
- the significance of the different elements of the requirement specifications including the product cost, shipment schedule and environmental conditions as well as the rationale are clear;

- requirements for health, safety and the environment have been identified;
- the health, safety and environmental policy and design targets and the validity of the societal requirements are defined and clarified.

The following points could be used in the dependability review:

- the target for environmental protection, for example rate of reusable parts or recycled materials and energy consumption are clear with verifiable data;
- the architectural design criteria, possible item configuration and options are identified;
- the technology selection for the design of item functions for realization is identified;
- the forecasted probabilistic evaluations are consistent with the dependability targets;
- the make-buy decision criteria are established;
- the means for verification and integration of item functions have been established;
- the criteria for hardware/software design functions have been established;
- the criteria for environmental and ergonomic designs have been established;
- the criteria for evaluation of item functions have been established;
- the interoperability of system functions and performance limits has been verified to meet item requirements;
- the dependability requirements in item specifications are incorporated as guidance for design and COTS acquisition;
- 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;
- risks to performance associated with different designs are evaluated.

C.3 Examples of dependability review considerations in the development stage

During the development stage, the dependability review could consider whether the assumptions made in the design methodology are valid and check the following:

- the customer's requirements for a product are analysed appropriately;
- the product performance and functional requirement specification data are available;
- the link between the requirement specification and the design activities is clearly defined;
- the product's functional design and development reflect the results of relevant analyses;
- the expected dependability performance is produced from design criteria and/or the market research;
- the dependability plan for the design of the item and its components are established;
- the quality assurance plan, obsolescence management plan and item configuration management process are established;
- the item design is verified and support programmes established for full-scale development;
- the tailoring process for various item and functional development projects is implemented and the responsibility for each part of the project assigned, including dependability inputs to the design process;
- the item verification and validation, and if relevant, certification/quality assurance plans have been developed;
- the dependability acceptance criteria and reliability growth programmes have been established;
- the forecasted probabilistic evaluations are consistent with the dependability targets;

- the design has been modified and reliability estimated;
- the verification that the forecasted probabilistic evaluations are consistent with the dependability targets has been performed;
- the predicted product performance and function dependability meet the target objectives;
- test plans and acceptance criteria are established and simulations and tests have been performed;
- the design and experimental results are as forecast;
- the item monitoring and control, incidents reporting and data management systems have been established;
- test results on a prototype confirm that the target functionality is met;
- a series of tests is planned and performed to check the validity of the design and highlight any weaknesses as well as to improve design analysis;
- component application has been reviewed with suppliers;
- the suppliers' dependability programmes have been established;
- a series of tests is planned to demonstrate the dependability of the suppliers' items, confirm the outcome with the suppliers and assess their ability to ensure the dependability;
- revision control of development documentation has been implemented;
- risks to functional and non-functional objectives and to dependability requirements have been assessed and treatment plans specified;
- the item maintenance and logistics support programmes are planned;
- the outsourcing programmes are planned;
- the spares provisioning programme is developed;
- the training programmes are planned;
- the warranty criteria for system service support are established;
- the item is fully developed and ready for production or construction;
- software specifications and flow charts have been finished and approved;
- the development of software module functions and subsystems has been initiated;
- requirements for health, safety and the environment have been analysed and the impact on dependability has been minimized.

C.4 Examples of dependability review considerations in the realization stage

During the realization stage, the dependability review could examine whether the dependability at the time of product introduction is matched to the output of reliability growth trials by checking whether:

- the production of hardware assemblies and functions has been initiated;
- verifiable production data demonstrates the required process maturity and product dependability;
- the assembly process is verified to be straightforward or clearly specified;
- special materials, components and processes are identified and availability and supply stability are verified;
- the reliability at the time of product introduction corresponds to the result of the reliability growth programme to examine whether the dependability achieved meets requirements at the time of product introduction is matched to the output of reliability growth trials (see IEC 61014 [8]);
- the make-buy decisions are established;
- the suppliers' dependability and obsolescence management programmes are implemented;

- the item functions and subsystem verification and validation, and if relevant, certification/quality assurance plans are implemented;
- the failure reporting, analysis and data collection systems are ready;
- it is possible to detect errors prior to product shipment;
- acceptance test conditions and test plans are prepared to ensure dependability;
- the system configuration for the acceptance test has been decided and agreed;
- the system which captures and manages initial failure data in the field functions correctly;
- the training programmes are developed;
- the item is produced, designed and realized in a form ready for implementation.

The installation procedure and support systems can also be verified by considering whether:

- the system integration plan is implemented;
- actions specified to address and control risks have been implemented;
- installation procedures and support systems are verified;
- the item verification and validation plans are implemented;
- the item qualification and acceptance and if relevant, certification/quality assurance plans are implemented;
- the item installation plan is implemented;
- the warranty plan is implemented;
- the training programmes for system operation and customer care services are initiated;
- training of the installation service engineers is complete;
- the process to communicate installation and operating information to the stakeholder, such as user manual, procedures and documents, is prepared and confirmed to be working effectively;
- the required design changes for fulfilling the dependability requirements have been implemented and verified;
- the process to analyse the failure mechanisms in the system and change the design in the development stage and/or the manufacturing procedure in the realization stage, has been prepared and verified;
- the item is ready for release to operation.

C.5 Examples of dependability review considerations in the utilization stage

In the utilization stage, the dependability review could use actual data from the field to consider whether:

- maintenance and support programmes are implemented and are appropriate and effective;
- risks are reassessed in the light of actual conditions;
- the dependability target is measurable from the number of product failures, the frequency of failures and other measures (see IEC 60605-6 [14] and IEC 60300-3-2 [15]);
- the item performance and service maintenance are monitored and controlled;
- facilities are available to receive products returned from the field and to analyse the real cause of failure (may result in "no-fault-found");
- the ability to communicate to the stakeholder about the appropriate usage is available;
- a maintenance plan has been generated and resources to carry it out are allocated (see IEC 60706-2 [10]);

- the maintenance organization has processes in place to verify the maintenance support system;
- the system update plan and the update procedure have been decided;
- the training programmes for operators and maintainers are implemented;
- the field data collection system is implemented;
- the design change and configuration controls are implemented;
- the customer satisfaction survey is implemented;
- the item performance data are analysed for continual improvement;
- the item continues to sustain operational dependability-related performance;
- a process to supply spare parts has been prepared;
- the maintenance system (including spare parts) is available for the required period of time after the sale of the product has ended (see IEC 62402 [6]);
- the product disposal method is defined and the reuse system is prepared and verified in case of reuse;
- the product return process and inspection system are established and verified;
- the reuse and/or recycle system for relevant products is prepared and verified with a guide to the dismantle method;
- the environmental protection targets can be measured with objective data;
- any required (re)certification/quality assurance activities are performed.

C.6 Examples of dependability review considerations in the enhancement stage

During the enhancement stage, the dependability review could consider whether the assumptions of the design methodology are valid and check that:

- the new item features and enhancement needs are identified;
- the requirements and scope of the enhancement are clearly articulated and understood;
- the decision to proceed with enhancement is justified in the light of information relating to design options and risks;
- the enhancement programmes and improvement time frame are determined;
- the results of any customer satisfaction survey resulting from the enhancement programmes are monitored to determine the value of the enhancement;
- specifications of the new design address reasons for enhancing the system;
- risks previously identified are addressed in the design and no new risks are introduced;
- the risk consequences, in particular those related to health, safety, environmental, regulatory and code requirements and the value of the proposed enhancement are assessed;
- change management programmes are in place including necessary communication plans;
- transition from the old to the new design is planned;
- any (re)certification/quality assurance requirements are identified.

Preparations for implementation of the enhancement should be checked including whether:

- the item maintenance and logistics support programmes are planned;
- the outsourcing programmes are planned;
- the training programmes are planned;
- the warranty criteria for system service support are established.

- whether the change achieves its objectives and solves the issues which led to an enhancement being initiated.

In addition, during the enhancement stage, considerations listed in Clause B.3 (the development stage) may be relevant.

C.7 Examples of dependability review considerations in the retirement stage

In the retirement stage, the dependability review would consider whether:

- the decommissioning and disposal, and if relevant, mothballing/preservation strategy is planned and initiated;
- the wear characteristics and the criteria for when to retire the product or system (e.g. dependability, safety, environmental/societal or maintenance costs) are clearly determined and verified with considering the possible recycling and the reuse of items;
- the influence on the environment in the disposal stage satisfies the criteria including legal restrictions;
- in case of components whose disposal lead to environmental, safety or health concerns, the process of collection, disassembly and containment of hazardous remnants has been decided and verified;
- materials and components which may influence the environment have been identified and managed.

In addition, the following points may be considered, as to whether:

- the reuse of components is possible;
- customers have been informed of the schedule and timing for service termination and the new or alternative service provisions have been notified to customers;
- the customer satisfaction survey resulting from termination of the old service and the use of the new service is monitored;
- required data is archived in a way that it is available to those who need it accessible for future operations;
- the impact of service termination is determined.

Lessons learnt and captured are documented and communicated to the future review team.

Annex D

(informative)

Functions and responsibilities of some key persons for a technical review

D.1 General

The members of the technical review team can include, but are not limited to:

- the chair;
- the secretary;
- relevant specialists;
- the project or team manager and members;
- customers or users, in some cases.

Annex D describes functions and responsibilities of these key persons

D.2 Chair

The chair should have broad technical knowledge and experience that includes, as applicable, design, operation and maintenance of the system as well as the ability and confidence to manage personnel and to work equally well with technical and non-technical persons. Leadership and recognized authority within the organization and understanding in dealing with others is of utmost importance.

The chair's responsibilities and authority should include the following:

- to agree to the objectives and scope for the review;
- to agree to the selection of review members in consultation with management;
- to establish meeting agendas for the delegated meeting or meetings;
- to ensure that participants understand what is required of them;
- to ensure that sufficient time is allocated for review activities;
- to ensure that actions identified during the meeting, are SMART and allocated to appropriate meeting attendees;
- to receive and collate questions from review team members ahead of the meeting, to answer them if possible and to ensure questions are added to the meetings input package;
- to ensure that the meeting's input package is issued to designated persons;
- to assign tasks to participants in preparation for meetings;
- to chair the review meeting;
- to ensure that the meeting is conducted in a professional manner;
- to ensure that relevant problems from the meeting are recorded;
- to ensure that actions and recommendations from earlier meetings have been satisfactorily addressed and closed, as appropriate;
- to ensure that the focus of the meeting is the review and not individuals;
- to ensure that there is input from all present;
- to review and approve the review meeting minutes;
- to ensure that the meeting minutes are issued to designated persons;

- to strive for consensus in the review team in case of differences of opinion. If consensus cannot be reached, forward minority as well as majority view(s) for decision.

To maintain the integrity and objectivity of the review team, where possible, the chair should not be associated with the activities being reviewed. However, in a small company, an employee with all necessary qualifications and not participating in some way in the activities might not be available. Consideration should then be given to engaging an outside person. However, the chair should be able to maintain the respect of all participants.

D.3 Secretary

A secretary should be appointed to record the results of the meeting and enable the chair to maintain focus on the meeting. Where possible, the same person should serve as the secretary for all the defined reviews for a specific system. The qualifications and experience for the secretary should be similar to those for the chair but may be less stringent.

The secretary's duties and responsibilities should include the following:

- to send out invitations with sufficient time for members to prepare for the meeting;
- to distribute agendas;
- to follow up on the distribution of input data for review by participants;
- to organize, assemble and distribute responses to enquiries or assignments;
- to take minutes;
- to prepare the meeting minutes;
- to issue the meeting minutes to designated persons in a timely manner;
- to assist the chair in following up action points and recommendations, as applicable.

NOTE If a separate, independent secretary cannot be appointed, it is usually better for a representative from the team to act as the secretary.

If the organization is of sufficient size, the position of secretary can be used as training for future service as review chair. In selecting a secretary, the following factors should be considered:

- previous participation in review activities;
- technical training and comparable experience;
- communication skills;
- involvement in similar activities or projects;
- non-involvement in work on the system or process under review.

D.4 Relevant specialists

Specialists who are not involved in development of the system under review should be selected taking into account the system, the system's objectives and the type of review.

Specialists should be represented on the review team at the appropriate stage in the system's development. Their specializations can include, but are not limited to:

- reliability and maintainability engineering;
- maintenance support and maintenance engineering;
- performance estimation;
- testing and acceptance and/or certification;
- quality management;

- structural engineering;
- manufacturing engineering;
- specialist fields for example mechanical engineering, electrical engineering (analogue, RF (radio frequency), digital), software programming, components and materials;
- functional and personal safety;
- environmental engineering;
- legal matters;
- advertising and marketing;
- finance;
- logistics;
- production and/or operation.

D.5 Project or team manager and members

The project or team manager and/or at least one representative of the project or relevant team need to participate in the whole review in order to explain the rationale of the design decision taken, answer questions and help the review members identify and evaluate potential problems, their probable consequences and possible actions. Representatives should be selected to attend review meetings pertaining to their respective roles during the life cycle processes.

It may not be possible for all designers and specialists to attend throughout in light of team size restrictions. Participants may therefore be invited only to those portions of a meeting that pertain to the area where they should contribute. However, all potential participants should receive the agenda and any portion of the input data package that is relevant to their expertise. Additional representatives from the team can participate as observers where agreed by the chair. These observers do not have the right to speak unless the chair gives permission.

D.6 Customers and users

In some cases, it will be appropriate for customers and/or users to participate in the review meetings to provide input on matters such as:

- user functional and non-functional requirements;
- dependability requirements;
- conditions of use;
- ergonomics and human factors.

Annex E (informative)

Dependability topics for a review

E.1 General

There are a number of specific topics centred around the basic attributes of dependability and associated matters that will generally be the focus for dependability reviews with applicability at all stages of the life cycle.

E.2 Reliability

Points to consider from a reliability viewpoint might include:

- reliability requirements, for example mean operating time between failures (MTBF), mean time to first failure (MTTFF), failure rate, failure probability, expected life;
- comparison of actual or predicted reliability of the product or process at the time of the design review with applicable requirements including assumptions, models and data sources;
- satisfying of reliability and cost objectives within the project plan;
- the most likely causes, for example the top ten, of product failure as identified by failure modes and effects analysis (FMEA IEC 60812 [4]) and/or fault tree analysis (FTA IEC 61025 [5]);
- actions for improving reliability, for example component improvement, substitution and derating, control of environment;
- special manufacturing processes necessary to achieve specified reliability including environmental step stress testing, screening and analyses;
- shipping package, transportation and storage requirements for procured components in relation to product reliability;
- shipping package, transportation and storage constraints affecting overall product reliability;
- comparison of shelf life of the product with requirements, including assumptions, models and data sources;
- reliability history of similar and competitive products or processes;
- effect of installation and maintenance on reliability;
- user's effect on reliability;
- the intended plan for reliability determination and compliance tests, for example number of units, test period, test conditions, life cycle phase for testing.

E.3 Maintainability

Points to consider from a maintainability viewpoint might include:

- maintainability requirements at each maintenance echelon and level of maintenance including any quantitative requirements in terms of mean time to restoration (MTTR) and maintenance man hours (MMH);
- compatibility of maintainability predictions and design with requirements, or comparison of maintainability targets and allocations with observed maintainability;
- maintainability design analyses, for example trade-off analyses between reliability, maintainability, maintenance support performance, accessibility and diagnostic equipment;
- maintainability verification by maintainability demonstration tests;

- maintainability performance history of similar and competitive products or processes.

E.4 Maintenance

Points to consider from a maintenance viewpoint might include:

- review of maintenance policy concerning preventive or corrective maintenance, maintenance echelon and level of maintenance in relation to the specification and operational requirements;
- use of replaceable units: identification, interchangeability benefits and risks, accessibility, removability, shipping package and labelling, test equipment requirements;
- detection and diagnosis of fault by use of built-in, plug-in and general test equipment;
- ease of maintenance and safety of maintenance tasks;
- provision for non-invasive inspection and measurement;
- prediction and avoidance of fault by on-going monitoring of known measurables such as power consumption or vibration.

E.5 Maintenance support

Points to consider from a maintenance support viewpoint might include:

- identification of maintenance support requirements, i.e. resources for satisfying proposed maintenance policy and customer specifications or expectations;
- adequacy of maintenance support plan and identification of interfaces with other engineering tasks;
- maintenance personnel, skills and number;
- specialized diagnostic, repair and test equipment and tools required at each level of maintenance;
- technical manuals, availability and clarity of maintenance and repair procedures;
- facilities needed for repair, storing of spares, material handling, administration and training;
- spare parts initial inventory at each maintenance echelon for corrective and preventive maintenance, availability and time delays in replenishment of spares, including assumptions, models and data sources, shipping package and labelling requirements, for example identification and shelf life;
- the potential for the unavailability of spare parts due to obsolescence;
- performance and maintenance activity reporting system and procedures;
- maintenance and maintenance support experience with earlier and similar products;
- maintenance and maintenance support cost, effect on-cost of ownership – life cycle cost, including identification of most significant cost factors and possible areas for improvement;
- modem or similar network access to machinery for diagnosis by remote experts;
- complete and accurate design documentation and requirements traceability matrix (RTM) for software.

E.6 Availability

Points to consider from an availability viewpoint might include:

- the most likely causes, for example top ten, for the product being down for an unacceptable period as identified by FMEA and/or FTA;
- risk of obsolescence;

- availability requirements, for example mean availability, instantaneous availability, downtime, useful life;
- comparison of predicted availability of the product or process with requirements, including assumptions, models and data sources;
- actions for improving availability, for example modularization, introduction of redundancy, component substitution, derating, control of environment, use of quick disconnects;
- performance history of similar and competitive products;
- effect of operating environment and field service on availability;
- special equipment and tools for operation and maintenance;
- effect of user factors on availability, for example personnel training and availability, equipment misuse, misappropriation of tools and components;
- the intended plan for availability determination and compliance tests, for example number of units, test period, test conditions, life cycle phase for testing.

E.7 Quality assurance

Points to consider from a quality assurance viewpoint might include:

- points pertaining to customer needs and satisfaction:
 - comparison of customer needs with technical specifications for materials, products and processes;
 - validation of design through prototype tests;
 - ability to perform under expected conditions of use and environment;
 - unintended uses and misuses;
 - compliance with regulatory requirements, national and international standards and corporate practices;
 - comparisons with competitive designs;
 - comparison with similar designs, especially analysis of internal and external problem history to avoid repeating problems;
- points pertaining to product specifications and service requirements:
 - permissible tolerances and comparison with process capabilities;
 - acceptance/rejection criteria;
 - ease of assembly and installation, storage needs, shelf life and disposability;
 - benign failure and fail safe characteristics;
 - aesthetic specifications and acceptance criteria;
 - ability to diagnose and solve problems;
 - labelling, warnings, identification, traceability requirements, user instructions and document control;
 - review and use of standard parts;
- points pertaining to process specifications:
 - manufacturability of the design, including special process needs, mechanization, automation, assembly and installation of components;
 - capability to inspect and test the product, including special inspection and test requirements;
 - calibration requirements;
 - specification of materials, components and subassemblies, including approved supplies and suppliers as well as their ability to deliver;

- shipping package, handling, storage and shelf life requirements, especially safety factors relating to incoming and outgoing items;
- points pertaining to design verification:
 - alternative calculations made to verify the correctness of the original calculations and analyses;
 - testing, for example by model or prototype tests, definition of test programmes and documentation of results;
 - independent verification of correctness of original calculations and other design activities;
 - configuration control, adequacy of identification system;
 - serialization or date of manufacture, evaluation and verification of information on product, location of records and cross references, recording of coded or uncoded information.

E.8 Environmental effects

Points to consider from an environment viewpoint might include:

- identification of environmental conditions likely to affect the product or process, such as climatic factors of temperature, humidity, wind and precipitation, effect of radioactivity, chemicals and their reactions over time, dust, fungus, electromagnetic radiation and radio frequency interference;
- determining whether relevant environmental conditions are clearly reflected in the specification;
- determining whether environmental effects on electronic components, mechanical parts, printed board material, connectors, mechanical structures, magnetic media, etc. have been properly considered;
- determining whether the anticipated conditions at the location of use are in agreement with the specification;
- comparing of the actual environmental conditions at the location of use with the conditions anticipated during the development cycle;
- whether the most important environmental parameters (e.g. temperature, humidity) at the location of use should be monitored and to recommend action;
- skill of operating staff to work safely in the environment;
- robustness against external electrical noise and transients of power supply, lightning and facilities for guarding against these disturbances;
- effect of contamination or pollution from water, snow, sand and dust;
- effect of having the product's environmental limits exceeded during maintenance or during an outage condition of the heating/cooling component;
- whether the product needs special environmental protection or qualification testing;

NOTE IEC 60721-2 (all parts) [16] and IEC 60721-3 (all parts) [17] provide relevant guidance on the environmental phenomena to be reviewed.

- laboratory simulation for evaluating product performance under various environmental conditions;
- testing criteria that correlate with actual conditions;
- determination of the adequacy of environmental testing acceleration factors;
- consideration of the normal environment in addition to also considering emergency conditions and the corresponding reduced, but still acceptable, minimum performance in those conditions.

E.9 Product safety

Points to consider from a safety viewpoint might include:

- assurance that emergency cut-off switches, lockout controls, signs, placards, circuit breakers, ground fault interrupters, sensors for fume and smoke and personnel intrusion are appropriately included;
- the intended use of the product, user access and categories, including age groups, user awareness of potential hazards and physical limitations of users;
- environmental conditions, for example temperature ranges, humidity, direct sunlight and rain;
- laws, regulations and standards governing the safety of the design for all locations of use, including during maintenance;
- safety approvals from outside agencies, including certification/quality assurance;
- safety hazards, for example chemical characteristics (corrosiveness, toxicity and flammability), explosion, implosion, electrical shock, fire, overheating, radiation and mechanical characteristics (entrapment and sharp edges);
- risks associated from misuse or abuse;
- contingency of safety on manufacturing or quality control process;
- operator error sensitivity and safety tests performed on the product;
- degradation of product safety between manufacture and use;
- feasibility and adequacy of warnings and instructions on product and in user manual;
- evaluation of purchased components for potential hazards, third party testing and certification;
- evaluation of fail-safe characteristics;
- the need for guarding around all or part of the product, its type and extent.

E.10 Human factors

Points to consider from a human-factors viewpoint might include:

- nature and complexity of the information used by the operator to handle, control and adjust the product or process;
- effectiveness of the information outputs, including the media of presentation, used by the operator to control the product or process;
- behaviour of the product in relation to human expectations and normal and emergency reactions;
- adequacy and suitability of warnings and instructions for operation, installation, maintenance, assembly and disposal;
- review of human interface with operation, maintenance and support requirements in relation to expected and foreseeable environmental conditions (maintenance, markings, work space);
- consideration of operator comfort when using product;
- visibility of instruments associated with product;
- accessibility of product controls;
- evaluation of degree to which the skill and training of likely installers, operators and maintainers has been taken into account in designing the product or process;
- specific evaluation of display requirements (format, number, scrolling);
- ease of use of product software programmes and documentation;

- need for and type of auditory and visual alarms to indicate performance, status and faults, including the recognition of potential for information overload or fatigue for operators;
- review of criteria to improve the adequacy of human performance and to simplify the interaction difficulties between man and the product;
- adequacy, accuracy, ambiguities, ease of use and understanding of all documentation and illustrations required for product operation and maintenance, including the availability in the local language, use of symbols etc.;
- skill of operating staff to be considered in developing training needs;
- potential risk of unskilled operators having access to the product;
- potential difficulty due to operators misusing the product.

E.11 Legal matters

Points to consider from a legal viewpoint might include:

- legal relationship with and obligations owed to buyer, suppliers, subcontractors and end users;
- conformity of proposed design to contract requirements (including specifications);
- conformity of proposed design to the relevant, specific, product-related regulations;
- conformity of proposed delivery schedules to contract requirements;
- determining penalties for non-compliance with contract requirements;
- definition of responsibility for loss during shipment, storage and installation;
- review of ownership and/or licensing of designs, patents, trademarks, trade secrets and tooling;
- review of information concerning reports and legal findings of defects in like, related, or competitive products or processes;
- review of information (e.g. literature, internally generated test data) concerning hazards associated with like, related, or competitive products or processes;
- examining how information concerning reports and legal findings regarding defects and hazards has been taken into account in the design of products or processes;
- determining whether hazards discovered in buyer-specified products have been adequately communicated to the buyer;
- determination of adequacy of communication methods to and from the direct purchaser, end-users and regulatory agencies, if necessary, of hazards discovered after delivery of the product;
- legal considerations affecting whether to recall or retrofit the product;
- adequacy of procedures employed for recall or retrofit programmes (including traceability of components);
- adequacy and comprehensibility of warranty provisions delivered to the customer;
- review of retained records concerning product design, hazard analysis and risk mitigation measures, personnel competence during design, development, manufacture and sale for appropriate content and compliance with legislation and contract provisions;
- adequacy of retention periods of records concerning the product;
- evaluation of data sheets, advertising information, instruction and installation manuals, warnings, labels and other literature for appropriate content and efficacy;
- adequacy of insurance for manufacturer and key personnel on project and facilities utilized;
- evaluation of potential product liability and other legal consequences of use and disposal of the product;
- scrutiny of suppliers' standard terms and conditions, especially any exclusions or limitations;

- evaluation of export restrictions to identified banned countries.

E.12 Durability

Points to consider from a durability viewpoint might include:

- definition of useful life of the item;
- clarification of design target for product useful life;
- definition or clarification of design assumption of operation or usage for overall product life cycle;
- scenario of product life cycle, including normal, abnormal and particular cases;
- type of stress and level prediction;
- adequacy of design specification;
- maintenance strategy, such as replacement, repair, adjustment, and support system preparation;
- estimated limits on economics of operation and maintenance;
- measures of durability, such as time, switching cycles, and referred PoF models;
- required use and operating term, i.e. planned operating time, possible operating time, economical use term, maintenance capable time;
- spare parts requirements prediction;
- obsolescence management strategy and plan;
- policy and planning on obsolescence (see IEC 62402 [6]).

E.13 Security

Points to consider from a security viewpoint might include:

- asset identification, security plan, organization structure and role;
- security policy as formulated and performed by the management;
- guidelines and regulations based on security policy;
- threat analysis;
- incident action process;
- vulnerability analysis and matching of threats to vulnerabilities – a threat is only significant if it aligns with a vulnerability.

E.14 Property damage

Points to consider from a property damage viewpoint might include:

- packaging for protecting products or systems in transit;
- installation of system/products considering environmental conditions and operation conditions;
- insurance for system or products failure or warranty for system reliability and availability;
- insurance for system or products non-operation due to environmental conditions including natural phenomena or disaster.

E.15 Accountability

Points to consider from an accountability viewpoint might include:

- definition, documentation and understanding of accountability;
- individual, as well as company/corporate accountability;
- requirement of the system, product, process or service;
- setting appropriate boundaries for stakeholders;
- activities and tasks for the system operations and process;
- activities for checking the required actions implemented.

IECNORM.COM : Click to view the full PDF of IEC 62960:2020

Bibliography

- [1] IEC 60300-1:2014, *Dependability management – Part 1: Guidance for management and application*
- [2] IEC 60300-3-3:2017, *Dependability management – Part 3-3: Application guide – Life cycle costing*
- [3] IEC 62741:2015, *Demonstration of dependability requirements – The dependability case*
- [4] IEC 60812, *Failure modes and effects analysis (FMEA and FMECA)*
- [5] IEC 61025:2006, *Fault tree analysis (FTA)*
- [6] IEC 62402:2019, *Obsolescence management*
- [7] IEC 62740:2015, *Root cause analysis (RCA)*
- [8] IEC 61014:2003, *Programmes for reliability growth*
- [9] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*
- [10] IEC 60706-2:2006, *Maintainability of equipment – Part 2: Maintainability requirements and studies during the design and development phase*
- [11] IEC 61078:2016, *Reliability block diagrams*
- [12] IEC 62853:2018, *Open systems dependability*
- [13] IEC 31010:2019, *Risk management – Risk assessment techniques*
- [14] IEC 60605-6:2007, *Equipment reliability testing – Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity*
- [15] IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*
- [16] IEC 60721-2 (all parts), *Classification of environmental conditions – Part 2: Environmental conditions appearing in nature*
- [17] IEC 60721-3 (all parts), *Classification of environmental conditions – Part 3: Classification of groups of environmental parameters and their severities*
- [18] ISO/IEC 20000-1:2018, *Information technology – Service management – Part 1: Service management system requirements*
- [19] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*
- [20] ISO/IEC 20246:2017, *Software and systems engineering – Work product reviews*
- [21] IEC/ISO/IEEE 15288:2015, *Systems and software engineering – System life cycle processes*

[22] ISO 9000:2015, *Quality management systems – Fundamentals and vocabulary*

[23] ISO Guide 73:2009, *Risk management – Vocabulary*

IECNORM.COM : Click to view the full PDF of IEC 62960:2020

SOMMAIRE

AVANT-PROPOS	59
INTRODUCTION.....	61
1 Domaine d'application	62
2 Références normatives	62
3 Termes et définitions	62
3.1 Termes et définitions	62
3.2 Termes abrégés.....	66
4 Introduction des revues de la sûreté de fonctionnement	66
4.1 Généralités	66
4.2 Revues techniques	67
4.3 Revues d'état.....	68
4.4 Vue d'ensemble de la méthode de revue de la sûreté de fonctionnement.....	69
4.4.1 Vue d'ensemble	69
4.4.2 Identification des parties prenantes	69
4.4.3 Identification des exigences.....	70
4.4.4 Collecte d'informations sur les performances réelles	70
4.4.5 Evaluation de l'écart entre les exigences et les performances réelles	70
4.4.6 Identification des risques et des secteurs critiques	71
4.4.7 Recommandation d'actions	71
4.5 Planification et définition de la fréquence des revues de la sûreté de fonctionnement	71
4.6 Niveaux des revues de la sûreté de fonctionnement.....	73
4.6.1 Vue d'ensemble	73
4.6.2 Revues d'équipe	74
4.6.3 Revues de projet	74
4.6.4 Revues d'état	75
5 Activités impliquées dans les revues de la sûreté de fonctionnement au cours du cycle de vie	75
5.1 Généralités	75
5.2 Phase de conception.....	76
5.3 Phase de développement.....	77
5.3.1 Vue d'ensemble	77
5.3.2 Revues de conception	77
5.4 Phase de réalisation	79
5.5 Phase d'utilisation.....	80
5.6 Phase d'amélioration.....	80
5.7 Phase de mise hors service	81
6 Mise en œuvre du processus de revue de la sûreté de fonctionnement	81
6.1 Généralités	81
6.2 Planification de la revue.....	82
6.3 Choix de l'équipe de revue.....	82
6.4 Préparation de la documentation d'entrée	82
6.5 Notification et ordre du jour des réunions	83
6.6 Conduite d'une réunion de revue.....	83
6.6.1 Généralités	83
6.6.2 Protocole de réunion	83
6.6.3 Eléments d'action	84

6.6.4	Recommandations	84
6.6.5	Refus d'éléments d'action et de recommandations	84
6.6.6	Conclusion de la réunion	85
6.7	Préparation et diffusion des procès-verbaux	85
6.7.1	Généralités	85
6.7.2	Procès-verbaux	85
6.8	Actions et recommandations établies au terme d'une revue	86
6.9	Suivi et exécution des éléments d'action et des recommandations	86
Annexe A	(informative) Exemples de documentation d'entrée d'une revue	87
A.1	Phase de conception	87
A.2	Phase de développement	87
A.3	Phase de réalisation	88
A.4	Phase d'utilisation	88
A.5	Phase d'amélioration	88
A.6	Phase de mise hors service	89
Annexe B	(informative) Exemples d'objectifs des revues de la sûreté de fonctionnement au cours du cycle de vie	90
B.1	Généralités	90
B.2	Phase de conception	90
B.3	Phase de développement	90
B.3.1	Revue d'étude conceptuelle	90
B.3.2	Revue de conception détaillée	90
B.3.3	Revue de conception finale	91
B.4	Phase de réalisation	92
B.5	Phase d'utilisation	92
B.5.1	Exploitation	92
B.5.2	Maintenance	92
B.6	Phase d'amélioration	93
B.7	Phase de mise hors service	93
Annexe C	(informative) Aspects à prendre en compte lors des revues de la sûreté de fonctionnement au cours du cycle de vie	94
C.1	Généralités	94
C.2	Exemples d'aspects à prendre en compte lors d'une revue de la sûreté de fonctionnement au cours de la phase de conception	94
C.3	Exemples d'aspects à prendre en compte lors d'une revue de la sûreté de fonctionnement au cours de la phase de développement	95
C.4	Exemples d'aspects à prendre en compte lors d'une revue de la sûreté de fonctionnement au cours de la phase de réalisation	97
C.5	Exemples d'aspects à prendre en compte lors d'une revue de la sûreté de fonctionnement au cours de la phase d'utilisation	98
C.6	Exemples d'aspects à prendre en compte lors d'une revue de la sûreté de fonctionnement au cours de la phase d'amélioration	99
C.7	Exemples d'aspects à prendre en compte lors d'une revue de la sûreté de fonctionnement au cours de la phase de mise hors service	100
Annexe D	(informative) Fonctions et responsabilités de certains intervenants stratégiques dans une revue technique	101
D.1	Généralités	101
D.2	Président	101
D.3	Secrétaire	102
D.4	Spécialistes compétents	102

D.5	Responsable et membres du projet ou de l'équipe	103
D.6	Clients et utilisateurs	103
Annexe E (informative) Sujets couverts au cours d'une revue de la sûreté de fonctionnement		104
E.1	Généralités	104
E.2	Fiabilité	104
E.3	Maintenabilité	104
E.4	Maintenance	105
E.5	Logistique de maintenance	105
E.6	Disponibilité	106
E.7	Assurance de la qualité	106
E.8	Effets environnementaux	107
E.9	Sûreté des produits	108
E.10	Facteurs humains	109
E.11	Questions juridiques	109
E.12	Durabilité	110
E.13	Sécurité	111
E.14	Domages matériels	111
E.15	Responsabilité	111
Bibliographie		112
Figure 1 – Déroulement logique des revues au cours d'une étape du cycle de vie		74
Figure 2 – Mise en œuvre du processus de revue		81

IECNORM.COM : Click to view the full PDF of IEC 62960:2020

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**REVUES DE LA SÛRETÉ DE FONCTIONNEMENT
AU COURS DU CYCLE DE VIE****AVANT-PROPOS**

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

La Norme internationale IEC 62960 a été établie par le comité d'études 56 de l'IEC: Sûreté de fonctionnement.

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

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

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette Norme internationale.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

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

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo '*colour inside*' qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

IECNORM.COM : Click to view the full PDF of IEC 62960:2020

INTRODUCTION

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

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

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

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

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

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

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

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

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

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

1 Domaine d'application

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

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

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

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

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60050-192, *Vocabulaire électrotechnique international – Partie 192: Sûreté de fonctionnement* (disponible à l'adresse <http://www.electropedia.org>)

3 Termes et définitions

3.1 Termes et définitions

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

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

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

3.1.1

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.

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

3.1.2

plan de sûreté de fonctionnement

ensemble d'activités planifiées dont la réalisation permet d'atteindre les objectifs de sûreté de fonctionnement d'une entité

[SOURCE: IEC 60300-1:2014, 3.1.6, modifié – "dont la réalisation" ajouté.]

3.1.3

revue de la sûreté de fonctionnement

revue axée sur les aspects liés à la sûreté de fonctionnement d'une entité, d'un système ou d'un processus faisant l'objet d'une revue

Note 1 à l'article: Une revue de la sûreté de fonctionnement peut prendre la forme d'une revue indépendante ou être intégrée à une revue plus vaste couvrant d'autres aspects.

3.1.4

revue de conception

revue planifiée et documentée d'une conception existante ou d'une proposition de conception

Note 1 à l'article: Une revue de conception a notamment pour objectif d'évaluer l'aptitude d'une conception à satisfaire aux exigences spécifiées, d'identifier toute lacune réelle ou potentielle et de proposer des améliorations.

Note 2 à l'article: La revue de conception ne suffit pas en soi à garantir une conception appropriée.

Note 3 à l'article: La conception peut concerner un produit ou un processus.

Note 4 à l'article: La revue de conception peut être réalisée par le biais d'une réunion ou par un autre processus documenté.

3.1.5

analyse des écarts

méthode visant à comparer les réalisations obtenues avec les exigences initiales afin d'identifier les écarts et d'apporter des améliorations

3.1.6

entité

sujet que l'on considère

Note 1 à l'article: L'entité peut être une pièce isolée, un composant, un dispositif, une unité fonctionnelle, un équipement, un sous-système ou un système.

Note 2 à l'article: L'entité peut être composée de matériel, de logiciel, de personnel ou d'une quelconque de leurs combinaisons.

Note 3 à l'article: L'entité est souvent composée d'éléments dont chacun peut être considéré individuellement.

[SOURCE: IEC 60050-192:2015, 192-01-01, modifié – La Note 3 a été modifiée par l'omission des références internes et les Notes 4 et 5 ont été supprimées.]

3.1.7

cycle de vie

suite des étapes identifiables que traverse une entité, de sa conception à sa mise au rebut

EXEMPLE Le cycle de vie classique d'un système comprend les phases suivantes: faisabilité et définition, conception et développement, fabrication et mise en service, exploitation et maintenance, rénovation en cours de vie ou prolongation de la durée de vie, mise hors service et mise au rebut.

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

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

3.1.8

management

activités coordonnées pour orienter et diriger un organisme

Note 1 à l'article: Le management peut inclure l'établissement de politiques et d'objectifs, et de processus pour atteindre ces objectifs.

Note 2 à l'article: En français, le terme "management" désigne parfois des personnes, c'est-à-dire une personne ou un groupe de personnes ayant les responsabilités et les pouvoirs nécessaires pour la conduite et la maîtrise d'un organisme. Lorsque le terme "management" est utilisé dans ce sens, il convient toujours de l'associer à une certaine forme de qualificatif pour éviter toute confusion avec le concept de "management" défini ci-dessus en tant qu'ensemble d'activités. Par exemple, l'expression "le management doit..." est déconseillée alors que l'expression "la direction doit..." est acceptable. Sinon, il convient d'employer d'autres termes pour exprimer le concept lorsqu'il se rapporte à des personnes, par exemple managers ou dirigeants.

[SOURCE: ISO 9000:2015, 3.3.3]

3.1.9

projet

processus unique qui consiste en un ensemble d'activités coordonnées et maîtrisées comportant des dates de début et de fin, entrepris dans le but d'atteindre un objectif conforme à des exigences spécifiques, incluant les contraintes de délais, de coûts et de ressources

Note 1 à l'article: L'organisme du projet est normalement temporaire et n'est mis en place que pour la durée de vie du projet.

Note 2 à l'article: La complexité des interactions entre les activités du projet n'est pas nécessairement liée à la taille du projet.

[SOURCE: ISO 9000:2015, 3.4.2, modifié – Les Notes 1 à 3 ont été supprimées.]

3.1.10

jalon du projet

point spécifique et prédéterminé au cours d'un projet correspondant à un moment auquel certains livrables sont censés avoir été atteints ou auquel un niveau de progression mesurable doit être attendu

3.1.11

revue de projet

revue des résultats du projet

3.1.12

revue

activité entreprise afin de déterminer l'adaptation, l'adéquation et l'efficacité de l'objet étudié pour atteindre les objectifs établis

[SOURCE: Guide ISO 73:2009, 3.8.2.2, modifié – La Note a été supprimée.]

3.1.13**partie prenante**

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

Note 1 à l'article: Cette définition couvre un domaine plus large que celle de l'IEC/ISO/IEEE 15288:2015.

[SOURCE: IEC 60300-1:2014, 3.1.5, modifié – La Note 1 a été ajoutée.]

3.1.14**revue d'état**

revue de l'état global d'un projet par rapport aux objectifs établis

Note 1 à l'article: La revue d'état se compose d'une partie technique, dans laquelle les informations d'état sont recueillies et structurées, et d'une partie management au cours de laquelle l'état est déterminé et les décisions appropriées sont prises.

3.1.15**système**

<en sûreté de fonctionnement> ensemble d'entités reliées entre elles qui satisfont collectivement à une exigence

Note 1 à l'article: Un système est considéré comme ayant une frontière définie, réelle ou abstraite.

Note 2 à l'article: Des ressources externes (provenant d'au-delà de la frontière) peuvent être nécessaires au fonctionnement du système.

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

Note 4 à l'article: Il convient d'exprimer ou de sous-entendre les conditions d'utilisation et de maintenance dans l'exigence.

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

3.1.16**équipe**

deux personnes ou plus travaillant ensemble et disposant d'un ensemble de compétences complémentaires nécessaires à la réalisation d'une tâche

Note 1 à l'article: Un membre de l'équipe est désigné comme responsable d'équipe.

Note 2 à l'article: L'équipe peut comprendre des personnes en formation.

3.1.17**revue d'équipe**

revue des résultats de l'équipe

EXEMPLE L'équipe mécanique, l'équipe électronique ou l'équipe logiciel servent d'éléments d'entrée pour la partie technique de la revue d'état.

3.1.18**revue technique**

revue des aspects techniques d'un processus ou d'un produit par une équipe de personnel techniquement qualifié, consistant à examiner l'adéquation du produit à son utilisation prévue et à identifier les risques et les écarts par rapport aux spécifications et normes établies

Note 1 à l'article: Les sujets dont les aspects techniques peuvent faire l'objet d'une revue incluent l'application d'une nouvelle technologie, la diversification de la gamme de produits, les décisions "fabriquer ou acheter", le calendrier du lancement de nouveaux produits et la revue de la pertinence/adéquation de la spécification technique.

[SOURCE: En anglais ISO/IEC 20246:2017, 3.18]

3.2 Termes abrégés

COTS	commercial-off-the-shelf (produits du commerce)
AMDE	analyse des modes de défaillances et de leurs effets
AAP	analyse par arbre de panne
MMH	maintenance man hours (durée équivalente de maintenance)
MTBF	mean operating time between failures (temps moyen entre défaillances)
MTTF	mean time to first failure (temps moyen de fonctionnement avant la première défaillance)
MTTR	mean time to restoration (temps moyen de restauration)
PoF	physics of failure (propriétés physiques de la défaillance)
RTM	requirements traceability matrix (matrice de traçabilité des exigences)

4 Introduction des revues de la sûreté de fonctionnement

4.1 Généralités

Les revues de la sûreté de fonctionnement constituent des activités essentielles du plan de sûreté de fonctionnement. Les personnes chargées des revues de la sûreté de fonctionnement ont la responsabilité de s'assurer que des revues de la sûreté de fonctionnement sont bien effectuées au cours du cycle de vie.

Les revues impliquent d'examiner la situation actuelle afin de la comparer aux attentes ou exigences. Les revues permettent d'identifier les écarts, les risques et les problèmes potentiels, avant de les analyser et de recommander des améliorations.

Les revues de la sûreté de fonctionnement comprennent un ensemble cohérent de revues couvrant différents aspects de la sûreté de fonctionnement. Ces revues sont répétées tout au long du cycle de vie, de manière à fournir continuellement des actions de suivi et à en évaluer l'efficacité.

Les revues de la sûreté de fonctionnement peuvent être réalisées selon différents points de vue, tels que:

- les attributs de sûreté de fonctionnement d'une entité, notamment la fiabilité, la maintenabilité, la supportabilité et la disponibilité;
- d'autres caractéristiques temporelles d'une entité, telles que la durabilité et la récupérabilité;
- les fonctions associées à la sûreté de fonctionnement, telles que la sûreté et la sécurité;
- la rentabilité, y compris les coûts du cycle de vie et les coûts à court terme;
- les activités réalisées pour atteindre ou évaluer les résultats de la sûreté de fonctionnement;
- l'efficacité des processus de sûreté de fonctionnement;
- la responsabilité, dans le cadre des défaillances potentielles, des différentes parties prenantes et la responsabilité vis-à-vis de ces dernières;
- l'adaptation aux changements d'exigences, d'environnements, d'objectifs et/ou de finalité du système.

Une revue de la sûreté de fonctionnement permet de garantir la sûreté de fonctionnement tout au long du cycle de vie, soit en démontrant que les exigences sont respectées, soit en identifiant les problèmes et en apportant des améliorations. Une revue de la sûreté de fonctionnement peut être utilisée pour apporter la preuve qu'une revendication de sûreté de fonctionnement est satisfaite dans le cadre d'un dossier de sûreté de fonctionnement (l'IEC 62741[3]¹ fournit des

¹ Les chiffres entre crochets se réfèrent à la Bibliographie.

recommandations sur le contenu d'un dossier de sûreté de fonctionnement et établit les principes généraux relatifs à son élaboration).

La mise en place de revues systématiques de la sûreté de fonctionnement sur l'ensemble du cycle de vie d'un système permet de réorienter les efforts d'une manière agile, en limitant les pertes. Cela se révèle particulièrement utile au vu des tendances actuelles, à savoir la complexité croissante des systèmes, la réduction des délais de développement et l'allongement des durées de vie en service.

Plusieurs environnements ou conditions sont à l'origine de ces tendances:

- l'extension des connexions réseau à une grande diversité de systèmes contrôlés par des tiers;
- les variations fréquentes dans le contexte du système, telles que les attentes des utilisateurs et la concurrence sur le marché;
- l'incapacité à renoncer aux anciens systèmes et à se tourner vers une nouvelle approche, par exemple pour des raisons de coûts ou par intérêt pour "l'économie circulaire".

Les revues de la sûreté de fonctionnement contribuent à identifier, prévoir et corriger les problèmes survenant au cours du cycle de vie du système tant qu'ils demeurent suffisamment mineurs pour être traités.

Il existe différents types de revues de la sûreté de fonctionnement. Il convient que le type de revue réalisé à une étape donnée du cycle de vie soit adapté à l'étape en question. L'idéal en matière de management et de documentation est d'utiliser un plan de sûreté de fonctionnement. Les activités de revue de la sûreté de fonctionnement entreprises pendant le cycle de vie sont décrites à l'Article 5.

Une revue peut être organisée en interne, auquel cas l'équipe de revue est constituée de personnes étroitement impliquées dans l'objet de la revue, ou peut prendre la forme d'une revue externe, l'équipe de revue ne comprenant alors que des personnes indépendantes. Dans ce cas, l'équipe faisant l'objet de la revue communique des éléments de preuve à l'équipe de revue externe.

Les problèmes de management, tels que l'attribution des responsabilités et les changements d'objectifs métier, ont des conséquences sur la sûreté de fonctionnement. De tels problèmes peuvent de ce fait être rattachés à une revue de la sûreté de fonctionnement. Dans ce cas, des experts techniques tout comme des responsables peuvent être impliqués.

Les revues de la sûreté de fonctionnement peuvent être classées en deux catégories: les revues techniques et les revues de management. Les principes du présent document peuvent s'appliquer indifféremment à tous les types de revues. Le présent document se concentre cependant davantage sur les revues techniques. Il ne couvre pas la partie management de la revue d'état. Les revues techniques et les revues de management sont organisées à chaque étape du cycle de vie, souvent dans le cadre d'autres revues plutôt que sous la forme d'activités indépendantes. Le 4.2 et le 4.3 décrivent les revues techniques et les revues d'état.

4.2 Revues techniques

Les revues techniques permettent d'identifier et d'analyser les problèmes potentiels et les perspectives, et de recommander des actions d'amélioration. Elles offrent également la garantie que les processus fonctionnent efficacement et que les exigences sont respectées.

Les revues techniques peuvent inclure des revues de conception, des revues d'exploitation, des revues de maintenance, des revues des risques ou encore des revues portant sur d'autres aspects techniques d'une entité ou d'un processus. Elles peuvent se concentrer sur la sûreté de fonctionnement, mais la sûreté de fonctionnement peut également être envisagée dans le cadre d'une revue de performances à plus grande échelle.

Les revues techniques de la sûreté de fonctionnement peuvent comprendre:

- les revues de réalisation ou de prévision de la sûreté de fonctionnement d'une entité, dans le but d'améliorer la sûreté de fonctionnement de l'entité elle-même en évaluant les mesures de sûreté de fonctionnement et en explorant les possibilités d'amélioration;
- les revues des processus et activités planifiés dans le cadre de la sûreté de fonctionnement, afin d'en tirer des enseignements et d'améliorer les futurs processus et activités.

Il convient que les participants acquièrent une compréhension technique du système faisant l'objet d'une revue et qu'ils maîtrisent les notions de fiabilité, de maintenance et de supportabilité.

Il convient d'inclure parmi les participants des experts qui ne sont pas intervenus dans la conception du système et qui disposent des compétences nécessaires pour analyser les modes de défaillance possibles des entités, systèmes et processus. La participation de tels experts est des plus importantes pour garantir l'indépendance et la qualité de la revue. Des professionnels de la qualité, des professionnels de la fiabilité, des professionnels de l'ergonomie, des analystes de sécurité et du personnel d'essai, par exemple, peuvent participer en qualité d'experts.

Il convient généralement que les membres de la direction ne prennent pas part à une revue technique. Le client ou l'utilisateur du système ou du processus peut participer à une revue technique.

Il convient, pour chaque revue technique, de désigner un président de la réunion (l'animateur), lequel peut nommer un secrétaire afin de l'assister.

4.3 Revues d'état

L'objectif d'une revue d'état est de fournir au groupe dirigeant, et parfois au client, des informations relatives à la progression d'un projet et, dans certains cas, d'autoriser le passage du projet à la phase suivante du plan de projet. Certaines revues d'état sont organisées à des jalons du projet et sont appelées "revues de jalon". Certaines revues de jalon impliquent également une décision quant au fait de pouvoir poursuivre ou non le projet, auquel cas elles peuvent désignées sous le nom de "revues de validation". Dans certains cas, les résultats de la revue d'état influent sur le paiement partiel demandé.

Une revue d'état de la sûreté de fonctionnement commence par une phase de collecte et de structuration des informations et preuves liées à la sûreté de fonctionnement. Les informations structurées sont ensuite présentées à la direction pour examen et sanction.

Il convient d'intégrer dans l'équipe participant à une revue d'état des personnes habilitées à affecter des ressources au projet et à éliminer les obstacles. Les participants à la partie technique de la revue d'état sont généralement le président, le secrétaire, les responsables de projet et les responsables d'équipe des différentes équipes de projet. Lorsque l'état des problèmes techniques a été approuvé de manière consensuelle, la revue d'état peut passer à la phase de management, à laquelle participent généralement le responsable de programme, la direction et éventuellement le client. Il convient de veiller à ne transférer à la phase suivante du projet aucun problème grave signalé par les responsables d'équipe au cours de la revue de projet, à moins d'en indiquer l'impact potentiel, si le problème n'est pas résolu.

4.4 Vue d'ensemble de la méthode de revue de la sûreté de fonctionnement

4.4.1 Vue d'ensemble

La sûreté de fonctionnement peut faire l'objet d'une revue distincte ou être comprise dans d'autres revues. Dans les deux cas, il convient de décomposer la revue de la sûreté de fonctionnement en différentes étapes:

- identification des parties prenantes;
- identification des exigences;
- collecte d'informations sur les performances réelles;
- évaluation de l'écart entre les exigences et les performances réelles;
- identification des risques et des secteurs critiques;
- recommandation d'actions.

Si des modifications sont apportées, il convient de vérifier leur efficacité et d'émettre un jugement quant à la nécessité d'entreprendre une ou plusieurs actions supplémentaires.

4.4.2 Identification des parties prenantes

Il est important que les personnes ou organisations qui développent et exploitent des systèmes reconnaissent clairement leurs parties prenantes, dans la mesure où elles ont pour principal objectif de satisfaire aux besoins de ces parties prenantes. Il convient donc d'identifier les parties prenantes et d'établir des moyens pour communiquer avec elles. Pour certains systèmes, l'identification des parties prenantes est relativement aisée, celles-ci n'évoluant pas au cours du cycle de vie. Pour d'autres systèmes, il peut être difficile d'identifier immédiatement toutes les parties prenantes et de déterminer leurs besoins de manière exhaustive. Par exemple, les parties prenantes peuvent évoluer lorsqu'un système entre en phase d'utilisation ou lorsqu'une entité développée est vendue à une personne différente ou à une autre organisation. Elles peuvent également évoluer lorsqu'un système entre en phase de mise hors service.

Pour identifier les parties prenantes concernées, il convient de tenir compte des points suivants:

- a) Sont comprises dans les parties prenantes celles qui peuvent être affectées par le système ou par une défaillance du système, par exemple par une divulgation non autorisée d'informations ou par des dysfonctionnements provoqués par des erreurs humaines ou une mauvaise utilisation.
- b) Certaines exigences des parties prenantes qui, par exemple, peuvent être à l'origine de défaillances lors du développement et de retards de livraison, peuvent être connues pendant le développement et il convient de les identifier et de les prendre en compte dans les revues.
- c) Après identification des parties prenantes concernées, il convient d'identifier les parties prenantes clés parmi celles-ci. Il convient de suivre une approche fondée sur le risque pour déterminer les parties prenantes clés. Les critères de détermination des parties prenantes réputées clés varient, en fonction des critères de réussite identifiés pour le système et selon le degré d'importance et l'influence de chaque partie prenante.
- d) La liste des parties prenantes peut évoluer lorsque le système passe aux phases d'utilisation ou de mise hors service. Par exemple:
 - 1) une entité développée peut être vendue à une personne différente ou à une autre organisation, admise par hypothèse lors des phases de développement ou de réalisation;
 - 2) une entité développée peut être utilisée par différentes personnes ou par la même organisation en interne.

4.4.3 Identification des exigences

Pour remplir les objectifs de sûreté de fonctionnement et atteindre le niveau de sûreté de fonctionnement attendu par les parties prenantes, il est utile de spécifier une finalité réalisable, accompagnée d'objectifs et d'activités mesurables et d'un plan d'action adapté pendant le cycle de vie. Ces éléments peuvent constituer les exigences servant de base aux revues. La finalité peut se rapporter à la fois à la fonctionnalité attendue du système et aux performances souhaitées. Les parties prenantes ou organisations intéressées par la sûreté de fonctionnement du système peuvent présenter des ordres du jour différents et peuvent varier ou non tout au long du cycle de vie. Par conséquent, il peut être nécessaire de revoir les objectifs et les finalités à chaque étape et de les adapter si besoin est. De nouveaux plans sont générés et exécutés étape par étape afin d'atteindre les objectifs, et les résultats sont passés en revue sous l'angle de la sûreté de fonctionnement. Le niveau relatif d'importance des parties prenantes pour la réussite du projet telle qu'elle est perçue peut varier. Par conséquent, cela peut avoir une influence sur le contenu des plans, compte tenu de leur importance relative.

Il convient de clarifier la finalité de la sûreté de fonctionnement par rapport aux détails de la spécification du système et au plan de projet. Cette finalité peut tenir compte des possibilités techniques, des risques, de la suffisance de chaque étape du cycle de vie et des exigences pertinentes obtenues à partir des résultats d'études de marché.

4.4.4 Collecte d'informations sur les performances réelles

Il convient de recueillir des preuves suffisantes sur la situation réelle pour permettre de tirer des conclusions fiables lors de la revue. Les preuves sont constituées d'informations destinées à être comparées avec chaque exigence, chaque objectif et chaque livrable compris dans le domaine d'application de la revue. Ces preuves peuvent comprendre des calculs de résultats d'essais, des simulations et d'autres analyses. Il convient d'évaluer tous les problèmes rencontrés, secteurs critiques ou fonctionnalités susceptibles d'avoir un impact sur les risques. L'Annexe A apporte des précisions sur certaines informations pouvant être collectées. L'incertitude du résultat de la revue est ainsi réduite le plus possible.

Si les preuves sont insuffisantes, soit parce qu'elles sont incomplètes, soit parce qu'elles ne présentent pas une qualité adéquate, ou si la compréhension et l'analyse de ces preuves sont incomplètes, il est probable que les résultats de la revue manquent de fiabilité ou d'exhaustivité. Dans ce cas, il convient de prendre des mesures soit pour obtenir davantage de preuves ou des preuves de meilleure qualité, soit pour en améliorer la compréhension.

Des preuves recueillies pour un dossier de sûreté de fonctionnement peuvent également être utilisées comme preuves dans le cadre d'une revue de la sûreté de fonctionnement. De même, les preuves d'une revue peuvent faire partie d'un dossier de sûreté de fonctionnement.

L'IEC 62741 [3] fournit des recommandations concernant le contenu et l'application d'un dossier de sûreté de fonctionnement et établit les principes généraux relatifs à son élaboration. Ces recommandations s'inscrivent dans le contexte d'un projet élémentaire, dans lequel un client commande un système qui satisfait aux exigences de sûreté de fonctionnement d'un fournisseur et gère ensuite le système jusqu'à sa mise hors service. Les méthodes fournies dans le présent document peuvent être si besoin modifiées et adaptées à d'autres situations. Les informations sont normalement définies et produites dans le cadre d'une coopération entre le client et le fournisseur, mais elles peuvent également être utilisées et mises à jour par d'autres organisations. Par exemple, des organismes de certification et de réglementation peuvent examiner le dossier soumis pour étayer leurs décisions, et les utilisateurs du système peuvent mettre à jour le dossier ou en élargir la portée, notamment lorsqu'ils utilisent le système à d'autres fins.

4.4.5 Evaluation de l'écart entre les exigences et les performances réelles

Il convient d'identifier les écarts entre le résultat réel et les attentes ou les exigences, d'évaluer l'importance de tout écart, d'identifier les actions correctives possibles et de prendre une décision quant à la nécessité d'entreprendre une action corrective.

Cela peut impliquer une analyse des causes d'écarts. Des techniques telles que l'analyse de cause initiale décrite dans l'IEC 62740 [7] peuvent être utilisées.

4.4.6 Identification des risques et des secteurs critiques

La revue peut également permettre d'identifier les secteurs critiques et les futurs problèmes potentiels, d'examiner les risques précédemment identifiés et d'évaluer les nouveaux risques. Des techniques telles que celles décrites dans l'IEC 31010 [13] peuvent être utilisées.

En outre, il est probable que des risques pour la sûreté de fonctionnement soient identifiés au cours des évaluations des risques entreprises à chaque étape du cycle de vie, dans d'autres contextes qu'une revue de la sûreté de fonctionnement. De la même façon, les résultats des revues des risques fournissent des informations sur les progrès réalisés pour le traitement de ces risques. Il convient d'intégrer ces informations aux revues de la sûreté de fonctionnement, le cas échéant.

4.4.7 Recommandation d'actions

En fonction du domaine d'application et des objectifs, les résultats de la revue peuvent être les suivants:

- confirmation que les exigences ont été respectées;
- autorisation de passer à l'étape suivante du projet;
- recommandations en vue d'améliorations;
- actions destinées à traiter les problèmes et les risques.

Lorsque l'équipe recommande des changements, selon la portée de la revue, elle peut également intervenir dans leur mise en œuvre. Dans certains cas, l'équipe identifie des solutions alternatives aux problèmes pour les soumettre à d'autres personnes ayant la responsabilité de mettre en œuvre les actions et d'en vérifier les résultats en s'appuyant sur des personnes extérieures à l'équipe de revue.

Il convient de vérifier les recommandations afin de s'assurer qu'elles n'introduisent pas de problèmes supplémentaires.

4.5 Planification et définition de la fréquence des revues de la sûreté de fonctionnement

Les revues de la sûreté de fonctionnement peuvent améliorer en permanence la sûreté de fonctionnement d'un système dans le cadre du modèle PDCA (Plan-Do-Check-Act) décrit dans l'ISO/IEC 27000 [19]. Il peut par exemple être nécessaire d'améliorer en continu la sûreté de fonctionnement d'une entité afin de préserver un avantage commercial; l'amélioration continue des contrôles de sécurité peut également être nécessaire pour maintenir les niveaux actuels de sécurité. Un processus PDCA (Plan-Do-Check-Act) peut être appliqué à une étape unique du cycle de vie ou au cours de plusieurs étapes du cycle de vie.

Les revues de la sûreté de fonctionnement interviennent à chaque étape du cycle de vie, en particulier lors du passage d'une phase à une autre ou lors du transfert de la responsabilité d'un projet. La phase de conception constitue une étape critique pour planifier la fréquence des revues d'état. Ceci est généralement effectué pour appuyer une demande d'autorisation de poursuivre un projet ou pour permettre l'envoi d'un devis à un client. Il convient d'identifier et d'évaluer les risques comme des éléments d'entrée pour la prise de décision concernant les revues de la sûreté de fonctionnement exigées aux étapes suivantes du cycle de vie.

Idéalement, il convient d'organiser des revues techniques avant de prendre une décision pouvant s'avérer coûteuse, chronophage ou difficilement réversible. Il convient de prendre en compte les risques identifiés pour la conception et/ou le projet. De cette manière, toutes les modifications résultant d'une revue de la sûreté de fonctionnement peuvent être introduites sans impact significatif sur le calendrier ou les coûts. De plus, il peut être plus facile de faire valider des améliorations de coût, de calendrier et de performances si des revues sont organisées avant tout engagement significatif, par exemple à un moment majeur du processus de conception.

Une revue de la sûreté de fonctionnement est également déclenchée par d'autres facteurs:

- Détection des défaillances

L'apparition de défaillances qui n'ont pas été anticipées peut indiquer que l'environnement et/ou le système a évolué et que les hypothèses précédemment formulées ne sont plus valides. Il convient, au cours des revues de la sûreté de fonctionnement, d'identifier les changements à l'origine de ces défaillances et de formuler des adaptations possibles. Après des défaillances, il convient que les revues de la sûreté de fonctionnement évaluent le degré d'adéquation des actions proposées et la nécessité d'empêcher leur récurrence.

- Evolution des exigences du marché

Si l'évolution rapide des technologies, notamment dans le domaine des logiciels et des technologies de l'information, peut donner naissance à de nouveaux marchés, elle peut aussi introduire de nouvelles exigences qui n'ont pas encore été anticipées. Dans le cas d'un téléphone portable, par exemple, les exigences du marché peuvent porter non pas sur la communication vocale, mais sur un terminal informatique mobile. Une évolution des exigences du marché, pour quelque raison que ce soit, peut conduire à des exigences supplémentaires en matière de sûreté de fonctionnement, telles que l'amélioration de la sécurité ou un changement au niveau des besoins d'assistance. La réalisation de revues de la sûreté de fonctionnement au cours du cycle de vie peut contribuer à clarifier les nouvelles exigences en matière de sûreté de fonctionnement, et la gestion des évolutions au niveau des exigences du marché peut ainsi être facilitée. Les revues de la sûreté de fonctionnement fondées sur les tendances du marché et sur la satisfaction client peuvent être réalisées à la fois à des fins marketing et de sûreté de fonctionnement.

- Spécifications des systèmes concurrents

Il peut être difficile de maintenir la compétitivité des systèmes tout au long de leur cycle de vie sans modifier la spécification du système et les performances de sûreté de fonctionnement, dans la mesure où des concurrents peuvent proposer des systèmes présentant des spécifications similaires ou alternatives. Il peut donc être nécessaire d'organiser des revues comparatives avec les spécifications des systèmes concurrents afin d'atteindre les objectifs établis pendant le cycle de vie. De telles revues peuvent conduire à des améliorations du système, à des renouvellements ou à des révisions de stratégies.

- Innovation technique

L'innovation technique peut orienter les exigences en matière de systèmes vers une amélioration de la sûreté de fonctionnement. Elle peut créer des possibilités pour de nouveaux produits ou permettre l'application de nouvelles méthodes destinées à améliorer la sûreté de fonctionnement de produits existants. La sûreté de fonctionnement est soumise aux pressions exercées par les fabricants qui souhaitent commercialiser rapidement de nouveaux produits novateurs. Les revues de la sûreté de fonctionnement sont cruciales, car elles garantissent la sûreté des changements opérés et la sûreté de fonctionnement des nouveaux produits.

- **Pression sociétale autour de la sûreté de fonctionnement**

Les activités de sûreté de fonctionnement réalisées au cours du cycle de vie, notamment la planification de la sûreté de fonctionnement, la revue de conception, la croissance de la fiabilité, la maintenance, la gestion de l'obsolescence et la mise au rebut des systèmes modernes, sont soumises à des pressions sociétales. Les revues de la sûreté de fonctionnement peuvent inclure un travail de recherche continu autour des exigences de la société et de leur tendance d'évolution. La pression sociétale concernant la sûreté de fonctionnement de chaque système peut varier, dans la mesure où les exigences des parties prenantes du système diffèrent selon le type de système. Différentes caractéristiques, telles que la fiabilité, la maintenabilité, la disponibilité, la sûreté et la sécurité, peuvent également être importantes. Si cela est approprié, une liste de vérification portant sur la pression sociétale peut être mise en place, dont les résultats peuvent être répercutés sur le plan de sûreté de fonctionnement et sur les activités réalisées dans le cadre de la revue de la sûreté de fonctionnement.

Il convient d'effectuer des revues de la sûreté de fonctionnement à la fois pour traiter les problèmes détectés engendrés par ces changements et pour identifier les futurs problèmes potentiels (risques).

Le fait que ces changements interviennent tout au long du cycle de vie du système soulève des inquiétudes quant à certaines exigences, telles que la notion de responsabilité. Ces questions sont traitées non seulement au cours des revues directement déclenchées par les changements, mais également par la mise en place de revues de la sûreté de fonctionnement couvrant l'ensemble du cycle de vie du système. Ces problèmes peuvent également conduire à la nécessité d'ajuster le plan de sûreté de fonctionnement.

Le type, la fréquence et le nombre des revues dépendent de la taille et de la complexité du système, notamment de s'il s'agit:

- d'une conception simple ou d'une mise à niveau mineure;
- d'un système impliquant plusieurs systèmes;
- d'un système complexe.

Les réunions organisées dans le cadre d'une revue de la sûreté de fonctionnement sont indépendantes de celles mises en place dans le cadre de la planification, du développement et de la maintenance en continu du système.

4.6 Niveaux des revues de la sûreté de fonctionnement

4.6.1 Vue d'ensemble

Les revues de la sûreté de fonctionnement peuvent être catégorisées en fonction du niveau de la revue, lequel est déterminé par les participants et leur niveau d'implication vis-à-vis de l'objet de la revue. Ces revues sont effectuées à chaque étape du cycle de vie et peuvent être conduites au niveau de l'équipe, du projet et de l'état. Elles sont réalisées de façon hiérarchique: les revues d'équipe servent à alimenter les revues de projet, qui elles-mêmes alimentent les revues d'état.

La Figure 1 représente la relation entre les revues d'équipe, les revues de projet et les revues d'état lors d'une étape du cycle de vie.

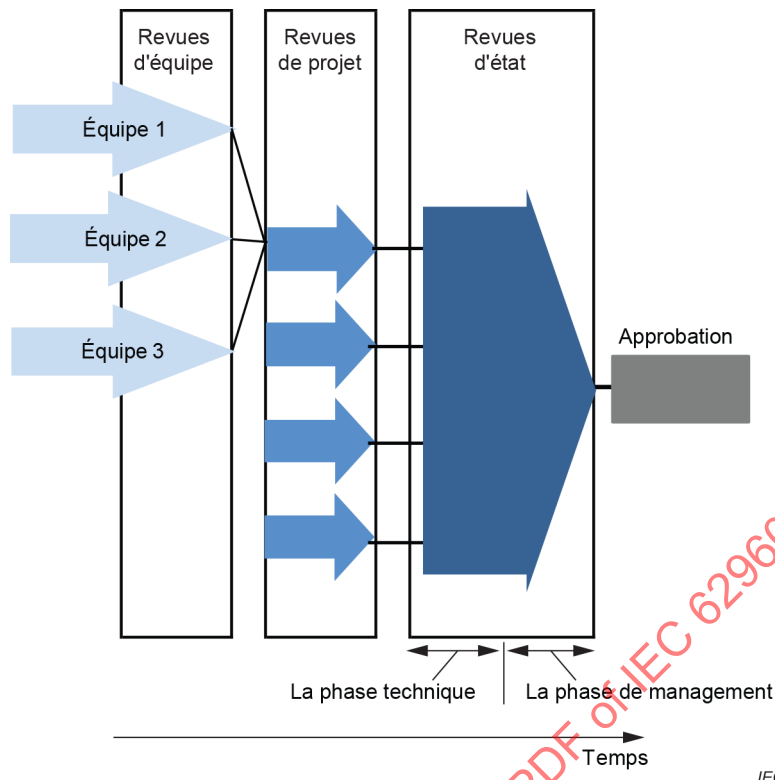


Figure 1 – Déroulement logique des revues au cours d'une étape du cycle de vie

4.6.2 Revues d'équipe

L'objectif d'une revue d'équipe est de passer en revue, sur le plan technique, les résultats de l'équipe, en se concentrant sur le rôle spécifique de l'équipe, par exemple électronique, mécanique ou logiciel. Un responsable d'équipe et au moins un membre de l'équipe participent à la revue d'équipe. Le responsable d'équipe préside la revue d'équipe. Il peut choisir de ne pas désigner de secrétaire. Le responsable utilise les informations relatives aux réalisations obtenues ainsi que les données découlant d'une analyse des écarts pour identifier les actions nécessaires de l'équipe. Il dresse également des listes de tâches afin d'affecter à chaque action les personnes compétentes et d'estimer les délais d'exécution. Les membres de l'équipe examinent ensuite leurs listes de tâches et tentent d'anticiper les problèmes ou retards éventuels. L'équipe se trouve alors en mesure d'encourager une forme d'assistance mutuelle dès que le besoin apparaît.

Le contenu d'une revue d'équipe peut faire partie d'une revue de projet et les conclusions de la revue d'équipe peuvent être utilisées comme élément d'entrée dans la revue de projet.

4.6.3 Revues de projet

Les revues de projet consistent à vérifier l'état technique d'un projet individuel associé à un programme global. Elles comprennent les données d'entrée fournies par les revues d'équipe. Le projet peut être de toute taille et une revue de projet peut être organisée à tout moment pendant le cycle de vie. Un projet peut avoir une portée importante, comme cela est généralement le cas pendant la phase de développement, ou une faible portée, ce qui peut être le cas lors de l'évaluation de la fiabilité de l'entité au cours de la phase d'utilisation. Les revues de projet servent à évaluer ce qui a été réalisé par rapport au plan du projet. Il convient de passer en revue les échéances et de surveiller les principaux livrables au moyen d'outils de management de projet appropriés et de techniques éprouvées. Participent à une revue de projet un responsable de projet et des membres du projet. Le responsable de projet préside la revue de projet. Il peut choisir de ne pas désigner de secrétaire. Les revues de projet peuvent être informelles si elles sont organisées avec le responsable de projet ou le mentor, ou être formelles si elles sont organisées avec le promoteur du projet ou le parrain du projet. Dans les

deux cas, cependant, le responsable de projet a la responsabilité d'encadrer la revue pour garantir la concrétisation des avantages recherchés. Chaque personne impliquée dans le projet doit contribuer en fonction de son impact sur les besoins et résultats du projet afin de mener la revue de projet à son terme. La conclusion de la revue de projet peut ensuite servir d'élément technique pour alimenter une revue d'état.

4.6.4 Revues d'état

Les revues d'état prennent en compte l'état global d'un projet. Elles visent normalement à informer la direction de la progression d'un projet et, dans certains cas, à débattre des risques techniques et à autoriser le passage du projet à la phase suivante du plan de projet. Il est cependant possible que le projet soit modifié, voire même interrompu, au terme d'une revue d'état.

Une revue d'état se déroule en deux phases: une phase technique qui prend en compte l'état technique du projet et une phase de management au cours de laquelle le groupe dirigeant évalue l'état technique et prend des décisions concernant les coûts, le calendrier, les risques, les perspectives et les performances. Le présent document traite uniquement de la partie technique de la revue d'état.

Les résultats des revues précédentes, y compris les recommandations et actions correctives éventuelles ainsi que toute mise à jour relative à leur mise en œuvre, sont utilisés comme données d'entrée pour les revues d'état. Il convient de répertorier l'état de tous les problèmes potentiels en indiquant un échéancier et une personne responsable pour chaque problème non résolu ou qui n'a pas été clos d'une quelconque autre manière.

Lorsque des problèmes sont identifiés au cours d'une revue de projet, il convient d'orienter la phase technique d'une revue d'état sur les solutions planifiées et mises en œuvre, sur les activités planifiées, ainsi que sur les risques technologiques résiduels du projet. Idéalement, la partie technique de la revue d'état n'identifie pas de problèmes qui n'ont pas été précédemment identifiés et analysés. Lorsqu'un problème identifié n'a pas encore été analysé, il convient de soumettre un plan d'analyse auprès de la personne responsable ainsi qu'une échéance de résultat, le tout accompagné d'une évaluation de l'impact potentiel sur le projet.

La revue d'état peut également consister à:

- analyser l'impact sur le plan de sûreté de fonctionnement et le mettre à jour en conséquence;
- vérifier si l'action nécessite une revue de l'intégralité du plan;
- autoriser/obtenir des ressources et mettre en œuvre les changements.

5 Activités impliquées dans les revues de la sûreté de fonctionnement au cours du cycle de vie

5.1 Généralités

Les cycles de vie varient selon le type, l'objet, l'utilisation et les conditions générales d'un système. Le cycle de vie peut être décrit d'une manière générale suivant plusieurs étapes:

- conception;
- développement;
- réalisation;
- utilisation;
- amélioration;
- mise hors service.

En règle générale, la sûreté de fonctionnement fait l'objet d'une revue à chaque étape. Selon le résultat de la revue, il est souvent nécessaire de répéter les revues au cours d'une même étape.

Le résultat de la revue influe sur la décision de poursuivre cette boucle ou de la quitter. Si la boucle est maintenue, le résultat de la revue sert à alimenter les activités réalisées à cette étape. Les données de sortie sont révisées, puis de nouveau examinées pour tenir compte du résultat de la revue précédente. A la sortie de la boucle, le résultat de la revue est transmis à l'activité réussie de la boucle, laquelle peut intervenir au cours de l'étape suivante du cycle de vie.

Certaines revues de la sûreté de fonctionnement sont effectuées dans des contextes plus ouverts, dans l'objectif de produire des résultats qui améliorent les activités et produits futurs de l'organisation. Le résultat de la revue effectuée lors de la phase de mise hors service, qui consiste souvent à "tirer des enseignements", est consigné dans la base de connaissances organisationnelles, utilisé dans le management du portefeuille de projets et transmis à la phase de conception du cycle de vie de la nouvelle entité, le cas échéant.

Il convient que la revue de la sûreté de fonctionnement réalisée soit de type adapté à l'étape du cycle de vie concerné. L'idéal en matière de management et de documentation est d'utiliser un plan de sûreté de fonctionnement. Si un problème est identifié au cours de la revue, quelle que soit la phase, il est important d'étudier la cause initiale du problème lors de la même phase, d'apporter des améliorations et de confirmer le résultat avec une revue technique. Il convient de transmettre les résultats des revues réalisées au cours d'une même étape du cycle de vie à l'étape suivante, le cas échéant.

Il convient que le responsable tienne compte des conditions et des contraintes imposées par une étape donnée du cycle de vie dans la planification des revues de la sûreté de fonctionnement; de même, il convient de déterminer le nombre optimal de revues, de manière à en optimiser le retour sur l'investissement en temps. Seuls quelques rares organisations ou projets ont besoin de tous les types de revues de la sûreté de fonctionnement à toutes les étapes du cycle de vie.

Les 5.2 à 5.7 ci-dessous présentent l'objectif de chaque étape du cycle de vie, les revues de la sûreté de fonctionnement qui peuvent être réalisées au cours de la phase correspondante, ainsi que les problèmes particuliers susceptibles d'être rencontrés. Des exemples d'objectifs de revues pour chaque étape du cycle de vie sont fournis en Annexe B. L'Annexe C dresse une liste générique des aspects d'une revue pouvant être pris en compte au cours des revues réelles de la sûreté de fonctionnement selon différents points de vue tout au long du cycle de vie.

5.2 Phase de conception

La phase de conception est la phase donnant une première vision de l'entité. Elle définit les exigences, les paramètres techniques et les contraintes. Des idées sont soulevées et traduites en concepts techniquement et économiquement réalisables. Une option préférentielle est retenue, compte tenu des compromis et risques potentiels. Au terme de cette phase sont produits une conception initiale pour l'option retenue et un plan de projet préliminaire comprenant un plan de sûreté de fonctionnement.

La revue comprend les activités suivantes:

- vérifier la conception compte tenu des besoins du client, des attentes et des contraintes;
- examiner la faisabilité de la conception proposée;
- examiner la faisabilité du plan de projet;
- améliorer la conception si cela est nécessaire;
- décider d'engager ou non des ressources jusqu'au développement complet.

Il convient que les revues tiennent compte des attentes au sens large en matière de sûreté de fonctionnement ainsi que de leur impact sur la conception, l'exploitation et la maintenance de l'entité. Il convient notamment de procéder à des revues d'état au terme de la phase de conception afin de s'assurer que la conception retenue pour la phase de développement satisfait aux besoins du client, aux attentes et aux contraintes. Les risques, y compris les risques de non-conformité aux exigences, sont identifiés et comparés à chaque étape suivante.

Il convient d'examiner les résultats de cette phase à une étape ultérieure du cycle de vie, à mesure que des informations complémentaires sont disponibles.

5.3 Phase de développement

5.3.1 Vue d'ensemble

La phase de développement fait suite à la celle de conception initiale, sa faisabilité ayant été vérifiée. Le but est de planifier et de mettre en œuvre les solutions de conception d'ingénierie choisies. La conception technique détaillée des solutions choisies est ensuite réalisée.

Au cours de l'étape de conception détaillée, les propriétés de tous les composants sont spécifiées et les dessins et autres documents, tels que les instructions d'exploitation, sont produits. Les besoins en maintenance et en soutien logistique sont définis.

Les risques associés à la conception choisie sont évalués plus en détail et les traitements sont spécifiés. Des techniques de modélisation et des approches probabilistes pertinentes peuvent être employées à cette étape afin prévoir de façon précise la sûreté de fonctionnement. Les prototypes (le cas échéant) sont soumis à l'essai.

5.3.2 Revues de conception

Les revues de conception sont un exemple de revues techniques qui s'intéressent plus spécifiquement à la conception d'une entité ou d'un système et vérifient que les exigences de conception ont été respectées, tout en encourageant l'amélioration de la conception.

En règle générale, une série de revues est effectuée au cours des phases de conception et de développement, sous la forme de revues de conception formelles. Une revue de conception évalue la conception compte tenu des exigences d'entrée, identifie les risques et les possibilités d'amélioration, et oriente le responsable de la conception vers les mesures appropriées. Elle accélère l'arrivée à maturité du produit en réduisant le temps nécessaire pour fixer les détails de la conception et permet la poursuite de la réalisation du produit sans interruptions fréquentes. Les revues de conception peuvent également stimuler une amélioration précoce du produit.

Correctement mises en œuvre, les revues de conception augmentent les chances de fournir un produit qui présente le niveau exigé de sûreté de fonctionnement, de qualité, de performances et de sécurité, avec la possibilité de réduire les coûts et les délais de livraison.

Le caractère atteignable du degré de sûreté de fonctionnement exigé peut dépendre de l'approche adoptée lors de la conception de l'entité, par exemple:

- s'il s'agit d'une conception personnalisée en fonction de composants et matériaux éprouvés choisis parmi l'éventail proposé;
- si la conception implique l'utilisation de composants et matériaux non éprouvés ou le recours à des sous-traitants qui n'ont pas été évalués;
- si la conception implique une interpolation de l'expérience existante;
- si la conception implique une extrapolation à partir de l'expérience existante;
- s'il s'agit d'une conception radicalement nouvelle ou de l'application d'une technologie non éprouvée.

Si la conception nécessite un prototype, il peut être indispensable de passer en revue les résultats des essais du prototype pour déterminer les activités nécessaires afin de garantir la fiabilité de la conception finale. Dans certains cas extrêmes, cela peut même aboutir à la décision, au cours d'une revue d'état, d'abandonner le projet.

Les revues de conception sont effectuées en présence d'une conception ou d'un processus préliminaire à analyser, de préférence suffisamment tôt pour faciliter l'introduction de modifications. Le coût de la correction des défauts d'une conception et les conséquences possibles augmentent à mesure que la conception est sur le point d'être finalisée. De même, il devient plus difficile au fil de l'avancement de la conception d'introduire une modification pour corriger un défaut ou optimiser la conception.

Les revues de conception peuvent avoir différents objectifs:

- déterminer si la solution proposée satisfait aux exigences d'entrée de la conception, qui peuvent inclure, entre autres: les exigences de performances générales spécifiées, la sûreté de fonctionnement, les coûts du cycle de vie, la sécurité, l'endurance, l'environnement, la compatibilité électromagnétique et les facteurs humains;
- déterminer si la solution proposée est la plus robuste, la plus efficiente et la plus efficace pour satisfaire aux exigences du produit;
- fournir si nécessaire des recommandations en vue de satisfaire aux exigences d'entrée de la conception;
- évaluer l'état de la conception du point de vue de l'exhaustivité des dessins et des spécifications;
- évaluer les preuves à l'appui de la vérification des performances de conception;
- évaluer l'état de l'application des composants pour 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;
- proposer des améliorations;
- déterminer si le produit et ses éléments peuvent être mis au rebut de façon sûre et économique;
- vérifier si les composants doivent être utilisés dans les limites de leurs caractéristiques assignées.

En règle générale, il convient d'organiser les revues de conception de la manière suivante:

- avant l'acceptation de l'ordre de conception, afin de s'assurer que le périmètre travail est établi de même que tous les paramètres qu'il est nécessaire de respecter pour aboutir à une conception acceptable;
- avant la conception détaillée, pour s'assurer que les membres de l'équipe de conception ont une connaissance préalable précise de toutes les exigences. Il convient d'établir les dispositions d'interface et de dresser une liste de documents de définition prévus pour présentation et approbation entre les parties;
- à des moments appropriés au cours de la conception détaillée, pour passer en revue toutes les dispositions d'interface et s'accorder sur les procédures d'essai afin de vérifier que la conception satisfait aux exigences du contrat et des parties prenantes;
- immédiatement avant le passage à la phase de réalisation.

Les réunions organisées dans le cadre d'une revue de la sûreté de fonctionnement sont indépendantes de celles mises en place dans le cadre de la planification, du développement et de la maintenance en continu du système.

Il convient de veiller à éviter que la revue de conception dicte les phases finales de conception et de développement du système. De nombreuses décisions peuvent affecter la sûreté de fonctionnement du système ou le processus en cours de revue. Si chaque décision fait l'objet d'une revue indépendante, l'équipe de revue devient, par nature, le concepteur ou le développeur, avec le risque d'augmenter les délais et les coûts de développement. A l'inverse, si la première revue de la sûreté de fonctionnement est intervenue juste avant la réalisation ou l'utilisation, ses avantages sont susceptibles d'être remis en question, puisqu'il est peu probable que la situation puisse être influencée, à moins d'y consacrer beaucoup de temps et/ou de l'argent.

Les revues de conception peuvent être internes ou externes. Dans le cas d'une revue externe est désignée une équipe de revue indépendante qui reçoit les présentations et les informations des personnes responsables de la conception. La composition classique d'une équipe de revue externe est décrite en 6.3.

5.4 Phase de réalisation

La phase de réalisation met en œuvre les décisions "fabriquer ou acheter" pour l'acquisition et/ou la fabrication de l'entité finale et de ses composants. La réalisation inclut les simulations de composants et de modules, l'analyse et les essais (y compris les essais d'intégration), suivis de l'installation de l'entité. Des épreuves peuvent être organisées dans l'usine réelle et/ou l'environnement d'exploitation avant la mise en service.

Afin d'identifier les problèmes pouvant survenir, les revues peuvent impliquer une comparaison des conditions de fonctionnement réelles et des caractéristiques et hypothèses utilisateur avec celles retenues au cours de la conception. Les performances de sûreté de fonctionnement obtenues sont comparées aux spécifications afin de fournir une preuve objective de la conformité. Les plans d'exploitation, tels que les plans de maintenance, qui ont été créés au cours de la phase de développement sont examinés afin de s'assurer que les tâches sont réalisables et qu'elles satisfont aux exigences relatives à l'objectif de conception.

Plusieurs revues peuvent tenir compte de la sûreté de fonctionnement:

- une revue de fournisseur destinée à vérifier la qualité des fournisseurs, les engagements concernant les délais de livraison, la capacité de traitement des commandes, l'efficacité, la politique d'approvisionnement 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 performances en matière de 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 production destinée à déterminer les exigences en matière de ressources 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. Les problèmes de sûreté de fonctionnement contribuent souvent pour une large part aux interruptions de service qui affectent la disponibilité de l'entité et, par conséquent, la production;
- une revue de lancement de produit avant la mise à disposition du produit pour livraison et/ou acceptation du client;
- une revue des informations de lancement de produit afin de s'assurer de la disponibilité des processus pour le stockage, l'installation, l'intégration, la mise en service et la maintenance appropriés.

5.5 Phase d'utilisation

Pendant la phase d'utilisation, l'entité est déployée pour remplir la ou les fonctions ou exécuter le ou les services pour lesquels elle a été conçue. Cette phase comprend diverses activités, notamment l'exploitation et la maintenance de l'entité conformément aux exigences de performances, la formation des opérateurs, la formation des agents de maintenance, la tenue de registres de performances et d'incidents de défaillance, afin d'entreprendre des actions correctives en temps opportun.

L'appréciation des risques en service et pendant les activités de maintenance peut permettre de traiter les problèmes qui surgissent en raison des conditions changeantes. La fiabilité, la disponibilité, la maintenabilité et la supportabilité peuvent être surveillées au cours d'éventuels essais de terrain à plus long terme et les résultats examinés afin de déterminer la nécessité de modifier la conception et d'améliorer les programmes de maintenance et de logistique de maintenance.

Au cours de la phase d'utilisation, les revues de la sûreté de fonctionnement peuvent prendre différentes formes, par exemple:

- une revue des opérations destinée à déterminer l'état d'intégrité et de fonctionnement d'un site de production ou d'une infrastructure de service;
- une revue de la fiabilité consistant à comparer les performances réelles aux performances attendues et à évaluer l'impact sur la disponibilité;
- une revue de maintenance et de soutien pour évaluer les performances en matière de logistique de maintenance et de soutien logistique des entités critiques, y compris les coûts, et préciser si la disponibilité et la fonctionnalité exigées sont obtenues;
- 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, la logistique de maintenance, les coûts de possession du stock et l'emplacement des entrepôts;
- une revue des risques destinée à déterminer si les risques ont changé et si le processus de management du risque est efficace;
- une revue de satisfaction client destinée à répondre aux préoccupations des utilisateurs et à élaborer des stratégies d'amélioration lorsque la sûreté de fonctionnement peut apparaître comme une priorité majeure.

Pour des entités ayant une longue durée de vie, les objectifs, les parties prenantes et les exigences peuvent évoluer au cours de la phase d'utilisation. Il convient d'effectuer des revues périodiques afin de vérifier les changements de sorte que les activités et leurs résultats continuent d'atteindre les objectifs.

5.6 Phase d'amélioration

La phase d'amélioration peut être nécessaire pour améliorer les performances de l'entité afin de satisfaire aux demandes croissantes des utilisateurs, d'allonger la durée de vie d'exploitation ou de corriger l'obsolescence (voir l'IEC 62402 [6]). Les activités peuvent inclure des mises à jour ou des 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 techniques de modélisation et les approches probabilistes pertinentes peuvent être utilisées afin d'évaluer l'impact des améliorations possibles et de choisir les meilleures solutions. L'appréciation des risques au cours de la phase d'amélioration consiste souvent à évaluer les coûts par rapport aux bénéfices et le retour sur investissement, ainsi que l'impact technique des modifications proposées.

Une revue est généralement effectuée afin d'identifier et d'évaluer les améliorations qu'il est nécessaire de mettre en œuvre. Selon l'ampleur des changements, des revues de conception, décrites en 5.3.2, peuvent être exigées lors de la conception des mises à niveau.

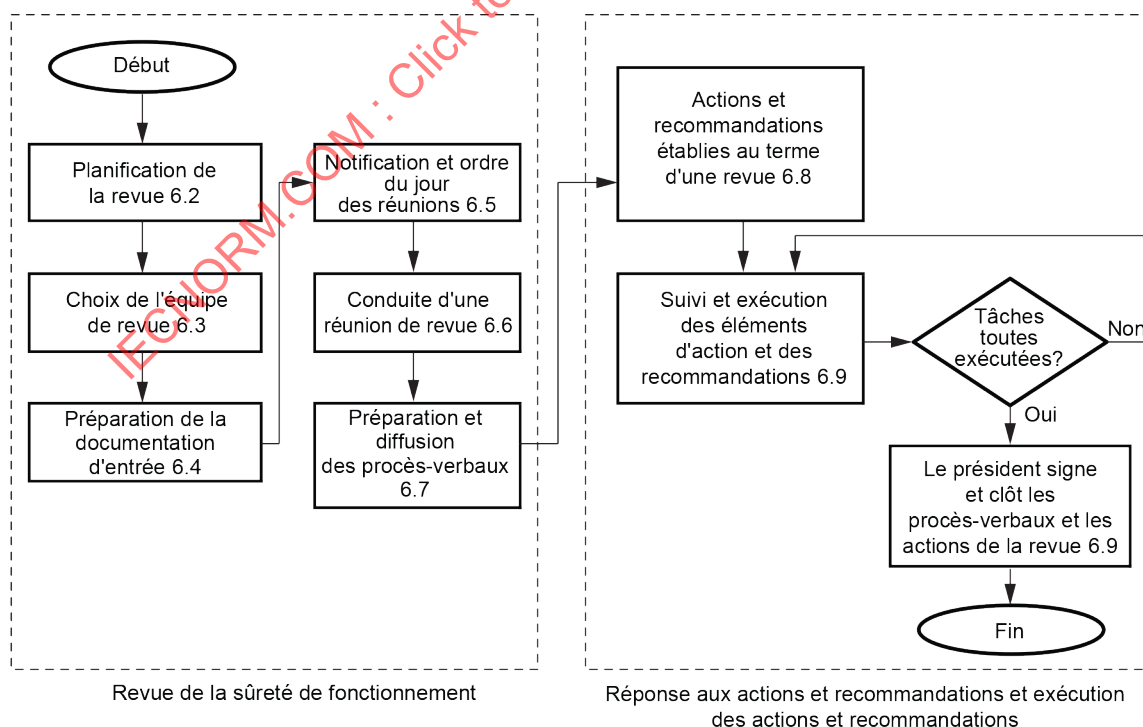
5.7 Phase de mise hors service

La phase de mise hors service intervient à la fin de la durée de vie utile d'une entité. Au terme du service d'une entité, celle-ci peut être démontée, redéployée pour d'autres utilisations, mise au rebut pour récupération des matériaux et des composants ou, dans certains cas, abandonnée sur place (un gazoduc, par exemple). Il convient de tenir compte des mesures à prendre pour la mise hors service ou la mise au rebut lors de la phase de conception. Il convient d'examiner les plans de mise hors service élaborés à une étape précédente du cycle de vie avant la mise en œuvre, de manière à prendre en compte la situation réelle. Pour les entités complexes, une stratégie de mise hors service peut 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 mise au rebut. Il peut être utile de passer en revue les enseignements tirés au cours du cycle de vie si des projets ou entités similaires sont à prendre en compte. Une exigence de mise en réserve/conservation du système pendant une période définie avant sa mise au rebut finale impose de déterminer des activités de conservation adaptées et de les appliquer pendant la période concernée. Il convient de consigner les résultats des revues effectuées lors de la phase de mise hors service, y compris les enseignements tirés, dans la base de connaissances organisationnelles, puis de les utiliser comme éléments d'entrée pour la phase de conception d'un nouveau projet, le cas échéant.

6 Mise en œuvre du processus de revue de la sûreté de fonctionnement

6.1 Généralités

Les revues de la sûreté de fonctionnement exigent une planification, une organisation et des comptes rendus soignés. L'Article 6 fournit un cadre pour la mise en œuvre du processus de revue et s'applique à la plupart des revues, sans se limiter à celles de la sûreté de fonctionnement. Les détails spécifiques dépendent de l'objet de la revue et du type de revue effectué. Le présent paragraphe s'appuie sur une revue impliquant une réunion de revue structurée. Le processus de revue est décrit à la Figure 2.



NOTE Les chiffres font référence aux paragraphes applicables du présent document.

IEC

Figure 2 – Mise en œuvre du processus de revue

6.2 Planification de la revue

La planification commence par la définition de la finalité de la revue, qu'elle soit interne ou externe, et de la portée de la revue, notamment s'il convient que l'équipe de revue formule des recommandations pour proposer des solutions à tout problème identifié ou si la finalité de la revue consiste en une simple analyse des écarts.

Les objectifs spécifiques dépendent du type de revue entrepris ainsi que du produit, système ou processus faisant l'objet de la revue. Le président clarifie les objectifs et la portée de chaque revue de la sûreté de fonctionnement en attirant l'attention sur les domaines spécifiques à couvrir et en limitant les commentaires déplacés.

6.3 Choix de l'équipe de revue

L'organisation de la revue et les positions adoptées par les personnes peuvent varier selon que la revue est menée en interne ou effectuée par une équipe de revue externe.

Une revue interne permet à une équipe ou à une équipe de projet de s'accorder des pauses pour évaluer les progrès réalisés et s'assurer que les activités et les résultats obtenus satisfont aux attentes. Une revue externe est plus formelle et fournit une évaluation indépendante donnant à l'équipe ou à l'équipe projet elle-même, à la direction ou à des parties prenantes externes une certaine garantie concernant la sûreté de fonctionnement d'une entité et les activités entreprises pour y parvenir.

Les membres de l'équipe de revue peuvent normalement inclure:

- le président;
- le secrétaire;
- des spécialistes compétents qui ne sont pas impliqués dans le développement du système faisant l'objet de la revue;
- le responsable de projet ou d'équipe et les membres de l'équipe nécessaires pour présenter le projet ou le type de revue et pour répondre aux questions.

Dans certains cas, les clients ou les utilisateurs peuvent également intégrer l'équipe.

Lorsque la finalité d'une revue est d'approuver le passage d'une étape à une autre, l'équipe de revue peut inclure les personnes habilitées à donner cette approbation.

Le responsable de projet ou d'équipe et les personnes directement impliquées ne président normalement pas les revues et il convient de désigner un président indépendant, ce qui peut se révéler plus avantageux.

Lors du choix de l'équipe de revue, il convient de veiller à éviter les conflits d'intérêts, les pensées de groupe ou les intérêts directs.

La revue peut engager des personnes ayant des connaissances et une expérience spécialisées dans différents domaines. Il convient de privilégier une composition telle que les participants, collectivement, couvrent des domaines de connaissances suffisamment larges et précis pour permettre la prise en compte de tous les aspects pertinents de la revue. Il convient de veiller à maintenir un nombre de participants raisonnable. L'Annexe D décrit les fonctions et les responsabilités de certains acteurs stratégiques d'une revue technique.

6.4 Préparation de la documentation d'entrée

Il convient de recueillir les informations pertinentes pour la revue à réaliser. Des exemples de types d'informations qu'il convient d'inclure dans la documentation d'entrée sont fournis en Annexe E.

6.5 Notification et ordre du jour des réunions

Il convient que le secrétaire, en collaboration avec le président, prépare une notification et un ordre du jour pour la réunion et qu'il les transmette aux participants ainsi qu'à leurs superviseurs, le cas échéant, suffisamment à l'avance pour permettre aux participants de préparer la réunion.

Il convient d'indiquer dans la notification et l'ordre du jour les informations suivantes:

- date, heure et lieu de la réunion;
- périmètre et objectifs de la réunion de revue;
- nom et numéro d'identification (le cas échéant) du projet;
- participants et leurs fonctions;
- type et durée de la revue de la sûreté de fonctionnement;
- équipe ou section du projet faisant l'objet de la revue, si cela est approprié;
- sujets relatifs à la sûreté de fonctionnement à couvrir (voir Annexe E);
- personnes chargées d'effectuer des présentations;
- documents de référence et contenu de toute documentation d'entrée jointe.

6.6 Conduite d'une réunion de revue

6.6.1 Généralités

Si les membres n'ont aucune expérience des revues, il convient d'organiser une session d'orientation expliquant les objectifs généraux, les principes et la pratique.

Il convient que les commentaires introductifs établissent un ton et un climat constructifs. Il convient que le président passe en revue les objectifs de la réunion et les relie aux objectifs et procédures généraux du processus de revue. Il convient que le président insiste sur la nécessité de poser des questions et d'éviter les commentaires négatifs et personnels.

Il convient d'éviter aussi les questions qui impliquent des préjugés.

Il convient que les participants se sentent libres de poser des questions à leurs homologues. Il convient qu'ils envisagent leurs responsabilités au-delà des simples questions visant à comprendre pourquoi une certaine chose a été effectuée d'une certaine manière.

Si nécessaire, il convient que les participants à la revue aient la garantie que toutes les questions soulevées, les enquêtes ultérieures demandées et les opinions exprimées ne reflètent en aucun cas la personnalité, l'aptitude ou l'intégrité d'une personne en particulier. Il convient que l'ensemble de l'équipe, sous la direction du président, veille à ce que la revue demeure proactive, objective et impartiale aussi bien au sein de l'équipe elle-même qu'auprès des autres équipes impliquées.

Il convient que les participants à une revue technique gardent toujours à l'esprit qu'ils ont un rôle consultatif et que leur objectif premier est d'aider les personnes responsables de la conception, de l'exploitation ou de la maintenance du système à atteindre un résultat optimal. Une équipe de revue technique ne fait normalement que formuler des recommandations pour proposer des solutions aux éventuelles lacunes identifiées.

6.6.2 Protocole de réunion

Le responsable concerné et les autres membres représentant l'équipe responsable ou le projet peuvent présenter, si cela est exigé, les aspects de la sûreté de fonctionnement du système examiné à l'occasion d'une revue d'équipe ou de projet.

Il convient que le président veille à ce que la présentation et les questions s'enchaînent de façon systématique et qu'un procès-verbal soit rédigé.

Le processus de revue est un jeu de questions-réponses constructif. Il convient de n'autoriser aucune question ou action désobligeante, de même qu'il convient de ne pas refuser de débattre d'un sujet à moins qu'il n'implique des problèmes spécifiques de confidentialité commerciale ou de sécurité nationale. Il convient de formuler les questions sous forme de demandes d'information ou de justification des raisons à l'appui des décisions de l'équipe ou du projet.

Les participants à la revue peuvent soumettre des questions au président à l'avance afin de lui permettre de préparer une action. Ces questions peuvent être vues comme complexes ou mineures. Pour faciliter l'évolution de la réunion, il convient si possible de clore les questions mineures avant le début de la réunion. Ces questions (et leurs réponses, si elles sont connues) sont alors intégrées à la documentation d'entrée de la réunion.

Il convient de ne pas discuter, au cours d'une revue, des erreurs typographiques ou des questions éditoriales mineures concernant les données d'entrée elles-mêmes. Il convient que le secrétaire prenne les mesures nécessaires pour les corriger. Il convient de couvrir les corrections de fond avec les participants.

Il convient que le processus de revue ne confère aucune approbation ou désapprobation des documents d'équipe ou de projet examinés.

6.6.3 Eléments d'action

Chaque fois qu'une action est exigée, il convient de consigner dans le procès-verbal de réunion la tâche, le nom de la personne ou des personnes désignées pour entreprendre cette tâche ainsi que la date de réponse. Il convient que les actions soient menées selon l'approche SMART (*Specific, Measurable, Achievable, Realistic, Time-bound*), c'est-à-dire qu'elles soient spécifiques, mesurables, réalisables, réalistes et temporellement définies.

Lorsque les éléments d'action ont été identifiés et que des recommandations ont été formulées, les aspects qu'il convient que le président prenne en compte peuvent inclure, entre autres, les suivants:

- modifications apportées à la conception, aux spécifications, aux plans et aux calendriers du système;
- impact sur les exigences de sécurité ou d'environnement, sur la qualité du système, sur la sûreté de fonctionnement, sur la fabrication, sur l'installation, sur les procédures d'exploitation et de maintenance, sur les options de support et sur les coûts.

L'équipe ayant un rôle consultatif, le responsable d'équipe ou de projet détermine la réponse réelle à tout élément d'action.

Il convient de définir la responsabilité du suivi des actions et de leurs effets.

6.6.4 Recommandations

Il convient de décrire avec précision toutes les recommandations dans le procès-verbal de la réunion et de les rapporter à la discussion initiale. Il convient, dans la mesure du possible, de consigner les raisons justifiant une recommandation. Les recommandations sont distinctes des éléments d'action, mais des actions peuvent être menées en conséquence à une date ultérieure.

6.6.5 Refus d'éléments d'action et de recommandations

Lorsque des éléments d'action résultant de revues précédentes n'ont pas été finalisés ou que des recommandations ont été rejetées, il convient d'expliquer les raisons de cette inaction ou de ce refus et de les documenter dans le procès-verbal de la réunion.

6.6.6 Conclusion de la réunion

Au terme de la réunion, il convient que le président dresse le bilan des actions et des recommandations découlant de la revue pour permettre une compréhension commune de l'équipe et atteindre un consensus.

6.7 Préparation et diffusion des procès-verbaux

6.7.1 Généralités

Les procès-verbaux de réunions ont pour but de:

- constituer un moyen de suivi des actions et recommandations;
- compléter les connaissances et l'expérience de l'organisation.

La tenue d'un registre dans lequel est consigné l'état d'une conception ou l'état d'un projet à un moment donné permet de compléter l'historique du système ou du projet. Cela peut s'avérer utile dans le cadre de la planification de conceptions et projets similaires à l'avenir. Il peut également être utile de consigner l'historique de développement d'une conception ou d'un projet pour protéger les brevets et autres droits de propriété intellectuelle ou pour protéger le système et ses processus en cas d'enquête ou de procédure judiciaire ultérieure.

Il convient de transmettre les procès-verbaux et les documents à l'appui aux membres de la revue et autres parties prenantes, le cas échéant. Il convient de conserver ces documents conformément aux procédures de gestion documentaire de l'organisation.

Il convient de transmettre les procès-verbaux de réunions non seulement aux participants de la revue, mais également au responsable de projet ou d'équipe, aux membres de l'équipe en charge de la sûreté de fonctionnement ainsi qu'à d'autres parties prenantes, le cas échéant.

6.7.2 Procès-verbaux

Le secrétaire a la responsabilité de consigner les problèmes importants, les questions et les réponses, les éléments d'action et les recommandations. Il convient d'éviter les déclarations littérales. Il convient de consigner suffisamment d'informations pour permettre l'élaboration d'un ensemble de procès-verbaux définitifs avec le degré de précision exigé.

Pour garantir un processus de revue efficace, il est nécessaire de documenter l'objet et les résultats des discussions au cours de chaque revue. Cela permet d'assurer une forme de continuité et de suivi jusqu'à ce que les décisions relatives à la sûreté de fonctionnement soient prises et que les tâches soient exécutées. Il convient d'inclure dans les procès-verbaux de réunions une documentation suffisante, de manière à éviter que les revues successives couvrent de façon répétée les mêmes problèmes et à éviter de perdre la notion ou la compréhension des problèmes pertinents. Si les efforts de continuité et de suivi sont correctement menés, l'effort de revues successives peut se concentrer sur des problèmes plus pertinents.

Il convient que les procès-verbaux contiennent les informations suivantes:

- une copie de la notification et de l'ordre du jour de la réunion;
- la liste des participants et leurs rôles;
- une identification du système ou du processus faisant l'objet de la revue, y compris les états de révision spécifiques des documents de référence;
- un récapitulatif des conclusions, un calendrier succinct des éléments d'action et, le cas échéant, les détails de la revue;
- les questions et réponses pertinentes;
- une copie de toute liste de vérification utilisée et, le cas échéant, les réponses aux questions;
- la liste des éléments d'action identifiés pour les questions non résolues;

- si une action a été attribuée, la personne à qui est confiée la responsabilité de cette action;
- si des éléments d'action ont été attribués, les dates de réalisation de ces éléments d'action;
- la liste des recommandations;
- dans le cadre d'une revue d'état, la liste des actions ou recommandations de projet prioritaires;
- dans le cadre d'une revue d'état, l'état ou la sanction établi(e) pour les éléments d'action et les recommandations au terme des réunions précédentes;
- la liste des documents de référence.

6.8 Actions et recommandations établies au terme d'une revue

Bien que de nombreuses recommandations puissent être formulées au cours d'une revue, le responsable d'équipe ou de projet est uniquement tenu d'examiner l'ensemble des recommandations et peut rejeter celles qu'il estime irréalisables. Par exemple, de nombreuses recommandations peuvent se révéler judicieuses et servir l'intérêt général de l'équipe ou du projet, mais il est possible que certaines, après un examen plus approfondi, s'avèrent non souhaitables ou peu pratiques.

Il convient que la personne chargée de déterminer la réponse à chaque action et recommandation étudie le caractère attractif et pratique des recommandations de l'équipe de revue et réponde en temps opportun. Il convient par ailleurs que cette personne:

- apporte une réponse à chacune des actions et recommandations de la réunion dans un délai convenu;
- prenne des mesures pour combler tout écart de compréhension;
- informe le président de façon formelle dès que des actions et recommandations ont été traitées et clôturées, si cela est approprié compte tenu du contexte organisationnel dans lequel est menée la revue de la sûreté de fonctionnement.

6.9 Suivi et exécution des éléments d'action et des recommandations

Le processus de revue ne s'achève que lorsque l'ensemble des éléments d'action et des recommandations qui en découlent ont été traités et exécutés selon les exigences établies.

Il convient de définir les responsabilités et les autorités compétentes pour l'exécution des éléments d'action, et il convient d'établir un budget et de préciser un échéancier. Ceci implique d'attribuer à une personne la responsabilité globale de s'assurer que les actions ont été exécutées et de clôturer la liste d'actions établie au cours de la réunion de revue de la sûreté de fonctionnement dans les délais convenus.

Lorsque toutes les actions et recommandations résultantes ont été réalisées, il convient de signer et clôturer la liste des actions et des recommandations établie dans le procès-verbal de la revue. Il convient ensuite de déposer cette liste auprès du responsable de l'organisation chargé des activités de sûreté de fonctionnement, conformément aux procédures de l'organisation.

Annexe A (informative)

Exemples de documentation d'entrée d'une revue

A.1 Phase de conception

Au cours de la phase de conception, il convient d'inclure dans la documentation d'entrée tout ou partie des informations suivantes:

- exigences initiales: ces exigences peuvent inclure la demande de devis du client, des spécifications, des normes et des exigences réglementaires ou industrielles;
- les besoins et attentes anticipés du client, établis et étayés par des études de marché et par les activités de la concurrence;
- les hypothèses d'étude conceptuelle;
- les objectifs et exigences généraux en matière de sûreté de fonctionnement;
- la base de données de fiabilité, le cas échéant;
- les exigences des parties prenantes, les exigences d'interfaces et les modifications qui peuvent exister;
- les risques anticipés faisant obstacle à la réalisation des exigences de sûreté de fonctionnement.

A.2 Phase de développement

Au cours de la phase de développement, il convient d'inclure dans la documentation d'entrée tout ou partie des informations suivantes:

- le plan de sûreté de fonctionnement;
- les hypothèses de conception documentées;
- les études et analyses d'arbitrage de conception;
- une liste de toutes les questions soulevées par l'équipe de revue concernant la conception devant faire l'objet de la revue;
- les affectations et prévisions en matière de fiabilité, de maintenabilité et de disponibilité;
- la maintenance planifiée et le soutien logistique;
- les propositions du concepteur et autres considérations, y compris les dessins et calculs;
- les informations et données relatives à des systèmes similaires;
- les données du système concurrent;
- les estimations de coûts et les justifications d'arbitrage;
- les spécifications et dessins;
- les résultats de prototypage;
- la base de données de fiabilité, le cas échéant;
- les exigences des parties prenantes, les exigences d'interfaces et les modifications qui peuvent exister;
- les objectifs de cycle de vie et les données relatives aux coûts;
- les exigences relatives aux activités de certification/d'assurance de la qualité;
- le registre/plan de management des risques du projet.

A.3 Phase de réalisation

Au cours de la phase de réalisation, il convient d'inclure dans la documentation d'entrée tout ou partie des informations suivantes:

- les études de fabrication, d'outillage et de productivité;
- l'état du processus de fabrication;
- l'état des décisions "fabriquer ou acheter";
- l'état des programmes de sûreté de fonctionnement et de qualité du fournisseur;
- les rapports, analyses et exigences des essais de performances;
- les analyses de contrôle qualité des processus et fournitures;
- les rapports d'inspection;
- les rapports de qualité des entités achetées ou fournies;
- la base de données de fiabilité, le cas échéant;
- les exigences des parties prenantes, les exigences d'interfaces et les modifications qui peuvent exister;
- l'état d'avancement de l'installation;
- les exigences relatives aux activités de certification/d'assurance de la qualité.

A.4 Phase d'utilisation

Au cours de la phase d'utilisation, il convient d'inclure dans la documentation d'entrée tout ou partie des informations suivantes:

- les données de disponibilité et d'indisponibilité en production ou en exploitation;
- les rapports et tendances de défaillance ou dysfonctionnement sur site et de non-conformité;
- les données de supportabilité pour les éléments de la logistique de maintenance, telles que les interruptions dues aux retards d'approvisionnement en ressources, par exemple pièces de rechange, personnel qualifié et équipement de soutien;
- les coûts de maintenance;
- les incidents de sécurité liés à une défaillance du système ou de l'équipement;
- les résultats et les recommandations obtenus à partir des analyses des causes initiales;
- les tâches de maintenance en cours;
- la disponibilité des pièces de rechange, en particulier pour les entités critiques;
- la comparaison entre la fiabilité prévue et réelle;
- la comparaison entre la maintenabilité prévue et réelle;
- la base de données de fiabilité, le cas échéant;
- les exigences des parties prenantes, les exigences d'interfaces et les modifications qui peuvent exister;
- la comparaison entre la supportabilité prévue et réelle;
- le registre/plan de management des risques du projet.

A.5 Phase d'amélioration

Au cours de la phase d'amélioration, la documentation d'entrée est similaire à celle de la phase de développement et il convient d'y inclure tout ou partie des informations suivantes:

- les hypothèses de conception documentées;

- les études et analyses d'arbitrage de conception;
- une liste de toutes les questions soulevées par l'équipe de revue concernant la conception devant faire l'objet de la revue;
- les affectations et prévisions en matière de fiabilité, de maintenabilité et de disponibilité;
- la maintenance planifiée et le soutien logistique;
- les propositions du concepteur et autres considérations, y compris les dessins et calculs;
- les estimations de coûts et les justifications d'arbitrage;
- la base de données de fiabilité, le cas échéant;
- les exigences des parties prenantes, les exigences d'interfaces et les modifications qui peuvent exister;
- les spécifications et dessins;
- le registre/plan de management des risques du projet.

A.6 Phase de mise hors service

Au cours de la phase de mise hors service, il convient d'inclure dans la documentation d'entrée tout ou partie des informations suivantes:

- toute exigence relative à une mise en réserve/conservation provisoire;
- la stratégie de mise hors service et de mise au rebut;
- l'influence de la mise au rebut des entités sur l'environnement;
- l'impact de la fin du service;
- la base de données de fiabilité, le cas échéant;
- les exigences des parties prenantes, les exigences d'interfaces et les modifications qui peuvent exister;
- le calendrier et la date de fin de service, ainsi que les offres de services nouveaux ou alternatifs;
- le registre/plan de management des risques du projet.

Annexe B (informative)

Exemples d'objectifs des revues de la sûreté de fonctionnement au cours du cycle de vie

B.1 Généralités

L'Annexe B répertorie les objectifs possibles à atteindre dans le cadre des revues de la sûreté de fonctionnement, à différentes étapes du cycle de vie. Le cycle de vie utilisé est un modèle générique et l'application réelle peut exiger un ensemble de phases différent. Certains points ci-dessous sont associés à des revues techniques et d'autres à des revues de management.

NOTE L'Annexe E répertorie des sujets spécifiques autour des attributs de base de la sûreté de fonctionnement et des questions associées.

B.2 Phase de conception

Les objectifs d'une revue de conception peuvent inclure la nécessité:

- d'évaluer si des exigences du client ont été identifiées et clarifiées, si nécessaire;
- d'évaluer si les exigences réglementaires applicables ont été identifiées;
- d'évaluer si d'autres exigences techniques ont été incluses dans les données d'entrée de la conception;
- d'évaluer si les interfaces organisationnelles et techniques ont été identifiées;
- d'évaluer si les risques associés à la conception ont été appréciés.

B.3 Phase de développement

B.3.1 Revue d'étude conceptuelle

Les objectifs d'une revue d'étude conceptuelle peuvent inclure la nécessité:

- d'interpréter, d'évaluer et de s'accorder sur les exigences, les besoins et les attentes du client, ainsi que sur les exigences relatives au produit;
- d'établir les exigences obligatoires, y compris les exigences réglementaires et du code, et de définir les caractéristiques souhaitables et facultatives;
- d'évaluer la communication entre les membres de l'équipe de projet responsables de la conception, des ventes, de la fabrication, des essais, de l'inspection, de l'installation, de l'exploitation, de la maintenance, de la mise au rebut, etc.;
- d'examiner les conditions et les technologies actuellement disponibles afin de satisfaire aux exigences du client et du marché, ainsi qu'aux exigences d'environnement et de sécurité;
- de passer en revue les informations relatives aux performances, à l'exploitation et aux responsabilités, obtenues soit à partir de registres de terrain constitués par l'organisation pour des produits similaires, soit auprès de l'industrie;
- de réviser les plans et calendriers de développement et de conception;
- d'évaluer les concepts proposés pour la conception.

B.3.2 Revue de conception détaillée

Les objectifs d'une revue de conception détaillée peuvent inclure la nécessité:

- de vérifier que la conception proposée continue de satisfaire aux exigences initiales du produit;

- de confirmer que les actions et recommandations définies au cours de la ou des revues précédentes ont été évaluées, traitées et clôturées;
- d'examiner les résultats des analyses, calculs et essais;
- d'évaluer la rentabilité du produit proposé;
- de s'assurer que le produit fonctionne comme prévu;
- d'évaluer si le produit proposé peut être fabriqué, inspecté, assemblé avec les tolérances adéquates, stocké, expédié et installé de manière fiable et, le cas échéant, mis au rebut en toute sécurité, de façon réglementaire et à moindres coûts;
- de passer en revue de la documentation justificative présentant en détail l'expérience et les données utilisées pour le développement du produit;
- d'évaluer la conception du système, l'isolement des fonctions (par exemple, diagramme de fiabilité – voir l'IEC 61078 [11]) et les interfaces entre les modules;
- d'examiner l'application des composants pour 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;
- d'établir une échelle hiérarchique des caractéristiques telles que les coûts, les performances, les paramètres physiques, la sûreté de fonctionnement, les contraintes environnementales, les exigences de livraison et les incitations contractuelles, à partir desquelles des décisions d'arbitrage peuvent être prises pour établir les caractéristiques obligatoires, souhaitables et facultatives.

B.3.3 Revue de conception finale

Les objectifs d'une revue de conception finale peuvent inclure la nécessité:

- de vérifier que la conception finale reflète les exigences initiales de la conception;
- de confirmer que les actions et les recommandations définies au cours de la ou des revues précédentes ont été évaluées, traitées et clôturées;
- d'évaluer si les enseignements tirés d'autres projets/conceptions qui ont été retenus ont permis d'améliorer efficacement la conception;
- de passer en revue les enseignements tirés d'autres projets/conceptions qui n'ont pas été retenus, de confirmer les raisons à cela et de vérifier les mesures d'atténuation mises en place pour traiter les problèmes;
- de s'assurer que des analyses, calculs et essais détaillés ont été réalisés et que la documentation relative à la fabrication, à la sécurité, à l'installation, à l'exploitation et à la maintenance du produit a été produite sous une forme exploitable;
- d'évaluer la rentabilité de la conception finale sur l'ensemble de son cycle de vie;
- de vérifier que la conception finale peut être fabriquée, inspectée, assemblée avec les tolérances adéquates, stockée, livrée et installée de manière fiable et, le cas échéant, mise au rebut en toute sécurité, de façon réglementaire et à moindres coûts, et qu'elle fonctionne comme prévu;
- d'assurer la livraison, la compatibilité, la qualité et la sûreté de fonctionnement des composants achetés;
- de passer en revue la documentation justificative présentant en détail l'expérience et les données utilisées pour la conception;
- d'évaluer l'exhaustivité du jeu de dessins, des codes logiciels et des spécifications de conception ainsi que leur applicabilité au produit au processus prévu;
- de vérifier qu'une étude adéquate a été menée avant d'adopter et d'intégrer dans la conception les recommandations acceptées à l'issue des revues de conception précédentes;
- de tirer des enseignements pour la conception future, de les justifier ou de consigner les mesures d'atténuation pour toutes les entités identifiées qui n'ont pas été intégrées.

B.4 Phase de réalisation

Les objectifs d'une revue de réalisation peuvent inclure la nécessité:

- de vérifier la qualité des fournisseurs, les engagements concernant les délais de livraison, l'efficacité du traitement des commandes, la politique d'approvisionnement et la gestion de la chaîne d'approvisionnement;
- d'examiner les risques associés à l'utilisation à la lumière des conditions de fonctionnement réelles;
- de déterminer l'état de non-conformité de la qualité, l'efficacité de l'assurance et les tendances de performances en matière de qualité, d'identifier les domaines d'amélioration et de préconiser des actions de gestion;
- de s'assurer que les processus de vérification et de validation appropriés, et si nécessaire les activités de certification et/ou d'assurance de la qualité, ont bien été réalisés;
- de comparer les performances de sûreté de fonctionnement obtenues avec les spécifications établies pour fournir une preuve objective de la conformité aux spécifications;
- de passer en revue les plans de maintenance qui ont été créés au cours de la phase de développement afin de s'assurer que les tâches sont réalisables et qu'elles satisfont aux exigences relatives à l'objectif de conception.

B.5 Phase d'utilisation

B.5.1 Exploitation

Les objectifs d'une revue d'exploitation peuvent inclure la nécessité:

- de surveiller les problèmes de fiabilité, de disponibilité et les problèmes de sûreté de fonctionnement associés, dans le but d'identifier la nécessité de modifier la conception;
- de surveiller les défaillances et non-conformités ainsi que les tendances des mesures de sûreté de fonctionnement;
- de passer en revue la production pour déterminer les exigences en matière de ressources et les calendriers de livraison, la capacité de production et le flux associé, l'externalisation et la sous-traitance de tâches de production, l'outillage, l'assemblage, le contrôle du matériel et les activités d'essai;
- de déterminer l'état d'intégrité et de fonctionnement d'une organisation, d'une subdivision, d'un site de fabrication ou d'une infrastructure de service;
- de comparer la fiabilité réelle par rapport aux performances attendues et d'évaluer l'impact sur la disponibilité;
- d'examiner la satisfaction client afin de répondre aux préoccupations des utilisateurs et d'élaborer des stratégies d'amélioration lorsque la sûreté de fonctionnement peut apparaître comme une priorité majeure.

B.5.2 Maintenance

Les objectifs d'une revue de maintenance peuvent inclure la nécessité:

- de surveiller la fiabilité, la maintenabilité, la supportabilité et la disponibilité en tant que caractéristiques et tendances de sûreté de fonctionnement de manière à identifier la nécessité de modifier la conception pour améliorer les programmes de maintenance et de soutien logistique;
- d'évaluer les performances en matière de logistique de maintenance et de soutien logistique des entités critiques, y compris les coûts;